Emmi Mäkinen

Kryptovarojen käyttö rahanpesussa

Vastaako sääntely tunnistettuihin riskeihin

Laskentatoimen ja rahoituksen akateeminen yksikkö
Talousoikeuden pro gradu -tutkielma
Talousoikeuden maisteriohjelma

Vaasa 2026

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen akateeminen yksikkö
Tekijä: Emmi Mäkinen
Tutkielman nimi: Kryptovarojen käyttö rahanpesussa: Vastaako sääntely tunnistettuihin riskeihin
Tutkinto: Kauppatieteiden maisteri
Opintosuunta: Talousoikeus
Työn ohjaaja: Mika Kärkkäinen
Valmistumisvuosi: 2026 **Sivumäärä:** 78

TIIVISTELMÄ:
Kryptovarat ovat kasvattaneet suosiotaan viime vuosien aikana, mikä on osaltaan lisännyt niihin liittyvää rikollisuutta, kuten rahanpesua. Kryptovaroilla on myös monia perinteisistä fiat-valuutoista poikkeavia erityispiirteitä, jotka tekevät niistä houkuttelevan välineen rahanpesussa. Kryptovarojen pseudonyymisyys tai anonyymisyys, hajautettu rakenne sekä mahdollisuus reaaliaikaisiin ja kansainvälisiin transaktioihin luovat rikollisille uusia mahdollisuuksia varojen alkuperän häivyttämiseen.

Tämän tutkielman tavoitteena on selvittää lainopillisin menetelmin, kuinka kryptovaroja ja niiden ominaisuuksia hyödynnetään rahanpesussa ja miten kryptovarapalvelun tarjoajia säännellään rahanpesun estämisen näkökulmasta. Tutkielmassa arvioidaan myös, onko nykyinen sääntely riittävällä tasolla ottaen huomioon kryptovarojen aiheuttamat riskit.

Vuonna 2018 voimaan tullut viides rahanpesudirektiivi sisällytti ensimmäistä kertaa tietyt kryptovarapalvelun tarjoajat osaksi rahanpesusääntelyä. Tämän jälkeen sääntelyä on täydennetty MiCA-asetuksella sekä maksajan tiedot -asetuksella, jotka asettivat kryptovarapalvelun tarjoajille uusia velvollisuuksia. MiCA-asetus myös laajensi kryptovarapalvelun tarjoajan määritelmää.

Sääntely asettaa kryptovarapalvelun tarjoajille velvollisuuksia, joilla pyritään estämään kryptovarasektorin hyödyntämistä rahanpesussa. Riskiperusteinen arviointi, asiakkaan tunnistamis- ja tuntemisvelvollisuus, liiketoimien seuranta sekä selonotto- ja ilmoitusvelvollisuus ovat tärkeitä toimenpiteitä rahanpesun estämisessä. Näitä velvoitteita täydentävät matkustussääntö sekä velvollisuus hakea kryptovarapalvelun tarjoajan toimilupaa.

Vaikka kryptovarapalvelun tarjoajien sisällyttäminen rahanpesusääntelyn soveltamisalaan on oikea askel riskien hallitsemiseksi, aiheuttavat kryptovarojen erityispiirteet edelleen haasteita sääntelylle. Kryptovarojen hajautetun rakenteen vuoksi osa kryptovarasektorista jää edelleen sääntelyn ulkopuolelle. Tämän lisäksi kryptovarojen pseudonyymisyys tai anonyymisyys vaikeuttaa varojen jäljittämistä sekä kansainväliset ja reaaliaikaiset transaktiot haastavat perinteistä liiketoimien seurantaa.

AVAINSANAT: Kryptovara, rahanpesu, kryptovarapalvelun tarjoaja, asiakkaiden tunteminen, riskiperusteinen arviointi, pseudonyymisyys, hajautettu rakenne

Sisällys

Lyhenteet

AML	Anti-Money Laundering
DeFi	Decentralized Finance
EBA	European Banking Authority
FATF	Financial Action Task Force

Säädösluettelo

Maksajan tiedot -asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2023/1113, annettu 31 päivänä toukokuuta 2023, varainsiirtojen ja tiettyjen kryptovarojen siirtojen mukana toimitettavista tiedoista ja direktiivin (EU) 2015/849 muuttamisesta (uudelleenlaadittu) (ETA:n kannalta merkityksellinen teksti)
MiCA-asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2023/1114, annettu 31 päivänä toukokuuta 2023, kryptovarojen markkinoista sekä asetusten (EU) N:o 1093/2010 ja (EU) N:o 1095/2010 ja direktiivien 2013/36/EU ja (EU) 2019/1937 muuttamisesta (ETA:n kannalta merkityksellinen teksti)
Neljäs rahanpesudirektiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/849, annettu 20 päivänä toukokuuta 2015, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2005/60/EY ja komission direktiivin 2006/70/EY kumoamisesta (ETA:n kannalta merkityksellinen teksti)
Rahanpesuasetus	Euroopan parlamentin ja neuvoston asetus (EU) 2024/1624, annettu 31 päivänä toukokuuta 2024, rahoitusjärjestelmän käytön estämisestä rahanpesuun ja terrorismin rahoitukseen (ETA:n kannalta merkityksellinen teksti)
Rahanpesulaki (RPL)	Laki rahanpesun ja terrorismin rahoittamisen estämisestä (444/2017)
Rikoslaki (RL)	Rikoslaki (39/1889)

Viides rahanpesudirektiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/843, annettu 30 päivänä toukokuuta 2018, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen annetun direktiivin (EU) 2015/849 ja direktiivien 2009/138/EY ja 2014/36/EU muuttamisesta (ETA:n kannalta merkityksellinen teksti)

1 Johdanto

1.1 Tutkimusaiheen tausta ja esittely

Kryptovarat ja kryptovarapalvelut ovat kasvattaneet suosiotaan viime vuosien aikana. Kryptovarat eivät ole kuitenkaan uusi ilmiö, sillä ensimmäinen laajasti tunnettu kryptovara bitcoin julkaistiin jo vuonna 2009. Nykyään kryptovaroja on tuhansia, ja palveluntarjonta niiden ympärillä on lisääntynyt. [1] Kryptovarojen yleistyminen on lisännyt niihin liittyvää rikollisuutta. Tämän lisäksi kryptovaroihin liittyvä rikollisuus on ammattimaistunut. Yhä useammat rikollisorganisaatiot ja -verkostot käyttävät kryptovaroja monimutkaisten toimintojensa toteuttamiseen. [2] Kryptovaroihin liittyy monenlaista rikollisuutta, kuten petos- ja huumausainerikoksia. Kryptovaroja käytetään myös rahanpesun välineenä varojen alkuperän häivyttämiseen.[3]

Kryptovaroilla on ominaisuuksia, jotka tekevät kryptovarasektorista alttiin rahanpesulle. Kryptovarat mahdollistavat henkilöllisyyden piilottamisen, mikä helpottaa rikollisia peittämään toimintansa. Lisäksi kryptovaroilla on kansainvälinen ulottuvuus, ja osa kryptovarasektorista on pysynyt sääntelemättömänä, mikä luo mahdollisuuksia rikollisille. [4] Kryptovaroihin liittyy siten merkittävä riski siitä, että niitä käytetään rahanpesussa. Tämä heikentää rahoitusjärjestelmän luotettavuutta.[5] Jos rahanpesua ei pystytä estämään tehokkaasti, seurauksena voi olla negatiivisia talousvaikutuksia sekä rahoitusmarkkinoiden epävakautta, kuten talouskasvun laantumista, maineriskejä, luottamuksen horjumista ja toiminnan vakauteen liittyviä riskejä. Lisäksi rahanpesulla on yhteiskunnallisia vaikutuksia. [6]

---

[1] HE 31/2024 vp, s. 6 ja 25
[2] Chainalysis, 2025
[3] Verohallinto, 2025
[4] EBA, 2024a
[5] HE 167/2018 vp, s. 45
[6] HE 228/2016 vp, s. 6

Rahanpesun torjuntaa koskeva sääntely on perinteisesti kohdistunut rahoitusalaan, ja voidaankin sanoa, että rahanpesun torjunnasta on tullut rahoitusalan sääntelyn yksi perustavoite [7] . Kryptovarapalvelun tarjoajat eivät kuuluneet rahanpesusääntelyn soveltamisalaan ennen vuotta 2018. EU antoi toukokuussa 2018 viidennen rahanpesudirektiivin, jonka myötä tietyt kryptovarapalvelun tarjoajat tulivat ensimmäistä kertaa rahanpesusääntelyn soveltamisalaan[8]. Sääntelyä on tämän jälkeen laajennettu ja vuonna 2024 tuli sovellettavaksi kaksi uutta EU-asetusta, joiden tavoitteena on yhdenmukaistaa kryptovarasektorin sääntelyä sekä parantaa kryptovarasiirtojen jäljitettävyyttä[9].

Kryptovarojen sääntely on kuitenkin haastavaa johtuen niiden hajautetusta rakenteesta, sillä se mahdollistaa toiminnan keskitetyn tahon tai viranomaisten ulottumattomissa. Lisäksi kryptovarojen kansainvälinen luonne vaikeuttaa sääntelyn tehokkuutta, sillä viranomaiset eivät pysty hallitsemaan, missä yksilöt tai yritykset toimivat.[10] Kryptovarat luovat uusia haasteita, jotka edellyttävät kehittyneempiä ja innovatiivisempia lähestymistapoja rahanpesun torjuntaan. Tästä syystä lainsäädäntöä ja muita sääntelytoimia on arvioitava uudelleen, jotta voidaan selvittää, ovatko ne riittävän tehokkaita torjumaan talousrikollisuutta uudessa toimintaympäristössä. [11]

1.2 Keskeiset tutkimuskysymykset ja aiheen rajaus

Tutkielman tavoitteena on selvittää, kuinka kryptovaroja ja niiden ominaisuuksia hyödynnetään rahanpesussa sekä miten nykyinen sääntely vastaa näihin riskeihin. Tutkielmassa tarkastellaan, miten kryptovarapalvelun tarjoajia säännellään rahanpesun estämisen näkökulmasta ja mitä velvoitteita sääntely asettaa kryptovarapalvelun tarjoajille. Tarkoituksena on myös tutkia, kuinka sääntelyä noudatetaan käytännössä sekä arvioida, onko sääntely tällä hetkellä riittävällä tasolla ottaen huomioon

[7] Wuolijoki, 2022, s. 113
[8] HE 167/2018 vp, s. 5 ja 28
[9] HE 31/2024 vp, s. 6–7
[10] Rahman ja muut, 2025, s. 2
[11] Khan ja muut, 2025, s. 409

kryptovarojen aiheuttamat riskit. Tutkielmassa pyritään vastaamaan syvällisesti seuraaviin kysymyksiin:

1. Kuinka kryptovaroja ja niiden ominaisuuksia hyödynnetään rahanpesussa?
2. Miten kryptovarapalvelun tarjoajia säännellään rahanpesun estämisen näkökulmasta?
3. Vastaako sääntely kryptovarojen aiheuttamiin riskeihin?

Tutkielmassa pyritään antamaan mahdollisimman laaja-alainen katsaus siihen, miten kryptovaroja hyödynnetään rahanpesussa ja kuinka kryptovarapalvelun tarjoajia säännellään sekä EU- että kansallisella tasolla rahanpesun estämiseen liittyen. Tutkimuskysymyksiä tarkastellaan rahanpesun eli varojen alkuperän häivyttämisen näkökulmasta. Terrorismin rahoittaminen jätetään siis tutkielman ulkopuolelle.

Tutkielmassa keskitytään keskeisimpiin kryptovarapalvelun tarjoajiin ja niitä koskevaan rahanpesusääntelyyn. Näin ollen tutkielman ulkopuolelle jätetään muut kryptovarasektorilla toimivat osapuolet, kuten kryptovarojen liikkeeseenlaskijat tai louhijat. Tutkielman kannalta tärkeimpiin kryptovarapalvelun tarjoajiin kuuluvat lompakkopalvelun tarjoajat sekä kryptovarojen kaupankäyntialustat ja vaihtopalvelut. On myös hyvä huomioida, että tutkielman tarkoituksena ei ole mennä kovin syvälle kryptovarojen taustalla vaikuttavaan teknologiaan, vaan pääpaino pysyy sääntelyn arvioinnissa.

Sisällön selkeyttämiseksi tutkielmassa käytetään yhtenevästi käsitettä kryptovara tai kryptovaluutta, vaikka osassa vanhemmista säädöksistä ja lähteistä on ollut vielä käytössä vanha virtuaalivaluutta termi. Uuden sääntelyn myötä on siirrytty käyttämään kryptovaran määritelmää virtuaalivaluutan sijaan, sillä kryptovaran määritelmä kuvaa paremmin ilmiötä ja sen kehitystä[12].

[12] HE 31/2024 vp, s. 26

1.3 Tutkimusmetodi ja keskeinen lähdeaineisto

Tutkielmassa sovelletaan voimassa olevaa sääntelyä. Metodina käytetään lainopillista eli oikeusdogmaattista metodia, joka tarkoittaa oikeudellisia tekstejä tutkivaa tulkintatiedettä. Lainoppi tutkii voimassa olevaa oikeutta sekä lakien ja muiden oikeuslähteiden merkitystä. Se tuottaa tieteellistä tietoa normien todellisuudesta sekä voimassa olevien normien sisällöstä. Oikeusnormilause antaa kielellisessä muodossa informaatiota oikeusnormeista, kun taas oikeusnormi muodostuu oikeusnormilauseesta ja sitä vastaavasta ajatussisällöstä. Lainopin tehtävänä on tutkia näitä oikeusnormeja ja niiden sisältöä hyödyntäen oikeusnormilauseita. [13]

Oikeuslähteet jaetaan kolmeen ryhmään niiden velvoittavuuden perusteella: vahvasti velvoittavat, heikosti velvoittavat sekä sallitut oikeuslähteet. Vahvasti velvoittavia oikeuslähteitä ovat laki ja maan tapa. Heikosti velvoittaviin oikeuslähteisiin kuuluvat lainvalmistelutyöt sekä tuomioistuinratkaisut. Sallittuja oikeuslähteitä ovat oikeustiede, oikeusperiaatteet, moraali ja reaaliset argumentit. [14]

Tutkielman lähteinä käytetään sekä kansallisia lakeja että EU-sääntelyä. EU-oikeuden normit ovat hierarkkisesti ylemmällä tasolla kuin kansallisen lainsäädännön normit eli ristiriitatilanteessa EU-oikeuden normi syrjäyttää kansallisen normin [15]. Tutkielmassa käytettäviä keskeisiä EU-säädöksiä ovat viides rahanpesudirektiivi (2018/843), MiCA-asetus (2023/1114) sekä maksajan tiedot -asetus (2023/1113). EU-asetus on välittömästi jäsenvaltioissa sovellettavaa oikeutta. Asetuksen voimaantulo ei siis edellytä erillistä kansallista toimeenpanoa, kun taas EU-direktiivit edellyttävät jäsenvaltioilta kansallisen toimeenpanon. Direktiiveissä osoitetaan jäsenvaltioille tavoitteet ja toimintaohjeet, jotka niiden tulee toteuttaa parhaaksi katsomilla keinoilla. Käytännössä tämä edellyttää yleensä lainsäädäntötoimenpiteitä, jotta direktiivin päämäärät saadaan toteutettua. [16]

---

[13] Hirvonen, 2011, s. 21–24
[14] Hirvonen, 2011, s. 42–43
[15] Hirvonen 2011, s. 41
[16] Huovila, n.d., s. 29

Keskeinen kansallinen säädös on laki rahanpesun ja terrorismin rahoittamisen estämisestä (444/2017). Tutkielman lähteinä käytetään myös virallislähteitä, kuten hallituksen esityksiä sekä valvonta- ja sääntelyviranomaisten ohjeita. Lähteinä käytetään myös muita viranomaislähteitä, FATF:n antamia suosituksia, kirjallisuutta sekä aiempia tieteellisiä tutkimuksia.

1.4 Tutkielman rakenne

Tutkielma koostuu kuudesta pääluvusta. Ensimmäisessä pääluvussa eli johdantoluvussa johdatellaan lukija tutkimusaiheeseen, sen ajankohtaisuuteen ja merkitykseen. Johdantoluvussa määritellään myös tutkielman keskeiset tutkimuskysymykset ja aiheen rajaukset. Lisäksi johdantoluvussa kuvataan tutkimuksessa käytettyä metodia ja keskeistä lähdeaineistoa.

Toisessa pääluvussa käsitellään kryptovaroja ja niiden käyttöä rahanpesussa. Ensimmäisenä määritellään rahanpesun ja kryptovaran käsitteet. Tämän jälkeen kuvataan, miten kryptovaroja ja niiden ominaisuuksia hyödynnetään rahanpesussa. Kryptovarojen keskeiset ominaisuudet on jaettu kolmeen kategoriaan.

Kolmannessa pääluvussa keskitytään kryptovarapalvelun tarjoajiin ja niitä koskevaan rahanpesusääntelyyn. Ensimmäiseksi määritellään keskeiset kryptovarapalvelun tarjoajat, joihin kuuluvat lompakkopalvelun tarjoajat sekä kryptovarojen kaupankäyntialustat ja vaihtopalvelut. Tämän lisäksi luvussa määritellään hajautetut palvelut. Määritelmien jälkeen tarkastellaan, miten keskitetyt kryptovarapalvelun tarjoajat on sisällytetty rahanpesun estämistä koskevan sääntelyn soveltamisalaan. Luvussa esitellään rahanpesudirektiivit, maksajan tiedot -asetus sekä MiCA-asetus ja kuvataan, miten nämä on täytäntöönpantu kansallisesti.

Neljännessä pääluvussa tarkastellaan mitä velvoitteita sääntely asettaa kryptovarapalvelun tarjoajille. Ensin tarkastellaan rahanpesulain asettamia velvoitteita, kuten riskiperusteista arviointia, asiakkaiden tuntemista, tehostettua

tuntemisvelvollisuutta sekä selonotto- ja ilmoitusvelvollisuutta. Luvussa käsitellään myös sääntelyn asettamia muita velvoitteita, joilla on vaikutuksia rahanpesun torjuntaan. Näitä ovat toimiluvan hakeminen sekä matkustussäännön noudattaminen.

Viidennessä pääluvussa arvioidaan voimassa olevaa sääntelyä sekä tarkastellaan, onko sääntely tällä hetkellä riittävällä tasolla ottaen huomioon kryptovarojen aiheuttamat riskit. Luvussa tarkastellaan, kuinka sääntelyä toteutetaan käytännössä ja mitä haasteita kryptovarojen erityispiirteet tuovat sääntelylle. Luvussa tarkastellaan lyhyesti myös EU:n uutta AML-pakettia ja sen tuomia muutoksia kryptovarasektorille. Kuudennessa ja viimeisessä luvussa kootaan yhteen tutkielman sisältö sekä esitetään keskeiset johtopäätökset ja vastataan tutkimuskysymyksiin.

2 Kryptovarat ja rahanpesu

2.1 Rahanpesun käsite

Rahanpesulla pyritään peittelemään laittomasta alkuperästä peräisin olevat varat kierrättämällä ne laillisen maksujärjestelmän läpi. Tarkoituksena on peittää varojen tosiasiallinen luonne, alkuperä tai varojen omistaja. [17] Kun rikollisella toiminnalla hankitut varat saadaan lailliseen maksujärjestelmään, on rikollinen raha vaikeaa erottaa puhtaasta rahasta, ja näin ollen rikolliset voivat helposti käyttää laittomia varojaan[18].

Rikoslain (39/1889) 32 luvun 6 §:ssä määritellään rahanpesun tunnusmerkistö. Mikäli henkilö ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää, välittää tai pitää hallussa rikoksella hankittua omaisuutta tarkoituksenaan hankkia itselle tai toiselle hyötyä, peittääkseen omaisuuden laittoman alkuperän tai avustaakseen rikoksentekijää välttämään rikoksen oikeudelliset seuraamukset, on hänet tuomittava rahanpesusta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Rikoslain 32 luvun 7 §:n mukaan törkeässä rahanpesussa rikoksen kautta saatu omaisuus on ollut erittäin arvokas tai rikos tehdään erityisen suunnitelmallisesti.

Rahanpesua edeltää aina esirikos, josta saatuun omaisuuteen tai hyötyyn rahanpesutoimet kohdistetaan. Esirikos on siis rahanpesurikokseen sisältyvä välttämättömyys. Rahanpesussa likainen raha voi olla peräisin mistä tahansa taloudellista hyötyä tuottavasta rikoksesta, kuten huumausainerikoksesta, veropetoksesta tai näpistyksestä. [19] Petokset, huumausainerikokset sekä maksuvälinepetokset ovat olleet yleisimpiä esirikoksia törkeää rahanpesua koskevissa tuomioissa aikavälillä 1.6.2022-30.4.2024[20].

[17] Wuolijoki, 2022, s. 113
[18] See, 2024, s. 416
[19] Hyttinen, 2021, s. 227 ja 29
[20] Rahanpesun selvittelykeskus, 2025, s. 11

Rahanpesu sisältää kolme vaihetta. Näitä ovat sijoitusvaihe, jossa likainen raha sijoitetaan lailliseen talousjärjestelmään, harhautusvaihe eli likaisen rahan alkuperän peittäminen tai häivyttäminen sekä integrointivaihe eli puhdistetun rahan integroiminen osaksi laillista taloutta. Rahanpesu on yleensä suunnitelmallista ja kansainvälistä. Sijoitusvaiheessa saatetaan käyttää hyväksi valtioita, joissa on tiukka pankkisalaisuus. Lisäksi järjestelmällisimmissä rahanpesutoimissa rikoshyötyä pyritään siirtämään maasta toiseen. Esimerkiksi jos henkilö siirtää Yhdysvalloista petoksella saadut varat Ruotsiin, jossa ostaa pörssiosakkeita ja antaa nämä asuntolainan vakuudeksi Suomessa, syyllistyy hän rahanpesuun.[21]

2.2 Kryptovaran käsite

Kryptovara määritellään MiCA-asetuksen (2023/1114) 3 artiklan 1 kohdan 5 alakohdassa arvon tai oikeuden digitaaliseksi edustajaksi, joka voidaan siirtää ja tallentaa sähköisesti käyttäen hajautetun tilikirjan teknologiaa tai vastaavaa teknologiaa. ”Krypto” viittaa kryptografiaan eli salaustekniikkaan. Lohkoketju on yhdentyyppinen hajautetun tilikirjan teknologia. Sitä ei hallitse yksi keskitetty taho, vaan useat toimijat yhdessä.[22]

Kryptovarat muodostavat rahan kaltaisen järjestelmän, joka toimii itsenäisesti ja riippumattomasti eikä ole välttämättä minkään valtion tai pankin ylläpitämä [23] . Kryptovaroja käytetään yleisimmin sijoittamiseen, mutta niitä saatetaan käyttää myös maksamiseen. Maksamisen mahdollisuus on kuitenkin käytännössä harvinaista esimerkiksi vähittäistavarakaupoissa. [24] Kryptovarat perustuvat yksityisiin ja julkisiin avaimiin, joiden avulla arvoa siirretään henkilöltä toiselle[25].

[21] Hyttinen, 2021, s. 24–27 ja 4
[22] Finanssivalvonta, 2025a
[23] Sammalisto & Asunmaa, 2021, s. 187
[24] Finanssivalvonta, 2025a
[25] HE 167/2018 vp, s. 45

Kryptovarat saivat alkunsa vuonna 2008, kun tuntematon henkilö nimeltä Satoshi Nakamoto keksi ensimmäisen kryptovaluutan bitcoinin [26]. Nykyään bitcoin on yksi tunnetuimmista kryptovaluutoista. Se on hajautettu, fiat-valuuttaan vaihdettava kryptovaluutta, jonka arvo muodostuu kysynnän ja tarjonnan kautta. Bitcoineja voidaan siirtää sähköisesti käyttäjien välillä. Maksuliikennetiedot on yksilöity bitcoin-osoitteisiin, ja ne ovat julkisesti saatavilla käyttäjien rekisterissä. Yksilöllistä tunnistetta ei voida kuitenkaan yhdistää yksittäiseen henkilöön. Käyttäjät voivat pitää bitcoin-tilejä joko vaihtopalvelun tarjoajien toimesta tai pilvipalveluna tarjottavassa lompakossa. [27]

MiCA-asetuksen 18 johdantokappaleessa kryptovarat jaetaan kolmeen tyyppiin sen mukaan miten niiden arvo pyritään vakauttamaan. Näitä ovat sähkörahatokenit, omaisuusreferenssitokenit sekä muut kryptovarat, kuten hyödyketokenit. MiCA-asetuksen 3 artiklan 1 kohdan 7 alakohdan mukaan sähkörahatokenilla tarkoitetaan kryptovaraa, jonka arvo pyritään vakauttamaan yhden virallisen valuutan avulla. Omaisuusreferenssitokenit määritellään MiCA-asetuksen 3 artiklan 1 kohdan 6 alakohdassa kryptovaraksi, jonka arvo pyritään vakauttamaan minkä tahansa referenssin, kuten usean valuutan yhdistelmän, avulla. Hyödyketokenit määritellään MiCA-asetuksen 3 artiklan 1 kohdan 9 alakohdassa kryptovaratyypiksi, jonka tarkoituksena on ainoastaan antaa pääsy sen liikkeeseenlaskijan toimittamaan tavaraan tai palveluun.

2.2.1 Kryptovarojen luominen

Kryptovaroja voidaan luoda joko louhimalla tai liikkeeseenlaskun eli ennakkomyynnin kautta. Louhinnassa kryptovaluuttaverkostoon liittyneet tietokoneet ratkaisevat matemaattisia kaavoja. Kun ratkaisu löytyy, syntyy lohko, jonne tallennetaan tiedot kryptovaluutan tapahtumista ja louhija palkitaan kryptovaluutalla.[28] Louhinnan kautta kryptovaroja syntyy siis ilman nimettyä liikkeeseenlaskijaa eli niiden liikkeeseenlasku on hajautettua. Bitcoin muodostuu louhinnan kautta, ja sen louhinta on mahdollista kenelle

[26] See, 2024, s. 417
[27] HE 167/2018 vp, s. 45
[28] Sammalisto & Asunmaa, 2021, s. 188

tahansa eikä sen arvoa taata mitenkään.[29] Kryptovaluuttajärjestelmän turvallisuus, eheys ja saldo perustuvat louhijoiden keskinäiseen luottamussuhteeseen[30].

Kryptovaroja voidaan luoda myös liikkeeseenlaskun eli niin sanotun kolikkoannin kautta[31]. Tällöin kryptovaralla on nimetty liikkeeseenlaskija eli myyjä tai henkilö, joka listaa kryptovaran kaupankäyntialustalle eli kryptopörssiin[32]. MiCA-asetuksen 3 artiklan 1 kohdan 10 alakohdan mukaan kryptovarojen liikkeeseenlaskija on luonnollinen henkilö tai yritys, joka laskee liikkeeseen kryptovaroja. Liikkeeseenlaskun kautta lohkoketjua hyödyntävä yritys tai muu toimija tarjoaa omaa kryptovaluuttaansa vastineeksi sijoitusta vastaan. Sijoituksia voi tehdä joko fiat-rahalla tai kryptovaluutalla, kuten bitcoinilla. [33]

2.2.2 Lohkoketju

Kryptovarojen toiminnan mahdollistaa lohkoketju, eli hajautetun tilikirjan teknologia. Se tarkoittaa yksinkertaisimmillaan luotettavaa digitaalista tilikirjaa, johon merkitään tapahtumia aikajärjestyksessä. Lohkoketjun avulla transaktiota tallennetaan niin, että kaikki lohkoketjun käyttäjät ovat samaa mieltä siitä, mitä on tapahtunut ja missä järjestyksessä. Lohkoketjun erityispiirre on se, että sitä ei lähtökohtaisesti hallinnoi vain yksi keskitetty instituutio, kuten pankki. Kuka tahansa tilikirjaa ylläpitävä toimija voi tehdä uusia merkintöjä tilikirjaan, mutta hyväksyntään vaaditaan aina kaikkien toimijoiden yhteisymmärrys, joka käytännössä luodaan matemaattisin menetelmin. Näin ollen luottamus saadaan aikaan käyttäen matemaattisia sääntöjä sekä salausjärjestelmiä sen sijaan, että luottamuksen takaa jokin ihminen tai instituutio.[34]

Bitcoinin taustalla toimiva lohkoketju on ensimmäinen ja alkuperäinen lohkoketjujärjestelmä. Teoriassa sillä tarkoitetaan yhtä isoa Excel-taulukkoa tai tilikirjaa,

[29] Finanssivalvonta, 2025a
[30] HE 167/2018 vp, s. 45
[31] Johansson ja muut, 2019, s. 110
[32] Finanssivalvonta, 2025a
[33] Johansson ja muut, 2019, s. 112
[34] Johansson ja muut, 2019, s. 27–30

joka koostuu käyttäjien välisistä transaktioista eli arvon siirroista. Mikäli henkilö A haluaa lähettää bitcoinia käyttäjälle B, tulee bitcoin-lohkoketjuun merkintä siten, että henkilön A saldo tilillä vähentyy ja henkilön B saldo tilillä lisääntyy vastaavan määrän. Transaktioita ei kuitenkaan lisätä tilikirjaan yksitellen, vaan järjestelmä kasaa ne yhteen ja muodostaa lohkon. Yhden lohkon sisälle mahtuu vain tietyn verran tapahtumia ja kun lohko on täynnä, sen sisältö varmistetaan ja linkitetään edeltävään lohkoon käyttäen kryptograafista salausmenetelmää. Näin syntyy lohkoketju.[35] Mikäli yhtä lohkoketjun lenkkiä yritetään muokata jälkikäteen, tuhoutuu kaikki sen jälkeen tulevat lenkit eikä sitä voida rakentaa taaksepäin. Näin ollen lohkoketju muodostaa pysyvän ja muuttumattoman arkiston datalle, kuten tapahtumille kryptovaluutoissa. [36]

Kryptovarojen siirtäminen ja tallentaminen perustuu kryptograafiseen salaukseen. Tämä toteutetaan käyttämällä julkisia ja yksityisiä avaimia. [37] Julkista avainta käytetään osoitteena, johon kryptovara voidaan kohdistaa. Se jaetaan muille lohkoketjun käyttäjille kryptovarojen vastaanottamista varten. Julkista avainta voikin siis verrata pankkitilin tilinumeroon. Mikäli kryptovaran haltija haluaa siirtää kryptovarojaan toiselle henkilölle, tulee hänen allekirjoittaa kyseinen lohkoketjutransaktio yksityisellä ja salassa pidettävällä avaimella. [38] Yksityistä avainta voisi siis verrata verkkopankkitunnuksiin, joiden paljastaminen muille voisi vaarantaa tilillä olevat varat[39].

[35] Johansson ja muut, 2019, s. 28
[36] Sammalisto & Asunmaa, 2021, s. 188
[37] Finanssivalvonta, 2025b
[38] Haffke ja muut, 2019, s. 128
[39] Silva Ramalho & Igreja Matos, 2021, s. 488

2.3 Kryptovarojen käyttö rahanpesussa

Kryptovarojen käyttö rahanpesussa vastaa pitkälti pankki- ja maksupalvelusektorilla tunnistettuja tekotapoja. Varojen rikollinen alkuperä pyritään peittämään siirtämällä kryptovaroja eri lompakoiden ja palveluiden välillä sekä tallettamalla ja nostamalla varoja fiat-valuutaksi. [40] Kryptovarasektorilla on havaittu, että erityisesti huumausainerikokset ovat kohtalaisen yleisiä esirikoksia rahanpesussa [41].

Kryptovaroihin liittyvä rahanpesu voidaan luokitella myös perinteisen kolmivaihemallin mukaisesti. Sijoitusvaiheessa likainen fiat-raha pyritään vaihtamaan kryptovaroiksi esimerkiksi tallettamalla käteinen raha kryptovara-automaattiin, joka muuntaa talletetun rahan kryptovaluutaksi ja lähettää sen tallettajan kryptovaralompakkoon. Fiat-rahaa pyritään vaihtamaan kryptovaroiksi myös eri vaihtopalveluita käyttämällä. Rikolliset käyttävät usein rahanpesusääntelyn ulkopuolella toimivia vaihtopalveluita, jotka mahdollistavat vaihdon anonyymisti.[42]

Harhautusvaiheessa varojen rikollista alkuperää pyritään peittämään tekemällä monimutkaisia transaktioita sekä käyttämällä anonymiteettia edistäviä palveluita. Viimeisessä vaiheessa eli integrointivaiheessa laittomat kryptovarat pyritään saamaan lailliseen talouteen vaihtamalla kryptovara takaisin fiat-valuuttaan tai hankkimalla muita omaisuuseriä. Tässä vaiheessa käytetään yleensä vaihtopalveluntarjoajia, joiden kautta kryptovarat vaihdetaan fiat-rahaan. [43] Kryptovarojen vaihto fiat-valuuttaan voidaan toteuttaa eri maassa kuin mistä laittomat varat tai kryptovaluutat ovat alun perin peräisin [44].

[40] Finanssivalvonta, 2024, s. 8
[41] Isoaho & Kaski, 2021, s. 38
[42] Wronka, 2022, s. 85–87
[43] Wronka, 2022, s. 85–87
[44] Haffke ja muut, 2019, s. 130

2.3.1 Kryptovarasektorin rahanpesuriskit

Kryptovarasektoriin kohdistuvaa rahanpesuriskiä on arvioitu kansallisissa ja ylikansallisessa riskiarvioissa. Vuoden 2021 kansallisessa riskiarviossa kryptovarasektoriin kohdistuvaa rahanpesuriskiä on pidetty erittäin merkittävänä. Riskinä ja uhkana on nähty erityisesti järjestäytyneet rikollisryhmät, jotka hyödyntävät kryptovaroja rahanpesussa. Kryptovarojen anonyymi tai pseudonyymi luonne on myös nostanut rahanpesun riskiä. [45] Euroopan komission laatimassa ylikansallisessa riskiarviossa kryptovaroihin liittyvää rahanpesuriskiä on pidetty myös erittäin merkittävänä. Kryptovarojen luontaista riskialttiutta on pidetty korkeana johtuen niiden rajat ylittävistä ja anonyymeistä ominaisuuksista. [46]

Vuoden 2023 kansallisen riskiarvion osittaispäivityksessä kryptovarasektoriin kohdistuvaa rahanpesun kokonaisriskitasoa on pidetty merkittävänä. Riskiin on katsottu vaikuttavan merkittävästi kryptovarojen taustalla oleva teknologia.[47] Finanssivalvonnan vuoden 2024 sektorikohtaisessa riskiarviossa kryptovarasektoriin kohdistuvaa rahanpesun kokonaisriskiä on pidetty myös merkittävänä. Erityisesti kryptovarasiirtojen reaaliaikaisuutta ja globaalia liikkuvuutta on pidetty riskiä kohottavana tekijänä.[48]

Riskiarviot osoittavat, että kryptovarasektoriin kohdistuvaa rahanpesuriskiä pidetään vähintään merkittävänä. Kryptovaroilla on monia perinteisistä valuutoista poikkeavia ominaisuuksia, joita pystytään käyttämään hyväksi rahanpesussa. Erityisesti kryptovarojen pseudonyymi tai anonyymi luonne, transaktioiden reaaliaikaisuus ja kansainvälisyys sekä kryptovarojen hajautettu rakenne tekevät niistä riskillisiä rahanpesulle.

[45] Isoaho & Kaski, 2021, s. 63
[46] Euroopan komissio, 2022, s. 101
[47] Valtiovarainministeriö, 2024, s. 80
[48] Finanssivalvonta, 2024, s. 3

2.3.2 Pseudonymiteetti ja anonymiteetti

Kryptovarat voivat olla joko pseudonyymejä tai anonyymejä[49]. Kryptovaran, kuten bitcoinin, pseudonyymisyys tarkoittaa, että liiketoimea tekevän henkilön tiedot eivät ole suoraan nähtävissä lohkoketjussa. Todellisuudessa kryptovaran taustalla oleva lohkoketju on julkinen, mikä mahdollistaa kolmansien osapuolien pääsyn tietoihin transaktiohistoriasta, siirrettyjen kryptovarojen arvosta sekä lähettäjä- ja vastaanottajaosoitteista. Julkisesti rekisteröidyt tiedot tekevät näin ollen teknisesti mahdolliseksi liiketoimen taustalla olevan henkilön tunnistamisen. [50]

Teoriassa käyttäjät toimivat siis julkisen avaimen muodostaman pseudonyymin alla, mutta todellisuudessa tapahtumat ovat julkisesti nähtävissä ja transaktioiden analysoiminen lohkoketjuissa on mahdollista erilaisten työkalujen avulla[51]. On kuitenkin hyvä huomioida, että lohkoketjussa saatavilla olevat tiedot mahdollistavat transaktioiden jäljittämiseen tiettyyn lompakko-osoitteeseen, mutta lompakko-osoitetta ei välttämättä voi yhdistää suoraan yksittäisen henkilön nimeen [52]. Tällainen etäisyys liiketoimien ja niitä tekevien henkilöiden henkilöllisyyden välillä tekee kryptovaroista houkuttelevan vaihtoehdon rahanpesuun[53].

Koska kryptovarojen transaktiohistoria on yleensä julkisesti saatavilla sekä kryptovarojen lähtö- ja kohdeosoitteiden sekä saldojen tunnistaminen on mahdollista, käyttävät rikolliset erilaisia sekoittajapalveluita transaktioiden ja osoitteiden piilottamiseen [54]. Sekoittajapalvelut ovat riskillisiä palveluita, sillä niiden avulla yritetään katkaista kryptovarojen jäljitettävyys [55]. Ne ottavat vastaan eri lähteistä peräisin olevia kryptovaluuttoja ja lähettävät ne yhteen osoitteeseen, jossa ne sekoitetaan. Tämän jälkeen sekoitetut varat jaetaan useisiin osiin ja lähetetään eri osoitteisiin. Tämän

[49] Wronka, 2022, s. 84
[50] Silva Ramalho & Igreja Matos, 2021, s. 496
[51] Wronka, 2022, s. 84
[52] FATF, 2019, s. 27
[53] Silva Ramalho & Igreja Matos, 2021, s. 496
[54] Silva Ramalho & Igreja Matos, 2021, s. 503
[55] Isoaho & Kaski, 2021, s. 64

seurauksena kryptovarojen yhdistäminen niiden todelliseen alkuperään on lähes mahdotonta.[56]

Useimmat kryptovarat ovat pseudonyymejä, mutta on olemassa myös lähes täysin anonyymejä kryptovaluuttoja. Tällaisia kryptovaroja hyödynnetään myös varojen alkuperän häivyttämisessä. [57] Privaattikryptovaluutat (engl. privacy coins) tarjoavat tavallisia kryptovaluuttoja korkeamman anonymiteetin lohkoketjutransaktioissa. Korkeampi anonymiteetti saavutetaan esimerkiksi salaamalla käyttäjäosoitteisiin liittyviä tietoja kolmansilta osapuolilta. Tämä tekee privaattikryptovaluutoista vaikeammin jäljitettävän verrattuna tavallisiin kryptovaluuttoihin, joiden käyttäjäosoitteet ovat kaikkien nähtävillä. Tämän lisäksi jotkin kryptovaluutat, kuten Monero, on suunniteltu alusta alkaen yksityisiksi. [58]

2.3.3 Kansainväliset ja reaaliaikaiset transaktiot

Kryptovaroilla voidaan toteuttaa siirtoja reaaliaikaisesti ja minne tahansa maailmaa, mikä tekee niistä houkuttelevan vaihtoehdon rahanpesuun. Erityisesti laajasti käytössä olevat automaattiset kaupankäyntibotit tehostavat kryptovarasiirtojen reaaliaikaisuutta. [59] Kun siirtoja voidaan tehdä reaaliaikaisesti, varat voivat kadota nopeasti viranomaisten ulottumattomiin. Kryptovaroilla toteutettavia siirtoja ei ole mahdollista myöskään peruuttaa, jolloin varojen palautuspyyntöjä ei voida soveltaa kryptovarasiirtoihin.[60]

Kryptovaroja voidaan siirtää useiden lainkäyttöalueiden kautta sekä paljon suuremmissa mittakaavoissa ja nopeammin kuin tavallisia sähköisiä rahanlähetyksiä [61] . Tämä mahdollistaa kryptovarojen hajauttamisen helposti ja nopeasti eri vaihtopalveluihin. Koska vaihtopalveluita on tarjolla kansainvälisesti erittäin paljon, onnistuu varojen

[56] United nations, n.d.
[57] Valtiovarainministeriö, 2024, s. 81
[58] United nations, n.d.
[59] Finanssivalvonta, 2024, s. 8
[60] Isoaho & Kaski, 2021, s. 64
[61] Euroopan parlamentti, 2022, s. 13

alkuperän häivyttäminen tehokkaasti käyttämällä useaa eri vaihtopalvelua. Globaali toiminta vaikeuttaa myös rahanpesun valvontaa. Epäilyttäviä liiketoimia koskevat ilmoitukset menevät vain toisen maan rahanpesun selvittelykeskukselle, mikä aiheuttaa puutteita informaatiossa. [62] Valvontavastuun määrittäminen ja valvonnan järjestäminen on myös usein vaikeaa[63].

2.3.4 Hajautettu rakenne

Kryptovaroille voidaan joissakin tilanteissa yksilöidä liikkeeseenlaskija, jolloin kyseessä on keskitetty järjestelmä ja sille voidaan asettaa myös velvollisuuksia. Hajautetussa järjestelmässä, kuten bitcoinin taustalla olevassa järjestelmässä, tällaista liikkeeseenlaskijaa ei pystytä yksilöimään, ja näin ollen sille ei pystytä asettamaan velvollisuuksia.[64]

Yksi kryptovaluuttojen keskeisistä ominaisuuksista on se, että ne perustuvat lohkoketjuteknologiaan, joka puolestaan perustuu hajautettuun tietokoneverkkoon[65]. Kryptovarojen taustalla toimivaa lohkoketjua kutsutaan myös vertaisverkoksi. Vertaisverkossa on mahdollista toimia ilman keskitettyä auktoriteettia, kuten pankkia, joka voisi havaita ja ilmoittaa epäilyttävistä liiketoimista. Hajautetun rakenteen ansiosta kryptovaroilla tehtävät liiketoimet eivät ole riippuvaisia kolmansista osapuolista tai välittäjistä, mikä tekee kryptovaroista houkuttelevan vaihtoehdon rahanpesijöille. [66] Lohkoketjun avulla niin sanottua sähköistä käteistä voidaan lähettää käyttäjältä toiselle ilman rahoituslaitoksia[67].

Vertaisverkossa tapahtuvat siirrot voivat olla houkutteleva vaihtoehto rikollisille niiden anonymiteetin, siirrettävyyden, rajoitusten puuttumisen sekä nopeuden vuoksi [68] .

---

[62] Valtiovarainministeriö, 2024, s. 81–82
[63] Finanssivalvonta, 2024, s. 8
[64] HE 167/2018 vp, s. 48
[65] Khan ja muut, 2025, s. 410
[66] Wronka, 2022, s. 81 ja s. 84–85
[67] Renda & Caneppele, 2024, s. 365
[68] FATF, 2021, s. 86

Käytännössä siirto tapahtuu siten, että kryptovarojen lähettäjä syöttää vastaanottajan lompakon osoitteen ja lähetettävän summan omaan lompakkoonsa, allekirjoittaa tapahtuman, jonka jälkeen varat lähetetään.[69] Kryptovarojen vastaanottajan tulee siis toimittaa lähettäjälle oma bitcoin-osoitteensa antamalla joko aakkosnumeerinen osoite tai kryptovaralompakon luoma QR-koodi, jonka jälkeen kryptovarojen lähettäjä syöttää vastaanottajan bitcoin-osoitteen tai skannaa QR-koodin ja todentaa siirron yksityisellä avaimellaan.[70]

[69] Investopedia, 2025
[70] Silva Ramalho & Igreja Matos, 2021, s. 489

3 Rahanpesun torjunnan sääntely kryptovarasektorilla

3.1 Keskeiset kryptovarapalvelun tarjoajat

Jos teknologia on luonteeltaan hajautettua, on lainsäätäjien loogista säännellä välittäjiä [71] . Kryptovarojen kohdalla tämä tarkoittaa kryptovarapalvelun tarjoajia. Kryptovarapalvelun tarjoajat toimivat virtuaalimaailman ja todellisen maailman rajapinnassa, joten niitä kutsutaan myös välittäjiksi [72]. Kryptovarapalvelun tarjoajalla tarkoitetaan MiCA-asetuksen 3 artiklan 1 kohdan 15 alakohdan mukaan yritystä, joka tarjoaa ammatti- tai liiketoimintana kryptovarapalveluita. MiCA-asetuksen 3 artiklan 1 kohdan 16 alakohdan mukaan kryptovarapalvelulla tarkoitetaan:

a) kryptovarojen säilytyksen tarjoaminen ja hallinnointi asiakkaiden puolesta
b) kryptovarojen kaupankäyntialustan ylläpito
c) kryptovarojen vaihto varoihin
d) kryptovarojen vaihto muihin kryptovaroihin
e) kryptovaroja koskevien toimeksiantojen toteuttaminen asiakkaiden puolesta;
f) kryptovarojen kohdennettu tarjoaminen
g) kryptovaroja koskevien toimeksiantojen vastaanottaminen ja välittäminen asiakkaiden puolesta
h) kryptovaroja koskevan neuvonnan tarjoaminen
i) kryptovaroja koskevan salkunhoidon tarjoaminen
j) kryptovarojen siirtopalvelujen tarjoaminen asiakkaiden puolesta

Tärkeimpiin kryptovarapalvelun tarjoajiin kuuluvat muun muassa kryptovarojen säilytystä ja hallinnointia tarjoavat yritykset eli lompakkopalvelun tarjoajat sekä kryptovarojen kaupankäyntialustan ylläpitoa tarjoavat yritykset eli kryptopörssit [73] .

[71] Haffke ja muut, 2019, s. 127
[72] Wronka, 2022, s. 82
[73] Salo-Lahti, 2023, s. 609

Useat markkinoilla toimivat yritykset tarjoavat molempia palveluita. Kaupankäyntialustat tarjoavat usein myös kryptovarojen säilytystä ja hallinnointia, mutta on myös olemassa ainoastaan lompakkopalveluita tarjoavia yrityksiä. Tämän lisäksi markkinoilla toimii kryptovarojen vaihtopalvelun tarjoajia.[74]

3.1.1 Lompakkopalvelut

Keskeisiä kryptovarapalvelun tarjoajia ovat lompakkopalveluiden tarjoajat. Jotta kryptovaroilla voidaan tehdä transaktioita tai käydä kauppaa kaupankäyntialustoilla, tarvitaan kryptovaralompakoita, joissa kryptovaroja säilytetään. Nimestään huolimatta lompakot eivät sisällä kryptovaroja, vaan joukon yksityisiä ja julkisia avaimia, jotka mahdollistavat kryptovarojen siirtämisen. Kryptovarat tallennetaan lohkoketjuun lompakko-osoitteen muodossa.[75] MiCA-asetuksen 3 artiklan 1 kohdan 17 alakohdan mukaan kryptovarojen säilytyksellä ja hallinnoinnilla asiakkaiden puolesta tarkoitetaan kryptovarojen tai tällaisiin kryptovaroihin pääsyä koskevan keinon, soveltuvin osin yksityisten salausavainten muodossa, säilyttämistä tai valvomista asiakkaiden puolesta.

Lompakot voidaan karkeasti jakaa kahteen luokkaan sen perusteella, miten lompakon hallintaan tarvittavia yksityisiä avaimia säilytetään. Yksityiset avaimet voi luovuttaa ainakin osittain palveluntarjoajalle, jolloin henkilöstä tulee asiakas ja palveluntarjoajalla on vähintään rajoitettu vastuu asiakkaan kryptovarojen ja yksityisten avainten säilyttämisestä.[76] Tällaiset säilytyslompakkopalvelun tarjoajat (engl. custodian wallet provider) ylläpitävät alustoja, esimerkiksi mobiilisovelluksia tai verkkosivuja, joihin käyttäjät voivat luoda tilejä yksityisten avainten säilyttämiseksi. Kryptovaratransaktion toteuttamiseksi käyttäjä tarvitsee ainoastaan kirjautumistiedot lompakkopalveluntarjoajan palveluun. Näin ollen käyttäjän ei tarvitse muistaa ulkoa pitkää ja usein monimutkaista yksityistä avaintaan.[77]

---

[74] Wronka, 2022, s. 83
[75] Chen ja muut, 2023, s. 20
[76] Finanssivalvonta, 2025a
[77] Haffke ja muut, 2019, s. 129

Vaihtoehtoisesti yksityisiä avaimia voi säilyttää omassa hallinnassa ilman muiden pääsyä avaimiin[78]. Tällaiset itsehallinnoitujen lompakoiden tarjoajat (engl. non-custodian wallet provider) eivät säilytä käyttäjien yksityisiä avaimia, vaan tarjoavat ainoastaan välineitä käyttäjille, joiden avulla he voivat säilyttää yksityiset avaimensa itse [79]. Tällöin vastuu kryptovarojen hallinnasta ja asianmukaisesta säilyttämisestä on täysin käyttäjällä itsellään. Jos käyttäjä kadottaa yksityiset avaimensa, ei niiden palauttaminen välttämättä ole koskaan mahdollista. Tällöin käyttäjä ei pääse enää käsiksi lompakossa säilytettäviin kryptovaroihin. [80]

3.1.2 Kaupankäyntialustat ja vaihtopalvelut

Keskeisimpiin kryptovarapalvelun tarjoajiin kuuluvat myös kaupankäyntialustat ja vaihtopalvelut. MiCA-asetuksen 3 artiklan 1 kohdan 18 alakohdan mukaan kryptovarojen kaupankäyntialustan ylläpidolla tarkoitetaan sellaisen monikeskisen järjestelmän hallinnointia, jossa saatetaan yhteen kryptovaroja koskevia osto- ja myynti-intressejä siten, että tuloksena on sopimus, joko vaihtamalla kryptovaroja varoihin tai muihin kryptovaroihin. Kaupankäyntialustat ovat digitaalisia markkinapaikkoja, joissa voi ostaa ja myydä kryptovaroja sekä vaihtaa kryptovaluuttoja toisiin kryptovaluuttoihin tai fiat-valuuttoihin[81].

Kryptovarojen kaupankäyntialustat voivat olla keskitettyjä tai hajautettuja. Suurin osa kryptopörsseistä toimii kuitenkin keskitetysti [82] . Keskistetyt kaupankäyntialustat, esimerkiksi Binance, Coinbase ja Kraken, ovat jonkin keskitetyn tahon omistamia ja ylläpitämiä. Ne välittävät käyttäjille pääsyn lohkoketjuun, jossa kryptovarat sijaitsevat. Ne myös osallistuvat kryptovaluuttoja koskevien osto- ja myyntisopimusten

[78] Finanssivalvonta, 2025a
[79] Haffke ja muut, 2019, s. 129
[80] Finanssivalvonta, 2025a
[81] Chen ja muut, 2023 s. 6
[82] Finanssivalvonta, 2025a

yhteensovittamiseen sekä kauppojen toteuttamiseen. [83] Keskitetyt kaupankäyntialustat hallinnoivat myös käyttäjien yksityisiä avaimia eikä käyttäjillä ole pääsyä avaimiinsa[84].

MiCA-asetuksen 3 artiklan 1 kohdan 19 ja 20 alakohtien mukaan kryptovarojen vaihdolla tarkoitetaan kryptovaroja koskevien osto- tai myyntisopimusten tekemistä asiakkaiden kanssa varoja tai muita kryptovaroja vastaan käyttämällä omaa pääomaa. Kryptovarojen vaihtopalvelun tarjoajat mahdollistavat kryptovaluuttojen vaihdon joko fiat-valuutoilla tai toisilla kryptovaluutoilla. Osa vaihtopalveluista mahdollistaa pelkästään fiat- ja kryptovaluuttojen välisen vaihdon, kun taas osa tarjoaa ainoastaan kryptovaluuttojen välisiä vaihtoja. Lisäksi markkinoilla on molempia vaihtoja tarjoavia palveluita.[85]

3.2 Hajautetut palvelut

DeFi eli hajautettu rahoitus on yleisnimitys erilaisille palveluille, jotka pyrkivät rakentamaan perinteisestä pankkimaailmasta riippumattoman kokonaan uuden finanssisektorin[86]. Hajautetuilla palveluilla tarkoitetaan lohkoketjun päälle rakennettuja sovelluksia, joiden avulla pystytään käyttämään finanssimaailman palveluita ilman kolmansia osapuolia, kuten pankkeja [87] . Perinteiset finanssipalvelut toimivat keskitetyissä järjestelmissä, mutta hajautetut palvelut tuovat nämä tutut palvelut uusiin hajautettuihin järjestelmiin [88] . Keskeistä on, että niiden toimintaa hallinnoidaan hajautetuilla protokollilla ja toteutetaan automaattisesti täytäntöönpantavilla sopimuksilla. Lisäksi niiden toimintaan ei liity välittäjän tai säilyttäjän asemassa olevaa henkilöä, joka toimisi muiden puolesta.[89]

[83] Chen ja muut, 2023, s. 9
[84] Dupuis & Gleason, 2021, s. 69
[85] Haffke ja muut, 2019, s. 128
[86] Soon, 2021
[87] Isto, 2023
[88] Soon, 2021
[89] Valtiovarainministeriö, 2024, s. 78

Hajautetut kryptopörssit ovat osa hajautetun rahoituksen ilmiötä [90] . Hajautetut kryptopörssit, kuten Uniswap, ovat kaupankäyntialustoja, joissa ei ole keskitettyä toimijaa, joka ylläpitäisi alustaa tai osallistuisi kryptotransaktioihin. Kryptovarojen hallinnoiminen sekä kaupankäynti toteutuvat käyttäjien toimesta suoraan lohkoketjussa. [91] Hajautetut pörssit eivät siis itse osta tai myy kryptovaluuttoja, vaan tarjoavat ainoastaan alustan käyttäjille kryptovaluuttojen kaupankäyntiin [92] . Käyttäjät myös hallitsevat yksityisiä avaimia ja siten kryptovaroja suoraan, eikä palvelulla ole pääsyä tai määräysvaltaa varoihin[93].

Hajautettujen kryptopörssien tehtävänä on ainoastaan yhdistää kryptovarojen ostajat ja myyjät toisiinsa. Käytännössä tämä toteutuu älysopimuksen avulla, joka tarkoittaa tietokoneohjelmaa tai transaktioprotokollaa, joka toteuttaa sopimuksen ehdot automaattisesti. [94] Osapuolet toteuttavat kaupan itse vertaisverkossa eli esimerkiksi omien itsehallinnoitujen lompakoidensa kautta[95]. Koska hajautetut kaupankäyntialustat toimivat verkossa anonyymisti hyödyntäen lohkoketjussa toimivia älysopimuksia, eivät ne sisällä kolmansia osapuolia eivätkä näin ollen ole sääntelyn alaisia.[96] Tämän lisäksi myös vaihtopalvelut voivat toimia hajautetusti. [97]

[90] Finanssivalvonta, 2025a
[91] Chen ja muut, 2023, s. 9
[92] Haffke ja muut, 2019, s. 128
[93] OECD, 2022, s. 18
[94] Xia ja muut, 2021, s. 4
[95] FATF, 2019, s. 15
[96] Dupuis & Gleason, 2021, s. 69
[97] Haffke ja muut, 2019, s. 128

3.3 Keskitetyt kryptovarapalvelun tarjoajat osaksi rahanpesusääntelyä

Perinteinen rahanpesun torjuntaa koskeva sääntely on kohdistunut erityisesti pankkeihin. Pankkeja on pidetty tärkeinä toimijoina rahanpesun torjunnassa, sillä ne toimivat keskeisessä tehtävässä maksujenvälityksessä. [98] Sääntely johtaa kuitenkin usein siihen, että rahanpesu saa uusia tekomuotoja, joita jo voimassa oleva sääntely ei tavoita. Näin kävi myös kryptovarojen kohdalla. Kun pankit alkoivat puuttua rahanpesuun entistä tarkemmin, siirtyivät rahanpesijät käyttämään kryptovaroja rahanpesun välineenä. [99] Tämä loi tarpeen laajentaa rahanpesun estämistä koskeva sääntely myös kryptovarapalvelun tarjoajiin.

Rahanpesua säännellään sekä EU-tasolla että kansallisesti. Koska rahanpesu on kansainvälinen ilmiö, on sitä koskeva sääntely kansainvälisesti pitkälti harmonisoitua. EU:n keskeisimpiin rahanpesun estämistä koskeviin säädöksiin kuuluvat rahanpesudirektiivit, jotka perustuvat FATF:n antamiin suosituksiin. [100] FATF on itsenäinen hallitusten välinen elin, joka johtaa globaalia toimintaa rahanpesun torjumiseksi. FATF:n antamat suositukset muodostavat kattavan viitekehyksen rahanpesun estämistä koskeviin velvoitteisiin. Suositukset eivät ole oikeudellisesti sitovia, mutta useimmat lainkäyttöalueet mukauttavat kansallisen sääntelyn vastaamaan näitä suosituksia. [101] Kansallinen rahanpesun estämistä koskeva sääntely perustuu EU-direktiiveihin sekä FATF:n suosituksiin[102]. Keskeinen kansallinen säädös on rahanpesulaki.

3.3.1 Rahanpesudirektiivit

Rahanpesun estämistä säännellään EU:ssa kahdella rahanpesudirektiivillä. Neljäs rahanpesudirektiivi pyrkii estämään unionin rahoitusjärjestelmän hyödyntämistä rahanpesuun. Se sääntelee rahanpesun estämistä koskevia toimenpiteitä, kuten

[98] Wuolijoki, 2022, s. 114
[99] Hyttinen, 2021, s. 104
[100] Wuolijoki, 2022, s. 114
[101] Chen ja muut, 2023, s. 30
[102] Isoaho & Kaski, 2021, s. 29

riskiperusteista lähestymistapaa, asiakkaan tuntemisvelvollisuutta sekä ilmoitusvelvollisuutta. Neljäs rahanpesudirektiivi implementoitiin kansalliseen lainsäädäntöön kesäkuussa 2017 säätämällä laki rahanpesun ja terrorismin rahoittamisen estämisestä (444/2017). Lain tavoitteena on rahanpesun ja terrorismin rahoittamisen estäminen, tällaisen toiminnan paljastaminen ja selvittäminen sekä rikoksen tuottaman hyödyn jäljittämisen ja takaisinsaannin tehostaminen. Rahanpesulakia on myöhemmin täydennetty useasti. [103]

Viidennen rahanpesudirektiivin avulla neljänteen rahanpesudirektiiviin tuotiin sekä yksittäisiä muutoksia että kokonaan uutta sääntelyä. [104] Viides rahanpesudirektiivi täydentää neljättä rahanpesudirektiiviä, ja se toi ensimmäistä kertaa tietyt kryptovarapalvelun tarjoajat rahanpesusääntelyn soveltamisalaan. Viidennen rahanpesudirektiivin (2018/843) 1 artiklan 1 kohdan c alakohta lisäsi kryptovaluuttojen ja fiat-valuuttojen välisten vaihtopalveluiden tarjoajat sekä lompakkopalvelujen tarjoajat neljännen rahanpesudirektiivin soveltamisalaan. Tämän seurauksena kyseisillä kryptovarapalvelun tarjoajilla oli neljännen rahanpesudirektiivin mukaisesti velvollisuus toteuttaa rahanpesun estämistä koskevia toimenpiteitä. Viides rahanpesudirektiivi implementoitiin Suomen lainsäädäntöön muun muassa virtuaalivaluutan tarjoajista annetulla lailla (575/2019) sekä tekemällä muutoksia rahanpesulakiin [105] . Virtuaalivaluuttalaki on myöhemmin kumottu, sillä EU sääntelyn kehitys on edellyttänyt myös kansallisen sääntelyn muuttamista.

Viidennen rahanpesudirektiivin 8 johdantokappaleen mukaan vaihtopalvelun tarjoajien sekä lompakkopalvelun tarjoajien sisällyttäminen direktiivin soveltamisalaan oli olennaisen tärkeää, sillä niillä ei aiemmin ollut unionista johtuvaa velvoitetta tunnistaa epäilyttävää toimintaa. Johdantokappaleen mukaan tämä on luonut rikollisille mahdollisuuksia siirtää rahaa unionin rahoitusjärjestelmään sekä toteuttaa siirtoja

[103] Hyttinen, 2021, s. 52–53
[104] Isoaho & Kaski, 2021, s. 28
[105] HE 261/2020 vp, s. 4

kryptovaluuttaverkostoissa salaamalla siirrot tai hyödyntämällä palveluiden osittaista anonyymiyttä. Johdantokappale korostaa, että viranomaisten on pystyttävä valvomaan kryptovarojen käyttöä ilmoitusvelvollisten kautta, jotta rahanpesua pystytään torjumaan mahdollisimman tehokkaasti.

Viidennessä rahanpesudirektiivissä tunnistetaan kuitenkin se, että kryptovaroilla voidaan tehdä transaktioita ilman palveluiden tarjoajia. Direktiivin 9 johdantokappaleessa todetaan, että kryptovarojen anonyymiyteen liittyvät ongelmat eivät täysin ratkea sillä, että vaihtopalveluiden ja lompakkopalveluiden tarjoajat sisällytetään direktiivin soveltamisalaan. Direktiivi kuitenkin pyrkii siihen, että viranomaiset saisivat mahdollisimman paljon tietoa, jonka avulla ne voivat yhdistää kryptovarojen osoitteet niiden omistajien henkilöllisyyteen.

Viides rahanpesudirektiivi toi ensimmäistä kertaa tietyt kryptovarapalvelun tarjoajat rahanpesusääntelyn soveltamisalaan. Tavoitteena oli säännellä portinvartioita eli tilanteita, joissa kryptovarat ovat joutumassa kosketuksiin perinteisen rahoitusjärjestelmän kanssa [106] . Näin ollen direktiivi ei kattanut kaikkia kryptovarapalvelun tarjoajia, mikä aiheutti edelleen haasteita. Direktiivi ei koskenut esimerkiksi vaihtopalveluita, jotka tarjosivat ainoastaan kryptovaluuttojen vaihtoa toisiin kryptovaluuttoihin. Tämä oli ongelmallista, sillä rikolliset pystyivät edelleen siirtämään laittomia varoja tällaisia vaihtopalveluita hyödyntämällä. [107]

3.3.2 Maksajan tiedot -asetus

Kryptovarojen sääntelyssä havaittiin viidennen rahanpesudirektiivin jälkeen puutteita. Euroopan unionissa ei ollut yhtenäistä sääntelyä, jonka soveltaminen olisi mahdollistanut kryptovarasiirtojen jäljittämisen vastaavalla tavalla kuin perinteiset varojen siirrot voitiin jäljittää. Aiempi maksajan tiedot -asetus velvoitti ainoastaan

[106] Silva Ramalho & Igreja Matos, 2021, s. 500
[107] Haffke ja muut, 2019, s. 134–135

maksupalvelun tarjoajia toimittamaan varainsiirtojen mukana tiedot maksajasta ja maksunsaajasta. Kun FATF teki kesäkuussa 2019 muutoksia kryptovarapalvelun tarjoajia koskeviin suosituksiin ja lisäsi vastaavat velvoitteet kryptovarapalvelun tarjoajille, tuli sääntelyä päivittää EU:ssa.[108]

Kesäkuussa 2023 astui voimaan uusi maksajan tiedot -asetus (2023/1113)[109]. Uuden asetuksen myötä kryptovarapalvelun tarjoajien tulee kerätä ja asettaa saataville tietyt tiedot välittämiensä kryptovarasiirtojen lähettäjästä ja vastaanottajasta. Tämän niin kutsutun matkustussäännön (engl. travel rule) tavoitteena on varmistaa kryptovarasiirtojen jäljitettävyys ja helpottaa epäilyttävien liiketoimien tunnistamista ja estämistä. Sääntelymuutos oli kokonaisuudessaan tärkeä toimenpide kryptovarojen vaihdannan avoimuuden varmistamiseksi sekä EU:n sääntelykehyksen yhdenmukaistamiseksi kansainvälisten standardien ja FATF:n suositusten kanssa. [110]

Maksajan tiedot -asetuksella muutettiin myös neljättä rahanpesudirektiiviä. Asetuksen 38 artiklan 2 kohdan myötä MiCA-asetuksessa määritetyt kryptovarapalvelun tarjoajat sisällytettiin neljännen rahanpesudirektiivin soveltamisalaan. Tämän muutos laajensi rahanpesusääntelyn koskemaan laajempaa joukkoa kryptovarapalvelun tarjoajia. Maksajan tiedot -asetuksen 59 johdantokappaleen mukaan tämä oli tärkeä uudistus, jotta sääntelyn porsaanreiät pystyttäisiin sulkemaan sekä lainsäädäntöä yhdenmukaistamaan kansainvälisten suositusten kanssa.

Maksajan tiedot -asetuksen myötä kryptovarapalvelun tarjoajat luokiteltiin rahanpesudirektiivissä finanssilaitoksiksi, eikä niitä pidetty enää erillisinä toimijoina. Muutos on seurausta teknologianeutraliteetista. EU-oikeuden yksi periaate on teknologianeutraalisuus, jonka perusteella samaa sääntelyä tulee soveltaa samoihin tuotteisiin ja palveluihin riippumatta niissä käytetystä teknologiasta[111]. Maksajan tiedot

[108] HE 31/2024 vp, s. 6 ja 15
[109] EBA, 2024b
[110] Euroopan unionin neuvosto, 2022a
[111] Salo-Lahti, 2023, s. 592

-asetuksen 59 johdantokappaleen mukaan tällä tavalla varmistetaan, että kryptovarapalvelun tarjoajiin sovelletaan samoja vaatimuksia ja samantasoista valvontaa kuin luotto- ja finanssilaitoksiin. Maksajan tiedot -asetusta täydentävät kansalliset säädökset sisällytettiin uuteen kansalliseen lakiin kryptovarapalvelun tarjoajista ja kryptovaramarkkinoista (402/2024)[112].

3.3.3 MiCA-asetus

MiCA-asetus tuli voimaan kesäkuussa 2023, ja sitä alettiin soveltamaan vaiheittain vuoden 2024 aikana. Asetuksen tarkoituksena on yhdenmukaistaa kryptovarojen sääntelyä EU-alueella. Ennen vain osalla jäsenmaista oli lainsäädäntöä kryptovaroihin liittyen, mutta MiCA-asetus tuo jäsenmaihin yhdenmukaisen kryptovarojen sääntelyn.[113] Sääntelykokonaisuus tarjoaa oikeudellista varmuutta sekä sijoittajille että yrityksille. Se myös suojaa kuluttajia ja torjuu rahanpesua, samalla kun se luo perustan kryptovaramarkkinoiden kestävämmälle kasvulle. [114] Tavoitteena on sijoittajien suojaaminen ja rahoitusvakauden säilyttäminen samalla kun mahdollistetaan innovointia ja edistetään kryptovara-alan houkuttelevuutta[115].

MiCA-asetus oli tärkeä askel kryptovarasektoria koskevan sääntelyn yhdenmukaistamiselle. Yhtenäisten eurooppalaisten sääntöjen puutteet aiheuttavat markkinoiden eheyteen kohdistuvia merkittäviä riskejä, kuten markkinoiden väärinkäyttöä ja talousrikollisuutta. Sääntelyn puutteet koskivat esimerkiksi kryptovarojen kaupankäyntialustojen ylläpitoa, kryptovarojen vaihtoa varoihin tai muihin kryptovaroihin sekä kryptovarojen säilytystä ja hallinnointia asiakkaiden puolesta. [116] MiCA-asetus asettaakin useita vaatimuksia kryptovarojen liikkeeseenlaskijoille sekä

[112] Keskusrikospoliisi, 2026, s. 19
[113] Valtiovarainministeriö, 2023
[114] Soon, 2025
[115] Euroopan unionin neuvosto, 2022b
[116] HE 31/2024 vp, s. 26

palveluntarjoajille[117]. Vaikka MiCA-asetus ei varsinaisesti ole rahanpesuun estämiseen keskittyvä säädös, on sillä välillisiä vaikutuksia myös rahanpesun torjuntaan.

Maksajan tiedot -asetuksen tavoin MiCA-asetus implementointiin Suomeen lailla kryptovarapalvelun tarjoajista ja kryptovaramarkkinoista (402/2024). Lakiin otettiin välttämättömät säännökset MiCA:n täytäntöönpanon toteuttamiseksi. Lisäksi kryptovaran ja kryptovarapalvelun määritelmää sekä muuta terminologiaa yhdenmukaistettiin MiCA-asetuksen kanssa. [118] Kryptovarapalvelulaki ei sääntele kansallisesti rahanpesun ehkäisemiseen vaadittavista toimista, kuten asiakkaiden tuntemisvelvollisuudesta. Nämä velvoitteet ovat rahanpesulaissa, jonka 1 luvun 2 §:n 8 a kohta tuo MiCA-asetuksessa määritetyt kryptovarapalvelun tarjoajat lain soveltamisalaan.

[117] Salo-Lahti, 2023, s. 587
[118] HE 31/2024 vp, s. 60

4 Kryptovarapalvelun tarjoajien velvollisuudet

4.1 Riskiperusteinen arviointi

Riskiperusteinen arviointi on keskeinen osa rahanpesun torjuntaa. Rahanpesulain 3 luvun 1 §:n 2 momentin mukaan kryptovarapalvelun tarjoajan on arvioitava asiakassuhteeseen liittyviä rahanpesun riskejä. Arvioinnissa tulee huomioida uusiin ja jo olemassa oleviin asiakkaisiin, maihin tai maantieteellisiin alueisiin sekä uusiin, kehitettäviin ja jo olemassa oleviin tuotteisiin, palveluihin ja liiketoimiin sekä jakelukanaviin ja teknologioihin liittyvät rahanpesun riskit. Rahanpesulain 3 luvun 1 §:n 3 momentin mukaan asiakkaan tuntemista koskevia toimia tulee noudattaa riskiperusteiseen arviointiin pohjautuen koko asiakassuhteen ajan. Asiakkaiden tuntemis- ja valvontatoimenpiteet tulee suhteuttaa asiakkaasta aiheutuviin riskeihin. Korkeamman riskin asiakkaat edellyttävät tehostetumpia tuntemis- ja valvontatoimia.[119]

Riskiperusteinen arviointi toimii lähtökohtana muille rahanpesun estämisen toimenpiteille, sillä nämä toimenpiteet tulee suhteuttaa tunnistettuihin riskeihin. Kryptovarapalvelun tarjoajien on siten ymmärrettävä, millaisia riskitekijöitä niiden toimintaan liittyy ja miten niiden tuotteita ja palveluita voidaan käyttää hyväksi rahanpesussa. Riskiperusteisessa arvioinnissa on luontaista painottaa tuotteisiin ja palveluihin liittyvää riskiä suhteessa muihin riskitekijöihin, sillä tuotteet ja palvelut määrittävät sen, miten tiettyä toimijaa voidaan käyttää hyväksi rahanpesussa[120].

Rahanpesulaki antaa raamit riskiperusteiselle arvioinnille, mutta valvonta- ja sääntelyviranomaiset ovat antaneet tarkempia ohjeistuksia tekijöistä, joita kryptovarapalvelun tarjoajien tulee ottaa huomioon riskiperusteisessa arvioinnissa. Euroopan pankkiviranomaisen mukaan erityisesti sellaiset kryptovarapalvelun tarjoajan

[119] Wuolijoki, 2022, s. 117
[120] Finanssivalvonta, 2024, s. 7

tuotteet tai palvelut, jotka tarjoavat korkeamman anonymiteetin, voivat lisätä rahanpesun riskiä[121]. Esimerkiksi aiemmin käsitellyt privaattikryptovaluutat tarjoavat korkeamman anonymiteetin lohkoketjussa, mikä vaikeuttaa varojen alkuperän selvittämistä. Tällaisten kryptovaluuttojen huomioiminen riskiperusteisessa arvioinnissa on tärkeää, jotta kryptovarapalvelun tarjoaja voi kohdentaa tehostetummat valvonta- ja seurantatoimet liiketoimiin, joihin liittyy tällaisia kryptovaluuttoja.

Euroopan pankkiviranomaisen mukaan myös sellaiset tuotteet tai palvelut, jotka mahdollistavat liiketoimet asiakkaan tilin ja itsehallinnoitujen lompakoiden tai hajautettujen palveluiden välillä ovat riskillisiä [122] . FATF:n mukaan tällaiset palvelut ovat erityisen riskillisiä, ja kryptovarapalvelun tarjoajien tulisikin arvioida, missä määrin tällaiset liiketoimet ovat heidän riskinottohalukkuuden mukaisia. Kryptovarapalvelun tarjoajat voisivat riskianalyysinsä mukaisesti päättää asettaa rajoituksia tai jopa kieltoja itsehallinnoitujen lompakoiden kanssa tapahtuville liiketoimille. [123] Itsehallinnoidut lompakot ja hajautetut palvelut perustuvat kryptovarojen hajautettuun rakenteeseen, joka mahdollistaa varojen hallinnoimisen ja siirtämisen ilman keskitettyä palveluntarjoajaa. Näin ollen niissä ei ole toimijaa, joka valvoisi varojen alkuperää tai määränpäätä, mikä korostaa tarvetta kohdistaa tällaisiin liiketoimiin tehostetumpia valvonta- ja seurantatoimia.

Vaikka tuotteet ja palvelut ovat keskeisessä asemassa riskiperusteisessa arvioinnissa, tulee kryptovarapalvelun tarjoajan huomioida myös muita riskitekijöitä. Asiakkaisiin liittyvien riskitekijöiden osalta Euroopan pankkiviranomainen on painottanut erityisesti asiakkaiden käyttäytymisen arviointia. Kryptovarapalvelun tarjoajien tulisi kiinnittää huomiota esimerkiksi tilanteisiin, joissa asiakas yrittää avata perusteetta useita kryptovaratilejä, ei suostu toimittamaan tuntemisvelvollisuutta koskevia tietoja tai antaa ristiriitaisia tietoja. Huomiota tulisi kiinnittää myös asiakkaisiin, jotka toteuttavat

[121] EBA, 2024c
[122] EBA, 2024c
[123] FATF, 2021, s. 86

asiakasprofiilille epätyypillisiä liiketoimia. [124] Tämä korostaa kokonaisvaltaisen riskiperusteisen arvioinnin merkitystä. Vaikka jokin tuote tai palvelu ei itsessään nostaisi rahanpesun riskiä, voi asiakkaan toiminta tehdä tilanteesta lopulta epäilyttävän. Liiallinen keskittyminen tuotteisiin ja palveluihin voi siten johtaa siihen, että muut rahanpesua indikoivat tekijät jäävät havaitsematta.

Koska kryptovaroja voi siirtää reaaliaikaisesti minne tahansa maailmaan, on myös maahan tai maantieteelliseen alueeseen liittyvien riskitekijöiden huomioiminen tärkeää. Euroopan pankkiviranomaisen mukaan rahanpesun riskiä voi kasvattaa tilanteet, joissa kryptovaroihin vaihdettavat varat, kryptovaratilin osoite, asiakkaan asuinpaikka tai liiketoimet liittyvät maahan, jossa on kohonnut rahanpesun riski. [125] Kryptovarojen kansainvälisen luonteen vuoksi rikolliset pystyvät hyödyntämään helposti maita, joissa rahanpesun torjunta on heikkoa. Tästä syystä myös maantieteellisiin alueisiin liittyvien riskitekijöiden huomioiminen on olennainen osa kokonaisvaltaista riskiarviota.

Kokonaisuudessaan kryptovarojen pseudonyymisyys tai anonyymisyys, mahdollisuus reaaliaikaisiin ja kansainvälisiin transaktioihin sekä hajautettu rakenne voivat muodostaa merkittäviä riskejä kryptovarapalvelun tarjoajien toiminnalle ja siten näiden tekijöiden huomioon ottaminen riskiperusteisessa arvioinnissa on tärkeää. Huolellisen riskiperusteisen arvioinnin avulla kryptovarapalvelun tarjoajat pystyvät kohdistamaan tehokkaasti muut AML-toimenpiteet niihin osa-alueisiin, joissa riski on suurin.

[124] EBA, 2024c
[125] EBA, 2024c

4.2 Asiakkaiden tunteminen

Asiakkaiden tunteminen on yksi tärkeimmistä rahanpesun estämiseen liittyvistä velvoitteista. Sen avulla voidaan lieventää erityisesti kryptovarojen pseudonyymistä tai anonyymistä luonteesta aiheutuvia riskejä. Vaikka kryptovarojen taustalla toimiva lohkoketju on julkinen, kryptovarapalvelun tarjoaja tarvitsee lisätietoja asiakkaistaan, jotta tietty lompakon osoite voidaan yhdistää todelliseen luonnolliseen henkilöön[126].

Rahanpesulain 3 luvun 2 §:n 1 momentin mukaan kryptovarapalvelun tarjoajalla ei saa olla anonyymejä tai tekaistuilla nimillä olevia tilejä tai asiakkuuksia. Rahanpesulain 3 luvun 1 §:n 1 momentin mukaan kryptovarapalvelun tarjoaja ei saa perustaa asiakassuhdetta, suorittaa liiketointa tai ylläpitää liikesuhdetta, mikäli se ei pysty toteuttamaan asiakkaan tuntemiseksi säädettyjä toimia. Rahanpesulain 3 luvun 2 §:n 1 momentin mukaan kryptovarapalvelun tarjoajan on tunnistettava asiakkaansa ja todennettava heidän henkilöllisyytensä vakituista asiakassuhdetta perustettaessa tai jos kyseessä on satunnainen asiakkuus ja kryptovarapalvelun tarjoajan alustalla on tehdään yli 1 000 euron suuruinen liiketoimi.

Rahanpesulain 1 luvun 4 §:n 1 momentin 6 ja 7 kohtien mukaan asiakkaan tunnistamisella tarkoitetaan henkilöllisyyden selvittämistä asiakkaan toimittamien tietojen perusteella, ja henkilöllisyyden todentamisen avulla varmistetaan asiakkaan henkilöllisyys luotettavien ja riippumattomien asiakirjojen tai tietojen perusteella. Kryptovarapalvelun tarjoaja voi omiin riskiperusteisiin menettelytapoihin perusten päättää, mitä se pitää luotettavasta ja riippumattomasta lähteestä peräisin olevina asiakirjoina tai tietoina. Asiakirjojen ja tietojen aitous tulisi kuitenkin varmistaa esimerkiksi vertaamalla tietoja Digi- ja väestöviraston ylläpitämän väestörekisterin tietoihin.[127] Kun kryptovarapalvelun tarjoaja on selvittänyt asianmukaisesti asiakkaansa henkilöllisyyden, on asiakkaan toiminnan seuraaminen ja jäljittäminen helpompaa.

[126] FATF, 2019, s. 27
[127] Finanssivalvonta, 2023, s. 33

Tällöin asiakas ei voi toimia enää pelkästään lohkoketjun muodostaman pseudonyymin alla, vaan asiakkaan toteuttamat liiketoimet ovat suoraan kytköksissä asiakkaan henkilöllisyyteen.

Asiakkaan tunnistamisen lisäksi kryptovarapalvelun tarjoajan tulee tuntea asiakkaansa. Asiakkaan tuntemisella tarkoitetaan asiakkaan taloudellisen tilanteen sekä liiketoiminnan tuntemista[128]. Rahanpesulain 3 luvun 3 §:n 2 momentissa on lueteltu asiakkaiden tuntemiseksi hankittavat tiedot. Näitä ovat perustietojen [129] lisäksi tiedot muun muassa asiakkaan toiminnasta, liiketoiminnan laadusta ja laajuudesta, taloudellisesta asemasta, perusteet liiketoimen tai palvelun käytölle sekä tiedot varojen alkuperästä. Asiakkaan tuntemisen avulla kryptovarapalvelun tarjoaja voi muodostaa kokonaiskuvan asiakkaasta ja tämän tyypillisestä toiminnasta. Kun kryptovarapalvelun tarjoaja tuntee asiakkaan normaalin toiminnan, on epäilyttävien liiketoimien havaitseminen helpompaa. Kryptovarapalvelun tarjoaja voi käyttää hyödyksi asiakkaan tuntemiseksi kerättyjä tietoja ja verrata näitä asiakkaan tosiasialliseen toimintaan.

4.3 Tehostettu tuntemisvelvollisuus

Tehostettu tuntemisvelvollisuus auttaa hallitsemaan tilanteita, joihin liittyy korkeampi rahanpesun riski[130]. Se edellyttää korostuneen huolellista menettelyä, kuten normaalia laajempaa selvitystä ja dokumentaatiota asiakkaan toiminnasta ja palveluiden käytöstä[131]. Rahanpesulain 3 luvun 11–13 a §:ssä luetellaan yhteensä viisi tilannetta, joissa on sovellettava tehostettua tuntemisvelvollisuutta. Kryptovaroihin liittyvien riskien hallinnassa keskeisimmät tilanteet liittyvät etätunnistamiseen, isännöimättömiin osoitteisiin sekä Euroopan talousalueen ulkopuolisiin korkean riskin valtioihin.

[128] Wuolijoki, 2022, s. 115–116
[129] Perustiedot eli asiakkaan nimi, syntymäaika, henkilötunnus ja osoite
[130] Finanssivalvonta, 2023, s. 51
[131] HE 31/2024 vp, s. 63

Kryptovarat mahdollistavat liikesuhteet ilman kasvokkain tapahtuvaa kontaktia, mikä voi lisätä niihin liittyviä rahanpesun riskejä[132] . Rahanpesulain 3 luvun 11 § 1 momentin mukaan jos asiakas ei ole läsnä tunnistettaessa tai henkilöllisyyttä todennettaessa, tulee kryptovarapalvelun tarjoajan todentaa asiakkaan henkilöllisyys luotettavien lisäasiakirjojen tai -tietojen avulla taikka vahvan sähköisen tunnistamisen kautta. Asiakkaiden huolellinen etätunnistaminen on tärkeää. Rahanpesun riski kasvaa, jos asiakkaan tunnistamis- ja todentamistoimenpiteet eivät huomioi tarpeeksi hyvin etäasiakassuhteista aiheutuvia riskejä. Heikot tunnistamismenetelmät voivat vaikeuttaa varojen jäljittämistä ja transaktioiden vastapuolten tunnistamista. [133] Tästä syystä kryptovarapalvelun tarjoajia suositellaan käyttämään vain vahvoja digitaalisia tunnistusratkaisuja[134].

Rahanpesulain 3 luvun 12 a §:n 2 momentin mukaan kryptovarapalvelun tarjoajan tulee soveltaa tehostettua tuntemismenettelyä, kun asiakas tekee liiketoimia, jotka liittyvät isännöimättömiin osoitteisiin. Maksajan tiedot -asetuksen 3 artiklan 1 kohdan 20 alakohdan mukaan isännöimättömällä osoitteella tarkoitetaan hajautetun tilikirjan osoitetta, johon ei liity kryptovarapalvelun tarjoajaa. Tällaisia ovat esimerkiksi itsehallinnoidut lompakot. Rahanpesulain 3 luvun 12 a §:n 2 momentin mukaan tehostettuihin tuntemismenettelyihin kuuluvat isännöimättömää osoitetta käyttävän henkilöllisyyden selvittäminen, lisätietojen vaatiminen siirrettyjen kryptovarojen alkuperästä ja määränpäästä sekä kyseisten liiketoimien jatkuva seuranta. Näiden toimenpiteiden avulla kryptovarapalvelun tarjoaja voi tunnistaa isännöimättömän osoitteen hallinnoijan ja ymmärtää paremmin liiketoimien tarkoitusta, mikä voi helpottaa rahanpesuun viittaavan toiminnan havaitsemista. Koska isännöimättömiin osoitteisiin liittyvissä liiketoimissa ei ole vastapuolella keskitettyä tahoa, joka toteuttaisi asiakkaan tuntemista tai muita seuranta- ja valvontatoimia, ovat tehostetut tuntemismenettelyt keskeinen keino hallita tästä aiheutuvia riskejä.

---

[132] FATF, 2019, s. 11
[133] FATF, 2019, s. 11–12
[134] FATF, 2021, s. 16

Rahanpesulain 3 luvun 13 a §:n 1 momentin mukaan kryptovarapalvelun tarjoajan tulee soveltaa tehostettuja tuntemismenettelyjä myös liiketoimiin, jotka liittyvät Euroopan talousalueen ulkopuolisiin korkean riskin valtioihin. Tämä on erityisen tärkeää kryptovarasektorilla ottaen huomioon kryptovarojen rajat ylittävän luonteen [135] . Rahanpesulain 3 luvun 13 a §:n 1 momentin mukaan tehostettuihin tuntemismenettelyihin kuuluvat muun muassa lisätietojen hankkiminen asiakkaasta, perustettavasta liikesuhteesta, varojen alkuperästä ja liiketoimen syistä. Kryptovarapalvelun tarjoajan tulee hankkia myös ylemmän johdon hyväksyntä asiakassuhteelle sekä järjestää tehostettu asiakassuhteen seuranta. Näiden menettelyiden avulla kryptovarapalvelun tarjoaja pystyy tehokkaammin lieventämään riskiä siitä, että rikolliset hyödyntäisivät kryptovarojen reaaliaikaista ja kansainvälistä luonnetta rahanpesussa.

Rahanpesulaissa lueteltujen tilanteiden lisäksi lain 3 luvun 10 §:n 1 momentin 2 kohdan mukaan tehostettua tuntemismenettelyä tulee käyttää myös tilanteisiin, joihin arvioidaan liittyvän korkeampi rahanpesun riski. Tämä jättää tehostetun tuntemismenettelyn soveltamisen kryptovarapalvelun tarjoajien oman riskiarvion varaan, mikä korostaa huolellisen riskiperusteisen arvioinnin merkitystä. Kryptovarapalvelun tarjoajien tulee tunnistaa, millaisiin tilanteisiin liittyy korkeampi rahanpesun riski, ja siten soveltaa niihin tehostetumpia tuntemistoimenpiteitä.

4.4 Liiketoimien seuranta

Liiketoimien seurannan avulla kryptovarapalvelun tarjoaja voi seurata asiakkaidensa tosiallista toimintaa ja tätä kautta havaita epäilyttäviä liiketoimia. Rahanpesulain 3 luvun 4 §:n 2 momentin mukaan kryptovarapalvelun tarjoajan tulee järjestää asiakkaiden toiminnan laatu ja laajuus, asiakassuhteen pysyvyys ja kesto sekä riskit huomioon ottaen

[135] FATF, 2019, s. 31

riittävä seuranta varmistaakseen, että asiakkaan toiminta vastaa kryptovarapalvelun tarjoajalla olevaa tietoa asiakkaasta ja tämän toiminnasta.

Jatkuvan seurannan avulla kryptovarapalvelun tarjoaja voi havaita sellaisia liiketoimia, jotka eivät vastaa asiakkaan profiilin mukaista käyttäytymistä tai muutoin poikkeavat tavanomaisesta liiketoiminnasta[136]. Tämä korostaa asiakkaan tuntemisen ja jatkuvan seurannan välistä yhteyttä. Kun kryptovarapalvelun tarjoaja toteuttaa huolellisesti asiakkaan tuntemista ja sitä kautta muodostaa kokonaiskuvan asiakkaastaan, on epäilyttävien liiketoimien tunnistaminen helpompaa.

Rahanpesulain 3 luvun 4 §:n 3 momentin mukaan erityistä huomiota on kiinnitettävä liiketoimien rakenteeseen ja suuruuteen sekä liiketoimiin, joilla ei ole ilmeistä taloudellista tarkoitusta tai ne eivät sovi yhteen tietoon, joka kryptovarapalvelun tarjoajalla on asiakkaasta ja tämän toiminnasta. Liiketoimien seurannassa tulisi ottaa huomioon myös, mikäli kryptovarapalvelun tarjoaja sallii liiketoimet sellaisten palveluiden kanssa, joiden ilmeinen tarkoitus on häivyttää varojen alkuperä[137]. Jatkuvaa seurantaa tulee soveltaa tehostetummin tällaisissa korkeamman riskin tilanteissa[138].

Kryptovarasiirtoja tapahtuu suuressa määrin koko ajan, jonka vuoksi automatisoidut järjestelmät ovat usein ainoa realistinen tapa seurata liiketoimia[139]. Kryptovarapalvelun tarjoajien tulee varmistaa, että niillä on käytössä asianmukaiset ja tehokkaat liiketoimien seurantatyökalut ja edistyneet analyysityökalut. Erityisesti isännöimättömän osoitteen kanssa toteutettuihin liiketoimiin tulee hyödyntää edistyneitä analyysityökaluja, koska niiden avulla voi jäljittää liiketoimien historian ja havaita mahdolliset yhteydet rikolliseen toimintaan, henkilöihin ja yhteisöihin. [140]

[136] FATF, 2021, s. 81
[137] Finanssivalvonta, 2023, s. 60
[138] FATF, 2021, s. 81
[139] FATF, 2021, s. 81
[140] EBA, 2024c

4.5 Selonotto- ja ilmoitusvelvollisuus

Jatkuvan seurannan lisäksi kryptovarapalvelun tarjoajilla on rahanpesulain mukainen selonotto- ja ilmoitusvelvollisuus. Rahanpesulain 3 luvun 4 §:n 3 momentin mukaan kryptovarapalvelun tarjoajien tulee tarvittaessa selvittää liiketoimeen liittyvien varojen alkuperä. Selonottovelvollisuus koskee erityisesti tavanomaisesta poikkeavia tai epäilyttäviä liiketoimia. Kryptovarapalvelun tarjoajan tulee selvittää liiketoimien tarkoitusta ja perusteita sekä tehdä niistä mahdollinen ilmoitus rahanpesun selvittelykeskukselle. [141] Selonottovelvollisuus täydentää liiketoimien seurantaa ja on siten keskeinen osa rahanpesun torjuntaa. Pelkkä liiketoimien tekninen seuranta ei yksinään riitä hallitsemaan rahanpesun riskejä, vaan kryptovarapalvelun tarjoajien tulee ymmärtää liiketoimien tarkoitusta ja arvioida, ovatko ne asiakasprofiilille tavanomaisia.

Kryptovarapalvelun tarjoajan tulee käytettävissä olevin kohtuullisin keinoin selvittää asiakkaansa epäilyttävän toiminnan taustaa sekä siihen liittyvien varojen alkuperää ja käyttötarkoitusta. Selvityksiä voi hankkia esimerkiksi viranomaisrekistereistä tai omista rekistereistä saatavista tiedoista. Asiakkaalta voi myös pyytää tarkempaa selvitystä liiketoimesta esimerkiksi pyytämällä liiketoimea tukevia sopimus- tai muita asiakirjoja.[142] Varojen alkuperän selvittämisessä on tarkoitus selvittää, mihin oikeustoimeen varat liittyvät. Näin ollen pelkkä tieto varojen lähettäjästä tai siirron toteuttaneesta tahosta ei riitä. Mikäli asiakas ei anna asiakirjoihin perustuvaa selvitystä, tulisi arvioida, onko selvitys riittävä kumoamaan herännyttä epäilyä.[143] Selonottovelvollisuus on siis prosessi, joka edellyttää kryptovarapalvelun tarjoajalta asiakkaan toiminnan kokonaisvaltaista ymmärrystä ja kriittistä arviointia.

Rahanpesulain 4 luvun 1 §:n 1 momentin mukaan kryptovarapalvelun tarjoajan tulee ilmoittaa viipymättä rahanpesun selvittelykeskukselle epäilyttävästä liiketoimesta.

[141] Finanssivalvonta, 2021
[142] Finanssivalvonta, 2021
[143] Finanssivalvonta, 2023, s. 62–63

Ilmoitusvelvollisuus koskee tilanteita, joissa asiakkaaseen ja asiakkaan toimintaan yleisesti liittyy epäilyttävyyttä tai jos asiakkaan yksittäiseen liiketoimeen liittyy epäilyttävyyttä[144]. Ilmoitusvelvollisuus jättää paljon harkintavaltaa kryptovarapalvelun tarjoajille, mikä korostaa niiden laajaa ymmärrystä rahanpesusta ja siihen viittaavista riskitekijöistä. Kryptovarojen erityispiirteet ja kryptovaroilla toteutettavat monimutkaiset liiketoimet voivat tehdä epäilyttävien liiketoimien havaitsemisesta ja arvioinnista hankalaa, mikä korostaa myös muiden AML-velvoitteiden huolellista noudattamista. Kun kryptovarapalvelun tarjoaja noudattaa asianmukaisesti kaikkia AML-velvoitteita, se pystyy tunnistamaan tehokkaammin epäilyttäviä liiketoimia ja siten raportoimaan ne viranomaisille.

4.6 Toimiluvan hakeminen

MiCA-asetus asettaa useita velvoitteita kryptovarasektorille. Rahanpesun torjunnan kannalta keskeisin MiCA-asetuksessa asetettu velvoite on toimiluvan hakeminen. MiCA-asetuksen 59 artiklan 1 kohdan mukaan vain sellainen yritys, jolle on myönnetty kryptovarapalvelun tarjoajan toimilupa, saa tarjota kryptovarapalveluja Euroopan unionin alueella. Lisäksi artiklan 7 kohdan mukaan toimiluvan saanut kryptovarapalvelun tarjoaja voi tarjota kryptovarapalveluja kaikkialla unionissa. Tätä kutsutaan EU-passimenetelmäksi, ja se mahdollistaa kryptovarapalveluiden tarjoamisen kaikissa EU-maissa yhdellä toimiluvalla[145].

EU-passimenetelmä helpottaa kryptovarapalvelun tarjoajien toimintaa, sillä jatkossa toimijoiden ei tarvitse selvittää sääntelyeroja eri jäsenvaltioiden alueella, vaan pelkkä ilmoitus mahdollistaa palveluiden tarjoamisen sisämarkkinoilla [146] . Esimerkiksi suomalainen kryptovarapalvelun tarjoaja Coinmotion Oy on saanut Finanssivalvonnan

[144] Finanssivalvonta, 2023, s. 69
[145] Salo-Lahti, 2023, s. 592
[146] HE 31/2024 vp. s. 31

myöntämän toimiluvan, ja yhteisön kotivaltiona toimii Suomi[147]. Yhdysvaltalainen Kraken on puolestaan saanut MiCA-asetuksen mukaisen toimiluvan Irlannin keskuspankilta[148].

MiCA-asetus ei ole rahanpesudirektiivien tavoin rahanpesun estämistä koskeva säädös eikä se säädä rahanpesun estämisen konkreettisista toimenpiteistä. MiCA-asetuksella on kuitenkin toimilupamenettelyn kautta välillisiä vaikutuksia rahanpesun torjuntaan. MiCA-asetuksen 62 artiklan 1 kohdan mukaan yritysten, jotka aikovat tarjota kryptovarapalveluja, tulee jättää toimilupahakemus oman kotijäsenvaltionsa toimivaltaiselle viranomaiselle. Hakemuksen on sisällettävä kaikki artiklassa vaaditut tiedot, joihin sisältyy muun muassa kuvaus kryptovarapalvelun tarjoajan sisäisen valvonnan mekanismeista, toimintaperiaatteista ja menettelyistä, joilla tunnistetaan, arvioidaan ja hallitaan rahanpesuun liittyviä riskejä. Kryptovarapalvelun tarjoajien tulee osoittaa, että niillä on rahanpesun torjumiseksi riittävät valvontamekanismit ja riskienhallintamenettelyt, jotka koskevat niiden toimintaa, organisaatiotaan ja hallintoaan [149]. Ilman toimilupamenettelyä nämä toimet voisivat jäädä puutteellisiksi ja mahdolliset epäkohdat voisivat paljastua vasta myöhemmin.

MiCA-asetuksen 63 artiklan 10 kohdassa luetellaan syitä, joiden perusteella toimivaltainen viranomainen voi evätä kryptovarapalvelun tarjoajan toimiluvan. Toimilupa voidaan evätä esimerkiksi jos kryptovarapalvelun tarjoajan ylin hallintoelin altistaa kryptovarapalvelun tarjoajan rahanpesuun liittyvälle vakavalle riskille tai jos kryptovarapalvelun tarjoaja ei täytä muita asetuksen vaatimuksia. Yritysten toiminta käydään toimilupahakemuksen jälkeen huolellisesti läpi, jotta varmistetaan, että ne täyttävät sääntelyn vaatimukset [150]. Näin ollen toimilupamenettelyllä on positiivisia vaikutuksia rahanpesun torjuntaan, sillä sen avulla markkinoilta jää pois sellaiset yritykset, jotka eivät täytä asianmukaisesti AML-vaatimuksia.

[147] Finanssivalvonta, n.d.
[148] Kraken, 2025
[149] EBA, 2024a
[150] He 31/2024 vp, s. 63

Toimiluvan saamisen jälkeen kryptovarapalvelun tarjoajien on varmistettava, että ne noudattavat jatkuvasti rahanpesun estämistä koskevia velvoitteita [151]. Toimilupa- ja valvontaviranomaiset varmistavat, että kryptovarapalvelun tarjoajilla on tehokkaat rahanpesun estämisjärjestelmät käytössä heti toimiluvan myöntämisestä lähtien [152]. MiCA-asetuksen 64 artiklan 1 kohdassa luetellaan syitä, joiden perusteella toimivaltainen viranomainen voi peruuttaa kryptovarapalvelun tarjoajan toimiluvan. Toimilupa voidaan peruuttaa muun muassa, mikäli kryptovarapalvelun tarjoaja ei ole ottanut käyttöön tehokkaita järjestelmiä, menettelyjä tai järjestelyjä rahanpesun havaitsemiseksi ja ehkäisemiseksi. Toimilupavaatimusten täyttäminen ei siten ole kertaluonteinen edellytys, vaan jatkuva prosessi, joka edellyttää kryptovarapalvelun tarjoajalta tehokkaita toimenpiteitä rahanpesun torjumiseksi. Kokonaisuudessaan MiCA-asetus vahvistaa AML-sääntelyä kryptovaramarkkinoilla edellyttämällä kryptovarapalvelun tarjoajilta riittäviä rahanpesun estämisen toimenpiteitä.

4.7 Kryptovarasiirtojen mukana toimitettavat tiedot

Kryptovaroilla on mahdollista toteuttaa liiketoimia ilman, että siirron osapuolten henkilöllisyys paljastuu. Tämä aiheuttaa merkittäviä riskejä rahanpesun torjuntaan, sillä tällaiset anonyymit liiketoimet vaikeuttavat varojen alkuperän ja määränpään selvittämistä. Anonyymeihin kryptovarasiirtoihin puututtiin maksajan tiedot -asetuksella, jonka keskeinen tavoite on estää tällaiset siirrot kryptovarapalvelun tarjoajien alustoilla. Maksajan tiedot -asetuksen 4 johdantokappaleen mukaan rahoitusalan eheys, vakaus ja maine, unionin sisämarkkinat sekä kansainvälinen kehitys voivat vahingoittua, mikäli kryptovarasiirtojen avulla pääsee liikkumaan laittomia rahavirtoja. Asetuksen 16 johdantokappaleessa korostetaan, että kryptovarasiirtojen jäljitettävyys voi olla erityisen tärkeä keino rahanpesun estämisessä sekä paljastamisessa.

[151] EBA, 2024a
[152] AMLA, 2025

Maksajan tiedot -asetusta sovelletaan 2 artiklan 1 kohdan mukaan kryptovarojen siirtoihin silloin, kun siirrossa on mukana kryptovarapalvelun tarjoaja ja kyseisellä palveluntarjoajalla on sääntömääräinen kotipaikka unionissa. Asetuksen 2 artiklan 4 kohdan mukaan asetusta ei sovelleta kahden henkilön välisiin kryptovarojen siirtoihin, jotka toteutetaan ilman kryptovarapalvelun tarjoajan osallistumista. Kryptovarojen hajautetun rakenteen vuoksi tämä luo haasteen, sillä anonyymit siirrot voivat toteutua edelleen vertaisverkossa.

Maksajan tiedot -asetus rajoittaa kryptovarojen anonyymejä siirtoja edellyttämällä kryptovarapalvelun tarjoajaa toimittamaan yksilölliset tiedot kryptovarasiirron osapuolista. Asetuksen 14 artiklan 1 ja 2 kohtien mukaan siirron toimeksiantajan käyttämän kryptovarapalvelun tarjoajan tulee varmistaa, että kryptovarasiirtojen mukana toimitetaan tiedot siirron osapuolten nimistä ja hajautetun tilikirjan osoitteesta tai kryptovaratilin numerosta. Lisäksi siirron toimeksiantajasta tulee välittää osoitetiedot ja yksilöivät henkilöllisyystiedot.

Maksajan tiedot -asetuksen 14 artiklan 6 kohdan mukaan kryptovarasiirtojen mukana toimitettavien tietojen oikeellisuus tulee todentaa luotettavasta ja riippumattomasta lähteestä saatujen tietojen perusteella ennen kryptovarojen siirtämistä. Kokonaisuudessaan siirron osapuolista kerättävät tiedot mahdollistavat kryptovarasiirtojen yhdistämisen tunnistettuihin henkilöihin, mikä tehostaa rahanpesun torjuntaa ja helpottaa epäilyttävien liiketoimien havaitsemista sekä seuraamista. Näin ollen siirron toimeksiantajan käyttämällä kryptovarapalvelun tarjoajalla on keskeinen asema tietojen huolellisena kerääjänä ja välittäjänä.

Maksajan tiedot -asetuksen 16 artiklan 1 kohta velvoittaa siirronsaajan käyttämää kryptovarapalvelun tarjoajaa varmistamaan, että kryptovarasiirtoon sisältyy vaaditut tiedot siirron osapuolista. Kryptovarapalvelun tarjoajan tulee pystyä havaitsemaan siirron aikana ja sen jälkeen toteutettujen valvontakäytäntöjen yhdistelmän avulla, jos tiedot ovat puutteellisia tai merkinnät ja sisällöt epäasianmukaisia. Tietoja tulisi pitää

puutteellisina, jos kentät on jätetty tyhjiksi tai jos annetut tiedot ovat epätäydellisiä ja merkityksettömiä, esimerkiksi satunnaisista ja epäloogisista merkeistä koostuvat merkkijonot tai puhuttelunimet.[153]

Maksajan tiedot -asetuksen 17 artiklan 1 kohdan mukaan siirronsaajan käyttämän kryptovarapalvelun tarjoajan tulee riskiperusteisen arvioinnin perusteella tehdä päätös evätäänkö, palautetaanko vai keskeytetäänkö puutteellisin tiedoin toteutettu siirto. Tämä tekee siirronsaajan käyttämästä kryptovarapalvelun tarjoajasta keskeisen toimijan tietojen oikeellisuuden ja uskottavuuden arvioinnissa. Tämä korostaa myös huolellisen riskiperusteisen arvioinnin soveltamista, jotta puutteelliset ja epäilyttävät siirrot havaitaan ja niihin voidaan tarvittaessa reagoida.

Maksajan tiedot -asetuksen 14 ja 16 artiklojen mukaan kryptovarasiirtojen osapuolet tulee yksilöidä myös tilanteissa, joissa kryptovarojen siirto tehdään isännöimättömän osoitteen ja kryptovarapalvelun tarjoajan välillä. Tiedot siirron toimeksiantajasta tai siirronsaajasta tulee kerätä asiakkaalta itseltään [154] . Yli 1 000 euron siirroissa kryptovarapalvelun tarjoajan on varmistettava isännöimättömän osoitteen omistaja tai hallinnoija. Varmennusmenetelmien tulee olla sellaisia, jotka mahdollistavat luotettavan ja turvallisen arvioinnin. Kryptovarapalvelun tarjoajan on oltava täysin vakuuttunut isännöimättömän osoitteen omistajasta tai hallinnoijasta. Käytännössä tämä voi tapahtua esimerkiksi testisiirrolla, jossa kryptovarapalvelun tarjoaja määrittelee ennalta summan, joka tulee lähettää kryptovarapalvelun tarjoajan tilille isännöimättömästä osoitteesta. [155] Tämä korostaa tarvetta hallita isännöimättömiin osoitteisiin liittyviä riskejä. Kun vastapuolella ei ole palveluntarjoajaa, joka voisi tunnistaa asiakkaan, tarvitsee kryptovarapalvelun tarjoaja menetelmiä, joiden avulla voidaan todentaa luotettavasti siirron vastapuolella oleva henkilö.

[153] EBA, 2024d
[154] EBA, 2024d
[155] EBA 2024d

5 Sääntelyn noudattaminen ja arviointi

5.1 Sääntelyn riittävyys kryptovarasektorilla

Kryptovarasektoria pidetään rahanpesun kannalta hyvin riskialttiina. Kryptovarojen pseudonyymiä tai anonyymiä luonnetta hyödyntämällä rikolliset voivat peittää henkilöllisyytensä. Lisäksi kryptovaroja voidaan siirtää nopeasti minne tahansa maailmaa ja siirtoja on mahdollista toteuttaa ilman keskitettyä palveluntarjoajaa. Sääntelemätön, hajautettu ja pseudonyymi kryptovarasektori on tehnyt siitä houkuttelevan vaihtoehdon rahanpesulle [156] . Kryptovarapalvelun tarjoajien sisällyttäminen rahanpesusääntelyn piiriin on ollut väistämätöntä.

MiCA-asetus, maksajan tiedot -asetus sekä rahanpesudirektiivit, jotka on täytäntöönpantu rahanpesulailla, ovat tällä hetkellä tärkeimmät säädökset rahanpesun torjunnan näkökulmasta. MiCA-asetuksessa määritellyt kryptovarapalvelun tarjoajat ovat muiden finanssilaitosten tavoin velvollisia noudattamaan rahanpesun estämisen velvoitteita, kuten riskiperusteista arviointia, asiakkaiden tunnistamis- ja tuntemisvelvollisuutta, liiketoimien seurantaa sekä selonotto- ja ilmoitusvelvollisuutta. Sääntelyn tavoitteena on saada mahdollisimman paljon tietoa, jotta julkiset avaimet on mahdollista yhdistää niiden taustalla oleviin henkilöihin[157] .

Kokonaisuudessaan kryptovarapalvelun tarjoajat ovat hyvin säänneltyjä rahanpesun estämisen näkökulmasta. AML-vaatimusten laajentaminen kryptovarapalvelun tarjoajiin pitäisi teoriassa vaikeuttaa kryptovarojen käyttöä rahanpesussa [158] . Kryptovarojen erityispiirteet tuovat kuitenkin käytännössä haasteita perinteisille AML-toimenpiteille. Kryptovarojen pseudonyymisyys ja hajautettu rakenne vaikeuttavat kryptovarasiirtojen tunnistamista ja jäljittämistä. Kryptovarojen kansainvälinen luonne johtaa laajaan ja

[156] Rahman ja muut, 2025, s. 5
[157] Wronka, 2022, s. 88
[158] Rahman ja muut, 2025, s. 5

monimutkaiseen transaktioympäristöön, mikä vaikeuttaa transaktioiden seurantaa entisestään. Tällaisia transaktioita perinteiset AML-teknologiat eivät pysty jäljittämään.[159] Tämän lisäksi kryptovarasektorilla on yleistynyt anonymiteettiä edistävät kryptovarat, sekoittajapalvelut sekä hajautetut alustat ja pörssit, jotka mahdollistavat varojen hämärtämisen[160].

Voidaan todeta, että vaikka AML-vaatimukset teoriassa vaikeuttavat kryptovarojen hyödyntämistä rahanpesussa, voivat kryptovarojen erityispiirteet aiheuttaa haasteita vaatimusten käytännön soveltamiselle sekä sääntelyn tehokkuudelle. Perinteiset rahanpesun havaitsemismenetelmät eivät ole kovin tehokkaita kryptovarasektorilla [161]. Tästä syystä onkin tarpeen tarkastella, miten sääntelyä noudatetaan käytännössä ja mitä haasteita kryptovarojen erityispiirteet tuovat sääntelyn toteuttamiselle.

5.2 Sääntelyn noudattaminen käytännössä

Sääntely asettaa kryptovarapalvelun tarjoajille laajat velvoitteet rahanpesun ehkäisemiseksi, mutta sääntelyn puutteellinen soveltaminen voi aiheuttaa merkittäviä riskejä. Kryptovarasektorilla on havaittu käytännön puutteita muun muassa riskiarvion laatimisessa ja soveltamisessa. Finanssivalvonta on havainnut, että osalla kryptovarapalvelun tarjoajista riskiarvio on pinnallista ja asiakkaiden riskiluokittelu perustuu vain yksittäisiin riskitekijöihin. Asiakkaalle määritetyissä riskiluokissa ei myöskään aina oteta huomioon riskiarviossa tunnistettuja riskejä. [162] Tämä voi johtua osittain siitä, että sääntely antaa melko laajat raamit riskiperusteiselle arvioinnille. Valvonta- ja sääntelyviranomaiset ovat antaneet tarkempia ohjeistuksia tekijöistä, joita riskiarviossa tulisi ottaa huomioon, mutta todellisuudessa riskitekijöiden arvioiminen jää lopulta kryptovarapalvelun tarjoajan vastuulle.

---

[159] Khan ja muut, 2025, s. 411
[160] FATF, 2019, s. 6
[161] Khan ja muut, 2025, s. 411
[162] Finanssivalvonta, 2024, s. 9

Jos riskiperusteinen arviointi jää puutteelliseksi, voivat myös muut rahanpesun estämisen toimenpiteet muodostua liian kevyiksi suhteessa riskeihin. Tämä on erittäin haasteellista erityisesti tilanteissa, joihin liittyy korkeampi rahanpesun riski, ja jolloin se edellyttäisi tehostettuja asiakkaan tuntemismenettelyjä. Tästä syystä kryptovarapalvelun tarjoajia tulisi auttaa tunnistamaan paremmin korkeariskisiä tilanteita esimerkiksi siten, että valvontaviranomainen ylläpitäisi julkista rekisteriä yhteisöistä, kryptovarapalveluista ja lompakon osoitteista, joihin liittyy suuri rahanpesun riski[163]. Kryptovarapalvelun tarjoajia voitaisiin kieltää toteuttamasta liiketoimia tällaisten tahojen kanssa[164].

Kryptovarapalvelun tarjoajien toiminnassa on havaittu, että asiakkaiden tuntemisvelvollisuuksia ei ole noudatettu yhdenmukaisesti johtuen puutteellisesta ohjeistuksesta. Puutteita on havaittu myös etätunnistamisratkaisuissa, asiakkaiden tuntemistietojen päivittämisessä ja tehostetussa tuntemismenettelyssä. Asiakkaiden liiketoimia myös seurataan liian kevyin menetelmin.[165]

Tällaiset puutteet AML-toiminnoissa voivat heikentää rahanpesun torjunnan onnistumista. Kryptovarapalvelun tarjoajien mahdollisuudet hahmottaa asiakkaidensa varojen alkuperä on jo lähtökohtaisesti heikommat verrattuna perinteisiin finanssisektorin toimijoihin[166]. Jos tämän lisäksi asiakkaiden tuntemis- ja seurantatoimenpiteet jäävät puutteellisiksi, voi epäilyttävät liiketoimet jäädä tunnistamatta. Tämä on osaltaan jo konkretisoitunut käytännössä, sillä on havaittu, että rahanpesun selvittelykeskukselle tehtävien ilmoitusten määrä on vähäistä kryptovarapalvelun tarjoajien keskuudessa[167].

Kokonaisuudessaan sääntelyn käytännön toteuttamisessa on vielä haasteita. Haasteet voivat johtua osittain siitä, että sääntelyn asettamia velvoitteita ei osata tulkita riittävän

[163] Euroopan parlamentti, 2022, s. 18
[164] Wronka, 2022, s. 90
[165] Finanssivalvonta, 2024, s. 9–10
[166] Isoaho & Kasi, 2021, s. 63
[167] Finanssivalvonta, 2024, s. 10

hyvin. Toisaalta osa haasteista on johtunut puutteellisesta ohjeistuksesta. Sääntelyn selkeys onkin kriittisessä roolissa kryptovarasektorilla, sillä ala on suhteellisen uusi, eikä vakiintuneita toimintatapoja ole vielä paljoa. Kryptovarasektorilla toimivat yritykset tarvitsevat selkeät ohjeet, miten asiakkaiden riskejä ja toimintaa arvioidaan ja millaista toimintaa tulee seurata ja pitää epäilyttävänä. [168]

5.3 Kryptovarojen erityispiirteet ja sääntelyn haasteet

Kryptovarojen pseudonyymistä, anonyymistä ja hajautetusta rakenteesta sekä reaaliaikaisista ja kansainvälisistä transaktioista aiheutuvia riskejä pyritään osittain hallitsemaan lainsäädännöllisin keinoin, kuten esimerkiksi tehostetun tuntemisvelvollisuuden avulla. Nämä erityispiirteet aiheuttavat myös haasteita sääntelyn soveltamiseen. AML-vaatimukset koskevat yhtenäisesti kaikkia varoja ja valuuttoja, mutta vaatimusten suora soveltaminen kryptovaluuttoihin voi olla hankalaa johtuen kryptovarojen erityispiirteistä[169].

5.3.1 Asiakkaan tuntemisen haasteet

Sääntely edellyttää kryptovarapalvelun tarjoajia tunnistamaan ja tuntemaan asiakkaansa, mikä on keskeinen keino hallita kryptovarojen pseudonyymistä tai anonyymistä luonteesta aiheutuvia riskejä. On kuitenkin havaittu, että sääntelyn kiristyminen voi lisätä sellaisia menetelmiä ja palveluita, joiden tarkoituksena on nimenomaisesti häivyttää kryptovarojen alkuperä. Tällaisia erittäin suuren rahanpesuriskin tuotteita ja palveluita ovat sekoittajapalvelut ja privaattikryptovaluutat.[170]

Sekoittajapalveluita hyödynnetään rikollisessa toiminnassa, koska ne etäännyttävät kryptovaran ja rikollisen henkilöllisyyden toisistaan ja näin ollen tekee varojen

[168] Khan ja muut 2025, s. 417–418
[169] Khan ja muut, 2025, s. 418
[170] HE 31/2024 vp, s. 78

jäljittämisestä vaikeaa[171]. Jos kryptovarapalvelun tarjoaja vastaanottaisi kryptovaroja sekoittajapalvelun kautta, on hyvin epäselvää, miten varojen alkuperää voitaisiin arvioida luotettavasti [172] . Sama pätee myös privaattikryptovaluuttoihin. Tällaiset kryptovarat tarjoavat korkean anonymiteetin piilottamalla tapahtumatiedot lohkoketjussa, mikä vaikeuttaa transaktioiden seurantaa huomattavasti [173] . Kun kryptovarapalvelun tarjoaja ei voi varmistua asiakkaan varojen alkuperästä tai liiketoimien tarkoituksesta, se heikentää mahdollisuuksia toteuttaa asiakkaan tuntemista koskevia velvoitteita ja siten haastaa AML-sääntelyn tavoitteiden toteutumista.

Sekoittajapalveluita ja privaattikryptovaluuttoja pidetään merkittävän riskillisinä, sillä niiden avulla yritetään häivyttää kryptovarojen alkuperä[174] . FATF:n mukaan valtioilla on harkintavaltaa kieltää tai rajoittaa tuotteita tai palveluita, joiden katsotaan aiheuttavan hyväksymättömän korkean rahanpesun riskin [175] . Nykyinen sääntely edellyttää kryptovarapalvelun tarjoajia huomioimaan tällaiset korkeamman riskin tuotteet ja palvelut riskiperusteisessa arvioinnissa, mutta se ei aseta nimenomaisia kieltoja tällaisille tuotteille ja palveluille.

Yhden näkemyksen mukaan sekoittajapalveluiden käyttö olisi sallittava ainoastaan tilanteissa, joissa voidaan osoittaa, että niiden käyttö on perusteltavissa esimerkiksi yksityisyyteen liittyvillä syillä. Tällöin kryptovarojen vastaanottajan tulisi osoittaa käytön laillinen tarkoitus. [176] Finanssivalvonta on myös selvittänyt sekoittajapalveluiden rajoittamisen mahdollisuutta ja havainnut, että niiden kieltäminen lainsäädännöllisin keinoin on haastavaa. Ala kehittyy jatkuvasti, joten lainsäädäntö saattaisi vanhentua jo pian valmistumisen jälkeen. Kieltäminen on myös tehotonta, sillä sekoittajapalvelut ovat anonyymeja ja ne toimivat myös EU/ETA-alueiden ulkopuolella. [177]

---

[171] Silva Ramalho & Igreja Matos, 2021, s. 503
[172] HE 31/2024 vp, s. 78
[173] Rahman ja muut, 2025, s. 11
[174] Valtiovarainministeriö, 2024, s. 81
[175] FATF, 2021, s. 40
[176] Euroopan parlamentti, 2022, s. 18
[177] Valtiovarainministeriö, 2024, s. 17

Privaattikryptovaluuttojen kohdalla on katsottu, että sääntely ei tuo merkittäviä hyötyjä ennen kuin privaattikryptojen kategoria kielletään[178].

Myös itsehallinnoidut lompakot aiheuttavat haasteita asiakkaiden tuntemiseen. Maksajan tiedot -asetus edellyttää kryptovarapalvelun tarjoajia keräämään ja välittämään tiedot kryptotransaktioiden osapuolista, myös silloin kun siirrot liittyvät isännöimättömiin osoitteisiin. Koska tällaisiin osoitteisiin ei liity kryptovarapalvelun tarjoajaa, tulee vaadittavat tiedot hankkia asiakkaalta. Tällaiset siirrot pysyvät kuitenkin edelleen riskillisinä rahanpesun näkökulmasta, sillä näissä tilanteissa asiakkaan ilmoittamia tietoja ei käytännössä pystytä verifioimaan mitenkään. Jos asiakas ilmoittaa siirtävänsä kryptovaroja henkilökohtaiseen lompakkoonsa, kryptovarapalvelun tarjoajien tulee käytännössä vain luottaa asiakkaan ilmoitukseen. [179] Jos asiakas antaisi väärää tietoa lompakon hallinnoijasta, pysyisivät tällaiset siirrot käytännössä edelleen anonyymeinä.

Itsehallinnoidun lompakon omistajuuden varmentamiseksi käytetään yleensä testisiirtoa. Testisiirto ei kuitenkaan anna täyttä varmuutta siitä, että asiakkaalla olisi määräysvalta varoihin. Testisiirto ei pysty varmentamaan sitä, ettei ulkopuolinen henkilö hallitse todellisuudessa lompakkoa tai ettei asiakas välittäisi testiä lompakon todelliselle omistajalle. [180] Näin ollen itsehallinnoidut lompakot vaikeuttavat maksajan tiedot -asetuksen tavoitteen toteutumista. Maksajan tiedot -asetuksen tavoitteena on estää anonyymit kryptovarojen siirrot, mutta käytännössä anonymiteetti ei poistu kokonaan itsehallinnoitujen lompakoiden kohdalla, sillä kryptovarapalvelun tarjoajan on lähes mahdotonta saada täysi varmuus lompakon omistajasta.

Voidaankin todeta, että nykyinen sääntely ei kykene täysin vastaamaan haasteisiin, joita kryptovarojen erityispiirteistä aiheutuu. Asiakkaiden tunteminen on keskeinen osa

[178] HE 31/2024 vp, s. 67
[179] HE 31/2024 vp, s. 66
[180] Renda & Caneppele, 2024, s. 374

rahanpesun torjuntaa, mutta osa kryptovarasektorilla toimivista tuotteista ja palveluista haastavat asiakkaiden tuntemisvelvoitteiden soveltamista. Sekoittajapalvelut, privaattikryptovaluutat ja itsehallinnoidut lompakot vaikeuttavat merkittävästi varojen alkuperän ja määränpään selvittämistä ja siten haastavat rahanpesun torjuntaa.

5.3.2 Liiketoimien seurannan haasteet ja teknologiset ratkaisut

Kryptovaroilla tehtävät liiketoimet voivat olla hyvin monimutkaisia, mikä asettaa haasteita liiketoimien seurannalle. Mahdollisuus nopeisiin ja rajat ylittäviin siirtoihin hämärtää varojen alkuperää ja määränpäätä sekä vaikeuttaa mahdollisuuksia tunnistaa epäilyttävää toimintaa ajoissa[181]. Kryptovarojen alkuperää voidaan pyrkiä peittelemään esimerkiksi tekemällä useita peräkkäisiä transaktioita. Käyttäjä saattaa luoda useita yksittäisiä kryptovaralompakoita ja siirtää kryptovaroja edestakaisin näiden lompakoiden välillä. Tämä vaikeuttaa huomattavasti alkuperäisten transaktioiden jäljittämistä.[182]

Kryptovarapalvelun tarjoajat tarvitsevat tehokkaita ja kehittyneitä järjestelmiä liiketoimien seurantaan, jotta sääntelyä pystytään soveltamaan käytännössä mahdollisimman tehokkaasti. Erilaiset automaattiset järjestelmät voivat käsitellä ja analysoida tietoja huomattavasti nopeammin ja tarkemmin kuin ihminen. Tämä mahdollistaa epäilyttävien liiketoimien nopeamman havaitsemisen, mikä on tärkeää kryptovarasektorilla, jossa siirrot ovat nopeita ja kansainvälisiä. [183]

Liiketoimien seurannassa tulisi hyödyntää erilaisia teknologiapohjaisia ratkaisuja, kuten lohkoketjuanalytiikkaa. Tällaisten kehittyneiden teknologioiden avulla voidaan tunnistaa tehokkaammin epäilyttäviä liiketoimia sekä paljastaa rahanpesulle tyypillisiä epäilyttäviä toimintamalleja. Lohkoketjuanalytiikka pystyy tarjoamaan helposti tietoa esimerkiksi varojen nopeasta siirtämisestä useisiin eri lompakon osoitteisiin sekä

[181] FATF, 2020, s. 3
[182] Wronka, 2022, s. 86
[183] Khan ja muut, 2025, s. 417

sekoittajapalvelujen käytöstä. Lisäksi yhteistyö teknologia-alan yritysten kanssa voi auttaa AML-toimenpiteiden tehokkuutta. Tällaiset yritykset voivat auttaa monimutkaisten liiketoimien seurannassa tarjoamalla kehittynyttä analytiikkaa sekä lohkoketjuteknologiaa. [184] Esimerkiksi tunnettu yhdysvaltalainen yritys Chainalysis tarjoaa työkaluja eri kryptovaluutoilla tehtyjen transaktioiden analysointiin epäilyttävien poikkeamien havaitsemiseksi[185].

Kryptotransaktioiden seuraamiseen ei kuitenkaan ole standardisoitua lähestymistapaa, mikä voi johtaa erilaisiin lähestymistapoihin eri teknologioiden käyttöönotossa. Osa kryptovarapalvelun tarjoajista saattaa käyttää yhtä lohkoketjuanalytiikan työkalua, kun taas toiset saattavat turvautua useampiin työkaluihin. Yhden palvelun tarjoajan käyttö voi nostaa riskiä siitä, että transaktioiden riskillisyys arvioidaan väärin ja kryptovarapalvelun tarjoaja hyväksyy varoja, joiden alkuperä on laiton.[186] Tästä syystä sääntelyviranomaisten olisi annettava kattavat ohjeet siitä, miten teknologisia työkaluja voidaan hyödyntää rahanpesun torjunnassa ja miten nämä integroidaan voimassa oleviin AML-järjestelmiin[187].

Kokonaisuudessaan kryptovarojen erityispiirteet luovat haasteita liiketoimien seurannalle, ja kryptovarapalvelun tarjoajilta tulisikin edellyttää erilaisten kehittyneiden teknologisten järjestelmien käyttöönottoa. Hälyttävät tapahtumat tulee kuitenkin käydä läpi asiantuntijan toimesta sen määrittämiseksi, ovatko ne todellisuudessa epäilyttäviä. Tämä edellyttää kryptovarapalvelun tarjoajan henkilöstöltä laajaa ymmärrystä kryptovarasektorista sekä erilaisista liiketoimintamalleista. [188] Kun kryptovarapalvelun tarjoaja sisällyttää AML-toimenpiteisiinsä sekä tehokkaat järjestelmät että osaavan henkilöstön, se pystyy varmistamaan rahanpesusääntelyn johdonmukaisen noudattamisen.

---

[184] Khan ja muut, 2025, s. 411, 416 ja 418
[185] Wronka, 2022, s. 92
[186] Renda & Caneppele, 2024, s. 375
[187] Khan ja muut, 2025, s. 418
[188] FATF, 2021, s. 81 ja 76

5.3.3 Sääntelyn ulkopuolelle jäävät kryptovarapalvelun tarjoajat

Kryptovarojen hajautettu rakenne muodostaa merkittävän haasteen rahanpesun torjunnalle. Hajautettu rakenne mahdollistaa kryptovarojen siirtämisen vertaisverkossa ilman, että kukaan valvoo transaktioita. Tämä mahdollistaa perinteisen rahoitusjärjestelmän ”portinvartijoiden” sekä niitä koskevien tiukkojen rahanpesun ehkäisemisen toimenpiteiden ohittamisen[189]. Vertaisverkossa toteutettaviin siirtoihin ei sovelleta rahanpesusääntelyn mukaista valvontaa, sillä velvoitteet asetetaan välittäjille, ei yksityishenkilöille[190]. Rikolliset pystyvät siis hyödyntämään vertaisverkkoa laittomien varojensa siirtämiseen. FATF:n havainnon mukaan laittomia varoja siirretäänkin vertaisverkossa enemmän verrattuna kryptovarapalvelun tarjoajien kanssa toteutettuihin siirtoihin[191].

Kryptovarasektorille on syntynyt palveluita, jotka toimivat hajautetusti. Hajautetut palvelut muodostavat sääntelyaukon, sillä rahanpesusääntely kohdistuu tällä hetkellä vain MiCA-asetuksessa määriteltyihin kryptovarapalvelun tarjoajiin. Asetus jättää hajautetut palvelut kryptovarapalvelun määritelmän ulkopuolelle. MiCA-asetuksen 2 artiklan 1 kohdan mukaan asetus tulee sovellettavaksi luonnollisiin henkilöihin ja oikeushenkilöihin, jotka tarjoavat kryptovaroihin liittyviä palveluita unionissa. Asetus edellyttää siis jonkin tunnistettavan tahon olemassaoloa. Yleisen käsityksen mukaan hajautettuja palveluita ei pidetä kryptovarapalvelun tarjoajina, sillä niillä ei ole tunnistettavaa tahoa, jolle voidaan asettaa vastuu niiden käytöstä[192].

Tunnistettavan tahon puuttuminen ja se, että hajautettuihin palveluihin osallistujat tekevät liiketoimia suoraan lohkoketjussa, herättää kysymyksen siitä, miten vaatimuksia on mahdollista noudattaa tällaisilla alustoilla[193]. Hajautettuihin palveluihin liittyykin merkittäviä rahanpesun riskejä, sillä niitä voidaan käyttää kiertämään

[189] Silva Ramalho & Igreja Matos, 2021, s. 496
[190] FATF, 2021, s. 18
[191] FATF, 2021, s. 18
[192] Euroopan komissio, 2022, s. 95
[193] Chen ja muut, 2023, s. 34

rahanpesusääntelyä [194] . Jos kenelläkään ei ole vastuuta noudattaa rahanpesulainsäädäntöä, ei asiakkaiden tuntemisen tai epäilyttävien liiketoimien valvomiseen ole myöskään velvollisuutta [195]. Tällöin kryptotransaktiot voivat pysyvä pseudonyymeinä ilman yhteyttä siirron tekijän todelliseen henkilöllisyyteen[196]. Tämä heikentää merkittävästi nykyisen rahanpesusääntelyn tehokkuutta. Vaikka keskitetyt kryptovarapalvelun tarjoajat ovat rahanpesusääntelyn soveltamisalassa, poistuu liiketoimien seuranta ja valvonta välittömästi, kun varat siirretään hajautettuihin palveluihin.

Hajautettuihin palveluihin osallistuminen edellyttää ainoastaan yhteyden kryptovaralompakkoon[197]. Merkittävänä riskinä nähdäänkin itsehallinnoidut lompakot, joissa kryptovarat ovat palvelun tarjoajan sijasta käyttäjän omassa hallinnassa ja näin ollen rahanpesusääntelyn ulkopuolella [198]. Itsehallinnoidut lompakot eivät myöskään kuulu MiCA-asetuksen määritelmän mukaisiin kryptovarapalvelun tarjoajiin, koska asetus koskee vain sellaisia lompakkopalveluita, jotka säilyttävät yksityisiä avaimia asiakkaiden puolesta.

Koska itsehallinnoidut lompakot eivät ole rahanpesusääntelyn piirissä, eivät ne yleensä noudata rahanpesun estämisen velvoitteita. Tällaiseen lompakkoon rekisteröityminen ei usein vaadi edes tunnistautumista eikä sähköpostivahvistusta tai muita yhteystietoja[199]. Näin ollen käyttäjät voivat pysyä täysin anonyymeinä ilman yhteyttä todelliseen henkilöllisyyteen. Varojen alkuperää ei myöskään valvota. [200] Tämä asettaa haasteita transaktioiden jäljittämiseen. Erityisesti tilanteissa, joissa käytetään useaa eri lohkoketjua, sekoittajapalveluita tai avataan useita uusia lompakoita jokaiselle transaktiolle, on hyvin vaikeaa todistaa, kuka transaktiot on suorittanut.[201] Tästä syystä

[194] Euroopan komissio, 2022, s. 95
[195] Valtiovarainministeriö, 2024, s. 78
[196] OECD, 2022, s. 17
[197] OECD, 2022, s. 11
[198] Valtiovarainministeriö, 2024, s. 82
[199] Benson ja muut, 2024, s. 85
[200] OECD, 2022, s. 11
[201] Benson ja muut, 2024, s. 85

tällaisten lompakoiden käyttöä voidaankin osittain verrata käteisen käyttöön ja siihen liittyviin riskeihin, mutta täysin digitaalisessa muodossa[202].

Toisaalta asiaa on hyvä tarkastella myös toisesta näkökulmasta. Vaikka käyttäjät voivat pysyä anonyymeinä hajautetuissa palveluissa, ongelmana on se, miten kryptovaluuttoja alun perin hankitaan. Hajautetut kryptopörssit mahdollistavat yleensä vain kryptovarojen väliset transaktiot. Näin ollen jos käyttäjät haluavat hankkia kryptovaluuttoja fiat-valuutoilla, joutuvat he yleensä käyttämään rahanpesusääntelyn soveltamisalassa olevia palveluita, kuten keskitettyjä pörssejä.[203] Näin ollen rikolliset voivat paljastua siinä vaiheessa, kun he yrittävät siirtää kryptovaroja säänneltyjen kryptovarapalvelun tarjoajien kautta[204].

Kokonaisuudessaan hajautettujen palveluiden ja itsehallinnoitujen lompakoiden asema sääntelyn ulkopuolella muodostaa merkittävän haasteen rahanpesun torjunnalle. Tällaiset palvelut eivät ole velvollisia noudattamaan rahanpesun estämisen velvoitteita, kuten asiakkaiden tunnistamista tai liiketoimien seurantaa. Rikolliset voivat käyttää tätä sääntelyaukkoa hyödyksi ja toteuttaa anonyymejä siirtoja sääntelemättömien palveluntarjoajien kautta. Riski kasvaa entisestään, sillä on arvioitu, että keskitettyjen kryptovarapalveluiden sääntelyn kiristyessä, toiminta siirtyy yhä enemmän erilaisiin hajautettuihin palveluihin[205].

5.3.4 Sääntelyn kansainväliset haasteet

Kryptovarojen globaali luonne tekee kansainvälisestä yhteistyöstä välttämätöntä. Kryptovaroja voidaan siirtää minne tahansa maailmaan, ja jos jokaisella lainkäyttöalueella on omat standardit sääntelyssä, valvonnassa ja täytäntöönpanoissa, syntyy rikollisille uusia mahdollisuuksia. [206] FATF on havainnut, että useilla

[202] Valtiovarainministeriö, 2024, s. 82
[203] Chen ja muut, 2023, s. 9 ja 34
[204] Benson ja muut, 2024, s. 87
[205] HE 31/2024 vp, s. 78
[206] Khan ja muut, 2025, s. 410–411

lainkäyttöalueilla on edelleen haasteita arvioida kryptovaroihin ja kryptovarapalvelun tarjoajiin liittyviä riskejä ja toteuttaa asianmukaisia lieventämistoimenpiteitä. Jos yhdellä lainkäyttöalueella on puutteita kryptovarapalvelun tarjoajia koskevassa sääntelyssä, voi sillä olla vakavia globaaleja seurauksia. [207]

Kansainvälisten standardien puute kryptovarasektorilla on nähty yhtenä merkittävänä rahanpesun riskiä nostavana tekijänä. Yhtenäisen sääntelyn puute aiheuttaa menetelmien ja käytäntöjen vaihtelevuutta eri maiden välillä. [208] Vaikka kansainväliset toimijat, kuten FATF, ovat antaneet yleisiä ohjeistuksia rahanpesun torjunnasta, on kansallisissa lähestymistavoissa merkittäviä eroja [209]. Tämä osoittaa sen, että vaikka kryptovarapalvelun tarjoajat tarvitsevat käytännönläheistä ohjeistusta sääntelyn soveltamiselle, se ei yksinään riitä globaalilla kryptovarasektorilla. Kryptovarojen rajat ylittävä luonne edellyttää myös kansainvälistä yhteistyötä ja kansainvälisesti yhdenmukaisempaa sääntelyä.

FATF:n arvion mukaan muun muassa matkustussäännön täytäntöönpano on ollut epäyhtenäistä. Alkuun täytäntöönpanon puutteet johtuivat osittain teknisistä rajoitteista sekä sääntely- ja valvontakapasiteetin puutteista. Viime vuosina on kuitenkin kehitetty matkustussäännön noudattamista tukevia työkaluja, mikä on osittain edistänyt säännön täytäntöönpanoa. Tästä huolimatta täytäntöönpanoon ja valvontaan tarvitaan lisäedistystä, jotta säännön tavoitteet saavutetaan. Esimerkiksi monet valtiot sallivat kryptovarapalvelun tarjoajien toteuttaa siirtoja itsehallinnoituihin lompakoihin ilman, että vastapuolesta kerättäisiin tietoja. [210] Tämä aiheuttaa vakavia huolenaiheita, sillä matkustussäännön tehokkuus riippuu johdonmukaisesta, tehokkaasta ja maailmanlaajuisesta täytäntöönpanosta[211].

[207] FATF, 2025a, s. 2 ja 25
[208] Valtiovarainministeriö, 2024, s. 82
[209] Khan ja muut, 2025, s. 413
[210] FATF, 2025b, s. 2
[211] FATF, 2025a, s. 18

Kansainvälisen sääntelyn erot aiheuttavat myös muita haasteita. On havaittu, että EU-tasoisen sääntelyn lisääntyessä kryptovaratoimijat ja asiakkaat siirtyvät Euroopan ulkopuolelle maihin, joissa rahanpesulainsäädäntö on löyhempää sekä rahanpesun valvonta heikompaa [212] . Tämä voi johtaa sääntelyarbitraasiin, jossa yritykset ja yksityishenkilöt siirtävät aktiivisesti toimintaansa kevyemmin säänneltyihin lainkäyttöalueisiin välttääkseen tiukempia velvoitteita[213]. Vaarana on, että markkinoiden jakaantuminen syvenee sekä muodostuu niin sanottuja ”kryptovaraparatiiseja”[214]. Tästä syystä kansainvälisen yhteistyön tehokas toteuttaminen on tärkeää. Kansainvälisen yhteistyön avulla voidaan estää sääntelyarbitraasia sekä rajoittaa sitä, että yhden lainkäyttöalueen kryptovarapalvelun tarjoajat saisivat kilpailuetua tiukemmin säänneltyihin lainkäyttöalueisiin nähden. [215]

Kokonaisuudessaan kryptovarasektori tarvitsee yksityiskohtaisen ohjeistuksen lisäksi kansainvälisesti yhtenäistä sääntelyä. Kryptovarojen kansainvälisen luonteen vuoksi sääntelyn tehokas toteuttaminen tulee tarvitsemaan rajat ylittävää yhteistyötä [216] . Kryptovarasektorin sääntelyn harmonisointi on tärkeää, jotta yritykset saavat tasavertaiset toimintaedellytykset sekä samalla pystyttäisiin minimoimaan sääntelyarbitraasin vaikutukset.[217]

5.4 Uusi AML-paketti

Rahanpesusääntelyä yhdenmukaistetaan EU-alueella uudella AML-paketilla, jonka Euroopan unionin neuvosto hyväksyi toukokuussa 2024. Pakettiin sisältyvät asetus uuden EU:n rahanpesutorjuntaviranomaisen perustamisesta, asetus yksityiseen sektoriin sovellettavista rahanpesunvastaisista velvoitteista, direktiivi rahanpesuvastaisista mekanismeista kansallisella tasolla sekä vuonna 2023 hyväksytyn

[212] Valtiovarainministeriö, 2024, s. 82
[213] Rahman ja muut, 2025, s. 10
[214] HE 31/2024 vp, s. 78
[215] FATF, 2021, s. 69
[216] Rahman ja muut, 2025, s. 12
[217] Khan ja muut, 2025, s. 415

varainsiirtoja koskevan asetuksen tarkistus. Uusi rahanpesuasetus yhdenmukaistaa ja selventää sääntöjä EU:ssa sekä estää rikollisia hyödyntämästä sääntelyn porsaanreikiä. Uuden sääntelyn tarkoituksena on myös varmistaa, että sääntöjä sovelletaan johdonmukaisemmin sekä niiden noudattamista valvotaan paremmin. Rahanpesuasetus yhdessä uuden rahanpesudirektiivin kanssa korvaavat viidennen rahanpesudirektiivin. [218]

Aiemmin rahanpesun estämistä koskeva sääntely EU-tasolla on sisältynyt pääosin rahanpesudirektiiveihin, mikä on jättänyt jäsenvaltioille paljon tulkinnanvaraa. Uuden rahanpesupaketin myötä lähes kaikki yksityistä sektoria koskevat velvoitteet, kuten asiakkaiden tuntemista koskevat velvoitteet, on siirretty rahanpesuasetukseen, joka on suoraan sellaisenaan sovellettavaa oikeutta. [219] Tämä on positiivinen askel kohti yhtenäisempää sääntelyä EU:ssa.

Rahanpesuasetuksen (2024/1624) 2 johdantokappaleessa tunnistetaan neljännen rahanpesudirektiivin haasteeksi kansallisten linjausten hajanaisuus sekä se, etteivät direktiivissä vahvistetut säännöt ole suoraan sovellettavissa. Tämä on johtanut siihen, ettei sääntöjä ole täytäntöönpantu yhdenmukaisesti yhdentyneiden sisämarkkinoiden vaatimusten kanssa. Rahanpesuasetus tuleekin vastaamaan tähän haasteeseen yhdenmukaistamalla rahanpesun torjuntaan liittyvää sääntelyä. Asetuksen 52 johdantokappaleessa korostetaan muun muassa tarvetta yhdenmukaistaa asiakkaiden tuntemisvelvollisuutta.

Rahanpesupaketin säännökset tulivat voimaan heinäkuussa 2024, ja niiden soveltaminen alkaa pääasiassa 10.7.2027. EU:n uusi rahanpesuasetus on suoraan sovellettavaa oikeutta ja velvoittaa sellaisenaan suomalaisia toimijoita. Tästä huolimatta Suomessa tulee päivittää kansallista rahanpesusääntelyä yhdenmukaiseksi EU-sääntelyn

[218] Euroopan unionin neuvosto, 2026
[219] Lexia, 2024

kanssa. Suomessa on jo aloitettu kansallinen implementointihanke, jolla täytäntöön pannaan EU-säädökset vuoteen 2027 mennessä. [220]

5.4.1 Soveltamisala

Rahanpesuasetus sääntelee aiempien rahanpesudirektiivien tavoin riskiperusteisesta arvioinnista, asiakkaiden tunnistamis- ja tuntemisvelvollisuudesta, tehostetusta tuntemisvelvollisuudesta, jatkuvasta seurannasta sekä ilmoitusvelvollisuudesta. Sääntely on kuitenkin täsmällisempää ja yksityiskohtaisempaa monella osa-alueella. Rahanpesuasetuksen 65 johdantokappaleessa todetaan, että erityisesti asiakkaiden tuntemisesta tulee antaa yksityiskohtaisempia ja täsmällisempiä sääntöjä.

Rahanpesuasetuksen soveltamisalaan kuuluvat MiCA-asetuksessa määritetyt kryptovarapalvelun tarjoajat. Rahanpesuasetuksen 14 johdantokappaleessa korostetaan, että MiCA-asetuksen mukaisten kryptovarapalvelun tarjoajien tulee kuulua myös tämän asetuksen soveltamisalaan, jotta kryptovarojen käyttöä rahanpesussa saadaan lievennettyä. Rahanpesuasetuksen 7 johdantokappaleessa todetaan, että kryptovarapalvelun tarjoajat ovat alttiita kanavia laittomien varojen siirtämiseen, joten niillä on hyvät mahdollisuudet havaita tällaisia siirtoja ja lieventää riskejä. Maksajan tiedot -asetuksen tavoin rahanpesuasetuksessa on säilytetty teknologianeutraliteetti ja asetuksen 2 artiklan 6 kohdassa kryptovarapalvelun tarjoajat on sisällytetty osaksi finanssilaitoksia.

5.4.2 Uutta sääntelyä

Sen lisäksi, että rahanpesuasetus yhdenmukaistaa rahanpesun estämisen toimenpiteitä, se sisältää myös uutta sääntelyä. Kryptovarojen aiheuttamien riskien kannalta yksi keskeisimmistä rahanpesuasetuksessa säädetyistä vaatimuksista on anonyymien tuotteiden ja palveluiden kieltäminen. Aiempi rahanpesusääntely ei ole asettanut

[220] Lexia, 2024

rajoituksia esimerkiksi privaattikryptovaluuttojen käytölle, mikä on nähty isona haasteena. Uusi rahanpesuasetus muuttaa tämän.

Rahanpesuasetuksen 160 johdantokappaleen mukaan kryptovaroihin liittyvä nimettömyys altistaa ne väärinkäytölle rikollisiin tarkoituksiin. Johdantokappale korostaa, että kryptovarojen siirtoa ei pystytä jäljittämään kryptovaratileillä tai muilla anonyymeillä rahoitusvälineillä, mikä tekee epäilyttävien liiketoimien tunnistamisesta sekä asiakkaiden tuntemisvelvollisuutta koskevien toimenpiteiden soveltamisesta hankalaa. Rahanpesuasetuksen 79 artiklan 1 kohdan mukaan kryptovarapalvelun tarjoaja ei saa pitää anonyymejä kryptovaratilejä, joissa tilinhaltija voi pysytellä anonyyminä tai joissa liiketoimia voidaan anonymisoida tai hämärtää anonymiteettiä edistävillä kryptovaroilla. Rahanpesuasetuksen 2 artiklan 1 kohdan 25 alakohdan mukaan anonymiteettiä edistävät kryptovarat tarkoittavat sellaisia kryptovaroja, joiden sisäänrakennetut ominaisuudet on suunniteltu tekemään kryptovarojen siirtoa koskevista tiedoista anonyymejä.

Anonymiteettiä lisäävien kryptovarojen kielto on askel kohti turvallisempaa kryptovaraympäristöä, mutta se ei välttämättä ole täysin tehokas toimenpide. Koska sääntely ei ole määritellyt tarkasti, mitä anonymiteettiä lisäävät tekniset ominaisuudet tarkoittavat, voi tämä johtaa sääntelyn tulkintaeroihin.[221] Tämä korostaakin edelleen sääntelyn selkeyden ja täsmällisyyden merkitystä kryptovarasektorilla. Sääntelyn kiristyminen saattaa myös lisätä laittomasti toimivia kryptovaratoimijoita, jotka hyödyntävät tilannetta ja korostavat anonymiteetin tarjoamia etuja. Lisäksi hajautetut palvelut tulevat todennäköisesti edelleen pysymään rikollisten suosiossa rahanpesuasetuksen ja anonyymien kryptovarojen kieltämisen jälkeen.[222] Kokonaisuudessaan rahanpesuasetus vahvistaa rahanpesun torjuntaa kryptovarasektorilla, mutta sen vaikutukset voivat jäädä rajallisiksi, sillä hajautetut

[221] Roussos, 2026, s. 22
[222] Roussos, 2026, s. 22–23

palvelut ja EU-alueen ulkopuoliset toimijat mahdollistavat edelleen EU-sääntelyn kiertämisen.

6 Johtopäätökset

Tutkielman tavoitteena oli selvittää, kuinka kryptovaroja hyödynnetään rahanpesussa ja miten kryptovarapalvelun tarjoajia säännellään rahanpesun estämiseen liittyen. Tutkielman tavoitteena oli myös arvioida, onko nykyinen sääntely tällä hetkellä riittävällä tasolla ottaen huomioon kryptovarojen aiheuttamat riskit.

Kryptovarasektoriin kohdistuvaa rahanpesuriskiä on pidetty kansallisissa ja ylikansallisessa riskiarvioissa vähintään merkittävänä. Kryptovaroilla on monia perinteisistä valuutoista poikkeavia ominaisuuksia, joita rikolliset pystyvät hyödyntämään varojen alkuperän häivyttämisessä. Keskeisimmät ominaisuudet liittyvät kryptovarojen pseudonyymisyyteen tai anonyymisyyteen, reaaliaikaisiin ja kansainvälisiin transaktioihin sekä hajautettuun rakenteeseen.

Kryptovarasektoria säännellään keskitettyjen kryptovarapalvelun tarjoajien kautta. MiCA-asetuksessa määritetyt kryptovarapalvelun tarjoajat kuuluvat rahanpesusääntelyn soveltamisalaan, ja niillä on muiden finanssilaitosten tavoin velvollisuus toteuttaa rahanpesun estämisen toimenpiteitä, kuten riskiperusteista arviointia, asiakkaiden tuntemista, tehostettua tuntemisvelvollisuutta, liiketoimien seurantaa sekä selonotto- ja ilmoitusvelvollisuutta. Rahanpesusääntelyä täydentävät maksajan tiedot -asetus, joka estää anonyymit siirrot kryptovarapalvelun tarjoajien alustoilla sekä MiCA-asetus, joka edellyttää kryptovarapalvelun tarjoajilta toimilupaa.

Rahanpesun estämistä koskevat velvoitteet vaikeuttavat teoriassa kryptovarojen käyttöä rahanpesussa, mutta kryptovarojen erityispiirteet tuovat haasteita velvoitteiden käytännön soveltamiselle. Kryptovarasektori on myös suhteellisen uusi, joten vakiintuneita käytäntöjä ei vielä kaikilta osin ole. Tämä on johtanut osittain sääntelyn puutteelliseen soveltamiseen. Kryptovarapalvelun tarjoajat tarvitsevatkin selkeät ohjeet sääntelyn tulkintaan ja käytännön soveltamiseen.

Privaattikryptovaluutat, sekoittajapalvelut sekä itsehallinnoidut lompakot vaikeuttavat asiakkaiden tuntemista ja varojen jäljittämistä. Riskeistä huolimatta nykyinen sääntely ei kiellä näitä palveluita, vaan edellyttää ainoastaan tehostettuja tuntemistoimia, mikä ei täysin pysty poistamaan niihin liittyviä riskejä. Sekoittajapalveluiden kohdalla on havaittu, että niiden kieltäminen on hankalaa johtuen teknologian jatkuvasta kehityksestä sekä siitä, että palvelut todennäköisesti siirtyisivät EU/ETA-alueen ulkopuolelle. EU:n uusi rahanpesuasetus tulee puolestaan kieltämään anonyymit kryptovarat. Tämä on positiivinen sääntelykehitys ja tulee osittain ratkaisemaan privaattikryptovaluuttoihin liittyvät ongelmat.

Liiketoimien seurannan avulla kryptovarapalvelun tarjoajat seuraavat asiakkaidensa tosiasiallista toimintaa, mikä mahdollistaa epäilyttävien liiketoimien havaitsemisen. Kryptovaroilla tehtävät liiketoimet ovat kuitenkin usein monimutkaisia ja rajat ylittäviä, mikä aiheuttaa haasteita perinteiselle liiketoimien seurannalle. Tästä syystä kryptovarapalvelun tarjoajien tulee hyödyntää liiketoimien seurannassa kehittyneitä teknologisia ratkaisuja, kuten lohkoketjuanalytiikkaa. Kehittyneet seurantatyökalut yhdistettynä osaavaan henkilökuntaan, tekee liiketoimien seurannasta ja epäilyttävien liiketoimien havaitsemisesta mahdollisimman tehokasta.

Tutkielmassa havaittiin, että kryptovarasektorin yksi keskeisimmistä haasteista on kryptovarojen hajautettu rakenne, joka mahdollistaa kryptovarojen hallinnoimisen ja siirtämisen vertaisverkossa ilman keskitettyä tahoa. Tällaiset kryptovarasiirrot pysyvät sääntelyn ulkopuolella, mikä tekee niistä houkuttelevan vaihtoehdon rikollisille. Kryptovarasektorille on syntynyt myös hajautettuja palveluita, jotka toimivat sääntelyn ulkopuolella eivätkä ne edellytä asiakkailtaan esimerkiksi tunnistautumista. Tämä asettaa merkittäviä haasteita rahanpesun torjunnalle, sillä laittomia varojen siirtoja voidaan edelleen toteuttaa tällaisten palveluiden kautta.

Tutkielmassa havaittiin myös, että kryptovarojen kansainvälinen luonne korostaa yhtenäisen kansainvälisen sääntelyn tarvetta. Eri maiden väliset erot sääntelyn

toimeenpanossa ja käytännöissä luovat mahdollisuuksia rikollisille. EU on yhtenäistänyt sääntelyä uudella AML-paketilla, mutta globaalisti epäyhtenäinen sääntely voi ajan myötä johtaa sääntelyarbitraasiin, jossa toimijat siirtyvät kevyemmin säänneltyihin maihin. Tämä korostaa kansainvälisesti yhdenmukaisen sääntelyn merkitystä.

Kokonaisuutena voidaan todeta, että kryptovarojen sisällyttäminen rahanpesun estämistä koskevaan sääntelyyn on ollut välttämätön askel riskien hallitsemiseksi. Sääntely kaventaa rikollisten mahdollisuuksia toimia erityisesti keskitettyjen kryptovarapalvelun tarjoajien kautta. Kryptovarojen erityispiirteet luovat kuitenkin edelleen haasteita sääntelyn käytännön toteutumiselle. Lisäksi kryptovarojen hajautettu rakenne sekä anonymiteettiä edistävät tuotteet ja palvelut jättävät sääntelyyn aukkoja, joita tulisi tarkastella uudelleen. Kokonaisuudessaan kryptovarasektori tarvitsee selkeää sääntelyä, kehittyneitä teknologisia ratkaisuja sekä kansainvälistä yhteistyötä.

Lähteet

AMLA. (2025, 15. heinäkuuta). *AMLA expects high standards against financial crime in crypto sector.* Noudettu 9.4.2026 osoitteesta https://www.amla.europa.eu/news-media/news-articles/amla-expects-high-standards-against-financial-crime-crypto-sector_en

Benson, V., Turksen, U. & Adamyk, B. (2024). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of financial regulation and compliance, 32(1)*, 80-97. http://dx.doi.org/10.1108/JFRC-04-2023-0065

Chainalysis. (2025, 15. tammikuuta). *2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized.* Noudettu 1.2.2026 osoitteesta https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/

Chen, Y., Gurrola-Pérez, P. & Lin, K. (2023, 29. elokuuta). *A review of crypto-trading infrastructure: Exchanges' engagement with crypto market functioning & development.* DigitalOcean. Noudettu 15.3.2026 osoitteesta https://wfe-live.lon1.cdn.digitaloceanspaces.com/org_focus/storage/media/Crypto%20Infrastructure%20Review.pdf

Dupuis, D. & Gleason, K. (2021). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime, 28(1),* 60-74. http://dx.doi.org/10.1108/JFC-06-2020-0113

EBA. (2024a). *Preventing money laundering and terrorism financing in the EU's cryptoassets sector.* Noudettu 14.12.2025 osoitteesta https://www.eba.europa.eu/sites/default/files/2024-12/25bb6d67-4bd1-4e54-805c-269d9657e7fb/Preventing%20ML%20TF%20in%20the%20EU%27s%20crypto%20assets%20sector.pdf

EBA. (2024b). *The EBA issues 'travel rule' guidance to tackle money laundering and terrorist financing in transfers of funds and crypto assets.* Noudettu 16.12.2025 osoitteesta https://www.eba.europa.eu/publications-and-media/press-

releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

EBA. (2024c). *Ohjeet, joilla muutetaan ohjeita EBA/GL/2021/02 direktiivin (EU) 2015/849 17 artiklan ja 18 artiklan 4 kohdan nojalla asiakkaan tuntemisvelvollisuudesta sekä tekijöistä, joita luotto- ja finanssilaitosten olisi tarkasteltava arvioidessaan yksittäisiin liikesuhteisiin ja yksittäisiin liiketoimiin liittyvää rahanpesun ja terrorismin rahoituksen riskiä (jäljempänä 'rahanpesun ja terrorismin rahoituksen riskitekijöitä koskevat ohjeet').* Noudettu 3.3.2026 osoitteesta https://www.eba.europa.eu/sites/default/files/2024-06/a3e89f4f-fbf3-4bd6-9e07-35f3243555b3/GL%20amending%20EBA%20GL%202021%2002%20%28EBA%20GL%202024%2001%29_FI_COR.pdf

EBA. (2024d). *Ohjeet tietovaatimuksista asetuksen (EU) 2023/1113 mukaisten varainsiirtojen ja tiettyjen kryptovarojen siirtojen yhteydessä (matkustussääntöjä koskevat ohjeet).* Noudettu 13.1.2026 osoitteesta https://www.eba.europa.eu/sites/default/files/2024-09/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines_Final%20Report%20%28EBA.GL_.2024.11%29_FI.pdf

Euroopan komissio. (2022, 27. lokakuuta). *Report from the Commission to the European Parliament and the council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities COM(2022) 554 final.* EUR-Lex. Noudettu 12.1.2026 osoitteesta https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN

Euroopan parlamentti. (2022, 6. huhtikuuta). *Mietintö ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi varainsiirtojen ja tiettyjen kryptovarojen siirtojen mukana toimitettavista tiedoista (uudelleenlaadittu) COM(2021).* Noudettu 12.1.2026 osoitteesta https://www.europarl.europa.eu/doceo/document/A-9-2022-0081_FI.pdf

Euroopan unionin neuvosto. (2026). *Rahanpesun ja terrorismin rahoituksen torjuminen EU:ssa*. Noudettu 9.4.2026 osoitteesta https://www.consilium.europa.eu/fi/policies/fight-against-terrorist-financing/

Euroopan unionin neuvosto. (2022a). *Rahanpesun torjunta: alustava yhteisymmärrys kryptovarojen siirtojen avoimuudesta.* Noudettu 1.12.2025 osoitteesta https://www.consilium.europa.eu/fi/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/

Euroopan unionin neuvosto. (2022b). *Digitaalinen rahoitus: yhteisymmärrys kryptovarojen markkinoita koskevasta asetuksesta (MiCA).* Noudettu 1.12.2025 osoitteesta https://www.consilium.europa.eu/fi/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

FATF. (2025a). *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*. Noudettu 28.4.2026 osoitteesta https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

FATF. (2025b). *Travel Rule Supervision*. Noudettu 20.2.2026 osoitteesta https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

FATF. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.* Noudettu 1.4.2026 osoitteesta https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf

FATF. (2020). *FATF report for Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing*. Noudettu 13.2.2026 osoitteesta https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf

FATF. (2019). *Guidance for a risk-based approach to virtual assets and virtual asset service providers.* Noudettu 1.2.2026 osoitteesta https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-VA-VASPs.pdf

Finanssivalvonta. (2025a). *Kryptovarat.* Noudettu 11.11.2025 osoitteesta https://www.finanssivalvonta.fi/kuluttajalle/kryptovarat/

Finanssivalvonta. (2025b). *Kryptovaratoimijat.* Noudettu 16.11.2025 osoitteesta https://www.finanssivalvonta.fi/finanssisektorin-toimijalle/paaomamarkkinat/kryptovaratoimijat/

Finanssivalvonta. (2024, 26. marraskuuta). *Virtuaalivaluutan tarjoajien rahanpesun ja terrorismin rahoittamisen riskiarvion yhteenveto.* Noudettu 15.2.2026 osoitteesta https://www.finanssivalvonta.fi/globalassets/fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2024/fi_vasp_julkaistava_riskiarvioyhteenveto_2024.pdf

Finanssivalvonta. (2023). *Määräykset ja ohjeet 2/2023. Rahanpesun ja terrorismin rahoittamisen estäminen.* Noudettu 3.2.2026 osoitteesta https://www.finanssivalvonta.fi/globalassets/fi/pankki/rahanpesun-ja-terrorismin-estaminen/saannokset-ja-poikkeusluvan-hakeminen-maaraykset-ja-ohjeet/02_2023.m2.pdf

Finanssivalvonta. (2021). *Selonotto- ja ilmoitusvelvollisuus.* Noudettu 8.4.2026 osoitteesta https://www.finanssivalvonta.fi/finanssisektorin-toimijalle/pankki/rahanpesun-estaminen/selonotto--ja-ilmoitusvelvollisuus/

Finanssivalvonta. (n.d.). *Valvottavaluettelo.* Noudettu 16.2.2026 osoitteesta https://www.finanssivalvonta.fi/rekisterit/valvottavaluettelo/

Haffke, L., Fromberger, M. & Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. *Journal of Banking Regulation, 21(2),* 125-138. https://doi.org/10.1057/s41261-019-00101-4

HE 31/2024 vp. *Hallituksen esitys eduskunnalle laiksi kryptovarapalvelun tarjoajista ja kryptovaramarkkinoista sekä eräiksi muiksi laeiksi.* Noudettu 8.4.2026 osoitteesta https://www2.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_31+2024.pdf

HE 261/2020 vp. *Hallituksen esitys eduskunnalle laeiksi rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain, rahanpesun selvittelykeskuksesta annetun lain sekä pankki- ja maksutilien valvontajärjestelmästä annetun lain 6 §:n muuttamisesta.* Noudettu 14.1.2026 osoitteesta https://www2.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_261+2020.pdf

HE 167/2018 vp. *Hallituksen esitys eduskunnalle laiksi pankki- ja maksutilien valvontajärjestelmästä ja eräiksi siihen liittyviksi laeiksi*. Noudettu 7.2.2026 osoitteesta https://www2.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_167+2018.pdf

HE 228/2016 vp. *Hallituksen esitys eduskunnalle laiksi rahanpesun ja terrorismin rahoittamisen estämisestä, laiksi rahanpesun selvittelykeskuksesta sekä eräiksi niihin liittyviksi laeiksi.* Noudettu 14.3.2026 osoitteesta https://www2.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_228+2016.pdf

Hirvonen, A. (2011). *Mitkä metodit? Opas oikeustieteen metodologiaan*. Yleisen oikeustieteen julkaisuja 17. Noudettu 13.11.2025 osoitteesta https://helda.helsinki.fi/server/api/core/bitstreams/20149471-38b2-4cc8-94b7-2f6b3feed81d/content

Huovila, M. (n.d.). *Oikeuslähdeoppi ja oikeudellinen argumentaatio rikostuomion perusteluissa.* Tuomioistuinlaitos. Noudettu 15.12.2025 osoitteesta https://tuomioistuimet.fi/hovioikeudet/helsinginhovioikeus/material/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/painetutjulkaisut/rikostuomionperusteleminen2005lisapainos2006./OS0uyDOHv/04_Oikeuslahdeoppi_ja_oikeudellinen_argumentaatio..._Mika_Huovila.pdf

Hyttinen, T. (2021). *Rahanpesu ja rikosvastuu.* Alma Talent Oy. Noudettu 11.10.2025 osoitteesta https://verkkokirjahylly-almainsights-fi.proxy.uwasa.fi/teos/BAXBBXATGBBEE#kohta:I((20)Johdanto/piste:t2Iw

Investopedia. (2025). *Understanding Peer-to-Peer Virtual Currency and Its Benefits*. Noudettu 14.3.2026 osoitteesta https://www.investopedia.com/terms/p/ptop.asp

Isoaho, E. & Kaski, I.-E. (2021). *Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021.* Valtiovarainministeriö. Noudettu 15.11.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/5688b9b9-5b3d-4f3a-8c97-32fd7b9b7414/content

Isto, M. (2023, 27. tammikuuta). *Mitä kryptovaluutoilla voi tehdä?* Northcrypto. Noudettu 15.2.2026 osoitteesta https://www.northcrypto.com/learn/blog/mita-kryptovaluutoilla-voi-tehda

Johansson, P.-E., Eerola, M., Innanen, A. & Viitala, J. (2019). *Lohkoketju.* Alma Talent Oy. Noudettu 14.11.2025 osoitteesta https://bisneskirjasto-almainsights-fi.proxy.uwasa.fi/teos/IABBGXDTEB#/kohta:((20)Lohkoketju/piste:t1R

Keskusrikospoliisi. (2026, 29. tammikuuta). *Rahanpesun selvittelykeskuksen vuosikertomus 2025.* Noudettu 16.3.2026 osoitteesta https://poliisi.fi/documents/25235045/67733116/2025-rahanpesun-selvittelykeskuksen-vuosikertomus.pdf/48df3380-929a-97df-5a68-f3f378a838b2/2025-rahanpesun-selvittelykeskuksen-vuosikertomus.pdf?t=1770983705780

Khan, A., Jillani, M., Ullah, M. & Khan, M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control, 28(2)*, 408-423. http://dx.doi.org/10.1108/JMLC-07-2024-0113

Kraken. (2025, 25. kesäkuuta). *Kraken cements European leadership with MiCA license from Central Bank of Ireland.* Noudettu 2.2.2026 osoitteesta https://blog.kraken.com/news/mica-license-central-bank-of-ireland

Lexia. (2024, 31. lokakuuta). *EU:n uusi rahanpesupaketti tuo merkittäviä muutoksia.* Noudettu 14.12.2025 osoitteesta https://www.lexia.fi/fi/eun-uusi-rahanpesupaketti-tuo-merkittavia-muutoksia/

OECD. (2022). *Why Decentralised Finance (DeFi) Matters and the Policy Implications.* Noudettu 21.1.2026 osoitteesta

https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/01/why-decentralised-finance-defi-matters-and-the-policy-implications_5f54eead/109084ae-en.pdf

Rahanpesun selvittelykeskus. (2025, 17. helmikuuta). *Rahanpesurikokset oikeuskäytännössä - Törkeä rahanpesu -tuomiot Suomen käräjä- ja hovioikeuksissa 6/2022-4/2024.* Poliisi. Noudettu 11.11.2025 osoitteesta https://poliisi.fi/documents/25235045/0/Tuomioanalyysi_2024%20(1).pdf/4dac4499-ecb8-7422-68d5-52e81b03e9ff/Tuomioanalyysi_2024%20(1).pdf?t=1755585035158

Rahman, J., Rahman, H., Islam, N., Tanchangya, T., Ridwan, M. & Ali, M. (2025). Regulatory landscape of blockchain assets: Analyzing the drivers of NFT and cryptocurrency regulation. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 5(1),* 100214. https://doi.org/10.1016/j.tbench.2025.100214

Renda, A. & Caneppele, S. (2024). Compliant or not compliant? The challenges of anti-money laundering regulations in cryptoassets: the case of Switzerland*. Journal of Money Laundering Control, 27(2),* 363-382. http://dx.doi.org/10.1108/JMLC-04-2023-0078

Roussos, M. (2026). Anti-money laundering in the crypto-market: Will the MiCA Regulation effectively support the European AML/CFT objectives? *Law and Financial Markets Review.* 1-24. https://doi.org/10.1080/17521440.2026.2626875

Salo-Lahti, M. (2023). *Regulating Crypto-Assets: Investor Protection Strategies and the 5-I's Model.* Osuva. Noudettu 11.11.2025 osoitteesta https://osuva.uwasa.fi/server/api/core/bitstreams/330a7e89-cae5-4b88-8c8f-193c47fb4dd2/content

Sammalisto, S. & Asunmaa, A. (2021). *Viisas pääsee vähemmällä taloudessakin.* Helsingin seudun kauppakamari. Noudettu 17.12.2025 osoitteesta https://kauppakamaritieto-fi.proxy.uwasa.fi/ammattikirjasto/teos/viisas-paasee-vahemmalla-taloudessakin-

2021#kohta:Viisas((20)p((e4)((e4)see((20)v((e4)hem((ad)m((e4)ll((e4)((20)talou des((ad)sakin

See, K. (2024). The Satoshi laundromat: a review on the money laundering open door of Bitcoin mixers. *Journal of Financial Crime, 31(2),* 416-426. http://dx.doi.org/10.1108/JFC-11-2022-0269

Silva Ramalho, D. & Igreja Matos, N. (2021). What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. *ERA Forum, 22(3),* 487-506. https://doi.org/10.1007/s12027-021-00676-4

Soon, M. (2025, 24. tammikuuta). *Kryptovaluuttojen kehitys ja trendit vuonna 2025: Mitä sijoittajien tulisi tietää?* Northcrypto. Noudettu 14.1.2026 osoitteesta https://www.northcrypto.com/learn/blog/kryptovaluuttojen-kehitys-ja-trendit-vuonna-2025

Soon, M. (2021, 25. maaliskuuta). *Mikä on DeFi?* Northcrypto. Noudettu 14.1.2026 osoitteesta https://www.northcrypto.com/learn/blog/mika-on-defi

United Nations. (n.d.). *Money laundering through cryptocurrencies.* Noudettu 12.12.2025 osoitteesta https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html

Valtiovarainministeriö. (2024, 8. helmikuuta). *Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2023: Osittaispäivitys.* https://urn.fi/URN:ISBN:978-952-367-635-0

Valtiovarainministeriö. (2023, 20. joulukuuta). *EU tuo kryptovaroihin yhdenmukaisen sääntelyn.* Noudettu 10.1.2026 osoitteesta https://vm.fi/-/eu-tuo-kryptovaroihin-yhdenmukaisen-saantelyn

Verohallinto. (2025). *Kryptovarat vakiintuneet vaihdannan välineiksi.* Noudettu 13.11.2025 osoitteesta https://www.vero.fi/harmaa-talous-rikollisuus/ilmiöt/virtuaalivaluutat/

Wronka, C. (2022). Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control, 25(1),* 79-94. https://doi.org/10.1108/JMLC-02-2021-0017

Wuolijoki, S. (2022). *Pankkioikeus I.* Alma Talent Oy. Noudettu 9.10.2025 osoitteesta https://verkkokirjahylly-almainsights-fi.proxy.uwasa.fi/teos/DABBGXETEB#piste:t1/kohta:I((20)Pankkis((e4)((e4)ntelyn((20)perusteet

Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., Zhang, C., Xiao, X. & Xu, G. (2021). Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange. *Proceedings of the ACM on measurement and analysis of computing systems, 5(3),* 1-26. https://doi.org/10.1145/3491051