Tampereen yliopisto

Aino Pukaralammi

VIRTUAALIVALUUTTOJEN AIHEUTTAMAN RAHANPESURISKIN TUNNISTAMINEN JA HALLINTA PANKIN NÄKÖKULMASTA

Johtamisen ja talouden tiedekunta
Pro gradu -tutkielma
Huhtikuu 2022

TIIVISTELMÄ

Aino Pukaralammi: Virtuaalivaluuttojen aiheuttaman rahanpesuriskin tunnistaminen ja hallinta pankin näkökulmasta
Ohjaaja: Lasse Koskinen
Pro gradu -tutkielma
Tampereen yliopisto
Kauppatieteiden tutkinto-ohjelma, Vakuutustiede
Huhtikuu 2022

Lohkoketjuteknologian viime vuosikymmenen vaikuttavin sovellusmuoto finanssimaailmassa on ollut virtuaalivaluutat, jotka mahdollistavat nopeita, osittain anonyymejä sekä pankeista riippumattomia transaktioita. Virtuaalivaluuttojen suosion pohjalta on noussut esiin kahdenlaista näkökulmaa: virtuaalivaluutat edustavat maksujärjestelmien tulevaisuutta, mutta samalla ne myös luovat tehokkaan työkalun rikollisille siirtää ja varastoida varoja viranomaisten ja muiden valvovien tahojen ulottumattomiin. Perinteinen maksujärjestelmäyhteiskunta on rakennettu pankkien ympärille, jolloin myös pankit voivat olla osallisina rahanpesuketjussa. Virtuaalivaluuttoihin liittyvä rahanpesuriski onkin nostettu merkittävämmäksi uudeksi ilmiöksi rahanpesun estämisen osalta useiden eri viranomaistahojen toimesta.

Tämän tutkielman tavoitteena on tutkia virtuaalivaluuttoihin liittyvää rahanpesua yleisesti sekä sen seurauksena syntyvää pankin rahanpesuriskiä. Tutkielmassa keskitytään löytämään virtuaalivaluuttojen rahanpesuun liitettäviä ominaisuuksia sekä erilaisia rahanpesutypologioita. Lisäksi tutkielman avulla pyritään ymmärtämään, kuinka merkittävän rahanpesuriskin virtuaalivaluutat pankin näkökulmasta aiheuttavat ja miten yksittäiset pankit voivat rahanpesun estämisen toimintatavoillaan hallita kyseistä riskiä.

Tutkielman teoriaosuus muodostuu virtuaalivaluuttoja, rahanpesuriskiä sekä rahanpesun estämistä käsittelevästä kokonaisuudesta. Teoriaosuuden tarkoituksena on taustoittaa mahdollisimman kattavasti tutkielman empiriapohjaa, joka on toteutettu kahdessa eri osassa. Teoriaosuudessa esitellään myös empiriassa hyödynnettävä rahanpesun estämisen viitekehys, kolmen puolustuslinjan malli sekä riskin nelikenttä. Ensimmäisessä empiriaosassa toteutetaan integroiva kirjallisuuskatsaus virtuaalivaluutoista rahanpesun välineenä, jota rikastetaan toisen empiriaosuuden teemahaastatteluilla. Haastateltavissa oli edustettuina kaikki pankin kolme riskienhallinnan puolustuslinjaa.

Tutkielman lopputuloksena tunnistetaan, että virtuaalivaluutat soveltuvat rahanpesuun erittäin hyvin erityisesti niiden pseudo-anonyymin luonteen, keskitetyn hallintatahon puuttumisen sekä sääntelyn puutteellisuuden takia. Virtuaalivaluuttojen aiheuttama rahanpesuriski on pankille known unknown -tyyppinen riski: kyseisen riskin olemassaolo tunnistetaan, mutta sen merkityksestä organisaatiolle ei ole täyttä tietoutta. Virtuaalivaluuttojen aiheuttaman rahanpesuriski voidaan nähdä pankin näkökulmasta merkittävänä sekä riittävän tietouden tason että hallintakeinojen puuttumisen takia. Tutkielman pohjalta esitetään konkreettisia riskienhallintakeinoja pankkien käyttöön liittyen neljään eri osa-alueeseen: rahanpesun estämisen politiikkaan ja koulutukseen, transaktiomonitorointiin, asiakkaan tuntemiseen sekä jatkuvaan kehittämiseen ja ennaltaehkäisemiseen.

Virtuaalivaluutat ovat täysin uudenlainen uhka perinteisille rahanpesun estämisen toimintatavoille. Lisäksi aihepiiriin liittyvä sääntely ei välttämättä pysy virtuaalivaluuttaekosysteemin kasvuvauhdin perässä. Sääntelyn tulisikin ohjata pankin riskienhallintakeinojen minimitasoa, jonka päälle pankin tulee luoda omaan riskiarvioonsa pohjautuvia toimintatapoja. Tässä tutkielmassa on rakennettu viitekehys, jonka avulla pankki voi ymmärtää paremmin virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä sekä miten sitä voidaan hallita.

Avainsanat: virtuaalivaluutat, kryptovaluutat, lohkoketju, rahanpesu, rahanpesun estäminen, rahanpesuriski, kolmen puolustuslinjan malli

SISÄLLYSLUETTELO

KUVIO- JA TAULUKKOLUETTELO

1 JOHDANTO

1.1 Aihealueen esittely ja merkitys

Vuonna 2008 maailmaa ravistelleen finanssikriisin jälkiseurauksena nousi huoli finanssijärjestelmän ja sen keskitettyjen toimijoiden luotettavuudesta. Samana vuonna mystinen hahmo Satoshi Nakamoto kirjoitti uraauurtavan julkaisunsa Bitcoin -nimisestä järjestelmästä. Tuo julkaisu antoi lähtölaukauksen lohkoketjuteknologiaan perustuvien virtuaalivaluuttojen aikakaudelle. Lohkoketjujen yksi kantava ajatus oli mahdollistaa talousjärjestelmään luottamusta ilman perinteistä pankkitoimintaa – sitä samaa luottamusta, joka finanssikriisin aikaan menetettiin. Lohkoketjuteknologiaan liittyvä kyky korvata kolmannet osapuolet matematiikan keinoin on yksi tärkeimmistä syistä sille, miksi kyseinen teknologia kasvattaa jatkuvasti suosiotaan (Johansson, Eerola, Innanen & Viitala, 2019, 72–73).

Lohkoketjuteknologian viime vuosikymmenen vaikuttavin sovellusmuoto finanssimaailmassa on ollut virtuaalivaluutat, jotka mahdollistavat nopeita, anonyymejä sekä pankeista riippumattomia transaktioita. Virtuaalivaluuttojen kasvavasta suosiosta ja vakiintuvasta asemasta kertoo merkittävien pääomasijoitusyhtiöiden investoinnit viime vuosina virtuaalivaluuttoihin liittyviin kasvuyrityksiin. Virtuaalivaluutoilla on mahdollisuus parantaa maksuliikenteen tehokkuutta, laskea eri maksutavoista aiheutuvia transaktiokuluja sekä luoda uusia innovaatioita maksuliikennealalle. (FATF, 2014, 8–10.)

Virtuaalivaluuttojen kasvavan suosion pohjalta on noussut esiin kahdenlaista näkökulmaa: virtuaalivaluutat edustavat tulevaisuutta maksujärjestelmille, mutta toisaalta virtuaalivaluutat mahdollistavat uusia toimintatapoja rikollisille, terrorismin rahoittajille sekä pakotteiden kiertäjille siirtää ja varastoida laittomia varoja viranomaisten ja muiden valvovien tahojen ulottumattomiin. (FATF, 2021, 5.) Erityisesti pakotteiden kiertäminen erilaisten virtuaalivaluuttojen kautta nousi ajankohtaiseksi näkökulmaksi keväällä 2022 Ukrainan sodan myötä (Kauppalehti, 2022). Virtuaalivaluutat nähdään sekä uusien innovaatioiden mahdollistajana ja finanssijärjestelmän mullistajana, mutta myös uudenlaisena työvälineenä rikollisille toimintansa kehittämiseksi.

Arkikielessä virtuaalivaluutoilla viitataan usein vain yhteen niiden alalajiin, kryptovaluuttoihin. Tämä johtuu pitkälti siitä, että vaihdantamäärällisesti kryptovaluutat ovat suurin yksittäinen osa-alue virtuaalivaluuttaekosysteemissä. Huolimatta Covid-19 pandemiasta ja muista viimeisten

vuosien aikana maailmantaloutta horjuttaneista tekijöistä, tunnetuin kryptovaluutta Bitcoin on rikkonut jatkuvasti uusia ennätyksiä sekä sen arvossa että suosiossa mitattuna. (Coinmarketcap.com, 2022). Erityisesti vuosi 2021 oli kryptovaluuttojen läpimurtovuosi, sillä suurin osa nykyisistä kryptovaluuttojen omistajista teki ensimmäiset ostonsa vasta viime vuoden puolella (Lang, 2022). Suosion laantumisesta ei toistaiseksi ole viitteitä.

Suosion nousu on näkynyt myös virtuaali- ja kryptovaluuttoihin liittyvän rikollisuuden kasvussa: vuonna 2021 kryptovaluuttoihin liitettävän rikollisuuden arvioitu määrä oli korkeammalla kuin koskaan aikaisemmin. Suurimmat kryptovaluuttoihin yhdistettävissä olevat rikokset liittyvät huijauksiin, darknet-markkinapaikkoihin, varastettuihin varoihin, kiristysohjelmiin sekä huumausaineisiin. (Chainanalysis, 2022, 3; Valtiovarainministeriö, 2021, 38). On tärkeää ymmärtää, että rahanpesu liittyy tiiviisti kaikkiin näihin rikosmuotoihin – saatuaan rikolliseen alkuperään liittyvää virtuaalivaluuttaa, rikollinen haluaa häivyttää rikollisen rahan todellisen alkuperän ja muuttaa virtuaalivaluuttaa sellaiseen varallisuusmuotoon, jossa sitä voidaan kuluttaa tai säilyttää pankissa tavallisen fiat-valuutan tapaan. Näin ollen myös pankit voivat huomaamattaan olla osallisina rahanpesuprosessiin ja altistua virtuaalivaluuttoihin liitettävälle rahanpesuriskille. (Isa, Sanusi, Haniff & Barnes, 2015, 8.) Rahanpesu on vakava ongelma pankkisektorille sekä laajemmin koko yhteiskunnalle (Chapman, 2018, 8). Rahanpesun vuosittaista määrää on vaikea arvioida ilmiön monitulkintaisuuden ja rikosluonteen takia, mutta joidenkin arvioiden mukaan se asettuu 800 miljardin ja 2 biljoonan Yhdysvaltain dollarin väliin (UNODC, 2022). Virtuaalivaluutat ovat vain yksi rahanpesun instrumenteista, mutta lukujen valossa ne ovat merkittävä ongelma (Chainanalysis, 2022). Myös eri viranomaistahot ovat viimeisten vuosien aikana nostaneet esiin virtuaalivaluuttoihin liitettävän erittäin korkean rahanpesuriskin (Valtiovarainministeriö, 2021; FATF, 2021; Basel, 2021).

Näin ollen myös pankkien tulee toiminnassaan osata ottaa huomioon virtuaalivaluuttoihin ja lohkoketjuteknologiaan liittyvät uudenlaiset riskit sekä etsiä kehittyneempiä tapoja monitoroida asiakkaidensa virtuaalivaluuttoihin liittyvää rahaliikennettä. Talousrikollisuuden torjunta ja rahanpesun estäminen ovat merkittävä osa pankkien riskienhallintaa, ja pankkien yhtenä roolina voidaankin nähdä rahanpesun estämisen portinvartijoina toimiminen (Chau & Nemcsik, 2020, 2–3.). Lisäksi pankit ovat Suomessa rahanpesulain nojalla velvoitettuja tuntemaan asiakkaansa sekä heidän maksuliikenteensä. Virtuaalivaluutat itsessään ovat Suomessa laillinen instrumentti, eikä niiden käyttöä yksityishenkilön näkökulmasta ole rajoitettu - ainakaan vielä. Virtuaalivaluuttoihin liittyvä ekosysteemi ja samalla myös tällä hetkellä tuntemamme maksuliikennejärjestelmä

muuttuvat kiihtyvällä vauhdilla, mihin finanssialan toimijoiden tulee olla varautuneita. Aihetta onkin mielekästä tutkia erityisesti perinteisen pankkisektorin näkökulmasta – miten ja miksi pankin tulisi itsenäisenä toimijana hallita virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä?

1.2 Tavoitteet, tutkimusongelmat ja keskeiset rajaukset

Tutkielman tavoitteena on tutkia virtuaalivaluuttoihin liittyvää rahanpesua yleisesti sekä sen seurauksena syntyvää rahanpesuriskiä ja kyseisen riskin hallitsemista pankin näkökulmasta. Tutkimuksessa keskitytään luomaan aihepiirin ympärille eräänlaista riskiarviota. Riskiarvioon kuuluu tyypillisesti riskien tunnistaminen, riskien arviointi sekä toimenpiteet riskeihin vastaamiseksi (Rausand, 2013). Näin ollen tutkimuskysymykset on asetettu muotoon:

1) *Millaisen rahanpesuriskin virtuaalivaluuttojen käyttäminen rahanpesun välineenä luo?*
2) *Kuinka merkittävä virtuaalivaluuttojen aiheuttama rahanpesuriski on pankille?*
3) *Millä eri keinoin pankkien tulisi huomioida virtuaalivaluuttojen aiheuttama rahanpesuriski osana riskienhallintaa?*

Ensimmäiseen kysymykseen sisältyy itse riskin määrittely sekä sen kuvaaminen, millä eri keinoilla virtuaalivaluuttoja voidaan hyödyntää rahanpesun välineenä. Toisen kysymyksen avulla ongelmaan pystytään pureutumaan syvällisemmin – kuinka merkittävä rahanpesuriski pankille muodostuu? Tutkielmassa tulee tarkastella muun muassa pankkeja velvoittavaa lainsäädäntöä sekä ilmiötä laajemmin. On myös tärkeää tuoda esiin pankkiin kohdistuvat riskit aihealueen tiimoilta. Kolmantena kysymyksen avulla selvitetään, millaisia keinoja pankeilla on tällä hetkellä käytössään riskin tunnistamiseksi sekä hallitsemiseksi ja mitä ne voisivat tulevaisuudessa olla.

Tämän pro gradu -tutkimuksen pohjalta tullaan tekemään eräälle suomalaiselle finanssilaitokselle erillinen raportti, jonka tarkoituksena on pyrkiä kuvastamaan yrityksen nykytila virtuaalivaluuttoihin liittyvän rahanpesuriskin hallinnassa sekä löytämään uudenlaisia riskin hallintakeinoja yrityksen käyttöön. Itse tutkielman tarkoitus ei ole ottaa kantaa mihinkään yksittäiseen suomalaiseen finanssilaitokseen, vaan tutkia asiaa yleisesti suomalaisten pankkien näkökulmasta. Rajaamalla tutkittavan aihealueen näkökulman pankkeihin jää rajauksen ulkopuolelle esimerkiksi aiemmin mainitut virtuaalivaluuttapalveluiden tarjoajat.

Talousrikollisuuden torjunnassa rahanpesun estämiseen liitetään usein myös terrorismin rahoittamisen estäminen. Koska myös jälkimmäinen aihe on laaja, rajataan tämä tutkielma

tarkastelemaan vain rahanpesun estämisen näkökulmaa. Rahanpesun estämiseen liittyvä sääntely on kansainvälistä, joten myös tutkielman taustateoria pohjautuu kansainväliseen tutkimukseen. Tutkimuskysymyksiin vastataan kuitenkin Suomessa toimivien Finanssivalvonnan alaisten pankkien näkökulmasta.

1.3 Keskeiset käsitteet ja lyhenteet

AML = Anti Money Laundering, viitataan yleisesti rahanpesun estämiseen ja siihen liittyviin toimintoihin.
FATF = The Financial Action Task Force (FATF) on itsenäinen hallitustenvälinen elin, joka tuottaa ja edistää asetuksia. Näiden asetuksien tarkoituksena on suojella kansainvälistä finanssijärjestelmää rahanpesulta, terrorismin rahoittamiselta sekä joukkotuhoaseiden rahoituksen leviämiseltä. (FATF, 2022, 2.)

Virtuaalivaluutta on digitaalisessa muodossa olevaa arvoa, jota voidaan siirtää, tallentaa ja vaihtaa sähköisesti. Se ei ole minkään keskuspankin tai viranomaisen liikkeelle laskemaa eikä se ole Suomessa laillinen maksuväline (Laki virtuaalivaluutan tarjoajista 572/2019). Virtuaalivaluutta voi toimia joko vaihdon välineenä tai sijoituskohteena. Virtuaalivaluutta erotellaan **fiat-valuutasta**, joka puolestaan tunnetaan jokaisen valtion omana perinteisenä kolikko- ja setelirahana. Virtuaalivaluutta ei ole sama asia kuin internet-valuutta, mikä on fiat-valuutan digitaalinen esiintymis- ja vaihdantamuoto. (FATF, 2021, 123.) Virtuaalivaluuttojen teoriaa käsitellään tarkemmin ensimmäisessä teorialuvussa.

Kryptovaluutalla tarkoitetaan matemaattisperusteista, lohkoketjuteknologiaan perustuvaa ja vaihtokelpoista virtuaalivaluutan alalajia, joka on suojattu kryptografiaksi kutsutulla salaustekniikalla. Kryptovaluutta nojaa julkisiin ja yksityisiin avaimiin siirtäessään arvoa yhdeltä entiteetiltä toiselle, ja jokaisen siirron tulee olla salaustekniikalla allekirjoitettu. Kryptovaluutan tilikirjojen turvallisuus, koskemattomuus ja tasapaino on varmistettu tasapuolisesti toisistaan riippumattomien tahojen toimesta. Tunnetuin kryptovaluutta on vuonna 2008 kehitetty Bitcoin. (FATF, 2014, 5.) Kryptovaluuttojen teoriaa käsitellään tarkemmin ensimmäisessä teorialuvussa.

Rahanpesu määritellään Suomen rikoslaissa 32 luvun 6–10 §:ssä toiminnaksi, jossa joku ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää tai välittää rikoksella hankittua omaisuutta peittääkseen tai häivyttääkseen hyödyn tai omaisuuden laittoman alkuperän (Rikoslaki 1889/39). Rahanpesua käsitellään tarkemmin toisessa teorialuvussa.

1.4 Tieteenfilosofiset lähtökohdat

Tutkielman tavoitteena yleisesti voidaan nähdä tutkittavan ilmiön kartoittaminen, kuvaaminen sekä ilmiön selittäminen ja ymmärtäminen. Tähän pyritään tutkielman empiria- ja teoriaosuuden tehokkaan vuoropuhelun kautta. Tieteenfilosofialla viitataan niihin uskomuksiin ja oletuksiin, jotka liittyvät tiedon kehittymiseen. Tieteenfilosofisilla lähtökohdilla tarkoitetaan metodologioita ja tutkimusstrategioita, joiden avulla muodostetaan tutkielman perusta. Tieteenfilosofia myös ohjaa tutkielmassa käytettävän tutkimusmenetelmän valintaa. (Saunders, Lewis & Thornhill, 2019, 128–130.)

Tutkimuksen tieteenfilosofisten lähtökohtien tunnistaminen heti tutkimusprosessin aluksi on tärkeää, sillä ne vaikuttavat siihen mitä, miten ja miksi ilmiötä tutkitaan. (Carson, Gilmore, Perry & Gronhaug, 2001, 12). Tieteenfilosofisten lähtökohtien tunnistamiseksi tulee ymmärtää taustalla vaikuttavat tutkijan tieteenfilosofiset oletukset. Nämä oletukset vaikuttavat sekä tiedostetusti että tiedostamatta koko tutkimusprosessin ajan. Oletukset voivat olla ontologisia, jotka liittyvät tutkijan oletuksiin todellisuudesta tai epistemologisia, jotka puolestaan viittaavat oletuksiin tietoudesta. Kolmantena tutkimukseen vaikuttavana oletustyyppinä ovat aksiologiset oletukset, jotka kuvastavat tutkijan omien arvojen vaikutusta tutkimusprosessiin. (Saunders ym, 2019, 133–134.)

Ontologia viittaa ilmiön todelliseen luonteeseen, joka tämän tutkielman tapauksessa voidaan nähdä riskiksi, joka syntyy virtuaalivaluuttojen käyttämisestä rahanpesun välineenä. Virtuaalivaluuttojen aiheuttaman rahanpesuriskin kokonaisvaltaisen hahmottamiseen edellytetään usean eri tieteenalan ja teoriapohjan, kuten esimerkiksi riskienhallinnan, rahanpesun, talousrikollisuuden torjunnan sekä lohkoketjuteknologian ymmärtämistä. Ontologisiin oletuksiin liittyy myös vahvasti ennakkoasenteet tutkittavaa ilmiötä kohtaan. (Saunders ym, 2019, 133.) Virtuaalivaluuttojen kohdalla niissä nähdään sekä riskiä, mutta myös mahdollisuuksia. Tämä tutkielma keskittyy pääosin negatiiviseen riskinäkökulmaan, mutta ei pyri myöskään tarkoituksenmukaisesti rajaamaan pois niiden mahdollistamia hyötyjä pankeille ja finanssimarkkinoille laajemmin.

Epistemologiset oletukset vaikuttavat tutkijan ajatuksiin tutkittavaan ilmiöön saatavilla olevasta tiedosta. Näihin oletuksiin liittyy tämän tutkielman yhteydessä kysymykset siitä, millaista tietoutta ilmiöstä on saatavilla ja mitä tietoa voidaan käyttää johtopäätösten luomiseen. Nämä kysymykset puolestaan vaikuttavat siihen, mikä tutkimusmetodi ilmiön tutkimiseen sopii parhaiten. (Saunders

ym, 2019, 133–134.) Virtuaalivaluuttojen käyttämisestä rahanpesun välineenä ei ole olemassa tarkkoja lukuja, joka johtuu rahanpesuun liittyvän ilmiön moniulotteisuudesta (Reuter, 2005, 2). Pitkälti tämän ontologisen päätelmän perusteella tutkielman tutkimusotteeksi valikoitui laadullinen tutkimus.

Aksiologialla viitataan arvojen vaikutukseen osana tutkimusprosessia, joka on erityisesti rahanpesuriskistä puhuttaessa tärkeä oletus. Yksi tärkeistä aksiologisista valinnoista on rajata, kuinka pitkälle tutkijan omat arvot ja uskomukset vaikuttavat tutkimuksen toteuttamiseen. (Saunders ym, 2019, 134.) Tämän tutkielman aihevalintaa ohjasi osaltaan tutkijan oma mielenkiinto ja kokemus talousrikollisuuden sekä rahanpesun torjunnan parissa. Lisäksi aksiologisena valintana voidaan nähdä myös haastatteluaineiston kerääminen puolistrukturoituna teemahaastatteluna, jossa tutkija pääsee myös keskustelun kautta esittämään tarkentavia kysymyksiä. Kysymyksissä näkyy myös tutkijan oma tietoisuus aihepiiristä. Tutkijan on kuitenkin olennaista ymmärtää oman subjektiivisen käsityksensä vaikutus tutkimuksen etenemiseen (Efron & Ravid, 2019, 17).

Näiden oletuksien pohjalta voidaan valita tutkielman tieteenfilosofinen suuntaus. Tässä tutkielmassa käytetään interpretivismia, joka korostaa tulkinnallisuutta ja tutkintojen tekemistä tiedon tuottamisessa. Interpretivismi on tyypillinen tausta kvalitatiivisissa tutkimuksissa ja sen avulla voidaan tutkia virtuaalivaluuttojen ja rahanpesun kaltaisia kompleksisia kokonaisuuksia. Interpretivismin avulla pyritään tuottamaan kontribuutiona uusia näkökulmia ja ymmärrystä tutkittavasta aiheesta. Tutkijalla voi myös olla hyvin läheinen ja subjektiivinen ote tutkittavaan ilmiöön, mikä nähdään tämän tutkielman kannalta eduksi. Interpretivismiin liitetään usein induktiivinen päättely, jolla tarkoitetaan aikaisemman teorian pohjalta rakennettavaa uutta teoriaa. Päättely etenee yksittäisistä havainnoista yleiseen. (Saunders ym, 2019, 148–153.) Tässä tutkielmassa on tarkoitus yhdistää perinteistä pankkien riskienhallintaan, rahanpesuun ja lohkoketjuteknologiaan liittyvää teoriaa ja muodostaa niistä virtuaalivaluuttojen aiheuttaman rahanpesuriskiin keskittyvää teoriapohjaa. Induktiivinen tutkimus alkaa tyypillisesti jostain havaitusta ja kiinnostavasta ilmiöstä, johon liittyy avonaisia kysymyksiä (Woiceshyn & Daellenbach, 2018, 185). Lohkoketjuteknologia ja virtuaalivaluutat ovat uusi ja kiinnostava tutkimuskohde varsin pitkään muuttumattomana pysyneen pankkijärjestelmän näkökulmasta. Rahanpesu puolestaan on kiinnostava tutkimuskohde rikokseen liittyvän luonteensa takia - erityisesti myös siitä näkökulmasta, jossa ilmiön laajuudesta ja mekanismeista ei ole saatavilla täyttä tietoutta ennen kuin rikollinen on jäänyt kiinni ja tapaukset tuodaan julki.

1.5 Tutkimusmenetelmät ja -aineistot sekä aikaisemmat tutkimukset

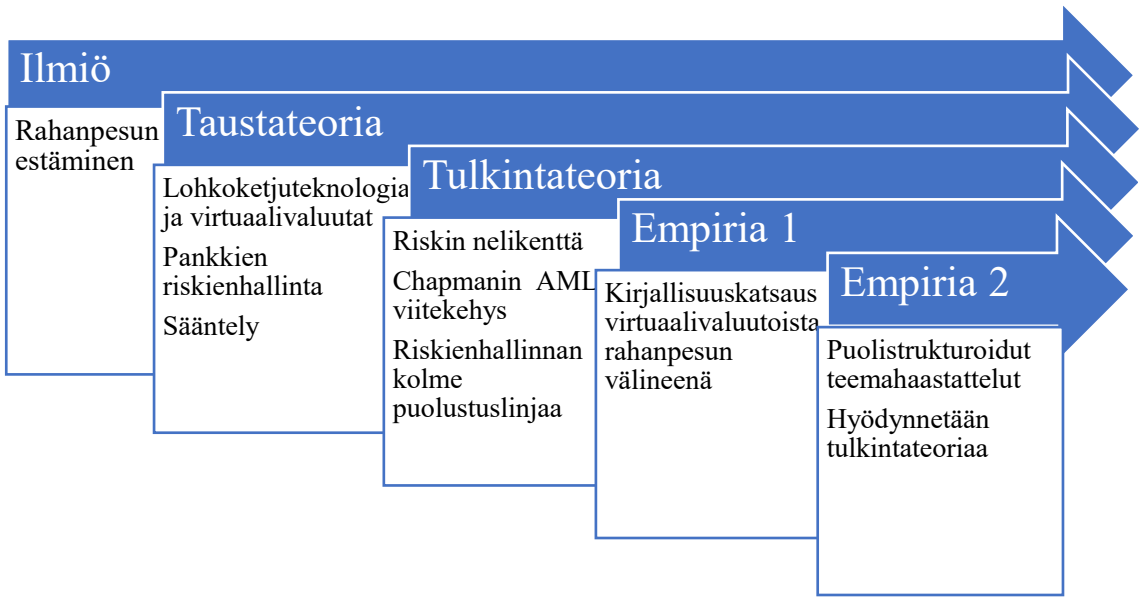
Tutkielman tavoitteiden ja tieteenfilosofisten lähtökohtien perusteella on valittu tutkimusmenetelmät, joiden avulla pyritään vastaamaan tutkimusongelmiin. Tutkimus voidaan toteuttaa perinteisesti joko kvalitatiivisena, kvantitatiivisena tai näitä yhdistävänä monimenetelmätutkimuksena (Efron & Ravid, 2019, 16). Tämä tutkielma toteutetaan laadullisena tutkimuksena keräämällä kvalitatiivista havaintoaineistoa kahdessa eri osassa. Kvalitatiivisen lähestymistavan avulla pyritään löytämään tosiasioita kokonaisvaltaisen tiedonhankinnan keinoin (Hirsjärvi, Remes & Sajavaara, 2009, 161–164). Kvalitatiivisessa tutkimuksessa hyödynnetään usein havainnointia, syvällisiä haastatteluita sekä erilaisten aineistojen analysointia (Efron & Ravid, 2019, 17).

Tutkielmassa toteutetaan ensimmäisenä empiriaosana integroiva kirjallisuuskatsaus, jonka jälkeen ensimmäistä empiriaosaa vahvistetaan kolmella teemahaastattelulla. Kyseiseen yhdistelmään päädyttiin, sillä kyseessä on kompleksinen kokonaisuus, joka koostuu sekä itse virtuaalivaluutoista aiheutuvan rahanpesuriskin ymmärtämisestä että sen yhdistämisestä osaksi suomalaisten pankkien riskienhallintaa ja rahanpesun estämistä. Aihetta ei ole tutkittu aikaisemmin suomalaisten pankkien näkökulmasta. Kahden eri laadullisen tutkimusmenetelmän yhdistämisellä pyritään paitsi ymmärtämään virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä, mutta myös kartoittamaan uusia riskienhallintakeinoja pankin näkökulmasta.

Kirjallisuuskatsauksen avulla pyritään tutkimaan aikaisemmin tehtyä tutkimusta. Tyypillisesti kirjallisuuskatsaus voi olla joko kuvaileva kirjallisuuskatsaus, systemaattinen kirjallisuuskatsaus tai meta-analyysi. Kuvaileva kirjallisuuskatsaus puolestaan jakautuu kahteen päämetodiin: kevyempään narratiiviseen sekä integroivaan kirjallisuuskatsaukseen. Integroivassa kirjallisuuskatsauksessa on paljon systemaattisen kirjallisuuskatsauksen piirteitä, mutta se tarjoaa systemaattista kirjallisuuskatsausta laajemman kuvan aihetta käsittelevästä kirjallisuudesta. Tutkimuksen kohteena olevasta ilmiöstä saadaan laajempi kuva, sillä integroivassa kirjallisuuskatsauksessa voidaan valita monipuolisemmin erilaisia lähteitä kuin systemaattisessa kirjallisuuskatsauksessa. (Salminen, 2011, 6–8.)
Empiriaosuuden toisessa vaiheessa toteutetaan puolistrukturoidut teemahaastattelut, jotka analysoidaan laadullisella sisällönanalyysillä. Puolistrukturoitu teemahaastattelu on lomake- ja avoimen haastattelun välimuoto. Tyypillistä on, että haastattelun teema on tiedossa etukäteen, mutta kysymyksillä ei ole tarkkaa muotoa ja järjestystä. Haastateltavalle annetaan mahdollisuus tutustua haastattelun teemoihin etukäteen. Haastattelijalla on myös mahdollisuus kysyä

tarkentavia kysymyksiä, jolloin haastattelussa voi olla myös keskustelulle tyypillisiä piirteitä. (Hirsjärvi ym., 2009, 208.) Tutkimusempiriaa kerätään tutkielman taustateoriassa esitellyn pankin riskienhallinnassa käytetyn kolmen puolustuslinjan mukaisesti. Ensimmäisen puolustuslinjan näkemyksiä esittää talousrikollisuuden torjunnan asiantuntija. Toista puolustuslinjaa edustaa kaksi compliance-asiantuntijaa ja kolmatta sisäisen tarkastuksen asiantuntija. Haastattelemalla ainakin yhtä asiantuntijaa kaikista kolmesta puolustuslinjasta pyritään saamaan samanaikaisesti tiivis, mutta kattava läpileikkaus pankin eri riskienhallintatoimintojen näkemyksestä virtuaalivaluuttojen aiheuttamaan rahanpesuriskiin.

Haastatteluiden painoarvoa ei haluttu kuitenkaan tuoda liian suureksi. Aiheen arkaluontoisuuden vuoksi tutkielmassa tukeudutaan jo olemassa olevaan laajaan teoriapohjaan. Haastatteluilla pyrittiin ensisijaisesti löytämään vahvistusta aiemmassa laadullisessa empiriaosuudessa löydettyihin virtuaalivaluuttojen rahanpesuliitännäisiin ominaisuuksiin sekä löytämään kyseiselle riskille hallintakeinoja. Haastattelut nähtiin tehokkaana keinona testata tutkielman teoriapohjan sekä kirjallisuuskatsauksen muodostamaa kokonaisuutta. Tutkielman tulokset muodostuvat kuvan 1 havainnollistamalla tavalla teorian ja empirian vuoropuheluna, jota hyödynnetään läpi koko tutkielman.



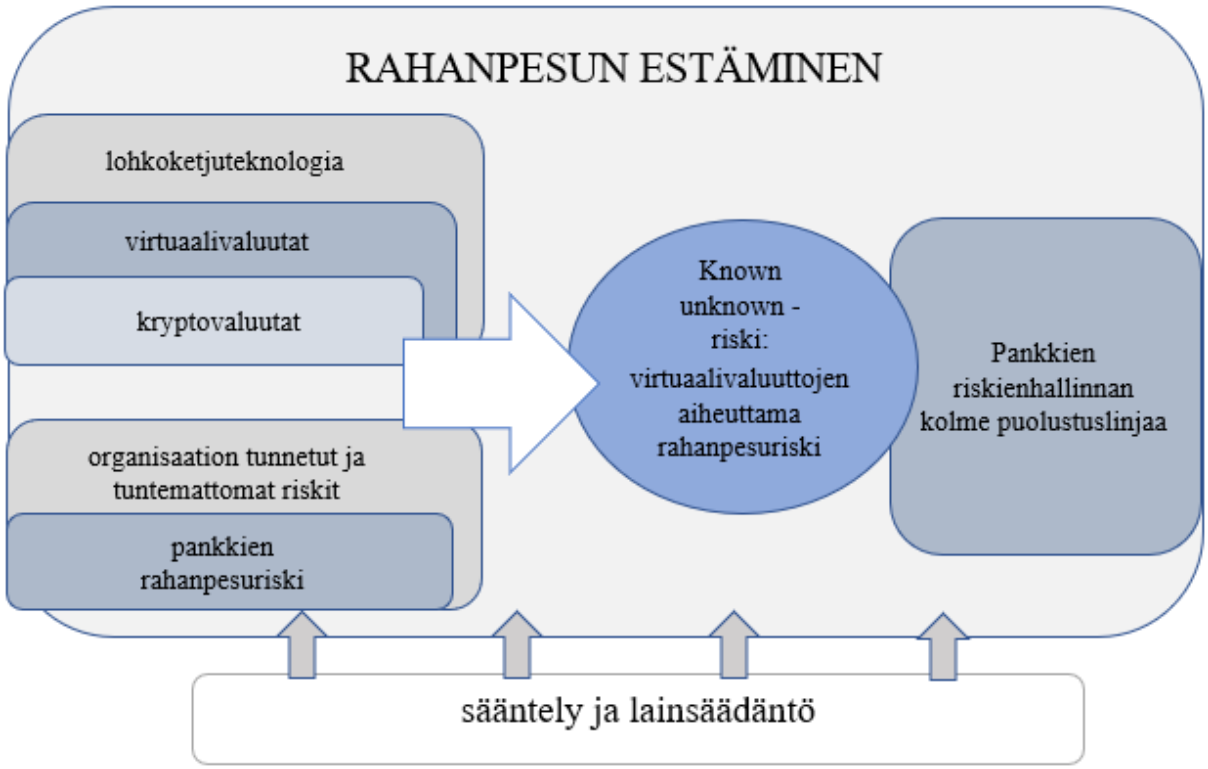
Kuvio 1. Tutkielman eteneminen

Virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä tarkastellaan integroivan kirjallisuuskatsauksen avulla tutkielman neljännessä luvussa, jonka yhteydessä esitellään myös tarkemmin katsauksessa käytetyt aineistot. Rahanpesusta ja compliance -toiminnoista on olemassa runsaasti

virtuaalivaluuttoja käsittelevää kirjallisuutta, mutta suurin osa kirjallisuudesta keskittyy vain estämisnäkökulmaan eikä riskin kokonaisvaltaiseen ymmärtämiseen (Teichmann & Falker, 2020, 504). Useat tutkimukset keskittyvät myös vain kryptovaluuttoihin. Virtuaalivaluuttojen soveltuvuutta rahanpesun tarkoituksiin on tarkasteltu muun muassa ohjelmistotekniikan, oikeustieteen ja taloustieteen näkökulmasta (Brenig, Accorsi & Müller, 2015, 2). Virtuaalivaluuttojen aiheuttama rahanpesuriski on kuitenkin verrattain tuore sekä vähän tutkittu ilmiö pankkien näkökulmasta. Pro gradu -tasolla rahanpesuriskiä on tutkittu vähän. Sonja Korpelan (2021) gradu käsitteli pankin rahanpesuriskin hallintaa asiakkaan tuntemisen avulla.

Virtuaalivaluuttoihin liittyvää rikollisuutta sekä rahanpesua ovat tutkineet myös alan suurimmat lohkoketjuanalytiikkaa ja transaktiomonitorointipalveluita tarjoavat yritykset kuten Chainanalysis ja Elliptic. Esimerkiksi FATF perustaa linjauksensa näiden yrityksien tuottamaan dataan, minkä perusteella raporttien voidaan todeta olevan tarpeeksi relevanttia hyödynnettäväksi osana tätä tutkielmaa. Myös suuret konsulttiyhtiöt sekä finanssialan eri toimijat ovat julkaisseet rahanpesun estämiseen liittyviä tutkimuksia ja raportteja, joissa käsitellään myös virtuaalivaluuttoja.

1.6 Tutkielman teoreettinen viitekehys



Kuvio 2. Tutkielman teoreettinen viitekehys

Tämän tutkielman teoreettinen viitekehys on luonteeltaan narratiivinen viitekehys, jonka avulla kuvataan sekä tutkielman teorian ympärille muodostuvaa laajempaa kokonaisuutta että yksittäisten kriittisten käsitteiden ja ilmiöiden yhteyttä toisiinsa. Viitekehyksen avulla määritellään aiheeseen liittyvä prosessimalli, joka selittää erilaisten tapahtumien yhteyttä toisiinsa. (Lindgreen, Benedetto, Brodie & Jaakkola, 2021, A4.) Tutkielman viitekehyksessä on myös piirteitä typologisesta tyylistä, sillä erilaisia lohkoketjuteknologiaan liittyviä käsitteitä esitetään taksonomian avulla viitekehyksen vasemmassa yläkulmassa. Myös pankkien rahanpesuriski nähdään sisältyvän organisaation riskeihin yleisesti. Typologisen tyylin yhtenä tarkoituksena on yhdistää erilaisia käsitteitä yhtenäiseksi joukoksi (Cornelissen, 2017, 3).

Tämän tutkielman viitekehyksen avulla halutaan kuvata sitä, mitä lohkoketjuteknologiasta, virtuaalivaluutoista ja pankkien rahanpesuriskistä jo tiedetään, mutta myös edistää olemassa olevaa tietoa ja yhdistää edellä mainitut käsitteet rahanpesun estämiseen ja pankkien riskienhallintaan. Tutkielman teorian taustalla vaikuttava ilmiö on rahanpesun estäminen, johon yhdistetään sekä virtuaalivaluuttoihin, rahanpesuun että pankkien rahanpesuriskiin liittyvää teoriaa. Tulkintateorian avulla tulkitaan tyypillisesti tutkielman tuloksia. Tämän tutkielman tulkintateoriana toimivat sekä riskin nelikenttä-jaottelu tunnettuihin ja tunnistamattomiin riskeihin, Chapmanin rahanpesun estämisen viitekehys sekä riskienhallinnan kolmen puolustuslinjan viitekehys. Pankin näkökulmasta virtuaalivaluuttojen aiheuttama rahanpesuriski tunnistetaan tutkielmassa known unknown-tyyppiseksi riskiksi ja sen hallintakeinot riippuvat riskin luonteesta, jota tulkitaan teorian ja ensimmäisen empiriaosuuden löydöksien pohjalta. Näin ollen tutkielman ensimmäisen empiriaosuuden löydöksien voidaan myös nähdä olevan osa tutkielman tulkintateoriaa.

Viitekehyksen vasen reuna kuvastaa, miten virtuaalivaluuttojen aiheuttama rahanpesuriski pankin näkökulmasta syntyy. Oikea puoli havainnollistaa, miten sitä hallitaan. Narratiivinen viitekehys tarkoitus onkin esittää se, miten prosessin tietyt elementit johtavat tiettyyn tulokseen (Cornelissen, 2017, 5–6). Uudenlaisen rahanpesuriskin syntyminen johtaa pankkien tarpeeseen huomioida virtuaalivaluuttojen aiheuttama rahanpesuriski osana riskienhallintaansa, jota toteutetaan pankissa kolmen puolustuslinjan periaatteen mukaisesti. Tärkein viitekehyksen kuvaama syy-seuraussuhde on se, miten tarve rahanpesun estämiselle osana pankkien riskienhallintaa syntyy rahanpesun olemassaolon seurauksena ja miten lohkoketjuteknologia vuorostaan synnyttää uudenlaisia rahanpesuriskejä. Viitekehyksessä on myös kuvattu syy-seuraussuhteena, miten sääntely ja

lainsäädäntö vaikuttavat vahvasti kaikkiin teoreettisen viitekehyksen eri osa-alueisiin ja luovat perustan koko rahanpesun estämisen toteuttamiselle.

1.7 Tutkielman rakenne

Tämä pro gradu -tutkielma on jaettu kuuteen eri lukuun. Ensimmäisenä kappaleena on Johdanto-kappale, jossa esitellään tutkittava aihe ja annetaan lukijalle käsitys aiheen merkityksestä. Tämän lisäksi pohjustetaan tutkielman kannalta tärkeätä termistöä, johon palataan kuitenkin vielä tarkemmin teorialukujen yhteydessä. Johdannossa esitellään myös tutkielman tutkimusongelmat sekä tutkielmassa käytetyt menetelmät.

Johdannon jälkeen lähestytään tutkittavaa aihetta kahden teorialuvun kautta, jotka nousevat myös merkittävään osaan myöhemmin tutkielman empiriaa rakennettaessa. Ensimmäisessä teorialuvussa käsitellään tarkemmin virtuaalivaluuttoja. Jotta voitaisiin ymmärtää tarkemmin virtuaalivaluuttoihin liittyvää rahanpesuriskiä, tulee tutkielmassa tarkastella myös lohkoketjuteknologiaa ja syvällisemmin virtuaalivaluuttoihin liittyviä eri osa-alueita. Tutkielman toisen teorialuvun otsikkona on ”Pankin rahanpesuriski ja rahanpesun estäminen”. Luvussa kuvataan rahanpesua ilmiönä, sen estämistä sekä lainsäädännöllistä ympäristöä. Rahanpesun estämistä käsitellään erityisesti pankin näkökulmasta tutkielman rajauksen mukaisesti. Tämän rinnalle tuodaan riskin teoriaa, jonka pohjalta tulkitaan pankin rahanpesuriskiä.

Neljännessä luvussa toteutetaan ensimmäisenä empiriaosana integroiva kirjallisuuskatsaus. Luvussa tarkastellaan virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä, jota peilataan myös kahden ensimmäisen teorialuvun sisältöön. Luvun aluksi käydään läpi tarkemmin integroivaa kirjallisuuskatsausta menetelmänä ja sen eri vaiheita. Viidennessä luvussa tutkielman empiriapohjaa täydennetään keräämällä aineistoa puolistrukturoiduilla teemahaastatteluilla pankin asiantuntijoilta, jotka edustavat eri riskienhallinnan puolustuslinjoja. Kuudes luku on teoriaa ja empiriaa yhdistelevä yhteenvetoluku, jossa vastataan tutkimuskysymyksiin sekä käydään läpi tutkielman loppupäätelmät.

2 VIRTUAALIVALUUTAT

Jotta tämän tutkielman taustateoriana voitaisiin käsitellä virtuaalivaluuttoja, tulee ensin käsitellä lohkoketjuteknologiaa, johon virtuaalivaluuttojen toiminta perustuu. Tämän teorialuvun tarkoitus ei ole pureutua syvällisesti lohkoketjuteknologian toimintaan teknisestä näkökulmasta, vaan tarjota lukijalle ymmärrys siitä, mihin virtuaalivaluuttojen toiminta ylemmällä tasolla perustuu. Teorialuvun sisältö auttaa tulkitsemaan sitä, mitkä virtuaalivaluuttojen ominaisuudet edistävät niiden käyttämistä rahanpesun välineenä.

2.1 Lohkoketjuteknologia

Lohkoketjuteknologiaa on verrattu jopa internetin kaltaiseen mullistukseen, joka vaikuttaa tulevaisuudessa lähes kaikkeen tekemiseemme. Lohkoketjuteknologian historian voidaan todeta alkaneen vuoden 2008 finanssikriisistä, jolloin perinteiset valtaapitävät instituutiot joutuivat merkittäviin ongelmiin mahdollistaen samalla uuden digitaalisen rahan esiintulon (Johansson ym. 2019, 23). Samana vuonna myös Satoshi Nakatomoto -nimimerkillä esiintynyt henkilö kirjoitti kuuluisan julkaisunsa (Nakamoto, 2008) vielä silloin täysin tuntemattomasta Bitcoin- nimisestä järjestelmästä. Nykyisistä lohkoketjuteknologian sovelluskohteista tunnetuin on virtuaalivaluutat, mutta vuodesta 2013 lohkoketjuteknologiaa on hyödynnetty ohjelmistoissa myös monilla muilla sektoreilla, esimerkiksi vakuutusalalla, valtiovallassa, mediassa ja lääketieteessä. (Bashir, 2018, 8–9.)

Eräät lähteet käyttävät lohkoketjuteknologiasta myös termiä *Distributed Ledger Technology* (DLT) eli hajautettujen tilikirjojen teknologia. Termiä käytetään erityisesti finanssisektorin sovellusten yhteydessä. Lohkoketjuteknologia ja DLT eivät ole kuitenkaan täysin synonyymejä toisillensa, sillä DLT viittaa käyttöoikeudelliseen lohkoketjuun, joita käyttävät aina tunnistetut ja luotettavat osapuolet. Hierarkkisesti määriteltynä kaikissa lohkoketjuteknologioissa käytetään hajautettujen tilikirjojen teknologiaa, mutta kaikki hajautetun tilikirjojen teknologiat eivät hyödynnä lohkoketjuteknologiaa. (Bashir, 2018, 31.) Yksinkertaistuksen vuoksi tutkielmassa käytetään pelkästään termiä lohkoketjuteknologia. Riippumatta puhutaanko termistä ”lohkoketjuteknologia” vai ”hajautettujen tilikirjojen teknologioista” on kyseessä kuitenkin uusi teknologia, joka luo pohjan virtuaalivaluuttojen toiminnalle.

2.1.1 Lohkoketju, lohko ja hajautetut tilikirjat

Termiä lohkoketju (*engl. blockchain*) käytetään monissa yhteyksissä, ja sille ei ole vakiintunut yhtä selkeää määritelmää. Oikein määritelmän löytäminen on täysin tilanteesta ja käyttötarkoituksesta riippuvaista. Yksinkertaistettu määritelmä on, että lohkoketjulla tarkoitetaan jatkuvasti kasvavaa, luotettavaa ja jaettua järjestelmää, johon voidaan kirjata ylös erilaisia tietoja. Kaikilla järjestelmän käyttäjillä on identtinen kopio järjestelmän sisältämistä tiedoista. Tietoja voidaan kirjata ylös kuitenkin vain niin, että jokainen järjestelmäkirjaukseen osallistuva taho vahvistaa tiedon muokkaamisen. (Bashir, 2018, 16.) Lohkoketjua kokonaisuudessaan voidaan ajatella kehittyneenä teknologisena versiona julkisista rekistereistä, joita on muinoin käytetty kaupungeissa ja kyläyhteisöissä kaiken tärkeän ylös kirjaamiseen kuten esimerkiksi syntymäpäivien, avioliittojen, ostojen ja myyntien sekä omaisuuden siirtojen (Johansson ym., 2019, 26–27).

Teknisempi määritelmä lohkoketjulle on vertaisverkko, joka hyödyntää kehittynyttä kryptografiaa sekä hajautettua järjestelmäarkkitehtuuria. Lisäksi se on turvallinen, läpinäkyvä ja muuttumattoman totuuden lähde. Teknisen määritelmän yksi avainsana on vertaisverkko (*engl. peer-to-peer*), jolla tarkoitetaan, ettei verkolla ole keskitettyä hallitsijatahoa, esimerkiksi pankkia, ja kaikki verkon osallistujat voivat kommunikoida vapaasti keskenään. Lohkoketjut on suunniteltu kestämään erilaisia hyökkäyksiä ja ulkopuolista manipulointia, mikä tekee niistä myös turvallisen sovelluskohteen. (Bashir, 2018, 16–17.)

Lohkoketjua voidaan siis ajatella digitaalisessa muodossa olevana tilikirjana, johon on merkitty erilaisia tapahtumia kronologisessa järjestyksessä. Lohkoketjussa esiintyvä termi ”lohko” saattaa kuitenkin olla hieman harhaanjohtava – lohkolla viitataan lähinnä tapaan, jonka avulla transaktiot liitetään toisiinsa kryptografian avulla. Lohkojen voidaan ajatella olevan tiedostoja, jotka sisältävät dataa. Lohkosta löytyy osa tai kaikki viimeisimmät lohkoketjuverkkoon lähetetyt tiedot, joita ei vielä ole sisällytetty mihinkään muuhun lohkoon. Kun lohko on täynnä eli valmis, antaa se tilaa seuraavalle lohkolle ketjussa. Esimerkiksi bitcoinin kohdalla lohkon sisältävä data on transaktiodataa. Satoshi Nakamoto käytti Bitcoin -julkaisussaan lohkoketjusta termiä ”*chain of blocks*” (Nakamoto, 2008), mutta vasta vuonna 2015 lohkoketjusta muodostui yleistermi uudelle teknologialle. (Johansson ym., 2019, 27.)

Tilikirjalla (*engl. ledger*) tarkoitetaan tapahtumarekisteriä, johon kaikki ketjussa suoritetut transaktiot tallennetaan ja josta ne voidaan tarkastaa reaaliaikaisesti kaikkien verkon eri osapuolten

toimesta (Bashir, 2018, 17). Kun tieto on kerran tallennettu tilikirjaan, sitä ei voi enää muuttaa. Hajautettua tilikirjaa voidaan puolestaan ajatella eräänlaisena jaettuna tietokantana, jota itsenäisesti toimivat osanottajat ylläpitävät. Hajautettua tilikirjaa ei hallita yhden tietyn toimijan esimerkiksi pankin keskuspalvelimen kautta, vaan jokainen tilikirjan osanottaja hallitsee omaa kopiotaan erillään muista osanottajista ja tekee tilikirjaan päivitykset muista riippumatta. Näin saadaan tilikirjasta tehtyä tehokkaasti hajautettu. Verkossa tapahtuvat transaktiot ja muutoksen tilikirjaan jaetaan kaikkien osapuolten kesken. Tämän jälkeen muodostetaan yhteisymmärrys eli konsensus siitä, miten tilikirja tulisi päivittää ja lopulta enemmistön mielipide määrittää lopullisen kirjauksen. Kun muutos uusien transaktioiden osalta on hyväksytty, tilikirja päivitetään ja jokaiselle osallistujalle jää oma identtinen kopio tilikirjasta. Transaktiot puolestaan tallennetaan kryptografian avulla allekirjoitettuun ja salattuun ketjuun, jota ei voida enää jälkikäteen muuttaa. (Johansson ym., 2019, 56–57, 267.) Kryptografialla viitataan salaustekniikkaan, jolla estetään kolmansien osapuolien pääsy salattuihin tietoihin (Bashir, 2018, 17).

2.1.2 Konsensusalgoritmit

Lohkoketjut toimivat hajautetuissa verkoissa, joissa jokaisella verkon osallistujalla voi olla identtinen kopio ketjuun kuuluvasta datasta. Mikäli joku verkon osallistuja poistuisi verkosta, tiedot säilyisivät yhä verkkoon liittyneissä laitteissa. Tästä syystä on ensiarvoiseen tärkeää, että jokaisella verkkoon osallistujalla on sama kuva siitä, miltä ketjun tilanne pitäisi kullakin hetkellä näyttää. Tilanteeseen päästään edellisessä alaluvussa kuvatun toimintamallin mukaisesti hyödyntämällä konsensusalgoritmia, jossa enemmistön päätöksellä löydetään yhteisymmärrys eli konsensus siitä, missä kukin muuttuja on tietyllä hetkellä. Konsensusalgoritmi voidaan nähdä siis lohkoketjun tärkeimpänä osana sen toimimisen kannalta. (Bashir, 2018, 17–18.)

Algoritmi määrää kirjataanko jokin tietty transaktio ketjuun tai hajautettuun tietokantaan sekä miten verkon osallistujien resurssit jaetaan eri tehtävien ja niitä suorittavien koneyksiköiden kesken. Näin ollen vaikka mukana olisi epärehellisiä toimijoita, järjestelmä toimii silti. Tähän perustuu ajatus siitä, että virtuaalivaluutat toimivat luotettavana maksuvälineenä ilman keskitettyä välitahoa kuten pankkia. Mullistava ajatus erityisesti finanssimaailman ja pankkien näkökulmasta siis on, että luottamus kehenkään yksittäiseen toimijaan ei ole tarpeen virtuaalivaluuttojen kontekstissa. (Johansson ym., 2019, 62.)

Tunnetuin virtuaalivaluutta Bitcoin hyödyntää Proof-of-Work (PoW) konsensusalgoritmia varmistaakseen verkkonsa toimivuuden. PoW perustuu verkon osallistujien tekemän laskennan

määrään sidottuna siihen kuluneeseen aikaan. Tämä johtaa puolestaan yhteisymmärrykseen siitä, mitkä transaktiot tulee liittää kussakin järjestyksessä bitcoin -tilikirjaan. Muita tunnettuja konsensusalgoritmeja ovat esimerkiksi Proof-of-Stake-algoritmi (PoS) ja Delegrated Proof-of-Stake-algoritmi (DPoS). Erona näissä algoritmeissa on tapa, jolla verkon sisäisten toimijoiden yhteisymmärrys verkon tilasta muodostetaan. (Bashir, 2018, 37–38.)

2.2 Julkiset ja yksityiset lohkoketjut

Lohkoketjuteknologiasta puhuttaessa on hyvä täsmentää, mitä tarkoitetaan lohkoketjujen ja hajautettujen tilikirjojen yhteydessä julkisilla (avoimilla) ja yksityisillä (suljetuilla) lohkoketjuilla. Yhtenevää näillä kahdella lohkoketjutyypillä on perustuminen edellä kuvattuun hajautettuun vertaisverkkoon, jossa jokainen osallistuja ylläpitää omaa kopiotaan jaetusta tilikirjasta. Merkittävimmät erot liittyvät siihen, kuka voi liittyä verkon jäseneksi, osallistua konsensusalgoritmin toimintaan ja ylläpitää jaettua tilikirjaa. (Johansson ym., 2019, 76.)

2.2.1 Julkiset lohkoketjut

Kuten jo julkisten lohkoketjujen nimi indikoi, ne ovat avoimia kaikille, jotka haluavat lukea, kirjoittaa tai liittyä julkiseen lohkoketjuverkkoon. Kuka tahansa voi siis käyttää julkista lohkoketjua lisätäkseen siihen transaktioita paikasta huolimasta, kunhan käyttäjä on liittyneenä kyseiseen verkkoon. Julkisia lohkoketjuja ei voi omistaa mikään tietty taho. (Bashir, 2018, 32.)

Julkisiin lohkoketjuihin liittyy tyypillisesti jokin kannustinmekanismi, jonka avulla saadaan kasvatettua verkon osallistujien määrää. Suurimpia julkisia lohkoketjuja ovat Ethereum ja Bitcoin – molempien kohdalla lohkoketjuja ylläpitää kymmeniä tuhansia noodeja. Noodit ovat koko lohkoketjun transaktio- tai merkintähistorian sisältäviä tietokoneita ja ne myös varmistavat lohkoketjuun tulevia uusia transaktioita. Palkkioksi noodi saa kyseisen lohkoketjuverkon sisäistä valuuttaa aina, kun ne varmistavat transaktioita. (Johansson ym., 2019, 76.)

2.2.2 Yksityiset lohkoketjut

Julkisiin lohkoketjuihin verrattuna yksityiset lohkoketjut eivät ole avoimia kaikille, vaan päästäkseen osalliseksi tällaiseen verkkoon henkilön tulee saada kutsu sekä varmentaa identiteettinsä. Kun osallistuja on hyväksytty verkon jäseneksi esimerkiksi jonkun viranomaisen

tai tietyn auktoriteetin toimesta, hän saa pääsyn hajautettuun tilikirjaan ja voi alkaa suorittamaan omaa rooliaan verkon ylläpitämisessä. (Bashir, 2018, 32; Johansson ym., 2019, 77.)

Useimmissa liiketoimintatransaktioiden suorittamiseen liittyvissä lohkoketjuissa digitaalisen identiteetin tunnistaminen on edellytys. Esimerkiksi yritys voi käyttää yksityistä lohkoketjua transaktioiden toteuttamiseen. Yksityinen lohkoketju mahdollistaa sen, että vain ja ainoastaan transaktion osapuolet voivat nähdä siihen liittyviä tietoja, pitäen kyseiseen transaktioon liittymättömät toimijat pimennossa. Eräs yksityisen lohkoketjun etu verrattuna julkiseen lohkoketjuun on myös niiden nopeus – kun lohkoketjua ylläpidetään tunnettujen toimijoiden kesken, saavutetaan konsensus lohkoihin kirjattavista merkinnöistä huomattavasti nopeammin. (Johansson ym., 2019, 78).

2.3 Virtuaalivaluutat

Ensimmäisistä talousjärjestelmistä, tai ainakin rahan käyttämisestä jossain muodossa, on löydetty merkkejä noin 2200 vuotta ennen ajanlaskun alkua. Rahan konsepti on aikojen saatossa muuttunut konkreettisista hyödykkeistä esimerkiksi viljasta ja arvometalleista kohti ei-konkretisoituvaa rahaa ja yhä edelleen paperirahaa, josta siirryttiin keskitettyyn fiat-valuuttaan. Yleisesti ottaen voidaan sanoa, että virtuaalisen rahan synty voidaan yhdistää internetin ja virtuaaliyhteisöjen kehitykseen. (Euroopan Keskuspankki, 2012, 11.)

Maailmanlaajuisen talousjärjestelmämme ja erityisesti virtuaalisen rahan historia on vielä verrattain nuori ja sen kehityksessä otetaan jatkuvasti askelia eteenpäin. Tällä hetkellä kehitys etenee kohti digitaalista ekosysteemiä, jossa rahaa ja muita vaihdannan välineitä voidaan vaihtaa tietoverkkojen välityksellä nopeasti ajasta ja paikasta riippumatta. Suurin osa maailman rahasta on jo tällä hetkellä sähköisessä muodossa. Nykyiset järjestelmät perustuvat kuitenkin pitkälti jo vanhentuneeseen ja tehottomaan teknologiaan. Tästä syystä lohkoketjuteknologia ja sen mukanaan tuomat virtuaalivaluutat ovat askel kohti uudenlaista ja kehittyneempää talousjärjestelmää. (Johansson ym., 2019, 79.)
Virtuaalivaluuttoihin kuuluva kryptovaluutta Bitcoin voidaan yleistää valtaväestön keskuudessa tunnetuimmaksi virtuaalivaluutaksi, mutta se on vain yksi tuhansien virtuaalivaluuttojen joukossa. Se ei myöskään ole ensimmäinen virtuaalivaluutta, sillä sähköistä vaihdannan yksikköä on pyritty luomaan maailmanlaajuisesti jo usean vuosikymmenen ajan. Ensimmäisenä virtuaalivaluuttana on yleisesti pidetty DigiCashia vuodelta 1992, jonka kantava ajatus pohjautui pitkälti nykyisten

virtuaalivaluuttojen tavoin siihen, ettei maksuja voitu jäljittää pankin, valtion tai muiden kolmansien osapuolten toimesta. (Johansson ym., 2019, 80.)

Virtuaalivaluuttojen yhteydessä niille annettu kritiikki liittyy usein teknologian monimutkaiseen ja valtayleisön tietämättömyyteen asiasta. Esimerkiksi väitteet siitä, että tiettyä virtuaalivaluuttaa voitaisiin tehdä loputon määrä tai henkilö voisi käyttää samaa virtuaalirahaa uudelleen kopioimalla sitä eivät pidä paikkaansa. (Johansson ym., 2019, 84). Kaksinkertaisen käytön ongelma (*double spend -problem*) on ratkaistu virtuaalivaluuttojen yhteydessä tallentamalla tiedot lohkoketjuun aikajärjestyksessä. Pankkeja tai muita keskitettyjen tilikirjojen ylläpitäjiä ei tarvita estämään kaksinkertaista käyttöä, kun lohkoketjuteknologiassa hyödynnettävä algoritmi edellyttää kaikkien transaktioiden varmistamista konsensusalgoritmin avulla. Mikäli joku yrittäisi käyttää esimerkiksi samaa bitcoinia kahdesti tekemällä kaksi toisistaan erillistä transaktiota samaan lohkoon, näitä kahta transaktiota ei koskaan verkon osallistujien toimesta varmistettaisi (Nakamoto, 2008, 8).

Jotta tässä tutkielmassa voitaisiin myöhemmin keskittyä virtuaalivaluuttoihin liittyvään rahanpesuriskiin, tulee virtuaalivaluutta käsitteenä pystyä ensin määrittelemään. Koska kyseessä on koko ajan kehittyvään lohkoketjuteknologiaan perustuva järjestelmä, on myös käsitteen määrittely muuttunut merkittävästi pelkästään viimeisen vuosikymmenen aikana. Puhekielessä havaitaan usein käytettävän termejä ”virtuaalivaluutta” ja ”kryptovaluutta” siten, että niillä pyritään tarkoittamaan samaa asiaa. Käyttötarkoituksesta ja kontekstista riippuen ne voivat viitata samaan asiaan, mutta tämän tutkielman kannalta on tarkoituksenmukaista erottaa ne erillisiksi termeiksi. Useat merkittävät toimijat niin kansallisella, eurooppalaisella ja kansainvälisellä tasolla ovat laatineet omia määritelmiään.

2.3.1 Virtuaalivaluutan määrittelyitä - Eurooppa

Ensimmäisen virallisen määrittelyn virtuaalivaluutasta teki Euroopan Keskuspankki (EKP). Virtuaalivaluutta määriteltiin digitaalisen rahan sääntelemättömäksi alalajiksi, jota hallitsee sen luonut taho ja sitä käytetään tietyn virtuaaliyhteisön sisällä (EKP, 2012, 13). EKP puhuu julkaisuissaan virtuaalivaluuttajärjestelmistä käyttäen sitä yläkäsitteenä ja kuvaa sitä konseptiksi, sillä se ottaa huomioon sekä virtuaalivaluutan arvon että transaktiot mahdollistavat mekanismit (EKP, 2015, 4). EKP kategorisoi vuonna 2012 virtuaalivaluuttajärjestelmät kolmeen kategoriaan:

1) suljettuihin virtuaalivaluuttoihin, joilla ei ole lähtökohtaisesti ollenkaan linkkiä reaalitalouteen. Virtuaalivaluuttaa ei voi vaihtaa rahaksi virtuaaliyhteisön ulkopuolella. Esimerkkinä mainitaan World of Warcraft Gold.
2) yksisuuntaisiin virtuaalivaluuttoihin, joita voidaan ostaa fiat-valuutalla, mutta ei voida vaihtaa takaisin alkuperäiseen hankintavaluuttaan. Esimerkkinä mainitaan Facebook krediitit.
3) kaksisuuntaisiin virtuaalivaluuttoihin, joissa käyttäjä voi hankkia virtuaalivaluuttaa fiat-valuutalla ja myös myydä sitä. Näillä virtuaalivaluutoilla voidaan siis ostaa sekä virtuaalisia että reaalimaailman hyödykkeitä ja palveluita. Esimerkkinä mainitaan Linden Dollarit. (EKP, 2012, 13–14.) Myöhemmin 2015 vuoden raportissaan EKP täsmensi myös Bitcoinin asemaa ja määritteli sen kuuluvan tähän kategoriaan (EKP, 2015, 9).

Vuonna 2015 EKP julkaisi päivitetyn määritelmän virtuaalivaluutasta todeten, että se on digitaalinen arvon mitta, jota ei hallitse mikään keskuspankki, luottolaitos tai e-raha instituutio. Sitä voidaan joissain tapauksissa käyttää vaihtoehtona perinteiselle rahalle, mutta vuoteen 2012 verrattuna määrittelystä oli poistettu sana ”raha”. EKP:n näkemyksen mukaan virtuaalivaluutat eivät täytä taloustieteessä määriteltyä rahan virallista määritelmää, jonka mukaan rahan tulisi olla 1) vaihdon väline 2) arvon säilyttäjä ja 3) tilin yksikkö. Virtuaalivaluuttajärjestelmien kolme kategoriaa oli pidetty ennallaan, Bitcoin määriteltynä kolmanteen kategoriaan. Määrittelystä oli myös poistettu termi ”sääntelemätön”, sillä yhä enemmissä määrin toimivallat olivat jo vuonna 2015 alkaneet sääntelemään virtuaalivaluuttojen käyttöä. (EKP, 2015, 4–23.) Sääntelyyn palataan myöhemmissä alaluvuissa tarkemmin.

2.3.2 Virtuaalivaluutan määrittelyitä – Suomi

Vuonna 2019 Suomessa tuli voimaan laki virtuaalivaluutan tarjoajista (572/2019), jonka avulla implementoidaan EU:n viidennen rahanpesudirektiivin (AMLD5) vaatimuksia kansallisella tasolla. Lain myötä on otettu käyttöön monia virtuaalivaluuttoihin liittyviä määritelmiä, mutta täsmällisesti lain mukaan virtuaalivaluutalla tarkoitetaan digitaalisessa muodossa olevaa arvoa:

a) jota keskuspankki tai muu viranomainen ei ole laskenut liikkeeseen ja joka ei ole maksuväline
b) jota henkilö voi käyttää maksuvälineenä; ja
c) jota voidaan siirtää, tallentaa ja vaihtaa säännöllisesti.

Määritelmä on hyvin pitkälti linjassa seuraavaksi esiteltävän FATF:in määritelmän kanssa, johon myös EU-lainsäädäntö nojaa. Virtuaalivaluutan tulee olla siis henkilöiden välillä hyväksytty maksuväline, mutta toisaalta sen ei tarvitse olla vaihdettavissa fiat-valuuttaan (Johansson ym., 2019, 269). Koska virtuaalivaluutoille ei löydy yksiselitteistä määritelmää, myös niiden ajantasaista määrää on vaikeaa arvioida tarkasti. Alan johtava markkinadatan tarjoaja Coinmarketcap määrittää sivuillaan (24.4.2022) ajantasaiseksi luvuksi erilaisia virtuaalivaluuttoja olevan hieman päälle 19 000 kappaletta.

2.3.3 Virtuaalivaluutan määrittelyitä – FATF

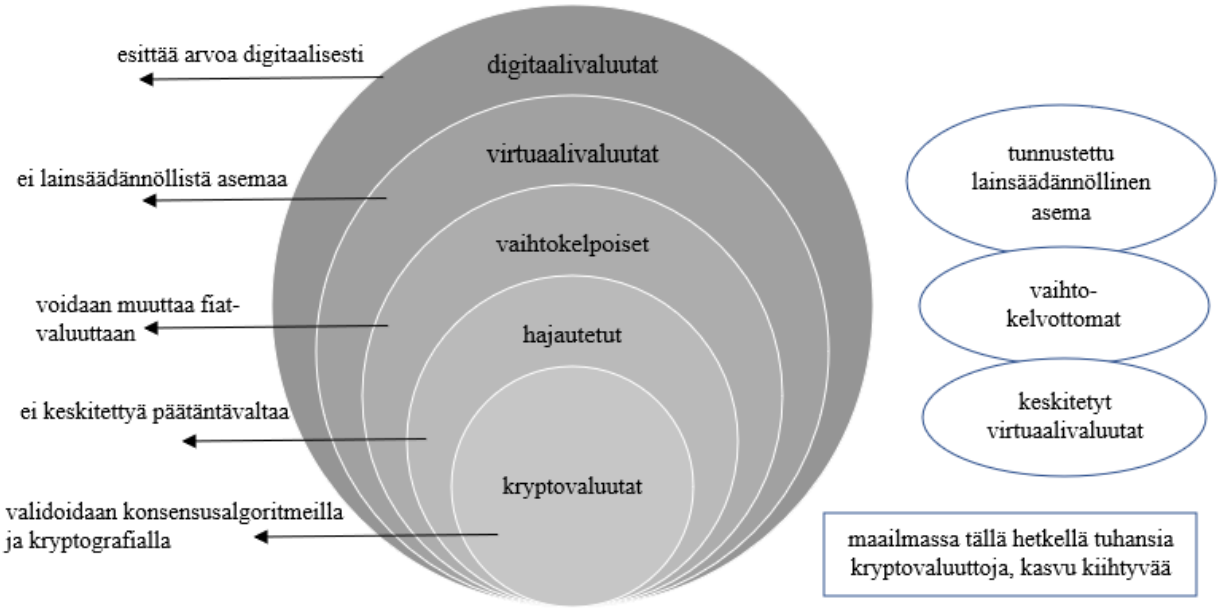
FATF on julkaissut viimeisen vuosikymmenen aikana useita virtuaalivaluuttoihin liittyviä artikkeleita sekä ohjeistuksia, jotka keskittyvät EKP:n julkaisuja enemmän virtuaalivaluuttojen aiheuttamiin riskeihin erityisesti talousrikollisuuden ja rahanpesun näkökulmasta. EKP:n tapaan myös FATF on päivittänyt määritelmiään ja luonut myös uusia käsitteitä virtuaalivaluuttamarkkinoiden kehittyessä. FATF:n käyttämä termi virtuaalivara (*engl. virtual asset*) esiteltiin ensimmäisen kerran vuonna 2018, jolloin se korvasi FATF:in virallisissa ohjeistuksissa termin virtuaalivaluutta.

Määritelmän mukaan virtuaalivaralla tarkoitetaan arvon digitaalista muotoa, jota voidaan digitaalisesti vaihtaa, siirtää tai käyttää maksuvälineenä sekä sijoitusinstrumenttina. Virtuaalivaroihin ei kuulu fiat-varojen digitaaliset muodot tai arvopaperit. (FATF, 2022, 132.) FATF:in mukaan virtuaalivarat voidaan jakaa karkeasti kryptovaroihin sekä muihin digitaalivaroihin. (FATF, 2021, 5.) Muut merkittävät instituutiot ja sääntelyviranomaiset eivät ole vielä omaksuneet termiä virtuaalivara, joten myös tässä tutkielmassa pysyttäydytään aineiston yhteneväisyyden vuoksi termin virtuaalivaluutta käytössä. Virtuaalivarojen yhteydessä FATF lanseerasi myös uuden termin virtuaalivarojen tarjoaja (*engl. virtual asset service provider*) VASP. Tällä tarkoitetaan mitä tahansa tahoa, joka joko vaihtaa virtuaalivaluuttaa fiat-valuuttaan tai toisiin virtuaalivaluuttoihin, siirtää tai säilyttää virtuaalivaluuttoja tai muutoin tarjoaa virtuaalivaluuttoihin liittyviä rahoituspalveluja (FATF, 2021, 130).

Viimeisin FATF:in määritelmä sanalle virtuaalivaluutta on vuodelta 2015, jonka mukaan virtuaalivaluutta voi toimia joko (1) vaihdon välineenä; ja/tai (2) laskennallisena yksikkönä; ja/tai (3) arvon säilyttäjänä, mutta sillä ei ole laillista maksuvälineen statusta missään oikeusjärjestelmässä. Tämä vuoden 2015 virallinen määritelmä on ehtinyt vanhenemaan viimeisen pointin osalta, sillä El Salvador otti ensimmäisenä valtiona maailmassa vuonna 2021 Bitcoinin

viralliseksi valuutakseen (HS, 2021). FATF:in kuitenkin toteaa, että virtuaalivaluutta ei ole minkään toimivallan tarjoamaa tai takaamaa ja se täyttää edellä mainitut kolme rooliansa vain ja ainoastaan sen käyttäjäjoukon keskinäisen luottamuksen ja sopimuksen ansiosta. Virtuaalivaluutta ei ole sama asia kuin internet-valuutta, mikä on fiat-valuutan digitaalinen esiintymis- ja vaihtamismuoto. (FATF, 2015, 26.)

2.4 Virtuaalivaluuttojen taksonomiaa ja jaottelua



Kuvio 3. Virtuaalivaluuttojen taksonomia. (Mukaillen He, Habermeier, Leckow, Haksar, Almeida, Kashima, Kyriakos-Saad, Oura, Sedik, Stetsenko & Verfugo-Yepes, 2016, 8.)

Kuviosta kolme nähdään tarkemmin virtuaalivaluuttoihin liittyvää taksonomiaa, jonka on määritellyt kansainvälinen valuuttarahasto IMF. Sen avulla on helpompi ymmärtää virtuaalivaluuttojen asemaa suhteessa kryptovaluuttoihin sekä saada parempi kuva siitä, millaisiin erilaisiin alalajeihin virtuaalivaluutat voidaan jakaa. Digitaalivaluutalla tarkoitetaan virtuaalivaluutan tai internet-valuutan ilmentymää (FATF, 2014, 4). Termejä digitaalivaluutta ja virtuaalivaluutta käytetään usein haitallisesti sekaisin, mutta kuten kuviosta kolme havaitaan, ne eivät tarkoita samaa asiaa. Kuviosta kolme nähdään myös tämän tutkielman kannalta olennainen näkökulma: kaikki kryptovaluutat ovat virtuaalivaluuttoja, mutta kaikki virtuaalivaluutat eivät ole kryptovaluuttoja. Kryptovaluuttoja käsitellään myöhemmin alaluvussa 2.5.

2.4.1 Vaihtokelpoiset vs. vaihtokelvottomat virtuaalivaluutat

Virtuaalivaluutat jaetaan perinteisesti kahteen eri perustyyppiin: vaihtokelpoisiin *(engl. convertible*) ja vaihtokelvottomiin (*engl. non-convertible*). On tärkeää huomioida, että virtuaalivaluuttojen kohdalla termi ”vaihtokelpoinen” ei viittaa lain turvaamaan asemaan vaan yksityisten tahojen mahdollistamaan vaihtokelpoisuuteen. Virtuaalivaluutta on siis niin kauan vaihtokelpoinen, kun yksityiset osallistujat tekevät vaihtamisesta tarjouksia ja hyväksyvät niitä. Vaihtokelpoisella (tai avoimella) virtuaalivaluutalla on yhtenevä arvo oikean valuutan kanssa ja sitä voidaan vaihtaa edestakaisin oikean valuutan kanssa. Esimerkkejä vaihtokelpoisista virtuaalivaluutoista ovat Bitcoin, e-Gold, Second Life Linden Dollarit ja WebMoney. (FATF, 2015, 27.)

Vaihtokelvottomat (tai suljetut) virtuaalivaluutat ovat tarkoitettu käytettävän tietyillä virtuaali-domaineilla tai -maailmoissa kuten esimerkiksi Amazon.com -verkkosivustolla tai Massively Multiplayer Online Role-Playing Game -alustoilla. Vaihtokelvottomia virtuaalivaluuttoja ei voi vaihtaa oikeaksi valuutaksi niitä hallitsevien tahojen sääntöjen takia. Tällaisesta voidaan mainita esimerkkeinä Q Coins sekä World of Warcraft Gold. On kuitenkin huomioitava, että vaihtokelvottomille virtuaalivaluutoille on olemassa epävirallisia sekundäärisiä black-market vaihdanta-alustoja, jolloin vaihtokelvottomasta virtuaalivaluutasta tulee tosiasiassa oikeaksi valuutaksi muutettavaa vaihtokelpoista virtuaalivaluuttaa. (FATF, 2015, 27.)

2.4.2 Keskitetyt vs. hajautetut virtuaalivaluutat

Kaikki vaihtokelvottomat virtuaalivaluutat ovat keskitettyjä, sillä vaihtokelvoton virtuaalivaluutta on aina jonkin tahon luomaa ja tarjoamaa, joka myös määrää niitä koskevista säännöistä (FATF, 2015, 27). Vastavuoroisesti vaihtokelpoinen virtuaalivaluutta voi kuulua joko kahteen alakategoriaan: keskitettyihin (*engl. centralized*) tai hajautettuihin (*engl. non-centralized*) virtuaalivaluuttoihin.

Keskitetyillä virtuaalivaluutoilla on olemassa kutakin valuuttaa hallitseva päätäntävalta, joka vastaa yksittäiseen virtuaalivaluuttaan liittyvien sääntöjen määrittelystä ja hallitsee virtuaalivaluuttaan liittyvää keskitettyä tilikirjaa. Päätäntävallalla on myös mahdollisuus lakkauttaa virtuaalivaluutta. Keskitetyn virtuaalivaluutan arvo voi olla joko kelluva, jolloin sen arvo määrittyy markkinoilla kysynnän ja tarjonnan mukaisesti. Arvo voi myös olla sidottu johonkin oikeaan valuuttaan tai esimerkiksi kultaan, jolloin arvon on päättänyt virtuaalivaluuttaa

hallitseva päätäntävalta. Suurimpaan osaan virtuaalivaluuttatransaktioista liittyvät keskitetyt virtuaalivaluutat. Esimerkkejä keskitetyistä virtuaalivaluutoista ovat esimerkiksi PerfectMoney, WebMoney sekä World of Warcraft Gold. (FATF, 2015, 27.)

Hajautetuilla virtuaalivaluutoilla tarkoitetaan puolestaan tyypillisesti virtuaalivaluuttojen tunnetuinta alalajia: kryptovaluuttoja. Tämän tutkielman kannalta niitä käsitellään kokonaan omassa alaluvussaan 2.5.

2.5 Kryptovaluutat

”What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.” - Satoshi Nakamoto, 2008

Yllä oleva sitaatti on Satoshi Nakatomoto -nimimerkin vuoden 2008 kirjoittamasta uraauurtavasta artikkelista, jossa esiteltiin ensimmäisen kerran kryptovaluutta Bitcoin. Kyseinen sitaatti tiivistää kryptovaluuttojen perusajatuksen – haluttiin luoda tehokas ja turvallinen vaihtoehto keskitettyjen päättäjien ja finanssitahojen hallinnoimalle fiat-valuutalle niin, että maksut kulkisivat suoraan lähettäjältä vastaanottajalle. Kyseisen artikkelin julkaisun jälkeen kryptovaluuttojen evoluutio on vähitellen alkanut herättää laajempaa akateemista kiinnostusta. Vuonna 2013 löytyi vain kaksi merkittävää vertaisarvioitua tutkimusta liittyen kryptovaluuttoihin, mutta nykyään niitä löytyy sadoittain. (Corbet, Lucey, Urquhart & Yarovaya, 2019, 183.)

Perinteisesti kryptovaluutalla tarkoitetaan matemaattisperusteista, hajautettua ja vaihtokelpoista virtuaalivaluuttaa, joka on suojattu salaustekniikalla. Kryptovaluutta nojaa julkisiin ja yksityisiin avaimiin siirtäessään arvoa yhdeltä entiteetiltä toiselle ja jokaisen siirron tulee olla salaustekniikalla allekirjoitettu. Kryptovaluutan tilikirjojen turvallisuus, koskemattomuus ja tasapaino on varmistettu tasapuolisesti epäluottavien tahojen joukon toimesta. (FATF, 2015, 27–28.) Kryptovaluutat ovat siis eräänlainen elektronisen rahan vertaisverkko, jonka avulla maksuja voidaan tehdä ilman keskitettyä hallintatahoa. Ei ole olemassa kryptovaluutta sääntelevää keskustahoa, joka voisi suoraan vaikuttaa esimerkiksi niiden arvoon tai liikkeellä olevaan määrään. Kryptovaluutoilla ei ole fyysistä muotoa, joten niitä voidaan jakaa lähes rajattomasti. (Corbet ym. 2019, 182.) Kryptovaluuttoja voidaan käyttää kansainvälisesti lähes rajoituksetta ja

niitä pidetään turvallisina, mutta ne ovat myös erittäin volatiileja. Päivittäiset arvonvaihtelut 10 ja 100 %:n välillä ovat normaaleja useimmille kryptovaluutoille. (Teichmann & Falker, 2020, 503.)

Vaikka perinteisissä akateemisessa kirjallisuudessa sekä viranomaisten määrittelyissä kryptovaluutat mielletään hajautetuiksi, on uudempana ilmiönä markkinoille ilmestynyt myös keskitettyjä kryptovaluuttoja. (Teichmann & Falker, 2020, 503.) Keskitettyjä kryptovaluuttoja ovat esimerkiksi stablecoinit, jotka ovat yksi kryptovarojen alakategoria. Niiden arvo on tyypillisesti sidottu johonkin fiat-valuuttaan, mikä tekee niistä vähemmän volatiileja kuin hajautetuista kryptovaluutoista. Kuuluisin esimerkki keskitetystä kryptovaluutasta on Facebookin (nykyisin Meta) kryptovaluuttaprojekti Libra. (Arner, Auer & Frost, 2020, 6; Giudici, Leach, Pagnottoni, 2022, 4.)

2.5.1 Bitcoin

Bitcoin voidaan määritellä joko protokollaksi, digitaaliseksi valuutaksi tai alustaksi (Bashir, 2018, 134). Tässä tutkielmassa sitä käsitellään pääosin digitaalisena valuuttana, jolloin sen kirjoitusasu on *bitcoin*. Laajemmassa, itse konseptia tai protokollaa käsittelevässä yhteydessä kirjoitusasu on *Bitcoin.*

Bitcoin on hajautettu vaihtokelpoinen virtuaalivaluutta eli kryptovaluutta. Sitä pidetään myös ensimmäisenä kryptovaluuttana, koska se on ensimmäinen lohkoketjuteknologian onnistunut käyttökohde. Bitcoinin toimintalogiikka hyödyntää vuosikymmenien aikana syntynyttä tietoutta ja tutkimuksia kryptografiasta ja digitaalirahasta. (Bashir, 2018, 129.) Se tuli toiminnalliseksi vuoden 2009 tammikuussa. Bitcoinilla ei ole keskitettyä kirjanpitoa ja kaikki tilisiirrot kirjataan julkiseen tilikirjaan. (Donet, Perez-Sola, Herrera-Joancomart, 2014, 87–88.) Bitcoinit ovat laskentayksiköitä, jotka koostuvat ainutlaatuisista numero- ja kirjainjonoista, jotka puolestaan muodostavat valuuttayksiköitä. Näillä valuuttayksiköillä on arvoa vain siksi, että yksittäiset käyttäjät ovat valmiita maksamaan niistä. Bitcoineilla käydään kauppaa korkealla anonymiteetillä ja niitä voidaan vaihtaa fiat-valuutaksi tai toisiksi virtuaalivaluutoiksi. Kuka tahansa voi ladata ilmaisen, avoimen lähdekoodin ohjelmiston internetistä lähettääkseen, vastaanottaakseen tai säilöäkseen bitcoineja ja valvoakseen bitcoin -transaktioita. (FATF, 2015, 28.) Näitä ohjelmistoja kutsutaan noodeiksi (*engl. node*), joissa tarkoitetaan yksittäistä toimijaa hajautetussa systeemissä (Bashir, 2018, 12). Noodi voi siis olla esimerkiksi pöytäkoneelle asennettu Bitcoin core -asiakasohjelma tai serveri (Bashir, 2018, 167–168), kun taas ohjelmiston kautta transaktioita

vahvistavaa eli bitcoinien louhintaa suorittavaa ihmistä kutsutaan termillä louhija (*engl. miner*) (FATF, 2015, 30).

Kuluttajan näkökulmasta Bitcoinin etuja on matalat transaktiokulut, anonymiteetti sekä sen immuniteetti hakkeroinnille (Teichmann & Falker, 2020, 502). Bitcoin syntyi liberaalin ideologian pohjalta, jossa Bitcoinia voitaisiin käyttää maksualustana pankkien sijasta. Pankkien ajateltiin saaneen liikaa valtaa ja Bitcoinin haluttiin olevan täysin anonyymiä ja riippumatonta luotettavasta kolmannesta osapuolesta. Tämä kuitenkin on ristiriidassa monien yritysten liiketoiminnan kanssa, jossa sääntely vaatii tehokkaita KYC-toimenpiteitä ja yksityiskohtaista tietoa yrityksen maksuliikenteestä. Tämä voidaan nähdä yhtenä syynä Bitcoinin suosion rajoittuneisuudelle virallisissa yhteyksissä. (Bashir, 2018, 133.) Tämän ajatuksen pohjalta on herännyt keskustelua, oliko Bitcoin alun perinkin luotu tahattomasti liian tehokkaaksi alustaksi rikolliselle toiminnalle. Tähän palataan tutkielman luvussa 4.

2.5.2 Bitcoinien louhinta

Kun uusi noodi on yhdistynyt bitcoin -verkkoon, se saa lohkoketjusta käyttöönsä täydellisen version ja se voi alkaa suorittamaan bitcoin -transaktioiden validointia ja louhintaa proof-of-work konsensusalgoritmin avulla. Louhinnalla tarkoitetaan prosessia, jossa uudet lohkot lisätään lohkoketjuun. Lohkot puolestaan koostuvat transaktioista, jotka validoidaan proof-of-work konsensusalgoritmin kautta louhintaprosessin yhteydessä. Uusien lohkojen lisääntyessä, myös uusien bitcoinien määrä lisääntyy. (Bashir, 2018, 167.)

Mikäli myös kaikki muut konsensusalgoritmiin osallistuvat noodit hyväksyvät saman transaktion kuin louhija, saa louhija palkkioksi tietyn määrän bitcoineja. Tällä tavalla saadaan kannustin louhijalle toimia luotettavana toimijana ja pidetään yllä tehokasta bitcoin -verkostoa. (Bashir, 2018, 168–169.) Ohjelmaa, joka säilöö täyden kopion lohkoketjusta, kutsutaan termillä *full node*. *Lightweight node* puolestaan sisältää lohkoketjun vain osittain ja niiden pääasiallinen rooli liittyy transaktioiden vahvistamiseen. (Teichmann & Falker, 2020, 502.) Full node muun muassa toimii lompakkona, louhii sekä säilöö kopion lohkoketjusta (Bashir, 2018, 180). Suomessa on väkilukuun suhteutettuna verrattain aktiivinen bitcoin -verkosto, sillä aktiivisia (full) noodeja oli vuoden 2022 alussa 218 kappaletta, mikä on 7. eniten maailmassa (bitnodes, 2022).

Yksinkertaistettu esimerkki yhden bitcoin -siirron tapahtumisesta:

1. Henkilö A haluaa siirtää henkilölle B bitcoineja

2. Siirrosta luodaan tapahtuma lohkoon
3. Transaktio menee hyväksyttäväksi kaikille bitcoin -verkkoon kuuluville noodeille
4. Siirto vahvistetaan noodien toimesta, jotka saavat palkkioksi tietyn määrän bitcoinia siirron vahvistuksesta
5. Siirto lukitaan osaksi lohkoa ja lohko päivittyy lohkoketjuun
6. Henkilön A lähettämä siirto henkilölle B on saatettu loppuun

Kuten pankkienkin toteuttamissa transaktioissa, myös bitcoin -transaktioista aiheutuu käyttäjälle kuluja. Louhijat veloittavat bitcoin -siirroista aiheutuvat transaktiokulut, jotka riippuvat transaktion koosta. Kuluja käytetään, koska ne toimivat kannustimena louhijalle liittää käyttäjän tekemä transaktio osaksi lohkoa (Bashir, 2018, 151). Tammikuussa 2022 transaktiokulu oli 1,67 Yhdysvaltain dollaria per bitcoin -transaktio (Ycharts, 2022). Kirjoitushetkellä yhden bitcoin -transaktion toteuttaminen kestää keskimäärin noin 10 minuuttia (Coinmarketcap.com, 2021).

2.5.3 Kryptovarat

FATF:in vuoden 2018 lanseeraaman termin virtuaalivarat pohjalta on syntynyt myös termi kryptovarat. Kryptovaroilla tarkoitetaan niitä virtuaalivaroja, jotka hyödyntävät kryptografiaa sekä hajautetun tilikirjan teknologiaa. (Pavlidis, 2020, 1.) Tarve uudelle termille on noussut esiin pohdittaessa eri kryptovaluuttojen saatavuutta. Esimerkiksi bitcoinin louhintaa ei ole mahdollista jatkaa ikuisesti – joidenkin arvioiden mukaan viimeinenkin mahdollinen bitcoin on louhittu vuoteen 2140 mennessä (Hayes, 2022). Bitcoinin (21 miljoonaa) sekä muiden kryptovaluuttojen rajattu määrä rajoittaa niiden toimimista tehokkaana maksutapana. Tästä syystä on järjestetty niin kutsuttuja ICO:ja (Initial Coin Offering), joiden tarkoituksena on kerätä kryptovaluuttojen kehittämiseen varoja fiat-valuuttojen sektorilta. Näin ollen kryptovaluutan arvoa saadaan nostettua louhinnasta riippumattomilla keinoilla. (Nair, 2019, 86.) ICO:jen seurauksena kryptovaluutat ovat muuttumassa yhä enemmissä määrin spekulatiivisiksi varoiksi kuin maksuvälineiksi ja termi kryptovara on ottanut paikkansa. Finanssivalvonta (2019) on täsmentänyt asiaa toteamalla, että ”bitcoinia ja muita virtuaalivaluuttoja voidaan pitää eräänlaisena varallisuuden muotona, mutta vain niin kauan, kun niillä on toimivat markkinat.”

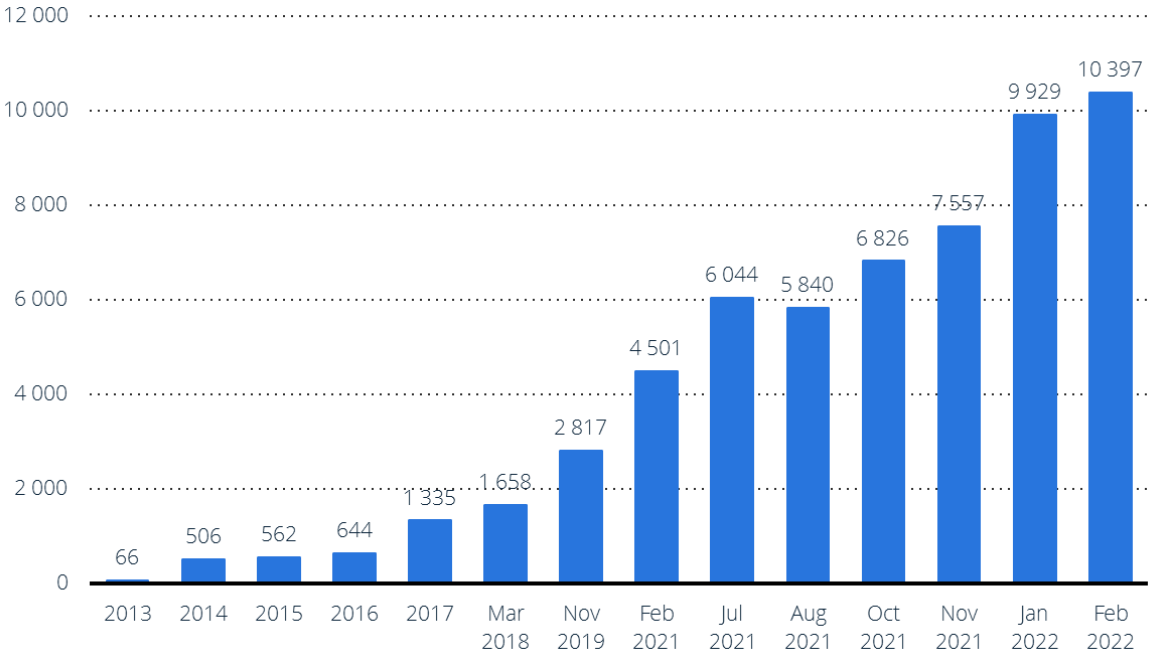
Eri kryptovaluutat voidaan luokitella kuuluvaksi tiettyyn kryptovarojen alakategorioihin. Tällä hetkellä voidaan erotella seitsemän erilaista kryptovarojen tyyppiä: monero, stablecoin, CBDC, privacy coin, governance token, utility token ja NFT (non-fungible token) (Sephton, 2021). Kryptovarojen termi on myös elänyt viime vuosina, sillä vielä vuonna 2019 Euroopan

pankkiviranomainen EBA luokitteli kryptovaroille vain kolme alakategoriaa (EBA, 2019, 5–7). Merkittävä huomio virtuaali- ja kryptovaluuttoihin liittyvän toimintaympäristön jatkuvasta muutoksesta on esimerkiksi se, ettei Finanssivalvonta ole päivittänyt virtuaalivaluutan määritelmää ja kryptovarojen luokittelua vuoden 2019 jälkeen – osa siis Suomessa virtuaalivaluuttojen valvonnasta vastaavan valvontaviranomaisen antamista tiedoista ovat vanhentuneita. (Finanssivalvonta, 2019.) Tässä tutkielmassa kryptovaroilla ja kryptovaluutoilla tarkoitetaan yksinkertaistuksen vuoksi samaa asiaa. Virtuaalivaluutat ovat kuitenkin sekä kryptovaroja että kryptovaluuttoja laajempi käsite, kuten kuviossa kolme tuotiin ilmi.

2.5.4 Kryptovaluuttojen määrä ja kryptovaluuttojen vaihdantapalvelut

Siinä, missä virtuaalivaluuttaa ja kryptovaluuttaa käytetään keskenään virheellisesti synonyymeinä, myös Bitcoinia käytetään usein kryptovaluutan synonyyminä. Kryptovaluuttoja on kuitenkin olemassa paljon muitakin kuin vain Bitcoin. Lokakuun 2021 lopussa maailmassa oli 6987 erilaista kryptovaluuttaa, ja joka päivä markkinoille syntyy kymmeniä uusia valuuttoja. Tammikuussa 2022 eri kryptovaluuttoja oli olemassa jo noin 10 000 kappaletta. Kryptovaluuttojen määrän kasvu kiihtyi entisestään erityisesti vuoden 2021 aikana jatkuen vuoteen 2022, kuten nähdään kuvasta 3. Markkina-arvoltaan viisi suurinta kryptovaluuttaa ovat kirjoitushetkellä huhtikuussa 2022 Bitcoin, Ethereum, Binance Coin, Tether ja USD Coin. (Coinmarketcap.com).

Koko kryptovaluuttamarkkinan markkina-arvo oli tammikuun 2022 alussa noin 2,4 biljoonaa Yhdysvaltain dollaria. Markkina-arvo kuvastaa kryptovaluutan kaikkien louhittujen yksiköiden kokonaisarvoa. Se lasketaan kertomalla kryptovaluuttayksiköiden määrä yksittäisen kryptovaluutan sen hetkisellä markkinahinnalla. Marraskuussa 2021 markkina-arvo ylitti kolmen biljoonan dollarin rajan ensimmäisen kerran. (Statista, 2022a.)



Kuvio 4. Erilaisten kryptovaluuttojen määrä 2013–2022 (Statista, 2022b).

FATF käytti vielä vuonna 2015 kryptovaluuttojen vaihdantapalvelusta nimitystä ”exchanger” (FATF, 2015, 29), mutta nykyisin FATF käyttää myös kryptovaluuttojen vaihdantapalveluista termiä ”Virtual Asset Service Provider” eli VASP. Alaluvussa 2.3 annetun määritelmän lisäksi VASP voi mahdollistaa osallistumisen ICO:ihin. (FATF, 2021, 130.) Initial Coin Offering (ICO) voidaan määritellä avoimeksi kasvuyrityksien rahoitusmalliksi, joissa rahaa kerätään kryptovaluuttoina. Vastineeksi yritys tarjoaa luomaansa virtuaalivaluuttaa eli ”tokeneita”, joita voidaan myydä internetissä tai käyttää tulevaisuudessa tuotteiden, palveluiden ja tuottojen hankkimiseen. (Adhami, Giudici, Martinazzi, 2018, 64–66.) Huhtikuussa 2022 maailman suurimmat kryptovaluuttojen vaihdantapalvelut olivat Binance, Coinbase Exchange, FTX sekä Kraken (Coinmarketcap.com, 2022).

2.5.5 Kryptovaluuttojen säilyttäminen ja kryptovaluuttalompakot

FATF:in mukaan lompakontarjoaja on entiteetti, joka tarjoaa digitaalisia virtuaalivaluuttalompakoita. Lompakko sisältää käyttäjän yksityiset avaimet, jotka mahdollistavat käyttäjälle käyttää sellaisia virtuaalivaluuttoja, jotka ovat kohdennettuja tiettyyn virtuaalivaluuttaosoitteeseen lohkoketjussa. Lompakontarjoaja ylläpitää käyttäjän virtuaalivaluuttavarantoja ja tarjoaa säilytystilaa sekä varmistaa transaktioiden turvallisuuden esimerkiksi erilaisten salausavaimien kautta. (FATF, 2015, 30.)

Bitcoinien (ja muiden kryptovaluuttojen) säilyttämiseen tarkoitettu kryptovaluuttalompakko (*engl. wallet*) on laite tai ohjelmisto, joka on yhteydessä lohkoketjuun. Lompakko sisältää julkisesta ja yksityisesti avaimesta koostuvan avainparin sekä lompakon kautta tapahtuneet transaktiot. Avaimia käytetään lähettämään ja vastaanottamaan kryptovaluuttoja ja ne koostuvat joukosta kirjaimia ja numeroita. Julkinen avain annetaan maksajalle vastaanottajan identifioimiseen ja yksityisiä avaimia käytetään transaktioviestien luomiseen sekä transaktioiden vahvistamiseen. Julkinen avain siis kertoo lompakon osoitteen ja toimii ikään kuin tilinumerona, kun taas yksityinen avain todistaa lompakon omistajuuden. (Eskandari, Barrera, Stobert, Clark, 2015, 1–4; Teichmann & Falker, 2020, 503.) Kryptovaluuttalompakoita on neljää eri päätyyppiä: puhelimeen tai tietokoneelle ladattava *software wallet*, puhtaasti kryptovaluuttojen säilytykseen tarkoitettu *hardware wallet*, vaihdantapalveluiden oma *web wallet* ja fyysiseen avainpariin perustuva *paper wallet* (Bitcoin.com, 2022).

2.6 Virtuaali- ja kryptovaluuttojen sääntely

"Regulation is probably one of the biggest overhangs in the crypto industry globally. We would very much welcome clear regulation." -Jeffrey Wang (2020)

Moni virtuaalivaluuttatoimija on peräänkuuluttanut selkeämpää ja yhtenäisempää lainsäädäntöä virtuaalivaluuttamarkkinoiden ympärille, sillä virtuaalivaluuttoja ei tällä hetkellä sääntele tai valvo mikään riippumaton ja luotettava kolmas taho. Yhtenäisen standardin syntymiseen liittyy kuitenkin omat haasteensa: kaikille innovatiivisille uusille teknologioille, kuten lohkoketjuteknologialle ja sen sovelluksille, on yhteistä, että ne kehittyvät nopeammin kuin niihin liittyvä lainsäädännöllinen viitekehys. Tämä johtaa sekä pätevän lainsäädännön syntymisen pitkittymiseen että tilanteeseen, jossa lainsäädäntö jo julkaistessaan on mahdollisesti vanhentunutta. (Teichmann & Falker, 2021, 775–776.)

Kiina ilmoitti syksyllä 2021, että kaikki kryptovaluuttoihin liittyvät transaktiot ovat jatkossa laittomia. Tämän seurauksena kryptovaluuttoihin liittyvän kaupankäynnin määrä Kiinassa romahti ja myös suurimpien kryptovaluuttojen kurssit kokivat rajuja pudotuksia (Yle Uutiset, 2021). Uutisen seurauksena kryptovaluuttojen louhinta lisääntyi erityisesti Venäjällä. Venäjän keskuspankki kuitenkin ilmoitti tammikuussa 2022 haluavansa kieltää sekä louhinnan että kryptovaluuttatransaktiot. (Bloomberg, 2022.) Myös Turkki ja Intia ovat ottaneet isoja lainsäädännöllisiä askeleita kohti kryptovaluuttojen käyttämisen ja omistamisen kieltämistä (Orji,

2022). Muualla maailmassa asialle ei ole saatu yhtä selkeää rajanvetoa: Yhdysvaltojen keskuspankin Federal Reserven pääjohtaja Jerome Powell on todennut, että heillä ei ole aikomusta kieltää Kiinan lailla kryptovaluuttatoimintaa. Samanaikaisesti Yhdysvaltain arvopaperi- ja pörssikomission (United States Secuirity and Exchange Commission) johtaja Gary Gensler taas on todennut, että sekä heillä että hyödykkeiden vaihdosta vastaavalla Commodity Futures Trading komissiolla (CFTC) on vahva vastuu toimialan sääntelyn lisäämisestä. Genslerin ja Powellin kommenteissa on kuitenkin yhteinen näkemys presidentti Bidenin hallinnon ja muiden Yhdysvaltain lainsäätäjien kanssa, että kryptovaluuttoihin liittyvää sääntelyä on joka tapauksessa lisättävä nykyisestään. Tiukemmalla sääntelyllä Yhdysvalloissa haluttaisiin myös edesauttaa ihmisten tietoutta siitä, miten kryptovaluuttoja tulisi esimerkiksi kirjata verottajalle. Systemaattinen raportointitapa taas mahdollistaisi amerikkalaisten tekemien kryptovaluuttatransaktioiden tehokkaamman seurannan. (Haar, 2022.)

Suomen kontekstissa virtuaalivaluutoilla tapahtuvan kaupankäynnin rajoittamisesta ei ole ollut merkittävää keskustelua. Suomessa virtuaalivaluutoista saatava tulo on verotettavaa tuloa tuloverolain 45 §:n 1 momentin mukaisesti. Verohallinnon antaman arvion (2020) mukaan viranomaisten osaaminen, analyysityökalujen ja resurssien saatavuus ei ole Suomessa vielä sillä tasolla, että virtuaalivaluuttojen hyödyntämistä rikollisuudessa voitaisiin torjua tehokkaasti. Tähän myötävaikuttaa vahvasti virtuaalivaluuttoihin liittyvän sääntelyn tuoreus – sääntelyn käyttöönotto ja tulkinta on maailmassa vasta alkutekijöissään ja Suomen lainsäädäntö nojaa vahvasti EU-tasoiseen lainsäädäntöön (Verohallinto, 2020.)

Finanssivalvonta vastaa Suomessa virtuaalivaluuttapalveluiden viranomaisvalvonnasta (Laki virtuaalivaluutan tarjoajista 572/2019). Keskusrikospoliisin Rahanpesun selvittelykeskuksen vastuulla on pyrkiä estämään, selvittämään, paljastamaan ja saattamaan esitutkinnan piiriin virtuaalivaluuttoihin liittyviä rikoskokonaisuuksia. Vaikka tehokkaan kansainvälisen sääntelyn käyttöönotossa on haasteita, on viime vuosina tapahtunut myös positiivista kehitystä. Suomessa virtuaalivaluuttojen ja lompakkopalveluiden tarjoajilla on velvollisuus rekisteröityä Finanssivalvonnalle ja muille finanssialan valvontaviranomaisille. Laki virtuaalivaluutan tarjoajista (572/2019) mahdollistaa virtuaalivaluuttojen suomalaisilta tarjoajilta kerättyjen tietojen laadun ja yksityiskohtaisuuden parantumisen. Toisaalta ilmiö voi myös aiheuttaa sen, että tietyt asiakasryhmät siirtyvät käyttämään ulkomaisia virtuaalivaluuttojen tarjoajia tiukentuneen lainsäädännön seurauksena (Verohallinto, 2020.)

Laki virtuaalivaluuttojen tarjoajista edellyttää, että myös virtuaalivaluutan tarjoajan on pankkien tapaan tunnettava asiakkaansa. KYC (Know Your Customer) -toiminnoilla tarkoitetaan kansalliseen ja kansainväliseen sääntelyyn sisältyviä velvoitteita tuntea asiakkaansa estääkseen ja ennaltaehkäistäkseen rahanpesua ja terrorismin rahoittamista. Lain (572/2019) mukaan virtuaalivaluutan tarjoajan on ”tunnistettava asiakkaan todellinen edunsaaja ja henkilö, joka toimii asiakkaan lukuun, sekä lisäksi tarvittaessa todennettava näiden henkilöllisyys”. Laissa myös todetaan, että ”virtuaalivaluutan tarjoajalla on oltava riittävät riskienhallintajärjestelmät, joilla se voi arvioida asiakkaista toiminnalleen aiheutuvia riskejä”.

3 PANKIN RAHANPESURISKI JA RAHANPESUN ESTÄMINEN

Rahanpesulla tarkoitetaan rikollisilla keinoilla hankittujen varojen muuttamista sellaiseen muotoon, jossa varojen alkuperää ei saada yhdistettyä alkuperäiseen rikokseen (Reuter & Truman, 2004, 1). Rahanpesu on moniulotteinen ilmiö, joka liittyy laajasti monenlaiseen rikollisuuteen. Tässä teorialuvussa pyritään kuvaamaan rahanpesua ilmiönä ja sen estämistä tutkielman taustateorian roolissa. Teorialuvun jälkipuolella keskitytään pankin rahanpesuriskiin sekä rahanpesun estämiseen pankin riskienhallinnan näkökulmasta.

3.1 Rahanpesu ilmiönä

Rahanpesun ilmiönä voidaan nähdä saaneen alkunsa yhdysvaltalaisen mafian alkuajoista – nauttiakseen rikollisesta rahasta sitä haluttiin myös käyttää. Jotta rikollisten varojen alkuperä saatiin näyttämään oikealta, niillä hankittiin muun muassa kiinteistöjä ja sijoitettiin lailliseen liiketoimintaan. Alun perin Yhdysvalloissa 1970 -luvulla rahanpesuun ilmiönä ja sen torjumiseen keskityttiin, sillä haluttiin välttää ulkomaisten pankkien käyttäminen veronkierron välineenä. (Levi, Reuter, 2006, 290.) Nopeasti kuitenkin huomattiin, että rahanpesun estämisen kontrolleista tuli myös tärkeä osa taistelussa siihen aikaan valtavasti kukoistanutta huumekauppaa vastaan. Rahanpesu tuomittiin laittomaksi Yhdysvalloissa ensimmäinen kerran vuonna 1986, sillä huumekaupan kannattavuutta haluttiin rajoittaa. (Teichmann & Falker, 2020, 501.)

Rahanpesu itsessään ei ole useinkaan tekijän ainoa ja yksittäinen rikos, vaan se seuraa muita esirikoksiksi kutsuttuja rikoksia (Levi & Reuter, 2006, 292). Rahanpesuun liitettäviä rikostyyppejä ovat esimerkiksi varkaus, petos, terrorismi ja huumekauppa (Chapman, 2018, 2; Reuter, 2005, 4). Rahanpesua on näistä rikoksista saatujen varojen näennäisesti lailliseksi tekeminen. Suomen rikoslaissa käsitellään rahanpesun aihepiiriä muun muassa termein kätkemisrikos ja rahanpesu. Rahanpesulla tarkoitetaan rikoslain mukaan toimintaa, jossa henkilö ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää, välittää tai pitää hallussaan rikoksella hankittua omaisuutta, rikoksen tuottamaa hyötyä tai näiden tilalle tullutta omaisuutta hankkiakseen itselleen tai toiselle hyötyä tai peittääkseen tai häivyttääkseen hyödyn tai omaisuuden laittoman alkuperän tai avustaakseen rikoksentekijää välttämään rikoksen oikeudelliset seuraamukset. Rikoslaki tuntee siis myös esimerkiksi tuottamuksellisen rahanpesun, jolla tarkoitetaan edellä mainittujen toimien täytäntöönpanoa johtuen omasta huolimattomuudesta. (Rikoslaki 1889/39, 2003, luku 32.)

Rahanpesuun saatetaan tyypillisesti käyttää paljon aikaa ja eri kerroksia rahan alkuperän naamioiseksi saattaa olla useita. Itse rahanpesutekniikoiden ei kuitenkaan tarvitse olla monimutkaisia – rahanpesua voi olla lompakkovaras käyttämässä varastamiaan seteleitä katukaupassa tai pimeää työtä tehnyt työläinen kuluttamassa palkkarahojaan maksamatta asiaankuuluvia veroja. Kun rikos on suoritettu ja siitä on hyödytty rahallisesti, kaikki tätä seuraavat vaiheet voidaan luokitella rahanpesuksi. (Chapman, 2018, 2.)

Perinteisen rahanpesun määrittelyn kohdalla täytyy muistaa, että se ei ota huomioon kaikkia rahanpesuun liittyviä näkökulmia. Näitä ovat esimerkiksi veronkierron helpottaminen, korkean markkina-arvon tuotteiden maksaminen käteisellä, todellisten edunsaajien piilottaminen pöytälaatikkoyritysten taakse, suurien käteismäärien ”smurffaaminen” eli tallettaminen pienissä osissa sekä näiden varojen nostaminen, laittomasti hankittujen varojen sekoittaminen käteispainotteiseen lailliseen yritystoimintaan kuten kukkakauppaan ja ravintoloihin sekä rahanpesu uhkapelaamisen kautta. Rahanpesun toteutumiseen ei tarvita myöskään aina rahaa. Mikä tahansa rikoksella saatu hyödyke kelpaa rahanpesun välineeksi. Esimerkiksi työpaikalta tuotteiden varastaminen ja niiden vaihtaminen katukaupassa huumeisiin luokitellaan myös rahanpesuksi. (Chapman, 2018, 2–3.)

Rahanpesun määrän ja yhteiskunnallisten vaikutusten arvioimisen haasteeksi on osoittautunut muun muassa erimielisyys siitä, mikä kaikki luokitellaan rahanpesuksi sekä heikkoudet mekanismeissa, joilla rahanpesua havaitaan (Reuter, 2005, 4). Vuosittaisen rahanpesun määrän arviointi on ollut hankalaa vuosituhannen alussa (Reuter, 2005, 9) ja on sitä yhä edelleen (Teichmann & Falker, 2020, 501). Rahanpesua käsittelevässä akateemisessa tutkimuksessa useimmiten käytetty luku on YK:n huumausaine- ja rikosasioiden toimiston UNODC:n arvio, jonka mukaan vuosittaisen rahanpesun määrä kansainvälisesti on 2–5 % kansainvälisestä bruttokansantuotteesta tai 800 miljardia – 2 biljoonaa Yhdysvaltain dollaria (UNODC, 2022).

Suomen osalta tuorein Basel AML Index (Basel, 2021, 24) antaa riskiluvuksi 3.06, joka on 110 maan joukosta toisiksi pienin. Riskiluokittelu perustuu FATF:in määrittämiin standardeihin, joissa arvioidaan muun muassa maakohtaisesti AML viitekehyksen laatua, korruptioriskiä, talousjärjestelmän läpinäkyvyyttä ja standardeja sekä poliittista riskiä (Basel, 2021, 47). Tämä ei kuitenkaan tarkoita sitä, etteikö Suomessa tapahtuisi rahanpesua. Keskusrikospoliisin alainen Rahanpesun selvittelykeskus vastaanottaa Suomessa rahanpesulaissa määritellyiltä ilmoitusvelvollisilta tahoilta epäilyttäviä liiketoimia koskevia ilmoituksia ja epäiltyä terrorismin

rahoittamista koskevia ilmoituksia. Vuoden 2021 ensimmäisellä puoliskolla rahanpesun selvittelykeskus vastaanotti 26 580 muiden kuin virtuaalivaluuttapalveluiden tarjoajien tekemiä ilmoituksia – jos myös virtuaalivaluuttapalveluiden tekemät ilmoitukset huomioidaan, oli ilmoituksia tehty yhteensä noin 3,5 miljoonaa. Yleisin syy rahanpesuilmoitukselle oli puutteellinen varojen alkuperäselvitys. (Keskusrikospoliisi, 2021, 3–6.)

3.2 Rahanpesun tunnistetut vaiheet

Rahanpesu on perinteisesti jaoteltu koostuvan kolmesta päävaiheesta: *sijoittaminen, häivyttäminen ja palauttaminen.*

Sijoitusvaihe (*engl. placement*) tapahtuu tyypillisesti rahanpesun vaiheista ensimmäisenä. Sijoitusvaiheessa rahat siirretään osaksi rahanpesuprosessia. Tästä esimerkkinä voi olla esimerkiksi rikoksella hankittujen varojen tallettaminen pankkitilille, josta varat voidaan siirtää yhä eteenpäin seuraaville tahoille. Varoilla voidaan myös hankkia fiat-valuutasta poikkeavia instrumentteja kuten jalometalleja, virtuaalivaluuttoja tai kryptovaluuttoja. (Chapman, 2018, 2; Anon, 2015, 302.)

Häivytysvaiheessa (*engl. layering*) varoja siirretään systemaattisesti eteenpäin eri finanssijärjestelmän toimijoiden kautta. Ajatuksena on saada varat näyttämään siltä, että ne olisivat tulleet monien eri kerrosten kautta mahdollisimman laillisista kohteista. Esimerkiksi rikollinen voi ottaa omiin tai jonkun toisen nimiin sijoitusvakuutuksen, joka perutaan hyvin nopeasti ja varat siirretään eteenpäin seuraavaan sijoitustuotteeseen. Näin ollen jälkimmäisen sijoitustuotteen myöntäjä ei luokittele varojen alkuperää laittomaksi, olettaen ettei tarkempia selvityksiä tehdä. Rahanpesijän tavoite on tehdä mahdollisimman selkeä ero laittomien varojen alkuperän ja niiden nostamisen välille. (Chapman, 2018, 2.)

Viimeinen rahanpesun vaihe on palautusvaihe (*engl, integration*). Kun varojen alkuperä on häivytetty eri kerrosten välille, voidaan näennäisesti lailliset varat nostaa käytettäväksi haluttuun kohteeseen. (Chapman, 2018, 2.)

3.3 Riski ja tietämyksen tasot

3.3.1 Riskin määrittelyä

Rahanpesu ilmiönä on merkittävä pankkiin kohdistuva riski (Isa ym., 2015, 7). Riskille ei ole olemassa yksiselitteistä ja vakiintunutta määrittelyä, mutta jotkin näkökulmat erottuvat kuitenkin selkeästi nykyisissä tutkimuksissa ja keskustelussa (Bergström, Svedberg Helgesson & Mörth, 2011, 1045).

Hansson (2010, 235–236) esittää, että riskiin liittyy kaksi ominaispiirrettä:

1. riski viittaa aina ei-toivottuun tapahtumaan ja
2. riskin toteutumiseen liittyy aina epävarmuutta.

Myös Bessiksen (2011) esittämä määrittely korostaa ei-toivotun tappion ja epävarmuuden liitännäisyyttä riskiin. Vaikka olennainen riskiin liittyvä piirre on epävarmuus, riski ei Bessiksen mukaan itsessään kuitenkaan tarkoita identtisesti samaa kuin epävarmuus. Epävarmuus viittaa tulosten satunnaisuuteen ja riskillä tarkoitetaan tällaisten tulosten haitallista vaikutusta tappion muodossa. Jos tappion mahdollisuutta ei ole, liittyy tilanteeseen epävarmuutta, mutta ei riskiä. Jos taas haitalliset vaikutukset voivat toteutua, on olemassa sekä epävarmuutta että riskiä. Riskiä on siis olemassa vain silloin, kun epävarmuudella voi olla mahdollinen haitallinen vaikutus, joka on tappion mahdollisuus. (Bessis, 2011, luku 3)

3.3.2 Riskien ja tietämyksen luokittelua

Aikaisemmin riski nähtiin hyvin subjektiivisena konseptina, mutta nykynäkökulma painottaa enemmän objektiivisuutta (Hansson, 2010). Muita tapoja luokitella riskejä satunnaisuuden perusteella ovat esimerkiksi jakaa riskit dynaamisiin ja staattisiin sekä spekulatiivisiin ja puhtaisiin. Dynaamisilla riskeillä viitataan olosuhteiden mukana muuttuviin riskeihin, kun taas staattiset riskit pysyvät muuttumattomina. Spekulatiiviset sisältävät perinteisessä (puhtaan) riskin määrittelyssä korostetun ei-toivotun tapahtuman lisäksi mahdollisuuden hyödylliseen tapahtumaan. (Koskinen, 2018, 15–16.)

Jotta tietyn riskin suhteen voitaisiin tehdä rationaalisia päätöksiä ja hallita sitä, riski tulee tuntea. Lisäksi riskistä voi olla olemassa tietoutta eri tietämyksen tasoilla. Diebold, Doherty ja Herring (2010, 103–105) esittävät seuraavat kolme tietämyksen tasoa liittyen pankkitoimintaan liittyviin riskeihin:

1. K (known) viittaa sellaiseen riskiin, joka voidaan tunnistaa tarkasti ja on mitattava. Esimerkiksi pankin vakavaraisuusriski.
2. u (unknown) viittaa riskiin, joka voidaan tunnistaa, mutta sitä ei voida mitata tarkasti. Esimerkkinä mainitaan maineriski, joka seuraa pankin toimitusjohtajan petosepäilyistä.
3. U (unknownable) viittaa riskiin, jota ei voida ennustaa eikä mitata. Riskiä ei siis tunneta. Esimerkiksi ennen 9/11-iskuja riski joutua terroristihyökkäyksen kohteeksi toimistotiloissa World Trade Centerissä.

3.4 Pankin rahanpesuriski

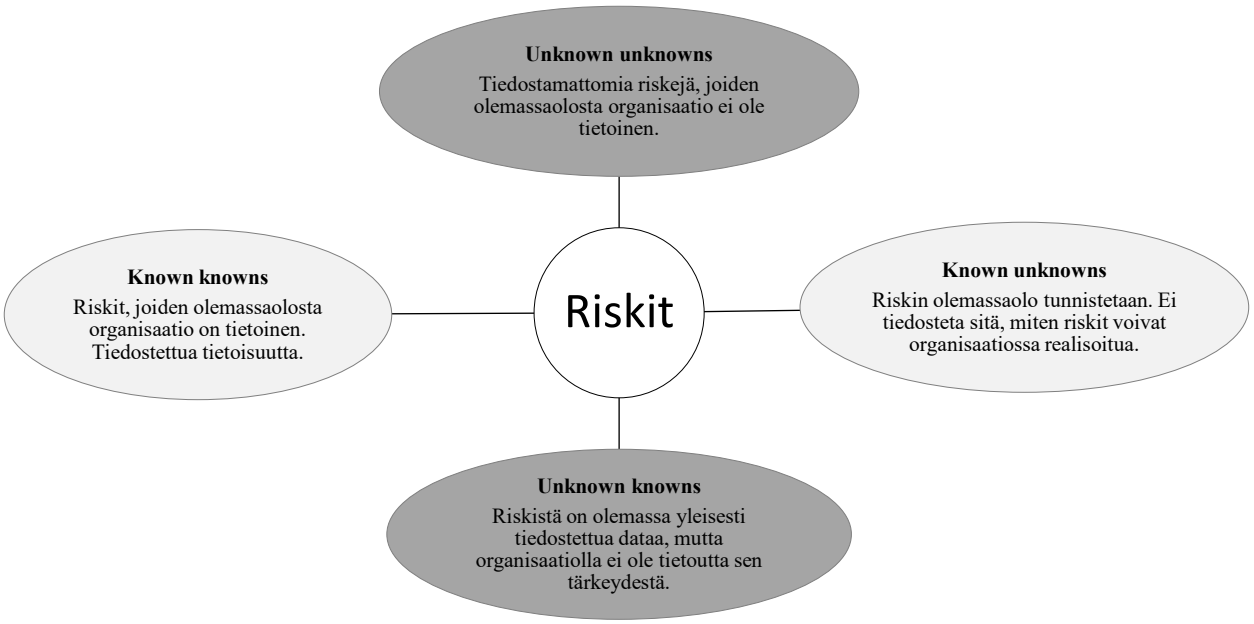
Rahanpesu on vakava ongelma koko pankkisektorille ja samalla myös laajemmin yhteiskunnalle. Ihmiskauppa, terrorismi, korruptio, huumeiden salakuljetus, veronkierto ja muu laiton toiminta aiheuttavat kustannuksia ja yhteiskunnallisia seurauksia kaikkialla maailmassa. Tällaisesta laittomasta toiminnasta peräisin olevien rahavirtojen jäljittäminen ja pysäyttäminen on keskeistä, jotta rikolliset saadaan kiinni. (Chapman, 2018, 8.) Kun tarkastellaan rahanpesuun liitettäviä toimintatapoja, pankit ovat usein rahanpesijöiden ensisijainen ensimmäisen tason yhteyspiste toteuttaa rahanpesua. Tämä johtuu pitkälti pankin liiketoiminnan luonteesta ja sen tarjoamista palveluista – rahanpesun instrumentteina käytetään talletuksia, lainoja, sijoituksia ja valuuttakauppaa. Näin ollen pankit altistuvat erilaisille rahanpesuriskeille, jotka niiden tulee ottaa huomioon osana riskienhallintaansa. (Isa ym, 2015, 8.) Suurin osa nykytutkimuksesta keskittyy pankin kohtaamaan rahanpesuriskiin, mutta rahanpesuriski voi syntyä myös pankin sisällä. Pankki voi olla osallisena rahanpesuun, jos se tietoisesti tai tiedostamattaan mahdollistaa rikoksella hankittujen varojen säilömistä tai siirtämistä eteenpäin. Pankilla voi olla pelkästään rahanpesuun suunniteltuja palveluja tai rikolliset voivat pankin huomaamatta soluttautua sen systeemeihin pestäkseen rahaa. (Chapman, 2018, 8.)

Bessisin (2011) mukaan pankkiin kohdistuvat riskit voidaan jakaa perinteisiin taloudellisiin riskeihin sekä ei-taloudellisiin riskeihin. Erityisesti ei-taloudelliset riskit ovat saaneet kasvavissa määrin huomiota pankkien riskienhallinnassa. Ei-taloudelliset riskit jakautuvat operatiivisiin riskeihin ja liiketoimintariskeihin. Operatiiviset riskit voidaan ajatella välittömien tai välillisten tappioiden riskinä, joka johtuu riittämättömistä tai epäonnistuneista sisäisistä prosesseista, ihmisistä ja järjestelmistä tai ulkoisista tapahtumista. Liiketoimintariskillä puolestaan tarkoitetaan altistumista organisaatiosta johtuville tekijöille, jotka alentavat pankin voittoja. (Diebold ym, 2010, 111.) Diebold ym. toteavat, että esimerkiksi sääntelyn noudattamisessa epäonnistuminen on pankille ei-taloudellisen riskikategorian riski, jossa on sekä operatiivisen riskin että

liiketoimintariskin piirteitä. Tämän perusteella voidaan päätellä, että myös pankin rahanpesuriski kuuluu samaan riskikategoriaan.

Edellä esitellyt tietämyksen tasot K, u ja U muuttuvat sen mukaan, mistä pankin liiketoimintaan liittyvästä riskistä on kyse. Perinteiset markkinariskit tunnetaan paremmin kuin esimerkiksi ei-taloudelliset riskit. Perinteisiä markkinariskejä on myös huomattavasti helpompi mitata kuin ei-taloudellisia riskejä. (Diebold ym, 2010, 103–113.) Pankin kohtaamaa rahanpesuriskiä voidaan pitää vähemmän tunnettuna riskinä, sillä perinteinen pankkien riskienhallintaa koskeva kirjallisuus ei ota suoraan kantaa rahanpesuriskiin (katso esim. Bessis, 2011; Diebold ym, 2011). Kuitenkin rahanpesua käsittelevä akateeminen tutkimus tuo selkeästi esille, että pankit ovat erittäin haavoittuvaisia rahanpesulle. Koska rahanpesuriskiä on vaikea mitata, mutta se kuitenkin tunnetaan, voidaan kyseisen riskin tietämyksen tason päätellä olevan u (unknown).

Myös Chapman vahvistaa tämän päätelmän toteamalla, että ”unknown-tyyppisten rahanpesuriskien sisällyttäminen osaksi riskienhallintaa joustavalla tavalla on tärkeää”. Chapman (2018, 108) käsittelee rahanpesuriskin torjuntaa yksittäisten organisaatioiden kuten pankkien näkökulmasta tunnettujen ja tuntemattomien riskien viitekehyksen avulla. Kyseinen viitekehys yhdistää perinteiset tietämyksen tasot organisaatioläheisempään kontekstiin, joten myös tämän tutkielman näkökulmasta pankkien rahanpesuriskiin liittyvää riskienhallintaa on mielekästä tutkia kyseisen viitekehyksen avulla.



Kuvio 5. Organisaation tunnetut ja tuntemattomat riskit (mukaillen Chapman, 2018, 108).

Viitekehyksessä on neljä ulottuvuutta, jotka kattavat sekä jo tunnetut että tuntemattomat riskit, joiden vaikutus puolestaan voi olla myös joko tunnistettu tai tuntematon. Rahanpesuriskit voivat olla Chapmanin (2018) mukaan joko unknown unknowns -tyyppisiä riskejä, joista ei ole olemassa dataa eikä pankki ole niiden olemassaolosta edes tietoisia tai known unknows -tyyppisiä riskejä, joiden olemassaolo on tunnistettu, mutta niiden merkittävyydestä pankille ei ole tietoutta.

3.4.1 Pankin rahanpesuriskin realisoituminen

Pankin riskienhallinnan näkökulmasta rahanpesuriski voi realisoitua sääntelyn määräämän ilmoitusvelvollisuuden laiminlyöntinä ja compliance-riskin toteutumisena, mahdollisina suurina sakkorangaistuksia sekä mainehaittana. (Isa ym., 2015, 8–9.) Compliance-riskillä tarkoitetaan riskiä, joka aiheutuu ulkoisen sääntelyn, sisäisten menettelytapojen tai eettisten periaatteiden noudattamatta jättämisestä. Pankit investoivat vuosittain kasvavalla tahdilla talousrikollisuuden torjuntaan. Pankeilla tulee olla ajantasaiset talousrikollisuuteen liittyvät riskienhallinnan standardit sekä ohjeistukset, joiden tehokkuutta ja implementointia tulee arvioida jatkuvasti. (Deloitte, 2019, 9.)

Vaikka rahanpesuriski edellä luokiteltiin ei-taloudellisiin riskeihin, ei se nimensä mukaisesti kuitenkaan tarkoita, ettei rahanpesuriskillä voisi olla mittavia taloudellisia seurauksia pankille. Mikäli pankki laiminlöisi velvollisuutensa rahanpesun estämisessä ja rahanpesuriski toteutuisi, voisi valvova viranomainen antaa pankille tuntuvan sakkorangaistuksen tai asettaa pankin toimintakieltoon. Syykuussa 2021 Helsingin Sanomat uutisoi, että Finanssivalvonta oli antanut S-Pankille 1,7 miljoonan euron sakot, sillä pankki oli laiminlyönyt epäilyttävien toimeksiantojen tunnistamista liittyen osakevälitykseen. Loppuvuodesta 2021 myös yksi maailman suurimmista pankkitoiminnan harjoittajista HSBC sai valvojalta 64 miljoonan punnan sakot, sillä se oli epäonnistunut transaktiomonitoroinnin kyvykkyyksien ylläpitämisessä ja tehokkaassa rahanpesun estämisessä (FCA, 2021). Myös mainehaitta rahanpesuskandaalista on ilmeinen, kuten on nähty Nordean ja ruotsalaisen Swedbankin kohdalla muutama vuosi sitten (Yle 2020).

3.5 Rahanpesuriskin hallinta osana pankkien riskienhallintaa

3.5.1 Riskienhallinta pankeissa

Riskienhallinnalla tarkoitetaan perinteisesti kaikkea organisaatioissa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Se on kuitenkin myös paljon enemmän kuin vain

teknisiä käytäntöjä – se ilmentää myös organisaation merkittäviä arvoja, ihanteita ja vastuullisuutta. (Power, 2004, 11.) Usein kun riski tunnistetaan, siihen yhdistetään myös vaatimus toimia ja halu vähentää sen haitallisia seurauksia erilaisilla toimilla (Garland, 2003, 52). Näin ollen voidaan ajatella, että siellä, missä on tunnistettuja riskejä, on myös riskienhallintaa sekä riskien arviointia. Riskienhallinta on laajentunut sekä julkisen että yksityisen sektorin kattavaksi ilmiöksi ja siitä on muodostunut nykyaikainen standardi epävarmuuden käsittelyyn eri organisaatioissa. (Power, 2004.)

Riskienhallinnasta rooli osana pankkien toimintaa korostui merkittävästi vuoden 2008 finanssikriisin jälkeen (Bessis, 2011, luku 1). Onnistuneen riskienhallinnan tavoitteena on riskien tunnistaminen ja niiden hallitseminen. Laadukas riskienhallinta on mahdollista, kun riskejä pyritään arvioimaan sekä määrällisesti että laadullisesti. Eri riskienhallinnan apuna käytettävien prosessien kantavana ajatuksena on yhdenmukaistaa riskinotto sekä riskinhallinta. (Bessis, 2011, luku 4.)

Pankin rahanpesuriskin hallinta on perinteisesti aikaisemmissa tutkimuksissa nähty olevan organisaatiolähtöistä, mutta Isa ym. (2015, 8) esittävät, että myös pankissa työskentelevillä yksilöillä on merkittävä rooli rahanpesuriskin tunnistamisessa ja hallinnassa. Pankin tulee laatia politiikka rahanpesuun liittyen, määrittää tarvittavat compliance-toiminnot sekä noudattaa viranomaisten asettamia valvontavaatimuksia.

3.5.2 Riskienhallinnan kolme puolustuslinjaa

Pankit nojaavat kolmen puolustuslinjan mallin mukaiseen riskienhallinnan viitekehykseen. Mallin soveltamisen taso riippuu muun muassa pankin liiketoiminnan luonteesta ja koosta. (Basel, 2020, 3.) Nämä kolme puolustuslinjaa ovat tyypillisesti 1. liiketoiminnat, 2. yritystoiminnot kuten riskienhallinta ja compliance sekä 3. sisäinen tarkastus. (Bessis, 2011, luku 4; Davies & Zhivitskaya, 2018, 34–37.) Esimerkiksi Suomen suurin finanssilaitos OP kertoo sivuillaan, että sen sisäiseen valvontaan ja riskienhallintaan liittyvät roolit ja vastuut on jaettu edellä kuvatusti kolmeen puolustuslinjaan (OP, 2022). Myös Nordea (2022) esittelee sivuillaan kolmen puolustuslinjan prosessin, jolla hallitaan talousrikollisuuteen liittyviä riskejä.

Ensimmäisen linjan muodostavat liiketoiminnot ovat ensisijaisessa vastuussa niihin liittyvien riskien tunnistamisesta, mittaamisesta ja hallitsemisesta (Bessis, 2011, kappale 4.2). Rahanpesun estämisen näkökulmasta ensimmäinen puolustuslinja koostuu talousrikollisuuden torjunnan eri

osa-alueista kuten asiakaspalvelu-, tutkinta- sekä asiantuntijayksiköistä, jotka vastaavat päivittäisestä riskienhallinnasta sekä pankkien omien ohjeistuksien asianmukaisesta noudattamisesta. Ensimmäiseen puolustuslinjaan kuuluu muun muassa tehokas asiakkaan tunteminen sekä transaktiomonitorointi. Asiakasrajapinnassa työskentelevien ihmisten on erityisen tärkeää pystyä tunnistamaan korkean riskin tilanteet ja toimimaan organisaation määrittämien riskienhallintakeinojen mukaisesti. (Isa ym., 2015, 9–10.)

Toisen puolustuslinjan muodostavat erilaiset yritystoiminnan tukitoiminnot kuten compliance- sekä riskienhallintatoiminnot (Davies & Zhivitskaya, 2018, 37), jotka valvovat päivittäistä toimintaa sekä neuvovat ensimmäistä linjaa talousrikollisuuden torjuntaan liittyvissä kysymyksissä sekä sääntelyn noudattamisessa. Jos rahanpesuriski on jäänyt huomaamatta ensimmäisessä puolustuslinjassa, on pankin compliance-toiminnot seuraavana vastuussa. (Isa ym., 2015, 12.) Toisen puolustuslinjan rooli on osana pankin rahanpesuriskin hallintaa Nordean (2022) mukaan ”juurruttaa rehelliset ja oikeudenmukaiset liiketoiminnan periaatteet sekä vastata tehokkaiden riskienhallintaprosessien käytöstä”. Kolmas puolustuslinja kattaa alleen pankin sisäisen tarkastuksen, joka tekee itsenäistä valvontaa parantaakseen hallinnon, riskienhallinnan sekä valvontaprosessien tehokkuutta (Davies & Zhivitskaya, 2018, 37).

3.5.3 Pankin oma riskiarvio rahanpesuriskeistä

Suomessa laki rahanpesun ja terrorismin rahoittamisen estämisestä (2017/444) velvoittaa pankkeja luomaan rahanpesun riskien tunnistamiseksi riskiarvion, jonka toteutumista valvoo Finanssivalvonta. Ilmoitusvelvollisena pankin tulee ottaa riskiarviossa huomioon harjoittamansa liiketoiminnan luonne, koko ja laajuus. Pankilla tulee olla asianmukaiset toimintaperiaatteet, menettelytavat sekä tarvittava valvonta rahanpesuriskin vähentämiseksi ja tehokkaaksi hallitsemiseksi. Laki ei määrittele tarkasti, millainen riskiarvion tulisi olla. Siitä tulee kuitenkin käydä ilmi esimerkiksi tunnistettujen riskien hallintakeinot sekä jäännösriskin arviointi. Pankin tulee esimerkiksi pystyä kertomaan Finanssivalvonnalle, millä perustein riskiarvio on laadittu, kuka siitä on vastuussa ja mikä sen päivitystiheys on. (Finanssivalvonta, 2021a.)

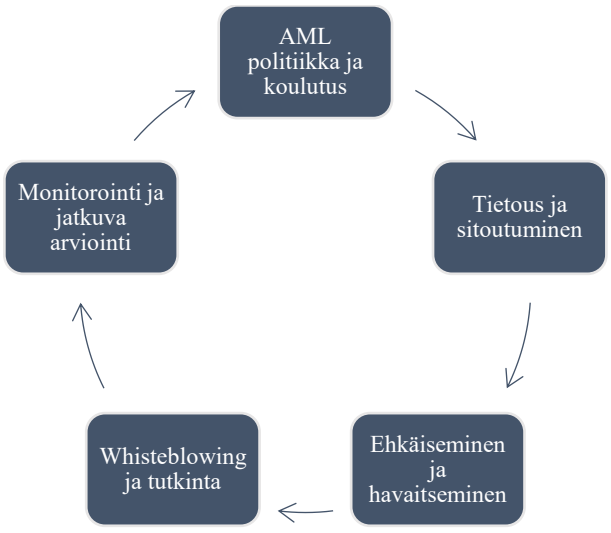
Finanssivalvonnan kuvaama riskiarvion laatimiseen liittyvä ohjeistus on pitkälti linjassa Koskisen (2018, 22) riskienhallinnan määrittelyn kanssa. Sen mukaan kyseessä on aktiivinen toiminta, jonka vaiheina ovat riskien tunnistaminen ja seuranta, suuruuden ja yhteisvaikutuksen arviointi sekä eri keinot rajata riskejä, suojautua niiltä tai siirtää niitä. Voidaan siis nähdä, että pankin itse luoma

rahanpesun estämisen riskiarvio on tärkeä elementti pankkien rahanpesuriskiin liittyvässä riskienhallinnassa.

3.5.4 Chapmanin rahanpesun estämisen viitekehys

Rahanpesuun liittyvä sääntely on maailmanlaajuisesti hyvin riippuvaista eri toimivaltojen omista käytänteistä, mutta tiettyjä AML-kontrolleja voidaan pitää myös maailmanlaajuisesti yleispätevinä. Organisaatioiden tulee tunnistaa rahanpesuriskit, järjestelmien heikkoudet sekä estää organisaation kautta tapahtuvaa rahanpesua. Pankkien kontekstissa voidaan todeta, että rahanpesuriskiin liittyvä riskienhallinta voidaan pilkkoa seuraaviin yhdeksään kohtaan (Chapman, 2018, 6.):

1. Hallinto- ja kontrolliympäristö
2. Työntekijöiden rekrytointi, koulutus ja johtaminen
3. Toimiala-, tuote- ja maantieteellisten riskien sekä asiakkaiden demografisten riskien hallintamallit
4. CDD – Asiakkaan tunteminen
5. Jatkuva transaktiomonitorointi ja transaktioscreenaus
6. Datan hyödyntäminen ja tiedolla johtaminen
7. Liiketoimintojen ohjeistus ja tuki
8. Sisäinen ja ulkoinen tarkastus
9. Kokonaisvaltainen rahanpesun estämisen kyvykkyyksien monitorointi ja parantaminen AML strategiaympyrän avulla



Kuvio 6. AML Strategiaympyrä. (mukaillen Chapman, 2008, 64.)

Esimerkiksi Nordea (2021) mainitsee talousrikollisuuden torjuntaan liittyvissä periaatteissaan kaikki edellä mainitut ensimmäiset kahdeksan kohtaa. Lisäksi periaatteissa mainitaan Chapmanin esittämien kohtien lisäksi yhtenä vaatimuksena sisäisen ja ulkoisen raportoinnin odotukset.

Kolmanteen tutkimuskysymykseen, ”millä eri keinoin pankkien tulisi huomioida virtuaalivaluuttojen aiheuttama rahanpesuriski osana riskienhallintaa”, vastataan osittain edellä esitellyn Chapmanin rahanpesun estämisen viitekehyksen avulla, ja se toimii myös tutkielman tulkintateoriana. Sen sisältämän AML-strategiaympyrän hyödyntäminen osana rahanpesun estämistä nostaa pankin compliance -tasoa sekä lisää tietoutta rahanpesun estämisestä organisaation sisällä (Chapman, 2018, 6).

3.6 Rahanpesun estäminen

Rahanpesun estäminen (AML, anti-money-laundering) sai alkunsa Yhdysvalloissa 1970 -luvulla, kun Bank Secrecy Act -laki otettiin käyttöön. Kyseinen laki koski aluksi vain kansallisia luottolaitoksia, mutta nykyään rahanpesun estämisestä on tullut strukturoitu kansainvälinen toimintatapa, johon liittyy useiden eri instituutioiden sääntely. (Reuter & Truman, 2006, 1.) Ensimmäisten kansainvälisten rahanpesun estämiseen liittyvien toimintojen voidaan taas nähdä liittyvän FATF:in perustamiseen vuonna 1989. Perustamisestaan asti FATF on antanut suosituksia ja vahvistanut valtioiden omia viitekehyksiä rahanpesun estämisen tehostamiseksi. (Jayasekara, 2021, 257.)

Kun rahanpesun estämistä alettiin säännellä enemmän 2000-luvun alussa, syntyi samanaikaisesti myös kokonaan uusi toimiala: compliance. Compliancesta, joka voidaan vapaasti suomentaa vaatimustenmukaisuutena, tuli suurelta osin synonyymi AML Compliancelle. Compliance-toimintojen syntymiseen vaikutti myös viranomaisten resurssipuute, jolloin myös pankit tehtiin osalliseksi rahanpesun estämiseen. Toiseksi ajatus yksityisten yritysten roolista yrityskansalaisina alkoi yleistyä, ja samalla yrityksiltä alettiin odottamaan moraalista vastuuta, kestävyyttä ja hyvää mainetta. (Chau & Nemcsik, 2020, 2–3.)

Rahanpesun estäminen ilmiönä nähtiin aluksi liittyvän vain pankkeihin, mutta nykyään siihen liittyvien instituutioiden määrä on kasvanut merkittävästi. Lain velvoittamat kontrollit Yhdysvalloissa rahanpesun estämiseksi koskevat nykyään niin autokauppoja, kasinoita,

rahanvälityspalveluita, panttilainaamoita sekä vakuutusyhtiöitä. (Levi & Reuter, 2006, 290.) Suomessa rahanpesun estäminen koskee muun muassa luottolaitoksia, arvopaperivälittäjiä, tilintarkastajia, vakuutusyhtiöitä, virtuaalivaluuttatoimijoita, rahapeliyhteisöitä sekä tietyin ehdoin myös asianajajia (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017/444, 2 §). Rahanpesun estäminen voidaan siis nähdä toimintana, jota esimerkiksi pankit tekevät täyttääkseen niille laissa määrätyt vaatimukset, joiden pohjalta epäilyttäviä toimia seurataan aktiivisesti ja raportoidaan (SAS, 2022).

Reuterin (2005, 23–24) mukaan vuosittaisella rahanpesun määrällä ei välttämättä tulisi olla suoraa korrelaatiota rahanpesun estämiseen käytettyihin resursseihin. Rahanpesu liittyy moniin eri rikollisuuden muotoihin, joilla on erilaisia yhteiskunnallisia vaikutuksia. Jos esimerkiksi tiettynä vuonna arvioidun rahanpesun määrä laskee johtuen korkean profiilin yrityspetosten laskusta, mutta samaan aikaan pienen volyymin terrorismin rahoittaminen nousee, ei sääntelyä pitäisi ohjata euromääräisen kokonaiskertymän pieneneminen. Hän tiivistää ajatuksensa toteamalla, että olisi tärkeää seurata sellaista rahanpesun määrää, joka liittyy kulloinkin painotettuihin rahanpesun estämisen tavoitteisiin.

3.7 Rahanpesun estämisen sääntely ja keskeiset viranomaiset

Rahanpesun sekä terrorismin rahoittamisen estämiseen liittyy sääntelyä, joka muodostuu sekä kansallisesta lainsäädännöstä että eurooppalaisesta ja kansainvälisestä sääntelystä. Suomessa noudatetaan rahanpesulakia, jota puolestaan täydentää useat erillislait. Suomessa käytettävän kansallisen lainsäädännön taustalla on Euroopan unionin omaa sääntelyä, joka muodostuu direktiiveistä ja asetuksista. Direktiivit pannaan täytäntöön kansallisten lakien kautta, asetuksia taas tulee soveltaa sellaisinaan. Kansallisen lainsäädännön ja EU-oikeuden taustallaa vaikuttavat merkittävästi myös rahanpesun ja terrorismin rahoittamisen vastaisen toimintaryhmän FATF:in kansainväliset suositukset. (Valtiovarainministeriö, 2021, 18–29.)

Kokonaisuudessaan talousrikollisuuteen liittyviä kansainvälisiä compliance-standardeja ja ohjeistuksia pidetään epäjohdonmukaisina. Viime vuosina on peräänkuulutettu erityisesti sääntelyn yhdenmukaisuutta ja selkeyttä. FATF:in antamat ylikansalliset ohjeistukset ja muu kansainvälinen sääntely, jotka eivät itsessään ole sitovia, tulee toimeenpanna kansallisella tasolla, jolloin eroavaisuuksia syntyy. Kansallisella tasolla saattaa ilmetä muuhun lainsäädäntöön liittyviä ristiriitoja, jolloin kansainvälisistä ohjeistuksista ei ole hyötyä. Riskinä on, että kansainvälisten

standardien epäjohdonmukainen implementointi kansallisella tasolla mahdollistaa lainsäädännöllisiä porsaanreikiä, joita rikolliset voivat hyödyntää. (Deloitte, 2019, 29.)

Rahanpesun estämiseen liittyvä kansallinen lainsäädäntö Suomessa koostuu pääosin rahanpesulaista, laista virtuaalivaluutan tarjoajista, valtioneuvoston asetuksesta poliittisesti vaikutusvaltaisista henkilöistä, laista pankki- ja maksutilien valvontajärjestelmästä, laista rahanpesun selvittelykeskuksesta sekä rikoslaista. (Valtiovarainministeriö, 2022.) Ajantasainen EU-lainsäädäntö puolestaan kattaa alleen kuudennen rahanpesudirektiivin, toisen maksajan tiedot -asetuksen, EU:n rahanpesupaketin sekä rahanpesun ja terrorismin rahoittamisen vastaisen toimintaryhmän suosituksia. Euroopan komissio julkaisi kesällä 2021 ehdotuksen uudeksi rahanpesun estämistä koskevaksi sääntelypaketiksi. Kuudennen rahanpesudirektiivin lisäksi yksi sen merkittävistä kohdista oli ehdotus luoda EU:n alueelle yhtenäinen rahanpesun ja terrorismin rahoituksesta vastaava torjuntaviranomainen vuoteen 2024 mennessä (Euroopan komissio, 2021, 1–34).

3.8 Rahanpesun estäminen pankeissa

Samanaikaisesti, kun pankki altistuu rahanpesuriskille teorialuvun alussa kuvatuista syistä, on pankilla kuitenkin ainutlaatuiset mahdollisuudet olla osa rahanpesun estämistä (Chapman, 2018, 8.). Selkein ja suurin pankin kohtaaman rahanpesuriskin hallintakeino on systemaattisen rahanpesun estämisen toteuttaminen (Isa ym, 2015). On kuitenkin tärkeää ymmärtää, mitkä ovat perustavanlaatuiset syyt pankille toteuttaa laadukasta rahanpesun estämistä. Syyt voidaan jakaa karkeasti moraalisiin ja sääntelyyn perustuviin, ja sääntelyyn perustuvat syyt voidaan nähdä myös taloudellisina (Chau & Nemcsik, 2020, 2–3).

Sääntelyn osalta pankeilla on lakiin perustuva velvollisuus (Suomessa laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444) tuntea asiakkaansa toimintaa sekä havaita ja selvittää epäilyttäviltä vaikuttavia transaktioita ja liiketoimia. Suomessa pankkien rahanpesun estämistä valvoo Finanssivalvonta. Finanssivalvonnan valvonnan alainen pankki tai sen toimihenkilö voidaan tuomita rangaistukseen asiakkaan tuntemiseen ja rahanpesun tai terrorismin rahoittamisen estämiseen liittyvien velvollisuuksien laiminlyönnistä. Valvottava voi syyllistyä tuottamukselliseen rahanpesuun esimerkiksi silloin, jos se avustaa tai neuvoo asiakasta sijoitustoiminnassa, peiteyhtiöiden perustamisessa tai varojen siirrossa, vaikka sillä on aihetta suhtautua epäillen asiakkaan liiketoimiin. (Finanssivalvonta, 2021b.)

Pankit ovat Suomessa rahanpesulain mukaisesti selonotto- ja ilmoitusvelvollisia. Pankkien tulee seurata esimerkiksi asiakkaiden päivittäistä maksukäyttäytymistä sekä palveluiden käyttöä. Selonottovelvollisuudella tarkoitetaan toimintaa, jossa pankki kysyy asiakkaalta lisätietoja liittyen havaitsemiinsa tavallisesta poikkeaviin transaktioihin. Ilmoitusvelvollisuus koskee tilanteita, joissa pankki on havainnut asiakkuuteen, asiakkaan liiketoimintaan, varojen alkuperään tai varojen käyttötarkoitukseen liittyviä epäselvyyksiä, ja asiakas ei ole kyennyt antamaan käytökselle rationaalista syytä. Pankin tulee tällöin täyttää rahanpesuilmoitus Keskusrikospoliisin Rahanpesun selvittelykeskukselle. (Finanssivalvonta, 2021b)

Pankkeihin kohdistuvan rahanpesuriskin ja sääntelyvelvoitteiden takia pankeilla on kehitettyinä sisäiset talousrikollisuuden torjunnasta vastaavat toiminnot, joiden tehtävä on muun muassa toteuttaa rahanpesun estämistä sekä toteuttaa selonotto- ja ilmoitusvelvollisuutta. Pankin liiketoiminnan näkökulmasta talousrikollisuuden torjunta on kuitenkin pelkkä kulu, ei tuottava yksikkö (Hasham, Joshi & Mikkelsen, 2019, 5). Tämä aiheuttaa tuottavan liiketoiminnan näkökulmasta ristiriidan, sillä pankkien tulee investoida jatkuvasti lisää tehokkaampiin valvontaratkaisuihin ja asiakkaan tuntemiseen täyttääkseen sääntelyn asettamat velvoitteet. Samanaikaisesti tulee kuitenkin varmistua, että asiakastyytyväisyys säilyy ja kulut eivät paisu liian suuriksi (Deloitte, 2019). Chau & Nemcsik (2020, 3–4) esittävät, että pankit ovat tähän mennessä hyväksyneet AML-toimintojen aiheuttaman kustannustaakan liiketoiminnoille myös moraalisin perustein yritysvastuun näkökulmasta. Vaatimuksien noudattamiselle on olemassa selkeä kannustin mahdollisten suurien sakkorangaistuksien muodossa, mutta tämän lisäksi pankeilla on myös aito hyväksyntä niiden roolista yhteiskunnan jäsenenä järjestelmän väärinkäytön estäjinä.

3.8.1 Riskiperusteinen lähestymistapa

Riskienhallinnan pitkäaikaisena trendinä on ollut riskiperusteisen lähestymistavan painottaminen sekä hallintakeinoissa että sääntelyssä (Power, 2004, 15). Myös pankin rahanpesun estämiseen liittyvien strategioiden tulisi pohjautua riskiperusteiseen lähestymistapaan, kuten alaan liittyvässä sääntelyssä määrätään (Ross & Hannan, 2007, 106). Pankkien tulee järjestää rahanpesuriskiin liittyvät ennaltaehkäisy- ja havaitsemistoimenpiteensä tunnistettuihin riskeihin suhteutetulla tavalla. (Chapman, 2018, 107–108.) Koska riskin käsitteellistäminen on kuitenkin myös AML-strategiatasolla vaikeaa, on riskiperusteisen lähestymistavan määrittelyssä ja toteuttamisessa epävarmuutta. Ennen riskiperusteista lähestymistapaa rahanpesuriskiä hallittiin sääntö- ja tapauspohjaisilla lähestymistavoilla, mutta tämä ei pitkällä tähtäimellä johtanut haluttuihin lopputuloksiin. Sääntö- ja tapauskohtainen lähestymistapa aiheutti pankeille huomattavaa

lisätyötä, kun ne ilmoittivat sääntöperusteisesti asiakkaiden epäilyttäviä transaktioita. Nykyään pankit voivat keskittää talousrikollisuuden torjunnan resurssejaan niiden oman riskiarvion pohjalta. (Ross & Hannan, 2007, 106–107.)

Riskiperusteiseen lähestymistapaan kuuluu myös itse riskiarvioiden luominen (Chapman, 2018, 62), ja Suomen rahanpesulaissa onkin omat määrittelynsä sekä valvojakohtaiselle että ilmoitusvelvollisen riskiarviolle (2017/444, luku 2). Pankin tulee myös pystyä selvittämään valvovalle viranomaiselle yksityiskohtaisesti sen käytössä olevat riskiperusteiset valvontamenetelmät. (Teichmann & Falker, 2020, 501–502.)

3.8.2 Asiakkaan tunteminen ja transaktiomonitorointi

Asiakkaan tunteminen ja transaktiomonitorointi ovat rahanpesun estämisen merkittäviä keinoja. Asiakkaan tuntemisella tarkoitetaan yksinkertaistettuna niitä toimia, joilla pankki tunnistaa asiakkaan taustat ja tyypillisen maksukäyttäytymisen (Chau & Nemcsik, 2020, 3.). Pankki luo riskiarvioonsa perustuen omat asiakkaan tuntemiseen liittyvät menettelytapansa ja asettaa vähimmäiskriteerit, joita se noudattaa asiakassuhteissaan. Pankin on voitava osoittaa valvojalle, miten se arvioi asiakassuhteisiinsa ja toimintaansa liittyvät rahanpesuriskit. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017/444). Tällaista toimintatapaa kutsutaan myös nimellä CDD (Customer Due Diligence) (Chau & Nemcsik, 2020, 3).

Asiakkaiden tunnistamisen ja riskiluokittelun lisäksi pankki valvoo asiakkaiden transaktioliikennettä. Transaktioiden joukosta halutaan löytää asiakkaan tyypillisestä käyttäytymisestä poikkeavia sekä epäilyttäviä transaktioita. Koska pankkien kautta kulkee miljardeja transaktioita päivittäin, ovat pankit ottaneet käyttöönsä analyyttisilla menetelmillä toimivia transaktiomonitorointijärjestelmiä helpottamaan valvontaa. (Deloitte, 2019, 31.) Transaktiomonitorointi pohjautuu tyypillisesti joukkoon skenaarioita, joiden tarkoituksena on havaita tietyntyyppistä epätavallista transaktiokäyttäytymistä. Tällaista käytöstä voi olla esimerkiksi suuret käteistalletukset ja -nostot, varojen nopea liikuttelu eri tilien välillä sekä samantyyppisten transaktioiden järjestelmällinen toteuttaminen. Transaktiomonitoroinnin tarkoituksena on nostaa hälytys, kun epätyypillistä käytöstä havaitaan. Tämän jälkeen hälytykset siirtyvät tutkittavaksi tähän tarkoitetuille tiimeille, jotka tarkistavat transaktiot ja tekevät päätöksen, tulisiko käytös raportoida viranomaisille. Tutkittavaksi menevistä hälytyksistä käytetään nimitystä true positive -hälytys. Suurin osa transaktiomonitoroinnin aiheuttamista hälytyksistä tuomitaan manuaalisessa tutkinnassa kuitenkin aiheettomiksi false positive -

hälytyksiksi, mikä aiheuttaa pankeille lisäkuluja. (Gupta, Dwivedi & Jain, 2022, 73; Chau & Nemcsik, 2020, 43–72.).

3.8.3 Analytiikan hyödyntäminen osana rahanpesun estämistä

Suurin osa akateemisesta tutkimuksesta transaktiomonitorointiin liittyen painottaa analytiikan ja koneoppivien mallien hyödyntämistä (Zhu, 2006; Shokry, Rizka & Labib, 2020; Lucchetti, 2018). Yksi alan johtavia palveluntarjoajia on kansainvälinen ohjelmistoyhtiö SAS, jonka rahanpesun torjuntaohjelma SAS AML sisältää datan ja analytiikan käyttöä. Uudenlaisten tekoälytekniikoiden hyödyntämisen tarkoituksena on automatisoida vanhoja manuaalisia tutkintaprosesseja (SAS, 2022; Sobh, 2020, 523–524). Hyvän teknologian tulisi tehdä rahanpesun estämisestä tehokkaampaa, sillä sen avulla voidaan helpottaa sekä ihmistutkijan tekemää työtä että helpottaa viranomaisraportointia. Kaikille olemassa oleville rahanpesun estämisen teknologioille on kuitenkin yhteistä tietyt ongelmat: tutkintatiimejä kuormittavien false positive-hälytysten liiallinen määrä, tiettyjen toistuvien kuvioiden tunnistamisen heikkous, heikko datan laatu, tehottomat asiakaskohtaiset raja-arvot sekä riippuvuus tutkijoiden osaamisesta liittyen rahanpesun estämiseen. (Sobh, 2020, 522).

Analytiikan, tekoälyn sekä koneoppivien mallien hyödyntäminen osana talousrikollisuuden torjuntaa on noussut viime vuosien aikana tärkeimmäksi rahanpesun estämisen trendiksi. Uudenlaisten innovaatioiden käyttämisellä pyritään kehittämään pankkien AML-tutkintaa sekä compliance-tasoa: pankit ovat raportoineet pystyvänsä havaitsemaan nopeammin uudenlaisia rahanpesutypologioita, vähentämään false positive -hälytysten määrää sekä nopeuttamaan transaktiomonitoroinnin tutkintaprosessejaan. Tarkoituksena ei ole korvata rahanpesun estämisen parissa työskentelevää ihmistyövoimaa vaan luoda olosuhteet, joissa asiantuntija kykenee tekemään parhaan mahdollisen päätöksen laadukkaan tutkintadatan pohjalta. (Chau & Nemcsik, 2020, 17–25.)

4 VIRTUAALIVALUUTAT RAHANPESUN VÄLINEENÄ

4.1 Tutkimusmenetelmä

Tämän tutkielman empiria-aineiston kerääminen on jaettu kahteen osaan. Ensimmäisenä tutkitaan virtuaalivaluuttojen käyttämistä rahanpesun välineenä keräämällä aineistoa integroivan kirjallisuuskatsauksen avulla. Kirjallisuuskatsauksen tavoitteena on sekä kehittää että arvioida olemassa olevaa teoriaa, mutta myös rakentaa uutta. Kirjallisuuskatsauksen tarkoituksena on rakentaa kokonaiskuva tietystä asiakokonaisuudesta. (Salminen, 2011, 3.) Ensimmäisessä empiriaosuudessa pyritään sekä luomaan kokonaiskuvaa virtuaalivaluutoista rahanpesun välineenä että tunnistamaan ilmiöön liittyviä merkittävimpiä ongelmia. Myöhemmin kirjallisuuskatsauksen avulla löydettyä aineistoa rikastetaan puolistrukturoiduilla teemahaastatteluilla pankin näkökulmasta.

Integroiva kirjallisuuskatsaus mahdollistaa systemaattista kirjallisuuskatsausta laajemman lähdeaineiston käyttämisen, mikä on virtuaalivaluuttojen kontekstissa selkeä etu, sillä monipuolista lähdemateriaalia löytyy myös vertaisarvioitujen tutkimusartikkeleiden ulkopuolelta. Integroivassa kirjallisuuskatsauksessa ei ole tarvetta valikoida ja seuloa aihetta käsittelevää kirjallisuutta yhtä tarkasti kuin systemaattisessa kirjallisuuskatsauksessa ja kirjallisuuden tyypit voivat olla tutkimusaineistossa vaihtelevia. (Salminen, 2011, 8.) Virtuaalivaluuttoihin liittyvää rikollisuutta käsitellään artikkeliaineiston lisäksi esimerkiksi kirjajulkaisujen sekä suurimpien lohkoketjuanalytiikkaa tarjoavien yrityksien julkaisujen avulla. Myös alan sääntelyyn liittyvät toimijat ja viranomaistahot julkaisevat aihetta käsitteleviä raportteja. Kattavan kokonaiskuvan saamiseksi myös näiden raporttien tarkastelu on ensiarvoisen tärkeää.

Integroivan kirjallisuuskatsauksen avulla ilmiöön liittyvää tietoa tarkastellaan, kritisoidaan ja syntetisoidaan integraation keinoin, jolloin aiheeseen liittyen löydetään uusia näkökulmia. Integroiva kirjallisuuskatsaus sopii erityisen hyvin uusien ja yhä jatkuvasti muuttuvien aihealueiden tutkimiseen. Integroivan kirjallisuuskatsauksen avulla voidaan löytää dynaamiseen ilmiöön liittyviä epäjohdonmukaisuuksia ja korjata niitä paremmin ajan kuvaa heijastaviksi. (Torraco, 2016, 404–405.) Myös tämä tukee integroivan kirjallisuuskatsauksen valintaa virtuaalivaluuttojen aiheuttaman rahanpesuriskin tutkimisen kontekstissa.

4.2 Tutkimuksen toteuttaminen

Integroiva ja systemaattinen kirjallisuuskatsaus ovat vaiheiltaan lähes identtiset. Integroiva kirjallisuuskatsaus toteutetaan prosessinomaisesti tyypillisesti viidessä eri vaiheessa, jotka ovat tutkimusongelman muotoilu, aineiston kerääminen, aineiston arvioiminen, aineiston analyysi sekä tuloksien kokoaminen (Cooper, 1989, 14). Torracon mukaan (2005, 359) integroiva kirjallisuuskatsaus tulee aloittaa aihealueen käsitteellistämisellä ja olemassa olevan tiedon arvioinnilla. Näin voidaan ymmärtää, mitkä ovat ne potentiaaliset alueet, joista uutta tietoutta kaivataan. Tässä tutkielmassa ilmiötä on käsitteellistetty jo kahdessa aikaisemmassa taustateoriana toimivassa teorialuvussa – virtuaalivaluutat aiheuttavan uudenlaisen rahanpesuriskin. Tietoutta kaivataan erityisesti siitä, miksi ja miten kyseisen riski syntyy. Tutkimusongelmat on asetettu ensimmäisessä luvussa.

Onnistuneessa integroivassa kirjallisuuskatsauksessa tutkija tarkastelee ilmiötä tutkimuksen aihepiirin kannalta olennaisesta näkökulmasta. Tutkijalla on velvollisuus tutustua tutkittavan aihealueen kirjallisuuteen huolellisesti voidakseen osoittaa aikaisemman kirjallisuuden pohjalta relevantteja löydöksiä. Tutkijan tarkoituksena ei ole siten tarkastella kaikkia aikaisempien tutkimuksien näkökulmia. Kirjallisuuskatsauksen aikana on tarkoitus luoda eräänlainen tarina tutkittavasta ilmiöstä analysoimalla kriittisesti saatavilla olevaa aineistoa ja tekemällä uusia johtopäätöksiä sen pohjalta. Integroivan kirjallisuuskatsauksen tuloksien kokoamisen kannalta oleellista on uuden tiedon syntetisointi, jolla tarkoitetaan vanhan tiedon yhdistämistä uusiin havaintoihin, jolloin lopputuloksena saadaan parempi käsitys tutkittavasta ilmiöstä. (Torraco, 2005, 361–363.)

Tämän tutkielman kannalta olennainen näkökulma on erityisesti tunnistaa kaikki ne ominaisuudet, jotka tekevät virtuaalivaluutoista houkuttelevan välineen rahanpesuun sekä ymmärtää erilaisia virtuaalivaluuttoihin liittyviä rahanpesutypologioita. Lisäksi tärkeänä näkökulmana on sääntely. Tässä tutkielmassa vastausta ensimmäiseen tutkimuskysymykseen ”Millaisen rahanpesuriskin virtuaalivaluuttojen käyttäminen rahanpesun välineenä luo?” haetaan mahdollisimman laajan sekä ajantasaisen aineiston avulla, sillä esimerkiksi virtuaalivaluuttojen määritelmä elää yhä edelleen ja aihepiiristä on jatkuvasti saatavilla uutta tietoutta.

4.3 Aineiston hankinta

Virtuaalivaluuttoihin ja rahanpesuun liittyvien tutkimusartikkeleiden sekä viranomaisjulkaisujen määrä on kasvanut viimeisen vuosikymmenen aikana merkittävästi. Koska kyseessä on moniulotteinen ja jatkuvasti muuttuva ilmiö, haluttiin käytettävät tutkimusaineistot jaotella kolmeen päätyyppiin, joita olivat 1. tutkimusartikkelit ja kirjallisuus, 2. viranomaislähteet sekä 3. lohkoketjuanalytiikkaa tarjoavien yritysten julkaisut. Toteuttamalla integroiva kirjallisuuskatsaus tarkastelemalla näitä verrattain erilaisia lähdemateriaalityyppejä saadaan monipuolisempi kuva tutkittavasti ilmiöstä, kuin vain keskittymällä pelkkiin vertaisarvioituihin tutkimusartikkeleihin, joita käytetyssä aineistossa oli kuitenkin kattava osuus.

4.3.1 Tutkimusartikkelit ja kirjallisuus

Aineiston hankinta aloitettiin listaamalla mahdollisimmat monta hakusanaa, joita haluttiin käyttää. Näistä valikoitui käytettäväksi tutkimusartikkeleiden ja kirjallisuuden osalta kaksi erilaista hakusanayhdistelmää. Ensin haettiin aiheeseen liittyviä artikkeleita ja kirjallisuutta kahden eri tietokannan, Tampereen Yliopiston kirjaston hakupalvelu Andorin sekä Google Scholarin, kautta.

Haku	Hakusanat	Tietokanta	Ensimmäisen vaiheen poissulkukriteerit
Haku 1	Money laundering AND (virtual currenc* OR cryptocurrenc*)	Andor	Julkaisuajankohta 2015–2022, julkaisukieli englanti, hakusanojen tulee löytyä aihetasolla, saatavilla kokonaan verkossa
Haku 2	"Money laundering" AND ("Virtual currency" OR "Cryptocurrency")	Google Scholar	Huomioidaan 100 ensimmäistä osuvuuden mukaisesti, julkaisukieli englanti, saatavilla kokonaan verkossa

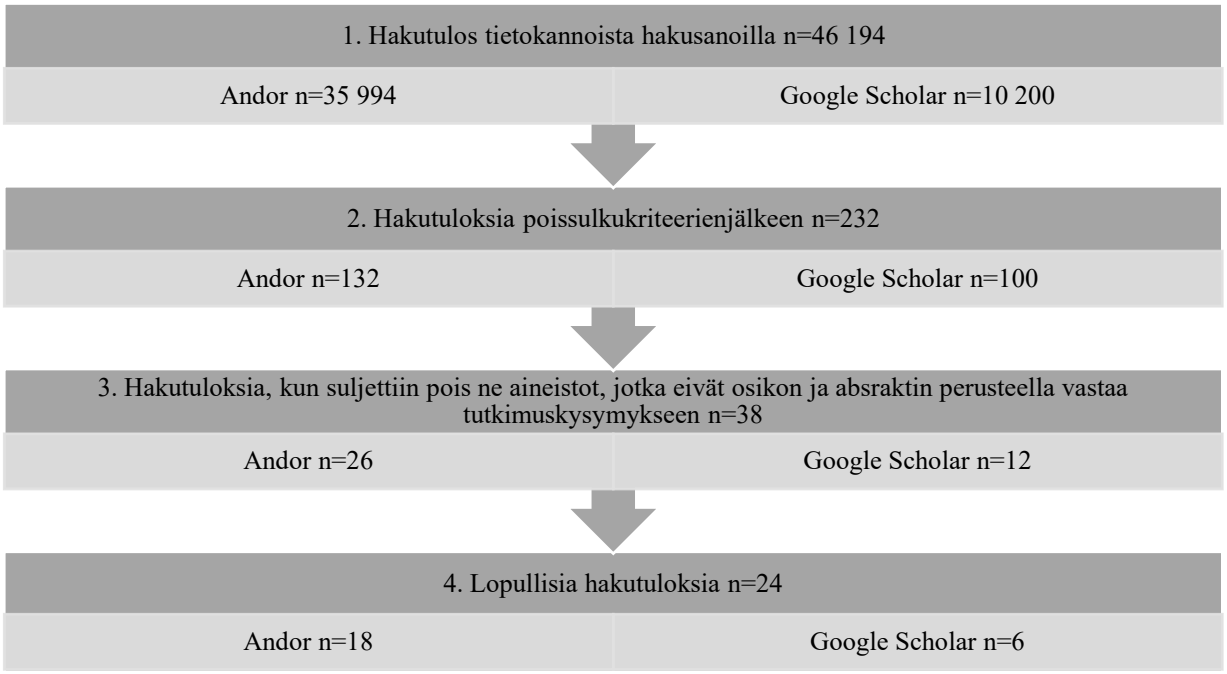
Taulukko 1. Tutkimuskirjallisuuden aineistohaku

Integroivaan kirjallisuuskatsauksen aineistoon liittyy läheisesti sekä sisäänotto- että poissulkukriteerit. Niiden avulla pyritään löytämään mahdollisimman laadukkaat aineistot. (Metsämuuronen, 2006, 37.) Torracon (2005, 365) mukaan aineiston valinnassa tulee huomioida hakusanat, tietokannat, poissulkukriteerit sekä silmämääräisen seulonnan kriteerien määrittäminen. Rahanpesuun viitattiin englanninkielisellä termillä *money laundering.* Rajaamalla hakua siten, että otsikon tulee sisältää kyseinen termi, saadaan samalla hakutuloksiin myös hakutulokset termillä *anti money laundering*. Virtuaalivaluuttoihin viitataan termillä *virtual currency* ja kryptovaluuttoihin *crypto currency*. Haku tehtiin katkaisumerkein, jotta termeistä kelpasi sekä yksikkö- että monikkomuodot. Molempia termejä käytettiin hakutuloksissa Boolen

operaattorilla OR, sillä tutkielmassa aiemmin osoitetun mukaisesti niitä käytetään laajasti toistensa synonyymeina.

Näiden hakusanayhdistelmien perusteella pyrittiin löytämään maailmanlaajuisesti relevantteja tutkimusartikkeleita, jotka käsittelevät virtuaalivaluuttojen kautta tapahtuvaa rahanpesua. Andorissa tehty haku 1 rajattiin koskemaan vain vuosia 2015–2022, sillä hakutulosten ajankohtaisuus haluttiin varmistaa ottaen huomioon ilmiön dynaaminen luonne. Kuten tutkielman taustateoriassa tuotiin esille, on virtuaalivaluuttojen määrittely selkiytynyt vuodesta 2015 alkaen. Google Scholarissa aikarajausta ei tehty, sillä aineistoon haluttiin mukaan myös monipuolisemmin ilmiön alkuajankohtaa käsitteleviä julkaisuja. Ilmiön kokonaisvaltaisen ymmärtämisen kannalta on tärkeää havainnoida myös se, milloin virtuaalivaluuttojen aiheuttama rahanpesuriski on huomioitu ensimmäisen kerran akateemisessa kirjallisuudessa. Sekä Andorin että Google Scholarin kautta löydettiin myös kiinnostavia kirjojen lukuja, jolloin vertaisarviointirajausta ei haluttu käyttää. Lopulliseen aineistoon hyväksyttiin vain englanninkielistä kirjallisuutta. Yhtenä poissulkukriteerinä käytettiin haussa 1 myös koko tekstin saatavuutta. Mikäli aineistoon ei kokonaisuudessaan päässyt yliopiston etäyhteydellä käsiksi, sitä ei käytetty.

Valintaprosessin ensimmäisessä vaiheessa saadut osumat tarvitsivat laajaa rajausta. Mikäli hausta 2 olisi jätetty pois kryptovaluuttojen osuus, olisi tuloksia ollut noin puolet vähemmän. Mahdollisimman monipuolisen aineiston takaamiseksi molemmat hakusanat haluttiin kuitenkin säilyttää. Google Scholarin tarjoama tarkennettu haku ei ollut yhtä kattava kuin Andorin. Näin ollen valintaprosessin toisessa vaiheessa haun 2 osalta aineistoa päädyttiin poissulkemaan Google Scholarin oman rajausominaisuuden perusteella, joka lajittelee tulokset osuvuuden mukaan. Valintaprosessin kolmanteen osioon valittiin osuvuuden mukaan 100 ensimmäistä tulosta, jolloin määrä on linjassa Andorin kautta saatujen hakutulosten kanssa.



Kuvio 7. Tutkimuskirjallisuuden valintaprosessi

Valintaprosessin kolmannessa vaiheessa rajattiin pois ne aineistot, jotka eivät otsikon ja abstraktin perusteella vastanneet ensimmäiseen tutkimuskysymykseen. Tässä kohtaa rajautui pois muun muassa aineistoja, jotka keskittyivät puhtaasti virtuaalivaluuttojen sääntelyyn ilman rahanpesun kontekstia sekä puhtaasti tiettyjen valtioiden lakien näkökulmasta aihetta käsitteleviä julkaisuja. Lisäksi hakujen 1 ja 2 hakutulosten joukossa oli joitakin duplikaatteja, jotka rajattiin pois. Valintaprosessin viimeiseen vaiheeseen valikoitui yhteensä 38 julkaisua, jotka luettiin kokonaisuudessaan. Tämän jälkeen poissuljettiin vielä 14 julkaisua, sillä ne eivät todellisuudessa olleet tutkielman kannalta relevantteja. Viimeisessä vaiheessa rajautui pois muun muassa julkaisuja, joissa rahanpesunäkökulman käsittely jäi pieneksi. Lopullinen aineisto on koottuna liitteessä 2.

4.3.2 Viranomaislähteet

Julkaisija	Käytetyt Hakusanat	Poissulkukriteerit	Hakusanoilla ja poissulkukriteereillä saadut tulokset	Seulonta otsikoiden ja abstraktin perusteella	Koko tekstin perusteella hyväksytyt julkaisut
Keskusrikospoliisi Rahanpesun selvittelykeskus	virtuaalivaluutat ja rahanpesu	vain raporttimuotoiset julkaisut	5	2	2

Finanssivalvonta	rahanpesu* ja virtuaalivaluut*	28	4	2
FATF	Money laundering AND (virtual currenc* OR cryptocurrenc*)	6	5	3
Euroopan Komissio	"money laundering" AND "virtual currencies"	60	10	3
EBA	Money laundering AND (virtual currenc* OR cryptocurrenc*)	20	5	2

Taulukko 2. Viranomaislähteiden aineistohaku

Toisena tutkimusaineiston päätyyppinä käytettiin viranomaislähteitä. Kohteiksi valikoituivat Valtiovarainministeriön (2022) listaamat merkittävimmät rahanpesun estämiseen liittyvät viranomaistahot. Suomalaisia instituutioita edustavat Keskusrikospoliisin alainen rahanpesun selvittelykeskus sekä Finanssivalvonta. Kansainvälisesti merkittävien toimijoiden osalta aineistolähteiksi valittiin FATF, Euroopan komissio sekä Euroopan pankkivalvontaviranomainen EBA. Aineistojen tietokantoina käytettiin instituutioiden omia virallisia nettisivuja, joissa suoritettiin taulukon 2 mukaiset haut. Ainostaan Rahanpesun selvittelykeskuksen tietokannan kautta saatuja hakutuloksia haluttiin rajata poissulkukriteerein, joissa raporttimuodoksi valittiin PDF uutisartikkeleiden poissulkemiseksi.

Seuraavaksi valittiin kaikkien hakutulosten joukosta ne julkaisut, jotka vastasivat haluttuun tutkimuskysymykseen otsikon ja abstraktin perusteella. Nämä julkaisut käytiin läpi kokonaisuudessaan ja poissuljettiin ne julkaisut, jotka eivät olleet tutkielman kannalta relevantteja. Tässä vaiheessa pois karsiutui erityisesti vain tiettyjä maita koskevia raportteja sekä vanhentuneita lausuntoja, joista oli saatavilla uudempi versio. Lopulliseksi aineistoksi valikoitui 12 viranomaisjulkaisua, jotka löytyvät liitteestä 3.

4.3.3 Lohkoketjuanalytiikkaa tarjoavien yrityksien julkaisut

Kolmantena tutkimusaineiston päätyyppinä haluttiin käyttää lohkoketjuanalytiikkaa tarjoavien yrityksien julkaisuja. Useat vertaisarvioidut tutkimusartikkelit sekä esimerkiksi FATF:in julkaisut

käyttävät lähdemateriaalinaan kahden suurimman lohkoketjuanalytiikkaa tarjoavien yritysten, Chainanalysisin sekä Ellipticin julkaisuja. Näiden julkaisujen osalta saadaan kirjallisuuskatsaukseen mukaan myös kvantitatiivista näkökulmaa tutkittavasta ilmiöstä.

Lohkoketjuanalytiikkaa tuottavien yrityksien osalta kirjallisuuskatsaukseen otettiin mukaan tuoreimmat virtuaalivaluuttoja ja rahanpesua käsittelevät julkaisut. Raportit haettiin yritysten nettisivuilta saatavilla olevista materiaalipankeista suodattamalla uusin julkaisuajankohta. Lopulliseksi aineistoksi valikoitui kaksi raporttia, jotka löytyvät liitteestä 4.

4.3.4 Aineiston analyysi ja laadunarviointi

Integroivassa kirjallisuuskatsauksessa löydettyjä aineistoja analysoitiin ja luokiteltiin aineistolähtöisellä sisällönanalyysillä. Aineistolähtöisessä sisällönanalyysissä aikaisemmat havainnot, teoria tai tiedot eivät vaikuta toteutustapaan tai tuloksiin. Aineistolähtöisessä analyysissä ei ole tarkoitus muodostaa etukäteen tiettyjä luokkia tai analyysiyksiköitä, vaan ne muodostuvat tutkimuksen tarkoituksien perusteella. Tutkielman empiriaosuuden ensimmäisessä vaiheessa aineisto pelkistettiin ja ryhmiteltiin aineistolähtöiselle sisällönanalyysille tyypillisellä tavalla. (Tuomi & Sarajärvi, 2018, 80–85.) Aineistojen perusteella tehdyt havainnot jaoteltiin neljään teemaan: ilmiön tunnistamiseen ja sääntelyyn liittyviin havaintoihin, virtuaalivaluuttojen rahanpesuun liitettäviin ominaisuuksiin, virtuaalivaluuttoihin liittyviin rahanpesutypologioihin sekä pankin näkökulmaan. Teemoittelun ideana on korostaa sitä, mitä kustakin teemasta on löydetty. Eri teemoista voidaan puolestaan ryhmitellä erilaisia tyyppejä. (Tuomi & Sarajärvi, 2018, 79.)

Virtuaalivaluuttoihin liitettävää rahanpesuriskiä voidaan tutkia sekä ohjelmistotekniikan näkökulmasta lohkoketjuteknologian kontekstissa, oikeusdogmaattisesta näkökulmasta sääntelyä tarkastelemalla sekä taloustieteellisestä näkökulmasta pohtimalla itse taloudellista houkutinta käyttää virtuaalivaluuttoja rahanpesun instrumenttina. Brenig ym. (2015, 13) esittävät, että ymmärtääkseen kokonaisuutta, tulee tarkastella kaikkia kolmea elementtiä. Tätä jaottelua on hyödynnetty myös tässä tutkielmassa aineiston teemoittelussa. Ensimmäisenä teemana sääntelyn ja ilmiön tunnistamisen osalta aineiston havainnot pyrittiin redusoimaan eli pelkistämään ja ryhmittelemään ne tilastollisiin, kansainvälisiin sekä Euroopan tason havaintotyyppeihin. Toisena teemana aineistosta pyrittiin löytämään virtuaalivaluuttojen eri ominaisuuksia, jotka voidaan liittää rahanpesuun. Samankaltaiset ilmaisut yhdistettiin yhdeksi ominaisuudeksi, jonka jälkeen nämä ominaisuudet taulukoitiin ja niihin liittyviä motivaatiotekijöitä arvioitiin. Toisella teemalla

on vahva linkitys sekä lohkoketjuteknologian teoriaan että taloustieteelliseen näkökulmaan. Kolmantena teemana pyrittiin tunnistamaan virtuaalivaluuttoihin liittyviä rahanpesutypologioita ja ryhmittelemään niitä eri alakategorioihin. Alalukujen 4.4–4.6 avulla pyritään vastaamaan ensimmäiseen tutkimuskysymykseen ja alaluvussa 4.7 kartoittamaan vastauksia kysymyksiin kaksi ja kolme.

Aineistolähtöisen analyysin laatu nojaa luonnollisesti käytettyjen aineistojen laatuun. Analyysissä tulee hyväksyä se perusoletus, ettei ole olemassa puhtaasti objektiivisia havaintoja, vaan on pitkälti tutkijasta riippuvaista, millaisia käsitteitä, tutkimusasetelmaa ja menetelmää käytetään. Tästä syystä on tärkeää, että tutkielman ontologiset lähtökohdat on tuotu esiin ensimmäisessä luvussa. (Tuomi & Sarajärvi, 2018, 81.) Tämän tutkielman aineistoista luotettavimpina voidaan pitää sekä vertaisarvioituja tutkimusartikkeleita että viranomaisjulkaisuja. Koska ilmiötä on vaikea kvantifioida, tulee käytettyjen lohkoketjuanalytiikkaa tarjoavien yrityksien raportteja tarkastella kriittisesti. Kyseessä ei ole tieteellinen lähde, mutta kyseisiä raportteja käytetään tässä tutkielmassa vielä verrattain tuntemattoman alan parhaina käytäntöinä.

4.4 Virtuaalivaluutat rahanpesun välineenä ja sen sääntely

Virtuaalivaluuttoihin, kuten muihinkin talousjärjestelmään liittyviin prosesseihin ja sovelluksiin, liittyy riskinsä (Bystriakov, Guirinskiy, Nan, Hidar & Din, 2020, 179). Elektronisten maksujärjestelmien ensiesiintyminen 1980-luvulla toimi merkittävän käännekohtana rahanpesun kehittymiselle. Rikolliset oppivat nopeasti hyödyntämään uutta saatavilla olevaa resurssia, joka mahdollisti varojen siirtämisen ympäri maailmaa aiempaa nopeammin. Myös Bitcoinin käyttöönotto 2009 ja muiden vaihdantakelpoisten virtuaalivaluuttojen ilmestyminen voidaan nähdä merkittävänä käännekohtana rahanpesun osalta. (Naheem, 2019, 516.) Virtuaali- ja kryptovaluuttoja onkin niiden laillisten käyttötarkoituksien lisäksi yhdistetty myös talousrikollisuuteen ja erityisesti rahanpesuun. (Choo, 2015; Teichmann & Falker, 2020; Dyntu & Dykyi, 2018, 79). Vuonna 2017 eri kryptovaluuttojen markkina-arvon voimakkaan heilahtelun nähtiin johtuvan erityisesti niihin liittyvästä rahanpesuriskistä (Bystriakov ym., 2020, 176). Ramalhon ja Matoksen (2021, 494) mukaan virtuaalivaluutat on yhdistetty jo pitkään osaksi rahanpesua johtuen pitkälti niiden luonteesta monimutkaisina ja keskitetystä valvojatahosta irrallisina toimijoina. Kuitenkin vasta vuonna 2013 ilmeni ensimmäiset merkittävät rikostutkinnat aihepiiriin liittyen, kun Liberty Reserve- ja Sild Road -tapaukset tulivat julkisuuteen. Samanaikaisesti bitcoin alettiin kuitenkin hyväksyä laajemmin myös laillisena maksuvälineenä.

Virtuaalivaluuttoihin liitettävien riskien yhteydessä ei tule kuitenkaan unohtaa virtuaalivaluuttojen tarjoamia mahdollisuuksia ja hyviä puolia. (Ramalho & Matos, 2021, 495.)

Virtuaalivaluutat ovat uniikki rahanpesun väline verrattuna perinteisiin rahanpesun muotoihin, esimerkiksi käteiseen, sillä niitä voidaan hyödyntää kaikissa kolmessa perinteisessä rahanpesuprosessin vaiheessa ja lisäksi ne voivat toimia prosessin aikana sekä talletettavina että nostettavina varoina. Ensimmäisiä virtuaali- ja kryptovaluuttoja ei itsessään luotu alun perin rahanpesun käyttötarkoitusta varten, mutta johtuen lohkoketjuteknologiaan liitännäisistä ominaisuuksista, jatkuvasti kasvavasta virtuaalivaluuttaekosysteemistä ja sääntelyn puutteesta, ne muodostavat nykyään merkittävän rahanpesuriskin. Virtuaalivaluuttaekosysteemillä viitataan itsenäiseen ja suljettuun systeemiin, jossa transaktioita voidaan toteuttaa vain verkostoon osallistuvien käyttäjien kesken. (Desmond, Lacey & Salmon, 2019, 482.) Sekä hajautettuja että keskitettyjä virtuaalivaluuttoja voidaan käyttää rahanpesun välineenä huolimatta niiden erilaisuuksista, mutta compliance -näkökulmasta keskitetyt virtuaalivaluutat ovat vähäriskisempiä (Teichmann & Falker, 2020, 509). Yksi poikkeuksellinen virtuaalivaluuttoihin liittyvä huomio rahanpesun näkökulmasta on, ettei perinteinen pankki ole välttämättä millään tavalla osallinen transaktioihin missään rahanpesun vaiheessa (Naheem, 2019, 521).

Virtuaalivaluuttoihin liitettävä rahanpesuriski on noussut laajemmin keskusteluun viimeisen vuosikymmenen aikana ja sen merkittävyyden odotetaan kasvavan entisestään tulevina vuosina. Virtuaalivaluuttoihin liittyvä ekosysteemi on laaja ja kasvaa vauhdilla, jossa sekä sääntelyviranomaisten että finanssilaitosten on vaikea pysyä mukana. (Goldbarsht, 2022, 161.) Rahanpesun näkökulmasta ekosysteemin haavoittuvaisin osa on virtuaalivaluuttojen vaihdantapalvelut, sillä transaktioita vahvistavilla noodeilla ei ole tietoa kuka asiakas on tai mistä varat tulevat (Naheem, 2019, 518). Virtuaalivaluuttojen osalta huomio rahanpesun kontekstissa on perinteisesti ollut kryptovaluutoissa, mutta myös suljetumpiin virtuaalivaluuttasovelluksiin kuten internet-pelien omiin valuuttoihin ja lentopistejärjestelmiin on yhdistetty rahanpesun riski. Perusajatukseltaan vaihdantakelvoton virtuaalivaluutta voi muuntua vaihdantakelpoiseksi, mikäli sille löytyy jälkimarkkinat darknet-alustoilta. (Goldbarsht, 2022, 161.) Suomessa kansallisen rahanpesun estämisen riskiarvion mukaan virtuaalivaluuttasektoriin kohdistuva kokonaisriskitaso on merkittävä (KRP, 2021, 34).

4.4.1 Tilastoja

Kuten taustateoriassa tuotiin esiin, rahanpesun määrää on vaikea arvioida. Ei siis ole yllättävää, ettei aineiston mukaan ole olemassa tarkkaa dataa siitä, paljonko virtuaalivaluuttoihin liitettävää rahanpesua tapahtuu vuositasolla. Arvioita vaikeuttaa myös se, että virtuaalivaluuttoihin liitettävälle rahanpesulle on tyypillistä sijoittua perinteisen finanssimaailman ulkopuolelle, jossa käytetään anonyymeja identiteettejä sekä rekisteröimättömiä toimijoita. (Desmond, Lacey & Salmon, 2019, 481.) Vuonna 2018 esitettiin, että neljännes bitcoinin käyttäjistä olisi todennäköisesti mukana laittomassa toiminnassa ja että 76 miljardia dollareissa mitattavasta vuosittaisesta laittomien varojen määrästä liittyisi bitcoineihin (Barone & Masciandaro, 2019, 235). Vuoden 2019 tutkimus puolestaan arvioi, että 46 % kaikista bitcoin -transaktioista liittyisi laittomaan toimintaan (Dupuis & Gleason, 2021, 60). Kryptovaluuttojen markkinat ovat kasvaneet viimeisten vuosien aikana valtavasti, joten näitä arvioita tulee tarkastella kriittisesti.

Aineistossa useimmin viitattu lähde tilastojen osalta oli Chainanalysisin tuottamat arviot. Chainanalysisin data keskittyy kuitenkin vain kryptovaluuttojen osuuteen, joten siitä ei voida tehdä yleistyksiä kaikkien virtuaalivaluuttojen osalta. Rahanpesuun käytettyjen kryptovaluuttojen määräksi arvioitiin 8,6 miljardia dollaria vuonna 2021, joka edustaa noin 30 %:n kasvua edelliseen vuoteen verrattuna. Vaikka lukujen odotetaan nousevan oikeuskäsittelyssä etenevien virtuaalivaluuttoihin liittyvien rikostapausten myötä, voidaan havaita laillisen kryptovaluuttakäytön määrän ylittävän selkeästi laittoman käytön. Myös tämä tukee havaintoa siitä, ettei virtuaalivaluuttojen perimmäinen tarkoitus ole liitettävissä rikollisuuteen. Raportin mukaan kryptovaluuttoihin liittyvä rahanpesu on myös todella keskittynyttä, sillä noin 600 kryptovaluuttaosoitteen joukko vastaanotti viime vuonna 54 % kaikista varoista, jotka on pystytty liittämään laittomaan kryptovaluuttatoimintaan. Keskitettyä kryptovaluuttojen rahanpesutoimintaa on pystytty yhdistämään erityisesti venäläisiin toimijoihin. (Chainanalysis, 2022, 10–15.)

Suomen osalta tarkinta tilastodataa aiheeseen liittyen tarjoaa Keskusrikospoliisin alainen Rahanpesun selvittelykeskus. Yleisesti ottaen Suomessa viranomaiselle tehtyjen rahanpesuilmoituksien määrä riippuu vuodesta, mutta virtuaalivaluuttoihin liittyvien ilmoituksien vuosittain nouseva määrä on ollut havaittavissa jo pitkään. Rahanpesun selvittelykeskuksen mukaan virtuaalivaluutat ovat yksi merkittävimmistä ilmiöistä heidän nykyisessä toiminnassaan. Vuoden 2021 ensimmäisellä puoliskolla virtuaalivaluutat liittyivät rahanpesuindikaattorina 38 prosenttiin kaikista rahanpesuilmoituksista. Samalla aikavälillä rahanpesun selvittelykeskus oli

kirjannut 3,4 miljoonaa ilmoitusta pelkästään virtuaalivaluuttapalveluiden tarjoajilta, kun vuonna 2020 vastaava luku koko vuodelta oli vain 8711 ja 2019 vuonna 75. Virtuaalivaluuttatoimijoiden ilmoitusvelvollisuus astui voimaan joulukuussa 2019, mikä selittää ilmoitusten määrän asteittaista nousua vuodesta 2020 alkaen. Virtuaalivaluuttoihin liittyvien rahanpesuilmoituksien määrä on aivan omassa luokassaan verrattuna mihin tahansa muuhun kategoriaan. Kaikista ilmoituksista muiden kuin virtuaalivaluutan tarjoajien tekemiä ilmoituksia oli vain noin 27 000 kappaletta, joista pankit tekivät 7214 ilmoitusta. Keskusrikospoliisi ei ole tarjonnut dataa, moniko pankin tekemistä rahanpesuilmoituksista liittyi virtuaalivaluuttoihin. (KRP, 2021, 2–6.)

4.4.2 Sääntely kansainvälisesti

Ensimmäisten virtuaalivaluuttojen luomisesta 1990-luvulta aina 2010-luvun alkuun asti virtuaalivaluuttoja koskevaa sääntelyä ei juurikaan ollut olemassa (Bandler, 2021, 570). Euroopan Keskuspankki julkaisi vuonna 2012 ensimmäisen virtuaalivaluuttojen riskejä käsittelevän julkaisunsa (Ramalho & Matos, 2021, 498). Vuonna 2014 Yhdysvaltain Valtionvarainministeriön alainen FinCEN linjasi, että rahanpesun estämiseen ja rekisteröintivelvoitteeseen liittyvä sääntely pätee myös virtuaalivaluuttoihin. Tuolloin sääntely osasi kuitenkin ottaa huomioon vain hajautetut virtuaalivaluutat kuten Bitcoinin. (Bandler, 2021, 570). Vaikka sääntelyä on pyritty lisäämään niin Yhdysvalloissa kuin Euroopassakin, hajautetuilla virtuaalivaluutoilla ei ole yhä edelleenkään olemassa keskitettyä hallintoelintä, joka määräisi esimerkiksi rahanpesun estämiseen liittyvästä sääntelystä. Toisaalta, kuten tutkielman taustateoriassa on tuotu ilmi, kryptovaluuttojen osalta alkuperäisenä ajatuksena oli luoda maksuliikennejärjestelmä, jolla ei olisi olemassa yhtä keskitettyä päätäntätahoa.

Vuonna 2014 FATF nosti esiin ensimmäisen kerran virtuaalivaluuttoihin liittyvän rahanpesuriskin (Ramalho & Matos, 2021, 497). Tuolloin riski luokiteltiin kuitenkin matalaksi johtuen puhtaasti vähäisestä tietämyksestä liittyen sekä lohkoketjuteknologiaan että virtuaalivaluuttojen käyttämiseen. Kun erityisesti kryptovaluutat kasvattivat suosiotaan seuraavina vuosina, alkoi myös viranomaisille tehtyjen rahanpesuepäilyilmoitusten (SAR – Suspicious Activity Report) määrä kasvaa. (Wronka, 2022, 83.) Sittemmin FATF on korostanut virtuaalivaluuttojen olevan merkittävä rahanpesuriski ja julkaissut aiheeseen liittyen useita selvityksiä ja ohjeistuksia (FATF, 2019,4).

Sääntelyä käsittelevissä julkaisussa yhteisenä teemana oli nykysääntelyn kuvaileminen puutteelliseksi sekä paremman ja selkeämmän lainsäädännön peräänkuuluttaminen (Sprenger &

Balsiger, 2018; Desmond, Lacey & Salmon, 2019; Dyntu & Dykyi, 2018; Dupuis & Gleason, 2021, 62) Tällä hetkellä sääntelyllä ei ole haluttua vaikutusta johtuen kryptovaluuttojen hajautetusta ja kansainvälisestä luonteesta. Epäjohdonmukaisuus koskien virtuaalivaluuttojen statusta sekä sääntelyä johtaa tilanteeseen, jossa rikolliset voivat hyödyntää katvealuetta siirtymällä aina uudelle sääntelemättömälle alueelle, mikäli heidän toiminnastaan nousee tietyssä valtiossa liikaa kysymyksiä. Sääntelyä pitäisi yhdenmukaistaa kansainvälisellä tasolla, jotta standardoitu lainsäädännöllinen viitekehys voitaisiin muodostaa. Jos kaikki finanssimaailman toimijat käyttäisivät samoja asiakkaan tuntemisen toimintamalleja, ei sääntelyä voisi enää kiertää asettumalla uudelle toimialueelle. (Teichmann & Falker, 2021, 782.)

Teichmanin ja Falkerin tutkimus (2021) keskittyi tarkastelemaan Liechtensteinissa käyttöön otettua lainsäädännöllistä viitekehystä, joka kattaa alleen pelkkiä kryptovaluuttoja laajemmin kaikki lohkoketjuteknologian sovellukset. Tällä tavalla lainsäädäntö pysyy uusien teknologioiden kehityksen vauhdissa. Sääntelemällä lohkoketjun konseptia itsessään eikä keskittymällä sen yksittäisiin sovelluskohtiin, lainsäätäjät voivat poistaa olemassa olevan lainsäädännön vanhentumiseen liittyvän ilmiön ja luoda pitkäkestoista sekä tehokasta sääntelyä, joka hyödyttää sekä virtuaalivaluuttojen käyttäjiä, yrityksiä sekä lainsäätäjiä. Sääntelyn kehittyessä on myös mahdollista, että virtuaalivaluutoilla tapahtuvat kuluttajatransaktiot kielletään kokonaan ja tilalle tulee keskuspankkien liikkeelle laskemaa digitaalivaluuttaa. Mikäli tämänkaltainen tilanne tapahtuisi, olisi selvää, että virtuaalivaluuttaliitännäisestä rahanpesusta tulisi erittäin vaikeaa tai mahdotonta. (Dupuis & Gleason, 2021, 71.)

4.4.3 Sääntely Euroopan tasolla

EU-lainsäädännön tasolla virtuaalivaluutat mainittiin ensimmäisen kerran viidennen rahanpesudirektiivin (AMLD5) yhteydessä vuonna 2018 (EU-komissio, 2019, 97). AMLD5:n tarkoitus oli vähentää virtuaalivaluuttaliitännäistä rahanpesuriskiä, sillä virtuaalivaluuttojen kautta tapahtuvan rahanpesun nähtiin muodostavan vakavan uhan koko EU:n finanssijärjestelmälle. AMLD5 toi sekä virtuaalivaluuttojen vaihdantapalvelut että lompakontarjoajat osaksi lainsäädäntöä ja ne velvoitettiin toteuttamaan rahanpesun estämistä. (Haffke, Fromberger & Zimmermann, 2019, 125; Ramalho & Matos, 2021, 498.) Näin ollen näillä palveluntarjoajilla on nykyään velvollisuus tunnistaa epäilyttävää toimintaa ja ilmoittaa siitä viranomaisille aivan kuten pankeillakin. AMLD5:n yhteydessä annettu määritelmä virtuaalivaluutoista huomattiin kuitenkin nopeasti vanhentuneeksi, sillä samanaikaisesti virtuaalivaluuttaekosysteemi kasvoi ja myös FATF päivitti omia ohjeistuksiaan. Kun finanssimarkkinoille luodaan uutta sääntelyä, on tyypillistä, että

se ei koske kaikkia ekosysteemin osapuolia erityisesti dynaamisten sovellusten kuten virtuaalivaluuttojen yhteydessä.

Nykyisen EU-tasoisen lainsäädännön uudistukset ovat keskittyneet sääntelemään tahoja, jotka mahdollistavat fiat-valuuttojen vaihtamisen virtuaalivaluutoiksi. (Naheem, 2018, 566.) Datinskyn (2020, 44) mukaan helpoin sääntelyn kehittämisen kohde onkin ollut virtuaalivaluuttojen vaihdantapalvelut, sillä yksittäisiä anonyymeja tahoja virtuaalivaluuttaekosysteemissä on mahdotonta säännellä. AMLD5:n ulkopuolelle jäivät muun muassa kokonaan tietyntyyppiset lompakkopalvelut, vain virtuaalivaluuttoja hyväksyvät vaihdantapalvelut (crypto to crypto -toimijat) sekä virtuaalivaluuttojen liikkeellelaskijat. (EU-komissio, 2019, 103.) Haffke, Fromberger ja Zimmermann (2019, 136) ehdottivatkin, että AMLD5:tä tulisi laajentaa koskemaan myös virtuaalivaluuttojen hajauttamiseen tarkoitettuja tumbler- ja mixer-palveluita sekä virtuaalivaluutan liikkeellelaskijoita. Uusin ra hanpesudirektiivi AMLD6 julkaistiin EU:n uuden rahanpesupaketin yhteydessä vuonna 2021, mutta virtuaalivaluuttoja käsittelevän rahanpesun sääntelyn osalta siinä ei ole tapahtunut merkittäviä muutoksia AMLD5: teen verrattuna (Ramalho & Matos, 2021, 498–499).

Toisin kuin monissa muissa Euroopan valtioissa, Suomessa virtuaalivaluutan liikkeellelaskuun tarvitaan viranomaisen myöntämä lupa. Suomessa käytössä olevan rahanpesusääntelyn ja lainsäädännön lähtökohtana voidaan pitää eri finanssitoimijoiden velvollisuutta oman toimintansa riskiperusteiseen arviointiin. Sekä pankkien että virtuaalivaluuttojen liikkeellelaskijoiden on pystyttävä arvioimaan omaa toimintaansa sekä asiakkaisiinsa liittyvää rahanpesuriskiä ja mitoittamaan rahanpesun estämiseen tarkoitetut toimenpiteet vastaamaan arvioitua riskitasoa. Pankeilla tämä tarkoittaa erityisesti sitä, että pankki kykenee tunnistamaan asiakkaansa asianmukaisesti KYC (Know Your Customer) -toimenpiteillä. (Finanssivalvonta, 2021.) Suomessa virtuaalivaluuttatoimijat ovat nähneet tiukentuneen sääntelyn etuna, sillä sen avulla ne ovat saaneet vakiintuneemman toimijan aseman ja ovat pystyneet avaamaan esimerkiksi pankkeihin tilejä (FATF, 2019, 49).

4.5 Virtuaalivaluuttojen rahanpesuun liitettävät ominaisuudet

Virtuaalivaluuttojen käyttämisen suosion nousun myötä kryptovaluuttoihin liittyvän rikollisuuden määrä kasvoi vuonna 2021 edellisiin vuosiin verrattuna. Suurimmat kryptovaluuttoihin yhdistettävissä olevat rikokset liittyivät huijauksiin, darknet-markkinapaikkoihin, varastettuihin varoihin sekä kiristysohjelmiin. (Chainanalysis, 2022, 3.) On tärkeää ymmärtää, että rahanpesu

liittyy tiiviisti kaikkiin näihin rikosmuotoihin, sillä hankittujen rikollisten varojen alkuperä tulee häivyttää ja muuttaa varat sellaiseen varallisuusmuotoon, jossa niitä voidaan kuluttaa tai säilyttää pankissa fiat-valuuttana. Ramalhon ja Matoksen (2021, 495) mukaan vuoden 2013 jälkeen ilmennyt virtuaalivaluuttaliitännäisten rahanpesutapausten nopea kasvu ei yksinään tarkoita, että rikollisuusaste olisi noussut merkittävästi, vaan ennemminkin ilmiö kuvastaa tutkintakeinojen kehittymistä. Virtuaalivaluuttojen rahanpesuun liitettävistä ominaisuuksista puhuttaessa tulee muistaa, että virtuaalivaluutoista on kuitenkin jatkuvasti tulossa myös laajemmin hyväksytty maksuväline maailmanlaajuisesti. Samat ominaisuudet, jotka tekevät niistä houkuttelevia instrumentteja rikolliseen toimintaan, tekevät niistä myös houkuttelevia instrumentteja laillisiin käyttötarkoituksiin.

Yleisesti ottaen virtuaalivaluutat nähdään perinteisiä fiat-valuuttoja houkuttelevampina instrumentteina rahanpesuun (Brenig. ym, 2015, 11). Aineiston perusteella kaikki virtuaalivaluuttojen rahanpesuriskiä käsittelevät tutkimukset ovat melko yksimielisiä nostettaessa esiin rahanpesuun liitännäisiä ominaisuuksia. Taulukkoon kolme on koottu tutkimusaineistosta havaitut virtuaalivaluuttojen ominaisuudet, jotka liittyvät rahanpesuun. Ominaisuudet on jaettu tyypeiltään yleisiin ominaisuuksiin sekä transaktioihin ja kontrolleihin liittyviin ominaisuuksiin. Aineistosta poimittujen havaintojen lukumäärien perusteella merkittävimpinä nähdään virtuaalivaluuttojen pseudo-anonyymi luonne, keskitetyn hallintatahon puuttuminen sekä sääntelyn puutteellisuus. Transaktioihin liittyvien ominaisuuksien osalta merkittävinä etuina nähdään transaktioiden nopeus, reaaliaikaisuus, kansainvälisyys ja helppo hajautettavuus. Useissa tutkimuksissa myös nostettiin esiin, ettei viranomaisilla tai finanssilaitoksilla ole tällä hetkellä käytössään kyvykkyyksiä, joilla transaktioita voitaisiin monitoroida tehokkaasti. Tämä näkökulma on erityisesti tämän tutkielman kannalta relevantti.

Jotta saataisiin kattava kuva virtuaalivaluutoista rahanpesun välineenä, tulee Brenigin ym. (2015, 6) mukaan tarkastella myös rikollisen motivaatiotekijöitä hyödyntää virtuaalivaluuttoja osana rahanpesua. Koska rikolliset käyttävät virtuaalivaluuttoja rahanpesuun, on niihin liitettävien ominaisuuksien motivaatiovaikutus lähtökohtaisesti positiivinen. Suurimmalla osalla taulukossa kolme kuvatuista ominaisuuksista on rahanpesijälle positiivinen motivaatiovaikutus, mutta esimerkiksi virtuaalivaluuttoihin liitettävä korkea volatiliteetti ja vähäiset suorat käyttömahdollisuudet kuluttajahyödykkeisiin ja palveluihin nähdään negatiivisina asioina. Osa ominaisuuksista mainittiin aineistossa sekä positiivisessa että negatiivisessa yhteydessä, jolloin motivaatiovaikutus voi olla molempia.

Ominaisuuden tyyppi	Ominaisuus	Kuvaus	Motivaatio-vaikutus	Esiintyvyys aineistossa
Yleinen	Pseudo-anonyymi luonne	Virtuaalivaluuttoihin ja -tileihin liittyy korkea anonymiteetti	+/-	28
Yleinen	Saavutettavuus	Virtuaalivaluuttoja voi käyttää kuka tahansa internet-yhteydellä, useita eri markkinapaikkoja	+	14
Yleinen	Keskitetyn hallintatahon puuttuminen	Transaktioiden toteutumisesta ei vastaa mikään keskitetty taho	+	24
Yleinen	Hinnan volatiliteetti	Virtuaalivaluuttojen arvo ei ole vakiintunut ja voi vaihdella suuresti	-	6
Yleinen	Vähäriskinen säilytys	Vähäriskisempi säilytys kuin pankkitilillä tai käteisenä	+	2
Yleinen	Käytettävyys	Virtuaalivaluuttoja ei voi käyttää laajasti tuotteiden ja palveluiden hankkimiseen	-	2
Transaktiot	Transaktioiden nopeus ja reaaliaikaisuus	Varoja voidaan tallettaa ja siirtää nopeasti useiden eri tahojen välillä ilman viivettä	+	14
Transaktiot	Kansainväliset maksut	Transaktioita on helppo toteuttaa maailmanlaajuisesti	+	12
Transaktiot	Transaktiokulut	Transaktiokulut ovat matalia tai niitä ei ole	+	3
Transaktiot	Vaihdettavuus	Virtuaalivaluuttoja voi vaivattomasti vaihtaa toisiksi valuutoiksi	+	9
Transaktiot	Hajautettavuus	Virtuaalivaluuttoja voidaan hajauttaa helposti useilla eri keinoilla	+	16
Transaktiot	Suuret volyymit	Transaktioiden suuruudelle ei ole asetettu ylärajaa	+	4
Kontrollit	Sääntely	Ei yhtenäistä kansainvälistä sääntelyä tai valvovaa viranomaista	+	20
Kontrollit	Jäljitettävyys	Finanssilaitoksilla ja viranomaisilla ei lähtökohtaisesti tehokkaita kyvykkyyksiä jäljittää transaktioita lohkoketjussa	+/-	17

Taulukko 3. Virtuaalivaluuttojen rahanpesuun liitettävät ominaisuudet

4.5.1 Yleiset ominaisuudet

Tietynasteinen anonymiteetti on alusta asti ollut virtuaalivaluuttojen avainominaisuus (Crosman, 2015, 1). Koska anonymiteetti ei kuitenkaan ole täydellistä, virtuaalivaluuttoihin liittyvästä anonymiteetistä käytetään perinteisesti termiä pseudo-anonyymiys. Tällä viitataan osittaiseen

anonymiteettiin, joka perustuu siihen, että käyttäjät siirtävät varoja oman nimensä sijasta osoitteiden välillä, joista ei lähtökohtaisesti pysty tunnistamaan virtuaalivaluuttaosoitteen omistajaa (Wronka, 2022, 84; Alarab, Prakoonwit & Nacer, 2020, 11). Lohkoketju itsessään on kuitenkin julkinen: siitä voidaan nähdä transaktiohistoria, lompakoiden arvo, transaktioon liittyvien lähettäjän ja vastaanottajan osoitteet sekä transaktioiden summat. Teoriassa näihin tietoihin pääsee käsiksi kuka tahansa kolmas osapuoli, esimerkiksi viranomainen tai pankki. Osoitteisiin perustuva pseudo-anonyymiys on verrattavissa tilanteeseen, jossa kaikkien kansalaisten tilinumerot ja tilien saldot olisivat kaikkien saatavilla, mutta tilin omistajan nimi on peitetty. (Ramalho & Matos, 2021, 496.) Sijoitusvaiheessa pseudo-anonyymius mahdollistaa muun muassa sen, että virtuaalivaluuttoja voi käyttää anonymiteetin takaa sekä rikolliset että heihin yhdistetyt liikekumppanit. Häivytysvaiheessa puolestaan anonymiteetti takaa sen, ettei epäilyttäviä nimiä tunnisteta, joka mahdollistaa turvallisen toiminta-alueen tunnetuille rikollisille ja terroristeille. Palautusvaiheessa virtuaalivaluuttoja voidaan helposti palauttaa anonyymeille vastaanottajille, joiden nimeä ei voida yhdistää virtuaalivaluuttatiliin, mutta ovat kuitenkin todellisia edunsaajia. (Choo, 2015, 303.) Virtuaalivaluuttojen anonyymi luonne on erityisesti pankkien rahanpesun estämisen näkökulmasta ongelmallista juuri tosiasiallisten edunsaajien tunnistamisen puutteellisuuden takia (Ramalho & Matos, 2021, 494-496).

Koska virtuaalivaluuttoihin liitettävä anonymiteetti ei ole täydellistä, sen motivaatiovaikutus voidaan nähdä myös negatiivisena. Verrattuna esimerkiksi rahanpesun perinteiseen instrumenttiin käteiseen, jää jokaisesta virtuaalivaluuttatransaktiosta pysyvä jälki lohkoketjuun. Käteissiirtoja taas on mahdollista tehdä täysin anonyymillä tavalla. Paradoksaalisella tavalla virtuaalivaluutat mahdollistavat käyttäjälleen korkean anonymiteetin, mutta ovat läpinäkyvämpiä kuin käteinen raha. Toisaalta jotkut virtuaalivaluuttojen palveluntarjoajat eivät vaadi asiakkaaltaan tunnistautumista. (Teichmann & Falker, 2021, 777.) Vuodesta 2014 asti on yritetty luoda täydellisen anonymiteetin takaavia virtuaalivaluuttoja, joiden taustalla oleva lohkoketjuratkaisu eroaa muun muassa Bitcoinista. Tämänkaltaisia virtuaalivaluuttoja kutsutaan nimellä *privacy coins*, mutta niiden puhtaasta anonymiteetistä ei ole saatu vielä täyttä näyttöä (Dupuis & Gleason, 2021, 68.)

Osittaisen anonymiteetin lisäksi rahanpesun kannalta merkittäväksi nähdään keskitetyn hallintatahon puuttuminen, jonka takia esimerkiksi tiedonsaanti viranomaisten ja pankkien osalta on vaikeaa. Mikäli jokin kansallinen valvojataho, esimerkiksi Finanssivalvonta Suomessa, haluaisi saada jonkun tietyn virtuaalivaluuttalompakon tapahtumista lisätietoja, ei ole olemassa sellaista

digitaalista keskitettyä auktoriteettia, joka tietoja voisi luovuttaa. (Ramalho & Matos, 2021, 496–497.) Keskitetyn hallintatahon puuttuessa ei voida olettaa, että virtuaalivaluuttaekosysteemiin olisi implementoitu tehokkaita rahanpesun estämisen toimintoja sisäsyntyisesti (Bandler, 2021, 570).

Virtuaalivaluuttojen ekosysteemissä erityisesti kryptovaluuttamarkkinoihin liittyvä korkea volatiliteetti saattaa aiheuttaa sen, että alkuperäisten pestävien varojen arvo saattaa heilahdella valuutan arvonmuutosten mukana. Lisäksi rahanpesijä altistaa itsensä viruksille ja hakkereille käyttäessään darknetin sovelluksia. (Teichmann & Falker, 2020, 507.) Toinen ominaisuus, jonka motivaatiovaikutus voidaan tällä hetkellä nähdä negatiivisena, on virtuaalivaluuttojen suorien käyttökohteiden pieni määrä. Vaikka virtuaalivaluutoilla hankittavien tuotteiden ja palveluiden määrä tulee tulevaisuudessa oletettavasti nousemaan, on se vielä varsin vähäinen. Näin ollen rahanpesijän tulee palautusvaiheessa muuttaa virtuaalivaluutat ensin fiat-valuutoiksi voidakseen käyttää niitä vapaammin. Suoria käyttökohteita löytyy kuitenkin jo esimerkiksi matkailu- ja tietotekniikka-alalla, jolloin hyödykkeiden ja palveluiden ostoa virtuaalivaluutoilla voidaan käyttää yhtenä rahanpesutypologiana (Sanz-Bas, Rosal, Alonso & Fernandez, 2021, 14–15).

Virtuaalivaluuttoihin liittyy myös laaja saavutettavuus, sillä transaktioita pystyy toteuttamaan kuka tahansa, jolla on tarvittava sovellus ja internet-yhteys. Varoja pystyy siirtämään toiselle henkilölle yksinkertaisesti lataamalla virtuaalivaluuttalompakon puhelimeen ja selvittämällä vastapuolen bitcoin -osoitteen. (Ramalho & Matos, 2021, 488; Wronka, 2022, 84.) Muun muassa Teichman ja Falker (2021, 780) nostivat esiin vähäriskisen säilytyksen näkökulman: laittomaan toimintaan liittyvien virtuaalivaluuttojen säilytys virtuaalivaluuttalompakossa on vähäriskisempää, kuin varojen säilytys esimerkiksi käteisenä tai pankkitilillä anonymiteetin ja valvontatoimenpiteiden puuttuessa.

4.5.2 Transaktioihin liitettävät ominaisuudet

Transaktioihin liitettäviä ominaisuuksia aineistosta nousi kuusi, joista merkittävimpänä nähdään virtuaalivaluuttatransaktioiden helppo hajauttaminen. Rikolliset voivat tallettaa rikollisia varoja useille eri virtuaalivaluuttatileille tai hankkia useita eri valuuttoja. Varoja voidaan myös samanaikaisesti myydä ja nostaa useilta eri tileiltä. Transaktioiden ketjuttaminen ja hajauttaminen on virtuaalivaluuttojen osalta vaivatonta. Lisäksi markkinoilla on saatavilla paljon erilaisia virtuaalivaluuttatransaktioiden hajauttamista helpottavia palveluita kuten mixereitä ja tumblereita. joita käsitellään myöhemmin. Hajauttamisen lisäksi transaktiot ovat nopeita ja niiden vahvistamisessa ei ole pitkäaikaista viivettä. Tämä mahdollistaa sen, että sijoitusvaiheessa

rikolliset varat voidaan nopeasti tallettaa ja siirtää toiselle tilille, muuttaa toiseksi valuutaksi tai siirtää toiseen maahan. (Choo, 2015, 30.)

Erityisesti juuri kansainväliset maksut nähtiin aineistossa usein ongelmallisiksi. Virtuaalivaluuttatransaktioiden toteuttaminen kansainvälisesti on paitsi helppoa, se on myös nopeampaa ja edullisempaa kuin fiat-valuutan kansainväliset transaktiot. (Teichmann & Falker, 2021, 780; Albrecht, Duffin, Hawkins & Rocha, 2019, 213.) Koska transaktiot tapahtuvat reaaliajassa, on niitä vaikea keskeyttää, vaikka epäilyttävää toimintaa olisikin havaittu (Ramalho & Matos, 2021, 497; Wronka, 2022, 84). Rahanpesun kannalta hyödyllisenä mainittiin myös fiat-valuuttoja matalammat transaktiokulut sekä korkean volyymin transaktioiden toteuttamisen mahdollisuus (Desmond ym., 2019, 482; Brenig ym., 2015, 2). Transaktioiden osalta aineistossa ei ilmennyt yhtään ominaisuutta, jonka motivaatiotekijää voitaisiin pitää negatiivisena. Rahanpesuun liitettävät virtuaalivaluuttatransaktioiden ominaisuudet ovat hyvin samankaltaisia kuin jo tutkielman taustateoriassa käsitellyt, mikä tukee ajatusta siitä, että virtuaalivaluutat ovat erittäin houkutteleva rahanpesun instrumentti.

4.5.3 Kontrolleihin liitettävät ominaisuudet

Kontrolleihin liitettävien ominaisuuksien osalta aineistossa korostui yhtenäisen sääntelyn puuttuminen. Sääntelyä kuvattiin joko olemattomaksi tai epäjohdonmukaiseksi aineiston julkaisuvuodesta ja kontekstimaan lainsäädännöstä riippuen. Vältelläkseen tuntemis- ja raportointivelvoitteita, rikolliset usein hakeutuvat käyttämään sääntelemättömiä tai osin säänneltyjä instrumentteja, kuten kryptovaluuttoja. Vaikka virtuaalivaluuttojen käyttö olisi säänneltyä joidenkin toimivaltojen alueella, on viranomaisten silti vaikeaa yhdistää transaktiot tosiallisiin edunsaajiin. (Teichmann & Falker, 2021, 780.)

Virtuaalivaluuttatransaktioiden ja samalla niiden käyttäjien jäljitettävyys nähtiin ongelmalliseksi johtuen pitkälti muista edellä esitellyistä ominaisuuksista kuten keskitetyn hallintatahon puuttumisesta ja pseudo-anonyymistä luonteesta. Teoriassa olisi myös mahdollista luoda ääretön määrä virtuaalivaluuttatilejä, jolloin kaikkia transaktioita olisi mahdotonta hallita (Dyntu & Dykyi, 2018, 79). Finanssilaitoksilla ja viranomaisilla ei lähtökohtaisesti ole käytössään tehokkaita kyvykkyyksiä jäljittää lohkoketjussa olevia transaktioita, jolloin ne joutuvat nojaamaan paljon manuaaliseen tutkintaan sekä päättelyyn. Monitoroinnin kehittämistä käsitellään myöhemmin tässä katsauksessa.

4.6 Virtuaalivaluuttaliitännäiset rahanpesutypologiat ja -indikaattorit

Desmond ym. esittivät tutkimuksessaan (2019, 482–483), että virtuaalivaluutoilla tapahtuva rahanpesu tapahtuu monimutkaisen sosiaalisteknisen systeemin sisällä, joka yhdistää ihmis-, teknologia- ja teknisliitännäisiä elementtejä toisiinsa. Jotta tämänkaltaisen systeemin toimintaa ja virtuaalivaluuttaliitännäisen rahanpesun estämistä voitaisiin ymmärtää, tulee tarkastella systeemin sisäisten komponenttien liitännäisyyttä toisiinsa. Virtuaalivaluuttojen ominaisuuksista sekä ekosysteemin uusista sovelluksista kuten erilaisista mixereista johtuen, virtuaalivaluutoilla tapahtuvien erilaisten rahanpesutypologioiden määrä on jatkuvassa nousussa (Dyntu & Dykyi, 2018, 79).

Virtuaalivaluuttoihin liittyvät rahanpesutypologiat ovat hyvin erilaisia kuin esimerkiksi käteiseen liittyvät, sillä virtuaalivaluuttaa ansaitaan, varastoidaan ja kulutetaan hyvin eri tavalla (Bandler, 2021, 570). Virtuaalivaluuttaliitännäiselle rahanpesulle on ominaista, että virtuaalivaluuttoja voidaan hyödyntää missä tahansa rahanpesun vaiheessa (Desmond ym., 2019, 482; Choo, 2015, 303). Myös taulukossa kolme kuvatut ominaisuudet voivat ilmetä eri tavalla kaikissa perinteisissä rahanpesun vaiheissa. Sijoitusvaiheessa on tyypillistä hankkia rikollisilla varoilla virtuaalivaluuttoja. Tämä voidaan tehdä joko lataamalla virtuaalivaluuttalompakko, virtuaalivaluutta-automaattien kautta tai ostamalla virtuaalivaluuttaa käteisellä kasvotusten suoraan myyjältä. Myös jotkut pankit saattavat vaihtaa käteistalletuksia kryptovaluuttoihin. (Teichmann & Falker, 2020, 506; Wronka, 2022, 85.) Häivytysvaiheessa on tyypillistä toteuttaa useita eri virtuaalivaluuttatransaktioita eri vaihdantapalveluiden ja -lompakoiden välillä. Palautusvaiheessa virtuaalivaluutta pyritään muuttamaan tyypillisesti fiat-valuutaksi tai hankkimaan virtuaalivaluutalla suoraan hyödykkeitä ja palveluita. (Wronka, 2022, 86–87; Desmond ym., 2019, 482.)

Alaluvuissa 4.6.1–4.6.3 on eritelty aineiston perusteella kuusi erilaista rahanpesutypologiaa. Näiden lisäksi yksittäisinä nostoina aineistosta havaittiin myös mahdollisuus käyttää virtuaalivaluuttoja perinteisten fiat-valuuttoihin yhdistettävien rahanpesutypologioiden tapaan kuten esimerkiksi Hawala-järjestelmiä hyödyntämällä (Bystriakov ym., 2020, 179). Rahanpesua voi tapahtua myös perinteisten virtuaalivaluuttojen vaihdantapalveluiden kautta. Myös muulitoiminta, jossa tuntemattomia tahoja pyydetään korvausta vastaan avaamaan lompakko ja toteuttamaan transaktiot rikollisen puolesta, on tyypillistä. (Wronka, 2022, 85–88). Uutena ilmiönä esiin on noussut myös prepaid virtuaalivaluuttaluottokortit, joita voi käyttää muun muassa verkko-ostoksiin (Sanz-Bas, 2021, 15).

4.6.1 Mixereiden ja tumblereiden käyttö

Niin kutsuttujen mixer ja tumbler -palveluiden käyttö on yleistynyt viidennen rahanpesudirektiivin myötä, sillä se ei velvoita kyseisiä palveluita (Haffke ym., 2019, 130). Palveluihin liitettävät kontrollien ja ilmoitusvelvoitteiden puute houkuttelee rahanpesijöitä käyttämään niitä virtuaalivaluuttojen alkuperän häivyttämiseen. (Ramalho & Matos, 2021, 501–503.) Mixerit ja tumblerit ovat anonymisointipalveluita, jotka häivyttävät yksittäisten transaktioiden yhteyden toisiinsa niin, ettei alkuperäistä lähettäjäosoitetta pystytä enää tunnistamaan (Goriacheva, Jakubenko, Pogodina & Silnov, 2017, 47; Haffke ym., 2019, 129). Mixereiden ja tumblereiden toiminta eroaa hieman toisistaan, mutta eroavaisuuksien käsittely ei tässä kontekstissa ole olennaista. Anonymisointipalveluiden käyttö on perinteisesti keskittynyt tunnetuimpiin kryptovaluuttoihin kuten Bitcoiniin, Litecoiniin ja Ethereumiin (Dupuis & Gleason, 2021, 66).

Käytettäessä tumblereita tai mixereitä, kryptovaluuttaa siirretään aluksi clearnet -lompakosta yhteen piilotettuun lompakkoon darknetissä (Dyntu & Dykyi, 2018, 79). Jokainen transaktio muodostaa niin kutsutun ”hopin”. Useita ”hopeja” voidaan tehdä peräkkäin ja jokainen ”hop” lisää aina yhden naamioidun kerroksen alkuperäisiin varoihin. Kun varat on asetettu darknet -lompakkoon, rahanpesijä voi alkaa sekoittamaan niitä. Mixer -palvelu jakaa automaattisesti esimerkiksi bitcoinit pienempiin osiin ja käyttää useita transaktioita ohjatakseen ne eri darknet -osoitteisiin satunnaisin aikavälein. Näin ollen transaktioita ei enää voida linkittää toisiinsa. Tämän jälkeen alkuperäinen kokonaissumma bitcoineja kootaan jälleen kasaan käyttäen toista darknet -lompakkoa. (Teichmann & Falker, 2020, 506–507.) Kun varojen alkuperä on häivytetty ja ne muutetaan fiat-valuutoiksi pankkien kautta, ei rahanpesijällä ole enää ongelmaa joutua vastaamaan rahanpesun estämiseen liittyviin kysymyksiin (Teichmann & Falker, 2020, 507). On kuitenkin liian suoraviivaista yhdistää mixer- ja tumbler- palveluiden käyttäminen aina rahanpesuun. Henkilö saattaa esimerkiksi haluta suojata henkilökohtaisia tietojaan kolmansilta osapuolilta. Tästä syystä palvelut eivät ole vielä itsessään laittomia. (Ramalho & Matos, 2021, 502–503.)

4.6.2 ICO:t ja reguloimattomat vaihdantapalvelut

Myös virtuaalivaluuttojen liikkeellelaskuun ja joukkorahoittamiseen liittyvä ICO voi olla tehokas rahanpesutypologia. ICO:t kasvattivat suosiotaan vuoden 2017 jälkeen, kun viisi suurta kryptovaluuttaa keräsi annin kautta lähes 700 miljoonaa dollaria. Rahanpesun osalta ICO:ihin voidaan liittää kolme elementtiä: sijoitettujen varojen tuotto, riski yrityksen selviämisestä ja legitimiteetistä sekä kiinnijäämisen riski. ICO:jen kautta tapahtuvassa rahanpesussa rikolliset varat

sijoitetaan uuteen virtuaalivaluuttaan. Mikäli virtuaalivaluutta menestyy, varat saadaan takaisin näennäisesti laillisina. Yhdysvalloissa arvopaperimarkkinoita valvoja SEC on ollut pitkään huolestunut ICO:ihin liittyvästä rahanpesuriskistä ja on aloittanut useita tutkintoja ICO:ihin liitettäviä toimijoita kohtaan. (Barone & Masciandaro, 2019, 240–243.) ICO:jen taustalla olevat toimijat ovat tyypillisesti ohjelmistokehittäjiä, jotka eivät itse osallistu aktiivisesti kyseisellä kryptovaluutalla tapahtuvaan kaupankäyntiin (Datinsky, 2020, 43). Tämä voidaan nähdä riskiä lisäävänä.

Yksi mahdollisuus rahanpesuun on hyödyntää reguloimattomia virtuaalivaluutan vaihdantapalveluita, joilla ei ole käytössään kunnollisia KYC tai AML-toimintoja. Usein tämänkaltaisessa toiminnassa hyödynnetään kryptovaluuttojen vaihtamista toisiin kryptovaluuttoihin saman vaihdantapalvelun sisällä, jolloin varoille muodostuu jälleen useita kerroksia kuten aiemmin kuvatussa ”hop” -metodissa. (Teichmann & Falker, 2020, 507.) FATF on linjannut, että kansallisen tason sääntelyn yksi kehityskohta olisi poistaa reguloimattomien vaihdantapalveluiden olemassaolo kokonaan (Sanz-Bas, Rosal, Alonso & Fernandez, 2021, 13).

4.6.3 Virtuaalivaluutta-automaatit ja erilaiset välittäjäpalvelut

Sijoitusvaiheessa voidaan hyödyntää muun muassa virtuaalivaluutta-automaatteja sekä erilaisia välityspalveluita kuten paikallisia välittäjiä sekä OTC-välittäjiä. Virtuaalivaluutta-automaatit ovat nimensä mukaisesti fyysisiin käteisautomaatteihin rinnastettavia laitteitta, joihin käyttäjä voi tallettaa fiat-valuuttaa ja vastaanottaa saman määrän bitcoineja kryptovaluuttalompakkoonsa (Sanz-Bas, 2021, 14). Nykyisin myös virtuaalivaluutta-automaatteja on alettu sääntelemään enemmän ja esimerkiksi Saksassa automaattien asiakasdataa säilötään systemaattisesti. Tästä syystä niiden käytön rikollisissa piireissä uskotaan vähentyneen. (Wronka, 2022, 85.)

Paikallisilla välittäjillä tarkoitetaan toimijoita, jotka tarjoutuvat vaihtamaan virtuaalivaluuttaa käteisvaroja vastaan. Toiminta sovitaan tyypillisesti internetin keskustelualustoilla ja kaupat toteutetaan kasvokkain. (Sanz-Bas, 2021, 13.) Niin kutsutuilla Over the Counter -välittäjillä tarkoitetaan puolestaan toimijoita, jotka mahdollistavat virtuaalivaluuttatransaktioiden toteuttamisen yksityisten myyjien ja ostajien välillä, jotka eivät halua käyttää julkisia vaihdantapalveluita (Teichmann & Falker, 2021, 777). OTC-vaihdantapalveluiden volyymin on arvioitu olevan jopa kolmin- tai nelinkertainen verrattuna julkisiin vaihdantapalveluihin. Yksinkertaisuudessaan OTC-välitys voi olla kahden julkisen avaimen vaihtaminen ostajan ja myyjän välillä. (Dupuis & Gleason, 2021, 68.)

4.6.4 Virtuaalivaluuttoihin liitettäviä rahanpesuindikaattoreita

Aineiston perusteella voidaan tunnistaa tiettyjä asiakkaan käyttäytymisestä havaittavia rahanpesuindikaattoreita, jotka saattavat olla liitettävissä virtuaalivaluuttojen kautta tapahtuvaan rahanpesuun. Havainnot voidaan jakaa karkeasti transaktio- ja tuntemistietoliitännäisiin indikaattoreihin. (KRP, 2021, 34–35) Asiakkaalla viitataan aineistossa yleisesti sekä pankkien että virtuaalivaluuttatoimijoiden asiakkaisiin, jotka toteuttavat virtuaalivaluuttatransaktioita.

Indikaattorin tyyppi	Rahanpesuindikaattori
Transaktiot	Asiakas tekee poikkeuksellisen suuria saapuvia tai lähteviä maksuja, jotka eivät sovi asiakkaan varallisuuteen tai riskiprofiiliin (Naheem, 2018, 270).
Transaktiot	Asiakas ei pysty osoittamaan virtuaalivaluuttojen alkuperää niiden hankinta-ajankohtaan asti (Naheem, 2018,270).
Transaktiot	Asiakas tallettaa käteistä ja siirtää tämän jälkeen varat välittömästi virtuaalivaluutan vaihdantapalvelulle (Sprenger & Balsiger, 2018, 2).
Transaktiot	Moni asiakas lähettää samanaikaisesti samankaltaisia summia tietylle virtuaalivaluuttatarjoajalle (Sprenger & Balsiger, 2018, 2).
Transaktiot / Tuntemistiedot	Asiakas tekee virtuaalivaluuttoihin liittyviä siirtoja ja nostoja useita kertoja päivässä pienemmillä summilla. Kyseessä saattaa olla tarkoituksenmukainen valvontakontrollien välttely. Laittomiin osoitteisiin yhdistetyt virtuaalivaluuttasiirrot jäävät tyypillisesti alle 1000 dollarin rajan johtuen yli kyseisen rajan menevien maksujen compliance-velvoitteista (Chainanalysis, 2022, 13).
Tuntemistiedot	Asiakas kysyy lisätietoja transaktioiden valvontaan liittyvistä raja-arvoista sekä sääntelyvaatimuksista ennen asiakkuuden avaamista. (KRP, 2021, 35.)
Transaktiot	Aiemmin esiteltyjen hajautuspalveluiden käyttäminen (Finanssivalvonta, 2019, 28; Naheem, 2018, 270).
Transaktiot	Varojen alkuperäselvitykseen liittyy puutoksia ja epäselvyyksiä (Finanssivalvonta, 2019, 28; FATF, 2019, 26)
Transaktiot / Tuntemistiedot	Asiakas suorittaa maksuja sellaiselle virtuaalivaluuttatoimijalle, joka toimii puutteellisten AML-kontrollien valtiossa (KRP, 2021, 35).
Tuntemistiedot	Asiakkaalla havaitaan yhteyksiä, matkustamista tai virtuaalivaluuttatransaktioita esimerkiksi Venäjälle, Iraniin, Pohjois-Koreaan, Ukrainaan tai Turkkiin (Sprenger & Balsiger, 2018, 2).

Taulukko 4. Virtuaalivaluuttoihin liitettäviä rahanpesuindikaattoreita

4.7 Virtuaalivaluutat rahanpesuriskinä pankille

Pankkisektorilla alkoi 1970-luvulla tehokkaan pohjan rakentaminen rahanpesun estämiseen liittyen, joka perustui pankkien sääntelyn velvoittamaan rooliin monitoroida niiden kautta tapahtuvaa maksuliikennettä ja saada asiakkailta epäilyttävistä transaktioista tarvittavat selvitykset. Mikäli asiakas ei kykene antamaan tarvittavia selvityksiä, on pankilla velvollisuus ilmoittaa epäilyistä viranomaisille. Virtuaalivaluutat ovat kuitenkin rikkoneet tämän pohjan, sillä pankki ei välttämättä enää kykene monitoroimaan ja jäljittämään virtuaalivaluuttatransaktioita johtuen niiden tarjoamasta anonymiteetistä sekä sääntelyn puutteesta. (Bystriakov ym., 2020, 178–179.) Teichmann ja Falker haastattelivat vuoden 2020 tutkimuksessaan 70 rahanpesun estämisen asiantuntijaa, joiden mukaan rahanpesun estämisen parissa työskentelevä tutkija törmää harvoin arkityössään virtuaalivaluuttaliitännäiseen rahanpesuun. Tämä ei kuitenkaan ole indikaattori ilmiön harvinaisuudesta vaan pikemminkin siitä, että pankilla on rajalliset mahdollisuudet havaita virtuaalivaluuttoihin liittyviä rahanpesutypologioita. Vaikka pankeilla ei ole tällä suoraa yhteyttä virtuaalivaluuttaekosysteemiin eivätkä ne ole nykyisen virtuaalivaluuttasääntelyn kohteita, ei tämä tarkoita, etteikö pankkien tulisi tehdä asialle mitään.

4.7.1 Virtuaalivaluuttaliitännäisen rahanpesun estäminen

Crosman (2015) esittää, että pankkien tulisi huomioida rahanpesuriskejä tarkastellessaan myös pankin asiakkaina olevat virtuaalivaluuttojen tarjoajat ja vaihdantapalvelut. Pankin tulee tuntea millaiseen toimintaan niiden tilien kautta kulkevat varat linkittyvät. Asiakkaan tuntemisen näkökulmasta pankin tulee ymmärtää, millainen transaktiokäytös on tyypillistä virtuaalivaluuttatoimijoille ja puuttua mahdollisiin anomalioihin. Lisäksi virtuaalivaluuttatoimijoita tulisi käsitellä korkean riskin asiakkuuksina. Pankkien tulee sääntelyn velvoittamana tuntea asiakkaidensa maksuliikenne, mutta harmaaksi alueeksi jää, paljonko pankkien tulee olla tietoisia siitä, mitä heidän asiakkaidensa asiakkaat tekevät.

Aineiston perusteella pankkien suurimmat haasteet virtuaalivaluuttojen aiheuttaman rahanpesuriskin hallintaan liittyen ovat muun muassa yhtenäisen sääntelyn puute sekä olemassa olevan sääntelyn muuttuminen, viranomaisten toiminta, aiheen kansainvälisyys ja nopeasti kehittyvän teknologian hallitseminen. Jotta pankki voisi liittää virtuaalivaluutat rahanpesun estämisen viitekehykseensä ja strategiaansa, tulee pankin ymmärtää millä eri tavoilla riski voi ilmetä (Naheem, 2019, 524). Henkilöstön kouluttamisen osalta tulee Ramalhon ja Matosin (2021, 491) mukaan huomioida kokonaisvaltainen ymmärrys virtuaalivaluutoista: jotta maksujen ja

rahanpesutypologioiden moninaisuutta voitaisiin ymmärtää, tulee pankissa työskentelevien rahanpesun estämisen asiantuntijoiden tietää, miten yksittäinen transaktio tapahtuu. Kokematon tutkija saattaa Ramalhon ja Matosin mukaan tehdä vääriä päätelmiä varojen alkuperästä, mikäli hän ei ymmärrä lohkoketjutransaktioiden välistä suhdetta.

Keskusrikospoliisi on lausunnossaan liittyen virtuaalivaluuttapalveluiden rahanpesun estämisen toimenpiteisiin todennut, että toimijoiden tulisi tunnistaa asiakkaisiin, tuotteisiin, palveluihin ja toimitustapoihin liittyvät korkean riskin tilanteet. Asiakkaisiin liittyen tällaisia tilanteita ovat muun muassa asiakkaan etätunnistamiseen liittyvät seikat, poikkeuksellisen suuret transaktiovolyymit sekä tilanteet, jossa asiakas ei kykene selvittämään varallisuuden alkuperää. Palveluihin liittyviä korkean riskin tilanteita on KRP:n mukaan esimerkiksi mixereiden ja muiden varojen alkuperää häivyttävien teknologioiden käyttö. Maantieteellisenä riskinä nähdään puolestaan tilanteet, joissa asiakkaalla tai liiketoimella on liittymäkohta valtioon, jonka rahanpesun estämisen toiminnot eivät täytä kansainvälisiä velvoitteita. Riskinä tulisi myös nähdä se, mikäli asiakkaan liiketoimet liittyvät konfliktialueisiin tai niiden lähialueisiin. (Finanssivalvonta, 2019, 22–25.) Kuten tutkielmassa aiemmin on tuotu ilmi, pankin velvollisuus on tuntea asiakkaansa ja heidän maksuliikenteensä. Ei ole syytä nähdä, etteikö Keskusrikospoliisin kuvailemien asiakkaiden korkean riskien tilanteiden tunnistaminen olisi myös tehokas virtuaalivaluuttaliitännäisen rahanpesuriskin hallitsemisen keino pankille.

4.7.2 Tulevaisuuden mahdollisuuksia

Choo (2015, 305) ja Wronka (2022, 89) ovat esittäneet, että pankkien kehittämien AML-strategioiden tulisi olla mahdollisimman ajantasaisia, jotta niiden avulla voitaisiin huomioida myös uudet maksuliikenteen sovellukset kuten virtuaalivaluutat. Pankin tulisi ennen kaikkea varmistua, että sen tekniset kyvykkyydet virtuaalivaluuttojen monitorointiin ovat ajantasaisia. Tarvittaessa resursseja tulisi kohdentaa sekä ICT-toimintoihin että henkilöstön kouluttamiseen. Myös alan osaajien lisärekrytoinnit nähdään tarpeellisiksi.

Lohkoketjun analysointi ja transaktioiden jäljittäminen julkisesta tilikirjasta ei ole kiellettyä, ja myös pankkien tulisi kehittää kyvykkyyksiä tähän. Lisäksi kansallisten viranomasitahojen yhteistyötä on kehitettävä (Teichmann & Falker, 2021, 785). Crosman esitti jo vuonna 2015, että pankkien tulisi tehdä yhteistyötä lainsäätäjien sekä tietosuoja- ja virtuaalivaluuttatoimijoiden kanssa, jotta voitaisiin ottaa askel kohti ”bitcoin-banking” aikaa, jossa virtuaalivaluuttoihin liittyvät riskit hallitaan kokonaisvaltaisesti. Kansainvälisesti erityisesti FATF on painottanut virtuaalivaluuttoihin liittyvän rahanpesuriskin hallitsemisessa neljää osa-aluetta: riskin

kokonaisvaltaista ymmärtämistä, selkeää ohjeistusta, henkilöstön koulutusta sekä tiedonvaihtoa. Tehokkaan tiedonvaihdon tulisi sisältää niin yksityisen kuin julkisenkin sektorin toimijat: perinteiset finanssilaitokset, virtuaalivaluuttatoimijat, poliisin sekä paikallisen valvojatahon. FATF painottaa, että tiedonkulun kuuluisi valua viranomaistahoilta yksityisille tahoille ja yksityisen sektorin toimijoita tulisi auttaa ymmärtämään paremmin sääntely- ja raportointivaatimuksia. (FATF, 2019, 37–39.)

Aineistossa toistui useasti kantava ajatus siitä, että puutteellinen virtuaalivaluuttoihin liittyvä sääntely on myös vaikeatulkintaista. Viranomaisyhteistyön yhtenä muotona on esitetty mahdollisuus luoda niin kutsutut whitelistattujen ja blacklistattujen tahojen listat. Sellaiset lompakot, jotka kuuluvat luotettavaksi tunnistetuille taholle, voitaisiin kirjata omaan listaansa ja vastaavasti rikolliseen toimintaan yhdistetyt lompakot toiseen. Ongelmaksi muodostuu kuitenkin se, että listat eivät voi olla julkisesti saatavilla väärinkäytössyistä. (Wronka, 2022, 90–91.) Mikäli tämänkaltaiset listat olisivat olemassa, myös pankit voisivat hyödyntää niitä.

Yhtenä oleellisimpana kehityskohteena pankkien ja viranomaistahojen osalta nähdään järjestelmätuetun transaktiomonitoroinnin kehittäminen niin, että se soveltuu myös virtuaalivaluuttatransaktioiden jäljittämiseen. Virtuaalivaluuttojen osalta itse transaktioiden tunnistaminen virtuaalivaluuttaliitännäisiksi on olennaista. Eri toimijoiden tulisi myös hyödyntää esimerkiksi Chainanalysisin ja Ellipticin kaltaisten yrityksien tuotteita, jotka hyödyntävät julkista lohkoketjua ja jäljittävät transaktioita rahanpesun estämisen tarkoitukseen (Alarab ym., 2020, 11; Dyntu, 2018, 269; Dupuis & Gleason, 2021, 61). Näitä palveluita on hyödyntänyt jo muun muassa FBI ja Interpol. Lohkoketjuanalytiikan avulla voidaan tunnistaa ihmissilmää tarkemmin rahanpesua indikoivia tilanteita. (Wronka, 2022, 92–93.) Crosmanin (2015) mukaan niin kauan, kun Chainanalysisin kaltaisille yrityksille on tarvetta, ovat pankkien omat monitorointikyvykkyydet puutteellisia. Hän kuitenkin esittää, että näiden yrityksien koko olemassaolo herättää kysymyksen siitä, uhataanko virtuaalivaluuttakäyttäjien yksityisyyttä liikaa, mikäli esimerkiksi pankit käyttäisivät näitä järjestelmiä löytääkseen sääntelyn edellyttämällä tavalla transaktioiden taustalla olevan todellisen edunsaajan.

Useat tutkijat ovat todenneet, että lohkoketjuteknologiaa voitaisiin mahdollisesti myös hyödyntää rahanpesun estämisen keinona, mikäli sitä ymmärrettäisiin paremmin (Naheem, 2019, 524; Sprenger & Balsiger, 2018, 3) Suurin osa pankeista ei hyödynnä lohkoketjuteknologiaa toiminnassaan, minkä takia ymmärryksen ja osaamisen taso ei ole samalla tasolla, kuin esimerkiksi

lohkoketjuteknologiaa hyödyntävillä virtuaalivaluuttatoimijoilla. Naheemin (2019, 524) mukaan helpoin tapa tietouden lisäämiseksi olisi sisällyttää lohkoketjuteknologian sovellusten käyttäminen osaksi pankin omia toimintoja. Rahanpesun estämisen ja rahanpesuriskin hallinnan osalta on ehdotettu, että lohkoketjuteknologiaa voitaisiin hyödyntää esimerkiksi rahanpesuepäilyilmoitusten kirjaamiseen sekä tosiasiallisten edunsaajien tunnistamiseen. Olisi ensiarvoisen tärkeää sisällyttää virtuaalivaluuttojen aiheuttamat rahanpesuriskit osaksi pankin käyttämää rahanpesuriskin hallintaan liittyvää viitekehystä.

5 VIRTUAALIVALUUTTOJEN AIHEUTTAMA RAHANPESURISKI PANKEILLE JA SEN HALLINTA

5.1 Tutkimusaineiston kuvaus ja kerääminen

Tutkielman empiriaosuuden toinen vaihe toteutettiin puolistrukturoituina teemahaastatteluina. Jokaisesta riskienhallinnan kolmesta puolustuslinjasta oli edustettuna ainakin yksi asiantuntija. Puolistrukturoiduilla teemahaastatteluilla saatiin rakennettua vähemmän tunnetusta aihepiiristä monipuolisempaa kuvaa, jolloin tutkielman tavoitteiden mukaisesti pystyttiin vahvistamaan aiempaa teoriaa sekä ensimmäistä empiriaosuutta. Lisäksi pystyttiin lähestymään virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä monipuolisesti eri riskienhallintatoimintojen näkökulmasta.

Haastateltavina olivat asiantuntija talousrikollisuuden torjunnasta, kaksi asiantuntijaa compliance-toiminnoista sekä yksi sisäisestä tarkastuksesta. Kaikki haastateltavat edustivat samaa suomalaista pankkia. Kyseiset tahot koettiin tämän tutkielman kannalta relevanteiksi kohteiksi, sillä tutkielma nojaa vahvasti pankkien riskienhallintaan, jossa kolmen puolustuslinjan malli on yleisesti käytetty riskienhallintamalli. Haastattelukysymykset pyrittiin muodostamaan niin, etteivät kysymykset liittyneet kyseisen pankin prosesseihin vaan laajemmin asiantuntijoiden omiin näkemyksiin ilmiöstä. Haastattelujen avulla haluttiin rikastaa ja testata sekä teoriapohjaa että kirjallisuuskatsauksessa löytynyttä aineistoa. Haastattelujen pohjalta saatu aineisto analysoitiin samalla metodilla kuin ensimmäisessä empiriaosuudessa ja se jaettiin haastattelurungon mukaisesti kahteen teemaan.

Haastateltavat saivat mahdollisuuden tutustua haastatteluteemoihin ja -kysymyksiin ennen varsinaista haastattelua sekä oikolukea valmis analyysi haastatteluiden pohjalta. Haastattelut toteutettiin maaliskuussa 2022 videotapaamisina ja ne kestivät noin 45 minuuttia. Itse haastatteluja toteutettiin kolme, sillä toisen puolustuslinjan asiantuntijat haastateltiin yhdessä. Tapaamiset nauhoitettiin, jotta tutkijalle annettiin mahdollisuus keskittyä itse haastattelutilanteeseen ja esittää täydentäviä kysymyksiä. Haastattelumateriaalin peruslitterointi toteutettiin haastatteluiden kanssa samana päivänä, jotta tulkintaeroja ehtisi syntyä mahdollisimman vähän. Haastateltavien nimiä ei tuoda esiin, mutta lukijalle tarjotaan taustatiedot henkilöiden työtaustoista luotettavuuden lisäämiseksi.

Asiantuntija A työskentelee ensimmäisessä puolustuslinjassa analyytikkona talousrikollisuuden torjunnassa, jossa hänen päävastuualueenaan on erilaiset kehitystehtävät rahanpesun estämisen toimintojen parissa. Hänellä on kokemusta erityisesti virtuaalivaluuttojen osa-alueella, jossa hän on ollut mukana luomassa muun muassa yrityksen sisäistä ohjeistusta. Hänellä on ohjelmistokehitysinsinöörin koulutus kesken.

Asiantuntija B työskentelee toisessa puolustuslinjassa compliance -alueen vastuuhenkilönä. Hänen vastuulleen kuuluu muun muassa sääntelyn noudattamisen varmistaminen sekä ohjeistuksiin ja koulutukseen liittyvät vastuut. Asiantuntija B:llä on lähes 20 vuoden kokemus alan tehtävistä. Koulutukseltaan hän on juristi, jonka lisäksi hän on lukenut myös kauppatieteitä.

Asiantuntija C työskentelee myös toisessa puolustuslinjassa compliance- alueen vastuuhenkilönä. Hänen vastuualueellaan on muun muassa riskilausuntojen antaminen, erilaiset valvontatehtävät sekä liiketoimintoja tukevat tehtävät. Hänellä on 23 vuoden kokemus rahoitusalalta, joista viimeisimmät vuodet toisen puolustuslinjan vastuiden parissa. Ennen sitä hän on toiminut myös rahanpesun estämisen ja pakotteiden parissa. Koulutukseltaan hän on juristi.

Asiantuntija D työskentelee kolmannessa puolustuslinjassa tarkastuspäällikkönä. Hänen vastuualueellaan on tarkastusten toteuttaminen, laadunarviointi ja kehitystehtävät pankkitoiminnan sisäisessä tarkastuksessa. Asiantuntija A:n päävastuualueena on rahanpesun estämiseen liittyvän sääntelyn seuranta sekä tarkastusten suunnittelu ja koordinointi. Koulutukseltaan hän on ekonomi.

5.2 Virtuaalivaluuttojen aiheuttaman rahanpesuriskin tunnistaminen

Haastatteluiden ensimmäisenä teemana oli virtuaalivaluuttojen aiheuttaman rahanpesuriskin tunnistaminen suomalaisella pankkisektorilla. Haastateltaville esitettiin tutkielman ensimmäisen empiriaosuuden päälöydökset, joita he saivat vapaasti kommentoida ja täydentää omilla ajatuksillaan. Haastatteluiden ensimmäisen teeman tarkoituksena oli näin ollen myös testata ensimmäisen empiriaosuuden tuloksia.

Kaikki haastateltavat olivat yksimielisiä siitä, että virtuaalivaluuttoihin liittyy kohonnut rahanpesun riski ja se on myös ainakin osittain tunnistettu pankkisektorilla. Asiantuntija A:n mukaan riskin tunnistaminen on pitkälti liitännäinen virtuaalivaluuttojen kasvaneeseen suosioon erityisesti yksityissijoittajien joukossa. Virtuaalivaluuttojen suosio ja käyttäjäkunta on kasvanut

viime vuosina paljon ja suurin osa transaktioista voidaankin yhdistää täysin lailliseen toimintaan. Asiantuntija A:n mukaan yhä useammalla on nykyään parempi kuva siitä, mitä virtuaalivaluutat ovat ja moni haluaa myös lähteä kokeilemaan niitä spekulatiivisen arvonnousun toivossa. Mitä enemmän virtuaalivaluuttojen käyttäjiä kuitenkin ilmaantuu, sitä vaikeampaa pankille on alkaa selvittämään varojen alkuperää. Pankit ovat joutuneet kohtaamaan täysin uudenlaisen tilanteen, jossa täytyy pohtia muun muassa sitä, mikä on riittävä selvitys virtuaalivaluuttavarojen alkuperästä. Asiantuntija A vahvistaa myös tutkielmassa aikaisemmin esiin tullutta näkökulmaa siitä, että virtuaalivaluuttaekosysteemi jatkaa jatkuvasti kasvuaan. Hänen mukaansa rahanpesuriski kasvaa, kun uusia suoria virtuaalivaluuttojen käyttökohteita ilmaantuu. Näistä hän mainitsee esimerkkinä sähköautovalmistaja Teslan ja nettikasinot. Vuonna 2021 Tesla hyväksyi hetkellisesti bitcoinin maksuvälineenä, mutta ympäristösyihin vedoten mahdollisuus poistettiin. Jotkin nettikasinot puolestaan hyväksyvät virtuaalivaluuttojen tallettamista pelitileille. Tämä on rahanpesun kannalta ongelmallista, sillä nettikasinoita ei välttämättä velvoita rahanpesusääntely samalla tavalla kuin esimerkiksi pankkeja. Yleisesti ottaen virtuaalivaluuttojen uudet käyttökohteet luovat lisää harmaita alueita likaisten varojen kuluttamiselle ja pesemiselle. Tutkielman ensimmäisessä empiriaosuudessa suorien käyttökohteiden vähyys nähtiin negatiivisena motivaatiotekijänä rahanpesulle, mutta käyttökohteiden lisääntyessä voidaan odottaa motivaatiotekijän kääntyvän positiiviseksi.

Kysyttäessä virtuaalivaluuttojen riskisyydestä verrattuna käteiseen rahanpesun näkökulmasta, oli näkemykset melko yksimielisiä. Asiantuntija A:n mukaan käteinen on edelleen rahanpesun kannalta ongelmallisempaa, sillä maailmanlaajuisesti käteinen on edelleen paljon suuremmassa roolissa kuin virtuaalivaluutat. Hän jättää kuitenkin mahdollisuuden sille, että tilanne saattaa tulevaisuudessa muuttua. Hän muistuttaa, että virtuaalivaluutat ovat vielä nuori ilmiö erityisesti käteiseen verrattuna. Toinen ja kolmas puolustuslinja korosti samaa asiaa sääntelyn ja toimintamallien näkökulmasta: asiantuntija C:n ja D:n mukaan finanssilaitokset ovat vuosien saatossa luoneet käteisen osalta rahanpesun estämiseen liittyvät tehokkaat toimintatavat, mutta virtuaalivaluuttojen osalta ne puuttuvat, mikä taas on suoraan yhteydessä puutteelliseen sääntelyyn ja aiheen tuoreuteen. Asiantuntija D pitikin virtuaalivaluuttoja käteistä merkittävämpänä riskinä siitä näkökulmasta, että virtuaalivaluutat ovat uusi ja nouseva riski, jolle ei ole vielä kehitetty tehokkaita hallintakeinoja. Hän nosti keskusteluun muun muassa Ukrainan sodan ja muuttuneen turvallisuustilanteen, joka saattaa aiheuttaa myös Suomessa sekä kasvanutta käteisen että virtuaalivaluuttojen käyttöä. Myös asiantuntija C nosti virtuaalivaluuttojen osalta yhdeksi

merkittäväksi riskiksi pakotteiden välttelyn näkökulman, joka taas saattaa lisätä niiden käyttöä myös rahanpesun välineenä.

Virtuaalivaluuttojen aiheuttaman rahanpesuriskin näkökulmasta asiantuntijat näkivät ongelmalliseksi myös tutkielmassa aiemmin käsitellyn virtuaalivaluuttojen pseudo-anonyymin luonteen. He tunnistavat siinä kuitenkin samat edut, jotka nousivat ensimmäisessä empiriaosuudessa esiin: siinä, missä virtuaalivaluuttatransaktiosta jää aina digitaalinen jälki, käteistapahtumasta ei välttämättä jää mitään. Asiantuntija C korosti myös virtuaalivaluuttojen kansainvälisten siirtojen ongelmallisuutta verrattuna käteiseen, sillä virtuaalivaluuttojen kohdalla ei edellytetä fyysistä varojen siirtelyä eri maiden välillä. Pankin kannalta nostettiin esiin myös se, että tosiasiallisia edunsaajia on vaikea tunnistaa heikon läpinäkyvyyden takia.

Asiantuntijat ottivat kantaa myös häivyttämisvaiheessa käytettäviin anonymisointipalveluihin. Häivytyspalveluiden teema oli vahvasti esillä myös ensimmäisen empiriaosuuden aineistossa ja sekä ensimmäisen että toisen puolustuslinjan asiantuntijat nostivat ne esiin ongelmakohtina. Asiantuntija C:n mukaan pseudo-anonyymiä luonnetta ei voida automaattisesti ajatella paljon parempana kuin käteisen tuomaa täyttä anonymiteettiä, sillä rikollinen voi hyödyntää virtuaalivaluuttojen alkuperän häivyttämisessä esimerkiksi mixereitä ja tumblereita. Kaikkien puolustuslinjojen edustajat muistuttivat, että rahanpesun estämisen osalta pankit tulevat aina eräällä tavalla yhden askeleen jäljessä rikollisia. Tähän asetelmaan pankkien tulisikin yrittää sopeutua paremmin kehittämällä omia toimintatapojaan.

Kun asiantuntijoilta kysyttiin, onko heidän näkemyksensä mukaan virtuaalivaluuttojen aiheuttama rahanpesuriski huomioitu riittävällä tavalla suomalaisella pankkisektorilla, oli yleinen mielipide, että riski kyllä tunnistetaan, mutta sitä ei hallita riittävästi. Asiantuntija A perustelee tätä muun muassa sillä, että kyseessä on tuore ilmiö. Yksikään suomalainen pankki ei tarjoa omaa virtuaalivaluuttatuotettaan, joten tietouden ja osaamisen lisääntyminen ilmiöön liittyen ei ole sisäsyntyistä. Tietouden lisääntymisen on laukaissut ulkoiset tekijät kuten sääntely ja erilaiset viranomaisraportit. Raporttien osalta haastateltavat nostivat esiin muun muassa FATF:in, Chainanalysisin ja Finanssivalvonnan julkaisuja, jotka ovat olleet myös tämän tutkielman lähdemateriaalia. Asiantuntija A:n mukaan erilaiset seminaarit ja koulutukset liittyen virtuaalivaluuttojen aiheuttamaan rahanpesuriskiin ovat alalla olleet erittäin suosittuja, ja niihin on osallistunut laajasti asiantuntijoita eri pankeista sekä viranomaistahoista.

”...tästä on tullut hyvin suosittu aihe ja tämä (osallistujien monipuolisuus) erityisesti minun mielestäni kertoo siitä, että halutaan lisätä ymmärrystä siitä ja pystyä myöskin ymmärtämään virtuaalivaluuttoja paremmin. Eikä pelkästään niiden luonteesta ja niiden hyödyistä ja haitoista vaan nimenomaan myöskin siitä riskipuolesta, millaisia riskejä niihin kohdistuu, jotta pystytään sitten hallitsemaan niitä myös pankkisektorilla.”

Asiantuntija D:n mukaan riskin tunnistaminen ei automaattisesti tarkoita, että samalla olisi myös täysi tietämys siitä, mitä kyseiselle riskille tulisi tehdä. Riskin tunnistamisen osalta hän korostaa erityisesti ensimmäisen puolustuslinjan roolia asiakasrajapinnassa. Tämä ajatus on linjassa myös ensimmäisessä empiriaosuudessa havaitun ajatuksen kanssa, ettei asiakasrajapinnassa työskentelevät henkilöt koe työssään kohtaavansa virtuaalivaluuttoihin liittyvää rahanpesua, sillä sitä ei osata tunnistaa oikein. Asiantuntija D muistuttaa, että riskin tunnistamista on tunnistaa myös tilanteet, joissa riskiä on vähemmän: pankin ei tulisi olettaa, että kaikkiin virtuaalivaluuttatapahtumiin liittyisi jotakin rikollista. Tämä sama tulee hänen mukaansa muistaa myös transaktiomonitoroinnin osalta. Asiantuntija B:n mukaan virtuaalivaluuttoihin liitettävistä rahanpesuindikaattoreista ollaan jo ainakin rahanpesun estämisen osalta tietoisia, mutta niiden lisäksi tarvitaan aidosti epäilyttävien tilanteiden tunnistamista ja tarvittavien toimenpiteiden arviointia.

Asiantuntija B nosti esiin myös riskin tunnistamisen siinä tapauksessa, mikäli pankilla on asiakkaanaan virtuaalivaluutan tarjoaja. Asiantuntija C:n mukaan henkilöasiakkaiden osalta riskiä voidaan hallita pitkälti asiakkaan tuntemisen keinoin, mutta yritysasiakkaan kohdalla se saattaa olla vaikeampaa erityisesti silloin, mikäli yrityksen toiminta liittyy virtuaalivaluuttoihin. Hän huomauttaa, että virtuaalivaluutan tarjoajat toimivat Suomessa luvanvaraisesti, joten pankit eivät voi alkaa kategorisesti sulkemaan tämänkaltaisia toimijoita asiakaskunnastaan. Asiantuntija B:n mukaan pankin tulee varmistua virtuaalivaluutan tarjoajan asiakkuutta pohtiessaan, onko potentiaalisen asiakkaan omat menettelytavat asianmukaisessa kunnossa. Myös asiantuntija C näkee kategorisen poissulkemisen huonona, mutta korostaa, että yksittäisten asiakkaiden kohdalla pankilla on enemmän harkintavaltaa.

Asiantuntija C muistuttaa, ettei virtuaalivaluuttoihin liittyvän rahanpesun tunnistaminen ja estäminen ole pelkästään pankkien vastuulla oleva asia. Suomessa virtuaalivaluutan tarjoajat ovat Finanssivalvonnan seurannan alaisia, ja samalla niitä velvoittaa nykyään myös rahanpesun

estämisen sääntely. Tämä osaltaan helpottaa myös pankkien roolia. Toisen puolustuslinjan edustajat toivat esiin myös jo aikaisemmin tässä tutkielmassa esitettyjä lukuja virtuaalivaluuttatoimijoiden tekemistä rahanpesuilmoituksista Keskusrikospoliisille. Asiantuntija C:n mukaan vaikuttaa siltä, ettei aidosti epäilyttäviä transaktioita osata havaita ja tästä syystä viranomaisille ilmoitetaan myös täysin turhia tapahtumia ikään kuin varmuuden vuoksi.

> *"...että se ei poliisin kannalta välttämättä ole kauhean niinku hyvä toimintatapa, koska sitten siellä tosiaan on samassa massassa sitten ne aidot keissit ja sitten ne varmuuden vuoksi raportoidut keissit. Varmaankin tarvittaisiin lisää ymmärrystä sitten juuri siitä, että miten tämä maailma toimii ja juuri ne varojen alkuperäselvitykset on kriittisiä ja siksi tullaankin juuri siihen, että millä me (pankki) voidaan tunnistaa se, että onko se ihan oikeasti vaan hyvin sijoitettua rahaa jonka arvo on muuttunut isoksi ja se kotiutetaan sieltä kryptolompakosta."*

Hänen mukaansa tulisikin olla sääntelyn osalta selvempää, millaisia tapahtumia kunkin ilmoittajatahon tulisi aidosti ilmoittaa viranomaisille ja kuinka tarkasti esimerkiksi asiakkaiden virtuaalivaluuttalompakoiden tapahtumia tulisi osata tarkastella. Toisen puolustuslinjan edustajat muistuttavat, etteivät pankin työntekijät ole poliiseja eikä tällöin myöskään tutkinnan ja käytettyjen resurssien tulisi olla täysin verrattavissa viranomaisten tekemään tutkintaan.

5.3 Virtuaalivaluuttojen aiheuttaman rahanpesuriskin hallitseminen

Toisena haastatteluteemana asiantuntijoilta kysyttiin ajatuksia virtuaalivaluuttojen aiheuttaman rahanpesuriskin hallintakeinoiksi. Haastateltaville oli etukäteen tarjottu tutkielman tulkintateoriana käytettävä Chapmanin rahanpesuriskin hallintaan luotu viitekehys, joka koostuu yhdeksästä eri osa-alueesta. Haastateltaville annettiin mahdollisuus hyödyntää kyseistä viitekehystä pohtiessaan pankkien eri keinoja huomioida tutkittava riski osana riskienhallintaansa. Jokaisen puolustuslinjan haastateltavia pyydettiin tämän jälkeen kuvailemaan oman puolustuslinjansa roolia kyseisten hallintakeinojen toimeenpanossa.

Asiantuntijoiden mukaan virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä tulisi ennen kaikkea ajatella jo olemassa olevana osana pankkien riskienhallintaa. Erityisen tärkeänä kaikki haastateltavat pitivät pankin omaa riskiarviota. Asiantuntija B:n mukaan on tärkeää tunnistaa ensin virtuaalivaluuttoihin liittyvät ominaisriskit ja jo olemassa olevat kontrollit. Tämän jälkeen voidaan muodostaa aihepiiriin liittyvä jäännösriski ja valita riskienhallintakeinot kyseisen jäännösriskin

perusteella. Hänen mukaansa on tärkeää sanoittaa pankin riskinottohalukkuus: millä edellytyksillä riski ja hyväksytään ja millä sitä hallitaan. Hän myös muistuttaa, että riskiarvio ei synny tyhjiössä, vaan sen laatimiseen on osallistettava koko organisaatiota. Asiantuntija A nosti myös esiin pankin omat rahanpesun estämiseen liittyvät politiikat, joista selviää kyseisen tahon suhtautuminen virtuaalivaluuttoihin yleisesti. Asiantuntija D:n mukaan virtuaalivaluuttoihin liittyvä riski tulisi yhdistää kokonaisvaltaisesti kaikkiin Chapmanin esittämiin riskienhallinnan osa-alueisiin eikä ajatella sitä irrallisena ja eräänlaisena päälle liimattavana ominaisuutena. Yhdeksi esimerkki osa-alueeksi hän nosti transaktiomonitoroinnin: mikäli virtuaalivaluuttoja ei ole huomioitu tällä osa-alueella lainkaan, on virtuaalivaluuttojen jälkikäteinen lisääminen haasteellista erityisesti nopealla aikataululla. Tästä syystä hän painottaa, että riski tulisi tunnistaa perustasolla eli pankin omassa riskiarviossa ja sen pohjalta lähteä implementoimaan virtuaalivaluuttojen näkökulmaa osaksi kaikkia rahanpesuriskin hallintaan liittyviä osa-alueita.

> *”... keskeisimmässä roolissa on kuitenkin ehkä edelleen se asiantuntijuus ja ymmärrys tämän asian ympärillä, mikä taas puolestaan tukee, että pystytään kouluttamaan henkilöitä ja sitten esimerkiksi rekrytoimaan sellaisia tahoja kenellä on tästä ymmärrystä. Mutta jos mietitään vaikka ihan viime vuosia, niin ainakaan itselleni ei ole tullut suoraan eteen tai olisin kuullut, että suomalaiseen pankkiin tai muuhun tunnetumpaan finanssilaitokseen haettaisiin suoraan jotain cryptoasiantuntijaa.”*

Yhtenä hallintakeinona Chapmanin viitekehyksen mukaisesti nousi esiin rekrytointi, koulutus ja osaaminen. Asiantuntija A kokee rahanpesun estämisen henkilöstön asiantuntijuuden virtuaalivaluuttoihin liittyen yhdeksi hallintakeinoksi itsessään. Asiantuntija A:n ja D:n mukaan pankilla tulisi olla tarjolla sisäistä koulutustarjontaa virtuaalivaluuttoihin liittyen, jotta voitaisiin varmistaa perusymmärrys aihepiiristä henkilöstön keskuudessa. Asiantuntija B muistutti, että esimerkiksi ohjeistukset yksinään eivät ole toimivia, sillä niihin tarvitsee liittää koulutuksia. Myös lisärekrytoinnit aihepiirin osaajista nähtiin yhtenä hallintakeinona. Vasta perusymmärryksen saavuttamisen jälkeen voidaan luoda laajempaa ymmärrystä virtuaalivaluuttoihin liittyvistä riskeistä sekä syväosaamista. Asiantuntija B:n mukaan kaikkien riskienhallinnan puolustuslinjojen tulisi huolehtia oman osaamisensa ylläpidosta aihepiiriin liittyen. Lisäksi hän korosti erityisesti ensimmäisessä puolustuslinjassa tehtävien rahanpesun estämiseen liittyvien tutkintaohjeiden merkitystä.

Syvällisemmän osaamisen kartuttamista riskienhallinnan näkökulmasta asiantuntija D peräänkuuluttaisi erityisesti ensimmäisen ja toisen puolustuslinjan osalta. Asiantuntija D:n mukaan sisäisiä tarkastuksia priorisoidaan riskiperusteisesti ja ihannetilanteessa tarkastuksen riskiarvion perusteella tarkastettavaan kohteeseen liittyvä jäännösriski on pieni. Kolmannen puolustuslinjan vastuulla tulisi olla rutiininomaiset ja riskiperusteiset tarkastukset, onko ensimmäisessä ja toisessa puolustuslinjassa toteutettu kontrollit ja hallittu kyseinen riski riittävällä tavalla. Ennaltaehkäisevä toiminta on aina parempi kuin se, että puutteita havaittaisiin vasta itse tarkastustilanteessa. Sama ajatus pätee myös ulkoiseen tarkastukseen, joka suomalaisten pankkien osalta tarkoittaa Finanssivalvontaa. Asiantuntija D kuitenkin painottaa, että kolmannen puolustuslinjan jokapäiväiseen työhön ja vastuisiin kuuluu ajankohtaisten ilmiöiden seuranta myös yksittäisten tarkastuksien ulkopuolella. Mikäli esimerkiksi jossain ulkoisessa raportissa nostettaisiin uudenlaisia näkökulmia virtuaalivaluuttaliitännäiseen rahanpesuriskiin, tulisi organisaatiossa keskustella asiasta ja punnita tarkastuskohteiden priorisointia. Hänen mukaansa tarvittaessa kohonneeseen riskiin voidaan reagoida nopeastikin. Asiantuntija D:n mukaan koulutuksen ja tietoisuuden lisäämistä ei tulisi toteuttaa pelkästään pankin sisällä, vaan hallintakeinona voidaan myös nähdä asiakkaiden tietoisuuden lisääminen virtuaalivaluuttoihin liittyvistä riskeistä.

Myös asiantuntija B:n mukaan yhtenä isona hallintakeinona ovat pankkien omat ohjeistukset ja niihin liittyvät toimenpiteet kuten koulutukset, mutta yksinään ne eivät riitä. Asiantuntija A:n mukaan ne toimivat hyvänä pohjana riskisten tilanteiden havaitsemiselle. Jatkossa tarvitaan erityisesti järjestelmätuettua transaktiomonitorointia poikkeavien virtuaalivaluuttatapahtumien havainnoimiseen. Pelkkä ohjeistus itsessään on riittämätön kontrollikeino, mikäli oikeasti epäilyttäviä tapahtumia ei kyetä tunnistamaan. Chapmanin viitekehyksen osa-alueista datan hyödyntäminen ja tiedolla johtaminen herätti myös keskustelua. Asiantuntija A:n mukaan toimivan transaktiomonitoroinnin yksi edellytys on se, että virtuaalivaluuttatransaktiot pystytään ylipäätään tunnistamaan transaktiodatasta. Myös asiantuntija C korosti, että käytettävän datan tulisi olla luotettavaa ja riittävää transaktiomonitoroinnin käyttötarkoituksia varten. Transaktiomonitoroinnin osalta asiantuntija D esitti ajatuksen, tulisiko tietyille hyvämaineisille virtuaalivaluuttatoimijoille tehtyjä maksuja monitoroida eri tavalla kuin riskisemmiksi todettujen toimijoiden kohdalla. Tämä sama ajatus on pitkälti linjassa ensimmäisessä empiriaosiossa esitellyn whitelistauksen ja blacklistauksen kanssa.

Perinteisistä rahanpesun estämisen keinoista tutkielmassa on tuotu esiin myös asiakkaan tunteminen, jonka merkitystä haastateltavat myös korostivat. Asiantuntija B nosti asiakkaan tuntemisen merkittävämmäksi hallintakeinoksi. Asiantuntija A:n mukaan asiakkaan tuntemisen toimintatavat tulisi huomioida erityisesti ensimmäisen puolustuslinjan toiminnoissa. Kun uutta asiakassuhdetta perustetaan, tulisi kartoittaa asiakkaan mahdolliset virtuaalivaluuttavarat ja profiloida asiakas niiden käyttäjänä. Asiantuntija A esittää, että tieto virtuaalivaluuttaomaisuudesta tulisi kirjata esimerkiksi rahoitustarvetta kartoittaessa ylös samaan tapaan kuin muutkin asiakkaan tulot ja menot. Myös asiantuntija D korostaa asiakkaan tuntemisen roolia: pankin tulisi varmistua siitä, että asiakkaasta on saatavilla ajantasaiset tiedot ja näin ollen voida tunnistaa, onko asiakkaan tekemät virtuaalivaluuttatransaktiot tälle tyypillisiä. Toiminnalle pitäisi löytyä aina jokin perustelu ja oikeutus. Pankin tulee myös tietää mitä tuotteita heidän asiakkaansa käyttää ja tuntea myös asiakkaan transaktiohistoria

Yhtenä hallintakeinona asiantuntija D näki myös ennaltaehkäisevän toimintatavan esimerkiksi väärinkäytösten hallinnan kautta. Mikäli esimerkiksi kryptovaluuttoihin liittyviä huijauksia saataisiin tehokkaasti estettyä, ei rikollisille päätyisi rikollisesti hankittuja varoja eikä näin ollen tapahtuisi myöskään näihin varoihin liittyvää rahanpesua. Virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä tulisi siis pyrkiä myös pienentämään mahdollisimman varhaisessa vaiheessa eikä pelkästään havaitsemaan jälkikäteen. Tämän mahdollistamiseksi hän myös korostaa yhteistyön merkitystä sekä pankin sisäisesti mutta myös muiden finanssilaitosten ja viranomaisten kanssa. Myös toisen puolustuslinjan asiantuntijat korostivat yhteistyön merkitystä yhtenä hallintakeinona. Heidän mukaansa yhteistyö Keskusrikospoliisin kanssa olisi tällä hetkellä todennäköisempää kuin pankkien keskinäinen yhteistyö johtuen kilpailulainsäädännöstä.

Tehokas ennaltaehkäisy vaatii myös aikaisemmin mainittua riskin kokonaisvaltaista tuntemista. Asiantuntija A esitti myös eräänlaisena ennaltaehkäisevänä riskienhallintakeinona tehokkaan markkinaseurannan erityisesti siitä näkökulmasta, että pankilla olisi tiedossa virtuaalivaluuttaekosysteemin uusimmat sovellukset, jotta ne osattaisiin ottaa riskiarviossa huomioon. Asiantuntija B nosti yhdeksi riskienhallintakeinoksi tehokkaan sääntelyseurannan, jotta pankki voisi mahdollisesti osallistua sääntelyn laatimiseen sekä olla varautunut sääntelyn tuomiin muutoksiin paremmin.

> *”…toisaalta tiedetään, minkä tyyppistä sääntelyä on suunnitteilla ja finanssilaitokset tekevät tietysti sitten myös tietynlaista edunvalvontaa sen suhteen suhteen, että ollaan*

myös aktiivisesti siinä mukana kertomassa näkemyksiä ja toisaalta sitten taas varautumassa tulevaisuuteen, että miten se sääntely sitten toisi uusia velvollisuuksia (pankille)…"

Ulkoisen sääntelyn seurannan lisäksi asiantuntija C nosti esiin pankin sisäisen sääntelyn roolin erityisesti virtuaalivaluuttoja koskevien linjauksien muodossa. Pankin tulisi varmistua siitä, että niillä on jo nyt olemassa riittävät linjaukset, joilla perustella eri toimintamallejaan virtuaalivaluuttoihin liittyen. Hän yhdisti toisiinsa sekä laadukkaan datan että johdon raportoinnin, jotta linjauksien ajantasaisuudesta ja laadusta voidaan varmistua.

Kaikki asiantuntijat uskovat virtuaalivaluuttaliitännäisen sääntelyn lisääntymiseen tulevina vuosina. Asiantuntija A uskoo tähän johtuvan erityisesti rahanpesuun liitettävästä riskistä. Asiantuntija D kuitenkin muistuttaa, että riski ja sääntely eivät välttämättä kulje käsi kädessä siinä mielessä, että riskin kasvaessa myös uutta sääntelyä ilmestyisi automaattisesti. Uuden sääntelyn toimeenpanoon menee aikaa, ja asiantuntijat esittivät huolen siitä, että voimaantullessaan sääntely saattaa olla jo vanhentunutta. Sääntelyn muuttumisen vaikean ennustettavuuden takia pankkien ei tulisi pohjata riskienhallintakeinojaan vain nykysääntelyn mukailevaksi. Asiantuntija D ei usko, että sääntely yksinään tulee poistamaan riskejä riittävästi. Sääntelyn tulisi ohjata riskienhallintakeinojen osalta minimitasoa, jonka päälle pankki luo omia toimintatapojansa riskiarvioon perustuen. Myös asiantuntija A:n mukaan pankkien tulee olla proaktiivisia omissa toimenpiteissään.

"…rahanpesuriskin integroimisen pitäis olla tämmöstä ihan jokaisen finanssilaitoksen omaa proaktiivista toimintaa, että niinku selvitetään asioita ja lähdetään sitä kautta sitten kehittämään omia ratkaisuja eikä jäädä periaatteessa siihen paikalleen odottelemaan, milloin mahdollisesti tapahtuisi jotain regulaation näkökulmasta."

Asiantuntija B toivoo kaikkien finanssialan toimijoiden osalta, että virtuaalivaluuttoja koskeva sääntely olisi yksiselitteistä: siitä tulisi ilmetä selkeästi, millaisia toimenpiteitä pankeilta odotetaan. Asiantuntija C toivoo, että tulevaisuuden sääntely painottuisi kuitenkin yhä enemmän virtuaalivaluutan tarjoajiin, sillä heille virtuaalivaluutat ovat ydinliiketoimintaa, kun taas pankille toistaiseksi pelkkä kulu rahanpesun estämisen näkökulmasta. Asiantuntija A toivoo sääntelyn kehittymistä myös siksi, että pankit saisivat uudenlaisia kontrollikeinoja käyttöönsä. Esimerkkinä

hän mainitsee keinot, joilla pankit ja viranomaiset pystyisivät tekemään asiakkaan virtuaalivaluuttatransaktioista läpinäkyvämpiä. Hän myös näkee tarpeelliseksi, että pankit harkitsisivat lohkoketjuanalytiikan käyttämistä osana transaktiomonitorointia. Toisen puolustuslinjan edustajat uskoivat, että pankeissa tullaan investoimaan virtuaalivaluuttaliitännäisen rahanpesun torjuntaan tulevaisuudessa yhä enemmän.

6 YHTEENVETO JA JOHTOPÄÄTÖKSET

6.1 Tutkimuskysymyksiin vastaaminen ja johtopäätökset

Tutkielman tavoitteena oli vastata kolmeen tutkimuskysymykseen, joiden muodostama yhtenäinen kokonaisuus käsittelee virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä sekä yleisenä ilmiönä että pankin näkökulmasta. Tutkielman tavoitteiden kannalta oli luontevaa tutkia ensin riskin luonnetta tarkemmin ja vasta tämän jälkeen keskittyä pankin näkökulmaan kyseisen riskin tunnistamisen ja hallinnan osalta. Tutkielman ensimmäinen tutkimuskysymys oli asetettu muotoon ”Millaisen rahanpesuriskin virtuaalivaluuttojen käyttäminen rahanpesun välineenä luo?”. Ensimmäisessä empiriaosuudessa keskityttiin tutkimaan virtuaalivaluuttojen käyttämistä rahanpesun välineenä. Tutkielman lopputulemana voidaan todeta, että virtuaalivaluutat sopivat rahanpesuun erittäin hyvin ja viimeisten vuosien aikana virtuaalivaluuttaliitännäisten rahanpesutapausten määrä on kasvanut voimakkaasti. Tarkkaa arviota ilmiön yleisyydestä on mahdotonta muodostaa rahanpesun luonteen takia, mutta ongelma on tunnistettu niin kansainvälisesti kuin kansallisestikin.

Virtuaalivaluutat ovat lohkoketjuteknologiaan perustuva digitaalinen arvon esiintymismuoto, ja niitä voidaan käyttää vaihdannan välineenä. Kun peilataan ensimmäisen empiriaosuuden löydöksiä virtuaalivaluuttojen rahanpesuliitännäisistä ominaisuuksista tutkielman taustateoriaan, käy ilmi, että suurimpaan osaan virtuaalivaluuttojen luontaisista ominaisuuksista voidaan liittää positiivinen motivaatiovaikutus rahanpesuun. Ominaisuudet pystyttiin luokittelemaan yleisiin, transaktioliitännäisiin sekä kontrolleihin liitettäviin. Yleisten ominaisuuksien osalta merkittävimmiksi nähtiin virtuaalivaluuttojen pseudo-anonyymi luonne ja keskitetyn hallintatahon puuttuminen. Transaktioiden osalta merkittävimpiä ominaisuuksia olivat nopeus, kansainvälisyys sekä helppo hajautettavuus. Kontrollikeinojen osalta esiin nousi ensisijaisesti niiden puuttuminen: virtuaalivaluuttoja koskeva yhtenäinen kansainvälinen sääntely on puutteellista eikä ole olemassa yhtä keskitettyä virtuaalivaluuttoja valvovaa viranomaistahoa. Kontrolleihin liitettävänä ominaisuutena voidaan myös nähdä se, ettei viranomaisilla ja finanssilaitoksilla ole tällä hetkellä tarvittavia kyvykkyyksiä jäljittää virtuaalivaluuttatransaktioita. Kaikki edellä mainitut ominaisuudet saivat vahvistusta myös tutkielman toisessa empiriaosuudessa toteutetuissa asiantuntijahaastatteluissa. Haastatteluissa korostettiin erityisesti osittaisen anonymiteetin sekä tehokkaiden monitorointikeinojen puuttumisen ongelmallisuutta. Myös puutteellinen sääntely nostettiin toisen ja kolmannen puolustuslinjan osalta esiin.

Kuten tutkielman taustateoriassa sekä ensimmäisessä empiriaosuudessa tuotiin esiin, virtuaalivaluuttoja ei luotu alun perin rikollisiin käyttötarkoituksiin. Niiden avulla haluttiin kehittää maksujärjestelmiä tehokkaimmiksi ja pankeista riippumattomiksi, mutta nopeasti myös rikolliset löysivät niiden edut likaisen rahan liikuttamiseen ja peittämiseen. Virtuaalivaluuttojen aiheuttama rahanpesuriski on yksi rahanpesuun liitettävien riskien muodoista, joka syntyy, kun joko suoraan tai välillisesti virtuaalivaluuttoina hankittujen rikollisten varojen alkuperää häivytetään. Alaluvussa 4.6 käytiin läpi virtuaalivaluuttaliitännäisiä rahanpesutypologioita, jotka eivät kuitenkaan lähtökohtaisesti vaatineet pankkia osalliseksi. Tyypillisiksi typologioiksi tunnistettiin muun muassa erilaiset anonymisointipalvelut, virtuaalivaluutta-automaatit sekä reguloimattomien vaihdantapalveluiden käyttäminen. Perinteinen maksujärjestelmäyhteiskunta on kuitenkin rakennettu pankkien ympärille, jolloin rikollisen tulee jossain kohtaa rahanpesuprosessia kierrättää varat pankin kautta, mikäli varoja haluaa hyödyntää perinteisessä fiat-muodossa. Tämä ilmiö yhdistettynä siihen, että virtuaalivaluutat ovat erittäin tehokas rahanpesun keino, luovat yhdessä pankkeihin kohdistuvan virtuaalivaluuttaliitännäisen rahanpesuriskin.

Tutkielman toisen tutkimuskysymyksen avulla pohdittiin, kuinka merkittävä tämä virtuaalivaluuttojen aiheuttama rahanpesuriski pankille on. Vastaus tähän muodostui sekä teoria- että empiriaosuuden löydöksien pohjalta. Tämän tutkielman tulkintateoriana käytettiin riskin nelikenttää, jonka avulla organisaation riskit voidaan jakaa tunnettuihin ja tuntemattomiin riskeihin. Taustateorian mukaan sääntelyn noudattamisessa epäonnistuminen on pankille ei-taloudellisen riskikategorian riski, jossa voidaan nähdä sekä operatiivisen riskin että liiketoimintariskin piirteitä. Pankin motiivit organisoida laadukasta rahanpesun estämistä voitiin jakaa sekä moraalisiin että sääntelyyn perustuviin. Yhdistämällä nämä kaksi havaintoa voidaan todeta, että myös pankin rahanpesuriski voidaan rinnastaa edellä mainittuun sääntelyn noudattamisessa epäonnistumisen riskiin. Toisessa teorialuvussa havaittiin myös, että pankin kohtaamaa rahanpesuriskiä voidaan pitää vähemmän tunnettuna riskinä kuin esimerkiksi perinteisiä markkinariskejä. Rahanpesuriskiin liittyvän tietouden tason voidaan nähdä vähenevän entisestään, kun rajataan tarkastelu koskemaan nimenomaan virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä. Virtuaalivaluuttaekosysteemi kasvaa jatkuvasti, minkä takia myös siihen liittyvät termistöt ja sääntely vanhenevat nopeammin kuin siihen liittyviä uusia sovelluksia ilmaantuu. Virtuaalivaluuttojen kaltaisille ilmiöille onkin tyypillistä, ettei organisaatioissa ymmärretä niitä kokonaisvaltaisesti, jolloin myöskään niihin liittyvien riskien realisoitumisen vaikutusta ei täysin tunneta. Tätä ajatusta vahvistaa toisen empiriaosuuden löydös, jonka mukaan esimerkiksi pankkien puutteellinen tietouden taso virtuaalivaluutoista voidaan yhdistää

liiketoimintanäkökulman puuttumiseen: yksikään suomalainen pankki ei tällä hetkellä tarjoa omaa virtuaalivaluuttatuotettaan, jolloin tietouden lisääntyminen aiheeseen liittyen ei ole organisaatiossa sisäsyntyistä. Puutteellinen tietous aihepiiristä voidaan nähdä tekijänä, joka myös lisää riskin merkittävyyttä pankille.

Toisessa teorialuvussa rahanpesuriskit jaoteltiin joko unknown unknowns -tyyppisiin riskeihin, joista ei ole olemassa dataa eikä pankki ole niiden olemassaolosta edes tietoinen sekä known unknows -tyyppisiin riskeihin, joiden olemassaolo on tunnistettu, mutta niiden merkittävyydestä pankille ei ole tietoutta. Sekä ensimmäisen että toisen empiriaosuuden havainnot tukevat, että virtuaalivaluuttojen aiheuttama rahanpesuriski pankille on known unkown -tyyppinen riski: riski on tunnistettu, mutta sen merkityksestä organisaatiolle ei ole täyttä tietoutta. Erityisesti pankkien kolmen eri puolustuslinjan asiantuntijoiden kanssa tehdyt haastattelut tukivat tätä ajatusta. Asiantuntijat kokivat, että virtuaalivaluuttojen aiheuttamasta rahanpesuriskistä ollaan suomalaisella pankkisektorilla yhä tietoisempia, mutta pankkien omat riskienhallintakyvykkyydet aiheeseen liittyen ovat toistaiseksi riittämättömiä. Virtuaalivaluuttojen aiheuttaman rahanpesuriskin voidaan nähdä olevan pankin näkökulmasta merkittävä sekä riittävän tietouden tason että hallintakeinojen puuttumisen takia. Virtuaalivaluutat eivät volyymiltaan ole yhtä suuri rahanpesuriski pankille kuin esimerkiksi käteinen raha, mutta tietouden puute teki virtuaalivaluutoista asiantuntijoiden mielestä jopa merkittävämmän riskin kuin käteinen. Molempien empiriaosuuksien perusteella pankeissa tunnistetaan rahanpesun kontekstissa virtuaalivaluuttoihin liittyvä ominaisriski muun muassa ulkoisen sääntelyn ja yleisen markkinailmapiirin ohjaamina, mutta jäännösriskitaso on korkea puutteellisten hallintakeinojen takia. Hallintakeinojen puutteellisuuteen puolestaan vaikuttavat pitkälti virtuaalivaluuttojen eri ominaisuudet, joiden motivaatiotekijä nähdään rahanpesun kannalta positiiviseksi.

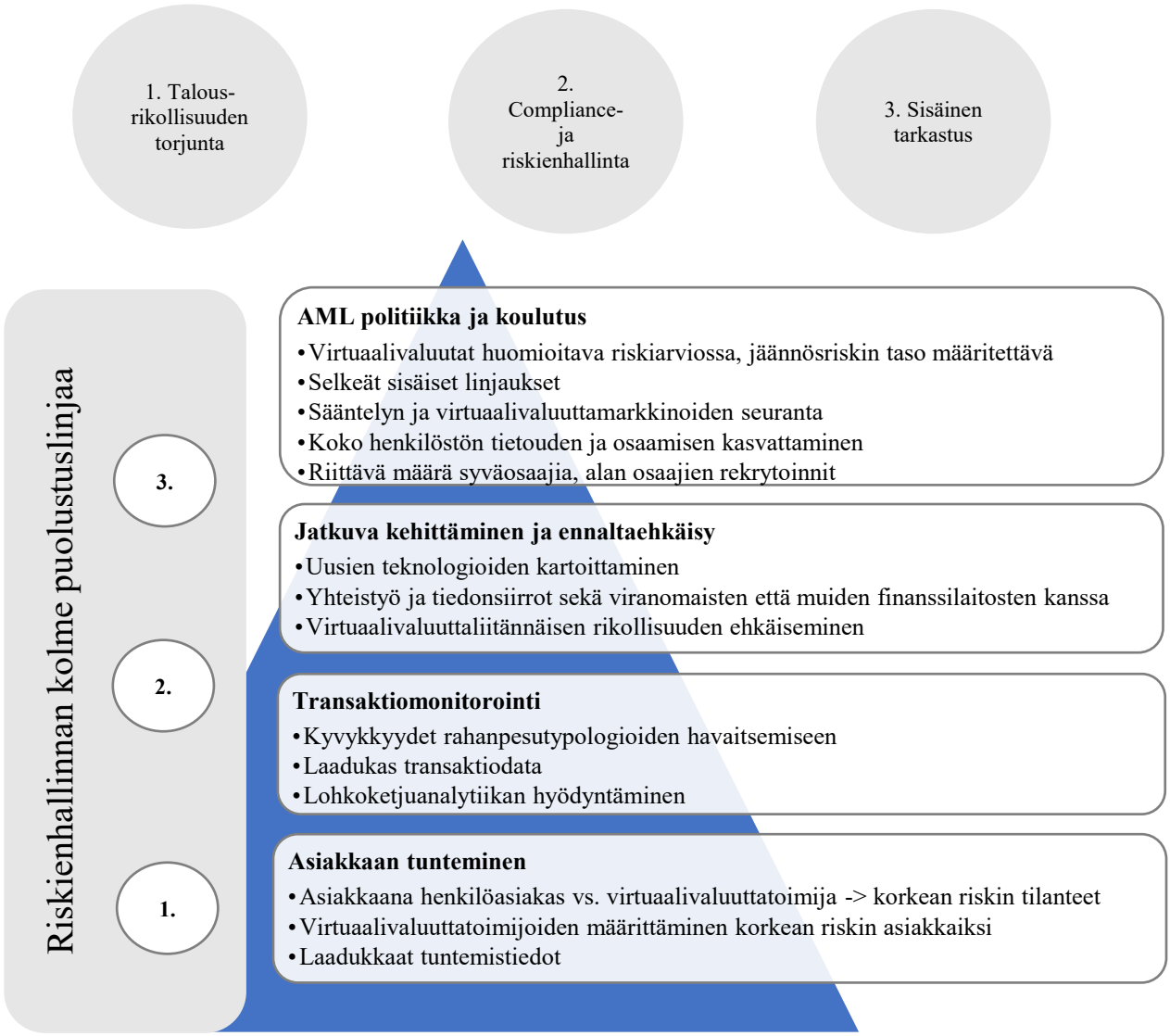
Yhdistämällä pankin rahanpesuriskin realisoitumista käsittelevä taustateoria virtuaalivaluuttojen kontekstiin voidaan ymmärtää, että pankin riskienhallintatoimintojen näkökulmasta virtuaalivaluuttojen aiheuttama rahanpesuriski voi toteutua sääntelyn määräämän ilmoitusvelvollisuuden laiminlyöntinä, suurina valvojan määrääminä sakkorangaistuksina sekä vakavana mainehaittana. Virtuaalivaluuttojen aiheuttaman rahanpesuriskin merkittävyyttä pankille lisää siis osaltaan myös sääntely. Suomessa kansallisen rahanpesun estämisen riskiarvion mukaan virtuaalivaluuttasektoriin kohdistuva kokonaisriskitaso on merkittävä, mikä pankin tulee huomioida myös omissa rahanpesun estämisen riskiarvioissaan. Riskin merkittävyyttä pankeille voidaan lähestyä myös riskin tuoreuden näkökulmasta: koska virtuaalivaluuttoihin liittyvä ilmiö

on vielä nuori esimerkiksi perinteisempään rahanpesun instrumenttiin käteiseen verrattuna, eivät jo olemassa olevat rahanpesun estämisen toimintatavat toimi virtuaalivaluuttojen kontekstissa. Virtuaalivaluutat ovat täysin uudenlainen uhka perinteisille rahanpesun estämisen toimintatavoille. Perinteisesti pankkien rooli on ollut sääntelyn velvoittamana monitoroida asiakkaiden maksuliikennettä ja hankkia epäilyttävistä transaktioista tarvittavat lisäselvitykset. Virtuaalivaluuttojen osalta pankki ei kuitenkaan kykene monitoroimaan ja jäljittämään varojen alkuperää johtuen aikaisemmin mainituista pseudo-anonymiteetistä ja monitorointikyvykkyyksien puutteesta. Myöskään nykysääntely ei tällä hetkellä anna pankeille esimerkiksi näkyvyyttä asiakkaan virtuaalivaluuttalompakkoon, vaan pankki on täysin niiden tietojen varassa, mitä asiakas haluaa pankille kertoa. Sääntely voidaan monessakin mielessä nähdä pankin kannalta sekä virtuaalivaluuttaliitännäisen rahanpesuriskin hallintaa ohjaavaksi että rajoittavaksi tekijäksi.

Kolmas tutkimuskysymys käsitteli riskin hallintakeinojen ja pankin toimintatapojen näkökulmaa. Kysymys oli asetettu muotoon ”Millä eri keinoin pankkien tulisi huomioida virtuaalivaluuttojen aiheuttama rahanpesuriski osana riskienhallintaa?”. Toisen empiriaosuuden perusteella kolmen puolustuslinjan riskienhallintamallia noudattamalla riski on hallittavissa, mutta ei kokonaan poistettavissa. Rahanpesuriskiä ei voida myöskään esimerkiksi siirtää vakuuttamalla. Molemmat empiriaosuudet tukivat ajatusta, jonka mukaan riski on hallittavissa perinteisillä rahanpesun estämisen keinoilla kuten transaktiomonitoroinnilla ja asiakkaan tuntemisella, mutta myös uudenlaiset teknologiat, tiedonsiirrot sekä tietouden lisääminen nousivat esiin.

Kuvioon kahdeksan on tiivistetty tutkielman tärkeimmät löydökset kolmanteen tutkimuskysymykseen liittyen. Kun peilataan ensimmäisen ja toisen empiriaosuuden löydöksiä Chapmanin rahanpesun estämisen viitekehykseen, virtuaalivaluuttojen osalta esiin nousi neljä tärkeintä teemaa: rahanpesun estämisen politiikka ja koulutus, jatkuva kehittäminen ja ennaltaehkäisy, transaktiomonitorointi sekä asiakkaan tunteminen. Virtuaalivaluuttojen aiheuttama rahanpesuriski tulee ensin huomioida pankin omassa riskiarviossa, josta se voidaan implementoida osaksi rahanpesun estämisen osa-alueita kaikkien kolmen puolustuslinjan tasolla. Virtuaalivaluuttoja ei voida nähdä muista toiminnoista irrallisena ja eräänlaisena päälle liimattavana ilmiönä. Transaktiomonitoroinnin osalta pankkien tulee kehittää valmiudet, joilla voidaan reagoida virtuaalivaluuttojen kaltaisten uusien teknologioiden ja sovellusten mukanaan tuomiin rahanpesuriskeihin nopeallakin aikataululla. Teorialuvussa 3.8 käsiteltiin pankkien skenaariopohjaista transaktiomonitorointia ja toisessa empiriaosuudessa korostui datan laadun tärkeys. Pankin tulee kyetä tunnistamaan transaktiodatastaan virtuaalivaluuttatransaktiot, jotta

kyseisiin transaktioihin perustuvia skenaarioita voitaisiin luoda transaktiomonitoroinnin tueksi. Transaktiomonitoroinnin osalta nähtiin myös tärkeäksi, että pankit hyödyntäisivät rahanpesun estämisessä lohkoketjuanalytiikkaa, jonka avulla pankki pystyy sekä tunnistamaan virtuaalivaluuttatransaktioita että jäljittämään varojen alkuperää aikaisempaa laadukkaammin.



Kuvio 8. Virtuaalivaluuttojen aiheuttaman rahanpesuriskin hallinta

Löydöksien perusteella pankin henkilöstön sekä asiakkaiden tietoisuuden lisääminen on myös avainasemassa: jotta virtuaalivaluuttojen aiheuttamaa rahanpesua pystyttäisiin estämään, niihin liittyvät korkean riskin tilanteet tulee pystyä tunnistamaan sekä asiakasrajapinnassa että asiantuntijatasolla. Myös syväosaamisen kehittäminen ja rekrytoinnit aihepiirin liittyen nähtiin yhdeksi keinoksi. Asiakkaan tuntemisen osalta virtuaalivaluuttojen aiheuttama rahanpesuriski on kaksijakoinen: pankilla voi olla asiakkaanaan sekä virtuaalivaluuttatransaktioita toteuttavia henkilöasiakkaita että virtuaalivaluuttatoimijoita, jotka ovat tyypillisesti Suomessa

virtuaalivaluutan vaihdantapalveluita. Molempien osalta on tärkeää tuntea, millainen maksuliikenne asiakkaalle on tavanomaista. Se, kuinka pitkälle pankin tulee tuntea sen asiakkaidensa asiakkaat, jää harmaaksi alueeksi ja sääntelyn päätettäväksi tulevaisuudessa. Tutkielman löydösten perusteella virtuaalivaluuttatoimijoita tulisi käsitellä korkean riskin asiakkuuksina. Henkilöasiakkaiden osalta tulee ylläpitää ajantasaisia tuntemistietoja, joihin sisältyy myös asiakkaan mahdollinen virtuaalivaluuttaomaisuus.

Virtuaalivaluuttaekosysteemi tulee kasvamaan entisestään tulevina vuosina, eikä siihen liittyvä sääntely pysy välttämättä kasvuvauhdin perässä. Sääntelyn tulisi ohjata pankin riskienhallintakeinojen minimitasoa, jonka päälle pankin tulee luoda omaan riskiarvioonsa pohjautuvia toimintatapoja. Tästä syystä tutkielman tuloksissa korostuu myös jatkuvan kehittämisen näkökulma. Tämä tarkoittaa muun muassa uusien teknologioiden aktiivista kartoittamista rahanpesun estämisen käyttöön. Lohkoketjujen onnistuneesta hyödyntämisestä rahanpesun estämisessä on jo olemassa esimerkkejä esimerkiksi tuntemistietojen tallentamisen osalta. Mitä enemmän pankilla on ymmärrystä virtuaalivaluuttojen ja lohkoketjuteknologian mahdollisuuksista, sitä todennäköisemmin riski hallitaan. Asiantuntijahaastatteluissa nousi esiin näkökulma, jonka mukaan virtuaalivaluuttojen liiallinen ”demonisointi” tai virtuaalivaluuttatoimijoiden kategorinen poissulkeminen asiakkuuksista olisi haitallista tulevaisuuden kannalta. Tilastojen valossa virtuaalivaluuttojen käyttö ei ole vähenemässä ja pankin tulee varautua siihen, että niiden volyymit voivat vielä jonain päivänä ylittää nykyisten fiat-valuuttojen käytön.

Kuvio kahdeksan kuvastaa myös sitä, miten kaikki tässä tutkielmassa tunnistetut virtuaalivaluuttaliitännäisen rahanpesuriskin hallintaan liittyvät teemat yhdistyvät kaikkiin kolmeen riskienhallinnan puolustuslinjaan. Riskiarvion luominen ja riskin tunnistaminen tulee tapahtua koko organisaation tasolla, jotta riskiä voitaisiin hallita kokonaisvaltaisesti. Ensimmäisen linjan osalta korostuu taustateorian mukaisesti kuitenkin esimerkiksi transaktiomonitoroinnin, asiakkaan tuntemisen ja syväosaamisen tärkeys, kun taas toisen linjan osalta sääntelyn ja virtuaalivaluuttaekosysteemin kehittymisen seuranta on merkittävässä roolissa. Mikäli kolmas ja viimeinen puolustuslinja tunnistaa virtuaalivaluuttojen aiheuttamaan rahanpesuriskiin liittyvän jäännösriskin pieneksi, on riski hallittu riittävällä tasolla ensimmäisessä ja toisessa linjassa. Kolmannen puolustuslinjan rooli onkin toimia riippumattomana arvioijatahoja, kuinka hyvin virtuaalivaluuttojen aiheuttama rahanpesuriski on pankissa hallittu.

6.2 Tutkielman laadun arviointi

Tutkielman luotettavuutta ja johdonmukaisuutta tulisi ensisijaisesti arvioida tutkimuskohteen ja -tarkoituksen perusteella (Tuomi & Sarajärvi, 2018, luku 6). Tämän tutkielman kohteen merkityksellisyyttä käsiteltiin ensimmäisessä luvussa, jota täydennettiin sekä teorian että empirian keinoin muun muassa tuomalla esiin ajankohtaisuuteen, sääntelyyn ja ilmiön laajuuteen liittyviä näkökulmia. Virheiden välttämiseksi yksittäisessä tutkielmassa tulee arvioida myös tehdyn tutkimuksen luotettavuutta, jota voidaan pohtia monista erilaisista näkökulmista. Tämän tutkielman osalta sen laatua ja luotettavuutta arvioidaan uskottavuuden, vastaavuuden, siirrettävyyden ja tutkimustilanteen arvioinnin kautta. (Tuomi & Sarajärvi, 2018, luku 6.)

Tutkielman ensimmäinen empiriaosio toteutettiin integroivana kirjallisuuskatsauksena. Laadukkaaseen kirjallisuuskatsaukseen liittyy selkeä ja strukturoitu kuvaus siitä, miten käytetty aineisto on kerätty. Integroivan kirjallisuuskatsauksen valinta vähän tutkitun aihealueen tutkimusmenetelmäksi ohjaa osaltaan myös aihepiiriin liittyviä tulevia tutkimuksia. Laadukas tutkimus mahdollistaa uusien ajatusten ja näkökulmien syntymisen aihepiiristä. Myös tulokset tulee esittää lukijan kannalta loogisessa ja strukturoidussa muodossa. (Torraco, 2005, 363–364.) Näiden osa-alueiden osalta tätä tutkielmaa voidaan pitää laadukkaana. Hakuprosessi on tarkasti dokumentoitu sekä aineisto teemoiteltu tiiviiseen, mutta informatiiviseen muotoon. Tutkielmassa tehty integroiva kirjallisuuskatsaus on toistettavissa. Käytetyn aineiston kriittinen arviointi on myös merkittävä tekijä tutkielman laadun arvioinnissa (Saunders ym., 2019, 104–105). Aineistoa arvioitiin kriittisesti sekä aineiston rajausvaiheessa, että itse analyysivaiheessa. Erityisesti vanhentuneiden käsitteiden määritelmien ja sääntelyn rinnalle tuotiin tuoreempia näkökulmia ajankohtaisuuden ja luotettavuuden lisäämiseksi. Integroivan kirjallisuuskatsauksen aineistoa on arvioitu jo aiemmin alaluvussa 4.3.

Tutkielman toisessa empiriaosuudessa aineistoa kerättiin haastattelemalla neljää asiantuntijaa. Tutkielman uskottavuuden kannalta oli tärkeää, että kaikki kolme puolustuslinjaa olivat edustettuina. Tällä tavoin saatiin tutkielman tarkoituksen mukaisesti riskistä kattava läpileikkaus suomalaisen pankin riskienhallintatoimintojen näkökulmasta. Haastatteluilla saatiin myös lisättyä tutkielman vastaavuutta, sillä asiantuntijat vahvistivat ensimmäisen empiriaosuuden löydöksiä. Toisen empiriaosuuden luotettavuuden näkökulmasta tulee kuitenkin huomioida, että haastateltavat edustivat samaa suomalaista pankkia, jolloin yhden yrityksen asiantuntijoiden näkemys ei edusta koko suomalaisen pankkisektorin näkemystä rahanpesun estämisestä. Tästä syystä haastattelujen painoarvoa ei haluttu korostaa liikaa tässä tutkielmassa, vaan niillä pyrittiin

rikastamaan ensimmäisen empiriaosuuden löydöksiä sekä lisäämään erityisesti suomalaisen pankin näkökulmaa. Haastattelujen laatua olisi voitu lisätä haastattelemalla riskienhallinnan asiantuntijoita kaikista suomalaisista merkittävistä pankeista.

Luotettavuutta nostaa kuitenkin se, että haastateltavat edustivat merkittävää suomalaista pankkitoimijaa ja kaikilla oli relevanttia kokemusta joko suoraan virtuaalivaluuttoihin tai edustamansa puolustuslinjan vastuualueisiin liittyen. Kaikissa haastatteluissa käytettiin samaa kysymyspohjaa, mutta haastatteluiden painopisteet erosivat hieman riippuen haastateltavan edustamasta puolustuslinjasta. Asiantuntija A:n kanssa käyty keskustelu painottui erityisesti virtuaalivaluuttojen rahanpesuliitännäisiin ominaisuuksiin sekä transaktiomonitorointiin, kun taas toisen ja kolmannen puolustuslinjan osalta keskustelu painottui sääntelyn näkökulmaan. Huomio ei ole yllättävä ja on myös linjassa tutkielman teorialuvussa 3.5 esiteltyjen eri puolustuslinjojen perinteisien vastuualueiden kanssa, mikä itsessään lisää tutkielman luotettavuutta vastaavuuden näkökulmasta. Haastateltavat saivat myös lukea tutkielman tulokset ennen niiden julkaisua, jotta voitiin varmistua tutkimustulosten ja päätelmien luotettavuudesta mahdollisimman hyvin. Suurempien tulkintaerojen välttämiseksi haastattelut litteroitiin heti samana päivänä. Haastattelujen aihepiirin osalta tulee kuitenkin tiedostaa se, että rahanpesun estäminen on aiheena itsessään pitkälti julkisuudelta suojattu eivätkä viranomaiset tai pankit paljasta julkisesti toimintatapojaan tai tiettyihin toimintatapoihin liittyviä puutteita. Haastateltavat eivät ottaneet kantaa aihepiiriin edustamansa pankin näkökulmasta vaan laajemmin edustamansa riskienhallinnan puolustuslinjan edustajana.

Tutkielman luotettavuuden arviointi siirrettävyyden näkökulmasta tarkoittaa Tuomen ja Sarajärven (2018, luku 6.2) mukaan sitä, voidaanko tulokset siirtää tutkimuskontekstin ulkopuoliseen vastaavaan kontekstiin. Tämä tutkielma olisi siirrettävissä monipuolisesti myös muiden kuin virtuaalivaluuttaliitännäisten rahanpesuriskien kontekstiin. Tutkielma toteutettiin kokonaisuudessaan kahdeksan kuukauden aikana, joka sisälsi tutkimusaiheen valinnan, rajauksen, aineiston hankinnan sekä itse tutkimuksen toteuttamisen. Tämä nähtiin sopivana ajanjaksona kattavan pro gradu -tutkielman toteuttamiseen. Tutkielman etenemistä ja aihevalintaa ohjasivat erityisesti tutkijan oma ammatillinen kiinnostus aihepiiriin sekä tarkoitus saada tuotettua eräälle suomalaiselle finanssilaitokselle tutkielman pohjalta erillinen raportti, jossa kuvataan yrityksen nykytila virtuaalivaluuttoihin liittyvän rahanpesuriskin hallinnassa. Lisäksi tarkoituksena oli löytää uudenlaisia riskiin liittyviä hallintakeinoja yrityksen käyttöön. Aihepiiri ei ollut tutkijalle entuudestaan tuttu, jolloin tutkijan omat oletukset eivät ohjanneet tutkielman lopputulosta.

Edellä esiteltyjen seikkojen pohjalta tutkielman aihe voidaan nähdä perusteltuna ja relevanttina valintana sekä itse tutkielman toteutus luotettavana ja johdonmukaisena. Tutkielma yhdistää virtuaalivaluutat ajankohtaisena ja monimutkaisena kokonaisuutena perinteisen rahoituslaitoksen riskienhallintaan.

6.3 Lopuksi

Tässä tutkielmassa on rakennettu viitekehys, jonka avulla pankki voi ymmärtää paremmin virtuaalivaluuttojen aiheuttamaa rahanpesuriskiä sekä miten sitä voidaan hallita. Tutkielmassa käsiteltiin riskin syntyminen, sen eri ilmenemismuodot, merkitys pankille ja yhteiskunnalle laajemmin sekä ilmiöön liittyvät tulevaisuudennäkymät. Virtuaalivaluuttojen käyttäminen rahanpesun välineenä tulee kasvamaan tulevina vuosina laillisen käytön myötä, jolloin myös pankkien tulee reagoida tähän. Tutkielman tuloksina esiteltiin hallintakeinoja jaoteltuna neljälle eri rahanpesun estämisen osa-alueelle. Virtuaalivaluuttaekosysteemin kasvaessa myös riskin merkittävyys kasvaa, jolloin uusia hallintakeinoja tulee löytää sääntelyn edistymisestä riippumatta. Yhtenä tulevaisuuden uhkakuvana virtuaalivaluuttojen rahanpesuriskin osalta nähdään esimerkiksi niiden suorien käyttökohteiden lisääntyminen hyödykkeiden ja palveluiden hankkimisessa. Virtuaalivaluuttoihin liittyvää yleistä tietoutta tulisi kasvattaa Suomessa koko finanssialan laajuudella.

Tulevaisuuden osalta tutkitun riskin hallitsemiseen liittyy vahvasti eri teknologioiden hyödyntämisen mahdollisuus. Pankkien näkökulmasta tarvitaan myös uudenlaista yhteistyötä ja tiedonsiirtoa sekä toisten pankkien että viranomaisten kanssa. Virtuaalivaluuttojen pseudo-anonyymin luonteen aiheuttamien esteiden purkamiseen pankki tarvitsee nykyisten toimintatapojensa tueksi muun muassa uudenlaista virtuaalivaluuttoihin ja tietoturvaan liittyvää lainsäädäntöä. Tutkielman viimeistelyvaiheessa Euroopan parlamentti ilmoitti yllättäen uudesta EU:ssa suunnitteilla olevasta rahanpesun estämiseen ja virtuaalivaluuttoihin liittyvästä lainsäädännöstä. Uuden sääntelyn päätarkoituksena on, että virtuaalivaluuttoja kyettäisiin jäljittämään fiat-valuuttojen tapaan. Valvojalle rekisteröityjen virtuaalivaluuttatoimijoiden tulisi jatkossa varmistaa, että niiden kautta kulkevat transaktiot sisältävät tietoja varojen alkuperästä sekä todellisesta edunsaajasta. Kyseisiä tietoja voisivat hyödyntää tietyt viranomaistahot. Lisäksi uudessa lainsäädännössä ehdotetaan perustettavan julkinen rekisteri korkean riskin virtuaalivaluuttatoimijoista. Uudesta sääntelystä on määrä äänestää huhtikuun aikana, mutta tämän tutkielman valmistumishetkellä tarkempia tietoja lainsäädännön edistymisestä ei ollut saatavilla.

(Euroopan parlamentti, 2022.) Ehdotuksessa ei erikseen erotella pankkien roolia uudessa mahdollisessa lainsäädännössä. Tieto on kuitenkin tutkielman kannalta merkittävä: tutkielman tulosten perusteella kyseinen lainsäädäntö edistäisi myös pankeissa tapahtuvaa rahanpesun estämistä, mikäli virtuaalivaluuttatoimijoiden kautta pankin tileille virtaaviin varoihin liittyisi aiempaa matalampi rahanpesun riski. Rahanpesun estämisen tehostumisen sekä virtuaalivaluuttojen roolin vakiinnuttamisen kannalta lisäsääntely on tervetullutta, kuten useissa tutkielman sääntelyä koskevissa kohdissa on todettu. Virtuaalivaluutoilla on monia hyviä laillisia käyttökohteita ja olisi monestakin näkökulmasta huono asia, mikäli ne nähtäisiin vain rahanpesun ja muun rikollisuuden instrumenttina.

Edellä mainitun pohjalta tutkielman jatkotutkimusehdotuksina nostetaan ensimmäisenä esiin aiheeseen liittyvän sääntely-ympäristön kehittyminen. Voisi olla mielekästä tarkastella tilannetta tulevaisuudessa siitä näkökulmasta, onko pankkien riskienhallintaa aiheeseen liittyen ohjannut enemmän sääntelyn kehittyminen vai sisäisten prosessien tehostuminen. Tutkimusprosessin aikana aineistosta nousi esiin myös virtuaalivaluuttatoimijat pankin asiakkaina ja tähän liittyvä de-risking ilmiö. Kyseisellä ilmiöllä tarkoitetaan tilannetta, jossa pankit pyrkivät välttämään uuteen asiakkuuteen liittyvää riskiä rajoittamalla ja kieltäytymällä kategorisesti samalla toimialalla operoivien yritysten asiakkuuksista. Mikäli pankit näkevät kaikki virtuaalivaluuttatoimijat kategorisesti liian riskisinä ja pankki kieltäytyy ottamasta niitä asiakkaikseen, päätyvätkö nämä toimijat hankkimaan pankkipalvelunsa toimialueilta, jossa rahanpesun estämiseen liittyvä sääntely ja toimintatavat ovat heikompia? Lisäksi tutkielmassa todettiin aiemmin virtuaalivaluuttoihin liittyvä rahanpesuriski aiheena siirrettäväksi, jonka perusteella yksi jatkotutkimusehdotus voisi olla virtuaalivaluuttojen käyttäminen terrorismin rahoittamisessa sekä pankin rooli sen estämisessä. Myös monet tässä tutkielmassa aineistona käytetyt tutkimukset sivusivat kyseistä aihepiiriä. Lisäksi tutkittava aihealue sopii siirrettäväksi pankkien sijasta itse virtuaalivaluuttatoimijoiden kontekstiin: miten niiden tulisi tunnistaa ja hallita virtuaalivaluuttojen kautta tapahtuvaa rahanpesua.

LÄHDELUETTELO

Kirjallisuuslähteet:

Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. Journal of Economics and Business, 100, 64-75.

Arner, D. W., Auer, R., & Frost, J. (2020). Stablecoins: Risks, Potential and Regulation. BIS Working paper no. 905/2020. University of Hong Kong Faculty of Law Research Paper N0. 2021/57.

Bashir, I. (2018). Mastering Blochain - Distributed ledger technology, decentralization and smart contracts explained. Birmingham: Packt Publishing.

Bessis, J. (2011). Risk management in banking. John Wiley & Sons.

Bergström, M., Svedberg Helgesson, K., & Mörth, U. (2011). A new role for for-profit actors? The case of anti-money laundering and risk management. JCMS: Journal of Common Market Studies, 49(5), 1043-1064.

Carson, D., Gilmore, A., Perry, C., & Gronhaug, K. (2001). Qualitative marketing research. Sage.

Chapman, R. (2018). Anti-Money Laundering: A practical guide to reducing organizational risk. Kogan Page Publishers.

Chau, D., & Nemcsik, M. (2020). Anti-Money Laundering Transaction Monitoring Systems Implementation: Finding Anomalies. Wiley.

Cornelissen. (2017). Editor's comments: Developing propositions, a process model, or a typology? Addressing the challenges of writing theory without a boilerplate. The Academy of Management Review, 42(1), 1–9. https://doi.org/10.5465/amr.2016.0196

Cooper, H. M. (1989). Integrating research: A guide for literature reviews. Sage Publications, Inc.

Davies, H. & Zhivitskaya, M. (2018). Three Lines of Defence: A Robust Organising Framework, or Just Lines in the Sand? *Global Policy*, *9*(S1), 34–42. https://doi.org/10.1111/1758-5899.12568

Diebold, Doherty, N. A., & Herring, R. (2010). The known, the unknown, and the unknowable in financial risk management measurement and theory advancing practice. Princeton University Press. https://doi.org/10.1515/9781400835287

Donet J.A., Pérez-Solà C., Herrera-Joancomartí J. (2014) The Bitcoin P2P Network. Julkaisussa Böhme R., Brenner M., Moore T., Smith M. (toim.) Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science, vol 8438. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44774-1_7

Efron, S. E. & Ravid, R. (2019). Writing the literature review: a practical guide. The Guilford Press.

Eskandari, S., Clark, J., Barrera, D., & Stobert, E. (2018). A first look at the usability of bitcoin key management. Cornell University.

Garland, D. (2003) 'The Rise of Risk'. Julkaisussa Ericson, R.V. & Doyle, A. (toim.) Risk and Morality. University of Toronto Press. https://arxiv.org/abs/1802.04351

Giudici, P., Leach, T., & Pagnottoni, P. (2022). Libra or Librae? Basket based stablecoins to mitigate foreign exchange volatility spillovers. *Finance Research Letters*, *44*, 102054.

Gupta, A., Dwivedi, D. N., & Jain, A. (2022). Threshold fine-tuning of money laundering scenarios through multi-dimensional optimization techniques. Journal of Money Laundering Control, 25(1), 72–78. https://doi.org/10.1108/JMLC-12-2020-0138

Hansson, S. O. (2010). Risk: objective or subjective, facts or values. Journal of risk research, 13(2), 231-238.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. McKinsey & Company, 1-11.

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T. S., Stetsenko, N. & -Verdugo-Yepes, C.(2016). Virtual currencies and beyond: initial considerations. International Monetary Fund.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2009). Tutki ja kirjoita (15. uud. p.). Tammi.

Isa, Y. M., Sanusi, Z. M., Haniff, M. N., & Barnes, P. A. (2015). Money laundering risk: from the bankers' and regulators perspectives. Procedia Economics and Finance, 28, 7-13.

Jayasekara, S. D. (2021) How effective are the current global standards in combating money laundering and terrorist financing? Journal of money laundering control. 24 (2), 257–267.

Johansson, P., Eerola, M., Innanen, A., Viitala, J., & Alasaarela, M. (2019). Lohkoketju : tiekartta päättäjille. Alma Talent Oy.

Koskinen, L. (2018). Riskienhallinta ja tietämyksen tasot. Julkaisussa Ahteensivu, A., Koskinen, L., Kulmala, J. & Havakka, P. (toim.) Riskienhallinnan ajankohtaisia teemoja. Tampere University Press.

Lindgreen, Di Benedetto, C. A., Brodie, R. J., & Jaakkola, E. (2021). How to develop great conceptual frameworks for business-to-business marketing. Industrial Marketing Management, 94, A2–A10. https://doi.org/10.1016/j.indmarman.2020.04.005

Levi, M., & Reuter, P. (2006). Money laundering. Crime and justice, 34(1), 289-375.

Lucchetti, U. Jr (2018). Measures to decrease the volume of false positive alerts in the transaction monitoring process. ProQuest Dissertations Publishing, p. 13422679.

Metsämuuronen. (2006). Tutkimuksen tekemisen perusteet ihmistieteissä: opiskelijalaitos (2. laitos, 3. uud. p.). International Methelp.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

Pavlidis, G. (2020) International regulation of virtual assets under FATF's new standards. The journal of investment compliance. 21 (1), 1–8.

Power, M. (2004). The risk management of everything. The Journal of Risk Finance.

Rausand, M. (2013). Risk assessment: theory, methods, and applications (Vol. 115). John Wiley & Sons.

Reuter, P. (2005). Chasing dirty money: The fight against money laundering. Peterson Institute.

Ross, S., & Hannan, M. (2007). Money laundering regulation and risk-based decision-making. Journal of Money Laundering Control.

Salminen, A. (2011), Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston Julkaisuja.

Saunders, Lewis, P., & Thornhill, A. (2019). Research methods for business students (Eighth edition.). Pearson Education.

Shokry, A. E. M., Rizka, M. A., & Labib, N. M. (2020). Counter terrorism finance by detecting money laundering hidden networks using unsupervised machine learning algorithm. In *International Conferences ICT, Society, and Human Beings*.

Sobh, T. S. (2020). An Intelligent and Secure Framework for Anti-Money Laundering. Journal of Applied Security Research, 15(4), 517-546.

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos.). Tammi.

Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. Human resource development review, 15(4), 404-428.

Torraco. (2005). Writing Integrative Literature Reviews: Guidelines and Examples. Human Resource Development Review, 4(3), 356–367. https://doi.org/10.1177/1534484305278283

Zhu, T. (2006), An outlier detection model based on cross datasets comparison for financial surveillance, IEEE Asia-Pacific Conference on Services Computing (AP- SCC'06)", pp. 601-604

Woiceshyn, J., & Daellenbach, U. (2018). Evaluating inductive vs deductive research in management studies: Implications for authors, editors, and reviewers. Qualitative Research in Organizations and Management: An International Journal.

Viranomaislähteet:

Basel (2021). Basel AML Index 2021: 10th Public Edition. Ranking money laundering and terrorist financing risks around the world. Saatavissa:

https://baselgovernance.org/sites/default/files/2021-09/Basel_AML_Index_2021_10th%20Edition.pdf

Basel (2020). Basel Committee on Banking Supervision: Revisions to the principles for the sound management of operational risk. Bank for International Settlements. Saatavissa: https://www.bis.org/bcbs/publ/d508.pdf

Euroopan Komissio (2021). Euroopan parlamentin ja neuvoston asetus rahanpesun ja terrorismin rahoituksen torjuntaviranomaisen perustamisesta ja asetusten (EU) N:o 1093/2010(EU) N:o 1094:2010 ja (EU) N:o 1095/2010 muuttamisesta. Saatavissa: https://eur-lex.europa.eu/resource.html?uri=cellar:ce0c29bb-ead1-11eb-93a8-01aa75ed71a1.0017.02/DOC_1&format=PDF

Euroopan Parlamentti (2022). Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets. Saatavissa: https://www.europarl.europa.eu/doceo/document/CJ12-AM-719852_EN.pdf

FATF (2022). The FATF Recommendations - International standards on combating money laundering and the financing of terrorism & proliferation. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FATF (2021). Second 12-month review of revised FATF standards on virtual assets and virtual asset service providers. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

FATF (2019). Anti-money laundering and counter-terrorist financing measures, Finland Mutual Evaluation Report. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Finland-2019.pdf

FATF (2015). Guidance for a risk-based approach - Virtual Currencies. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

Valtiovarainministeriö (2021). Kansallisen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021.Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163051/VM_2021_17.pdf?sequence=1&isAllowed=y

Oikeudelliset lähteet:

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

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

Rikoslaki 19.12.1889/39. Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L32

Internet-lähteet

Bitnodes (2022). Global Bitcoin Nodes Distribution. Viitattu 15.1.2022. Saatavissa: https://bitnodes.io/

Bloomberg (2022). Bank of Russia seeks to outlaw mining and trading of crypto. Viitattu 24.1.2022. Saatavissa: https://www.bloomberg.com/news/articles/2022-01-20/russia-s-fsb-tells-nabiullina-to-ban-crypto-to-defund-opposition

Coinmarketcap (2021). How Long Does a Bitcoin Transaction Take? Viitattu 15.1.2022. Saatavissa: https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take

Deloitte (2019). The global framework for fighting financial crime. Viitattu 26.1.2022. Saatavissa: https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/financial-services/gx-fsi-iif-financial-crime-report-ap7.pdf

EBA (2019). Report with advice for the European Commission on crypto assets. Viitattu 15.1.2022. Saatavissa: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1

Euroopan Keskuspankki (2012). Virtual currency schemes. Viitattu 9.1.2022. Saatavissa: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Euroopan Keskuspankki (2015). Virtual currency schemes – A further analysis. Viitattu 9.1.2022. Saatavissa: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf?fe92070cdf17668c02846440e457dfd0

Euroopan Parlamentti (2022). Crypto assets: new rules to stop illicit flows in the EU. Viitattu 24.4.2022. Saatavissa: https://www.europarl.europa.eu/news/fi/press-room/20220324IPR26164/crypto-assets-new-rules-to-stop-illicit-flows-in-the-eu

Financial Conduct Authority FCA (2021). FCA fines HSBC Bank plc £63.9 million for deficient transaction monitoring controls. Viitattu 25.1.2022. Saatavissa: https://www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls

Finanssivalvonta (2021a). Riskiarvio. Viitattu 12.2.2022. Saatavissa: https://www.finanssivalvonta.fi/rahanpesun-estaminen/riskiarvio/

Finanssivalvonta (2021b). Selonotto- ja ilmoitusvelvollisuus. Viitattu 12.2.2022. Saatavissa: https://www.finanssivalvonta.fi/rahanpesun-estaminen/selonotto--ja-ilmoitusvelvollisuus/

Finanssivalvonta (2019). Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu? Viitattu 14.1.2022. Saatavissa: https://www.finanssivalvonta.fi/kuluttajansuoja/virtuaalivaluutat/

Haar Ryan (2022). Time.com: The Future of Cryptocurrency: 5 Experts' Predictions After a 'Breakthrough' 2021. Viitattu 8.1.2022. Saatavissa: https://time.com/nextadvisor/investing/cryptocurrency/future-of-cryptocurrency/

Hayes, A. (2022). What Happens to Bitcoin After All 21 Million Are Mined? Viitattu 19.2.2022. Saatavissa: https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/

Helsingin Sanomat (2021), Bitcoinista tuli El Salvadorin virallinen valuutta, mutta sen käyttöönotto kompasteli pahasti: virtuaali-lompakkoa ei saanutkaan ladattua sovellus-kaupoista, viitattu 2.2.2021, saatavilla: https://www.hs.fi/talous/art-2000008247580.html

Kauppalehti (2022). USA määräsi uusia pakotteita Venäjää vastaan – nyt isketään kiinni kryptovaluuttafirmoihin. Viitattu 24.4.2022. Saatavissa: https://www.kauppalehti.fi/uutiset/usa-maarasi-uusia-pakotteita-venajaa-vastaan-nyt-isketaan-kiinni-kryptovaluuttafirmoihin/b09f3711-9066-4a0c-8dda-44bf2d3320fe

Lang, H. (2022). Nearly half of crypto owners first bought digital assets in 2021, survey shows. Viitattu 25.4.2022. Saatavissa: https://www.reuters.com/technology/nearly-half-crypto-owners-first-bought-digital-assets-2021-survey-2022-04-04/

Nordea (2022). Kolme puolustuslinjaa. Viitattu 12.2.2022. Saatavissa: https://www.nordea.com/fi/tietoa-meista/nordea-yhteiskunnassa/kolme-puolustuslinjaa

Nordea (2021). Nordea AML/CFT/ATE Policy statement. Saatavissa: https://www.nordea.com/en/doc/aml-cft-ate-policy-statement.pdf

OP (2022). Sisäinen ja ulkoinen valvonta. Viitattu 12.2.2022. Saatavissa: https://www.op.fi/op-ryhma/tietoa-ryhmasta/hallinnointi/sisainen-ja-ulkoinen-valvonta

Orji (2022). Bitcoin ban: These are the countries where crypto is restricted or illegal. Viitattu 10.4.2022. Saatavissa: https://www.euronews.com/next/2022/01/11/bitcoin-ban-these-are-the-countries-where-crypto-is-restricted-or-illegal2

SAS (2022). Rahanpesun torjunta - mitä se on ja miksi sillä on merkitystä. Viitattu 23.1.2022. Saatavissa: https://www.sas.com/fi_fi/insights/fraud/anti-money-laundering.html

Septhon, C. (2021). Crypto assets explained. Viitattu 14.1.2022. Saatavissa: https://currency.com/what-are-crypto-assets

Statista. (2022a). Overall cryptocurrency market capitalization per week from July 2010 to January 2022 (in billion U.S. dollars) [Graph]. In Statista. Retrieved January 16, 2022, from https://www-statista-com.libproxy.tuni.fi/statistics/730876/cryptocurrency-maket-value/

Statista. (2022b). Number of cryptocurrencies worldwide from 2013 to January 2022 [Graph]. In Statista. Viitattu 16.1.20222. Saatavissa: https://www-statista-com.libproxy.tuni.fi/statistics/863917/number-crypto-coins-tokens/
UNODC (2022). Money Laundering. Viitattu 22.1.2022. Saatavissa: https://www.unodc.org/unodc/en/money-laundering/overview.html

Valtiovarainministeriö (2022). Rahanpesun ja terrorismin rahoittamisen estäminen. Viitattu 19.3.2022. Saatavissa: https://vm.fi/rahanpesun-estaminen

Verohallinto (2020). Virtuaalivaluutat vakiintuneet vaihdannan välineiksi. Viitattu 8.1.2022. Saatavissa: https://www.vero.fi/harmaa-talous-rikollisuus/ilmi%C3%B6t/virtuaalivaluutat/

Yle Uutiset (2020). Selvitys: Swedbank epäonnistui rahanpesun torjunnassa – epäilyttävää rahaa kulki pankin tilien kautta vähintään 37 miljardia euroa. Viitattu 30.10.2021. Saatavissa: https://yle.fi/uutiset/3-11271107

Ycharts (2022). Bitcoin Average Transaction Fee. Viitattu 15.1.2022. Saatavissa: https://ycharts.com/indicators/bitcoin_average_transaction_fee

LIITTEET

Liite 1: Haastattelurunko

Haastateltavien taustatiedot

1. Kerro taustastasi: koulutuksesi, työtehtäväsi ja nykyiset vastuualueesi

Teema 1: Virtuaalivaluuttojen aiheuttaman rahanpesuriskin tunnistaminen

Muun muassa FATF on nostanut viime vuosina virtuaalivaluutat yhdeksi merkittävämmäksi uudeksi ilmiöksi ja riskiksi rahanpesuun liittyen. Virtuaalivaluutat ovat tehokas keino rahanpesuun muun muassa johtuen niiden pseudo-anonyymistä luonteesta ja helposta hajautettavuudesta. Virtuaalivaluuttatransaktiot ovat lisäksi nopeampia ja matalakuluisempia kuin perinteiset fiat-valuutoilla toteutettavat transaktiot. Lisäksi virtuaalivaluuttatransaktioita on helppo toteuttaa sekä kansallisesti että kansainvälisesti. Riskiä lisää myös keskitetyn valvojatahon sekä yhtenäisen kansainvälisen sääntelyn puuttuminen.

2. Verrattuna muihin rahanpesuun liittyviin riskeihin, esimerkiksi käteiseen, kuinka merkittävänä riskinä näet virtuaalivaluutat?
3. Onko mielestäsi suomalaisella pankkisektorilla huomioitu virtuaalivaluuttojen aiheuttama rahanpesuriski riittävällä tavalla?

Teema 2: Virtuaalivaluuttojen aiheuttaman rahanpesuriskin hallintakeinoja

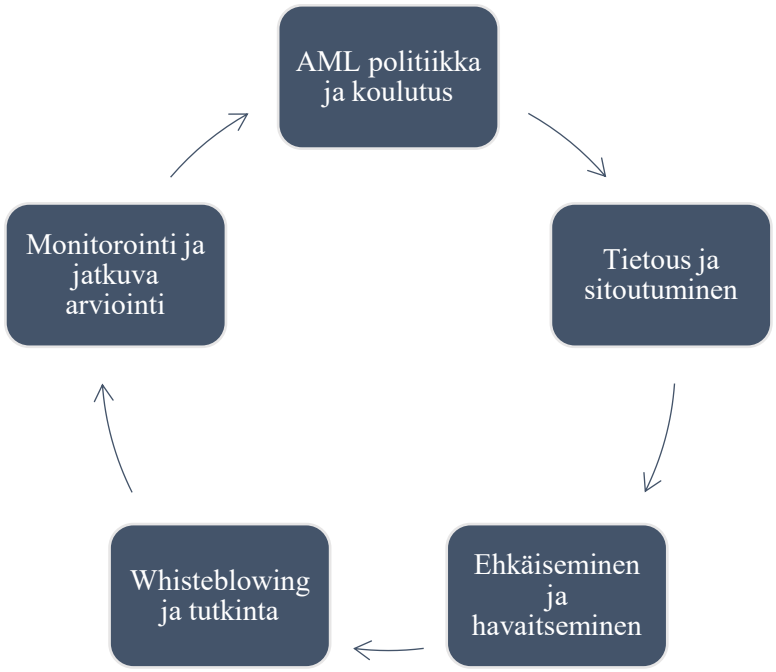
Organisaatioiden tulee tunnistaa rahanpesuriskin, järjestelmien heikkoudet sekä estää organisaation kautta tapahtuvaa rahanpesua. Pankkien kontekstissa voidaan todeta, että rahanpesuriskiin liittyvä riskienhallinta voidaan pilkkoa seuraaviin yhdeksään kohtaan (Chapman, 2018, 16):

1. Hallinto- ja kontrolliympäristö

2. Työntekijöiden rekrytointi, koulutus ja johtaminen

3. Toimiala-, tuote- ja maantieteellisten riskien sekä asiakkaiden demografisten riskien hallintamallit

4. *CDD - Asiakkaan tunteminen*
5. *Jatkuva transaktiomonitorointi ja transaktioscreenaus (pakotteet)*
6. *Datan hyödyntäminen ja tiedolla johtaminen*
7. *Liiketoimintojen ohjeistus ja tuki*
8. *Sisäinen ja ulkoinen tarkastus*
9. *Kokonaisvaltainen rahanpesun estämisen kyvykkyyksien monitorointi ja parantaminen AML-strategiaympyrän avulla (alapuolella)*



4. Millä eri keinoin pankit voivat huomioida virtuaalivaluuttojen aiheuttaman rahanpesuriskin osana riskienhallintaansa? Halutessasi voit käyttää vastauksessa apuna edellä esiteltyjä rahanpesuriskin hallinnan osa-alueita.
5. Millaisena näet edustamasi riskienhallinnan puolustuslinjan roolin näitä keinoja sovellettaessa?
6. Millaisena näet yleisen kehityksen liittyen virtuaalivaluuttojen aiheuttamaan rahanpesuriskiin ja sen hallintaan tulevaisuudessa?
7. Millaiseksi toivoisit aihepiiriin liittyvän sääntely-ympäristön kehittyvän tulevaisuudessa?

Liite 2: Kirjallisuuskatsauksessa käytetyt tutkimusartikkelit ja muu kirjallisuus

Taulukko 5: Tutkimusartikkelit ja muut julkaisut

	Tutkimuksen tekijä(t), nimi ja julkaisutiedot. Aineistot hakusanojen antamien osumien mukaisessa järjestyksessä.	Julkaisun teema
1.	Bystriakov, Guirinskiy, A. V., Nan, T. N., Hidar, S., & Din, L. C. (2019). Crypto Currencies and Possible Risks. In Digital Economy: Complexity and Variety vs. Rationality (pp. 175–181). Springer International Publishing.	Tutkimus keskittyy kryptovaluuttoihin liittyviin riskeihin sekä niihin liittyviin prosesseihin.
2.	Crosman. (2015). Can You Really "Know" a Customer Who Uses Bitcoin? The American Banker, 1(184).	Artikkeli käsittelee virtuaalivaluuttoihin liitettäviä rahanpesun estämisen mekanismeja.
3.	Silva Ramalho, & 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.	Tutkimus esittelee Bitcoinin aiheuttamia ongelmia rahanpesun kontekstissa.
4.	Teichmann, & Falker, M.-C. (2020). Money Laundering Through Cryptocurrencies. Artificial Intelligence: Anthropogenic Nature Vs. Social Origin, 1100, 500–511	Tutkimus analysoi virtuaalivaluuttoihin liittyviä compliance-riskejä ja kryptovaluuttaliitännäisiä rahanpesutypologioita.
5.	Barone, & Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques. European Journal of Law and Economics, 47(2), 233–254	Tutkimus käsittelee eri kryptovaluuttaliitännäisiä rahanpesutypologioita.
6.	Teichmann, & Falker, M.-C. (2021). Cryptocurrencies and financial crime: solutions from Liechtenstein. Journal of Money Laundering Control, 24(4), 775–788.	Tutkimus tarkastelee, miten kryptovaluuttoja käytetään osana rahanpesua. Lisäksi nykylainsäädäntöä peilataan Liechtensteinissa käytettävään lainsäädännölliseen viitekehykseen.
7.	Datinský. (2020). European Legal Regulation of Cryptocurrencies through the AML Scope. Public Governance, Administration and Finances Law Review, 5(1), 38–47.	Tutkimus keskittyy kryptovaluuttojen vaikutukseen rahanpesun estämiseen Euroopan Unionin tasolla.
8.	Desmond, Lacey, D., & Salmon, P. (2019). Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. Journal of Money Laundering Control, 22(3), 480–497.	Tutkimus tarkastelee virtuaalivaluuttojen kautta tapahtuvaa rahanpesua systeemiteorian avulla.

9.	Wronka. (2022). Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. Journal of Money Laundering Control, 25(1), 79–94	Tutkimuksen tarkoituksena on taustoittaa kryptovaluuttojen aiheuttamaa rahanpesuriskiä sekä peilata siihen liitettäviä toimenpiteitä AMLD5:n kontekstissa.
10.	Sanz-Bas, del Rosal, C., Náñez Alonso, S. L., & Echarte Fernández, M. Á. (2021). Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. Laws, 10(3), 57–.	Tutkimuksen tarkoituksena on havainnollistaa, miten eri tahot käyttävät virtuaalivaluuttoja osana rikollisia toimenpiteitä ja miten lainsäädännön keinoin tätä voidaan estää.
11.	Albrecht, Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210–216.	Tutkimuksen tarkoituksena on käsitellä rahanpesun prosessia ja sitä, miten kryptovaluuttoja voidaan hyödyntää prosessin osana.
12.	Dyntu, & Dykyi, O. (2019). Cryptocurrency in the system of money laundering. Baltic Journal of Economic Studies, 4(5), 75–81.	Tutkimuksen tarkoitus on tutkia virtuaalivaluuttoja osana rahanpesuprosessia.
13.	Choo. (2015). Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks? In Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data (pp. 283–307).	Kirjan luku käsittelee erilaisia korruptioon ja rahanpesuun liittyviä riskejä, joista merkittävin on virtuaalivaluuttoihin liittyvä rahanpesuriski.
14.	Naheem. (2018). Regulating virtual currencies – the challenges of applying fiat currency laws to digital technology services. Journal of Financial Crime, 25(2), 562–575.	Tutkimus tarkastelee, miten kryptovaluuttoihin liittyvä uusi lainsäädäntö vaikuttaa pankkien riskiarvioihin.
15.	Naheem. (2019). Exploring the links between AML, digital currencies and blockchain technology. Journal of Money Laundering Control, 22(3), 515–526.	Tutkimus tarkastelee FATF:in vuoden 2014 ohjeistuksien vaikutusta lohkoketjuteknologiaa ja rahanpesun estämistä koskevaan sääntelyyn liittyen
16.	Goldbarsht. (2022). Virtual currencies as a quasi-payment tool: the case of frequent-flier programs and money laundering. Journal of Money Laundering Control, 25(1), 150–164.	Tutkimuksen tarkoitus on käsitellä lentopistejärjestelmän kautta tapahtuvaa rahanpesua ja sen aiheuttamaa uhkaa Australian kontekstissa.
17.	Bandler. (2021). Investigations: Money Laundering. In Encyclopedia of Security and Emergency Management (pp. 565–577). Springer International Publishing.	Kirjan luku käsittelee rahanpesun tutkimista sekä lainsäätäjien että finanssitoimijoiden näkökulmasta.
18.	Haffke, Fromberger, M., & Zimmermann, P. (2019). 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.	Artikkeli analysoi AMLD5:n vaikutusta virtuaalivaluuttaekosysteemin eri toimijoihin.

19.	Alarab, I., Prakoonwit, S., & Nacer, M. I. (2020). Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In Proceedings of the 2020 5th International Conference on Machine Learning Technologies (pp. 11–17).	Tutkimus vertailee kahta eri tapaa tulkita epäilyttäviä transaktioita lohkoketjusta.
20.	Sprenger, P., & Balsiger, F. (2018). Anti-money laundering in times of cryptocurrencies. KPMG.ch.	Julkaisun tarkoituksena on tarjota pankeille eri keinoja hallita paremmin virtuaalivaluuttaliitännäistä rahanpesua.
21.	Goriacheva, A., Jakubenko, N., Pogodina, O., & Silnov, D. (2018). Anonymization technologies of cryptocurrency transactions as money laundering instrument. KnE Social Sciences, 46-53.	Artikkelin tarkoituksena on käsitellä erilaisia virtuaalivaluuttatransaktioiden anonymisointipalveluita.
22.	Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. Journal of Financial Crime.	Tutkimuksen tarkoituksena on kuvata virtuaalivaluuttojen käyttämistä rahanpesun välineenä kuuden eri rahanpesumekanismin kautta.
23.	Brenig, C., & Müller, G. (2015). Economic analysis of cryptocurrency backed money laundering. ECIS 2015 Completed Research Papers.	Tutkimus tarkastelee rahanpesumekanismeja, joissa hyödynnetään kryptovaluuttoja.

Liite 3: Kirjallisuuskatsauksessa käytetyt viranomaislähteet

Taulukko 6: Viranomaisjulkaisut

	Julkaisija	Julkaisun tiedot
1.	Keskusrikospoliisi – Rahanpesun Selvittelykeskus	Rahanpesuindikaattorit. 2021.
2.	Keskusrikospoliisi – Rahanpesun Selvittelykeskus	Puolivuosikatsaus – Rahanpesun Selvittelykeskus. 2021.
3.	Finanssivalvonta	Määräykset ja ohjeet 4/2019 - Virtuaalivaluutan tarjoajat: yhteenveto ja palaute lausunnoista. 2019.
4.	Finanssivalvonta	Virtuaalivaluutan liikkeeseenlasku edellyttää lupaa Finanssivalvonnalta – keskiössä asiakkaansuoja ja rahanpesun estäminen. 2021.
5.	Financial Action Task Force – FATF	Guidance for a Risk-Based Approach - Virtual Assets and Virtual Asset Service Providers. 2019.
6.	Financial Action Task Force – FATF	Virtual Currencies – Key Definitions and Potential AML/CFT Risks. 2014.
7.	Financial Action Task Force – FATF	FATF Report to the G20 Finance Ministers and Central Bank Governors. 2018.

8.	Euroopan Komissio - ENISA	Distributed Ledger Technology & Cybersecuirity – Improving information secuirity in the financial sector. 2016.
9.	Euroopan Komissio	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. 2019.
10.	Euroopan Komissio	Euroopan Parlamentin ja Neuvoston asetus varainsiirtojen ja tiettyjen kryptovarojen siirtojen mukana toimitettavista tiedoista. 2021.
11.	European Banking Authority EBA	Report with advice for the European Commission on crypto-assets. 2019.
12.	European Banking Authority EBA	Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector. 2021.

Liite 4: Kirjallisuuskatsauksessa käytetyt lohkoketjuanalytiikkaa tarjoavien yrityksien julkaisut

Taulukko 7: Lohkoketjuanalytiikkaa tarjoavien yrityksen julkaisut

Yritys	Julkaisun nimi	Uusin julkaisu
Chainanalysis	The Crypto Crime Report 2022	2022
Elliptic	Preventing Financial Crime in Cryptoassets: Typologies Report 2022	2022