Haaga-Helia
ammattikorkeakoulu Oy

Kryptovaluutat ja AML-lainsäädäntö

Sini Siekkinen

Opinnäytetyö
Johdon assistenttityön ja kielten koulutusohjelma
2018

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Sini Siekkinen

Koulutusohjelma
Johdon assistenttityön ja kielten koulutusohjelma

Raportin/Opinnäytetyön nimi
Kryptovaluutat ja AML-lainsäädäntö

Sivu- ja liitesivumäärä
34

Tutkin opinnäytetyössäni rahanpesua ja sen estämistä uusien teknologioiden ja erityisesti kryptovaluuttojen yleistymisen myötä. Sivusin yleisimpiä kryptovaluuttoja ja keskityin bitcoiniin, sillä se on parhaiten tunnettu lohkoketjuun perustuva kryptovaluutta. Tavoitteenani oli tehdä läpileikkaus nykytilanteesta ja tutkia, helpottavatko kryptovaluutat rahanpesun ja terrorismin rahoittamista.

Teoriaosuudessa kuvailen blockchain- eli lohkoketjuteknologiaa, sen toimintaperiaatetta ja sovelluksia sekä bitcoinin historiaa ja nykytilannetta. Aikaisemmat tutkimukset osoittavat, että rikollisuus ja jopa hybridisodankäynti linkittyy vahvasti bitcoiniin. Kerron Suomen rahanpesulainsäädännöstä edeten kansainvälisiin standardeihin, jotka vaikuttavat lakeihin kansallisella tasolla. Käsittelen myös uutta rahapesudirektiiviä, joka ulottuu jatkossa tarkemmin kryptovaluutta-alustoihin ja palveluntarjoajiin.

Toteutin työn tapaustutkimuksena ja käytin menetelmänä kirjallisuuskatsausta. Tapaustutkimuksen kohteena oli Danske Bankin hiljattain paljastunut rahanpesuskandaali ja siitä julkaistu riippumattoman tanskalaisen asianajotoimiston laatima raportti. Dansken Virossa sijaitsevan sivuliikkeen kautta virtasi miljardeja venäläistä alkuperää olevaa rahaa, ja epäillään, että osaa rahoista on kierrätetty pankissa ainoastaan rahanpesutarkoituksessa. Nostin esiin erityisesti riskienhallinnan kannalta puutteellisia tekijöitä.

Tutkimuksestani kävi ilmi, että Danske Bankin Viron yksikköön liittyi sekä sisäisiä että ulkoisia riskejä. Sisäiset riskit liittyivät esimerkiksi puutteisiin valvonnassa ja asiakkaan tuntemisessa. Ulkoiset riskit puolestaan geopoliittisiin tekijöihin, kuten Viron ja Venäjän välisiin suhteisiin. Työssäni selvisi myös, että monet yritykset, joita asiakkaan tuntemisvelvollisuus koskee, eivät ole riittävän perillä kehittyvistä teknologioista ja niihin liittyvistä uusista liiketoimintamalleista. Viranomaisten ja yritysten tulisi tehdä tiiviimpää yhteistyötä kryptovaluuttojen palveluntarjoajien kanssa voidakseen ymmärtää ja säännellä näiden toimintaa paremmin.

Toteutin työn syksyllä 2018.

Asiasanat
Kryptovaluutat, bitcoin, lohkoketju, rahanpesun ja terrorismin rahoittamisen estäminen, Financial Action Task Force

Sisällys

1 Johdanto

Tutkin opinnäytetyössäni rahanpesua ja sen estämistä uusien teknologioiden ja erityisesti kryptovaluuttojen näkökulmasta. Sivuan yleisimpiä kryptovaluuttoja mutta keskityn Bitcoiniin, sillä se on parhaiten tunnettu ja eniten esillä ollut virtuaalivaluutta. Tavoitteenani on tutkia ja selittää laadullisin menetelmin ilmiöksikin muodostunutta kryptovaluuttabuumia ja tutkia, lisäävätkö kryptovaluutat rahanpesua. Esittelen myös blockchain- eli lohkoketjuteknologian bitcoinin takana. Kuvailen lyhyesti lohkoketjun toimintaperiaatetta ja sovelluksia. Lohkoketjuteknologia on saanut oman osansa hypestä ja tulee todennäköisesti laajempaan käyttöön lähitulevaisuudessa.

Virtuaalivaluutat ovat saaneet alkunsa 1990-luvun alkupuolella, mutta ovat suhteellisen tuore ilmiö talouselämässä. Uutisotsikot ovat usein kaksijakoisia; joko bitcoin nähdään uhkana ja pankkijärjestelmän horjuttajana tai uudenlaisena rahoitusjärjestelmän mullistajana, joka mahdollistaa suoran rahansiirron ilman välikäsiä. Toisaalta bitcoin voi olla mielenkiintoinen sijoituskohde, toisaalta sen arvon heittely koko olemassaolonsa ajan tekee siitä arvaamattoman ja heikosti ennustettavan valuutan.

Tutkin, mitä toimia eri viranomaisilla ja finanssialan tahoilla on ollut ja tulee olemaan rahanpesun ja terrorismin rahoittamisen estämiseksi, nyt kun kryptovaluuttojen käyttäjien anonymiteetti ja valvonnan puute tuovat uusia tapoja liikuttaa rikollista rahaa. Käytän apunani laadullisia menetelmiä: pyrin tutkimaan ilmiötä teoriaosuudessa kirjallisuuskatsauksen avulla ja tutkin riskienhallinnan näkökulmasta Danske Bankin rahanpesuskandaalia. Käytän tapaustutkimuksessa Danske Bankin ulkopuolisella asianajotoimistolla teettämää raporttia.

Hiljattain on paljastunut useita rahanpesuepäilyjä, joissa globaalisti suuret rahoitusalan toimijat kuten HSBC, BNP Paribas, ING ja muun muassa Deutsche Bank ovat syytettyjen listalla. On arvioitu, että maailmassa pestään vuosittain rahaa kahden biljoonan dollarin edestä. (Jenkins 2018.) Viimeisimpänä listalle on päätynyt myös pohjoismainen Danske Bank, jonka Viron sivukonttorin kautta pestiin miljardien eurojen arvosta rahaa (Boxberg 2018, 10).

Pankkien johtavassa asemassa olevat henkilöt on erotettu ja pankkeja on sakotettu rikoksista. Keskustelua käydään kuitenkin siitä, ovatko seuraamukset riittäviä ja valvonta ajantasaista ja tarpeeksi tehokasta. Varsinkin eurooppalaiset viranomaiset saavat moitteita toiminnastaan tai pikemminkin sen puutteesta. Jenkins (2018) väittää artikkelissaan, että eu-

rooppalainen rahanpesun valvonta on kaaoksessa: EU:n jäsenmaiden valvontaviranomaisten laatu ei ole tasaista, rahanpesudirektiiviä ei ole implementoitu yhtenäisesti, osa maista perustaa taloutensa ulkomaiseen rahaan ilman kunnollista selvitystä alkuperästä, kansalliset viranomaiset eivät tee yhteistyötä keskenään eikä EU:lla ole yhteistä tietokantaa rahanpesusta. Vaadittavia toimenpiteitä rahanpesun kitkemiseksi ei ole toisin sanoen kehitetty riittävästi, eivätkä viranomaiset pysy muuttuvien liikeideoiden ja toimintamallien perässä.

Valtioiden suhtautuminen rahanpesuun muistuttaa niiden suhtautumista kryptovaluuttojen sääntelyyn: otetaan sivustakatsojan rooli (Künnapas 2016, 114) eikä puututa asioiden kulkuun ennen kuin ne menevät huolestuttavaan suuntaan. Esimerkiksi Danske Bankin tapauksessa rivityöntekijät olivat raportoineet rahanpesuepäilyistä Viron yksikön johdolle, joka ei puolestaan puuttunut asiaan (Boxberg 2018, 10). Tutkin kirjallisuuskatsauksessani ja tapaustutkimuksessani, onko rahanpesutapauksissa yhteisiä piirteitä, joista voisi tehdä jonkinlaisia päättelyitä.

Käytän bitcoinista vaihtelevasti termiä kryptovaluutta, virtuaalivaluutta ja digitaalivaluutta. Bitcoin on kaikkea näitä (Miller 2015, 14), mutta täytyy ottaa huomioon, etteivät ne ole synonyymejä. Kryptovaluutat ovat luonteeltaan salaisia (kryptografisia) ja vaativat erilaisia avaimia koodin muodossa, jotta niihin pääsee käsiksi. Virtuaalivaluutta-termiä käytetään valuutoista, joita ei säännellä ja joiden arvoa ei ole sidottu mihinkään perinteiseen valuuttaan. Digitaalivaluutta on valuutta, jolla ei ole lainkaan fyysistä olemusta, kuten seteleitä tai kolikoita. Digitaalivaluutta on olemassa ainoastaan pilvessä tai paikallisella tietokoneella, ja kaikki rahansiirto tapahtuu digitaalisesti. (Miller 2015, 14-15.)

Käsittelen rahapesun ja terrorismin estämiseen ja asiakkaan tuntemiseen liittyvää termistöä. AML tai PML, Anti-money laundering tai preventing money laundering on kansainvälinen termi rahanpesulainsäädännölle (Financial Action Task Force 2018a). FATF eli Financial Action Task Force on G7-maiden perustama kansainvälinen toimintaryhmä, joka laatii standardeja ja suosituksia rahanpesuun, terrorismin rahoittamiseen ja muihin kansainvälisiin rahoitusjärjestelmiin kohdistuviin uhkiin (Keith 2018, 245).

2 Varhaisista virtuaalivaluutoista kryptografiaan

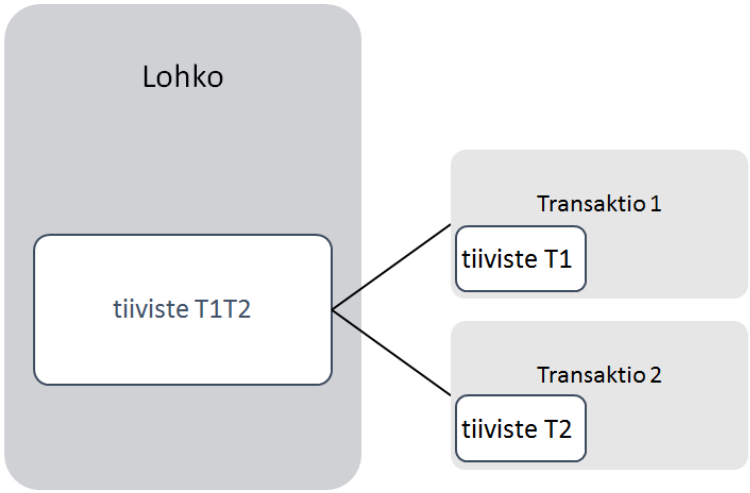
Bitcoin on nykypäivänä tunnetuin krypto-, digi- ja virtuaalivaluutta, muttei suinkaan ensimmäinen. Jo 1990-luvulta lähtien on syntynyt erilaisia virtuaalivaluuttoja, jotka ovat sittemmin lopetettu viranomaisten toimesta tai konkurssin seurauksena. Esimerkiksi E-gold oli virtuaalivaluutta, jonka arvo perustui kultaan. Kulta vaihtoi omistajaansa anonyymisti, mikä houkutteli myös rikollisia pesemään rahaa. Järjestelmän tietoturva oli heikko ja altis hakkeroinnille. Myöhemmin Yhdysvaltain viranomaiset syyttivät E-goldin johtoa rahanpesusta ja tämä johti lopulta varojen jäädyttämiseen ja liiketoiminnan lopettamiseen. Samoihin aikoihin on perustettu myös verkkokaupan maksuihin tarkoitettuja virtuaalirahoja, kuten Beenz ja Flooz, jotka kaatuivat viranomaisselvittelyihin ja uskottavuuden puutteeseen. (Miller 2015, 18-19.)

Nykyään lohkoketjuteknologian myötä erilaiset kryptovaluutat ovat yleistyneet ja tulleet lähes kaikkien tietoisuuteen. Internet on kehittynyt 90-luvulta tähän päivään ja taannut globaalin pääsyn valtavaan tietomäärään. Ihmisten teknisten taitojen kehittyminen ja kiinnostus teknologioihin sekä maailmanlaajuiset finanssikriisit ovat yksi syy kryptovaluuttojen yleistymiseen. Yksilön henkilökohtaista tietoa on helposti saatavilla internetissä ja identiteettivarkaudet ovat yleistyneet. Kryptovaluuttojen tarjoama anonyymi rahansiirto suoraan henkilöltä toiselle ilman tietoja pyytäviä ja säilyttäviä välikäsiä on siten houkutteleva vaihtoehto pankeille. Käsittelen lohkoketjuteknologiaa ja bitcoinin käyttäjäkuntaa seuraavissa luvuissa tarkemmin.

2.1 Blockchain- eli lohkoketjuteknologia

Lohkoketju on eräänlainen sähköinen, hajautettu tilikirja, josta näkee reaaliajassa kaikkien vertaisverkkoon yhdistyneiden käyttäjien transaktiot. Lohkoketjun ominaispiirteitä ovat muun muassa julkisuus, hajautuneisuus ja salaisuus. (Tapscott & Tapscott 2016, 6.) Julkiseksi lohkoketjun tekee se, että tilikirjan tapahtumat ovat näkyvissä kaikille käyttäjille, jotka ovat ladanneet avoimen lähdekoodin ohjelmiston koneelleen (Künnapas 2016, 113). Hajautetulla järjestelmällä tarkoitetaan keskitetyn tietokannan puuttumista ja sitä, että kaikki käyttäjät osallistuvat uusien lohkojen luomiseen. Lohkoketju on myös omalla tavallaan salainen; käyttäjillä on omat suojausavaimensa, jotka toimivat varmenteena. (Tapscott & Tapscott 2016, 6-7.) Drescherin (2016, 206) mukaan lohkoketju ei ole kuitenkaan täysin yksityinen, sillä kaikki käyttäjät saavat tietoa esimerkiksi rahansiirron määrästä, ajankohdasta ja tileistä, joiden välillä siirto tapahtuu.

Lohko koostuu koodista ja tapahtumista, kuten rahansiirrosta. Lohkon luomisessa on kyse algoritmista, jota kutsutaan tiivistefunktioksi. Tiivistefunktion avulla tuotetaan sekalainen merkkijono, joka liittyy osaksi lohkoketjua (Storås 2016). Kuvassa 1 on kuvattu yksinkertaistaen ketjun ensimmäisen lohkon rakenne. Ketjun seuraava lohko sisältää aina viittauksen edelliseen lohkoon. Transaktioilla on oma tiivisteensä (= hash), joista algoritmi laskee uuden merkkijonon. Laskentatapa on sama kaikilla käyttäjillä, ja tietystä datasta tulee tietynlainen merkkijono. (Storås 2016.) Lohkoketjulla on aikaleima (= time stamp), jonka avulla pystytään seuraamaan transaktioita reaaliajassa. Uusien lohkojen syntyminen näkyy kaikille vertaisverkon käyttäjille, ja pienikin muutos esimerkiksi edellisissä lohkoissa johtaa koko ketjun muutoksiin. (Drescher 2017, 141.) Siksi ketjua on vaikea mennä muuttamaan jälkikäteen rikkomatta sitä ja jäämättä kiinni.



Kuva 1. Yksinkertaistettu ensimmäisen lohkon rakenne (mukaillen Drescher 2017)

Lohkoketjuteknologia nojaa käyttäjiensä rehellisyyteen ja palkitsemisjärjestelmään. Uuden lohkon tuottaja voidaan palkita bitcoineilla (Miller 2015, 128) tai muulla kryptovaluutalla, ja riittää, että suurin osa käyttäjistä on rehellisiä ja korjaa esimerkiksi väärin muodostuneen lohkon. Kuitenkin esimerkiksi sähköisessä äänestyksessä voi olla mahdollista, että epärehelliset käyttäjät yrittävät muuttaa lohkoketjun rakennetta niin, että heillä on 51 % prosentin enemmistöomistus lohkoihin. Tällöin voidaan puhua keskitetystä vallasta. (Drescher 2017, 178, 209.)

2.2 Lohkoketjusovellukset ja mahdollisuudet

Lohkoketjua on kehuttu useassa tietotekniikan ja liike-elämän mediassa sen edistyksellisyydestä, vallankumouksellisuudesta ja mahdollisuuksista. On sanottu, että lohkoketju on yhtä mullistava keksintö kuin internet aikanaan. Lohkoketjuteknologialla on mahdollista uudistaa muun muassa pankki- ja finanssialaa, sopimuksia, omistusoikeuksia, tietoturvaa

ja yksityisyydensuojaa (Tapscott & Tapscott 2016, 51-52). Esimerkiksi älykkäiden sopimusten (= smart contracts) avulla voidaan automatisoida sopimusprosesseja siten, että tietty tapahtuma aktivoi toisen: kun tavara on saapunut vastaanottajalle, maksu tulee myyjän tilille (Lahti 2016).

Lohkoketjun ympärille on syntynyt uusia yrityksiä, jotka hyödyntävät teknologiaa eri tarkoituksiin. Kehitteillä on esimerkiksi musiikintoistopalvelu, joka näyttää avoimesti, mihin tai kenelle musiikista saadut korvaukset menevät, mikä lisää musiikkialan läpinäkyvyyttä (Lahti 2016). Erilaisia rekistereitä on kehitetty omistajuutta varten, kuten maa-, arvoesine- ja tuotteen alkuperään liittyviä rekistereitä. Näitä yhdistää tiedon luotettavuus, ajankohtaisuus ja läpinäkyvyys. Monet yritykset keskittyvät myös jakamistalouden, kuten kyytipalvelujen, asunnonvuokrauksen ja vakuutusten edistämiseen. Myös keinoja demokratian kehittämiseen on etsitty lohkoketjuteknologiasta. (Lahti 2016.)

Pankki- ja finanssimaailma nähdään vanhentuneena ja jähmeänä systeeminä (Tapscott & Tapscott 2016, 58), joka tarvitsisi uudistusta. Monet pankit ovat varoitelleet kryptovaluutoista ja yleinen suhtautuminen on ollut epäilevää, mutta jotkin toimijat ovat tulleet mukaan lohkoketjurintamaan. Pankki on tyypillisesti toiminut välikätenä tilisiirroissa, mutta lohkoketjun vertaisajattelun myötä niiden asema alkaa menettää merkitystään. Siksi niiden pitää keksiä uusia tapoja siirtää rahaa ja palvella asiakkaita. Ensi vuonna esimerkiksi arvopapereita ollaan digitalisoimassa Suomessa ja lukuisat pohjoismaiset pankit, kuten Nordea, OP ja Danske Bank ovat mukana yhteenliittymässä, jossa tutkitaan hajautettujen tilikirjojen hyödyntämistä finanssialalla (Leppänen 2018). Myös yhdysvaltalainen pörssi, Nasdaq on kutsunut kryptomarkkinoiden toimijoita keskustelemaan niiden roolista kansainvälisillä markkinoilla ja tavoitteesta saada laillinen ja säännelty asema (Verhage 2018).

2.3 Bitcoin

Bitcoinin alkutaival sijoittuu vuoden 2008 elokuuhun. Tuolloin Charles Bry, Neal King ja Vladimir Oksman jättivät patenttihakemuksen keksinnölleen, joka mahdollisti uudenlaisen sähköisten salausavainten päivittämisen ja jakamisen. Pian sen jälkeen rekisteröitiin verkkotunnus ”bitcoin.org”. Hieman myöhemmin samana vuonna nimimerkki Satoshi Nakamoto julkaisi artikkelin, joka kuvaili vertaisverkkoon perustuvaa maksujärjestelmää. (Miller 2015, 24.) Vuonna 2009 luotiin bitcoinin-lohkoketjun ensimmäiset lohkot (Fiorillo 2018). Myöhemmin on esitetty, että Nakamoto on pelkkä salanimi ja että nimen taustalla on useampi tekijä. (Miller 2015, 24.) Artikkelissaan Nakamoto (2008, 2) myös viittaa kirjoittajaan

persoonapronominilla ”we” eli me. Tämä vahvistaa käsitystä siitä, että tekijöitä on useampia.

Bitcoinin ydinajatus on maksaminen ilman välikäsiä, kuten pankkia. Rahansiirrot menevät suoraan käyttäjältä toiselle ilman, että henkilökohtaista tietoa jaetaan kolmannelle, valvovalle osapuolelle. Rahansiirtojen toimintaympäristönä on vertaisverkkosysteemi, jossa samassa verkossa olevat tietokoneet jakavat tietoa transaktioista toisilleen. Ainut tieto, jota yksittäisestä käyttäjästä annetaan, on hänen julkinen avaimensa (= public key). (Nakamoto 2008, 6.) Julkinen avain on generoitu koodi, joka toimii ikään kuin vastaanottajan tilinumerona. Käyttäjällä on myös oma yksityinen avaimensa (= private key), joka on ainoastaan hänen tiedossaan (Techopedia), ja jolla hän pääsee käsiksi kryptovaluuttoihinsa. Yksityisen ja julkisen avaimen yhdistelmällä voidaan sekä salata että purkaa viestejä, joita vertaisverkossa liikkuu.

Bitcoineja tuotetaan louhimalla (= mining), eli tuottamalla uusia lohkoja ketjuun. Louhinta tarkoittaa käytännössä matemaattista laskentaa, joka suoritetaan vertaisverkossa. Vertaisverkko koostuu useista tietokoneista, jotka ovat yhteydessä toisiinsa anonyymisti. Jokaisesta transaktiosta muodostetaan laskennan avulla tiivistefunktio, jonka muut verkossa toimivat yksittäiset laitteet, ”solmut” eli nodet varmistavat ketjuun sopivaksi. Jos funktio varmistetaan oikeaksi, siitä tulee osa ketjua ja sen tuottaja palkitaan bitcoineilla. Laskenta on monimutkaista ja vaatii tehokasta suorituskykyä. Keskimäärin joka kymmenes minuutti uusia lohkoja syntyy ja bitcoineja tulee lisää. (Miller 2015, 125-127.)

2.4 Virtuaalilompakko

Virtuaalilompakko on sovellus tai ohjelma, jossa säilytetään bitcoineja tai muuta virtuaalivaluuttaa. Käytännössä säilytys tarkoittaa käyttäjän yksityisten avainten säilytystä. Yksityisillä avaimilla varmennetaan bitcoin-transaktiot, jonka jälkeen bitcoineihin päästään käsiksi. Virtuaalilompakkoja on kolmenlaisia: tietokoneohjelmisto, joka asennetaan käyttäjän henkilökohtaiselle koneelle, mobiilisovellus puhelimessa ja pilvipalveluihin perustuva lompakko. Jokaisen käytössä on riskinsä, eikä esimerkiksi varastettuja tai kadotettuja bitcoineja voida palauttaa. (Miller 2015, 90-91.)

2.5 Bitcoinin arvo ja asema

Millerin (2015, 51-52) mukaan bitcoinin arvo muodostuu kysynnästä ja tarjonnasta sekä osittain sen rajallisesta määrästä. Bitcoinin rajallinen määrä, 21 miljoonaa, perustuu matemaattiseen koodiin. Kun 21 miljoonan rajapyykki täyttyy, ei bitcoineja pystytä louhimaan enempää. Siksi on sanottu, ettei inflaatio vaikuttaisi bitcoinin arvoon. Bitcoinin yksikkö voi

kuitenkin olla hyvinkin pieni ja sitä voidaan jakaa edelleen pienempiin yksiköihin lisäämällä nollia eteen. Tämä vaikuttaa bitcoinin todelliseen arvoon, joten Kingin (2014, 128) mukaan ei teknisesti ottaen voida sanoa, etteikö se olisi altis inflaatiolle tai deflaatiolle.

Bitcoin ei ole sidonnainen valuuttakursseihin, eikä mikään virallinen taho sääntele sen käyttöä tai vakautta (Verohallinto 2018). Se perustuu täysin osapuolten väliseen sopimukseen. Siksi sitä ei katsota esimerkiksi arvopaperiksi vaan käyttäjien väliseksi sopimussuhteeksi.

Suomessa Verohallinnon (2018) mukaan virtuaalivaluutoilla käyty kauppa muistuttaa luonteeltaan hinnanerosopimusten (= Contract for Difference, CFD) kauppaa. CFD-kaupan kohteena voivat olla osakkeet, raaka-aineet tai indeksit ilman, että sijoittaja varsinaisesti omistaa näitä. Voitot ja tappiot perustuvat kohdeinstrumentin myynti- ja ostohinnan välisiin erotuksiin. (Verohallinto 2016.) Bitcoin-kaupankäynnissä myyjä tai ostaja voi halutessaan asettaa rajahintoja kaupalle (Miller 2015, 86-87) ja tehdä voittoa tai tappiota hintaeroilla. Verohallinto (2018) Katsookin, että virtuaalivaluuttojen realisoitunut arvonnousu on veronalaista pääomatuloa, kun taas niiden arvonlasku ei ole tuloverotuksessa vähennyskelpoinen.

Bitcoinin arvon kehitys on ollut täynnä ylä- ja alamäkiä. Vielä vuonna 2009 yhdellä dollarilla sai 1 309,03 bitcoinia, eikä sillä pystynyt maksamaan mitään. Jo seuraavana vuonna bitcoineilla tehtiin maksu yksityishenkilöiden välillä ja bitcoinin käyttäjille luotiin oma markkinapaikkansa. 2011 yksi bitcoin maksoi yhden dollarin. Saman vuoden aikana se sai sekä positiivista että negatiivista huomiota, ja kaiken näkyvyyden siivittämänä kiinnostus kryptovaluuttoihin kasvoi. Vuoteen 2013 mennessä bitcoinin arvo oli kasvanut tuhanteen dollariin ja tähän mennessä korkeimmillaan arvo on käynyt melkein 20 000 dollarissa vuonna 2017. Tämän vuoden aikana bitcoinin arvo on heittelehtinyt noin 6 000 dollarin molemmin puolin. (Fiorillo 2018.)

2.6 Yksityisyys

Nykymaailmassa on lähes mahdotonta olla anonyymi. Ihmisestä kerätään henkilökohtaista tietoa syntymästä lähtien. Erilaiset instituutiot keräävät ja säilyttävät yksilön tietoja: sairaalat terveyshistoriaa ja rokotetietoja, poliisi sormenjälkiä, pankit tilitietoja ja kaupat ostotapahtumia. Erilaiset sovellukset keräävät käyttäjästään sijaintitietoja ja evästeiden avulla voidaan seurata, millä verkkosivuilla on vierailtu. Sosiaalisessa mediassa jaetaan kuvia, josta voidaan tunnistaa henkilöitä. Kaikesta jää jälki kyberavaruuteen.

Yleisesti ottaen luottamus dataa säilyttäviin viranomaisiin on ollut korkealla, mutta lisääntyvien kyberuhkien, kuten systeemien haavoittuvuuden ja tietomurtojen myötä pelko omien tietojen päätymisestä vääriin käsiin on aiheellisesti kasvanut. Identiteettivarkaudet ja petokset ovat nykyään yleisempiä Suomessa kuin asuntomurrot. Identiteettivarkauksista aiheutuu usein taloudellista vahinkoa, ja rikollisia on vaikea saada kiinni. (Yrittäjät 2018.) Voi siis sanoa, että yksilöllä on nykyään hyvin vähän valtaa omaan dataansa. Uudistuva GDPR-lainsäädäntö on kiinnittänyt huomiota tähän ongelmaan, muttei takaa, etteikö tietoja silti päätyisi vääriin käsiin.

Kryptovaluuttojen viehätys perustuu osittain siihen, että transaktioihin ei välttämättä tarvita kolmansia osapuolia ja maksu menee suoraan käyttäjältä toiselle. Tietoa ei siis tarvitse jakaa yhtään enempää kuin mitä bitcoin-siirto edellyttää. Kun kolmannelle osapuolelle ei tarvitse jakaa tietoa, riski identiteettivarkauksille pienenee. (Miller 2015, 63.) Siksi todennäköisesti yksityisyydestään kiinnostuneet ovat kiinnostuneita myös kryptovaluutoista.

Osa bitcoinin käyttäjistä saattaa olla kiinnostunut puhtaasti vain teknologiasta sen takana, osa sen tarjoamista sijoitusmahdollisuuksista ja osa on kaikkea sääntelyä vastaan. Libertaristit ovat Millerin (2015, 65) mukaan kiinnostuneita bitcoinista siksi, ettei sitä säätele mikään valtio tai keskuspankki, vaan se perustuu puhtaasti kysynnän ja tarjonnan lakiin. Myös tavalliset kuluttajat ovat kiinnostuneet bitcoinista, sillä monet palveluntarjoajat ovat alkaneet hyväksyä maksuvälineenään kryptovaluuttoja. Tässä mielessä bitcoin on maksuväline siinä missä muutkin (Miller 2015, 67). Virtuaalikolikon kääntöpuolena on sitten toisaalta rikolliset käyttäjät, jotka ovat valjastaneet bitcoinin laittomiin käyttötarkoituksiin.

2.7 Rikollisuus

Bitcoinin suosio ja sen takaama anonymiteetti on herättänyt huolta lainsäätäjissä ja pankeissa. Erityisesti rikollisen toiminnan rahoittaminen on noussut suurimmiksi huolenaiheiksi. Foley, Karlsen & Putniņš (2018) väittävät tutkimuksessaan, että alkuvuodesta 2018 lähestulkoon puolet bitcoin-transaktioista liittyi rikolliseen toimintaan. Rikollisella toiminnalla tässä yhteydessä tarkoitetaan esimerkiksi huumekauppaa, verkkorikoksia kuten tietomurtoja ja hakkerointia, laitonta pornokauppaa, rahanpesua ja terrorismin rahoittamista. Bitcoineja väitetään käytetyn myös palkkamurhien maksuvälineenä (Foley ym. 2018). Pääosin rikollista toimintaa harjoitetaan pimeässä tai anonyymissä verkossa (= dark web). Pimeä verkko toimii internetin sisällä, mutta sinne ei pääse tavanomaisia reittejä. Tunnetuin pimeä verkko on Tor-verkko, jossa käyttäjät pystyvät anonyymiuden turvin käymään esimerkiksi keskustelufoorumeilla laitonta kauppaa keskenään ilman välikäsiä. (Viestintävirasto 2016.)

Verkon palvelimet tarvitsevat ylläpitoa toimiakseen normaalisti. Tätä varten on erilaisia palveluntarjoajia, jotka toimivat datakeskuksena palvelimille. Palveluntarjoajat voivat valvoa, mitä palvelimilla tapahtuu ja tarvittaessa sulkea ne. (Norton.) Myös pimeän verkon palvelimet tarvitsevat ylläpitoa, ja markkinoille onkin tullut niin kutsuttuja bulletproof hosting -palveluja (Viestintävirasto 2016). Bulletproof hosting -yritykset eivät valvo palvelinten sisältöä tai käyttötarkoitusta (Norton), eivätkä ne tiedä tai paljasta asiakkaistaan mitään (Viestintävirasto 2016). Ne toisin sanoen toimivat alustana mille tahansa toiminnalle sitä kyseenalaistamatta ja siihen puuttumatta. Lainsäädäntö on joissakin maissa niin puutteellista, etteivät viranomaiset pysty puuttumaan tällaiseen toimintaan (Norton).

Kryptovaluutat näyttelevät suurta roolia pimeän verkon maksutapahtumissa niiden anonyymin luonteen vuoksi. Kryptovaluutoilla voidaan maksaa sekä suoraan käyttäjältä toiselle että bulletproof hosting -yrityksille palveluista. Kryptovaluutat ovat helpottaneet rikollisten toimintaa pimeissä verkoissa (Foley ym. 2018). Kuitenkin esimerkiksi bitcoin alkaa menettää merkitystään rikollisen toiminnan rahoittajana: sen käyttö yleistyy jatkuvasti tavallisten ihmisten keskuudessa, sen arvo on hankalasti ennustettavissa ja rinnalle syntyy jatkuvasti uusia, eri tavalla toimivia kryptovaluuttoja, jotka ovat mahdollisesti vielä hankalampia jäljittää. (Foley ym. 2018.)

2.7.1 Vaalivaikuttaminen ja hybridisodankäynti

Hybridiuhkien osaamiskeskuksen mukaan hybridiuhista on tullut pysyvä osa turvallisuusympäristöämme. Nykyajan digitaalisen kehityksen myötä hybridiuhat myös todennäköisesti lisääntyvät (Hybrid CoE). Toimijat voivat olla valtiollisia tai muita tahoja, kuten aktivisteja ja verkkorikollisia (Nortio 2017). Hybridiuhkiin sisältyy monenlaista toimintaa, joka perustuu kohteen heikkouksiin.

Hyökkäyksissä voidaan erottaa kaksi vaihetta: valmisteluvaihe ja toimintavaihe. Valmisteluvaiheessa kohdetta tarkkaillaan ja tehdään hienovaraisia vaikuttamistoimenpiteitä. (Hybrid CoE.) Näitä voivat olla esimerkiksi kalasteluviestit, joita lähetetään yrityksille ja organisaatioille. Halutessaan rikolliset voivat sitten käynnistää laajemman hyökkäyksen, jota voi olla vaikea jäljittää, mutta jonka vaikutukset ovat kohteelle haitalliset (Hybrid CoE).

Brexit-äänestyksen aikoihin venäläisiltä Twitter-tileiltä lähetettiin 45 000 viestiä, jotka liittyivät Brexitiin. Tilit, jotka olivat aikaisemmin keskittyneet esimerkiksi Ukrainan konfliktiin, käänsivät huomion Brexit-keskusteluun juuri ennen äänestyksiä. Suurin osa viesteistä oli

Brexit-myönteisiä, mutta joukossa oli myös mielipiteitä ja uutisia Brexitiä vastaan. Tavoitteena oli lietsoa erimielisyyksiä ja vaikuttaa kansanäänestykseen. (Mostrous, Bridge & Gibbons 2017.) Hybridisodankäynti on monimutkaista ja vaatii runsaasti resursseja. Eri toimijat pyrkivät siihen, ettei hyökkääjän alkuperää tunneta.

2.7.2 Yhdysvaltain presidentinvaalit 2016

Useita venäläisiä tiedustelupalvelun työntekijöitä syytetään muun muassa demokraattien kansallisen komitean tietoverkon hakkeroimisesta, salasanojen ja asiakirjojen varastamisesta (Katz 2018). Tällä uskotaan olevan vaikutusta vuoden 2016 Yhdysvaltain presidentinvaalien tulokseen. Jo vuonna 2014 alkanut sekaantuminen edisti Donald Trumpin vaalikampanjaa ja laski Hillary Clintonin kannatusta (Öhrnberg 2018). Kyberhyökkäyksessä oli hyödynnetty muiden kryptovaluuttojen lisäksi Bitcoinia. Kryptovaluutoilla ostettiin palvelimia ja servereitä ja muita hakkeroimiseen tarvittavia instrumentteja. Erilaisten virtuaalirahansiirtojen ja anonymiteetin turvin heidän onnistui pestä yli 95 000:n dollarin arvosta rahaa. (Katz 2018.)

2.8 Hajautettu tietokanta ja demokratia

Lohkoketjuteknologiaa on kehuttu sen demokraattisesta, vertaisverkkoon perustuvasta rakenteesta ja keskitetyn vallan ja valvonnan puuttumisesta. Varsinkin alkuaikoina jokainen pystyi osallistumaan esimerkiksi bitcoinien louhintaan saaden reilun palkkion toiminnastaan (Tapscott & Tapscott 2016, 36). Palkkiot ajavat vertaisverkon käyttäjiä keskinäiseen kilpailuun siitä, kuka saa ensin ratkaistua matemaattisen kaavan ja siten lisättyä uuden lohkon. Kilpailu kovenee ja palkkiot vähenevät, mitä enemmän käyttäjiä on ja dataa luodaan. Algoritmien pyörittäminen vaatii tietokoneelta valtavasti suorituskykyä, mikä lisää ammattimaisten yhteistyöryhmittymien määrää. (Miller 2015, 129.) Voidaankin pohtia, onko tässä mielessä kyse enää tasavertaisuudesta, jos suorituskyky keskittyy tietyille ryhmille, joilla on tarpeeksi varallisuutta hankkia tehokkaita koneita kerryttämään lisää varallisuutta.

Lähivuosina käydyt tärkeät vaalit ja kansanäänestykset ovat herättäneet kysymyksiä äänestysjärjestelmien ja jopa demokratian toimivuudesta. Muun muassa Yhdysvaltojen presidentinvaalit, Brexit-äänestys ja monet muut poliittisesti tärkeät tapahtumat ovat olleet epäilyjen kohteena. Venäjää on epäilty kahdessa ensimmäisessä vaikutusyrityksistä. Gabbatin (2018) mukaan USA:n välivaaleissa Georgian osavaltiossa republikaanien ehdokas Brian Kemp toimi myös ministerinä, joka hallinnoi äänestysjärjestelmää. Äänestysjärjestelmässä havaittiin vika, joka mahdollisti pääsyn äänestäjien tietoihin ja äänten manipuloinnin. Kemp syytti demokraatteja hakkerointiyrityksistä. Äänten laskennat ovat vielä

kesken ja syytöksiä satelee puolin ja toisin. Tämänkaltaiset tapahtumat saavat aikaan huolta äänestysjärjestelmien ja -valvojien riippumattomuudesta ja luotettavuudesta.

Yhdeksi ratkaisuksi äänestyksien luotettavuuden takaamiseksi on ehdotettu lohkoketjua. Etuna siinä on, ettei tietoja voi muuttaa, vaan systeemi tunnistaa pelkästään matemaattisesti (Storås 2016), jos esimerkiksi ääniä yritettäisiin manipuloida jälkikäteen. Ymmärtääkseni jokainen ääni olisi käytännössä sähköisessä järjestelmässä oleva tiedosto, jolla on oma tunnisteensa. Tiedoston sisältöä muutettaessa myös tunniste muuttuu, jolloin ketju hajoaa ja yritys paljastuu. Storåsin (2016) mukaan lohkoketjua hyödyntävässä sähköisessä järjestelmässä jokainen ääni olisi myös kaikkien nähtävillä heti, kun se on annettu, eikä sitä enää pysty muuttamaan jäämättä kiinni. Euroopassa on kehitteillä projekti D-Cent, joka pyrkii suoran demokratian edistämiseen juuri lohkoketjuteknologian avulla (Lahti 2016).

3 Rahanpesun ja terrorismin rahoittamisen estäminen

Rikoslain 32 luvun 6 § (4.3.2011/191) mukaan rahanpesu on

1. rikoksella hankitun omaisuuden tai hyödyn hallussapitoa, käyttämistä, välitystä, siirtämistä tai muuntamista tai
2. rikoksella hankitun omaisuuden tai hyödyn peittämistä tai häivyttämistä ja tällaisessa toiminnassa avustamista.

Terrorismin rahoittaminen on mainittu rahanpesun yhteydessä. Terrorismin rahoittamisella tarkoitetaan joko suoraa tai välillistä ja tietoista varojen keräämistä tai antamista terroristisiin tarkoituksiin. (Rikoslaki 34a luku 5 § 24.1.2003/17)
Rahanpesussa tarkastelun kohteeksi joutuu varojen alkuperän laillisuus, kun taas terrorismin rahoittamiseen liittyvässä epäilyssä tutkitaan varojen käyttötarkoitusta (Finanssivalvonta 2015a).

Rahanpesulainsäädäntöä kehitettiin alun perin kitkemään huumekauppaa, joka oli 1900-luvun alkupuoliskolta maailmansotien jälkeiseen aikaan räjähtänyt käsiin. Uudenlaisten huumeiden saatavuus ja laajat ongelmat väärinkäytössä ja riippuvuuksissa pakottivat käsittelemään asiaa maailmanlaajuisesti. (Keith 2018, 245-246.) Ensimmäiset AML-säädökset keskittyivät estämään nimenomaan huumekartellien varojen käsittelemistä. Myöhemmin Wienin yleissopimuksessa vuonna 1988 huomio siirtyi toisaalle, kun 43 maata alkoi keskittyä pelkän huumekaupan valvomisen sijaan rahanpesuun. (Keith 2018, 245.) Rahanpesu on nykypäivänäkin laaja-alainen ja monimutkainen ongelma, eikä se koske pelkästään huumekauppaa, vaan myös ihmiskauppaa, prostituutiota, petoksia, veronkiertoa ja terrorismin rahoittamista (Keith 2018, 271).

Terrorismin rahoittamiseen havahduttiin 2000-luvun alkupuolella 9/11-hyökkäysten myötä, ja maailmanlaajuisiin suosituksiin lisättiin terrorismin rahoittamisen kriminalisointi (Keith 2018, 249). Suosituksissa, joita suurin osa maailman maista noudattaa, mainita myös terroristien varojen jäädyttäminen, epäilyttävän toiminnan raportointi viranomaisille ja voittoa tavoittelemattomien yhdistysten valvonta. Voittoa tavoittelemattomat yhdistykset ja hyväntekeväisyysjärjestöt eivät usein kuulu AML-lainsäädännön piiriin, joten riskinä on, että ne hyväksikäyttävät asemaansa rikollisiin tarkoituksiin (Keith 2018, 249, 274).

Rahanpesuprosessi on jaettu kolmeen vaiheeseen: sijoitusvaihe, harhautusvaihe ja palautusvaihe (Keskusrikospoliisi, rahanpesun selvittelykeskus 2012, 6). Sijoitusvaiheessa rikollisesta toiminnasta saatu laiton raha pyritään siirtämään laillisen talouden piiriin esimerkiksi pankkitalletuksella tai maasta toiseen siirtämällä. Sijoitusvaihe on rikollisen kannalta

riskialtteinta ja kiinnijäämisen todennäköisyys on suuri (Keith 2018, 249). Harhautusvaiheessa pyritään peittämään lailliseen järjestelmään siirretty raha ja henkilön identiteetti. Usein tätä varten perustetaan yhtiö, joka sijaitsee veroparatiisimaassa. Lopuksi palautusvaiheessa palautuvat rikoksentekijälle, sillä ne on saatu harhauttamalla näyttämään laillisella tulolta (KRP, rahanpesun selvittelykeskus 2012, 6). Palautusvaihe sisältää usein lainojen antamista perustetun yhtiön tyttärille tai esimerkiksi kiinteistöjen ostamista (Keith 2018, 250).

Keithin (2018, 275) mukaan rahanpesulainsäädäntö on kehittynyt reaktiivisesta proaktiivisempaan suuntaan. Lainsäädäntö ja viranomaiset ovat siis ottaneet ennaltaehkäisevän ja aikaisen vaiheen lähestymistavan rahanpesun ja terrorismin rahoittamisen estämiseen. Kehittämällä lainsäädäntöä, luomalla sääntelyä ja kynnyksiä sekä parantamalla raportointijärjestelmiä voidaan rikolliset saada jo sijoitusvaiheessa kiinni (Keith 2018, 275).

3.1 Suomen rahanpesulainsäädäntö

Rahanpesulainsäädäntö ulottuu Suomessa muun muassa vakuutusyhtiöihin, rahastoyhtiöihin, sijoituspalveluihin, rahapeliyhtiöihin, tilintarkastusyhtiöihin, pankkeihin ja asianajotoimistoihin (laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017 1 luvun 2 §). Toisin sanoen lakia sovelletaan sellaisiin toimijoihin, jotka jollain tavalla käsittelevät varoja. Rahanpesulakia ei kuitenkaan sovelleta esimerkiksi peliautomaatteihin, oikeudenkäyntiapuun tai -neuvontaan eikä tapauksissa, joissa toiminta on vähäistä ja sivutoimista (Rahanpesulaki 444/2017 1 luvun 3 §).

Suomen rahanpesulainsäädäntöä kehittää sisäministeriö ja valtiovarainministeriö. Keskusrikospoliisin yhteydessä toimii rahanpesun selvittelykeskus, joka käsittelee ilmoitukset kyseenalaisista liiketoimista liittyen rahanpesuun ja terrorismin rahoittamiseen. (Finanssivalvonta 2015a) Finanssivalvonta taas on suomalainen rahoitus- ja vakuutusvalvontaviranomainen, jonka tehtävä on valvoa rahalaitoksia, kuten pankkeja, sijoituspalveluyrityksiä ja vakuutus- ja eläkeyhtiöitä (Finanssivalvonta 2018). Viimeaikaisten Euroopassa sattuneiden rahanpesutapausten myötä Finanssivalvonta aikoo lisätä resursseja valvontaan Suomessa. Valvonta näkyy siten, että pankin kysyvät nykyistä tarkemmin esimerkiksi ulkomaisen rahan alkuperästä. (Lehto 2018.)

3.2 Kansainväliset standardit

Kansainväliset standardit vaikuttavat rahanpesun ja terrorismin rahoittamisen estämisen keinoihin. Sääntelyn avulla pyritään globaaleihin pelisääntöihin asiakkaan tuntemista koskevissa asioissa. FATF eli Financial Action Task Force on Money Laundering on OECD:n

alaisuudessa toimiva ja hallitusten välinen rahanpesun ja terrorismin rahoittamisen vastainen yhteenliittymä, joka antaa suosituksia valtioille. EU-direktiivit perustuvat näihin suosituksiin. (Finanssivalvonta 2015a.)

FATF julkaisee raportteja, joissa esitetään globaalin talouden uhkia erityisesti rahanpesun ja terrorismin rahoittamisen kannalta. Tällä hetkellä FATF (2018b) on julkisessa lausunnossaan todennut, että Pohjois-Korea ja Iran ovat jatkuvassa tarkkailussa lainsäädännöllisten puutteidensa ja laittomuuksiensa vuoksi. Pohjois-Korea kuuluu korkean riskin maihin muun muassa sen joukkotuhoaseiden laittoman rahoituksen ja valmistamisen takia. Iran ei taas ole pystynyt säätämään riittäviä terrorismin rahoittamisen estämiseen tähtääviä lakeja (FATF 2018b.) YK ja EU asettavat finanssipakotteita maille, jotka osallistuvat terroritekoihin tai niiden edistämiseen (Finanssivalvonta 2015a.) Kansainvälisistä standardeista huolimatta EU:lla ei ole yhtenäistä rahanpesuviranomaista, vaan valvonta on kansallisten viranomaisten vastuulla (Boxberg 2016,10).

3.3 AMLD 5: Uusi rahanpesudirektiivi

EU:n rahanpesudirektiiviä uudistetaan säännöllisesti ja melko tiuhaan tahtiin, jotta lainsäädäntö voisi vastata alati monimutkaistuviin teknologioihin, transaktioihin ja rahoitusjärjestelyihin. Neljäs rahanpesudirektiivi julkaistiin vuonna 2015, mutta pian sen jälkeen vuonna 2016 Euroopan komissio ehdotti siihen parannuksia ja lisäyksiä. Komissio katsoi, että lisäykset ovat tarpeen alkuvuodesta 2016 tapahtuneiden terrori-iskujen ja myöhemmin julkaistujen Panaman papereiden takia. (Krais 2018.) Panamalaisen lakiyhtiön Mossack Fonsecan kaksi edustajaa pidätettiin rahanpesusta epäiltynä viime vuonna. Yhtiöstä varastettiin ja vuodettiin dokumentteja, jotka paljastivat yhtiön osallistuneen epäilyttävästä alkuperästä olevien varojen piilottamiseen ja veroparatiisitilien ylläpitämiseen. (Räisänen 2017.)

Viidennessä rahanpesudirektiivissä valvonta ja tunnistus on laajennettu koskemaan virtuaalivaluuttoja-alustoja sekä virtuaalilompakkopalveluja. Viides direktiivi tuli voimaan 9.7.2018 ja jäsenvaltiot ovat velvoitettuja ottamaan lait käyttöön alkuvuonna 2020. (Krais 2018.) Kansallisille rahanpesun selvittelykeskuksille (= FIU, Financial Intelligence Unit) annetaan laajemmat valtuudet ja yhteistyötä ja tiedonantoa eri viranomaisten välillä parannetaan. Rahanpesun selvittelykeskukset voivat jatkossa saada helpommin tietoa esimerkiksi sähköisen rahan käyttäjistä ja prepaid-tileistä. (Krais 2018.)

Entistä tarkempaa huomiota kiinnitetään myös poliittisesti vaikutusvaltaisten henkilöiden (= politically exposed person, PEP) osallisuuteen ja tunnistamiseen. Poliittisesti vaikutusvaltaiset henkilöt on mainittu siksi, että heidän valta-asemaansa voidaan käyttää hyväksi rahanpesutarkoituksissa tai muussa rikollisessa toiminnassa (FATF 2013, 3). PEP:ksi katsotaan henkilöt, jolla on merkittävä julkinen rooli, kuten muun muassa poliittiset johtajat ja päättäjät, puolustusvoimien johtajat, valtion omistamien yritysten johtajat ja kansainvälisten organisaatioiden hallitusten jäsenet sekä näiden henkilöiden lähipiiri (FATF 2013, 4-5).

EU:n jäsenmaat velvoitetaan luomaan kansallinen rekisteri virastoista ja julkisyhteisöistä, jotka luokitellaan poliittisesti vaikutusvaltaisiksi. Myös kansainväliset, mutta kansallisesti rekisteröidyt yhdistykset ja organisaatiot kuuluvat näihin. (Krais 2018.) EU luo vastaavasti EU-tason listan ja lopuksi yhdistää jäsenmaiden listat yhdeksi, julkiseksi rekisteriksi. Yksittäisten henkilöiden nimiä ei ole kuitenkaan listattu (Krais 2018), vaan rahoituslaitosten ja muiden raportoimisvelvollisten tulee harjoittaa riskiperusteista arviointia, jossa määritetään, onko henkilö PEP vai ei (FATF 2013, 14).

FATF (2018c) on todennut, että virtuaalivaluutat ovat riski rahanpesun ja terrorismin rahoittamisen kannalta, ja kehottaa eri maita tekemään tiiviimpää yhteistyötä rahanpesun kitkemiseksi. Viranomaiset ja yksityinen sektori eivät tunnu olevan perillä siitä, miten ja mihin toimintaan lakeja sovelletaan. FATF onkin päivittänyt suosituksensa ja sanastonsa ajan tasalle. Tämä tarkoittaa käytännössä sitä, että yritysten ja viranomaisten on aina käytettävä riskiperusteista arviointia työskennellessään virtuaalivaluuttojen palveluntarjoajien kanssa. Toimintaan liittyviä riskejä pitää jatkuvasti arvioida ja tunnistaa, ja epäilyttävästä toiminnasta täytyy raportoida eteenpäin. Lain soveltamisessa on kuitenkin tulkinnanvaraisuutta; viranomaisilla on valta päättää, minkälaisena instituutiona kutakin virtuaalivaluuttojen palveluntarjoajaa kohdellaan ja miten rahanpesulainsäädäntöä niihin sovelletaan. Päivitetyssä suosituksessa kehotetaan maita rekisteröimään ja/tai lisensioimaan virtuaalivaluuttojen palveluntarjoajat, jotta niitä voidaan tehokkaammin valvoa (FATF 2018a, 15).

Suomessa lompakkopalveluita, sijoitusneuvontaa ja valuutanvaihtopalveluita tarjoaa muun muassa Prasos Oy. Yrityksen Coinmotion-palvelussa voi ostaa, myydä, tallettaa ja säilyttää virtuaalivaluuttoja (Prasos 2018). Heidän käyttöehdoissaan mainitaan AML-laki, jota he ”suurelta osin noudattavat”. Yhtiö siis kertoo tunnistavansa asiakkaan ja vaativansa tältä kattavia tietoja. Käytännössä AML-lain noudattaminen näkyy tilisiirtojen kestossa. Prasoksen mukaan siirroissa voi kestää useita tunteja tai ne voidaan hylätä kokonaan, mikäli niissä havaitaan ”AML-lain mukaisia riskejä”. Prasos käyttää asiakkaan tunnistamisessa eli KYC-prosessissa ulkopuolista palveluntarjoajaa. ISignthis-niminen yritys on erikoistunut sähköiseen asiakkaan tunnistamiseen ja maksujen varmentamiseen. Asiakas

tunnistetaan maksukortin perusteella ja transaktioita pystytään valvomaan osana riskienhallintaa (iSignthis).

3.4 Tosiasiallinen edunsaaja

Tosiasiallisella edunsaajalla tarkoitetaan luonnollista henkilöä, joka omistaa suoraan tai välillisesti yli 25 prosenttia yrityksen osakkeista tai muilla tavoin vastaavan osuuden yrityksestä. Tosiasialliseksi edunsaajaksi lasketaan myös henkilö, jolle on määritelty esimerkiksi yhtiöjärjestyksessä yli 25 prosentin osuus yrityksen äänioikeuksista. (Rahanpesulaki 444/2017 1 luvun 5 §.) Pankkien ja muiden ilmoitusvelvollisten tulee aina tunnistaa ja ylläpitää asiakkaan todelliseen edunsaajaan liittyviä tietoja ja todentaa näiden henkilöllisyys. Poikkeuksena ovat yhtiöt, joiden arvopaperi on julkisen kaupankäynnin kohteena Suomessa tai Euroopan talousalueen maassa (Mäntylä 2017). Jos taas yksittäistä tosiasiallista edunsaajaa ei pystytä tunnistamaan tai ehdot eivät täyty, yrityksen hallitus, toimitusjohtaja, vastuunalaiset yhtiömiehet tai vastaavan aseman henkilö katsotaan tosiasiallisiksi edunsaajiksi (rahanpesulaki 444/2017 1 luvun 5 §).

Suomessa yritysten, joita rahanpesulait koskevat, on ilmoitettava tosiasialliset edunsaajansa ja näiden tiedot Patentti- ja rekisterihallituksen rekisteriin viimeistään vuonna 2019. Viranomaisilla ei ole kuitenkaan velvollisuutta tarkistaa tietojen paikkansapitävyyttä, vaan vastuu oikeasta tiedosta on yrityksillä ja ilmoitusvelvollisilla. Tämä tarkoittaa käytännössä sitä, että esimerkiksi pankin on aina tarkistettava asiakkaaltaan, ovatko tiedot oikeita ja ajan tasalla. (Castrén & Snellman 2016.)

Tosiasiallisen edunsaajan tunnistaminen on osa riskienhallintaa. Kun tiedetään, miksi asiakas vaatii tiettyjä palveluita ja ketä palvelut loppujen lopuksi hyödyttävät, voidaan paremmin arvioida, onko riski rahanpesuun tai terrorismin rahoittamiseen olemassa. Suomessa riskejä liittyy esimerkiksi kiinteistösijoituksin, käteisen siirtoon ja pöytälaatikkoyrityksiin (Castrén & Snellman 2016). Luonnollinen henkilö voi esimerkiksi yrittää kiertää veroja perustamalla pöytälaatikkoyrityksen, jonka nimissä rahansiirrot tai -talletukset tehdään.

3.5 EU:n laajuinen rahanpesuvalvonta?

Vakavat rahanpesuepäilyt eivät katso välttämättä pankin kokoa tai asemaa kansainvälisillä markkinoilla. Tämä käy ilmi Danske Bankin hiljattain tapahtuneesta rahanpesuskandaalista. Danske Bankin suhteellisen pienen Virossa sijaitsevan sivuliikkeen kautta virtasi miljardeja venäläistä alkuperää olevaa rahaa, ja epäillään, että osaa rahoista on kierrätetty pankissa ainoastaan rahanpesutarkoituksessa (Boxberg 2018, 10). Euroopassa on

herätty aiheen vakavuuteen ja toiveissa on EU:n laajuinen valvontaviranomainen, joka valvoisi jäsenmaita samaan tapaan kuin Euroopan keskuspankki pankkeja (Lehto 2018).

Tällä hetkellä FATF:n suosituksissa ei ole mainintaa keskitetystä viranomaisesta, joka Euroopan keskuspankin lailla valvoisi EU:n jäsenmaiden rahanpesulainsäädäntöä ja toimeenpanoa. FATF (2018a, 25) kuitenkin kehottaa suosituksessaan kaikkia maita tekemään tiivistä yhteistyötä ja käyttämään tarvittaessa keskinäistä rikosoikeusapua. Keskinäinen rikosoikeusapu voi olla todisteiden hankkimista esitutkintaa ja oikeudenkäyntiä varten ja oikeudenkäyntiasiakirjojen tiedoksiantoa, jotka edellyttävät oikeusapupyyntöä toiselta valtiolta (oikeusministeriö).

4 Danske Bankin rahanpesuskandaali

Tapaustutkimukseni kohteena on Danske Bankin (= Danske) Viron osaston rahanpesuskandaali. Dansken Virossa sijaitsevan sivuliikkeen kautta virtasi miljardeja venäläistä alkuperää olevaa rahaa, ja epäillään, että osaa rahoista on kierrätetty pankissa ainoastaan rahanpesutarkoituksessa. Käytän aineistona tanskalaisen lakitoimisto Bruun & Hjejlen tänä syksynä laatimaa raporttia, jossa selvitetään tapauksen taustoja ja kerrotaan tarkemmin asiakasportfoliosta, johon kuuluu asiakkaita Viron ulkopuolelta ja joka on suljettu vuonna 2016. Tutkin, esiintyykö raportissa mahdollisia yhteyksiä kryptovaluuttoihin ja mitkä tekijät johtivat epäonnistumiseen valvonnassa. Nostan esiin muutaman olennaisen osatekijän ja liitän ne osaksi laajempaa kokonaisuutta.

Finanssivalvonta (2015b) korostaa rahanpesun ja terrorismin rahoittamisen estämisen riskiperusteista arviointia: valvottavien, eli tässä tapauksessa pankkien tulee kehittää riittävät menetelmät riskienhallintaan ja arviointiin. Riskejä arvioitaessa täytyy huomioida toimialaan, tuotteisiin, palveluihin, teknologian kehitykseen, asiakkaisiin ja niiden toiminnan luonteeseen liittyviin riskeihin. Valvottavalla täytyy olla sisäiset ohjeet ja prosessit asiakkaan tuntemisesta ja rahanpesusta ja terrorismin rahoittamisen estämisestä ja sen täytyy pystyä osoittamaan valvojalle, että riskienhallintamenetelmät ovat riittävällä tasolla. Riskiarvioita on myös jatkuvasti päivitettävä ajan tasalle (rahanpesulaki 444/2017 2 luvun 3 §).

AML-lainsäädännössä on yleiset, kaikkia valvottavia koskevat ohjeet ja velvollisuudet asiakkaan tuntemisesta ja riskienhallinnasta, mutta arviointi täytyy tehdä aina tapaus- ja asiakaskohtaisesti. Täytyy siis arvioida, synnyttääkö asiakas itsessään riskejä, vai onko esimerkiksi asiakkaan yksittäisessä toiminnossa jotain epäilyksiä herättävää. Finanssivalvonnan (2015b) mukaan valvottavan yrityksen henkilöstöä täytyy jatkuvasti kouluttaa ja työyhteisöön täytyy nimittää yhteyshenkilö, joka on yhteydessä valvontaviranomaisiin, jos epäillään epätavallisia liiketoimia.

Käyn raportin läpi riskien näkökulmasta: mitä riskejä Dansken toimintaan on liittynyt ja miten niihin on reagoitu. Etsin avainsanoja, jotka kuvaavat riskitekijöitä, niihin vastaamista ja lopputulosta.

Raportin (Bruun & Hjejle 2018, 3) mukaan Danskella ei ollut konsernitasolla riittävää tietoa sen Viron osaston toiminnasta. Viron osaston valvonta ja johdon toiminta oli puutteellista ja tilanne kesti pitkään Viron ja Tanskan valvontaviranomaisten varoituksista ja selvityspyynnöistä huolimatta. Pääosin epäilyjen kohteena on osaston ulkomaisten asiakkaiden

asiakasportfolio. (Bruun & Hjejle 2018, 7-8.) Portfoliossa oli asiakkaita muun muassa Venäjältä, Tanskasta, Suomesta, Virosta sekä CIS- ja veroparatiisimaista. Joitakin virolaisia oli portfoliossa mukana siksi, että niillä oli toimintaa myös ulkomailla. CIS-mailla tarkoitetaan itsenäisten valtioiden yhteisöä (= The Commonwealth of Independent States), johon kuuluu valtioita entisestä Neuvostoliitosta (Worldatlas 2018). Veroparatiisimaat, kuten Brittiläiset Neitsytsaaret, ovat alhaisen verotason maita, joita suojelee usein muun muassa tiukat pankkisalaisuudet ja lait, jotka mahdollistavat todellisten omistajien salaamisen (Finnwatch).

Dansken Viron yksikkö oli osa suomalaista Sampo Pankkia vielä 2000-luvun alussa, kunnes Danske osti pankin vuonna 2007. Ulkomaisten asiakkaiden portfolio oli olemassa jo suomalaisomisteisessa pankissa ja se siirtyi yritysoston myötä Danskelle. (Bruun & Hjejle 2018, 5.) Viron yksiköllä oli omat IT-järjestelmänsä, joita ei oltu integroitu konsernin järjestelmiin. Asiakastiedot, tilisiirrot ja riskien valvonta eivät siten olleet samalla tasolla konsernin kanssa, eikä konsernin johdolla ollut kunnollista pääsyä yksikön järjestelmiin (Bruun & Hjejle 2018, 3.) Raportissa tarkastellaan Viron yksikön ja Dansken konsernin toimintaa yritysoston alusta vuoteen 2016, jolloin ulkomaisten asiakkaiden portfolio suljettiin.

4.1 Ulkomaisten asiakkaiden portfolio

Raportin keskiössä on asiakasportfolio, johon kuului asiakkaita muun muassa Viron ulkopuolelta. Osa portfolion asiakkaista oli virolaisia, mutta niillä oli toimintaa tai niiden tosiasiallinen edunsaaja sijaitsi ulkomailla. Viron yksiköstä tuli suomalaisen Sampo Pankin tytäryhtiö vuonna 2000, kun Sampo Pankki osti sen Viron keskuspankilta (Lassila 2018). Asiakasportfolio oli perustettu jo 90-luvulla ja se siirtyi yritysoston myötä Sampo Pankille. Vuonna 2007 Danske Bank osti Sampo Pankin, ja vuotta myöhemmin myös Viron yksiköstä tuli osa Dansken konsernia (Bruun & Hjejle 2018, 5.) Ulkomaisten asiakkaiden portfolio suljettiin vuonna 2015 ja osa tileistä vasta alkuvuodesta 2016 (Bruun & Hjejle 2018, 15).

Vuoteen 2013 mennessä 44 prosenttia Viron yhtiön ulkomaisten asiakkaiden portfolion talletuksista tuli ulkomailta, kun vuonna 2007 prosenttiosuus oli 27. Vain yhdeksän prosenttia ulkomaisten asiakkaiden portfolion talletuksista tuli virolaisilta asiakkailta. Portfolioon kuuluvien asiakkaiden määrä on vaihdellut, mutta arviolta 10 000 asiakkuutta kuului portfolioon vuoteen 2015 mennessä. Yksiköllä oli kuitenkin myös ulkomaisia asiakkaita, jotka eivät kuuluneet ulkomaisten asiakkaiden portfolioon, mutta niiden luonteen ja sijainnin vuoksi tulivat osaksi tutkintaa. Yhteensä tutkinnassa on siis 15 000 asiakasta. (Bruun & Hjejle 2018, 5-6.)

Ulkomaisten asiakkaiden portfoliossa oli yritys- ja yksityisasiakkaita 90 eri maasta, joista kolme suurinta määrältään olivat Venäjä, Yhdistynyt kuningaskunta ja Brittiläiset Neitsytsaaret. Ulkomaiset asiakkaat oli Viron yksikössä luokiteltu korkean riskin asiakkaiksi, mutta raportin mukaan toimet asiakkaan tunnistamiseksi olivat olleet riittämättömiä ja kansainvälisten standardien sekä Viron lain vastaisia. (Bruun & Hjejle 2018, 23, 27.)

Ulkomaisten asiakkaiden portfolion asiakkaiden toiminta oli aktiivista: vuosien 2007 ja 2015 välillä oli runsaasti maksutapahtumia, rahansiirtoja eri valuutoissa, rahanvaihtoa ja joukkolainojen sekä arvopaperien kauppaa. Paljon oli myös tilien välisiä talletuksia ja tilisiirtoja, jossa rahaa siirtyi ulkomaisten asiakkaiden portfolion asiakkailta muille Viron yksikön asiakkaille. Asiakkaiden välisiä maksutapahtumia oli noin 7,5 miljoonaa, johon ei ole laskettu tilien välisiä talletuksia. Rahavirta on ollut 200 miljardin euron luokkaa vuosina 2007-2015 näiden tutkinnassa olevien 15 000 asiakkaan ja ulkopuolisten toimijoiden välillä. (Bruun & Hjejle 2018, 6.)

Tutkinnan kohteena olivat myös Viron yksikön entiset ja nykyiset työntekijät. Työntekijöissä on asiakassuhdepäälliköitä, assistentteja, lakiosaston henkilöstöä, johtaja ja agentteja, jotka saivat palkkioita asiakashankinnasta. Tutkittuja oli yli sata, joista 42 katsottiin epäilyjä herättäviksi. Nämä 42 henkilöä olivat jollakin tavalla osallisena epäilyttävissä maksutapahtumissa ja he tunsivat yhden tai useamman asiakkaan henkilökohtaisesti. Kahdeksasta entisestä työntekijästä on tehty ilmoitus Viron poliisille rikoksesta epäiltyinä. (Bruun & Hjejle 2018, 35.)

Ulkomaisten asiakkaiden portfolio sisältää huomattavan määrän riskejä. Ulkomaisuus ei välttämättä itsessään ole riski, mutta jotkin valtiot vaativat tehostettua valvontaa. Esimerkiksi Brittiläiset Neitsytsaaret, joka oli yksi suurimmista asiakkaista, on tunnettu veroparatiisimaa. Veroparatiisit helpottavat rahanpesua, sillä niitä suojelee usein muun muassa tiukat pankkisalaisuudet, alhainen verotus ja lait, jotka mahdollistavat todellisten omistajien salaamisen (Finnwatch). Raportin mukaan tutkinnassa on lisäksi tunnistettu 177 asiakasta, jotka olivat osallisena ”Russian Laundromat” -nimisessä rahanpesurikoksessa. Suurin osa näistä asiakkaista oli rekisteröityneenä veroparatiisimaihin ja sai maksuja epäilyttäviltä venäläispankeilta (Bruun & Hjejle 2018, 33).

Viron yksikön työntekijät epäonnistuivat asiakkaan tuntemisessa. Rahanpesulain (444/2017 3 luvun 2 §) mukaan asiakassuhdetta perustettaessa asiakas on tunnistettava ja tämän henkilöllisyys on todennettava. Sama koskee myös asiakkaan mahdollisia edus-

tajia. Raportin mukaan tosiasiallisia edunsaajia ei tunnistettu eikä asiakkaista hankittu tarpeeksi tietoa. Asiakkaina oli myös sääntelemättömiä välimiesyrityksiä, eikä loppuasiakasta tunnistettu. (Bruun & Hjejle 2018, 27.)

Pankit ovat velvollisia seuraamaan asiakkaidensa toimintaa ja varmistamaan, että toiminnan laatu vastaa niitä tietoja, joita asiakkaasta on alun perin annettu (rahanpesulaki 444/2017 3 luvun 4 §). Viron yksikkö ei valvonut asiakkaiden toimintaa. Mitään sanktio- tai terrorismiuhan listoja asiakkaita vasten ei tarkistettu, mahdollisia poliittisesti vaikutusvaltaisia henkilöitä ei tunnistettu eikä tulevien maksujen valvontaan ollut automaattisia valvontajärjestelmiä. Myös raportointivelvollisuutta laiminlyötiin: epäilyttävistä toimista ei juuri raportoitu. (Bruun & Hjejle 2018, 27.)

Viron yksikön työntekijät ja heidän toimintansa olivat osa ongelmaa. Henkilökuntaa ei ollut koulutettu riittävästi eivätkä yksikön AML-toiminnot olleet riittävän itsenäisiä (Bruun & Hjejle, 2018, 27). Ajantasaisella ja riittävällä koulutuksella nämä riskit oltaisiin voitu minimoida, mutta epärehellisten työntekijöiden kohdalla asia on toisin. Epäiltyjen agenttien, joiden palkkio perustui asiakashankintaan, toiminta oli tarkoituksellista ja sitä ohjasi rahalliset motiivit. Yksi epärehellinen työntekijä erotettiin ja viidelle annettiin kirjalliset varoitukset (Bruun & Hjejle 2018, 35).

4.2 IT-ohjelmistojen integrointi

Viron yksiköllä oli oma IT-järjestelmänsä, jota ei yritysoston yhteydessä integroitu Danskenkonsernin järjestelmiin. Alun perin suunnitelmissa oli systeemien yhtenäistäminen toiminnallisten riskien hallitsemiseksi ja ajankohtaisen tiedon saamiseksi, mutta suunnitelma hylättiin kesällä 2008. Katsottiin, että integroiminen olisi kallista ja veisi liikaa kapasiteettia. (Bruun & Hjejle 2018, 41.) Täytyy huomata, että maailmanlaajuinen finanssikriisi vuonna 2008 lienee vaikuttanut Dansken investointi-intoihin.

Koska konsernilla ei ollut pääsyä Viron yksikön systeemeihin, ei sillä myöskään ollut kunnollista käsitystä yksikön asiakkaista tai liiketoiminnoista. Samasta syystä konsernin AML-prosessit, riskien ja transaktioiden valvonta sekä asiakassysteemit jäivät Viron yksiköllä puutteellisiksi. (Bruun & Hjejle 2018, 8.) Jatkuva valvonta oli myyntipäälliköiden vastuulla: he pitivät kirjaa kaikista asiakkaistaan käsin. Tehokas valvonta oli käytännössä mahdotonta asiakkaiden suurien määrien vuoksi. (Bruun & Hjejle 2018, 52.)

IT-järjestelmien yhteensopimattomuus on riski nimenomaan toimintatapojen yhtenäisyyden kannalta. Finanssivalvonta (2015b) painottaakin valvottavan sisäisten työprosessien

ja ohjeiden selkeää määrittelyä. Myös erityisesti sisäisten valvontajärjestelmien toimivuuteen tulisi kiinnittää huomioita. Päätös jättää konsernin ja Viron yksikön järjestelmät erilleen oli siis ajantasaisen lainsäädännön puitteissa kohtalokas virhe.

4.3 Sääntelemättömät maksuratkaisut

Raportin sivulla 22 mainitaan sääntelemättömistä maksujärjestelmistä:

> Customers in the Non-Resident Portfolio were both private persons and corporate entities. A small number of customers were non-regulated entities acting as intermediaries providing cross-border payment solutions to unknown end-clients in Russia and other CIS countries. (Bruun & Hjejle 2018.)

Raportissa ei korostettu sääntelemättömien toimijoiden roolia ehkä niiden pienen määrän vuoksi, mutta koin tärkeäksi nostaa sen esille. Raportissa ei rahanvaihtopalveluita lukuun ottamatta yksilöity tarkemmin, mitä nämä toimijat ovat. Käyttämällä hakusanaa ”cross-border payment solutions” sain monia tuloksia, mutta esimerkiksi Agarwal (2018) mainitsee muutamia mielenkiintoisia toimijoita. Pääosin toimijat ovat finanssiteknologian yrityksiä, kuten vertaisverkkoratkaisuille perustuvia rahansiirto- ja vaihtopalveluita sekä hajautetun tilikirjan tekniikan maksupalveluita. Lohkoketju on myös eräänlainen hajautettu tilikirja (Belin).

Finanssiteknologian (= fintech) yritykset ovat keskittyneet pankki-, vakuutus-, rahoitus-, sijoitus- ja maksupalveluiden tuottamiseen tietotekniikkaa hyväksi käyttäen (Finanssivalvonta 2017). Fintech tarjoaa paljon mahdollisuuksia finanssialan palvelujen kehittämiseen, mutta erityisesti sääntelemättömien palveluntarjoajien toiminnassa piilee myös riskejä. De Nederlandsche bank (= DNB) jaottelee raportissaan (22-23) fintechin tuomat riskit viiteen kategoriaan: taloudellisiin, toiminnallisiin, integraatio- makrovakaus- ja valvonnallisiin riskeihin.

Taloudelliset riskit liittyvät erityisesti vakiintuneiden ja perinteisten instituutioiden markkinaosuuksiin: jos uudet fintech-yritykset toimivat tarpeeksi tehokkaasti ja nopealla tahdilla ja valtaavat markkinaosuuksia perinteisiltä pankeilta, taloudellinen vakaus voi järkkyä. Ei ole myöskään takeita siitä, etteivätkö fintech-yritykset epäonnistuisi. (DNB, 22.)

Uusien teknologioiden käyttöönotto sisältää aina toiminnallisia riskejä. Uusien prosessien ja IT-systeemien käyttöönotto eivät välttämättä suju perinteisissä yrityksissä ongelmitta. Toimitusketjujen hallinta ja eri osien ulkoistaminen voivat aiheuttaa tietoturvariskejä. (DNB, 22.)

Finanssiala monimutkaistuu uusien toimijoiden myötä, ja toiminnan läpinäkyvyys saattaa kärsiä. Valvonta ja epärehellisen toiminnan ehkäisy saattaa vaikeutua. Toisaalta voi olla vaikea tunnistaa rikollisia asiakkaita ja toisaalta teknologioiden takaama pääsy asiakkaiden tietoihin voi olla ristiriidassa tietosuojalakien kanssa. Useimmiten uudet toimijat ovat vähemmän säänneltyjä verrattuna esimerkiksi pankkeihin. (DNB, 22-23.)

Makrovakauden riskillä tarkoitetaan taloudellisen järjestelmän ja kuluttajien yleiseen luottamukseen liittyviä riskejä. Esimerkiksi vertaislainat siirtävät riskejä instituutioilta kuluttajille, joilla ei välttämättä ole tarvittavaa kantokykyä. Jos uudet finanssialan toimijat dominoivat rahoituspalvelusektoria, niistä tulee liian tärkeitä ja syntyy keskittymäriski. Jos ne joutuvat vaikeuksiin, koko järjestelmä horjuu. Myös kuluttajan luottamus järjestelmään voi horjua, jos tietoturva pettää. (DNB, 23.)

Teknologiset innovaatiot ja uudenlainen toiminta voivat olla haastavia valvonnan kannalta: ne eivät välttämättä kuulu valvonnan piiriin, mutta niillä voi olla vaikutuksia instituutioihin ja talouteen. Algoritmien ja asiakasdatan hyväksikäyttö voi edelleen vaikuttaa kuluttajan luottamukseen. (DNB, 23.) Siksi valvottavilta tarvitaan jatkuvaa arviointia, koulutusta ja päivitystä sisäisiin AML-prosesseihin, jotta voidaan tunnistaa uusiin teknologioihin ja liiketoimintoihin liittyvät riskit.

4.4 Johdon toimet

Raportissa tutkittiin institutionaalisia ja inhimillisiä tekijöitä ja sitä, keitä voidaan pitää vastuussa Viron yksikön tapahtumista. Raportissa olivat mukana Viron yksikön johtoryhmä, Danske Bankin konserni, Baltian osaston johtoryhmä, sisäinen valvontaryhmä, Compliance & AML -ryhmä, konsernin lakiosasto ja konsernin hallitus. (Bruun & Hjejle 2018, 38-39.)

Jo yritysoston yhteydessä 2007 Venäjän keskuspankki ilmoitti Tanskan finanssivalvontaviranomaisille huolensa Viron yhtiön ulkomaisista asiakkaista. Venäjän keskuspankki varoitti miljardien ruplien rahansiirroista, joiden alkuperä oli epäilyksiä herättävää ja jotka saattoivat olla yhteydessä puhtaasti rikolliseen toimintaan, kuten rahanpesuun. Tanskan finanssivalvontaviranomainen pyysi selvitystä Dansken operatiiviselta johdolta. Compliance & AML -ryhmä vastasi johdon puolesta, että Viron valvontaviranomainen oli tutkinut asiaa ja todennut yhtiön noudattavan lakeja ja säännöksiä. Myöhemmin myös lakiosasto ja sisäinen valvontaryhmä vakuuttivat Tanskan viranomaisille kaiken olevan kunnossa. (Bruun & Hjejle 2018, 41.)

Pääasiassa Viron yksikön operatiivista johtoa syytetään puutteellisesta toiminnasta: AML-prosessit ja asiakkaiden valvonta eivät olleet riittävällä tasolla, työntekijöitä oli mahdollisesti sekaantunut rikolliseen toimintaan ja toiminta yleensä ei ollut riittävän itseohjautuvaa (Bruun & Hjejle 2018, 78). Puutteita oli myös muiden ryhmien toiminnassa ja viestinnässä viranomaisten kanssa.

4.4.1 Yhteistyö viranomaisten kanssa

Venäjän keskuspankki sekä Viron että Tanskan finanssivalvontaviranomaiset olivat lukuisia kertoja yhteydessä Dansken Viron yksikön johdon kanssa vuodesta 2007 alkaen. Viranomaiset olivat kiinnittäneet huomiota Viron yksikön ulkomaisten asiakkaiden portfolioon ja puutteisiin AML-prosesseissa. Katsottiin, että erityisesti venäläisasiakkaat ja niiden varojen alkuperä näyttivät epäilyttäviltä rahanpesulainsäädännön valossa. Viron yksikön johto vastasi, ettei venäläislähtöisissä tilisiirroissa ole mitään epäilyttävää (Bruun & Hjejle 2018, 84.) Raportista käy ilmi, että Viron yksikön johto, lakiosasto ja sisäinen valvonta ovat toistuvasti vähätelleet ulkomaisten asiakkaiden yhteyksiä rikoksiin. Viron valvontaviranomaisten mukaan Danske oli toistuvasti aloittanut asiakassuhteita, joissa on selkeästi epäilyttäviä piirteitä. (Bruun & Hjejle 2018, 60.)

Viron valvontaviranomainen vihjasi myös, että Dansken Viron yksikön toiminnassa taloudellinen hyöty on ajanut asiakkaan tehostetun tunnistamisen ohi (Bruun & Hjejle 2018, 49). Esimerkkinä mainitaan yksikön johdon muistio, jossa esitellään venäläisille välimiehille myytyjä joukkovelkalainoja nopeampana, halvempana ja luotettavampana tapana siirtää loppuasiakkaiden varoja ulkomaille kuin perinteisen venäläisen pankin kautta. Muistiossa mainittiin kaksi selkeää riskiä: loppuasiakkaita ei tunnistettu ja siten rahanpesuriski on suurempi, ja pääomapaon avustamisesta voi tulla mainehaittaa yritykselle. (Bruun & Hjejle 2018, 49.)

Tässä tapauksessa riskit liittyvät viestintään ja itse valvottavien toimintaan. Toimiva lainsäädäntö ei aina takaa, että valvottavat noudattaisivat sitä. Kuten Jenkins (2018) mainitsi, jotkin yritykset perustavat taloutensa ulkomaisiin asiakkaisiin ja ulkomaiseen, ”helppoon” rahaan, jonka alkuperää ei selvitetä ja omistajaa ei tunneta.

4.4.2 Ilmiantajan raportti

Viron yksikössä oli työntekijä, joka täytti ilmiantoraportin ulkomaisten asiakkaiden portfoliosta vuonna 2013 ja toisen vuonna 2014. Raportti lähetettiin yksikön johdolle, konsernin Compliance & AML -ryhmälle ja konsernin sisäiselle valvonnalle. Raportissa oli useita väi-

töksiä tietyistä asiakkaista, ja osa väitöksistä todettiin myöhemmin paikkansapitäviksi. Ilmiantaja väitti muun muassa, että pankilla ei ollut hallussaan asiakkaan taloudellisia tietoja, ja asiakas oli ilmoittanut vääriä tilitietoja. Pankki oli myös tietoisesti jatkanut yhteistyötä rikollisten asiakkaiden kanssa. Ilmiantaja linkitti asiakkaat sellaisiin tosiasiallisiin edunsaajiin, jotka olivat olleet tekemisissä venäläisten, viime aikoina suljettujen pankkien kanssa, ja jotka olivat jollakin tavalla olleet yhteydessä Vladimir Putinin ja venäläisen salaisen palvelun (= FSB) lähipiiriin (Bruun & Hjejle 2018, 50-51.)

Kuinka yksikön johto reagoi ilmiantoihin, on asia erikseen. Asiasta päätettiin käynnistää sisäinen selvitys, johon käytettäisiin Viron yksikön ulkopuolisia työntekijöitä. Konsernin johtoryhmää tiedotettiin selvityksestä, mutta ei sen aiheuttajasta. Sisäinen valvontaryhmä lähetti konsernin johdolle kaksi tarkistuskirjettä vuonna 2014. Ensimmäisessä kirjeessään sisäinen valvontaryhmä varmisti joitakin ilmiantajan syytöksiä todeksi. Joidenkin asiakkaiden tarjoamat asiakirjat tilien avausten yhteydessä osoittautuivat riittämättömiksi. Sisäinen valvonta totesi myös, että Viron yksikön työntekijät ovat saattaneet osallistua laittomuuksiin. Sisäinen valvonta lisäsi kuitenkin, ettei selvityksen perusteella ollut asioita, joista olisi välittömästi tarvinnut ilmoittaa finanssivalvontaviranomaisille. (Bruun & Hjejle 2018, 51-52.)

Selvityksiä varten perustettiin ryhmä, joka teki aloitteita väärinkäytösten tutkimiseksi ja kitkemiseksi. Raportti toteaa kuitenkin, että toimet eivät olleet riittäviä eikä niitä viety loppuun asti. Ilmiantajan raportin syytöksiä ei myöskään tutkittu kunnolla, siihen liittyvää tutkimusta ei saatettu loppuun eikä siitä raportoitu selkeästi eteenpäin. Tanskalaiselle finanssivalvontaviranomaiselle oli annettu virheellistä tietoa vuosina 2012 ja 2013, ja siitä ilmoitettiin vasta vuonna 2015. Viron yksikön johto oli väittänyt ennen vuotta 2014, että yksiköllä on vahvat AML-prosessit, mutta raportin mukaan tämä ei pitänyt paikkaansa. Johtoa vastaan ei kuitenkaan ryhdytty toimenpiteisiin vielä vuonna 2014. (Bruun & Hjejle 2018, 78.)

4.5 Johtopäätökset

Nostoista voidaan päätellä, että Dansken viron yksikön toimintaan liittyi paljon sekä sisäisiä että ulkoisia riskejä. Sisäiset riskit liittyivät työntekijöiden toimintaan, sisäisiin prosesseihin ja viestintään. Ulkoiset riskit tulivat olosuhteista: Viron historialliset ja taloudelliset siteet Venäjään muodostivat osan riskeistä. Venäjä on nykyäänkin Viron kymmenen tärkeimmän kauppakumppanien joukossa (Puura 2018). Virolainen yksikkö juontaa juurensa vuoteen 1992 ja Neuvostoliiton hajoamisen jälkeiseen aikaan. Tuolloin perustettiin kaksi virolaispankkia, Eesti Forekspank ja Eesti Investeerimispank. Forekspank perusti laajan asiakaskunnan venäläisistä yritysasiakkaista, jotka keskittyivät rahanvaihtotilisiirtoihin ja

maksuihin ulkomaille. Myöhemmin Viro ajautui pankkikriisiin Venäjän talouden kurjistuessa ja Viron keskuspankki osti Forekspankin ja Investeerimispankin. Ne fuusioituivat Optiva Pankiksi, jonka suomalainen Sampo Pankki osti 2000-luvun alussa. (Bruun & Hjejle 2018, 39-40.)

Dansken nykyinen johto syyttää Sampoa mahdollisista rikollisista asiakkaista. Noin kolmasosa ulkomaisen portfolion asiakkaista oli perustettu jo Sammon aikana ja kaksi kolmasosaa asiakkaista tuli Dansken aikana. HS:n haastatteleman entisen Sammon johtajan mukaan joitakin työntekijöitä ja asiakkaita siivottiin Sammon aikana, sillä ne eivät sopineet asiakasprofiiliin. Myös Venäjän ja Viron viranomaisten kanssa käytiin jatkuvaa keskustelua asiakkaista. Danske oli ennen yritysostoa tehnyt Due Diligence -tarkastuksen. (Lassila 2018.) Vaikkakin Sammolla olisi ollut osuutta asiaan, olisi Dansken konsernin pitänyt huomata Viron yksikköön liittyvät riskit ja valvoa sen toimintaa paremmin.

Kolmas rahanpesudirektiivi implementoitiin Viron lakiin vuoden 2008 alussa (Bruun & Hjejle 2018, 11). Kolmas direktiivi ei ollut yhtä tiukka esimerkiksi poliittisesti vaikutusvaltaisten henkilöiden tai tosiasiallisten edunsaajien suhteen kuin neljäs (ja sitä seuraava viides), mutta siinäkin oli tarkat ohjeet valvontaan ja raportointiin. Euroopan rahanpesulainsäädäntöä on kehitetty paljon 2000-luvulta alkaen tähän päivään ja Viro liittyi Euroopan unioniin vuonna 2004 ja Euroalueeseen 2011 (Euroopan unioni). Joko yksikössä ei ole järjestetty tarpeeksi kattavaa koulutusta lainsäädännöstä tai siitä ei ole välitetty.

Raportista ei käy ilmi, onko rahanpesussa käytetty kryptovaluuttaa. Mainինta sääntelemättömistä maksuratkaisuista ja tuntemattomista loppuasiakkaista kiinnitti kuitenkin huomioni. Vuonna 2013 rahaliikenne oli Dansken Viron yksikössä vilkkainta (Boxberg 2018), ja esimerkiksi bitcoinin arvo lähti nousuun 2012, saavuttaen tuhannen dollarin vuonna 2013. Jää kuitenkin spekulaatioksi, onko kryptovaluuttoja käytetty jossain rahansiirtojen välillä.

5 Pohdinta

Tutkimussuunnitelmani muuttui matkan varrella. Aluksi tarkoitukseni oli tehdä skenaarioanalyysiä bitcoinin ja muiden kryptovaluuttojen sääntelyn ja rahanpesun estämisen tulevaisuudesta, mutta aikarajoitteet tulivat vastaan. Laadukkaan skenaarioanalyysin varmistamiseksi olisin tarvinnut useita haastatteluita ja aikaa kysymysten strukturointiin. Syyskuussa julkaistu Danske Bankin rahanpesuselvitys tuli sopivaan aikaan ja oli ajankohtaisuutensa ja Suomi-kytköstensä takia mielenkiintoinen tarkastelukohde. Se auttoi myös rajaamaan tutkimuksen yhteen tapaukseen, johon pystyi peilaamaan teoriapohjaa.

Aloitin teorian kirjoittamisesta etsimällä ajankohtaista tietoa lainsäädännöstä ja kryptovaluuttojen yhteydestä rahanpesuun. Kryptovaluutat ovat mielenkiintoinen ja toisaalta arvaamaton kohde; tilanne tänään voi olla hyvin erilainen kuin se on esimerkiksi vuoden päästä. Siksi tutkimukseni pitää nähdä tämänhetkisen tilanteen kuvauksena. Tutkimuksestani ei suoraan voi antaa toimintaohjeita lainsäätäjille tai ilmoitusvelvollisille, vaan se täytyy pikemminkin nähdä tilannepäivityksenä ja keskustelun herättäjänä.

Tutkimus onnistui mielestäni avaamaan rahanpesuongelman monimuotoisuutta ja laaja-alaisuutta. Löysin yhteyksiä rahanpesun ja poliittisten agendojen välillä; kuinka kryptovaluutoilla voidaan rahoittaa vaaleihin sekaantumista ja millaiset seuraukset sillä voi olla. Kuten aikaisemmin mainitsin, rahanpesussa ei ole enää pelkästään kyse huumekaupasta, vaan siihen liittyy myös yhteiskunnallisia ja poliittisia tekijöitä ja intressejä. Rahanpesun estämisellä voidaan siis mahdollisesti vaikuttaa myös poliittisiin vaikutusyrityksiin ja parhaimmillaan hillitä kybersodankäyntiä.

Käytin uutta ja ajankohtaista tutkimustietoa kryptovaluuttojen ja rahanpesun yhteydestä. Tein hakuja kryptovaluutta-, rahanpesu- ja lakitermistöllä. Pyrin etsimään tietoa viranomaislähteistä ja talouselämän medioista. Suomen kielellä on melko vähän tutkimusta aiheesta, joten suurin osa käyttämästäni materiaalista oli englanniksi ja vaati käännöstyötä. Joillekin sanoille oli vaikea löytää käännöstä, joka kuvailisi sanaa ymmärrettävästi suomeksi. Esimerkiksi sanaa ”node”, jonka suomensin solmuksi, käytetään monissa suomenkielisissä julkaisuissa sellaisenaan. Myös Bruun & Hjejlen raportti oli englanniksi ja sen termien kääntäminen oli haastavaa. Lukiessani suomenkielisiä artikkeleita, jotka kertoivat raportista, huomasin tulkintaeroja kirjoittajien välillä. Koen, että tutkimukseni voi hyödyttää kotimaista tutkimusta, sillä kieli on ajattelua. Kieli vaikuttaa siihen, miten ilmiöitä ymmärretään. Abstraktit käsitteet on ehkä helpompi ymmärtää oman kielen kautta.

Aiheesta tarvitaan jatkotutkimusta. Kyseessä on kuitenkin laaja ongelma, joka vaikuttaa talouteen, politiikkaan ja lopulta ihmisten hyvinvointiin. Mielestäni lainsäätäjät ja kryptomarkkinoiden toimijat ovat olleet liian erillään toisistaan. Niiden tulisi tehdä enemmän yhteistyötä, jotta voitaisiin lisätä molemminpuolista ymmärrystä. Seurasin mielenkiinnosta muutamia kryptovaluuttafoorumia, jossa puhuttiin melko negatiiviseen sävyyn lainsäätäjistä ja muista rahanpesusta huolestuneista tahoista. FATF toteaa melko yksipuolisesti kryptovaluuttojen olevan riski globaalille taloudelle rahanpesun näkökulmasta. Yleisesti ottaen sääntelijöillä tuntuu olevan vain vähän tietoa kryptomarkkinoista. Niiden laillista asemaa parantamalla voitaisiin todennäköisesti helpottaa myös rahanpesun ja terrorismin rahoittamisen estämistä.

Haastavaa on myös tunnistamiseen ja kryptovaluuttojen anonymiteettiin liittyvä yhteentörmäys. Lompakkopalvelut vaativat tunnistamista, mutta louhiminen tai käyttäjältä suoraan toiselle siirtäminen eivät. Osa näistä rahansiirroista tapahtuu aina piilossa. Osa käyttäjistä haluaa pysyä anonyyminä anonyymiyden vuoksi, osa hämärän toiminnan takia. Pimeä verkko on osa ongelmaa, vaikkakin joitain palvelimia ja kauppapaikkoja on saatu viranomaisvoimin suljettua (Komonen 2016). Joidenkin maiden lainsäädäntö ei puutu herkästi rikolliseen toimintaan verkossa, joten ne houkuttelevat rikollisia. Valtioiden toimintaan on vaikea puuttua loukkaamatta diplomaattisia suhteita. Siksi suhteita tulisi ylläpitää ja parantaa, jotta voidaan tehdä yhteistyötä tällaisten riskivaltioiden kanssa.

Kryptovaluuttojen tulevaisuus on myös mielenkiintoinen aihe. Monet ovat puhuneet kuplasta, joka puhkeaa jossain vaiheessa tulppaanikuumeen tai IT-kuplan lailla. Valuuttojen louhimisesta aiheutuva sähkönkulutus on herättänyt keskustelua. Maailman sähköntuotanto pitäisi kaksinkertaistaa lähivuosina, jos bitcoin jatkaa kasvuaan nykytahtiin (Tuominen 2017). Tämä ei sovi yhteen ympäristötavoitteiden kanssa. Tässä vaiheessa on mahdotonta ennustaa, mihin kehitys johtaa. Voi olla, että kryptovaluutat ovat vain hetken kestävä buumi, tai että niistä tulee täysin laillinen ja kelpo valuutta muiden joukossa.

Uskon kuitenkin lohkoketjuteknologian jäävän käyttöön ja kehittyvän edelleen. Näyttää siltä, että se on sovellettavissa moneen käyttötarkoitukseen. Kaikkein ihanteellisinta olisi, että se valjastettaisiin edistämään demokratiaa, tasavertaisuutta ja ihmisten hyvinvointia.

Lähteet

Agarwal, S. 2018. Will fintechs dominate the cross-border payments market? Accenture Banking Blog. Luettavissa: https://bankingblog.accenture.com/will-fintechs-dominate-cross-border-payments-market?lang=en_US. Luettu 15.11.2018.

Belin, O. The Difference Between Blockchain & Distributed Ledger Technology. Tradeix. Luettavissa: https://tradeix.com/distributed-ledger-technology/. Luettu 15.11.2018.

Boxberg, K. 2018. Selvitys rahanpesusta voi pudottaa päitä Danskessa. Talouselämä, 31, s. 10.

Bruun & Hjejle. 2018. Report on the Non-Resident Portfolio at Danske Bank's Estonian Branch. Bruun & Hjejle Advokatpartnerselskab. Kööpenhamina. Luettavissa: https://danskebank.com/-/media/danske-bank-com/file-cloud/2018/9/report-on-the-non-resident-portfolio-at-danske-banks-estonian-branch-.-la=en.pdf. Luettu 29.9.2018.

Castrén & Snellman. 2016. Finnish Anti-Money Laundering Act Reformed: New Obligations, Tightened Supervision. Blog & News. Luettavissa: https://www.castren.fi/blogand-news/news-2016/finnish-anti-money-laundering-act-reformed-new-obligations-tightened-supervision/. Luettu 17.11.2018.

De Nederlandsche Bank. Technological innovation and the Dutch financial sector. Opportunities and risks for financial institutions, new market participants and supervision. Luettavissa: https://www.dnb.nl/en/binaries/Themaonderzoek%20%20uk_tcm47-336322.PDF. Luettu 15.11.2018.

Drescher, D. 2017. Blockchain Basics. A Non-Technical Introduction in 25 Steps. Apress. New York.

Euroopan unioni. Viro: Perustiedot. Luettavissa: https://europa.eu/european-union/about-eu/countries/member-countries/estonia_fi. Luettu 19.11.2018.

Financial Action Task Force (FATF). 2013. FATF Guidance: Politically exposed persons (recommendations 12 and 22). Luettavissa: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf. Luettu 13.11.2018.

Financial Action Task Force (FATF). 2018a. International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations. Luettavissa: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf. Luettu 12.11.2018.

Financial Action Task Force (FATF). 2018b. Public Statement – October 2018. Luettavissa: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-october-2018.html. Luettu 12.11.2018.

Financial Action Task Force (FATF). 2018c. Regulation of virtual assets. Luettavissa: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html. Luettu 12.11.2018.

Finanssivalvonta. 2015a. Rahanpesun ja terrorismin rahoittamisen estäminen. Sääntely ja toimijat. Luettavissa: http://www.finanssivalvonta.fi/fi/Valvonta/Rahanpesun_estaminen/saantely_toimijat/Pages/Default.aspx. Luettu: 18.4.2018.

Finanssivalvonta. 2015b. Riskiperusteinen arviointi, sisäinen ohjeistus ja henkilöstön koulutus. Luettavissa: http://www.finanssivalvonta.fi/fi/Valvonta/Rahanpesun_estaminen/Sisainen_ohjeistus/Pages/Default.aspx. Luettu 14.11.2018.

Finanssivalvonta. 2018. Tietoa Finanssivalvonnasta. Luettavissa: http://www.finanssivalvonta.fi/fi/Fiva/Pages/Default.aspx.. Luettu 26.9.2018.

Finnwatch. Veroparatiisit nakertavat julkista taloutta. Luettavissa: https://www.finnwatch.org/fi/blogi/22-suomi/teemat/492-veroparatiisit-nakertavat-julkista-taloutta. Luettu 14.11.2018.

Fiorillo, S. 2018. Bitcoin History: Timeline, Origins and Founder. The Street. Luettavissa: https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578. Luettu 15.11.2018.

Foley, S., Karlsen, J. & Putniņš, T. 2018. Sex, drugs and bitcoin: How much illegal activity is financed through cryptocurrencies? Luettavissa: https://poseidon01.ssrn.com/delivery.php?ID=218125068102114126122084027094097010103082061020005063086101085127013127113101121078123118100120050104112112073087122017004105020059005039077081121109101113070073049014011079114118089012011068031087114067105025087109006117068095020073122108001023098&EXT=pdf. Luettu 13.10.2018.

Gabbat, A. 2018. Stacey Abrams condemns Brian Kemp after he accuses Democrats of voter 'hack'. The Guardian. Luettavissa: https://www.theguardian.com/us-news/2018/nov/05/stacey-abrams-brian-kemp-georgia-race-democrat-voter-hack-claim. Luettu 13.11.2018.

Hybrid CoE. The European Centre of Excellence for Countering Hybrid Threats. Hybrid threats: Countering hybrid threats. Luettavissa: https://www.hybridcoe.fi/hybrid-threats/. Luettu 8.9.2018.

iSignthis. Your complete identity and payment solution. Luettavissa: https://www.isign-this.com/. Luettu 19.10.2018.

Jenkins, P. 2018. Why EU banks have become a money launderer's dream. Financial times. Luettavissa: https://www.ft.com/content/64ec1f54-b825-11e8-b3ef-799c8613f4a1. Luettu 26.9.2018.

Katz, L. 2018. Bitcoin Was Russian Hackers' Currency of Choice, U.S. Says. Bloomberg. Luettavissa: https://www.bloomberg.com/news/articles/2018-07-13/bitcoin-was-russian-hackers-currency-of-choice-u-s-says. Luettu 3.9.2018.

Keith, N. 2018. Anti-Money Laundering: A Comparative Review of Legislative Development. Business Law International. Vol 19 No 3. International Bar Association Legal Practice Division. Lontoo.

Keskusrikospoliisi. Rahanpesun selvittelykeskus. 2012. Rahanpesun torjunnan parhaat käytänteet. Luettavissa: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/26327_Rahanpesun_torjunnan_parhaat_kaytanteet_27.8.2012.pdf?0b268987a9eed488. Luettu 13.11.2018.

King, B. 2014. Breaking Banks. The Innovators, Rogues and Strategists Rebooting Banking. John Wiley & Sons Singapore Pte. Ltd.

Komonen, O. 2016. Suosittu huumekauppa suljettiin – myynti kolminkertaistui. Tivi. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/suosittu-huumekauppa-suljettiin-myynti-kolminkertaistui-6572964. Luettu 19.11.2018.

Krais, J. 2018. EU: 5th EU Anti-Money Laundering Directive published. Global Compliance News. Luettavissa: https://globalcompliancenews.com/eu-5th-anti-money-laundering-directive-published-20180716/. Luettu 1.9.2018.

Künnapas, K. 2016. From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of *de lege ferenda*? Teoksessa Kerikmäe, T. & Rull, A. The Future of Law and eTechnologies. Springer International Publishing.

Lahti, V. 2016. Lohkoketju muuttaa maailmaa. Sitran blogit. Luettavissa: https://www.sitra.fi/blogit/lohkoketju-muuttaa-maailmaa/. Luettu 12.11.2018.

Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017.

Lassila, A. 2018. Danske Bank vierittää vastuuta rahanpesusta Sampo-pankille – Mika Ihamuotila kiistää epäilyt, Björn Wahlroos ei kommentoi. Helsingin sanomat. Luettavissa: https://www.hs.fi/talous/art-2000005833593.html. Luettu 14.11.2018.

Lehto, T. 2018. Finanssivalvonta: rahanpesuvalvonta tehostuu Suomessakin – ”pankeilla on parannettavaa”. Kauppalehti. Luettavissa: https://www.kauppalehti.fi/uutiset/finanssivalvonta-rahanpesunvalvonta-tehostuu-suomessakin--pankeilla-on-parannettavaa/MFshG3VT. Luettu 26.9.2018.

Leppänen, M. 2018. Lohkoketjun “kolmas vallankumous” on käsillä – mullistavatko digitaaliset arvopaperit sijoittamisen, vai tuleeko niistä vain kryptohypen seuraava aalto? Yle uutiset. Luettavissa: https://yle.fi/uutiset/3-10454370. Luettu 12.11.2018.

Miller, M. 2015. The Ultimate Guide to bitcoin. Que Publishing. Indianapolis.

Mostrous, A., Bridge M. & Gibbons, K. 2017. Russia used Twitter bots and trolls ‘to disrupt’ Brexit vote. The Times. Luettavissa: https://www.thetimes.co.uk/article/russia-used-web-posts-to-disrupt-brexit-vote-h9nv5zg6c. Luettu 8.9.2018.

Mäntylä, T. 2017. Rahanpesulaki uudistuu. Intrumin verkkolehti. Luettavissa: https://www.intrumlehti.fi/lakitietoa/rahanpesulaki-uudistuu/. Luettu 17.11.2018.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Luettavissa: https://bitcoin.org/bitcoin.pdf. Luettu 30.8.2018.

Nortio, J. 2017. Suomen kyberturvallisuutta kiusaavat “valtiolliset toimijat” – mitä se tarkoittaa? Tekniikan maailma. Luettavissa: https://tekniikanmaailma.fi/suomen-kyberturvallisuutta-kiusaavat-valtiolliset-toimijat-mita-se-tarkoittaa/. Luettu 8.9.2018.

Oikeusministeriö. Keskinäinen rikosoikeusapu. Luettavissa: https://oikeusministerio.fi/keskinainen-rikosoikeusapu. Luettu 13.11.2018.

Prasos. 2018. Coinmotion – käyttöehdot. Luettavissa: https://coinmotion.com/fi/terms-of-service. Luettu 19.10.2018.

Puura, E. 2018. Trade reached record level last year. News release no 16. Statistics Estonia. Luettavissa: https://www.stat.ee/news-release-2018-016. Luettu 17.11.2018.

Rikoslaki 39/1889.

Räisänen, P. 2017. Panama-papereissa ryvettyneen lakifirman perustajat pidätettiin – syytteenä rahanpesu. Kauppalehti. Luettavissa: https://www.kauppalehti.fi/uutiset/panama-papereissa-ryvettyneen-lakifirman-perustajat-pidatettiin---syytteena-rahanpesu/YQevTzSh. Luettu 1.9.2018.

Storås, N. 2016. Lohkoketjuteknologia pähkinänkuoressa – tämä kannattaa tietää. Tivi. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/lohkoketjuteknologia-pahkinakuoressa-tama-kannattaa-tietaa-6537904. Luettu 19.9.2018.

Symantec Corporation (Norton). What is bulletproof hosting? Luettavissa: https://us.norton.com/internetsecurity-emerging-threats-what-is-bulletproof-hosting.html. Luettu 16.10.2018.

Tapscott, D. & Tapscott, A. 2016. Blockchain revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World. Portfolio Penguin.

Techopedia. Private Key. Luettavissa: https://www.techopedia.com/definition/16135/private-key. Luettu 12.9.2018.

Tuominen, J. 2017. Bitcoin-louhimisen sähkönkulutus valtavaa - enemmän kuin monilla valtioilla. Tivi. Luettavissa: https://www.tivi.fi/Kaikki_uutiset/bitcoin-louhimisen-sahkonkulutus-valtavaa-enemman-kuin-monilla-valtioilla-6691437. Luettu 19.11.2018.

Tuominen, J. 2018. Suomen pankin asiantuntija pitää bitcoinia illuusiona - ”ei ole tahoa, joka olisi luvannut, että saat bitcoinin vastineeksi jotain”. Tekniikka & Talous. Luettavissa: https://www.tekniikkatalous.fi/talous_uutiset/suomen-pankin-asiantuntija-pitaa-bitcoinia-illuusiona-ei-ole-tahoa-joka-olisi-luvannut-etta-saat-bitcoinin-vastineeksi-jotain-6732979. Luettu 1.9.2018.

Verhage, J. 2018. Nasdaq Holds Closed Door Event to Discuss Policing Crypto. Bloomberg. Luettavissa: https://www.bloomberg.com/news/articles/2018-07-27/crypto-players-gather-as-nasdaq-bids-to-burnish-industry-s-image. Luettu 1.9.2018.

Verohallinto. 2016. Johdannaisten verotus. Luettavissa: https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48914/johdannaisten_verotu/#4-hinnanerosopimukset-(cfd). Luettu 15.9.2018.

Verohallinto. 2018. Virtuaalivaluuttojen verotus. Luettavissa: https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen-verotus/. Luettu 1.9.2018.

Viestintävirasto. 2016. Verkkorikollisuus ja pimeä verkko – verkkorikollisille suunnatuilla palveluilla omat markkinansa. Luettavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603021442.html. Luettu 16.10.2018.

Worldatlas. 2018. Commonwealth of Independent States – Map & History. Luettavissa: https://www.worldatlas.com/aatlas/infopage/cis.htm. Luettu 3.10.2018.

Yrittäjät. 2018. Identiteettivarkaus voi iskeä sinuunkin – Niitä tehdään jo enemmän kuin asuntomurtoja, näin suojaudut. Luettavissa: https://www.yrittajat.fi/uutiset/593462-identiteettivarkaus-voi-iskea-sinuunkin-niita-tehdaan-jo-enemman-kuin-asuntomurtoja. Luettu 19.10.2018.

Öhrnberg, P. 2018. USA julkisti syytekirjelmän: Venäjä harjoitti “informaatiosodankäyntiä” Yhdysvaltoja vastaan. Kauppalehti. Luettavissa: https://www.kauppalehti.fi/uutiset/usa-julkisti-syytekirjelman-venaja-harjoitti-informaatiosodankayntia-yhdysvaltoja-vastaan/jAgGh7Vd. Luettu 3.9.2018.