Tampereen ammattikorkeakoulu

Virtuaalivaluuttojen riskienhallinta rahanpesun estämisen näkökulmasta

Työkalut virtuaalivaluuttojen riskienhallintaan

Markus Makkonen

OPINNÄYTETYÖ

Marraskuu 2023

Liiketalous
Taloushallinto

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden tutkinto-ohjelma
Taloushallinto

MAKKONEN, MARKUS:
Virtuaalivaluuttojen riskienhallinta rahanpesun estämisen näkökulmasta

Opinnäytetyö 56 sivua, joista liitteitä 2 sivua
Marraskuu 2023

Tämän opinnäytetyön tärkeimpänä tavoitteena oli selvittää, miten virtuaalivaluuttoja käytetään osana rahanpesua, sekä miten finanssialan toimijat voivat minimoida asiakkaidensa virtuaalivaluuttojen käytöstä muodostuvia riskejä. Opinnäytetyössä tutkittiin virtuaalivaluuttojen tekniikkaa ja tavallisimpia rahanpesun toimintatapoja, ja miten rikolliset voivat hyödyntää virtuaalisten valuuttojen erityispiirteitä omaksi edukseen.

Opinnäytetyön toteuttamisessa hyödynnettiin laajasti alan julkaisuja ja tutkimuksia, sekä kansallisten ja kansainvälisten rahanpesun estämisen toimijoiden raportteja. Tutkimus keskittyi virtuaalivaluuttojen teknisiin ominaisuuksiin, jotka mahdollistavat niiden käytön rahanpesussa. Erityisesti keskityttiin siihen, miten rikolliset voivat hyödyntää näiden valuuttojen epätavallisia ominaisuuksia verrattuna perinteisiin valuuttoihin pyrkiessään piilottamaan laittomasti hankittuja varojaan.

Opinnäytetyön tärkeimpänä tuloksena huomattiin virtuaalivaluuttojen käytön olevan hankalaa huomata perinteisen talousjärjestelmän puolelta, ja virtuaalivaluuttojen liikkeiden ymmärtäminen vaatii huomattavia panostuksia datan keräämiseen ja sitä tukevien ohjelmistojen tuottamiseen. Tämän haasteen voittamiseksi tarvitaan yhteistyötä sääntelyviranomaisten, teknologisten innovaatioiden ja finanssialan toimijoiden välillä. Lisäksi finanssialan toimijoiden on tärkeää huomata asiakaskuntansa virtuaalivaluuttojen käyttö ja ottaa se huomioon asiakkaan tuntemistietoja kerättäessä ja riskiarviota muodostettaessa.

Tässä opinnäytetyössä käsitellään myös virtuaalivaluuttojen tulevaisuutta osana kansainvälistä maksuliikennettä, ja miten teknologiset kehitysaskeleet ja keskuspankkien liikkeelle laskemat virtuaalivaluutat voivat vaikuttaa nykyisten valuuttojen suosioon.

Asiasanat: rahanpesun estäminen, virtuaalivaluutat, asiakkaan tunteminen

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Administration
Financial Administration

MAKKONEN, MARKUS:
AML Risk Management for Virtual Currencies

Bachelor's thesis 56 pages, appendices 2 pages
November 2023

The main objective of this thesis was to investigate the use of virtual currencies in money laundering and explore how financial sector entities could minimize the risks arising from customers' use of virtual currencies. This thesis examined the technology behind virtual currencies, common money laundering techniques, and how criminals exploit the features of the virtual currencies to their advantage.

A wide selection of AML publications and studies, as well as reports of national and international money laundering preventing entities were used in this thesis. This thesis focused on virtual currencies technical characteristics that enable their use in money laundering, especially how these currencies differ from the regular currencies to conceal illegally acquired funds.

The primary finding of this thesis was that detecting the use of virtual currencies is challenging from the perspective of the traditional financial system, and comprehending virtual currency transactions requires substantial efforts in data collection and the development of supporting software. Overcoming this challenge requires collaboration among regulatory authorities, technological innovations, and financial sector entities. Additionally, it is crucial for financial sector entities to recognize their customer base's use of virtual currencies and consider it when performing customer due diligence and making risk assessments.

This thesis also addresses the future of virtual currencies in international payment systems and how technological advancements and central bank-issued digital currencies may influence the popularity of existing virtual currencies.

Key words: anti-money laundering, virtual currency, know-your-customer

SISÄLLYS

LYHENTEET JA TERMIT

BKT	Bruttokansantuote
CBDC	engl. Central Bank Digital Currencies, keskuspankkien liikkeelle laskemat digitaaliset valuutat
CEX	engl. Centralized Exchange, keskitetty markkinapaikka
DEX	engl. Decentralized Exchange, hajautettu markkinapaikka
FATF	engl. The Financial Action Task Force, OECD:n alainen toimintaryhmä taloudellisen yhteistyön kehittämiseksi
FIAT	Keskuspankin liikkeelle laskema valuutta, jota ei ole taattu millään hyödykkeellä, kuten kullalla tai hopealla
KYC	engl. Know-Your-Customer, asiakkaan tuntemisen tiedot
ODD	engl. Ongoing-Due-Diligence, jatkuva asiakkaan tunteminen
P2P	Peer to Peer, vertaisverkko, jossa osapuolet yhdistävät suoraan toisiinsa, ilman kolmannen osapuolen palveluita
PEP	engl. Politically exposed person, poliittisesti vaikutusvaltainen henkilö
PoS	engl. Proof-of-Stake, konsensusmetodi, jossa verkon validaattorit saavat äänivaltaa konsensuksen luomisessa virtuaalivaluuttojen omistuksen suhteella
PoW	engl. Proof-of-Work, konsensusmetodi, joka todistaa osapuolen käyttäneen energiaa salausavaimen muodostamiseen
RBA	engl. Risk-based Approach, riskiperusteinen lähestymistapa
RCA	engl. Relative or Close Associate, poliittisesti vaikutusvaltaisen henkilön perheenjäsen tai yhtiökumppani
SAR	engl. Suspicious Activity Report, ilmoitus epäilyttävästä liiketoimesta

TM	engl. Transaction Monitoring, liiketapahtumien seuranta
UBO	engl. Ultimate Beneficial Owner, tosiasiallinen edunsaaja

1 JOHDANTO

Virtuaalivaluutat ovat digitaalisia valuuttoja, joita käytetään ostosten tekemiseen sekä omaisuuden siirtämiseen perinteisen rahan tapaan. Niitä kutsutaan myös kryptovaluutoiksi, sillä niiden arvo perustuu osittain kysynnän ja tarjonnan lakiin, sekä erityisesti algoritmien säätelemään rajoitettuun tarjontaan. Tunnetuimpia ja suurimpia virtuaalivaluuttoja ovat Bitcoin, Ethereum, Litecoin ja Ripple. Niiden arvoa ei ole sidottu mihinkään fyysiseen omaisuuteen tai valuuttaan. Toisin sanoen ne eivät ole keskuspankin liikkeelle laskemia eikä laillisia maksuvälineitä, ja toimivat perinteisen rahoitusmaailman ulkopuolella.

Virtuaalivaluuttoja ei tule sekoittaa keskuspankkien liikkeelle laskemaan sähköiseen rahaan. Nykyään käteisen osuus liikkuvasta rahasta on häviävän pieni ja suurin osa maailman rahaliikenteestä tapahtuu digitaalisesti tietoverkkojen välityksellä. Yksinkertaistetusti keskuspankit luovat sähköistä rahaa osana rahapolitiikkaansa lainatessaan sitä liikepankeille. Liikepankit taas luovat rahaa lainatessaan rahaa asiakkailleen, jolloin asiakkaan velka pankille sekä asiakkaan saamiset pankilta (asiakkaan raha tilillä) kasvaa yhtä paljon. Tätä koko järjestelmää pitää pystyssä keskuspankit, joiden tehtävä on varjella taloudellista vakautta. Sähköiset rahat, kuten myös käteinen, ovat esimerkkejä keskitetystä valuutoista. Keskitetyt valuutat ovat yhden tai muutaman tahon hallitsemia ja ohjaamia, eivätkä ne usein tarjoa minkäänlaista läpinäkyvyyttä rahan liikkeistä. Emme esimerkiksi tiedä kuinka paljon naapurillamme on tilillä rahaa, tai missä hän sitä käyttää.

Virtuaalivaluutat toimivat täysin erilaisesti. Virtuaalivaluuttoja ei hallinnoi yksittäinen taho, vaan koko järjestelmä on hajautettu useille toimijoille, ja toimintaan voi kuka vain osallistua. Vaikka virtuaalivaluutat ovat myös nimellisesti sähköistä rahaa, sen toimintamalli on hyvin erilainen perinteisiin FIAT-valuuttoihin verrattuna. Virtuaalivaluuttojen arvo perustuu niiden hyödyntämään kryptografiseen lohkoketjuun. Lohkoketju on eräänlainen digitaalinen kirjanpitomuoto, jossa kaikki virtuaalivaluuttojen transaktiot liitetään kronologiseen tapahtumaketjuun. Tämä ketju estää aikaisempien lohkojen muuttamisen, ja tekee virtuaa-

livaluuttojen tapahtumien väärentämisestä käytännössä mahdotonta. Virtuaalivaluuttojen hallinta on hajautettu kymmenille tuhansille tietokoneille, jotka varmistavat, että useimmat osallistujat verkossa ovat samaa mieltä tapahtumien oikeellisuudesta ennen kuin ne lisätään lohkoketjuun. Virtuaalivaluutat eivät vaadi esimerkiksi valuutan siirrossa rahan siirtyvän ensin pankista toiseen, vaan varat siirtyvät suoraan käyttäjien digitaalisista lompakoista toiseen, ilman kolmatta osapuolta. Virtuaalivaluuttojen enimmäismäärä on useimmiten myös rajattu, toisin kuin FIAT-valuutoilla, jossa keskuspankki voi laskea rahaa liikkeeseen tai rajoittaa rahan saantia. Esimerkiksi Bitcoineja voi olla olemassa maksimissaan 21 miljoonaa kappaletta, ja tämä rajallisuus voi auttaa säilyttämään tai jopa lisäämään sen arvoa ajan mittaan.

Samalla kun virtuaalivaluuttojen käyttö kaupankäynnissä, sijoittamisessa ja rahan siirrossa on ollut voimakkaassa kasvussa viimeisen kymmenen vuoden aikana, ovat ne myös aiheuttaneet uuden ongelman maailmanlaajuiselle talousrikollisuuden estämistyölle. Virtuaalivaluuttoihin ja lohkoketjuteknologiaan liittyvät teknologiset mullistukset ovat tehneet rahan liikkeen ja käytön seuraamisesta entistä hankalampaa talousrikollisuutta vastaan toimiville tahoille. Tämän vuoksi finanssialan toimijat ovat nopeasti joutuneet muuttamaan ja tehostamaan toimintamallejaan. Virtuaalivaluuttoja pidetään rahanpesun näkökulmasta merkittävän riskialttiina tuotteena.

Rahanpesulla tarkoitetaan rikollisia toimia, joilla pyritään peittämään laittomasti hankitun omaisuuden alkuperä ja saamaan laittomat varat näyttämään laillisilta. Rahanpesu on laaja ongelma, joka vaikuttaa kansainvälisesti ja joka liittyy vahvasti erilaisiin rikollisiin toimintoihin, kuten huumekauppaan, ihmiskauppaan ja terrorismiin. Varojen alkuperää pyritään häivyttämään monimutkaisilla rahansiirtotavoilla, jotka tekevät varojen alkuperän selvittämisen vaikeaksi.

Rahanpesun torjuntaan on laadittu kansainvälisiä lakeja ja sääntöjä, joiden tarkoituksena on estää rikollisten varojen pääsy lailliseen talousjärjestelmään. Esimerkiksi pankit ja muut rahoituslaitokset ovat velvollisia noudattamaan sääntöjä ja direktiivejä, joiden avulla pyritään tunnistamaan rahanpesu ja estämään laittomat rahaliikenteet.

Virtuaalivaluuttojen käyttö rahanpesussa avaa uusia pulmia rahanpesua vastaan taisteleville tahoille. Virtuaalivaluuttojen käyttäminen, siirtäminen ja kuljettaminen on nopeaa, edullista ja mahdollisesti anonyymiä. Ne käyttäytyvät hyvin samaan tapaan kuin käteinen, mutta osa ominaisuuksista vastaa pankkien tilisiirtoja. Virtuaalivaluuttojen käyttöön liittyvät regulaatiot ovat tiukentuneet huomattavasti FATF:n (The Financial Action Task Force) ja EU:n AMLD5 ohjeistusten ja direktiivien seurauksena.

Tämän opinnäytetyön tavoitteena on selvittää ja tutkia, miten yleisimpiä virtuaalivaluuttoja voidaan käyttää rahanpesun välineenä. Tavoitteena on ymmärtää virtuaalivaluuttojen erityispiirteitä, jotka tekevät niistä houkuttelevia rikollisille käyttää osana rahanpesuketjua. Työssä analysoidaan myös erilaisia rahanpesun menetelmiä ja tekniikoita, joita käytetään digitaalisten varojen kanssa.

Opinnäytetyön toinen keskeinen tavoite on selvittää, miten finanssialan toimijat voivat torjua ja vähentää asiakkaidensa virtuaalivaluuttojen käytöstä johtuvia rahanpesun riskejä. Opinnäytetyössä käsitellään erityisesti asiakkaan tuntemistietojen, riskiperusteisen arvioinnin sekä liiketoimien tutkimisen merkitystä asiakkaasta nousevien riskien minimoinnissa. Lisäksi tarkastellaan, miten nykyiset rahanpesun vastaiset lait ja säännökset vaikuttavat virtuaalivaluuttojen käyttöön ja finanssialan vaatimuksiin.

Opinnäytetyön kolmantena tavoitteena on hahmottaa, millainen rooli virtuaalivaluutoilla saattaa olla tulevaisuuden maailmanlaajuisessa rahaliikenteessä. Tässä osassa tutkitaan kryptovaluuttojen haasteita ja mahdollisuuksia tulevina vaihtoehtoisina maksuvälineinä.

Tämän opinnäytetyön tarkoitus on tuottaa helposti ymmärrettävä ja käyttöönotettava tietopaketti eri finanssipalveluiden asiakkaiden virtuaalivaluuttojen käytön riskien hallintaan osana rahanpesua estäviä prosesseja. Tällaisia finanssipalveluiden tarjoajia ovat esimerkiksi pankit, tilitoimistot, kirjanpitäjät, perintätoimijat ja oikeudelliset toimijat sekä muut mahdollisesti tulevaisuudessa virtuaalivaluuttojen kanssa tekemisiin joutuvat tahot. Riskien hallinnassa käsitellään esimerkiksi eri virtuaalivaluuttatoimijoiden aiheuttamia riskejä, eri virtuaalivaluuttojen tekniikoiden aiheuttamia riskejä sekä millaisia riskejä itse asiakas aiheuttaa

virtuaalivaluuttojen käytöllään.

Opinnäytetyön teoriaosuudessa tarkastellaan lohkoketjujen tekniikkaa ja toimintamalleja erityisesti rahanpesun estämisen näkökulmasta, sekä virtuaalivaluuttojen säätelyyn liittyviä direktiivejä ja käytännön rahanpesutapahtumia. Opinnäytetyön loppupuolella kerrotaan tarkemmin, millaisilla käytännön toimenpiteillä finanssialan toimijat voivat hallita asiakkaidensa virtuaalivaluuttojen käyttöön liittyviä rahanpesun riskejä.

Tulevaisuudessa keskuspankkien luomat lohkoketjut ja virtuaalivaluutat ovat mahdollinen korvike nykyiselle rahajärjestelmälle. Opinnäytetyössä tutkitaan myös, miten lohkoketju voisi hyödyttää globaalia rahanpesun estämistyötä sekä taistelua talousrikollisuutta vastaan.

Opinnäytetyön aihe valittiin rahanpesun toimintatapojen mielenkiintoisuuden ja lohkoketjuteknologian tarjoamien hyötyjen ja haittojen vuoksi. Aihe on ajankohtainen, sillä virtuaalivaluuttojen käyttäjämäärät ja käyttökohteet ovat olleet kasvussa useiden vuosien ajan, ja käyttö tulee myös varmasti tutummaksi yhä suuremmalle yleisölle lähitulevaisuudessa. Tämän vuoksi taloustoimijoiden on hyvä varautua etukäteen muuttuviin sääntelyihin sekä kasvavaan käyttäjäkuntaan, ja sen seurauksena arvioida ja kehittää omia riskimallejaan.

Opinnäytetyö toteutettiin ilman toimeksiantajaa. Finanssialan toimijat ovat hyvin suojelevaisia omista talousrikollisuuden estämiseen liittyvistä prosesseistaan, eikä näitä haluttu saattaa julkisesti saataville. Työn aineistona käytetään alan kirjallisuutta, tutkimuksia, viranomaisten julkaisuja sekä muita relevantteja lähteitä.

2 VIRTUAALIVALUUTAT

2.1 Bitcoin ja muut virtuaalivaluutat

Virtuaalivaluutoilla tarkoitetaan digitaalisessa muodossa olevia valuuttamaisia vaihdannan välineitä. Ne muodostavat uudenlaisen tavan siirtää arvoa ilman perinteisiä keskitettyjä rahoituslaitoksia tai valvontaelimiä digitaalisesti internetin välityksellä. Virtuaalivaluuttojen perusidea on tarjota digitaalinen arvonsäilytys- ja siirtojärjestelmä, joka on turvallinen, hajautettu ja avoin kaikille. Lohkoketjuteknologia mahdollistaa jokaisen valuuttasiirron tallentamisen lohkoon, ja uusi lohko liitetään aikajärjestyksessä edelliseen. Tämä takaa siirtojen luotettavuuden ja estää niiden manipuloimisen tai väärentämisen. Lisäksi virtuaalivaluutat käyttävät monimutkaisia salausalgoritmeja suojaaman käyttäjien yksityisyyttä.

Bitcoinia pidetään maailman ensimmäisenä ja tunnetuimpana virtuaalivaluuttana. Se syntyi "Satoshi Nakamoto" -nimellä esiintyneen henkilön tai ryhmän luomana vuonna 2008, ja se julkaistiin käyttöön vuonna 2009. Bitcoin toimii usein yleisnimityksenä kaikille virtuaalivaluutoille, vaikka todellisuudessa se on vain yksi tuhansista nykyisin toiminnassa olevista virtuaalivaluutoista. Bitcoinin suosio kasvoi aluksi pienissä teknologiayhteisöissä, ja se tunnettiin lähinnä harrastajien ja kryptovaluuttaan erikoistuneiden toimijoiden keskuudessa. Kuitenkin vuosien varrella Bitcoin alkoi saada lisää huomiota ja mediajulkisuutta sen arvon kasvaessa. Bitcoinista tuli ensimmäinen kryptovaluutta, joka herätti laajempaa kiinnostusta ja hyväksyntää.

Vuonna 2023 käytössä olevia virtuaalivaluuttoja arvioidaan olevan noin 23 tuhatta kappaletta. Virtuaalivaluuttojen kokonaismarkkina-arvo on noin 1 biljoonaa Yhdysvaltain dollaria, josta Bitcoin edustaa noin puolta. (Coinmarketcap.com n.d.)

Virtuaalivaluuttojen tärkeimpinä etuina perinteiseen valuuttaan verrattuna pidetään sen hajautettua toimintaa sekä nopeita kansainvälisiä rahansiirtoja. Virtuaalivaluutat tarjoavat pankkipalveluita vastaavat palvelut myös sellaisille ihmisille,

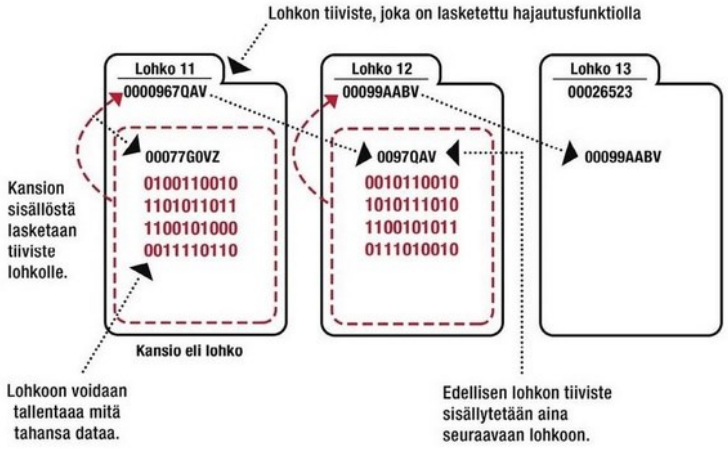
jotka eivät muuten pääse perinteisen talousjärjestelmän piiriin. Selkeinä haittapuolina ovat virtuaalivaluuttojen heikohko sääntely, nopeat arvonmuutokset sekä rikollisuuden hyötyminen virtuaalivaluuttojen osittaisesta anonymiteetistä.

2.2 Lohkoketju

Lohkoketju on tullut tunnetuksi pääasiassa Nakamoton ”Bitcoin: A Peer-to-Peer Electronic Cash System” -julkaisun (2008) jälkeen, mutta itse lohkoketjuteknologia on kehitetty paljon aikaisemmin, jo vuonna 1982 (Kriptomat.io n.d).

D.L.Chaum (1979) kirjoitti väitöskirjan kryptografian ja ”useiden epäilyttävien tahojen” yhteistyöllä luotavasta tietokannasta, jossa jokainen taho voi osaltaan varmistaa tietokannan olevan muokkaamaton muiden tahojen toimesta. Koska tiedon tulee myös pysyä turvassa peittelyltä tai poistamiselta, Chaum ehdotti koko tietokannan jakamista useille eri verkkoa tukeville laitteille. Tämän väitöskirjan ajatellaan pitkälti olevan pohja nykyiselle lohkoketjuteknologialle. Vajaa 30 vuotta myöhemmin Satoshi Nakamoto -nimimerkkiä käyttävä henkilö tai ryhmä julkaisi konseptin: ”Bitcoin: A Peer-to-Peer Electronic Cash System”.

Lohkoketju muodostuu nimensä mukaisesti yksittäisten lohkojen muodostamasta ketjusta. Yksinkertaistetusti lohkoketju on ketjumainen tietokanta, jonka sisältämää dataa ei voi jälkikäteen enää muuttaa tai poistaa. Useimmiten lohkoketjun sisältämä data jaetaan kaikille verkon osapuolille, jolloin jokainen voi varmistua itse datan paikkansapitävyydestä. Lohkojen tehtävä on toimia tietokannan datavarastona, Bitcoinin tapauksessa lohkot sisältävät transaktiodataa: mitä on siirretty, mistä, minne ja kuinka paljon. Bitcoin-verkko luo uuden lohkon keskimäärin joka 10. minuutti. Uusi lohko syntyy edellisen lohkon datasta muodostettavasta ”tiivisteestä”, salausavaimesta, joka on uniikki jokaiselle lohkolle.



KUVIO 2. Lohkoketjun rakenne (Kotilainen 2017)

Koska jokainen lohko on aloitettu edellisen lohkon tiivisteellä, kuten kuviossa 2, linkittyvät näiden lohkojen sisältämät tiedot toisiinsa. Lohkoista muodostuu kronologinen ketju, jossa jokainen ketjun päähän tuleva uusi lohko sulkee edellisen lohkon tiedot (Laurence 2019).

Lohkojen tiiviste lasketaan monimutkaisen matemaattisen operaation avulla, Bitcoinin osalta SHA-256 salausalgoritmilla. SHA-256 on hash-algoritmi, jonka tehtävä on salata viesti niin, että sitä on mahdotonta enää purkaa. (N-able 2019.) Lohkoketjussa tämä tarkoittaa, että ketjun uudemmasta lohkosta on mahdotonta laskea edellisen lohkon sisältämää dataa ja taas sitä edellisen lohkon tiivistettä. Tiivisteen avulla kuka tahansa voi tarkistaa lohkoketjun olevan ehyt ja muokkaamaton. Bitcoin-ketjussa verkon algoritmit muokkaavat tiivisteen laskennan vaikeutta, jotta uusi lohko muodostuu verkkoon vain keskimäärin joka 10. minuutti, riippumatta käytössä olevasta laskentakapasiteetista.

Bitcoinin lohkoketjua pidetään ensimmäisenä toimivana ratkaisuna Bysanttilaisen kenraalin ongelmaan. Kun uusi lohko lisätään ketjuun, verkon osallistujien on suoritettava laskentatehoa vaativia matemaattisia operaatioita. Vain kun suurin osa verkon louhijoista on yhtä mieltä lohkon oikeellisuudesta, lohko lisätään lohkoketjuun. Tämä menetelmä varmistaa, että vähintään 51 % verkon osallistujista on yhtä mieltä ennen kuin muutos hyväksytään. Jokainen ketjuun lisättävä lohko saa verkon suostumuksen ”Proof-of-Work” konsensusmetodin avulla. Proof-of-

Work tarkoittaa yksinkertaistetusti sitä, että jokainen verkon taho todistaa käyttävänsä energiaa verkon ylläpitoon.

Tämän vuoksi jokainen verkon toimija voi luottaa, että kaikki verkon toimijat toimivat yhteisesti verkon eduksi. Koska verkon konsensus saavutetaan yli 50 % hyväksyessä uuden lohkon osaksi ketjua, tarvitsisi verkkoa vastaan toimivan tahon käyttää yli 50 % koko Bitcoin-verkon tehosta valheellisen lohkon luomiseen. Tämä tarkoittaisi noin 750 000 $ sähkökustannuksia per tunti, puhumattakaan 10 miljardin dollarin laskentatehokaluston hankkimisesta (Merchant 2022). Suurten kustannusten ja valtavan laskentatehokapasiteetin saattamiseksi yhden valheellisen toimijan haltuun on käytännössä mahdotonta. Verkossa valheellisesti toimiva ”petturi kenraali”, joutuisi käyttämään valtavan määrän sähköenergiaa ja pääomaa saadakseen edes hetkeksi muutettua verkon konsensusta omaksi edukseen.

Virtuaalivaluuttojen louhinta on olennainen osa lohkoketjupohjaisten virtuaalivaluuttojen toimintaa. Virtuaalivaluuttoja louhiessa verkkoon liitetty tietokone osallistuu Proof-of-Work konsensusmetodin muodostamiseen yrittämällä löytää transaktiodatalla täytettyyn lohkoon sopivaa tiivistettä matemaattisella operaatiolla. Kun louhija onnistuu "löytämään" oikean tiivisteavaimen, hän ehdottaa uutta lohkoa lisättäväksi lohkoketjuun. Muut verkon osallistujat voivat tarkistaa ehdotetun lohkon tiivisteen oikeellisuuden nopeasti. Kun lohko on hyväksytty, louhija saa palkkion virtuaalivaluutan muodossa, esimerkiksi Bitcoinissa tämä on tietty määrä bitcoineja. Tämä palkkio toimii kannustimena louhijoille osallistua järjestelmään ja käyttää resurssejaan (laskentatehoa ja energiaa) lohkojen luomiseen ja verkon turvallisuuden ylläpitämiseen.

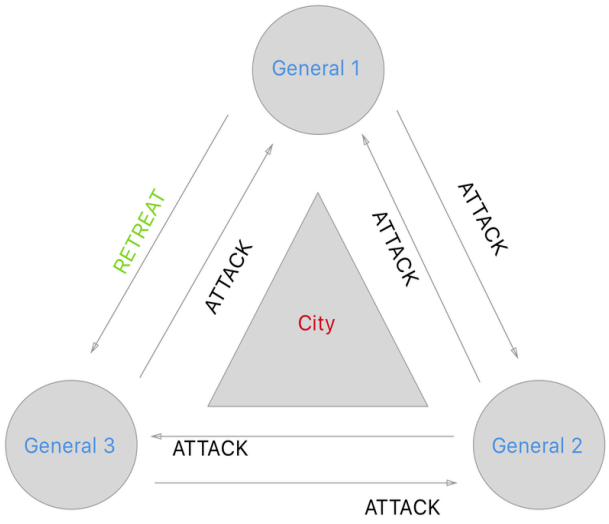
Proof-of-Stake (PoS) on vaihtoehtoinen konsensusmekanismi, joka vahvistaa verkon turvallisuutta ja luotettavuutta ilman suurta laskentatehovaatimusta. PoS-metodissa lohkoketjun transaktiot vahvistavat validaattorit, jotka valitaan heidän asettaman virtuaalivaluuttapanoksen mukaan. Validaattorit saavat äänivaltaa heidän asettaman panoksen suhteellisen määrän mukaan verrattuna muihin panoksen asettajiin, joten verkkoa vastaan toimiminen vaatisi yli 50 % osuuden kaikista asetetuista panoksista. Tämä taas ei kannusta toimimaan lohkoketjua vastaan, koska se suoraan laskisi panokseksi asetettujen valuuttojen arvoa. Tämä

tekee PoS:sta yhä houkuttelevamman vaihtoehdon monille kryptovaluutoille, jotka pyrkivät olemaan turvallisempia, ympäristöystävällisempiä ja skaalautuvampia.

2.3 Bysanttilaisen kenraalin ongelma

Lohkoketjuteknologiaan ja hajautettuihin järjestelmiin yhdistetään hyvin usein Bysanttilaisen kenraalin ongelma. Bysanttilaisen kenraalin ongelmaksi kutsutaan kuvitteellista tilannetta, jossa kahden tai useamman toisistaan erillään olevan, toisilleen tuntemattomien kenraalien tulee koordinoida yhdessä hyökkäys vihollisen linnaketta kohti. Ongelmana kuitenkin on, etteivät he voi luottaa heidän välisensä viestiyhteyden olevan suojattu, tai kaikkien kenraalien olevan lojaaleja suunnitelmalle. Epälojaali kenraali voi kaapata toisen kenraalin lähettämän hyökkäyssuunnitelman, ja estää tai vaihtaa viestin sisällön niin, että hyökkäys vääjäämättä epäonnistuu. Kenraaleilla on siis haaste saavuttaa konsensus, miten ja milloin hyökkäys tapahtuu, tai tapahtuuko se ollenkaan. (Lamport & Shostak & Please 1982.)

Keskitetyssä mallissa viestin salaisi ja välittäisi kaikkien kenraalien luottama taho, kuten esikunta. Tällöin kenraalit voivat luottaa kenraalin ja esikunnan väliseen yhteyteen tai hyödyntää etukäteen sovittua salausavainta. Kuvitteellisessa tilanteessa kenraalit toimivat yksittäisinä, hajautettuina toimijoina. He vahvistavat itse lähettämänsä viestit ja ne lähetetään suoraan vastaanottajalle, ilman esikunnan vahvistusta. Kuinka kenraalit voivat saavuttaa konsensuksen, siis tulla yhteisymmärrykseen suunnitelmasta? Vastaus on, ei mitenkään.



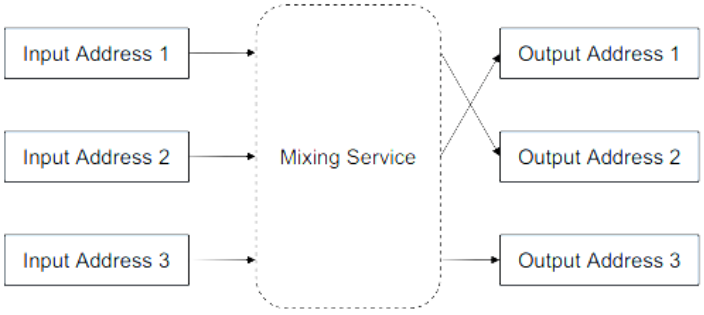
KUVIO 1. Bysanttilaisen kenraalin ongelma, kenraali 1 on petturi. (Islomov, S. Byzantine Generals Problem 2017)

Bysanttilaisen kenraalin ongelma on mahdotonta ratkaista perinteisin keinoin ja täydellä varmuudella. Esimerkiksi kolmen kenraalin tilanteessa, jossa yksi on petturi, voi epälojaali kenraali vaihtaa saamansa viestin sisällön, jolloin toinen kenraali saa alkuperäiseltä kenraalilta, sekä petturilta, eroavat suunnitelmat, kuten kuviossa 1 kenraali 3. Viestin ensimmäisenä lähettävä kenraali voi myös yrittää ratkaista ongelman todennäköisyyksillä, esimerkiksi lähettämällä jokaiselle kenraalille sata viestiä, ja toivoa, ettei epälojaali kenraali ehdi muokata kaikkia viestejä sovituissa vastauksen aikarajoissa. Sadan viestin lähettäminen on kuitenkin kallista, aikaa vievää, eikä siltikään välttämättä saavuta täydellistä yhteisymmärrystä kenraalien välillä.

Bysanttilaisen kenraalin ongelma on yksinkertaistettu havainnollistamaan hajautettujen tietoverkkojen keskeistä ongelmaa, konsensuksen saavuttamista. Kenraali havainnollistaa yhtä tietoverkon tietokonetta ja kenraalin lähettämä viesti mitä tahansa verkossa liikkuvaa datapakettia. Tavallisesti maailman rahaliikenne kiertää keskitettyjen toimijoiden kautta, kuten pankkien, luottolaitosten tai maksukorttioperaattoreiden, jotka itse varmistavat ja hyväksyvät jokaisen transaktion. Näiden toimijoiden tehtävä rahan liikkumisen näkökulmasta on olla luotettu välikäsi, ”esikunta”, johon rahan lähettäjä ja vastaanottaja voivat molemmat erikseen luottaa. (Markman 2021.)

2.4 Julkinen vai salattu lohkoketju?

Tässä opinnäytetyössä keskitytään suurimpien julkisten virtuaalivaluuttojen käyttöön osana rahanpesua. Näiden valuuttojen toimintamekaniikat ovat selkeät ja niistä on paljon lähdetietoa saatavilla. Julkisilla lohkoketjuilla tarkoitetaan lohkoketjuverkon toimintamallia, johon kellä tahansa on oikeus osallistua. Lähes kaikki virtuaalivaluuttojen pohjalla olevista lohkoketjuista ovat julkisia. Monien uskomusten vastaisesti lohkoketjuun tallentuvat tiedot ovat myös julkisia, joka mahdollistaa kenen tahansa tarkastella aikaisempia lohkoihin tallennettuja transaktioita, kuten mitä on maksettu, koska, keneltä ja kenelle. Tavallisen pankkirahan siirtämisen erona on, että lohkoketjussa ainoastaan lähettäjän ja vastaanottajan lompakon osoite tunnetaan. Varallisuus siirtyy käyttäjien lompakoiden välillä, eikä kummankaan, vastaanottajan tai lähettäjän, tarvitse tietää toisen todellista henkilöllisyyttä tai nimeä. Eri lohkoketjuja, lohkoja ja transaktioita voi seurata esimerkiksi osoitteessa www.blockchain.com.



KUVIO 3. Sekoituspalveluiden rakenne (Kenneth, S. 2023)

Vaikka suurimpien virtuaalivaluuttojen lohkoketjut ovatkin julkisia, saatavilla on useita palveluita hämäämään varojen todelliset lähtöpaikat ja määränpäät. Näitä palveluita kutsutaan yleisesti sekoituspalveluiksi (engl. Mixers). Näiden palveluiden tarkoitus on ottaa vastaan siirrettäviä varoja useilta eri käyttäjiltä, sekoittaa niitä eri osoitteiden välillä, ja lopuksi siirtää ne kohteeseensa kuvion 3 mukaisesti. Tämä hankaloittaa huomattavasti virtuaalivaluuttojen jäljittämistä, muttei toki tee sitä mahdottomaksi. Jos jäljittäjä tunnistaa esimerkiksi yhden sekoituspalvelua käyttävän osapuolen, on loput osapuolet helpompi selvittää, jos siirrettävät sum-

mat täsmäävät. Selvittämistyö kuitenkin merkittävästi hankaloituu, jos osa siirrettävästä virtuaalivaluutasta kuluu esimerkiksi palvelun kuluihin, joka ei näy ulos siirtyvissä summissa. (Kenneth 2023.)

Virtuaalivaluutoissa löytyy myös erityisesti anonymiteettiin keskittyneitä vaihtoehtoja. Tunnetuimpina ovat esimerkiksi Monero, Zcash ja DASH. Nämä valuutat käyttävät myös julkista lohkoketjua ja toimivat hajautettuna, mutta hyödyntävät muita tekniikoita salatakseen julkisesti saatavilla olevan tiedon. Vuonna 2014 julkaistun Moneron kehittäjätiimin arvoina ovat turvallisuus, yksityisyys ja hajauttaminen. Monero toimii pitkälti samaan tapaan kuin Bitcoin, mutta sen lohkoketjuun on implementoitu useita automaattisia yksityisyyttä parantavia toimintoja. Moneron julkisessa lohkoketjussa esimerkiksi lähettäjän ja vastaanottajan osoitteet ovat piilotettu, samoin siirretyn varallisuuden määrä. (Monero n.d.)

Tällaiset hajautetut ja anonyymit virtuaalivaluutat aiheuttavat huomattavan rahanpesu- ja rikollisuusriskin, koska niiden jäljittäminen on mahdotonta tai erittäin hankalaa. Tämän vuoksi Monero ja muut anonyymit virtuaalivaluutat ovat nousseet yleiseksi maksutavaksi pimeän verkon (engl. Dark web) verkkokauppa-alustoilla. Arvioiden mukaan Moneroa käytettiin maksutapana 44 prosentissa kiristysohjelmien avuilla tehdyissä hyökkäyksissä (Rooney 2018).

2.5 CEX vastaan DeFi

Virtuaalivaluuttojen hajautetun toiminnan vuoksi niillä voi käydä kauppaa sekä keskitettyjen toimijoiden kautta että hajautetusti verkossa. Keskitetyistä markkinapaikoista käytetään lyhennettä CEX (engl. Centralized Exchange), ja ne ovat perinteiseen tapaan olemassa olevia yrityksiä, jotka erikoistuvat virtuaalivaluutoilla käytävään kaupankäyntiin. Ne toimivat keskitetyn ylläpidon alla ja kaupankäynti tapahtuu yhtiön palvelimilla. Keskitettyjen markkinapaikkojen tulee useimmiten täyttää FATF:in ja EU-alueella AMLD5 -direktiivien vaatimukset rahanpesun estävistä toimista (Zharun 2022). Nämä tarkoittavat esimerkiksi KYC (Know-your-Customer) tietojen keräämistä sekä muita riskiperusteisia analyysejä. Näiden tietojen keräämisen lisäksi keskitettyjen markkinapaikkojen tulee huolehtia

riittävästä tietoturvasta, sisäisestä kirjanpidostaan sekä riskienhallinnasta, koska ne säilyttävä sekä asiakkaidensa virtuaalivaluuttoja että FIAT-valuuttoja.

Koska pääasiassa kaikki keskitetyt markkinapaikat noudattavat rahanpesun estämisen direktiivejä, niiden käyttäminen rahanpesun sijoittamisvaiheessa virtuaalivaluuttojen ostoon on hankalaa ja yhtä riskialtista kuin muillakin finanssialan toimijoilla.

Virtuaalivaluutoilla voi käydä myös kauppaa hajautetuilla markkinapaikoilla, toiselta nimeltään DEX (Decentralized Exchange), jotka toimivat ilman keskitettyä ylläpitäjää. Tämä tarkoittaa, että kaikki kaupankäynti tapahtuu käyttäjien välillä lohkoketjussa, eikä keskitettyä palvelua tarvita. Koska DEX ei ole keskitetty, siellä ei ole samanlaisia KYC- ja AML-sääntöjä kuin CEX:ssä, mikä voi tehdä rahanpesun estämisestä vaikeampaa. Vaikka DEX:issä ei ole keskitettyä ylläpitäjää, kaikki kaupankäynti tallentuu julkisesti lohkoketjuun, mikä voi helpottaa epäilyttävien siirtojen tunnistamisessa.

DEX:it eivät kuitenkaan käy pankkien tileillä olevan tai käteisen rahan sijoittamiseen, sillä ne toimivat osana hajautettua verkkoa. Hajautetuilla markkinapaikoilla kaupankäynnin hoitavat älysopimukset, ja niillä voi käydä kauppaa vain palvelun tukemilla virtuaalivaluutoilla. Tämän vuoksi DEX:jä käytetään enemmän osana rahanpesun harhautusvaihetta.

2.6 Virtuaalivaluuttojen säilyttäminen

Virtuaalivaluuttojen säilyttäminen perustuu virtuaalivaluuttalompakon muodostamaan kahteen salausavaimeen: julkiseen ja yksityiseen avaimeen. Yksityinen avain on useimmiten 256-bittinen merkkijono, johon ainoastaan lompakon omistajalla on pääsy. Yksityinen avain mahdollistaa lompakossa olevien varojen omistajan varmistamisen, sillä kyseinen merkkijono voi edustaa ainoastaan yhtä virtuaalivaluuttalompakkoa. Ainoastaan tietämällä kyseisen lompakon yksityinen avain, voidaan lompakossa olevat varat siirtää eteenpäin.

Julkinen avain on yksityisestä avaimesta salausalgoritmilla johdettu osoite, jolla

voi tunnistaa tietyn lompakon ja johon voi siirtää kyseisen lompakon hyväksymää virtuaalivaluuttaa. Vaikka julkinen avain on johdettu yksityisestä avaimesta, sen selvittäminen on käytännössä mahdotonta nykyisen tietotekniikan tarjoamalla laskentakapasiteetilla. Julkisen avaimen voi nimensä mukaisesti kertoa kelle vain, ja sen avulla pystyy selvittämään lompakon varallisuuden sekä aiemmat tehdyt siirrot. (Cryptopedia 2022.)

Useimmiten virtuaalivaluuttoja säilytetään suoraan CEX-kauppapaikan omissa lompakoissa, joihin käyttäjällä on pääsy esimerkiksi internetin tai älypuhelinsovelluksen kautta. Näissä lompakoissa käyttäjällä useimmiten ei ole pääsyä lompakon yksityisavaimeen, vaan tarvittaessa kauppapaikka vahvistaa siirrot omalla yksityisavaimellaan. Varojen säilyttäminen kauppapaikkojen omissa lompakoissa on useimmiten turvallista, mutta esimerkiksi hakkeroinnit, kauppapaikan konkurssi tai nopeat lainsäädännölliset muutokset voivat altistaa käyttäjät varojen menettämisen riskille.

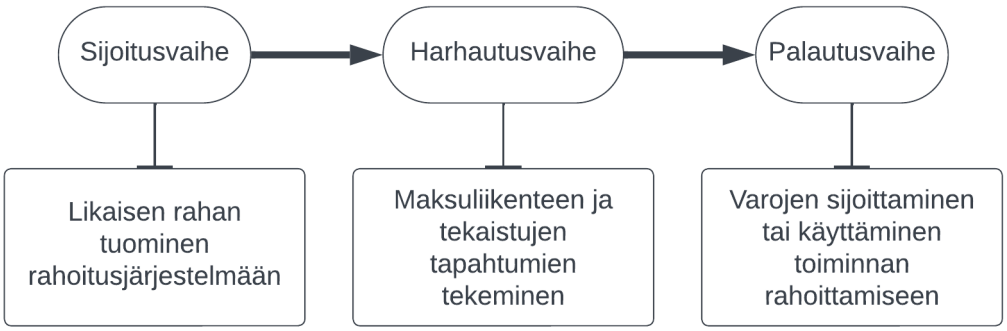
Toinen yleinen vaihtoehto säilyttää virtuaalivaluuttoja on käyttäjän omat yksityiset lompakot. Nämä lompakot sijaitsevat tavallisesti erillisellä lompakkolaitteella tai käyttäjän älypuhelimessa sovelluksena. Yksityisessä lompakossa käyttäjällä on täysi hallinta omista varoistaan sekä yksityisistä avaimistaan. Yksityiset lompakot vähentävät vastapuoliriskiä, koska virtuaalivaluuttojen hallintaan ei liity muita osapuolia. Sen sijaan muita esiin nousevia riskejä ovat esimerkiksi hakkeroinnin uhriksi joutuminen, laitteen rikkoutuminen tai sen katoaminen. Yksityisavaimen hukkaaminen tekee lompakossa olevien varojen käyttämisen mahdottomaksi.

Harvinaisempia tapoja säilöä virtuaalivaluuttoja ovat esimerkiksi yksityisavainten tulostaminen paperille tai kaivertaminen metallilaatalle. Nämä säilömistavat ovat suhteellisen turvallisia, koska niitä ei ole liitettynä verkkoon, eivätkä siksi ole alttiita esimerkiksi hakkeroinnille. Tällaisia lompakoita kutsutaan yleisesti kylmiksi lompakoiksi. Toisaalta nämä tavat ovat yhä alttiita varkauksille ja tulipaloille.

3 VIRTUAALIVALUUTTOJEN NOUSU RAHANPESUN VÄLINEENÄ

3.1 Rahanpesun tapahtumaketju

Rikollisen omaisuuden puhtaaksi pesemiseen liittyy yleisesti käytetty kolmivaiheinen malli, kuten kuviossa 1. Ennen kuin itse rahanpesuprosessi alkaa, on rikollinen taho saanut haltuunsa laitonta omaisuutta, useimmiten käteistä rahaa huumausainekaupoista. Suuren määrän käteisen hallussapito on hankalaa, riskialtista sekä sen kuljettaminen on kallista. Käteisen hyötykäyttäminen on myös hankalaa, sillä esimerkiksi harva asunnon myyjä haluaa kymmeniä tuhansia euroja käteistä omaksi ongelmakseen. Niinpä rikollisen on saatava käteinen raha sijoitettua jotenkin talousjärjestelmän piiriin, useimmiten pankkitilillä olevaksi varallisuudeksi.



KUVIO 1. Esimerkki rahanpesun kolmevaiheisesta mallista

Sijoitusvaiheessa rikollinen yrittää useimmiten tallettaa saamansa käteisvarat tai tekee tilisiirron kahden tai useamman tilin välillä. Sijoitusvaihe on rahanpesun eri vaiheista yleisimmin kaikkein riskialttein kiinnijäämiselle (Buchanan 2004), koska summiltaan suuret käteistalletukset tai tilisiirrot herättävät nopeasti finanssialan toimijoiden mielenkiinnon. Niinpä rahat pyritään useimmiten sijoittamaan talousjärjestelmään näennäisesti laillisten toimien kautta, kuten käteisvaltaisten toimialojen, laskutuspetosten tai ”smurffien” avulla.

Esimerkkejä sijoitusvaiheen peittelytavoista: (ST Paul’s Chambers 2021)

Rahavirtojen yhdistäminen:
Rikolliset perustavat laillisen liiketoiminnan käteisvaltaiselle alalle, kuten ravintolan, autokorjaamon, kasinon, yökerhon tai muun vastaavan. Listaan voi kuulua myös korkean arvon tuotteiden tarjoajat, kuten merkkiliikkeet tai jalometallikauppiaat. Laillisen liiketoiminnan käteisliikenteen talletuksen ohella voidaan tallettaa tekaistuina myyntituloina myös muualta tullutta käteistä, jolloin ”likainen raha” saadaan piilotettua yrityksen tilille.

Laskupetokset:
Likaista rahaa voidaan peitellä esimerkiksi kahden yrityksen välisellä tekaistulla kaupankäynnillä, jossa kauppatavara yli- tai aliarvotetaan tarkoituksena siirtää omaisuutta osapuolelta toiselle. Kauppaperusteinen rahanpesu on erittäin hankalaa huomata maailmanlaajuisen kaupan suuren volyymin ja vienti-tuontikaupan monimutkaisten rahoitusvälineiden vuoksi. (FATF 2021.)

Esimerkkitapauksena tuontiyritys ostaa vientiyritykseltä 1 miljoonalla dollarilla tuotteita. Vientiyritys lähettää tuontiyritykselle tuotteita 500 000 dollarin arvosta, ja vääristelee viralliset toimitusdokumentit vastaamaan kauppasummaa. Kun rahti on vastaanotettu, tuontiyritys on onnistunut siirtämään vientiyritykselle 500 000 dollaria sille liiketaloudellisesti kuulumatonta varallisuutta. Tällaisten kauppojen toteuttajina voidaan lisäksi käyttää finanssilaitoksia esimerkiksi remburssin välittäjinä, jolloin kaupat voivat ulkoisesti näyttää todenperäisemmiltä.

Smurffien hyödyntäminen:

> Smurffeilla tarkoitetaan henkilöitä, joita käytetään esimerkiksi piilottamaan tosiasiallisen rikollisen henkilöllisyys. Smurffeja voidaan hyödyntää esimerkiksi käteisen talletuksessa, jossa suuri määrä käteistä jaetaan pieniksi, vähemmän huomiota aiheuttaviksi summiksi, ja talletetaan eri henkilöiden pankkitileille. Tämän jälkeen talletetut varat voidaan esimerkiksi siirtää liiketoiminnan tai yksityisten kauppojen jälkeen takaisin alkuperäisen rikollisen hyödyksi.

Virtuaalivaluuttojen rahanpesun sijoitusvaiheen tunnistamisen hankaluus liittyy siihen, ettei virtuaalivaluutoilla tapahtuvat transaktiot ole liitettynä kenenkään henkilöllisyyteen. Rahanpesun sijoittamisvaiheessa virtuaalivaluuttoja voidaan hyödyntää monella eri tavalla riippuen, onko pestävä omaisuus jo valmiiksi virtuaalivaluuttana vai muuna omaisuutena. Jos pestävä omaisuus on esimerkiksi esineitä tai muuta aineellista omaisuutta, voivat rikolliset hyödyntää internetin markkinapaikkoja myymällä laitonta omaisuutta, missä maksuvälineenä käyvät virtuaalivaluutat. Tällaisessa toiminnassa on usein kyse P2P-tapahtumasta (Peer-to-Peer), joka suoritetaan kahden ihmisen välillä. Tätä kautta rikolliset onnistuvat välttämään kaikki perinteisen finanssialan toimijat.

Jos omaisuus on kuitenkin esimerkiksi käteisenä, täytyy se saada muutettua virtuaalivaluutoiksi jotain kautta. Tällaisessa tapauksessa käteinen usein sijoitetaan pankkijärjestelmään jonkinlaisen harhautustekniikan kautta tai P2P vaihtokaupalla, jonka jälkeen varat siirretään virtuaalivaluuttoja tarjoaviin markkinapaikkoihin. Edellä mainittujen harhautustekniikoiden lisäksi rikolliset voivat siirtää varoja kuoriyhtiön (engl. shell corporation) tileille korkean pankkisalaisuuden maahan tai muualle ulkomaiseen pankkiin, joissa myös rahanpesun estämisen lainsäädäntö on muita maita löyhempää. Tällaisia maita ovat esimerkiksi Kongo, Haiti, Myanmar sekä Mosambik (Sanctions Scanner 2022).

2. Harhautusvaihe

Rahanpesun harhautusvaiheella tarkoitetaan rahanpesun toista vaihetta, jossa tarkoituksena on hämärtää saadun laittoman varallisuuden alkuperä ja tekemään sen jäljittämisestä vaikeampaa. Harhautusvaiheessa voidaan käyttää yk-

sittäisiä varallisuuden muotoja, kuten käteistä, pankkitilejä, arvometalleja, virtuaalivaluuttoja, taide-esineitä tai mitä tahansa muuta omaisuuden muotoa tai näiden yhdistelmiä. Tyypillisimpiä välineitä ovat kuitenkin pankkitilit, niiden tarjoaman nopeuden ja helppokäyttöisyyden vuoksi. Esimerkkinä laittomasti saadut käteisvarat voidaan tuoda lailliseen talousjärjestelmään edellä mainittujen smurffien avulla, jonka jälkeen varoja aletaan siirtää korkean pankkisalaisuuden tai matalan sääntelyn maiden pankkeihin perusteettomina tilisiirtoina esimerkiksi väärennetyillä laskuilla tai hämärillä rahoitusjärjestelyillä. (Andersen 2020, 22.)

Harhautusvaiheessa voidaan myös hyödyntää useimmiten arvokkaita tuotteita, kuten luksusvaatteita ja -asusteita, ajoneuvoja, koruja ja taide-esineitä tai muuta fyysisesti arvokasta ja helposti vaihdettavaa tuotetta, jolla on hyvät ja likvidit markkinat, ja joilla pystyy myös käymään vaihtokauppaa. Tällaisten tuotteiden käytöllä voidaan tehdä varallisuuden jäljittämisestä hyvin hankalaa, koska varallisuus vaihtaa muotoaan ja sijaintia sekä laillisen talousjärjestelmän pankkitilien piirissä, että myös P2P-tapahtumana ilman kaupan kolmannen osapuolen vahvistamista. Joillakin näistä tuotteista arvot ovat myös subjektiivisia, kuten taide-esineillä, joita voidaan arvottaa lähes täydellisellä vapaudella.

Online-Casinot ja vedonlyönti on yleistynyt rahanpesun harhautustekniikkana. Internetissä toimivat pelisivustot ovat useimmiten ulkomaisia ja sijaitsevat matalan regulaation tai veroasteen alueilla, kuten Maltalla. Tavallisimpia harhautustapoja on esimerkiksi tahallinen häviäminen, jossa samassa digitaalisessa pelipöydässä pelaavista henkilöistä toinen häviää tarkoituksella toiselle, jolloin tämän varallisuus siirtyy näennäisesti laillisina voittoina toiselle henkilölle. Samalla pelaajat voivat yrittää välttää kasinoiden tuntemismenettelyjä pelaamalla ja voittamalla tunnistamiskäytäntöjen rajan alittavilla summilla tai ostamalla pelimerkkejä ”likaisella rahalla” ja muuntamalla ne myöhemmin ”puhtaaksi” jättämättä juurikaan pelijälkeä. (Complyadvantage.com 2023.)

Virtuaalivaluuttojen käyttämistä rahanpesun harhauttamisvaiheessa helpottaa niiden tarjoama pseudoanonyymisyys. Vaikka suurin osa virtuaalivaluutoilla tapahtuvista siirroista ovat kenen tahansa seurattavissa, siirron osapuolten henkilöllisyyttä on hankala selvittää ilman pääsyä valuutanvaihtopalveluiden tai lompakkopalveluntarjoajien asiakastietoihin. Lisäksi monimutkaiset ja kerrostetut

siirrot eri lompakoiden ja valuuttojen välillä voivat tehdä varojen jäljittämisestä entistä vaikeampaa. Varojen siirroissa voidaan hyödyntää sekä CEX- että DEX-kauppapaikkoja, pelipalveluita, sekoituspalveluita, useiden eri henkilöiden tai yritysten lompakoita sekä virtuaalivaluutta-automaatteja. Vaikka rikolliseen tarkoitukseen hankittujen virtuaalivaluuttojen kulusta päästäisiin selville, on niiden sen hetkistä hallussapitäjää erittäin hankala tunnistaa, ja virtuaalivaluuttojen luonteen takia varoja ei voida jäädyttää selvittelyä varten. Lopulta virtuaalivaluutat saatetaan ladata virtuaalivaluuttapalveluntarjoajan tarjoamalle Prepaid-maksukortille, jota pystyy käyttämään tavallisen maksukortin tapaan, jolloin käynnistyy rahanpesun ketjun kolmas vaihe.

3. Palautusvaihe

Rahanpesun palautusvaiheessa rikolliset tahot pyrkivät palauttamaan pestyn rahan takaisin osaksi talousjärjestelmää edelleen hyödynnettäväksi. Varallisuus pyritään saamaan näyttämään laillisista lähteistä tulleelta, kuten myyntivoitoista, kauppatapahtumasta tai uhkapelivoitoista. Aiemman vaiheen monimutkaisten siirtojen ja harhautusten vuoksi varojen todellista alkuperää on hankala selvittää, koska rikollisilla on esittää esimerkiksi todistuksia varojen pelaamisesta kasinolla tai todenmukaisia, mutta summiltaan väärennettyjä laskuja kaupankäynnistä. Joissain tapauksissa varat voivat saapua tiukan pankkisalaisuuden alaisista maista, jolloin niiden tarkempi tutkiminen on käytännössä mahdotonta. Kun varat on saatu palautettua takaisin talousjärjestelmän piiriin, voivat rikolliset hyödyntää varoja tukeakseen toimintansa jatkumista ilman pelkoa kiinni jäämisestä. (Dixon 2023.)

Virtuaalivaluuttojen osalta palautusvaihe ei juurikaan eroa muista palautusvaiheessa käytetyistä tavoista. Suurimpana ongelmana on kuitenkin virtuaalivaluuttojen vielä vähäiset käyttökohteet tavallisessa talousjärjestelmässä. Tämä rajoittaa niiden käytön mahdollisuuksia tehdä laajoja ja huomaamattomia investointeja verrattuna perinteisiin FIAT-valuuttoihin. Virtuaalivaluutoille on kuitenkin olemassa kaupankäyntipalveluita esimerkiksi kiinteistöjen ostoon. Kuten aiemmin mainittu, virtuaalivaluutoilla voi myös ladata Prepaid-maksukortteja, jolla varoja pääsee käyttämään suoraan kaikkialla korttimaksuja hyväksyvissä paikoissa.

Jotkin virtuaalivaluuttapalvelut myös tarjoavat FIAT-valuuttalainaa virtuaalivaluuttapanttia vastaan. Jos lainanottaja ei kykene maksamaan lainaa takaisin sovitussa ajassa, palveluntarjoaja voi myydä panttina olevat virtuaalivaluutat kattamaan lainasumman. Tällaisilla järjestelmillä lainanottajan ei tarvitse myydä hallussaan olevia virtuaalivaluuttoja, ja voi silti sijoittaa näennäisesti laillista rahaa perinteisessä rahoitusmaailmassa. Näitä tapahtumia voi olla myös vaikea huomata, sillä varallisuuden lähde näyttää lailliselta lainalta, vaikka taustalla olevat pantatut virtuaalivaluutat voivat olla osa rahanpesuketjua.

Palautusvaiheen jälkeen rikollisilla toimijoilla on varoja, jotka näyttävät laillisilta pinnallisesti tarkasteltuna. Nämä varat on integroitu osaksi laillista talousjärjestelmää, mikä tekee niiden jäljittämisestä ja alkuperän paljastamisesta haastavaa viranomaisille.

3.2 Rahanpesun vaikutukset

Rahanpesu on mittakaavaltaan globaali talousjärjestelmän ongelma. Rahanpesun arvioidaan olevan kokoluokaltaan noin 2–5 % maailman BKT:sta, mikä vastaa noin 800 miljardia – 2 triljoonaa Yhdysvaltain dollaria joka vuosi (United Nations n.d). Rahanpesun mahdollistaa osaltaan rikollisten toiminnan, ja auttaa heitä hyödyntämään rikollisin tavoin saatua omaisuutta laillisesti osana yhteiskuntaa.

Rahanpesun vaikutukset jaetaan usein kolmeen eri luokkaan: (Andersen 2020, 39)

> Sosiaaliset vaikutukset:
> Rahanpesun lieveilmiöihin kuuluu laaja määrä sosiaalisesti vaikuttavia ilmiöitä. Rahanpesu mahdollistaa rikollisten toiminnan osana yhteiskuntaa ja rahajärjestelmää. Suuressa mittakaavassa rahanpesu työllistää paljon rikollisia ja toiminnassa voidaan hyödyntää ihmiskaupan uhreiksi joutuneita, esimerkiksi muuleina tai bulvaaneina. Rahanpesun sivuilmiöiden tai esirikosten uhriksi joutuneet kokevat usein taloudellisia menetyksiä tai sosioekonomista eriarvoisuutta. (Shah n.d.)

Poliittiset vaikutukset:

Poliittisiin rahanpesun vaikutuksiin voidaan lukea esimerkiksi poliittinen korruptio ja poliittisen järjestelmän vääristyminen. Poliittisesti vaikutusvaltaiset (PEP) henkilöt ovat huomattavan alttiita toimimaan osana rahanpesuketjua, ottamaan vastaan lahjuksia tai muuten toimimaan rikollisille edullisella tavalla poliittisen vaikutusvaltansa kautta. (IDEA.int 2017.)

Taloudelliset vaikutukset:

Taloudellisiin vaikutuksiin kuuluu konkreettisesti esimerkiksi verotulojen pieneneminen sekä kaupan ja rahavirtojen häiriintyminen. Rahanpesu on myös oleellinen osa harmaata taloutta, mikä vääristää kilpailuasemia sekä heikentää talouden tehokkuutta. (Andersen 2019, 40.)

Rahanpesulla on kokonaisuutena valtavan haitallisia vaikutuksia, ja tämän vuoksi erityisesti 2001 New Yorkin terrori-iskujen jälkeen rahanpesun sekä terrorismin rahoittamisen estämiseen on käytetty huomattavia resursseja (IMF n.d).

Rahanpesulla on useita kielteisiä vaikutuksia kehittyvissä maissa. Näissä maissa ei välttämättä ole riittävän vahvaa lainsäädäntöä, pankkijärjestelmää tai valtion johtoa, jotta rahanpesun mukanaan tuomia ongelmia voitaisiin tehokkaasti estää. Poliittisen korruption myötä ihmisten taloudellinen ja sosioekonominen eriarvoisuus lisääntyy rahanpesun lisääntyessä, eikä lahjotuilla poliittisilla päättäjillä ole intressejä korjata tilannetta. Epäoikeudenmukaisessa talousjärjestelmässä organisoidun rikollisuuden osuus on huomattavan suurta, ja sen seurauksena laillisesti toimivilla yrityksillä on vaikeuksia kilpailla reilusti. Tämän seurauksena kehittyvien maiden on entistä vaikeampaa luoda oikeudenmukaista talouskasvua ja tasavertaisia mahdollisuuksia kansalaisille. (Ayodeji & Mahmood 2012, 442, 445 – 446.)

4 LAIT JA SÄÄDÖKSET VIRTUAALIVALUUTTOJEN KAUPANKÄYNNIN SÄÄNTELYSSÄ

4.1 Laki virtuaalivaluutan tarjoajista (572/2019)

Euroopan unionin vuonna 2018 julkaiseman viidennen rahanpesudirektiivin (AMLD5), jossa otettiin voimakkaasti kantaa virtuaalivaluuttojen sääntelyyn, seurauksena myös Suomessa tuli nopeasti luoda laki uusien säädösten noudattamiseksi. Suomen virtuaalivaluuttalaki tuli lopulta voimaan toukokuussa 2019, noin 8 kuukautta ennen määräaikaa.

Lain 2 pykälässä määritellään mitä virtuaalivaluutta on (572/2019):

1) *Digitaalisessa muodossa olevaa arvoa:*
    a. *Jota keskuspankki tai muu viranomainen ei ole laskenut liikkeeseen ja joka ei ole laillinen maksuväline;*
    b. *Jota henkilö voi käyttää maksuvälineenä; ja*
    c. *Jota voidaan siirtää, tallettaa ja vaihtaa sähköisesti;*

Lain seurauksena kaikkien Suomessa virtuaalivaluuttapalveluita tarjoavien tulee rekisteröityä Finanssivalvonnan valvontarekisteriin sekä päivittämään tietojaan toiminnastaan säännöllisesti. Lisäksi heidän tulee täyttää asiakkaan tuntemisvelvollisuudet sekä ottaa käyttöön riittävät riskienhallintajärjestelmät, jotta se voi arvioida asiakassuhteista aiheutuvia talousrikollisuuden riskejä. Myös raportointivelvollisuus viranomaisille laajeni huomattavasti.

Uuden lain myötä virtuaalivaluuttapalveluita tarjoavien palveluiden on noudatettava varovaisuutta asiakkaiden varojen säilytyksessä: ne ovat säilytettävä omalla tilillään sekä sellaisissa kohteissa, jotka ovat helposti rahaksi muutettavissa, eli nopeasti likvidoitavissa, tai erillisellä asiakasvaratilillä.

4.2 Laki rahanpesun ja terrorismin rahoittamisen estämisestä

Suomessa astui vuonna 2017 voimaan uusi laki rahanpesun ja terrorismin rahoittamisen estämisestä (28.6.2017/444). Kyseisen laki toi mukanaan merkittäviä tarkennuksia ja päivityksiä edelliseen vuoden 2008 lainsäädäntöön, sekä otti Suomessa kansallisesti käyttöön EU:n neljännen rahanpesudirektiivin. (Eduskunta.fi 2017.)

Lain ytimessä on finanssilaitosten velvollisuus tunnistaa ja raportoida epäilyttävät liiketoimet ja kehittää omia toimintamallejaan yhä paremmiksi näiden tapausten tunnistamiseksi. Merkittävimpinä eroina vuoden 2008 ja 2017 lainsäädännössä on virtuaalivaluuttojen huomioon ottaminen osana rahanpesun estämisen toimintoja. Lain seurauksena myös virtuaalivaluuttavälittäjien ja -palveluntarjoajien tulee noudattaa finanssilaitoksille tuttua valvonta- ja ilmoitusvelvollisuutta, sekä muodostaa sisäiset riskiarviot omista prosesseistaan ja hallita näistä muodostuvia riskejä tehokkaammin.

Uusi rahanpesulaki tarkensi asiakastuntemisen menettelyjä sekä mahdollisti riskiperusteisen lähestymistavan (engl. RBA, Risk-Based Approach). Riskiperusteisella lähestymistavalla tarkoitetaan, että rahoituslaitoksilla on velvollisuus arvioida yksittäisistä asiakkaista nousevia riskejä, sekä ottaa käyttöön erilaisia tuntemismenettelyjä riippuen asiakkaan riskitasosta. Korkean riskin asiakkaille voidaan suorittaa esimerkiksi syvällisempi tunnistaminen, toiminnan tutkiminen ja tiheämpi seuranta kuin matalan riskin asiakkaille, joille voidaan suorittaa kevyempiä menettelyitä. Laki korostaa jatkuvan asiakastuntemisen merkitystä: ilmoitusvelvollisten on säännöllisesti tarkkailtava asiakkaidensa toimintaa ja tutkittava havaitut epäilyttävät muutokset säädetyssä ajassa sekä raportoida niistä tarvittaessa viranomaisille.

Laissa määrätään ilmoitusvelvollista tekemään välittömästi ilmoitus rahanpesun selvittämiskeskukselle asiakkaan tekemistä epäilyttävästä liiketoiminnasta. Vastaavasti jos asiakkaasta on tehty ilmoitus ja asiakkaan tapahtumien epäillään liittyvän terrorismin rahoittamiseen, on ilmoitusvelvollisella oikeus ja velvollisuus keskeyttää asiakkaan maksuliikenne ja jäädyttää asiakkaan varat selvitysten ajaksi tai kieltäytyä asiakkuudesta kokonaan.

Vuoden 2017 laki rahanpesun ja terrorismin rahoittamisen estämisestä toi mukanaan merkittäviä muutoksia finanssi- ja rahoitusalan rahanpesun estämisen toiminnoille. Virtuaalivaluuttapalveluntarjoajien osalta nämä muutokset olivat erityisen huomattavia. Laki antoi selkeät ohjeet ja vaatimukset virtuaalivaluuttapalveluille, kuten kryptovaluuttapörsseille ja lompakkopalveluille, koskien heidän toimintaansa ja vastuutaan rahanpesun estämisessä. Rahanpesun estämiseen liittyviä keinoja arvioidaan tarkemmin opinnäytetyön viidennessä kappaleessa.

4.3 EU-tason lait ja direktiivit

EU-lainsäädäntö virtuaalivaluuttojen rahanpesun estämiseksi on kehittynyt merkittävästi vuonna 2015 käyttöön otetun AMLD4-direktiivin tarkentaessa toimintamalleja myös virtuaalivaluuttojen osalta. AMLD4 sisälsi vaatimuksen virtuaalivaluutanvaihto ja -lompakkopalveluntarjoajien ottavan käyttöön asiakkaiden tuntemisten menettelytavat sekä rekisteröityvän paikalliselle viranomaiselle maksupalveluiden tarjoajana. Direktiivi ei kuitenkaan tarkentanut esimerkiksi mitä virtuaalivaluutat ovat, eikä vaatimuksia korkean riskin siirtojen tutkimiseen ja raportoimiseen. Tämän vuoksi vuonna 2018 käyttöön otettu viides rahanpesun vastainen direktiivi (AMLD5) toi paljon tarkennuksia erityisesti virtuaalivaluuttojen osalta. Direktiivi määritteli virtuaalivaluutat:

> ”Digitaalisia arvonkantajia, jotka eivät ole keskuspankin tai viranomaisen liikkeeseen laskemia tai takaamia, joita ei välttämättä ole kytketty lailliseksi maksuvälineeksi vahvistettuun valuuttaan ja joilla ei ole samaa oikeudellista asemaa kuin valuutalla tai rahalla, mutta jotka luonnolliset henkilöt tai oikeushenkilöt hyväksyvät vaihdantavälineenä ja joita voi siirtää, varastoida ja myydä sähköisesti” (EU 2018/843).

AMLD5 direktiivin myötä myös virtuaalivaluuttapalveluntarjoajat luetaan samaan kategoriaan muiden finanssialan toimijoiden kanssa, ja näin joutuvat noudattamaan samoja rahanpesun estämisen keinoja ja prosesseja. Näihin kuuluvat esimerkiksi velvoitteet kerätä monipuolisemmin tietoja asiakkaista sekä perusta-

maan riskiperusteiset toiminnot eri asiakassuhteille. Lisäksi virtuaalivaluuttapalveluntarjoajien pitää toimittaa SAR-raportteja (Suspicious Activity Report) kansallisille valvontaviranomaisille epäilyttävistä liiketapahtumista. SAR-raportin tarkoitus on auttaa viranomaisia havaitsemaan mahdolliset rahanpesu- ja terrorismin rahoitustapaukset. SAR-raporttien pohjalla voivat olla esimerkiksi asiakaan suuret käteistalletukset tai nostot, epäilyttävät ulkomaansiirrot, monimutkaiset varallisuuden siirrot tai muut epäilyksiä nostavat tekijät. Suomessa SAR-ilmoituksia käsittelee Keskusrikospoliisin alainen Rahanpesun selvittämiskeskus.

Virtuaalivaluuttojen säädännön ohella AMLD5 sisältää lisäyksiä muun muassa ”esiladattujen” prepaid-maksukorttien sääntelyyn ja tunnistamisvelvoitteeseen. Prepaid-maksukorteilla tarkoitetaan perinteisistä pankki- ja luottokorteista eroavia maksukortteja, joita ei ole liitetty pankkitiliin ja/tai niihin ei liity yksittäiseen henkilöön tai yritykseen yhdistettävää luotto-ominaisuutta. Prepaid-maksukortille ladataan etukäteen varallisuutta esimerkiksi kaupoissa tai tilisiirrolla, ja korttia voi käyttää maksuvälineenä lähes kaikkialla. Näihin kortteihin liittyy rahanpesun riskejä, koska maksuliikennettä ei ole liitetty usein tarkan regulaation kohteena olevaan pankkiin tai luottolaitokseen. Maksukortti on myös huomattavasti helpompi kuljettaa rajan yli kolmansiin maihin kuin nippu käteistä. Prepaid-maksukortit tarjoavat suhteellisen paljon anonymiteettiä maksutapahtumiin, sillä kortin voi ladata esimerkiksi käteisellä rahalla kaupassa, ja rahat käyttää tämän jälkeen digitaalisesti lähes missä tahansa maapallolla. Prepaid-kortit tarjoavat myös virtuaalivaluuttojen käyttäjille ”entry-” ja ”exit”-pisteet varojen käyttämiseen. Käyttäjät voivat esimerkiksi ladata varoja kortille käteisellä, käyttää korttia virtuaalivaluuttojen hankintaan ja lopuksi käyttää omistamiaan tai myymiään virtuaalivaluuttavaroja suoraan tai epäsuorasti ladatakseen varoja toiselle prepaid-kortille edelleen käytettäväksi maksutapahtumissa. AMLD5 direktiivin seurauksena myös prepaid-korttien tarjoajien tulee noudattaa samoja sääntöjä kuin perinteisten rahoituslaitosten, jolloin prepaid-korttien käyttö osana rahanpesuketjua on hankalampaa.

Lisäyksiä tuli myös poliittisesti vaikutusvaltaisten (engl. PEP, Politically Exposed Person) henkilöiden sekä yritysten tosiasiallisten edunsaajien (engl. UBO, Ultimate Beneficial Owner) tunnistamiseen. Poliittisesti vaikutusvaltaisella henkilöllä tarkoitetaan henkilöä, joka on ollut tai on korkea-arvoisessa julkisessa tehtävässä tai poliittisesti merkittävässä virassa 12kk aikana. Lisäksi heidän lähipiiriänsä

(kumppania, lapsia ja heidän aviopuolisoita, vanhempia tai yhtiökumppaneita) voidaan pitää RCA-henkilöinä (engl. Relative or Close Associate). PEP/RCA-henkilöillä on korkeampi riski syyllistyä esimerkiksi korruptioon tai muuten hyväksikäyttämään asemaansa omaksi tai läheistensä eduksi. (Almatalent.fi, n.d.)

Tosiasiallisella edunsaajalla tarkoitetaan henkilöä tai henkilöitä, jotka tosiasiassa hallitsevat yritystä tai yhteisöä tai muuta kautta hyötyvät yrityksen kautta muodostuvista varoista ja tuloista. Suomessa yritysten tulee ilmoittaa tosiasialliset edunsaajat kaupparekisteriin, josta näitä tietoja saa käyttöönsä rahanpesulain mukaista valvontatehtävää suorittavat viranomaiset, tuntemisvelvollisuuden omaavat yritykset, median edustajat sekä muut tahot, joilla on oikeus tietoihin rahanpesulain nojalla. (PRH.fi, 2023.)

5 KÄYTÄNNÖN RISKIENHALLINTA FINANSSIALAN TOIMIJOILLE

5.1 Asiakkaan tuntemisen velvollisuudet (KYC)

Finanssialan ja muiden rahoitusalan toimijoiden (ilmoitusvelvollisten) on velvollisuus tunnistaa ja todentaa asiakkaidensa henkilöllisyys vakituisia asiakassuhteita perustettaessa. Näitä kerättäviä tunnistamisen tietoja kutsutaan usein KYC-tiedoiksi (engl. Know-Your-Customer). Näihin velvollisuuksiin kuuluu muun muassa tiedon kerääminen asiakkaan toiminnasta, liiketoiminnan laajuudesta, perusteet ilmoitusvelvollisen tuotteiden tai palveluiden tarpeelle sekä tiedot edustajasta, edunsaajasta ja omistusketjusta sekä taloudellisesta asemasta ja varojen alkuperästä. (Andersen 2020, 77.)

Yksityishenkilöiden ja yritysten sekä muiden yhteisöjen tunnistamiseen voidaan käyttää erilaisia tunnistamisen keinoja ja vaatimuksia asiakassuhteen mukaan. Esimerkiksi yksityishenkilöitä tunnistaessa tärkeitä dokumentoitavia asioita ovat esimerkiksi kansalaisuus ja mahdollinen poliittinen asema, kun taas yritysasiakkaiden kohdalla merkityksellisempiä tietoja ovat liiketoimintamaat sekä omistajarakenne.

Koska tässä opinnäytetyössä keskitytään virtuaalivaluuttojen rahanpesuriskin hallintaan, ei työssä oteta kantaa jo olemassa oleviin asiakkaan tuntemisen toimiin. Sen sijaan tarkoituksena on tuoda esiin ehdotuksia, miten esimerkiksi KYC-tietojen keräämisessä voidaan ottaa huomioon virtuaalivaluuttojen käyttö, ja miten arvioida niistä muodostuvia riskejä. Virtuaalivaluuttoja käyttävä asiakas voi olla yksityis- tai yritysasiakas, ja olla minkä tahansa ikäinen, toimia millä tahansa alalla tai missä tahansa maanosassa.

KYC-tietoja kerättäessä asiakkaalta on hyvä selvittää, miksi asiakas haluaa käyttää virtuaalivaluuttoja. Yleisimpiä syitä saattaisivat olla spekulatiivinen sijoittaminen, maksuvälineenä käyttäminen tai mielenkiinto teknologiaa kohtaan.

Spekulatiivinen sijoittaminen:
Asiakas saattaa hakea virtuaalivaluutoista tuottoa ja käyttää niitä sijoituskohteina. Tällöin hän pyrkii hyötymään virtuaalivaluuttojen hinnanvaihteluista ja arvonnoususta. Asiakkaalta voi tarkentaa, pitääkö hän ostamiaan virtuaalivaluuttoja lompakossaan odottaen arvonnousua (engl. Holding) vai sijoittaako nämä eteenpäin korkotuottoa tarjoaviin palveluihin (engl. Staking). Asiakkaalta on myös hyvä varmistaa hänen ymmärtävän virtuaalivaluuttojen toimintaperiaatteet, riskinottohalukkuuden sekä verotuskäytänteet.

Maksuvälineenä käyttäminen:
Asiakas haluaa käyttää virtuaalivaluuttoja maksuvälineenä sitä tukevissa palveluissa ja kaupoissa. Vaikkakin virtuaalivaluutoilla suoritettavat maksut ja sitä tukevat kaupat ovat yhä melko harvinaisia, teknologia on tullut yhä useamman saataville. Lähitulevaisuudessa yhä useammat kaupat ja erityisesti verkkokaupat saattavat tarjota vaihtoehtoisia maksutapoja juuri virtuaalivaluuttojen muodossa. Asiakkaalta voi kysyä, millaisia maksutapahtumia asiakas suunnittelee tekevänsä tai kuinka paljon aikoo käyttää virtuaalivaluuttoja maksuvälineenä. Riskiarvioinnissa tulee erityisesti kiinnittää huomiota aktiiviseen FIAT-valuutan vaihdantaan suuntaan tai toiseen eri markkinapaikoilla, jotta voidaan tehokkaasti rajoittaa ilmoitusvelvollisen osuutta rahanpesuketjussa.

Mielenkiinto teknologiaa kohtaan:
Jotkut asiakkaista ovat kiinnostuneita lohkoketjuteknologiasta ja haluavat kokeilla erilaisia virtuaalivaluuttojen mahdollistamia palveluita. He saattavat osallistua esimerkiksi yksityishenkilöinä tai yrityksenä virtuaalivaluuttojen louhintaan tai ylläpitää hajautettua verkkoa, joista muodostuu tuloja. Asiakkaalta on hyvä varmistaa, muodostuuko hänelle tuloja tällaisista lähteistä tai onko toiminta merkittävä osa yrityksen liiketoimintaa.

Joissain tapauksissa voi olla myös tarpeen selvittää, mitä välitysalustaa asiakas on suunnitellut käyttävänsä virtuaalivaluuttojen hankintaan ja kaupankäyntiin. Näitä tietoja on helppo verrata toteutuneisiin tietoihin esimerkiksi tiliotteiden tai tositteiden perusteella. Useimmiten kauppapaikat ovat ulkomaisia, joten kaupankäyntiin käytettävät FIAT-valuutat siirretään ensin joko tilisiirrolla tai korttimaksuja tarjoavan palvelun välityksellä itse kauppapaikkaan. Käytettävästä kauppapaikasta tulisi selvittää, missä se on rekisteröity, kuuluuko se yleisimpiin ja turvallisimpiin kauppapaikkoihin ja onko itse kauppapaikalla oma KYC velvollisuus. Erityistä huomiota tulisi kiinnittää asiakkaan käyttämiin vähemmän tunnettuihin kauppapaikkoihin, jotka voivat toimia laittomasti, ilman talousrikollisuuden estämiseen liittyviä toimenpiteitä tai jo itsessään olla petossivustoja.

Itse kauppapaikassa virtuaalivaluuttojen hankinta voidaan suorittaa joko samassa palvelussa olevaan virtuaalivaluuttalompakkoon tai asiakkaan omaan lompakkoon. Kauppapaikoissa pysyvät lompakot ovat talousrikollisuuden estämisen kannalta hieman turvallisempia, koska kauppapaikat ovat usein velvollisia suorittamaan rahanpesun estämisen prosesseja ja esimerkiksi seuraamaan asiakkaan tekemiä varasiirtoja. Sen sijaan asiakkaan omaan lompakkoon tehdyt siirrot siirtyvät pois tarkkailun alta, ja voivat siten siirtyä käytettäväksi rikollisiin tarkoituksiin.

Asiakkaalta voidaan kysyä, miten paljon hän aikoo siirtää kuukausittain varallisuutta FIAT-valuutoista virtuaalivaluutoiksi ja päinvastoin. Vertaamalla näitä tietoja aiemmin annettuihin sekä asiakkaan tulon lähteisiin voidaan arvioida, liittyykö toimintaan mitään epäilyttävää. Jos asiakas on esimerkiksi aiemmin sijoittanut vain pieniä summia virtuaalivaluuttoihin, mutta haluaa nostaa yhtäkkiä palvelusta huomattavia kertasuorituksia ja siirtää niitä eteenpäin, voi olla syytä selvittää varojen alkuperää.

Tärkeänä osana on myös selvittää varojen alkuperä asiakkaan käydessä kauppaa virtuaalivaluutoilla. Yksityisasiakkailla tulot muodostuvat useimmiten palkasta ja yrityksillä liiketoiminnan tuotoista. Asiakkaalta voidaan kysyä, hankkiiko hän omistamansa virtuaalivaluutat ostamalla suoraan pörsseistä, onko hän saanut ne esimerkiksi lahjoituksena vai tekeekö hän jotain toimintaa virtuaalivaluut-

tojen eduksi, kuten louhintaa tai verkon ylläpitoa, josta maksetaan suoraan virtuaalivaluuttana. Virtuaalivaluutoista muodostuvia tuloja voidaan verrata asiakkaan muihin tuloihin tai liikevaihtoon, jolla saadaan parempi kokonaiskuva asiakkaan tulorakenteesta.

Joissain tapauksissa ainoa tapa saada selvyys asiakkaan virtuaalivaluuttojen maksuliikenteelle on pyytää toimittamaan transaktio-ote, josta selviää maksujen lähettäjät, vastaanottajat ja summat. Julkisia avaimia sisältävät otteet helpottavat rahaliikenteen selvittämistä suuremmissa kokonaisuuksissa, sekä viranomaisten työtä, jos asiakassuhteesta on tehtävä SAR-ilmoitus.

Oleellisena osana KYC:in muodostamisessa asiakkaasta on myös jatkuvan tuntemisen (engl. Ongoing-Due-Diligence, ODD) merkitys. Koska asiakkaasta kerättyjä KYC-tietoja voidaan käyttää arvioimaan asiakkaan liiketoimien oikeudellisuutta, on tietoja päivitettävä säännöllisin väliajoin, riippuen esimerkiksi asiakkaan toiminnan laajuuden tai asiakkaan muodostamaan riskiprofiiliin verraten (Andersen 2020, 84). Osana jatkuvaa tuntemista on tärkeää tarkastella, miten asiakkaan todellinen toiminta on vastannut alun perin KYC:ille kerättyjä tietoja, ja päivittää tietoja ja riskiarvioita sitä mukaan, kun muutoksia asiakkaan toimissa ilmenee. Esimerkiksi yksityishenkilön pääsääntöiset tulonlähteet tai yritysten vastuuhenkilöt voivat muuttua, jotka saattavat vaikuttaa asiakkaan muodostamaan riskitasoon.

Liitteeseen 1. on kerätty perusmuotoinen listaus asiakkaalle esitettävistä KYC-kysymyksistä juuri virtuaalivaluuttojen käytön osalta, sekä arviointitaulukko asiakkaan riskiprofiilin muodostamiseen. Lomake ja arviointitaulukko on tarkoitettu esimerkiksi, ja jokaisen ilmoitusvelvollisen tulee itse arvioida, millainen virtuaalivaluuttojen käyttö aiheuttaa minkäkin verran riskiä asiakassuhteelle. Annettuja tietoja tulee myös verrata asiakkaan muuhun toimintaan ja maksukäyttäytymiseen, jotta ilmoitusvelvollinen voi kokonaisuutena arvioida asiakkaan käyttäytymistä.

5.2 Transaction monitoring (TM)

Liiketapahtumien seurannalla (engl. Transaction monitoring) tarkoitetaan finanssilaitosten ja muiden ilmoitusvelvollisten prosesseja ja järjestelmiä, joilla seurataan asiakkaiden tekemiä epätavallisia tai epäilyttäviä siirtoja ja tapahtumia laittomien toimintojen estämiseksi. Maksulaitoksilla, kuten pankeilla, rahoituslaitoksilla ja maksukorttiyhtiöillä nämä toiminnot ovat usein automatisoituja osaksi maksujärjestelmiä. Kuitenkin myös muiden ilmoitusvelvollisten, kuten tilitoimistojen ja kiinteistönvälittäjien on hyvä tuntea ja tunnistaa, millaisia liiketapahtumia heidän asiakkaansa tyypillisesti tekevät, sekä erottaa epätavalliset ja korkean riskin tapahtumat.

Virtuaalivaluuttojen osalta ilmoitusvelvollisilla on usein hyvä näkyvyys vain Fiat-valuuttojen ja virtuaalivaluuttojen välisistä siirroista, koska virtuaalivaluuttojen siirrot näkyvät ainoastaan lohkoketjussa. Tämän vuoksi erityisesti virtuaalivaluuttojen ja perinteisen rahoitusjärjestelmän rajapinnoilla toimivien tahojen, kuten kryptovaluuttapörssien ja pankkien, on oltava erityisen tarkkoja heidän alustoillaan tapahtuvista siirroista. Perinteisessäkin rahoitusjärjestelmässä toimivien tahojen on tärkeää tarkkailla asiakkaidensa tekemiä siirtoja, niiden suuruksia ja erityisesti vastapuolia.

Asiakkaiden maksuista selviävät virtuaalivaluuttapörssit voivat auttaa ymmärtämään, millaisia palveluita asiakas käyttää sekä mahdollisesti niistä nousevia riskejä. Jos asiakas käyttää esimerkiksi tunnetusti rahanpesulainsäädäntöä välttävää virtuaalivaluuttavälittäjää, on hänen liiketapahtumiansa syytä tarkkailla erityisen tarkasti. Vastaavasti jos asiakas käyttää suurimpia ja tunnetuimpia virtuaalivaluuttapörssejä, jotka jo itsessään käyttävät rahanpesun ja terrorismin rahoittamisen estämisen prosesseja osana toimintaansa, voi tätä tietoa hyödyntää asiakkaan riskiarvioinnissa.

Tahot, joilla on näkymä myös asiakkaidensa virtuaalivaluuttasiirtoihin, voivat saada yhä paremman kuvan, miten varallisuus liikkuu eri osapuolten välillä lohkoketjuissa. Vaikka virtuaalivaluuttasiirrot ovat nopeita, kansainvälisiä ja osittain anonyymejä, hyödyntämällä tehokkaita työkaluja lohkoketjuanalyysiin voidaan selvästi pienentää riskiä joutua osaksi rikollista toimintaa.

Esimerkiksi Yhdysvaltalainen Chainalysis Inc. on kehittänyt Bitcoinin lohkoketjun tutkimiseen soveltuvan tekoälyä hyödyntävän analysointityökalun. Työkalu on suunniteltu erityisesti rahanpesun ja muiden rikollisten toimien havaitsemiseen virtuaalivaluuttamaailmassa. Työkalun avulla tutkijat ja muut organisaatiot pystyvät esimerkiksi visualisoimaan virtuaalivaluuttojen alku- ja loppupisteet ja pysymään mukana varojen liikkeissä. Jos virtuaalivaluuttojen siirroissa on mukana lompakoita, jotka ovat aiemmin ollut yhteydessä epäilyttäviin toimijoihin, voidaan näistä automaattisesti muodostaa riskiarvioita tai ottaa siirrot tarkemmin tutkittaviksi. Työkalussa on myös oma tietokanta tunnetuista lompakoista, joita käytetään tai on käytetty rikollisiin toimintoihin, jotka voidaan nopeasti yhdistää esimerkiksi asiakkaan tekemiin siirtoihin. (Chainalysis.com n.d.)

Tällaiset lohkoketjun analysointityökalut kuitenkin vaativat jonkinlaisen pohjatiedon, jolla päästä kiinni perinteisestä rahoitusmaailmasta virtuaalivaluuttamaailmaan siirtyviin maksuihin, kuten lompakon julkisen osoitteen tai muun yksilöivän tunnisteen. Tämän vuoksi tällaisia analysointityökaluja voivat hyödyntää vain virtuaalivaluuttapalveluntarjoajat tai muut tahot, jotka tunnistavat asiakkaidensa käyttämät lompakot. Tulevaisuudessa rahanpesun estämiseen kerätyn datan avoimuus voisi mahdollistaa entistä tehokkaamman ja reaaliaikaisen tutkimisen sekä perinteisessä rahoitusmaailmassa toimivien tahojen että virtuaalivaluuttapalveluiden välillä. Kuitenkin, samalla kun tiedon avoimuus voi helpottaa rahanpesun estämistyötä, se tuo myös mukanaan haasteita liittyen yksityisyyteen ja tietoturvaan.

5.3 Mahdollisuus riskiperusteiseen arviointiin

Vuoden 2015 EU:n AMLD4 direktiivin myötä otettiin käyttöön riskiperusteinen lähestymistapa rahanpesun ja terrorismin rahoittamisen estämiseen. Suomessa tämä direktiivi vahvistettiin kansallisella lainsäädännöllä 2017. Riskiperusteisella lähestymistavalla tarkoitetaan sitä, että ilmoitusvelvollisen tekemiä asiakkaan tuntemisen toimia suhteutetaan asiakkaasta nouseviin riskitasoihin, kuten liiketoimiin, tarvittuihin palveluihin ja tuotteisiin tai aiempaan maksukäyttäytymiseen. (Andersen 2020, 73.)

Käytännössä ilmoitusvelvollisen tulee myös arvioida omista tuotteista, palveluista sekä toimintamalleistaan nousevia riskejä. Nämä riskit voivat olla erilaisia riippuen ilmoitusvelvollisen toimialasta, kuten onko kyseessä tilitoimisto, pankki tai vaikkapa kiinteistönvälittäjä. Tilitoimistot voivat esimerkiksi kohdata asiakkaiden pyyntöjä kirjata kirjanpitoon virheellisiä tai harhaanjohtavia tietoja, joilla pyritään piilottamaan rahan todelliset summat ja käyttötarkoitus. Pankit taas voivat kohdata asiakkaiden väärinkäyttävän monimutkaisia maksutapoja, kuten remburs-seja tai hyödyntävän tavallista pankkitiliä ja käteismaksuja osana rahanpesuketjua. Ilmoitusvelvollisen tulee huomioida oman toimintansa riskiarviossa toiminnan luonne, koko ja laajuus, sekä varmistua sisäisten prosessien suorittavan riittävää toiminnan valvontaa ja toimenpiteitä. Riskiarvion pohjaa ei kuitenkaan ole määritelty, vaan jokaisen ilmoitusvelvollisen tulee tehdä oma tulkinta, millaisia riskejä ja haavoittuvuuksia omaan toimintaan liittyy ja millaisilla keinoilla riskejä voidaan tehokkaasti hallita. (Andersen 2020, 66.)

Virtuaalivaluuttojen osalta ilmoitusvelvollisten tulee käyttää omaa harkintaa kuinka suuria riskejä ne voivat aiheuttaa asiakkaidensa kautta. Asiakassuhteet voi olla tarpeellista jakaa matalaan, normaaliin, korkeaan ja erittäin korkeaan riskiluokkaan, tai mihin tahansa näiden luokkien yhdistelmiin. Andersen (2020) on antanut tuntemisen luokkaesimerkeiksi yksinkertaistettu, normaali sekä tehostettu tunteminen. Virtuaalivaluuttojen käyttö jo itsessään sisältää merkittäviä riskejä esimerkiksi varallisuuden peittelystä, veronkierrosta sekä petoksista. Tämän vuoksi asiakasta voi olla mahdotonta pitää pienimmän riskitason asiakkaana, jos hän käyttää virtuaalivaluuttoja. Kuitenkin on tärkeää ymmärtää, että kaikki virtuaalivaluuttojen käyttäjät eivät ole rikollisia tai epärehellisiä. Monet käyttävät virtuaalivaluuttoja laillisesti ja eettisesti esimerkiksi sijoituksena, maksuvälineenä tai teknisen kiinnostuksen kohteena.

Ilmoitusvelvollisten tahojen tulisi ottaa huomioon asiakkaan kokonaistilanne arvioitaessa riskiä. Esimerkiksi asiakkaan sijoituskäyttäytyminen, siirtojen luonne ja määrä, sekä mahdolliset yhteydet tunnettuihin korkean riskin osapuoliin voivat antaa tarkemman kuvan asiakkaan riskiprofiilista. Näiden tietojen perusteella hänet voidaan luokitella paremmin sopivaan riskiluokkaan. Tässä yhteydessä myös

asiakkaan toimittamat selvitykset ja dokumentaatio voivat auttaa vähentämään epäilyjä ja ymmärtämään paremmin hänen toimintamotiivejaan.

Toisaalta, kun otetaan huomioon virtuaalivaluuttojen monimutkaisuus ja nopeasti muuttuva luonne, ilmoitusvelvollisten laitosten on syytä olla varovaisia ja ajan tasalla alan kehityksestä. Jatkuva koulutus ja yhteistyö sekä paikallisten että kansainvälisten viranomaisten kanssa ovat elintärkeitä riskien ymmärtämiseksi ja niiden oikeanlaiseen arviointiin.

6 TULEVAISUUDEN SUUNNAT

6.1 Keskuspankkien virtuaalivaluutat

Sääntelemättömien virtuaalivaluuttojen yleistyminen viimeisten kymmenen vuoden aikana on kiinnittänyt myös keskuspankkien huomion. Tavallisen käteisen käsitteleminen on kallista, aikaa vievää sekä mahdollistaa osaltaan harmaan talouden toiminnan jatkumisen. Sen vuoksi yhä useammat keskuspankit ovat suunnitelleet tai jo ottaneet käyttöön omia keskuspankkien digitaalisia valuuttoja (engl. Central Bank Digital Currencies, CBDC). Maailmanlaajuisesti keskuspankkien liikkeeseen laskemia digitaalisia valuuttoja on 11 kappaletta, ja ne ovat käytössä kymmenessä Karibian saarivaltiossa sekä Nigeriassa (Atlantic Council n.d).

Keskuspankkien digitaaliset valuutat eroavat jonkin verran jo tutuksi tulleista virtuaalivaluutoista. Keskuspankkien valuutat ovat keskitetyn toimijan liikkeeseen laskemia, eikä niillä välttämättä ole samankaltaisia yksityisyyteen liittyviä ominaisuuksia kuin tällä hetkellä olemassa olevilla virtuaalivaluutoilla. Keskuspankkien digitaalisten valuuttojen ei edes tarvitse perustua lohkoketjuun, eikä ne välttämättä tarjoa samankaltaista läpinäkyvyyttä kuin esimerkiksi Bitcoin. Toisaalta digitaaliset valuutat mahdollistaisivat nopeat pankeista riippumattomat varasiirrot, ilman riskiä pankkien palvelukatkoksille tai pahimmassa tapauksessa likviditeettikriiseille. Tällainen järjestelmä, jossa useat rahaliikenteen välikädet, kuten pankit, maksukorttioperaattorit ja rahoituslaitokset olisivat turhia, toisi huomattavia yksinkertaistuksia maailman rahaliikenteeseen ja siihen liittyviin kuluihin. Digitaaliset valuutat mahdollistaisivat myös rahapalveluiden saamisen syrjäisillä seuduilla, joissa ei muuten saa perinteisiä pankkipalveluita. Vaikka tämä ei ole Suomessa merkittävä ongelma, voisivat monet kehittyvät maat hyötyä digitaalisten valuuttojen tuomista hyödyistä. (Shobhit 2023.)

Rahanpesun estämisen näkökulmasta digitaaliset keskuspankkivaluutat toisivat toivottuja apuja rahan jäljitettävyyteen. Käyttivätpä ne lohkoketjua tai ei, keskitetty keskuspankin hallinta sekä maksuliikenteen välikäsien väheneminen toisi huomattavia helpotuksia rahan liikkeiden seurantaan. Tällaisessa tilanteessa transaktioihin liittyvää dataa ei olisi hajautetusti pankeissa, korttioperaattoreilla ja

muilla ilmoitusvelvollisilla, vaan kaikki data löytyisi keskitetysti joko keskuspankilta tai lohkoketjusta. Tämä myös voisi vähentää jokaisen ilmoitusvelvollisen tarvetta suorittaa asiakkaan tuntemisen ja transaktiomonitoroinnin tehtäviä, jolloin koko rahaliikennettä voisi tutkia keskuspankin alainen toimija. Digitaaliset valuutat mahdollistaisivat myös käteisen määrän vähenemisen maksutapana, jolla voidaan myös tehokkaasti kitkeä sen aiheuttamia rahanpesun riskejä.

Myös Euroopan keskuspankki on suunnitellut ottavansa käyttöön digitaalisen euron digitaalisena keskuspankkivaluuttana. Projekti on käynnistetty lokakuussa 2021 tutkimusvaiheella ja sen on tarkoitus päättyä syksyllä 2023. Digitaalisen euron on tarkoitus toimia kolikko- ja setelirahan vastikkeena, tarjoten uudenlaisen, modernin maksutavan. Nykyisistä virtuaalivaluutoista poiketen se olisi keskuspankin takaamaa ja sidottu euron arvoon, mikä helpottaisi sen käyttöä ensisijaisena maksutapana (Euroopan keskuspankki n.d).

6.2 Teknologiset kehitysaskeleet

Tulevaisuuden tuomat teknologiset mullistukset voivat vaikuttaa merkittävästi virtuaalivaluuttojen käytön yleisyyteen ja turvallisuuteen. Erityisesti kvanttitietokoneet muodostavat merkittävän uhan virtuaalivaluuttojen lohkoketjujen hyödyntämille salausalgoritmeille. Kvanttitietokoneiden moninkertainen laskentateho mahdollistaisi kaikkien perinteisillä tietokoneilla muodostettujen salausavainten purkamisen ennennäkemättömän nopeasti, mikä aiheuttaisi merkittäviä riskejä lohkoketjujen integriteetille, sekä myös kaikelle maailmanlaajuiselle tietotekniikalle. Vaikkakin kvanttiteknologia on vielä kehitysvaiheessa, ennustetaan niiden pystyvän purkamaan lohkoketjujen salaukset noin 10–20 vuoden sisällä (Van der Haegen 2022).

Samanaikaisesti myös tehokkaiden tekoälypalveluiden ja koneoppimisen kehittyminen tarjoaa uusia keinoja rahanpesun estämiseksi ja havaitsemiseksi. Rahanpesun estämistyöhön kuuluvan datamäärän analysoinnissa tekoäly voi toimia erittäin tehokkaana apukeinona ja vähentää manuaalisen käsittelyn tarvetta. Tämä ei ainoastaan nopeuta prosesseja, vaan myös lisää niiden tarkkuutta, kat-

tavuutta ja luotettavuutta. Lisäksi tekoälyn itseoppivat ominaisuudet mahdollistavat, että se voi jatkuvasti parantaa ja mukautua rahanpesun uusiin ja kehittyviin tekniikoihin, tarjoten siten ajan myötä entistä tehokkaamman suojan rikollisilta toiminnoilta. Tekoälyn käyttö voi myös vapauttaa ihmistyöntekijöitä keskittymään monimutkaisempiin ja vaativampiin tehtäviin, kuten poikkeavien tapausten syvälliseen tutkimukseen ja analysointiin.

6.3 Virtuaalivaluuttojen tulevaisuus

Aiemmin mainitut keskuspankkien digitaaliset valuutat voivat olla se tekijä, joka tuo virtuaalivaluutat laajasti kansan käyttöön. Keskuspankkien takaus ja tuttu euro tekevät näistä valuutoista helpommin lähestyttävän, sekä se toisi vihdoin laajasti käyttömahdollisuuksia virtuaalisten valuutoiden omistajille. Samalla kun keskuspankkien valuutat yleistyisivät, toisi se mukanaan kiinnostuneita myös nykyisille virtuaalivaluutoille.

Suurimmat ongelmat nykyisten virtuaalivaluuttojen skaalautuvuuden tiellä ovat energian käyttö, sääntelyn puute sekä volatiliteetti. Bitcoinin Proof-of-Work konsensusmetodi käyttää vuosittain noin 127 TWh sähköenergiaa (Huestis 2023), kun esimerkiksi Suomi käytti vuonna 2020 noin 81 TWh (Tilastokeskus 2021). Valtava energian käyttö hankaloittaa Bitcoinin käytön laajentumista, vaikkakin korkea energiankäyttö on tuonut mukanaan investointeja uusiutuviin energianlähteisiin. Useat muut virtuaalivaluutat käyttävät Proof-of-Stake konsensusmetodia, jonka energiankäyttö on vain murto-osia Bitcoinin vastaavasta. Sääntelyn vähäinen määrä tai sen täydellinen puuttuminen vaikeuttaa osaltaan virtuaalivaluuttojen yleistymistä. Virtuaalivaluutat nähdään yhä spekulatiivisena sijoituskohteena, eikä monet virtuaalivaluuttojen omistajat ole ikinä käyttäneet niitä maksuvälineenä. Koska esimerkiksi bitcoinin takana ei toimi mikään yksittäinen taustaorganisaatio, perustuu bitcoinin käytön laajeneminen yksin loppukäyttäjien tahtoon. Taustaorganisaation puuttuminen vaikeuttaa avun saamista ongelmatilanteissa, ja jättää kuluttajat suojattomaan asemaan. Monimutkaiset verotuskäytänteen taas vaikeuttavat sekä kauppiaiden että kuluttajien siirtymistä virtuaalivaluuttojen maksukäyttäjiksi, koska jokaisesta transaktiosta, jossa virtuaalivaluutta vaihtuu euroiksi tai päinvastoin, muodostuu verotettava tapahtuma.

Tapahtumien monimutkaisuus tekee päivittäisestä kaupankäynnistä hyvin hankalaa.

Myös yksi merkittävimpiä ongelmia ovat virtuaalivaluuttojen volatiliteetti, eli arvon nopeat muutokset lyhyellä aikavälillä. Kaupankäynnissä tuotteiden ja palveluiden arvot pitää muuttaa virtuaalivaluutoiksi juuri sillä kaupantekohetkellä, jotta kummallekaan osapuolelle ei synny merkittävää valuuttariskiä. Tilannetta voisi verrata ulkomaisella valuutalla käytävään kauppaan, jossa valuuttakurssit tavallisesti muuttuvat hieman esimerkiksi viikon sisällä. Ongelma virtuaalivaluuttojen kohdalla on arvon nopeat, jopa useiden prosenttien, muutokset minuuttien sisällä. Tämä vaikeuttaa huomattavasti valuuttariskin hallintaa, sekä aiheuttaa ylimääräisiä kuluja ja työtä, sekä saattaa täysin mitätöidä virtuaalivaluuttojen käyttämisen hyödyt kaupankäynnissä.

7 POHDINTA

Opinnäytetyössä keskityttiin virtuaalivaluuttojen osuuteen rahapesun prosesseissa sekä arvioitiin, miten ilmoitusvelvolliset pystyvät vähentämään näiden käyttöön liittyviä riskejä. Lisäksi tutkittiin, millaisia tulevaisuuden näkymiä virtuaalivaluutoilla on osana finanssimaailmaa. Opinnäytetyön tuloksena saatiin koottu tietopaketti virtuaalivaluutoista ja lohkoketjuteknologiasta, rahanpesusta, lainsäädännöstä sekä mahdollisista riskien minimoinnin toimista, erityisesti asiakkaan tuntemistietojen ja liiketoimien seurannan osalta. Opinnäytetyön yhtenä tavoitteena oli ymmärtää, miten virtuaalivaluuttoja voidaan käyttää rahanpesun välineenä. Tähän onnistuttiin vastaamaan tutkimalla virtuaalivaluuttojen tekniikkaa sekä tutustumalla tämän teknologian mahdollistamiin rahanpesun keinoihin.

Toisena tavoitteena oli selvittää finanssialan toimijoille sopivia työkaluja, joilla voidaan hallita virtuaalivaluuttojen käytöstä nousevia riskejä. Asiakkaan tuntemistietojen muodostamiseen virtuaalivaluuttojen käytön osalta sekä siihen liittyvä riskiarvio-lomake antaa suuntaa ilmoitusvelvollisille, jotka haluavat tarkemmin arvioida asiakkaidensa virtuaalivaluuttojen käyttöön liittyviä riskejä ja minimoida niitä.

Virtuaalivaluuttojen käytön yleistyessä henkilökunnan on tärkeää saada koulutusta, jotta he voivat tunnistaa asiakkaan virtuaalivaluuttojen käytön sekä mahdolliset perusteettomat liiketapahtumat. Vaikka suurin osa virtuaalivaluutoista tarjoaa läpinäkyvyyttä maksuliikenteeseen, sen ymmärtäminen vaatii paljon mukautumista, uudenlaisia työkaluja sekä aktiivista otetta.

Lisäksi opinnäytetyössä käytiin lyhyesti läpi virtuaalivaluuttojen tulevaisuuteen liittyviä mahdollisuuksia ja ongelmia. Virtuaalivaluutat ja lohkoketju ovat teknologiana vielä hyvin uusia, joten niiden käytön laajuus riippuu suuresti eri toimijoiden panostuksista tähän teknologiaan sekä sääntelyn vaikutuksista. Keskuspankkien kiinnostus virtuaalisia valuuttoja kohtaan kuitenkin avaa paljon mahdollisuuksia niiden käytölle osana maailmanlaajuista rahaliikennettä.

Opinnäytetyön osana olisi voinut muodostaa kattavamman työkalupaketin ilmoitusvelvollisten käyttöön esimerkin KYC-lomakkeen lisäksi. Ilmoitusvelvollisia on

kuitenkin liian paljon jakautuneena eri toimialoille ja erilaisiin finanssimaailman tehtäviin, ettei yksi yleiseen käyttöön suunniteltu työkalusarja olisi tukenut ilmoitusvelvollisten tarpeita riittävän kattavasti eri osa-alueilla. Työkalusarjan koostaminen yksittäiselle toimeksiantajalle, esimerkiksi tilitoimistolle, olisi ollut huomattavasti helpompi ja suoraviivaisempi prosessi ja se olisi kattanut juuri kyseisen ilmoitusvelvollisen riskienhallinnan tarpeet.

8 LÄHTEET

Almatalent. n.d. PEP- ja pakotelistakysely - tunne asiakkaasi taustat. Verkkosivu. Luettu 5.9.2023. https://www.almatalent.fi/kaikki-tuotteet-ja-palvelut/pep-ja-pakotelistakysely/

Atlantic Council. n.d. Central Bank Digital Currency Tracker. Verkkosivu. Viitattu 9.10.2023. https://www.atlanticcouncil.org/cbdctracker/

Ayodeji, Aluko & Mahmood, Bagheri. 2012. The impact of money laundering on economic and financial stability and on political development in developing countries: The case of Nigeria. Emerald.com. https://www-emerald-com.libproxy.tuni.fi/insight/content/doi/10.1108/13685201211266024/full/html

Chainalysis. 2022. The 2022 Crypto Crime Report. Verkkolähde. Viitattu 18.3.2023. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf

Chainlysis.com. n.d. Chainlysis Reactor. Verkkolähde. Viitattu 2.10.2023. https://www.chainalysis.com/chainalysis-reactor/

Coinmarketcap. n.d. Global Cryptocurrency Charts. Verkkolähde. Viitattu 11.9.2023. https://coinmarketcap.com/charts/

Complyadvantage.com. 2023. Understanding Money Laundering in Casinos. Verkkolähde. Viitattu 18.9.2023. https://complyadvantage.com/insights/understanding-money-laundering-in-casinos/

Cryptopedia. 2022. What Are Public and Private Keys? Verkkolähde. Viitattu 12.9.2023. https://www.gemini.com/cryptopedia/public-private-keys-cryptography

Euroopan keskuspankki. N.d. Digitaalinen euro. Verkkolähde. Viitattu 9.10.2023. https://www.ecb.europa.eu/paym/digital_euro/html/index.fi.html

Eduskunta. 2017. Rahanpesulainsäädännön kokonaisuudistus. Verkkosivu. Viitattu 4.9.2023. https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/rahanpesulainsaadannon-kokonaisuudistus.aspx

Euroopan Unionin direktiivi 2018/843. Luettu 4.9.2023. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32018L0843

FATF. 2021. Trade.Based Money Laundering. Verkkolähde. Luettu 25.3.2023. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Risk-Indicators.pdf

Huestis, Samuel. 2023. Cryptocurrency's Energy Consumption Problem. RMI.org. Verkkolähde. Viitattu 10.10.2023. https://rmi.org/cryptocurrencys-energy-consumption-problem/

IDEA.int (International Institute for Democracy and Electoral Assistance). 2017. Money, influence, corruption and capture: can democracy be protected? Verkkolähde. Luettu 25.3.2023. https://www.idea.int/gsod-2017/files/IDEA-GSOD-2017-CHAPTER-5-EN.pdf

IMF (International Monetary Fund). n.d. The imf and the fight against money laundering and terrorism financing. Verkkolähde. Luettu 25.3.2023. https://www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-money-laundering-and-terrorism-financing

Isoaho, Essi & Kaski, Ida-Ellen. 2021. Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021. Valtionvarainministeriö. Luettu 18.3.2023. http://urn.fi/URN:ISBN:978-952-367-715-9

Kenneth, See. 2023. The Satoshi laundromat: a review on the money laundering open door of Bitcoin mixers. Journal of Financial Crime. Luettu 25.3.2023

Kuskowski, Pawel. 2020. Europe's New AML Directive Means Banks Can No Longer Shut Crypto Out. Verkkolähde. Viitattu 18.3.2023. https://www.forbes.com/sites/pawelkuskowski/2020/02/20/europes-new-aml-directive-means-banks-can-no-longer-shut-crypto-out

Kriptomat. n.d. A Brief History of Blockchain Technology That Everyone Should Read. Verkkolähde. Luettu 19.3.2023. https://kriptomat.io/blockchain/history-of-blockchain/

Laki 572/2019. Laki virtuaalivaluutan tarjoajista. Luettu 4.9.2023. https://www.finlex.fi/fi/laki/alkup/2019/20190572

Laki 28.6.2017/444. Laki rahanpesun ja terrorismin rahoittamisen estämisestä. Luettu 4.9.2023. https://www.finlex.fi/fi/laki/ajantasa/2017/20170444

Lamport, Leslie & Shostak, Robert & Please, Marshall. 1982. The Byzantine Generals' Problem. Artikkeli. Luettu 19.3.2023. https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf

Laurence, Tiana. 2019. Blockchain for dummies. Toinen painos. Luettu 22.3.2023.

Markman, Jon. 2021. Why Decentralized Finance Won't Kill Off Mastercard. Forbes. Luettu 19.3.2023. https://www.forbes.com/newsletters/jonmarkman/2021/12/08/why-decentralized-finance-wont-kill-off-mastercard

Merchant, Murtuza. 2022. What is a 51% attack and how to detect it? Cointelegraph.com. Verkkolähde. Luettu 25.3.2023. https://cointelegraph.com/news/what-is-a-51-attack-and-how-to-detect-it

Monero.com. N.d. About Monero. Verkkosivu. Luettu 25.3.2023. https://www.getmonero.org/resources/about/

N-Able. 2019. SHA-256 Algorithm Overview. Verkkolähde. Luettu 25.3.2023. https://www.n-able.com/blog/sha-256-encryption

Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Luettu 19.3.2023. https://bitcoin.org/bitcoin.pdf

Prh.fi. Edunsaajaote. Luettu 5.9.2023. https://www.prh.fi/fi/kaupparekisteri/tietopalvelut/edunsaajaote.html

Rooney, Kate. 2018. $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. CNBC. Luettu 25.3.2023. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html

Sanctions Scanner. 2022. Major Money Laundering Countries. Luettu 28.3.2023. Verkkolähde. https://sanctionscanner.com/blog/major-money-laundering-countries-251

Shah, Pathik. n.a. Socio-economic impact of money laundering. Amluae.com. Verkkolähde. Luettu 18.3.2023. https://amluae.com/socio-economic-impact-of-money-laundering/

Shobhit, Seth. 2023. What Is a Central Bank Digital Currency (CBDC)? Investopedia.com. Verkkolähde. Viitattu 9.10.2023. https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp#toc-issues-cbdcs-address-and-create

Statista.com. n.d. Cryptocurrencies – Worldwide. Verkkolähde. Viitattu 18.3.2023. https://www.statista.com/outlook/dmo/fintech/digital-assets/cryptocurrencies/worldwide

Tilastokeskus. 2021. Uusiutuva energia nousi fossiilisten ja turpeen ohi energian kokonaiskulutuksessa vuonna 2020. Verkkolähde. Viitattu 10.10.2023. https://www.stat.fi/til/ehk/2020/04/ehk_2020_04_2021-04-16_tie_001_fi.html

United Nations. n.d. Money Laundering. Verkkolähde. Viitattu 18.3.2023. https://www.unodc.org/unodc/en/money-laundering/overview.html

Van der Haegen, Jeremy. 2022. Could Quantum Computers Defeat Bitcoin? Not So Fast. Decrypt.co. Verkkolähde. Viitattu 9.10.2023. https://decrypt.co/101340/bitcoin-quantum-computing

Zharun, Taras. 2022. How to Legally Structure Cryptocurrency Exchanges (CEX & DEX). Legalnodes.com. Verkkolähde. Viitattu 29.3.2023. https://legalnodes.com/article/cex-and-dex-legal-structuring

LIITTEET

Liite 1. Esimerkki riskiarviolomakkeesta

Esimerkki virtuaalivaluuttojen KYC-lomakkeesta

Päivämäärä: _____

Käsittelijä: _____

Asiakkaan nimi: _____

Henkilötunnus/y-tunnus: _____

1. **Virtuaalivaluuttojen käyttötarkoitus (valitse yksi tai useampi)**
   - ☐ Sijoittaminen
   - ☐ Ostokset tai kaupankäynti
   - ☐ Rahasiirrot
   - ☐ Muut (tarkenna): _____

2. **Kuinka usein teet siirtoja FIAT-valuutan ja virtuaalivaluuttojen välillä?**
   - ☐ Päivittäin
   - ☐ Viikoittain
   - ☐ Kuukausittain
   - ☐ Harvemmin kuin kerran kuukaudessa

3. **Kuinka suuria siirtoja teet keskimäärin FIAT-valuutan ja virtuaalivaluuttojen välillä kuukaudessa?**
   - ☐ Alle 100 €
   - ☐ 100 € - 999 €
   - ☐ 1000 € - 9 999 €
   - ☐ Yli 10 000 €

4. **Kuinka usein teet siirtoja virtuaalivaluuttojen välillä?**
    - ☐ Päivittäin
    - ☐ Viikoittain
    - ☐ Kuukausittain
    - ☐ Harvemmin kuin kerran kuukaudessa

5. **Kuinka suuria siirtoja teet keskimäärin virtuaalivaluuttojen välillä kuukaudessa?**
    - ☐ Alle 100 €
    - ☐ 100 € - 999 €
    - ☐ 1000 € - 9 999 €
    - ☐ Yli 10 000 €

6. **Miten säilytät omistamiasi virtuaalivaluuttoja?**
    - ☐ Virtuaalivaluuttapörssissä
    - ☐ Omassa lompakossa (Sovellus, laite, muut tavat)

7. **Jos käytät keskitettyä (CEX) virtuaalivaluuttapörssiä/-pörssejä, mainitse eniten käyttämäsi:**
    - _____

8. **Käytätkö hajautettuja markkina-alustoja ja pörssejä? (DEX, DeFi)**
    - ☐ Kyllä
    - ☐ Ei

9. **Omistatko jotain seuraavista virtuaalivaluutoista:**
    - ☐ Bitcoin (BTC), Ether (ETH), Ripple (XRP)
    - ☐ Monero (XMR), Zcash (ZEC), Dash (DASH)

Käsittelijän arvio asiakkaan riskistä

Virtuaalivaluuttoihin liittyy käytännössä aina huomattavia riskejä veronkierrosta varallisuuden peittelyyn. Tämän vuoksi ilmoitusvelvollisen tulee arvioida, voidaanko asiakasta koskaan pitää virtuaalivaluuttojen osalta matalan riskin asiakkaana.

Asiakassuhdetta voidaan käsitellä virtuaalivaluuttojen osalta esimerkiksi:

Normaalin riskin asiakkaana:

- Asiakkaalla on selkeä syy käyttää virtuaalivaluuttoja sijoitusmielessä tai pieniin ostoksiin
- Asiakas tekee siirtoja harvoin FIAT-valuutan ja virtuaalivaluuttojen välillä
- Asiakas tekee siirtoja harvoin eri virtuaalivaluuttojen välillä
- Asiakkaan siirtämät summat ovat suhteellisen pieniä
- Asiakkaan käyttämät CEX-pörssit ovat KYC-velvollisia ja luotettavia toimijoita.
- Asiakas ei käytä hajautettuja pörssiratkaisuja (DEX, DeFi)
- Asiakas ei käytä erittäin korkean riskin anonymisoituja valuuttoja (Monero, ZCash, Dash)

Korkean riskin asiakkaana:

- Asiakkaalla on syy käyttää virtuaalivaluuttoja sijoittamisen lisäksi kaupankäyntiin ja siirtoihin
- Virtuaalivaluuttojen käyttö sopii asiakkaan toimenkuvaan, ja/tai sitä voidaan käyttää kaupankäyntiin asiakkaan palveluissa
- Asiakas tekee usein siirtoja FIAT-valuutan ja virtuaalivaluuttojen välillä
- Asiakas tekee useasti siirtoja eri virtuaalivaluuttojen välillä
- Asiakkaan siirtämät summat ovat merkittävä osa asiakkaan tuloista/varallisuudesta
- Asiakkaan käyttämät CEX-pörssit ovat KYC-velvollisia ja luotettavia toimijoita.
- Asiakas käyttää hajautettuja Defi-ratkaisuja
- Asiakas ei käytä erittäin korkean riskin anonymisoituja valuuttoja (Monero, ZCash, Dash)

Erittäin korkean riskin asiakas korkean riskin kriteerien lisäksi:

- Asiakas siirtää erittäin suuria summia suhteessa asiakaan tuloihin/varoihin
- Asiakas kertoo käyttävänsä (ja tosiasiassa käyttää) korkean riskin kauppapaikkoja, joilla ei ole KYC-velvollisuutta tai ne toimivat korkean riskin maissa.
- Asiakas kertoo yksinomaan käyttävänsä Defi-ratkaisuja, eikä ilmoitusvelvollisella ole luotettavaa lähdettä mistä, miten ja koska varat on alun perin siirretty Defi-palveluihin.
- Asiakas käyttää erittäin korkean riskin anonymisoituja valuuttoja (Monero, ZCash, Dash)