

Janne Kaisto – Eelis Paukku – Juhana Riekkinen



# LOHKOKETJUJURIDIIKAN PERUSTEET



LAPIN YLIOPISTO  
UNIVERSITY OF LAPLAND



JANNE KAISTO – EELIS PAUKKU – JUHANA RIEKKINEN

# LOHKOKETJUJURIDIIKAN PERUSTEET



LAPIN YLIOPISTO  
UNIVERSITY OF LAPLAND

Rovaniemi 2023

Kirjoittajat:

**Janne Kaisto**, varallisuus oikeuden professori, OTT  
<https://research.ulapland.fi/fi/persons/janne-kaisto>

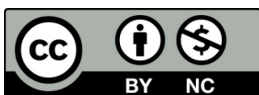
**Eelis Pauku**, tutkijatohtori, OTT, KTM, DI  
<https://research.ulapland.fi/fi/persons/eelis-pauku>

**Juhana Riekkinen**, oikeusinformatiikan yliopistonlehtori, OTT, VT  
<https://research.ulapland.fi/fi/persons/juhana-riekkinen>

**Vipuvoimaa**  
**EU:lta**  
2014–2020



**Euroopan unioni**  
Euroopan sosiaalirahasto



Kannen suunnittelu: Juhana Riekkinen

Kannen kuvat: Stable Diffusion Online ja Shubham Dhage / Unsplash

ISBN 978-952-337-353-2 (pdf)

Julkaisun pysyvä osoite: <https://urn.fi/URN:ISBN:978-952-337-353-2>

## ESIPUHE

Käsillä olevan teoksen laadintaan on saatu rahoitusta Euroopan sosiaalirahastosta. Teos pohjautuu ensi kerran keväällä 2021 järjestettyyn Lapin yliopiston oikeustieteiden tiedekunnan verkkokurssiin, joka kuului yhtenä toimenpiteenä Oulun yliopiston, Lapin yliopiston, Vaasan yliopiston ja Kajaanin ammattikorkeakoulun Tehoa lohkoketjuista -hankkeeseen (S22027), joka alkoi keväällä 2020. Tekstiä on kehitetty ja päivitetty niin, että sitä voidaan hyödyntää materiaalina hankkeen loppuvaiheen koulutuksissa. Tehoa lohkoketjuista -hanke päättyy vuoden 2023 aikana.

Lohkoketjuista ja erilaisista lohkoketjusovelluksista on nykyisellään jo suuri määrä tieteellistä ja muunlaista kirjallisuutta. Myös oikeudelliseen näkökulmaan on kiinnitetty huomiota. Erilaisia juridiikan kannalta relevantteja kysymyksiä on kaiken kaikkiaan valtava määrä, mikä hankaloittaa kokonaiskuvan muodostamista lohkoketjuteknologian ja oikeuden välisestä suhteesta.

Tässä teoksessa käsitellään lohkoketjuja ja lohkoketjusovelluksia oikeudellisen sääntelyn näkökulmasta. Kyse ei kuitenkaan ole kaiken kattavasta esityksestä, vaan olemme joutuneet tekemään lukuisia rajauksia. Lukijan on hyvä ottaa huomioon myös, että teos pohjautuu opetuskäyttöön tarkoitettuun materiaaliin. Emme vastaa tekstistä mahdollisesti löytyvistä puutteista, epätarkkuuksista ja jopa suoranaisista virheistä. Lohkoketjuteknologiaan liittyy koko joukko oikeudellisia kysymyksiä, joihin ei nykytiedon valossa voi antaa varmoja vastauksia.

Vaikka lohkoketjuteknologiaan liittyvien oikeudellisten kysymysten tarkastelu edellyttää tiettyjä perustietoja myös kyseessä olevasta teknologiasta yleensä, emme ole sisällyttäneet teokseen yleistä johdatusta lohkoketjuihin. Luotamme tässä suhteessa ole-massa olevaan materiaaliin kuten Kajaanin ammattikorkeakoulun Tehoa lohkoketjuista -hankkeen puitteissa laatimaan johdatuskurssiin. Syvemmälle tekniikkaan on menty vain, jos tämä on ollut tarpeellista oikeudellisen analyysin kannalta. Olemme esimerkiksi avanneet jonkin verran erilaisten rahakestandardien teknistä toteutusta. Keskustelut Tehoa lohkoketjuista -hankkeen muiden osallistujien kanssa ovat olleet hyödyllisiä, ja kiitämme tässä suhteessa erityisesti Joonaa Kaurasta, joka on myös lue-nut käsikirjoituksen jaksot 4.2 ja 6.2 sekä esittänyt niistä hyviä kommentteja.

Rovaniemellä 1.2.2023

Janne Kaisto

Eelis Paukku

Juhana Riekkinen

# SISÄLLYS

ESIPUHE .....	V
1 Johdannoksi.....	1
1.1 Lohkoketjuteknologia pääpiirteissään.....	1
1.2 Lohkoketju ja sosiotekninen muutos.....	3
1.3 Oikeudellinen näkökulma.....	6
1.4 Teoksessa tarkasteltavista kysymyksistä .....	9
2 Bitcoin ja muut vastaavanlaiset originaalit virtuaalivaluutat .....	11
2.1 Virtuaalivaluutta objektina ja varallisuus oikeuksien kohteena .....	11
2.2 Tunnistautumiseen liittyvistä ongelmista ja niiden ratkaisemisesta .....	14
2.3 Laillinen maksuväline vai jotain muuta?.....	18
2.4 Saantomuodot .....	22
2.5 Virtuaalivaluutan luovutus ja velkojasuoja .....	26
2.6 Toiselle kuuluvan virtuaalivaluutan luovutus.....	28
2.7 Säilytystä sisältävät palvelut .....	30
2.8 Virtuaalivaluutat ja verotus.....	37
3 Älypimukset ja sopimusoikeus.....	41
3.1 Älypimukset pääpiirteissään .....	41
3.2 Lohkoketjuun sijoitettu ohjelma – oikeushenkilö?.....	42
3.3 Soveltuvasta sääntelystä .....	43
3.4 Älypimus sopimuksen täytäntöönpanon välineenä .....	44
3.5 Tarjouksen tekeminen lohkoketjuun sijoitetun ohjelman avulla .....	46
4 ICO ja tokenit .....	50
4.1 Initial Coin Offering (ICO) pääpiirteissään .....	50
4.2 Perusteita rahakkeista tekniseltä ja oikeudelliselta kannalta.....	51
4.3 Sijoittamista koskeva sääntely .....	57
4.4 Hyödykerahakkeet (utility tokens).....	64

4.5	Laki virtuaalivaluutan tarjoajista liikkeeseenlaskijan kannalta .....	67
5	Tietosuojalainsäädäntö.....	70
5.1	Lähtökohtia .....	70
5.2	Rekisterinpitäjät ja henkilötietojen käsittelijät .....	73
5.3	Tietosuojaperiaatteet ja käsittelyn oikeusperusteet .....	79
5.4	Rekisteröidyn oikeudet.....	84
5.5	Henkilötietojen käsittelyn turvallisuus.....	92
6	Immateriaalioikeudellisia näkökohtia.....	97
6.1	Lohkoketju ja tekijänoikeus.....	97
6.2	Tekijänoikeus ja tokenisoitu taide .....	99
6.3	Lohkoketjupatentit .....	106
7	Lopuksi.....	110





# 1 JOHDANNOKSI

## 1.1 Lohkoketjuteknologia pääpiirteissään

Lohkoketjuteknologiassa on perimmältään kyse teknologiasta, joka mahdollistaa tiedon luotettavan varastoinnin ja kerryttämisen hajautetusti. Kyse on verraten tuoreesta innovaatiosta, jolla on läheinen yhteys virtuaalivaluuttojen (englanniksi *virtual currency*) kehittymiseen ja yleistymiseen. Hyvin tärkeä kirjoitus tässä suhteessa on nimimerkillä Satoshi Nakamoto julkaistu kirjoitus *Bitcoin: A Peer-to-Peer Electronic Cash System*, jossa esiteltiin hajautettu lohkoketjuteknologia helposti ymmärrettävässä muodossa. Kirjoittajan tai kirjoittajien tarkoituksena oli esitellä maksujärjestelmä, joka ei edellyttänyt erillistä välittäjäorganisaatiota, kuten pankkia, ja jota näin ollen voitiin käyttää käteisen tapaan. Kirjoitus liittyy läheisesti Bitcoinin kehittymiseen.

Lohkoketjulle ei vielä ole vakiintunut täysin yksiselitteistä määritelmää. Melko hyvän kuvan yleisesti vallitsevista käsityksistä tarjoaa kuitenkin esimerkiksi TEPA-termipankista löytyvä määritelmä, jonka mukaan kyseessä on ”jatkuvasti kertyvä hajautettu datakokonaisuus, jonka kaikki tapahtumat ovat aikajärjestyksessä, kaikkien osapuolten vahvistamia ja tallennettu niin, ettei mitään voi muuttaa tai väärentää”.

Siteeratusta määritelmästä ei käy ilmi, kuinka kuvattujen tunnusmerkkien mukainen hajautettu datakokonaisuus saadaan aikaan. Syvällinen ymmärtäminen tässä suhteessa edellyttää varsin hyviä tietoja ohjelmoinnista ja kryptografiasta. Esimerkiksi epäsymmetrisellä salauksella, jossa salaukseen ja salauksen purkamiseen käytetään eri avaimia, on keskeinen asema monissa lohkoketjusovelluksissa. Toiseksi esimerkiksi teknistä osaamista vaativista asioista voi mainita *hash*-funktion. Sen avulla mistä tahansa merkkijonosta voidaan tuottaa sitä kuvaava tiiviste, joka on käytännössä uniikki arvo, jonka käsittely on merkkijonoa nopeampaa.

Lohkoketjut koostuvat nimensä mukaisesti ketjussa olevista lohkoista, joihin on varastoitu tietoa. Samat tiedot on talletettu useaan paikkaan, joita yleensä kutsutaan englannin kielellä termillä *node*, joka voidaan kääntää esimerkiksi *solmuksi* tai *noodiksi*. Tällaisessa hajautetussa järjestelmässä tarvitaan väistämättä mekanismeja, joilla varmistetaan lohkojen samuus kaikissa solmuissa. Jokaista lohkoketjua perustettaessa täytyy määrittää konsensusmekanismi eli mekanismi, jolla transaktioiden oikeellisuus määritetään ja jonka avulla päästään haluttuun lopputulokseen eli siihen, että osallisilla on luotettavasti hallussaan sisällöltään vastaava datakokonaisuus.

Lohkoketjuteknologialla ei ole vain yhtä muotoa, mikä osaltaan hankaloittaa täysin yleispätevän määritelmän esittämistä. Erilaisia lohkoketjuja saatetaan ryhmitellä muun muassa sillä perusteella, kuinka lohkoketjuun voi osallistua. Jos tarvitaan lupa järjestelmän perustajalta tai muulta taholta, kyse on luvanvaraisesta lohkoketjusta. Esimerkiksi Bitcoin on tyyppiesimerkki ei-luvanvaraisesta lohkoketjusta, johon kuka tahansa internetiin pääsyn omaava voi liittyä. Lohkoketjuja erotetaan toisistaan usein myös lohkoketjuun kirjattujen transaktioiden näkyvyyden perusteella. Julkiselle lohkoketjulle ominaista on, että transaktiot näkyvät kaikille. Näin on asia esimerkiksi Bitcoinin yhteydessä. Yksityisestä lohkoketjusta voidaan puhua muun muassa silloin, kun transaktio näkyy vain niille tahoille, jotka suoraan liittyvät transaktioon. Terminologia ei ole täysin yhdenmukaista, ja esimerkiksi termin julkinen lohkoketju käyttöön on saatettu kytkeä myös ei-luvanvaraisuus eli kaikkien halukkaiden mahdollisuus liittyä.

Lohkoketjuja ryhmitellään usein myös avoimiin ja suljettuihin lohkoketjuihin. Jonkin verran yksinkertaistaen voidaan sanoa, että avoimista lohkoketjuista puhuttaessa tarkoitetaan yleensä ei-luvanvaraisia ja julkisia lohkoketjuja. Jos termiä julkinen käytetään laajassa merkityksessä, julkinen ja avoin ovat siten synonyymejä. Suljetut lohkoketjut, joita on voitu nimittää myös yksityisiksi, puolestaan viittaavat luvanvaraisiin lohkoketjuihin, joissa tavallisesti on myös rajoitettu transaktioiden näkyvyyttä.

Julkisuudessa on puhuttu varsin usein Bitcoiniin liittyvästä huomattavasta sähkönkulutuksesta. Tämä on seurausta Bitcoinin ja muiden vastaavien sovellusten käyttämästä *proof-of-work*-konsensusmekanismista (ns. työvarmennus), jolle on ominaista järjestelmän luotettavuuden varmistaminen hajautetusti suoritettavien työläiden matemaattisten tehtävien avulla. Tämä ei suinkaan ole ainoa mahdollinen konsensusmekanismi. Esimerkiksi *proof-of-authority* tarkoittaa menetelmää, jossa joillakin määritellyillä osallistujilla on valta määrätä lohkoketjuun lisättävistä lohkoista.

Se, millainen konsensusmekanismi valitaan, riippuu paljon kyseessä olevan lohkoketjusovelluksen teknisestä perusluonteesta ja tavoitteista. Esimerkiksi *proof-of-authority* sopii luontevasti järjestelmään, jossa alkuperäiset perustajat ovat sinänsä valmiit ottamaan järjestelmään myöhemmin mukaan muitakin osallisia mutta jossa he haluavat itselleen erityisaseman. Alkuperäiset perustajat voivat tällaisessa järjestelmässä helposti pidättää itsellään myös vallan määrätä siitä, keitä myöhemmin ylipäättään otetaan mukaan järjestelmään. Kyse on siis luvanvaraisesta lohkoketjusta, johon usein liittyy luontevasti myös yksityisyys. Lohkoketju voidaan järjestää teknisesti esimerkiksi niin, että vain tiettyyn transaktioon osalliset voivat nähdä transaktioon liittyvät tiedot.

Lohkoketjuteknologia liittyy läheisesti hajautetun tilikirjan teknologiaan (*Distributed Ledger Technology*), jonka alalajiksi lohkaketjuteknologia usein luetaan. Näiden teknologioiden käsitteellisistä suhteista ei kuitenkaan vallitse täyttä yhteisymmärrystä. Oikeudelliselta kannalta on kiinnostavaa, että ainakin Euroopan unionin lainsäädäntö vaikuttaa olevan kehittymässä siihen suuntaan, että sääntelyä suunnataan lohkaketjuteknologian sijasta hajautetun tilikirjan teknologiaan. Esimerkiksi voidaan mainita Euroopan parlamentin ja neuvoston asetus (EU) 2022/858, annettu 30 päivänä toukokuuta 2022, hajautetun tilikirjan teknologiaan perustuvien markkinainfrastruktuurien pilottijärjestelmästä ja asetusten (EU) N:o 600/2014 ja (EU) N:o 909/2014 sekä direktiivin 2014/65/EU muuttamisesta.

Hajautetun tilikirjan teknologia eli DLT ymmärretään asetuksessa (EU) 2022/858 tavalla, joka muistuttaa monessa suhteessa lohkaketjuteknologiaa. Hajautetun tilikirjan teknologialla tarkoitetaan 2 artiklan mukaan teknologiaa, jolla mahdollistetaan hajautettujen tilikirjojen toiminta ja käyttö. Hajautetulla tilikirjalla puolestaan tarkoitetaan tietorekisteriä, jossa säilytetään tiedot liiketoimista ja joka jaetaan joukolle DLT-verkon solmuja ja synkronoidaan niiden välillä konsensusmekanismia käyttäen. Konsensusmekanismit määritetään säännöiksi ja menettelyiksi, joita soveltaen saavutetaan DLT-verkon solmujen välinen yhteisymmärrys liiketoimen validoinnista. DLT-verkon solmu määritetään laitteeksi tai prosessiksi, joka on osa verkkoa ja jolla on täydellinen tai osittainen kopio kaikista hajautetun tilikirjan liiketoimia koskevista tiedoista.

## 1.2 Lohkoketju ja sosiotekninen muutos

Jokaisen innovaation todelliset taloudelliset ja yhteiskunnalliset vaikutukset riippuvat lopulta siitä, miten ja missä laajuudessa keksintöä hyödynnetään yhteiskunnassa. Esimerkiksi höyryvoiman keksiminen ei itsessään saanut aikaan sitä teollista vallankumousta, jota nykyään kutsutaan ensimmäiseksi teolliseksi vallankumoukseksi. Olennaista on, että höyryvoimalla toimivia koneita ryhdyttiin käyttämään laajamittaisesti, mikä muun muassa lisäsi olennaisesti tuottavuutta ja toi ihmisten elämään rautatiet ja höyryvoimalla kulkevat teräsalukset. Vastaavasti sähköön ja öljyyn liittyvät hieman myöhemmät keksinnöt olisivat voineet jäädä vähämerkityksisiksi, jos ihmisyhteisöt eivät avosylin olisi ottaneet vastaan esimerkiksi polttomoottorilla kulkevia autoja, sähkövaloja, radiota, puhelinta ja televisiota. Ensimmäinen ja toinen teollinen vallankumous, joka usein kytketään sähkövoimaan ja myös polttomoottorin keksimiseen, merkitsivät lopulta laajoja yhteiskunnallisia muutoksia, jotka liittyivät muun muassa uuteen energialähteeseen, uudenslaisiin kommunikaatiomenetelmiin ja aiemmasta poikkeaviin kuljetusjärjestelmiin.

Teknologiset innovaatiot saattavat siis tuoda mukanaan erilaisia sosioteknisiä muutoksia. Tällä hetkellä eletään kolmannen tai jopa neljännen teollisen vallankumouksen aikaa, jossa puolijohteen ja transistorin keksimisestä alkanut kehitysketju on ehtinyt muovata monin tavoin yhteiskuntia. Digitalisaatiosta on seurannut digitalisoituminen, joka on mahdollista erottaa käsitteellisesti digitaalisaa tiosta siinä mielessä, että se ilmentää sosioteknistä muutosta digitalisaation viitattaessa enemmän vain tekniseen ilmiöön. Lohkoketjuteknologia lukeutuu tietoteknisten innovaatioiden tuoreimpaan kerrostumaan. Siihen kohdistuu paljon odotuksia sosioteknisten muutosten tasolla erityisesti sen vuoksi, että lohkoketjuteknologia mahdollistaa luottamuksen toisilleen tuntemattomienkin välillä ilman, että jotain ulkopuolista tahoja tarvittaisiin luottamuksen synnyttämiseen.

Tällä haavaa on vaikea ennustaa lohkoketjuteknologiaan liittyvän sosioteknisen muutoksen luonnetta ja laajuutta. Sinänsä selvää on, että virtuaaliset valuutat ovat jo saavuttaneet kohtalaisen suosion. Erilaisia virtuaalivaluuttoja on suuri määrä, ja joillain niistä on myös merkittävästi arvoa. Esimerkiksi yhden bitcoinin arvo tätä kirjoitettaessa on noin 19 000 euroa, ja bitcoineja on yhteensä jonkin verran alle 20 miljoonaa. Bitcoinin arvo tosin on todennäköisesti jotain aivan muuta, kun luet tämän tekstin. Kuten myöhemmin jaksossa 2.3 tarkemmin kerrotaan, Bitcoin-järjestelmä on suunniteltu siten, että bitcoinien enimmäismäärä on 21 miljoonaa bitcoinia.

Virtuaaliset valuutat eli virtuaalivaluutat merkitsevät lohkoketjuteknologiassa kehitysvaihetta 1.0, jonka yhteiskunnallinen merkitys on osin vielä arvailujen varassa. Virtuaalivaluutat eivät ole syrjäyttäneet perinteisiä valuuttoja maksuvälineenä, ja monesti niitä hankitaan suurelta osin spekulatiivisiin tarkoituksiin. Esimerkiksi bitcoinin arvo vaihtelee verrattain paljon. Monet viranomaiset eri aloilla ovat suhtautuneet varsin epäilevästi bitcoiniin ja muihin sen kaltaisiin virtuaalivaluuttoihin. Esimerkiksi yleisen lainvalvonnan ja pakkotäytännön kannalta virtuaalivaluuttojen erityisen haitallinen piirre on, että niitä on monesti vaikea jäljittää tai yhdistää luonnollisiin henkilöihin. Tämän vuoksi esimerkiksi erilaisissa kiristystapauksissa pyydetään nykyään usein maksua bitcoineina, ja järjestäytynyt rikollisuus on yleisestikin ottaen yhä enemmän alkanut suosia bitcoinia. Virtuaalivaluuttoihin sijoituskohteena liittyy myös riskejä, joista muun muassa keskuspankit ja markkinoita valvovat viranomaiset eri puolilla maailmaa ovat varoittaneet sijoittajia.

Virtuaalivaluutan käsite ei vielä ole vakiintunut, eli virtuaalivaluutasta puhuttaessa saatetaan tarkoittaa jossain määrin erilaisia asioita. Virtuaalivaluutat kytetään varsin usein lohkoketjuteknologiaan tai hajautetun tilikirjan teknologiaan. Käsite on kuitenkin ymmärretty usein myös laajemmaksi. Koska tässä teoksessa käsitellään vain lohkoketjuja ja lohkoketjusovelluksia, virtuaalivaluutoista puhuttaessa tarkoitetaan yleensä vain lohkoketjupohjaisia sovelluksia.

Virtuaalivaluutan ohella puhutaan usein myös virtuaalisesta varallisuudesta, kryptovaroista tai kryptovaluutoista ilman, että termeillä olisi täysin vakiintunutta merkityssisältöä. Krypto-etuliite sopii hyvin lohkoketjuihin siinä mielessä, että se vie ajatukset kryptografiaan, jolla on läheinen yhteys lohkoketjuteknologiaan. Lohkoketjuihin keskityttäessä lienee selkeintä lähteä liikkeelle virtuaalisen varallisuuden tai kryptovarojen käsitteestä ja katsoa, että virtuaalivaluutat lukeutuvat tällaisen varallisuuden muodon alaisuuteen. Virtuaalivaluuttojen alaisuudessa on puolestaan mahdollista erottaa omia alaryhmiään. Niin historiallisten kuin puhtaasti käytännöllisten syiden vuoksi omaksi ryhmäkseen voidaan erottaa bitcoin ja muut sitä asiallisesti vastaavat ”natiivit” tai ”originaalit” virtuaalivaluutat. Näille tyypillistä on paitsi se, että ne on käytännössä rakennettu sisäisesti kyseessä olevaan lohkoketjujärjestelmään, ettei niillä itsellään ole mitään varsinaista substanssiarvoa ja että ne ainakin periaatteessa on tarkoitettu etupäässä maksuvälineiksi. Käsitteiden ja termien vakiintumattomuuden vuoksi on kuitenkin muistettava erikseen tarkastella kussakin kielenkäyttötilanteessa, missä merkityksessä esimerkiksi virtuaalivaluutan tai kryptovaran käsitettä on käytetty.

Lohkoketjuteknologian kehitysvaiheeseen 2.0 voidaan laskea erilaisten ohjelmoitavien alustojen puitteissa lohkoketjuun sijoitettavat ohjelmat tai sovellukset, joilla voi olla mitä erilaisempia toimintoja. Tunnetuin tällaisista alustoista on Ethereum, joka monessa suhteessa muistuttaa Bitcoin-järjestelmää. Myös Ethereumissa on oma originaali virtuaalivaluuttansa, nimeltään ether, mutta Ethereum-järjestelmää suunniteltaessa on erityisesti kiinnitetty huomiota siihen, että järjestelmässä voidaan sijoittaa ohjelmia lohkoketjuun. Ethereiden yhteenlaskettu arvo on tätä kirjoitettaessa lähes 200 miljardia euroa, mikä sijoittaa etherin yhteisarvoltaan toiseksi tärkeimmäksi kryptovaluutaksi bitcoinin jälkeen.

Myös lohkoketjuun sijoitettavilla ohjelmilla, joita yleensä kutsutaan älysovimuksiksi, on jo useita käytännön sovelluksia. Niihin liittyvän sosioteknisen muutoksen luonne ja laajuus on kuitenkin vielä auki. Sama koskee suurelta osin myös lohkoketjuteknologian kehitysvaihetta 3.0, jolle ei vielä liene vakiintunut täysin selkeää merkityssisältöä, vaikka monissa lohkoketjua koskevissa kirjoituksissa puhutaankin jo tästä ja sen jälkeenkin tulevista kehitysvaiheista. Kehitysvaiheeseen 3.0 saatetaan lukea esimerkiksi rahakehityksen talousjärjestelmän kehittymistä, monimutkaisia lohkoketjussa autonomisesti toimivia ohjelmia ja erilaisia lohkoketjuinnovaatioiden kombinaatioita.

Lohkoketjuteknologiaa voidaan pyrkiä hyödyntämään niin julkisessa kuin yksityisessä toiminnassa. Erilaisia ehdotuksia ja ideoita on esitetty maailmanlaajuisesti niin paljon, että niistä on hankala luoda systemaattista kokonaiskuvaa. Lohkoketjuteknologian perusluonteen vuoksi kyse on viime kädessä hajautetusta tiedon varastoinnista ja kerryttämisestä. Lohkoketjusovellukset voivat perusmuodossaan olla tekninen perusta rekisterinpidolle, joka voi olla luonteeltaan myös

dynaamista siinä mielessä, että rekisterinpidon keskiössä ovat joitain vaihdettavia varoja koskevat transaktiot. Lohkoketjuun voidaan kuitenkin tallentaa niin momenttyyppistä tietoa, että pelkästään rekisterinpidosta puhuminen saattaa joissain tilanteissa antaa harhaanjohtavan kuvan, vaikka kyse viime kädessä onkin tiedon ylläpitämisestä hajautetussa rekisterijärjestelmässä.

Myös Suomessa on jo suhteellisen paljon kirjoituksia lohkoketjun mahdollisuuksista niin yleisesti kuin erityisesti Suomen oloissa. Esimerkkeinä voidaan mainita Markus Rahkola: *Raportti tulevaisuusvaliokunnalle: Katsaus lohkoketjuteknologioiden hyödyntämiseen Suomessa* (Eduskunta 2019) ja Patrik Elias Johansson – Mikko Eerola – Antti Innanen – Juha Viitala: *Lohkoketju – tiekartta päättäjille* (Alma Talent 2019) sekä myös Juri Mattila (toim.) – Timo Seppälä – Taneli Hukkinen – Arto Laikari – Kalle Markkanen – Riikka Koulu – Kai Jia: *Lohkoketjuteknologian hyödyntämismahdollisuudet palkkatulojen verotuksessa* (Valtioneuvoston kanslia 2019), jossa otsikon mukaisesti on päähuomio palkkatulojen verotuksessa.

Lohkoketjua on viime vuosina soviteltu liki kaikkiin mahdollisiin ympäristöihin ja konteksteihin, ja monet ehdotukset ovat olleet varsin innovatiivisia. Se, millaiset sovellukset lopulta osoittautuvat elinvoimaisiksi, selviää kuitenkin vasta vuosien tai vuosikymmenten jälkeen. Toisinaan on jouduttu toteamaan, ettei lohkoketjuteknologiasta ehkä olekaan saatavissa etuja. Esimerkiksi *Lohkoketjuteknologian hyödyntämismahdollisuudet palkkatulojen verotuksessa* -raportin mukaan lohkoketjuteknologialla ei vaikuttaisi olevan juurikaan hyödyntämismahdollisuuksia palkkatulojen verotuksen prosesseissa. Raportissa myös arvioidaan yleisemmin, että lohkoketjuteknologiaan on kohdistunut suhteettoman paljon odotuksia ja että myös lohkoketjuteknologian luonne on saatettu ymmärtää erheellisesti, mikä puolestaan on johtanut epärealistisiin odotuksiin. Raportissa on hahmotettu lohkoketjuteknologia melko suppeasti niin, että sillä on tarkoitettu ennen muuta menetelmää vertaistietojärjestelmien luomiseksi täysin ilman keskuskontrollia harjoitettavia palveluntarjoajia. Raportissa otetaan erikseen kantaa myös hajautettujen tilikirjojen teknologiaan, joka nähdään lohkoketjuteknologiaa lupaavamaksi palkkaverotuksen kontekstissa.

### 1.3 Oikeudellinen näkökulma

Nykymuotoisissa yhteiskunnissa valtioilla on paljon valtaa. Esimerkiksi Suomen perustuslakiin (731/1999) on kirjattu klassinen vallan kolmijako-oppi siten, että toisistaan erotetaan lainsäädäntövalta, hallitusvalta ja tuomiovalta (3 §). Lainsäädäntövaltaa käyttää eduskunta, jolla näin ollen on valta määrätä Suomessa voimassa olevista oikeusnormeista. Perustuslakiin on toisaalta kirjattu sekkin, että Suomi on Euroopan unionin jäsen (1.3 §).

Oikeusjärjestyksellä tarkoitetaan yleensä jossain valtiossa kuten Suomessa voimassa olevien oikeusnormien muodostamaa kokonaisuutta. Niissä valtioissa,

jotka ovat EU:n jäseniä, tulee kuitenkin oikeudellisia kysymyksiä tarkasteltaessa ottaa huomioon myös erilaiset EU-tason sopimukset ja lainsäädäntötoimet kuten EU:n perussopimukset sekä EU:n asetukset ja direktiivit. Oikeusjärjestyksissä tyypillisesti on voimassa myös sellaisia oikeusnormeja, joita ei voida ainakaan suoraan johtaa kirjoitetusta lainsäädännöstä. Esimerkiksi kotimaisen oikeudenkäymiskaaren (4/1734) 1:11:ssä säädettiin alun perin siitä, että tuomarin ohjeena oli säädetyn lain puuttuessa maan tapa, kunhan tämä tapa ei ollut kohtuuton. Tämä säännös ei enää ole voimassa, mutta sen ilmentämä ajatus kirjoitetun lainsäädännön mahdollisesta epätäydellisyydestä pitää edelleen paikkansa.

Oikeusjärjestykset koskettavat lukuisin tavoin niin ihmisiä kuin erilaisia oikeushenkilöitä. Oikeusnormit määrittävät muun muassa sen, mikä on kiellettyä ja mikä ei. Monet oikeusnormit ovat perusluonteeltaan teknologianeutraaleja, mikä tulee ottaa huomioon myös erilaisia lohkoketjusovelluksia tarkasteltaessa. Se, että lohkoketjuteknologia itsessään on uusi innovaatio, ei näin ollen suinkaan tarkoita sitä, että siihen osalliset tahot toimisivat jonkinlaisessa oikeudellisessa tyhjiössä. Toisaalta tulee ottaa huomioon myös, että lohkoketjuihin sovelletaan pääosin sääntelyä, jota annettaessa ei ole pidetty silmällä lohkoketjuteknologiaa.

Moniin oikeudellisiin kysymyksiin on otettu suoraan kantaa kirjoitetussa lainsäädännössä sellaisella tavalla, että oikeustilaa voidaan pitää sisällöltään selvänä. Tällainen selvyys voidaan saavuttaa myös ilman lainsäädäntöä esimerkiksi tilanteessa, jossa tietty kanta on jo aikaa sitten vakiintunut oikeuskäytännössä. Oikeustila voi kuitenkin olla myös epäselvä. On itse asiassa lukuisia oikeudellisia kysymyksiä, joista asiantuntijatkin ovat eri mieltä. Tällaisia tilanteita syntyy helposti esimerkiksi silloin, kun yhteiskunnassa ilmenevän uudenlaisen ilmiön yhteydessä syntyy kysymyksiä, joihin ei ole lainkaan otettu kantaa kirjoitetussa lainsäädännössä tai jotka synnyttävät tulkintavaikeuksia voimassa olevan lainsäädännön kannalta.

Esimerkiksi bitcoiniin ja muihin sen kaltaisiin virtuaalivaluuttoihin liittyvä suhteellisen paljon oikeudellisia kysymyksiä, joita voidaan pitää enemmän tai vähemmän tulkinnanvaraisina. Tällaista epäselvyyttä ei pidä kuitenkaan liioitella. Vaikka bitcoin ja muut sen kaltaiset virtuaalivaluutat ovat itsessään uudenlainen ilmiö, käytännössä kaikissa oikeusjärjestyksissä on sellaista sääntelyä, jonka voidaan soveltamisalansa yleisyyden vuoksi katsoa koskevan myös monia virtuaalivaluuttoihin liittyviä asioita. Monesti voi tosin olla hankala havaita olennaista varsinkin sen vuoksi, että virtuaalivaluuttoihin liittyy erityispiirteitä, jotka hankaloittavat oikeudellista hahmottamista. Oikeustilan epäselvyys joka tapauksessa vähentyy väistämättä ajan kanssa niin lainsäädännön ja oikeuskäytännön kehittymisen kuin myös oikeuskirjallisuudessa esitettyjen kannanottojen lisääntymisen vuoksi.

Uudet teknologiat tuovat usein mukanaan uudenlaisia oikeudellisia ongelmia, joihin saattaa olla tarve reagoida myös lainsäädännössä. Yhteiskunnallisessa keskustelussa voi esimerkiksi käydä ilmi, että voimassa olevassa oikeusjärjestyksessä suhtaudutaan liian ankarasti tai toisaalta lempeästi johonkin uuden teknologian mahdollistamaan toimintaan. Helposti käy myös niin, että oikeustila joudutaan toteamaan epätarkoituksenmukaisen epäselväksi. Vaikka epäselvyyden voisi odottaa ajan kuluessa katoavan esimerkiksi oikeuskäytännön vuoksi, lainsäätäjä saattaa todeta selkeyttävän lainsäädännön tarpeelliseksi. Selkeyttävä sääntely voi olla erityisen tarpeellista silloin, kun lainkäyttäjän tulkintavalta on vähäisempi. Tämä korostuu erityisesti oikeudenaloilla, joilla laillisuusperiaatteen asema on vahva, kuten rikos- ja vero-oikeudessa.

Myös lohkoketjuteknologia on synnyttänyt painetta kehittää lainsäädäntöä ainakin joissain suhteissa. Jo tällä hetkellä voidaan osoittaa monista valtioista ja EU-tasoltakin sääntelyä, joka selvästi liittyy ainakin tosiasiallisesti lohkoketjuihin. Esimerkiksi voidaan mainita edellä jaksossa 1.1 jo mainittu asetus (EU) 2022/858, jossa muun muassa luodaan oikeudellinen perusta hajautetun tilikirjan teknologiaan perustuvien markkinainfrastruktuurien pilottijärjestelmälle. Toiseksi esimerkiksi käy kotimainen laki virtuaalivaluutan tarjoajista (572/2019), joka puolestaan liittyy läheisesti EU:n viidenteen rahanpesudirektiiviin (EU) 2018/843. Tässä laissa oleva virtuaalivaluutan määritelmä on tosin sitä luontoa, ettei sitä ole suoranaisesti suunnattu juuri lohkoketjupohjaisiin virtuaalivaluuttoihin tai edes hajautetun tilikirjan teknologiaan.

Sellaista lainsäädäntöä, jossa nimenomaisesti tai ainakin tosiasiallisesti otetaan kantaa lohkoketjuihin, tultaneen lähivuosina antamaan enenevässä määrin eri puolilla maailmaa. Nykytilanteen voi olettaa jossain mielessä muistuttavan internetin alkuvaihetta. Monet saattoivat ajatella tuolloin, että internet on jollain tavalla sääntelystä vapaata aluetta, jossa kaikki on mahdollista. Oletus oli erheellinen ainakin siinä mielessä, että internetissäkään toimiminen ei todellisuudessa tapahtunut oikeudellisessa tyhjiössä. Nykyään tämä on merkittävästi aiempaa selvempää, sillä koko joukko lainsäädäntöä on annettu internetiä silmällä pitäen, internetissä toimimista valvotaan monin tavoin ja erilaisia ongelmatilanteita käsitellään tarpeen vaatiessa tuomioistuimissa.

Monet lohkoketjusovellukset saattavat näyttää erityisen hankalilta voimassa olevan sääntelykehikon kannalta sen vuoksi, että sovellukset eivät välttämättä kunnioita valtioiden rajoja. Esimerkiksi Bitcoinin ja Ethereumiin osallistutaan ja niitä käytetään käytännössä globaalisti. Vaikka tästä kansainvälisyydestä epäilemättä koituu erilaisia tulkinta- ja rajanvetovaikeuksia, asian merkitystä ei pidä liioitella. Erilaisia rajat ylittäviä tilanteita on ilmennyt aina, ja internetin kehittyminen on vauhdittanut alan oikeudellista kehitystä. Vaikka erilaisia lohkoketjuspe-



sifejä tulkinta- ja rajanvetovaikeuksia voi tietysti ilmetä, oikeusjärjestyksistä löytyy vastaus myös lohkoketjusovellusten rajat ylittävään luonteeseen liittyviin ongelmiin.

Myös Suomen kannalta on tärkeää, että EU on verraten aktiivisesti seurannut lohkoketjujen ja yleisemmin ottaen hajautetun tilikirjan teknologian kehitystä. Innovaatioita halutaan edistää, mitä muun muassa edellä mainittu asetus (EU) 2022/858 osoittaa. Toisaalta tarvitaan eri tahojen intressit asianmukaisella tavalla huomioon ottavaa sääntelyä. Tällä hetkellä odotukset kohdistuvat ennen muuta kryptovarojen markkinoita koskevaan asetukseen, jota valmistellaan paraikaa Euroopan unionissa. Asetusehdotukseen palataan tämän teoksen 4 luvussa, jossa tarkastellaan lähemmin myös asetusta (EU) 2022/858.

#### **1.4 Teoksessa tarkasteltavista kysymyksistä**

Lohkoketjusovellusten moninaisen luonteen vuoksi niihin voi liittyä monentyyppisiä oikeudellisia kysymyksiä. Kun tällaisiin kysymyksiin lähdetään hakemaan vastausta, tulee ottaa huomioon, että maapallolla on suuri määrä yksittäisiä oikeusjärjestyksiä. Jos halutaan kokonaisvaltainen kuva jonkin globaalisti toimivan lohkoketjusovelluksen oikeudellisesta kohtelusta, tarkkaan tulokseen pääseminen edellyttää lukuisten oikeusjärjestysten tarkastelua. Tästä tulee helposti ylivaikeaa, vaikka kansainvälisen yhteistyön vuoksi voitaisiinkin todeta, että monessa valtiossa noudatetaan identtisiä sääntöjä joissain suhteissa.

Tässä teoksessa käsitellään lohkoketjuja ja lohkoketjusovelluksia oikeudellisen sääntelyn näkökulmasta varsin valikoidusti. Päähuomio on EU-tason sääntelyssä sekä kotimaisessa kansallisessa oikeustilassa, joskin tarkastelu on luonteeltaan laaja-alaisempaa silloin, kun tämä on tarkoituksenmukaista käsiteltävänä olevan kysymyksen kannalta. Jos ajatellaan rajankäyntiä yksityisoikeuden ja julkisoikeuden välillä, teos painottuu ensin mainittuun. Yksityisoikeuteen luetaan yleensä ne oikeusnormit, jotka sääntelevät yksityisten henkilöiden välisiä oikeudellisia suhteita. Muutamaa poikkeusta lukuun ottamatta teoksessa ei juurikaan käsitellä julkisoikeuden piiriin kuuluvia oikeusnormeja eli oikeusnormeja, jotka sääntelevät julkisten yhteisöjen organisaatiota ja toimintaa sekä yksilön asemaa suhteessa julkisyhteisöihin.

Lukijan on hyvä panna merkille, että oikeustila on paraikaa dynaamisten muutosten vaiheessa. Lukuisissa eri valtioissa kuten myös EU:ssa työstetään paraikaa uutta sääntelyä, ja uutta sääntelyä ilmaantuu globaalisti ajatellen liki päivittäin. EU-tasolla tapahtuu tällä hetkellä paljon, sillä EU:n toimielimet kuten komissio ja parlamentti haluavat olla aktiivisesti kehittämässä lohkoketjujen oikeudellista viitekehystä.

Jos huomioon ei oteta teoksen johdantoa ja lopetusta, teoksessa on viisi käsittelylukua. Ensin eli luvussa 2 tarkastellaan bitcoinia ja muita vastaavanlaisia ”originaaleja” virtuaalivaluuttoja, mikä sopii tietyllä tavalla myös lohkoketjuteknologian ajalliseen kehitykseen eli siihen, että lohkoketjuteknologia käytännössä yleistyí juuri bitcoinin kautta. Luvussa 3 puolestaan käsitellään älysovimuksia yleisesti ja erityisesti sopimusoikeuden näkökulmasta. Oma lukunsa on omistettu *Initial Coin Offering*- eli ICO-ilmioille, jota tarkastellaan 4 luvussa, jossa käsitellään yleisesti myös erilaisia tokeneita eli rahakkeita. Luvussa 5 puolestaan tarkastellaan lohkoketjuja ja lohkoketjusovelluksia eurooppalaisen tietosuojalainsäädännön näkökulmasta. Viimeisessä varsinaisessa käsittelyluvussa eli 6 luvussa nostetaan esille erilaisia immateriaalioikeudellisia näkökohtia siten, että erityistarkastelun kohteeksi otetaan viime aikoina paljon osakseen huomiota saanut taiteen tokenisointi lohkoketjuteknologiaa hyväksi käyttäen.

## **2 BITCOIN JA MUUT VASTAAVANLAISET ORIGINAALIT VIRTUAALIVALUUTAT**

### **2.1 Virtuaalivaluutta objektina ja varallisuusosoikeuksien kohteena**

Omaisuus koostuu varallisuusosoikeuksista, joiden tyypillisesti sanotaan kohdistuvan johonkin. Esimerkiksi saamisoikeuden välittömäksi kohteeksi jäsentyy henkilö, jota kutsutaan velalliseksi. Saamisoikeuden haltijaa puolestaan sanotaan velkojaksi, joka voi edellyttää velalliselta suoritusta, jonka tekemisellä velallinen täyttää velvoitteensa. Muina varallisuusosoikeuksina voidaan mainita vaikkapa teokseen kohdistuva tekijänoikeus ja omistusoikeus, joka perinteisesti on ymmärretty kiinteään tai irtaimen esineeseen kohdistuvaksi oikeudeksi. Omistusoikeus voi kohdistua esimerkiksi kiinteistöön, ajoneuvoon tai tynnyrilliseen öljy.

Monissa lohkoketjusovelluksissa voidaan tunnistaa varallisuusosoikeuksia, jotka kohdistuvat perinteisen varallisuusosoikeuden järjestelmän mukaisiin kohteisiin. Bitcoin ja muut sitä vastaavat originaalit virtuaalivaluutat merkitsevät kuitenkin haastetta perinteiselle tavalle hahmottaa varallisuusosoikeuksia ja niiden kohteita. Niissä ei loppujen lopuksi ole kyse muusta kuin hajautetusti ylläpidetyn tietojärjestelmän sisällöstä eli viime kädessä siitä, että binäärijärjestelmän mukaiset luvut, nollat ja ykköset, on järjestetty tietyllä tavalla. Tällaisilla yksityisillä virtuaalivaluutoilla ei ole varsinaista substanssiarvoa, taustallaan julkisvallan auktoriteettia samoin kuin virallisilla fiat-valuutoilla (valuutoilla, joiden arvo ja asema perustuu sääntelylle ja keskuspankeille) eikä myöskään laillisen maksuvälineen asemaa, minkä vuoksi ne saattavat näyttää olevan tietyllä tavalla tyhjän päällä. Toisaalta esimerkiksi bitcoineilla on huomattavasti arvoa, ja kaikkien bitcoinien yhteenlaskettu arvo on lähes 400 miljardia euroa tätä kirjoitettaessa. Johtuipa tämä luottamuksesta Bitcoin-järjestelmään vai jostain muusta seikasta, lukuisat henkilöt ovat valmiita maksamaan suuria summia, jotta hajautetun tietojärjestelmän tietoja muutettaisiin heidän haluamaansa suuntaan. Bitcoin-järjestelmä on luotu siten, että tietojärjestelmän sisällöstä voidaan määrätä tavalla, jonka myötä bitcoineja voidaan käyttää muun muassa maksuvälineenä.

Bitcoin ja muut sitä vastaavat virtuaalivaluutat ovat saaneet oikeustieteilijät useissa maissa keskustelemaan käsitteellisistä lähtökohdista. Erilaisten kansallisten traditioiden näkökulmasta on voinut olla relevanttia kysyä, millaisesta omaisuuden lajista on kyse, tai onko ylipäätään perusteltua puhua omaisuudesta virtuaalivaluuttojen yhteydessä.

Kotimaisessa lainsäädännössä on lukuisia säännöksiä, joissa puhutaan omaisuudesta. Esimerkiksi holhoustoimilain (442/1999) 23.1 §:ssä lähdetään siitä, että

vajaavaltaisella ei ole oikeutta itse vallita omaisuuttaan. Säännöstä voidaan epäilemättä tulkita siten, että vajaavaltaiselle, jolla holhoustoimilaisissa tarkoitetaan alle 18-vuotiasta tai täysi-ikäistä vajaavaltaiseksi julistettua, kuuluvat bitcoinit ja muusta vastaavanlaisesta originaalista virtuaalivaluutasta koostuva varallisuus ovat omaisuutta. Ainakin varallisuus oikeuden alalla voidaan myös yleisemmin lähteä siitä, että *tarkastellun kaltaiset originaalit virtuaalivaluutat ovat omaisuutta*. Kun oikeustieteellisissä yhteyksissä käsitellään kotimaista varallisuus oikeuden järjestelmää, huomioon tulee ottaa myös bitcoinin kaltaiset virtuaaliset valuutat omana erityisenä objektityypinään, joka voidaan rinnastaa objektina esimerkiksi teokseen tai irtaimeen esineeseen.

Kun esimerkiksi tietyn kiinteistön tai ajoneuvon sanotaan kuuluvan jollekulle, silmällä pidetään juuri tiettyyn kiinteistöön tai ajoneuvoon kohdistuvaa omistusoikeutta. Vastaava pätee paikkansa myös bitcoinin ja muiden vastaavanlaisten originaalien virtuaalivaluuttojen osalta. Kun jotain henkilöä pidetään esimerkiksi bitcoinien omistajana, silmällä täytyy pitää joitain tiettyjä bitcoineja. Vaikka kyse lopulta on vain hajautetun tietojärjestelmän sisällöstä, voidaan hyväksyä kielenkäyttö, jonka mukaan tileillä tai osoitteissa on tietty määrä virtuaalista valuuttaa. Esimerkiksi Bitcoin-järjestelmässä tällainen saldoajattelu merkitsee yksinkertaisuudesta senkin vuoksi, että lohkoketjuun sijoitetaan oikeastaan tiedot transaktioista, joista voidaan laskea bitcoinien määrä. Mahdollisuus määrätä bitcoineista kytkeytyy puolestaan osoitteeseen tavalla, joka ainakin maallikoiden ymmärryskyvyn ja tarpeiden näkökulmasta oikeuttaa puhumaan osoitteissa tai tileillä olevista bitcoineista.

Ei ole aivan selvä, mikä tarkkaan ottaen tulee hahmottaa objektiksi tiettyssä osoitteessa ”olevia” virtuaalisia varoja tarkasteltaessa. Silloin kun ei ole mitään keinoa erottaa valuutta- tai varallisuusyksiköitä toisistaan, tuntuu luontevalta lähteä siitä, että *osoitteeseen liittyvät varat muodostavat yhden objektin*. Perinteisestä esinejärjestelmästä voidaan ottaa vertailukohdaksi esimerkiksi tiettyssä öljysäiliössä oleva öljy tai perunalarissa oleva erä perunoita. Kummassakin tapauksessa esineeksi voidaan käsittää kyseessä oleva yksilöity erä öljyä tai perunoita, vaikka perunan tapauksessa on mahdollista käsittää kukin yksittäinen peruna vielä itsessään esineeksi. Tiettyssä osoitteessa olevia virtuaalivaluutan yksiköitä kuten bitcoineja saatetaan myös verrata tiettyssä mielessä vaikkapa arvo-osuustilillä oleviin arvo-osuuksiin ja myös pankkirahaan, jonka yhteydessä vakiintuneesti puhutaan tiettyllä tilillä olevista varoista, vaikka tilimerkinnot tarkkaan ottaen ilmentävät pankin ja sen asiakkaan välisen velkasuhteen sisältöä. Verrattaessa esimerkiksi bitcoinia pankkirahaan tulee kuitenkin pitää mielessä, että Bitcoin-järjestelmässä ei ole tahoja, jota voitaisiin pitää velallisenä siten kuin pankkia pankkirahan yhteydessä. Bitcoineissa käytettävät yksiköt perustuvat vain teknisiin rajoituksiin eli käytettävien bittien määrään; pienin mahdollinen yksikkö on 0,00000001 bitcoinia, kun

taas euromääräisen tilirahan tapauksessa mahdollista on käyttää ainoastaan pienintä sallittua rahayksikköä eli senttiä.

Bitcoineista tai muista vastaavista virtuaalivaluutoista koostuvien omaisuuserien osalta ei voida tunnistaa niiden sijaintia samoin kuin esimerkiksi öljyerän sijaintia, vaikka tekniseltä kannalta voidaan tietysti todeta, että tietoa viime kädessä aina varastoidaan tietyissä paikoissa. Myös valtion rajat ylittyvät helposti, eli kyse voi olla käytännössä globaalisti pidetystä tietokannasta. Tästä koituu erinäisiä ongelmia pohdittaessa, minkä valtion oikeusjärjestys erilaisiin virtuaalista omaisuutta koskeviin oikeuskysymyksiin soveltuu. Esimerkiksi tavanomaisten irtainten esineiden osalta jotkin kysymykset ovat luonteeltaan sellaisia, että ne ratkeavat esineen sijaintipaikan oikeusjärjestyksen perusteella. Jos virtuaalisen valuutan osalta halutaan vastaavalla tavalla kysyä ”sijaintipaikkaa”, yksi vaihtoehto olisi antaa ratkaiseva merkitys sille, minkä valtion alueelle asettuu kyky määrätä omaisuudesta eli yksinkertaistettuna yksityisen avaimen sijainti, joka saattaa konkreettisesti merkitä esimerkiksi avaintiedot sisältävän muistilaitteen kuten muistitikun ja periaatteessa myös avaimen tietävän henkilön sijaintia. Toisaalta on aiheellista kysyä, onko ylipäättään tarvetta pyrkiä imitoimaan niitä oppeja, jotka on suunnattu irtaimiin esineisiin. Muuta tarkoittavan erityissääntelyn puitteissa tuntuu tosin siltä, että irtaimia esineitä koskevat opit sopivasti sovellettuna tarjoavat käyttökelpoisen lähtökohdan.

Jos tietyllä tilillä olevat varat voivat kuulua jollekulle, tulee huomioon ottaa sekin, että niihin ehkä voi soveltuvan oikeusjärjestyksen mukaan kohdistua muitakin varallisuusoikeuksia. Tarkastellaan vaikkapa tilannetta, jossa A on ottamassa euromääräistä luottoa B:ltä, joka ei kuitenkaan tyydy pelkästään siihen, että hän saisi rahamääräisen saamisoikeuden A:ta kohtaan. B haluaa myös vakuuden siltä varalta, että A jättää velkansa maksamatta. A kertoo tällöin B:lle, että hänellä on tietyllä tilillä bitcoineja, joita A voisi käyttää vakuutena. Luototus järjestyykin. Osapuolet menettelevät vakuuden osalta siten, että A siirtää tilillään olevat bitcoinit B:n juuri vakuutta varten perustettuun osoitteeseen, johon B:llä yksin on yksityinen avain. Osapuolten tarkoituksena on, että B ei saa määrätä millään tavalla osoitteessa olevista varoista. Jos kuitenkin A jättää velkansa maksamatta, B saa muuntaa tarvittavan määrän bitcoineja euroiksi ja ottaa itselleen velkaa vastaavan suorituksen euroista.

Oikeusjärjestyksissä tyypillisesti tunnistetaan panttioikeudeksi kutsuttu varallisuusoikeus ja se, että omaisuutta on mahdollista pantata toisen hyväksi. Esimerkiksi Suomessa on paljon panttaukseen soveltuvaa sääntelyä. Vaikka kutakin säännöstä tulee tarkastella erikseen, liikkeelle voinee monesti lähteä siitä, että esimerkkinä B:lle on perustettu sääntelyssä tarkoitettu panttioikeus. Saatetaanpa pohtia, olisiko panttaus voitu toteuttaa niinkin, että A olisi antanut B:lle oman

tilinsä yksityisen avaimen ja samalla tehokkaasti hävittänyt yksityisen avaimen itseltään. Jos tietyssä osoitteessa olevista varoista määrääminen edellyttää yhtä useampaa yksityistä avainta (tämäkin on teknisesti mahdollista), panttauksen voinee toteuttaa tehokkaasti niin, että yksi vaadittavista avaimista on yksin pantinsaajan tiedossa.

Tietyssä osoitteessa olevat varat eivät siis välttämättä kuulu sille henkilölle, joka tietää niin yksityisen avaimen kuin siihen liittyvän julkisen avaimen. Onkin tärkeätä erottaa *tosiasiallinen määräysvalta varallisuus oikeuksien tasosta*. Aina tulee kysyä erikseen, kenelle esimerkiksi tietyt bitcoinit kuuluvat. Mahdollista on tietysti sekin, että jotkin varat ovat kahden tai useamman henkilön yhteisomistuksessa. Oikeudellisten virhepäätelmien riski on suuri, jos olettaa suoraviivaisesti, että julkisen ja yksityisen avaimen tietäminen automaattisesti aineellisen normiston kannalta synnyttää joitain oikeuksia niihin varoihin, joista määräämiseen tieto antaa mahdollisuuden.

## 2.2 Tunnistautumiseen liittyvistä ongelmista ja niiden ratkaisemisesta

Moniin originaaleihin virtuaalivaluuttoihin on helppo päästä osalliseksi. Esimerkiksi bitcoinien hallinnointi edellyttää sähköistä lompakkoa, jonka hankkiminen käy verraten helposti eli käytännössä lompakko-ohjelman asentamisella. Lompakoilla on käytännön toimintojen kannalta niin suuri merkitys, että se näkyy myös kielenkäytössä. On muun muassa verraten tavallista puhua lompakossa olevista virtuaalivaluutoista, eli lompakko rinnastuu tässä mielessä perinteisiin fyysisiin lompakoihin, joissa säilytetään seteleitä ja kolikoita.

Siinä missä esimerkiksi pankilla tai vastaavalla on velvollisuus tuntea asiakkaansa, virtuaalisesta valuutasta koostuvia varallisuususeriä voi monesti hallita ja käyttää ilman, että käyttäjä olisi tunnistettu vastaavalla tavalla kuin pankkijärjestelmässä. Esimerkiksi bitcoineja voi ryhtyä käyttämään ilman mitään erityistä rekisteröitymis- tai tunnistautumismenettelyä.

Erot pankkijärjestelmään johtuvat paljolti siitä, että originaalit virtuaalivaluutat perustuvat tyypillisesti hajautetuille järjestelmille, joissa ei samoin kuin pankkijärjestelmässä ole tunnistautumisesta huolehtivaa tahoa. Vaikka tunnistautumisen puuttuminen on saattanut olla omiaan lisäämään virtuaalisten valuuttojen kuten bitcoinin suosiota, anonymisuus tai pseudonymisuus on ongelmallista muun muassa rahanpesun ja rikollisen toiminnan kannalta. Monet virtuaalisen valuutan järjestelmät merkitsevät ainakin perusmuodossaan merkittävää riskiä myös käyttäjille. Jos esimerkiksi tietyssä lompakossa olevat bitcoinit omistava A menettää tiedon yksityisestä avaimesta, ei lähtökohtaisesti ole ketään pankkijärjestelmän mukaiseen pankkiin rinnastuvaa tahoa, jonka avulla A voisi saada takaisin tosiasiallisen mahdollisuuden määrätä varoista. Yksityisen avaimen hukkaaminen

rinnastuu käteisten rahavarojen hukkaamiseen tosiasiallisesti peruuttamattomalla tavalla. Mikäli A toisaalta esimerkiksi siirtää bitcoineja erehdyksessä väärään osoitteeseen, hän ei voi samoin kuin pankkirahan yhteydessä pyrkiä selvittämään pankin tai pankkien avulla vastaanottajan henkilöllisyyttä eivätkä asiaa mahdollisesti tutkivat viranomaisetkaan voi hankkia tietoja samoin kuin pankkijärjestelmässä.

Virtuaalisen varallisuuden ympärille on käytännössä rakentunut jo moninaista palvelutoimintaa, jonka avulla käyttäjät voivat muun muassa vähentää riskejään. Kyse voi olla esimerkiksi säilyttämiseen liittyvästä palvelusta. Tällaisen palvelutoiminnan olemassaolo on merkittävää myös lainsäätäjän kannalta, sillä palvelua tyypillisesti tarjoaa yksittäinen oikeushenkilö. Lainsäädännössä voidaan varsin helpostikin asettaa tällaisille palveluntarjoajille erilaisia velvollisuuksia, kuten velvollisuus tunnistaa asiakkaansa ja pitää asiakkaista rekisteriä. Sama koskee myös muun muassa sellaisia tahoja, jotka vaihtavat virtuaalista varallisuutta euron ja dollarin kaltaisiin fiat-valuuttoihin.

Tunnistautumiseen liittyviin ongelmiin on kiinnitetty huomiota EU-tasolla erityisesti rahanpesun näkökulmasta. Viidennellä rahanpesudirektiivillä laajennettiin direktiivin (EU) 2015/849 eli ns. neljännen rahanpesudirektiivin soveltamisalaa siten, että myös virtuaalivaluuttojen ja fiat-valuuttojen välisten vaihtopalvelujen sekä lompakkopalvelujen tarjoajat otettiin sääntelyn piiriin. Virtuaalivaluutat määritettiin direktiivin 3 artiklassa digitaalisiksi arvonkantajiksi, ”jotka eivät ole keskuspankin tai viranomaisen liikkeeseen laskemia tai takaamia, joita ei välttämättä ole kytketty lailliseksi maksuvälineeksi vahvistettuun valuuttaan ja joilla ei ole samaa oikeudellista asemaa kuin valuutalla tai rahalla mutta jotka luonnolliset henkilöt tai oikeushenkilöt hyväksyvät vaihdantavälineenä ja joita voi siirtää, varastoida ja myydä sähköisesti”.

Virtuaalivaluutan käsitettä ei mainitun määritelmän puitteissa ole kytketty lohkoketjuteknologian hyödyntämiseen, joten sääntelyn merkitys ei rajoitu lohkoketjusovelluksiin. Määritelmän tulkinnanvaraisin kohta lienee vaatimus siitä, että arvonkantaja hyväksytään ”vaihdantavälineenä”. Tämä tuntuisi ainakin ensi katsannossa viittaavaan jonkinlaiseen tosiasialliseen asemaan taloudessa. Vaihdantaväline (direktiivin englanninkielisessä versiossa käytetään termiä *means of exchange*) viittaa yleisesti ottaen kohteeseen, jonka esimerkiksi tuotteen myyjä on valmis ottamaan vastaan, koska myyjä tietää muidenkin hyväksyvän kohteen vastaavalla tavalla. Vaihdantavälineen asema ei sinänsä tarkoita sitä, ettei arvonkantajalla voisi olla muutakin merkitystä, esimerkiksi sijoituskohteena.

Ei ole kuitenkaan selvä, että vaatimuksella ”luonnolliset henkilöt tai oikeushenkilöt hyväksyvät vaihdantavälineenä” olisi edellä mainittu sisältö. Päinvastoin voidaan esittää perusteluja kannalle, jonka mukaan direktiiviä (EU) 2018/843

annettaessa pyrittiin laajempaan ja melko kattavaan virtuaalivaluutan käsitteeseen. Esimerkiksi direktiivin johdanto-osan 10 perustelukappaleessa kerrotaan seuraavaa:

Virtuaalivaluuttoja ei pitäisi sekoittaa Euroopan parlamentin ja neuvoston direktiivin 2009/110/EY 2 artiklan 2 alakohdassa määriteltyyn sähköiseen rahaan, Euroopan parlamentin ja neuvoston direktiivin (EU) 2015/2366 4 artiklan 25 alakohdassa määriteltyyn laajempaan ”varojen” käsitteeseen eikä rahalliseen arvoon, joka on tallennettu välineisiin, joille on myönnetty poikkeus direktiivin (EU) 2015/2366 3 artiklan k ja l alakohdassa, eikä pelin sisäisiin valuuttoihin, joita voidaan käyttää yksinomaan tietyssä peliympäristössä. Vaikka virtuaalivaluuttoja voidaan useasti käyttää maksuvälineenä, niitä voitaisiin myös käyttää muihin tarkoituksiin ja soveltaa laajemmin, kuten vaihdanta- tai investointivälineenä, arvon säilyttäjinä tai verkkokasinokäytössä. Tämän direktiivin tavoitteena on kattaa virtuaalivaluuttojen kaikki mahdolliset käytöt.

Sääntelyä voidaan kaiken kaikkiaan pitää yllättävänkin epäselvänä sen suhteen, kuinka laaja virtuaalivaluutan määritelmä direktiivissä (EU) 2018/843 on omaksuttu. Erilaisia mielipiteitä onkin esitetty sen osalta, kattaako määritelmä myös esimerkiksi sellaiset digitaaliset rahakkeet, jotka synnyttävät haltijalleen oikeuden saada jokin suoritus rahakkeen liikkeeseenlaskijalta. Päähuomio lienee joka tapauksessa ollut siinä, että sääntelyllä vähennetään bitcoinin kaltaisiin originaaleihin virtuaalivaluuttoihin liittyviä ongelmia rahanpesun näkökulmasta. Mainittakoon vielä, että direktiivin (EU) 2018/843 johdanto-osan 11 perustelukappaleessa on erikseen todettu:

Paikallisvaluuttoja, joista käytetään myös nimitystä rinnakkaisvaluutat, joita käytetään rajoitetuissa verkostoissa, kuten tietyssä kaupungissa tai tietyllä alueella ja pienen käyttäjäjoukon keskuudessa, ei tulisi pitää virtuaalivaluuttoina.

Keskeinen direktiivimuutoksen seurauksena annettu kotimainen säädös on laki virtuaalivaluutan tarjoajista (572/2019; VvTL), jossa virtuaalisen valuutan tarjoajalla tarkoitetaan virtuaalivaluutan liikkeeseenlaskijaa, virtuaalivaluutan vaihtopalvelua ja sen markkinapaikkaa sekä lompakkopalvelun tarjoajaa (2.1 §:n 2 kohta). Sitä, että myös virtuaalivaluutan liikkeeseenlaskijat ovat sääntelyn piirissä, ei edellytetä direktiivissä (EU) 2018/843. Hallituksen esityksessä eduskunnalle laiksi pankki- ja maksutilien valvontajärjestelmästä ja eräksi siihen liittyviksi laeiksi (HE 167/2018 vp), joka sisälsi myös ehdotuksen laiksi virtuaalivaluutan tarjoajista, pidettiin virtuaalivaluuttaan liittyvien riskien vuoksi perusteltuna, että laki koskee myös liikkeeseenlaskijaa. Esityksessä nimenomaisesti viitataan käsillä olevan teoksen 4 luvussa lähemmin tarkasteltaviin, ICO-lyhenteellä kulkeviin järjestelyihin (s. 84): ”Erityisesti väärinkäytöksiä on havaittu niin sanottujen Initial Coin Offeringin (ICO) yhteydessä, jossa liikkeeseenlaskija kuvaa virtuaalivaluutan ominaisuuksia, käyttötarkoitusta ja liikkeeseenlaskun ehtoja.”



Virtuaalivaluutan liikkeeseenlaskijalla tarkoitetaan virtuaalivaluutan tarjoajista annetussa laissa luonnollista henkilöä tai oikeushenkilöä, joka laskee virtuaalivaluutan liikkeelle (VvTL 2.1 §:n 3 kohta). Hallituksen esityksessä katsottiin, ettei virtuaalivaluutalla aina ole sääntelyssä tarkoitettua liikkeeseenlaskijaa. Esityksessä muun muassa kerrotaan (s. 48):

Virtuaalivaluutoille voidaan joissakin tapauksessa yksilöidä liikkeeseenlaskija. Tällöin kyseessä on niin sanottu keskitetty järjestelmä. Hajautetussa järjestelmässä, kuten Bitcoinin taustalla olevassa järjestelmässä, liikkeeseenlaskijaa ei pystytä yksilöimään. Kun liikkeeseenlaskija pystytään määrittämään, sille voidaan asettaa myös velvollisuuksia.

Samaan tapaan lain 2 §:n määritelmäpykälän yksityiskohtaisten perustelujen yhteydessä (s. 84) lausutaan:

Virtuaalivaluutta on aina digitaalisessa muodossa. Sillä voi olla liikkeeseenlaskija tai se voi perustua hajautettuun järjestelmään, kuten Bitcoinin taustalla olevaan lohkoketjuteknologiaan.

Jotta henkilö voisi olla virtuaalivaluutan liikkeeseenlaskija, virtuaalivaluutan tunnusmerkkien pitää täytyä. Virtuaalivaluutan tarjoajista annetussa laissa virtuaalivaluutalla tarkoitetaan lain 2.1 §:n 1 kohdan mukaan digitaalisessa muodossa olevaa arvoa:

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

Erityisesti b alakohta saattaa aiheuttaa tulkintaongelmia. Joudutaan esimerkiksi kysymään, sisältääkö maksuvälineenä käyttäminen myös jonkinlaisen teoreettisen mahdollisuuden maksukäyttöön. Kun ajatellaan liikkeelle laskemisen hetkeä, ainakin toisinaan voisi kuvitella hankalaksi määrittää, voiko liikkeelle laskettua digitaalisessa muodossa olevaa arvoa käyttää maksuvälineenä tai täytyykö edes ”arvon” vaatimus. Tulkintaongelmiin palataan tämän teoksen 4 luvussa.

Virtuaalivaluutan tarjoajista annetussa laissa on asetettu lukuisia erilaisia velvollisuuksia niin virtuaalivaluutan liikkeeseenlaskijalle kuin virtuaalivaluutan vaihtopalvelun ja sen markkinapaikan sekä lompakkopalvelun tarjoajalle. Elinkeinonharjoittaja saa esimerkiksi yleensä tarjota virtuaalivaluuttaan liittyviä palveluita vain, jos se on rekisteröity säädöksen mukaisesti virtuaalivaluutan tarjoajaksi. Virtuaalivaluuttaan liittyvällä palvelulla tarkoitetaan VvTL 2.1 §:n 6 kohdan mukaan virtuaalivaluutan liikkeeseenlaskua, virtuaalivaluutan vaihtopalvelua ja lompakkopalvelun tarjoamista. Virtuaalivaluutan tarjoajan on VvTL 13 §:n mukaan

myös tunnettava asiakkaansa. Laissa on lisäksi sääntelyä muun muassa asiakasvarojen säilyttämisestä, markkinoinnista sekä palveluihin liittyvien asiakirjojen ja tietojen säilyttämisestä.

Asiakkaan tuntemista koskeva velvollisuus koskettaa lainsäädännön mukaan yleisesti virtuaalivaluutan tarjoajia. Kyse on näin ollen myös liikkeeseenlaskijaa koskevasta velvollisuudesta. Oikeuskirjallisuudessa Kristian Keskitalo ja Jaakko Väyrynen ovat pohtineet artikkelissaan *Virtuaalivaluutan tarjoajan asiakkaan tuntemisvelvollisuus – liikkeellelaskijaa koskevat erityiskysymykset* (Liikejuridiikka 3/2022 s. 45–64), voiko asiakkaan tuntemisvelvollisuus kohdistua myös niihin kolmansiin tahoihin, joille liikkeelle laskijalta virtuaalivaluutan saanut henkilö on luovuttanut virtuaalivaluutan. Kirjoittajat suhtautuvat epäillen tähän tulkintaan, ja he suhtautuvat kriittisesti myös siihen, että laki virtuaalivaluutan tarjoajista ylipäätään ulotettiin myös liikkeeseenlaskijoihin.

Virtuaalivaluutan tarjoajista annetun lain ja sen nojalla annettujen säännösten ja määräysten noudattamisen valvominen kuuluu VvTL 3 §:n mukaan Finanssivalvonnalle. Sen lisäksi, että Finanssivalvonnasta on annettu oma lakinsa, virtuaalivaluutan tarjoajista annetussa laissa on verraten paljon sääntelyä Finanssivalvonnan tehtävistä, oikeuksista ja velvollisuuksista. Finanssivalvonta esimerkiksi pitää rekisteriä virtuaalivaluutan tarjoajista. Finanssivalvonta voi myös antaa tarkempia määräyksiä muun muassa asiakkaan tuntemisessä noudatettavista menettelytavoista. Finanssivalvonta antoi 14.6.2019 virtuaalivaluutan tarjoajista määräyksiä ja ohjeita, jotka tulivat voimaan 1.7.2019 (Määräykset ja ohjeet 4/2019).

### 2.3 Laillinen maksuväline vai jotain muuta?

Laillisesta maksuvälineestä puhuttaessa viitataan yleensä siihen, ettei velkoja voi kieltäytyä maksusta, jota tarjotaan laillisen maksuvälineen muodossa. Esimerkiksi euroalueella laillisia maksuvälineitä ovat etenkin säädettyssä järjestyksessä liikkeelle lasketut eurosetelit. Myös kolikot voivat olla laillisia maksuvälineitä, joskin kolikkoihin pätee monilla valuutta-alueilla erityissääntöjä kuten se, ettei ainakaan kaikkien velkojien tarvitse ottaa samalla kertaa vastaan tietyn arvon tai kolikkojen lukumäärän ylittävää suoritusta. Vaikka laillisen maksuvälineen (englanniksi *legal tender*) käsite sinänsä on yleisesti tunnettu ja käytetty, yksityiskohtin mentäessä joudutaan havaitsemaan, ettei käsitteelle välttämättä löydy täysin yleisesti hyväksyttyä sisältöä. Saatetaan esimerkiksi kysyä, riittääkö lailliseksi maksuvälineeksi katsomiseen, että julkisten toimijoiden tulee ottaa vastaan tietyllä välineellä suoritettut maksut. Huomiota saatetaan kiinnittää myös siihen, millaisessa yksikössä lakiperusteiset maksuvelvollisuudet syntyvät ja kuinka hinnat tulee esittää tuotteita markkinoitaessa. Kun laillinen maksuväline ymmärretään sopivasti, jopa bitcoin voidaan katsoa lailliseksi maksuvälineeksi ainakin joissain maissa kuten El Salvadorissa, jossa toteutettiin vuonna 2021 varsin mittava bitcoinin ympärille

rakentuva rahauudistus ja jossa bitcoin itse asiassa täyttää verraten monet laillisen maksuvälineen tyypilliset tunnusmerkit. El Salvador luopui omasta kansallisesta valuutasta jo vuonna 2001, jolloin se ryhtyi käyttämään Yhdysvaltain dollaria, jolla nykyisin lienee rinnakkaisasema bitcoinin kanssa.

Virtuaalivaluutoista puhuttaessa lähdetään useimmissa maissa liikkeelle siitä, ettei kyse ole laillisesta maksuvälineestä. Esimerkiksi virtuaalivaluutan tarjoajista annetussa laissa tarkoitetaan virtuaalivaluutalla digitaalisessa muodossa olevaa arvoa vain tiettyjen edellytysten täytyessä. Yksi näistä edellytyksistä on, että kyseessä on arvo, jota keskuspankki tai muu viranomainen ei ole laskenut liikkeeseen ja joka ei ole laillinen maksuväline. On sinänsä täysin mahdollista, että lohkoketjua hyväksi käyttäen laskettaisiin liikkeelle sellaisia objekteja, joille annettaisiin lainsäädännössä laillisen maksuvälineen asema. Euroalueella tällaista sääntelyä ei ole annettu, mutta jos tällaiseen ratkaisuun päädyttäisiin, kyse ei olisi virtuaalivaluutan tarjoajista annetussa laissa tarkoitettua virtuaalisesta varallisuudesta, vaan laillisesta maksuvälineestä. Perusteeksi säädöksen soveltumattomuudelle nousisi todennäköisesti myös, että kyse olisi keskuspankin tai muun viranomaisen liikkeelle laskemasta digitaalisesta arvosta.

Laillisen maksuvälineen asema ei loppujen lopuksi ole aivan niin tärkeä kuin ensi katsannossa voisi kuvitella. Esimerkiksi Euroopan komissio on katsonut 22.3.2010 antamassaan suosituksessa euroseteleiden ja -metallirahojen laillisen maksuvälineaseman soveltamisalasta ja vaikutuksista (2010/191/EU), että laillisen maksuvälineaseman olisi ensinnäkin merkittävä pakollista hyväksymistä. Tällä tarkoitetaan, että ”[m]aksuvelvoitteen velkoja ei voi kieltäytyä ottamasta vastaan euroseteleitä ja -metallirahoja, jolleivät osapuolet ole sopineet muusta maksutavasta”. Lisäksi laillinen maksuvälineasema merkitsee hyväksymistä täydestä nimellisarvosta (”Euroseteleiden ja -metallirahojen arvo vastaa seteleissä ja kolikoissa ilmoitettua määrää”) ja maksuvelvollisuudesta vapautumista (”Velallinen voi vapautua maksuvelvoitteesta tarjoamalla velkojalle euroseteleitä ja -metallirahoja”).

Pakollinen hyväksyminen ei siis ole ehdotonta vaan edellyttää sitä, ettei muusta maksutavasta ole sovittu. Esimerkiksi kaupanteossa vallitsee ainakin lähtökohteisesti sopimusvapaus siten, että osapuolet voivat haluamallaan tavalla sopia siitä, kuinka maksu on tehtävä. Näin voidaan sopia esimerkiksi siitä, että A luovuttaa B:lle omistusoikeuden johonkin irtaimeen esineeseen sitä vastaan, että B puolestaan velvoittautuu luovuttamaan A:lle esimerkiksi 0,1 bitcoinia. Onpa mahdollista sekin, että B velvoittautuu tekemään A:lle suorituksen euroissa tai dollareissa mutta että B vapautuu velvoitteestaan siinäkin tapauksessa, että hän luovuttaa A:lle 0,1 bitcoinia. Johonkin virtuaalivaluuttaan on mahdollista päätyä myös siten, että B:llä on sopimus- tai lakiperusteisesti syntynyt velvoite esimerkiksi euro- tai dollarimääräiseen suoritukseen mutta että B sopii velkojansa A

kanssa myöhemmin siitä, että B:llä on mahdollisuus vapautua velvoitteestaan myös virtuaalivaluutan luovutuksella tai että B:n täytyykin luovuttaa A:lle juuri virtuaalivaluutaa.

Laillisen maksuvälineen asema ei myöskään ole varsinaisesti rahan tunnusmerkki, joskin paljon riippuu tietysti siitä, kuinka ”raha” tässä yhteydessä ymmärretään. Jos raha ymmärretään eritoten vaihdon välineeksi, rahaksi käy periaatteessa mikä tahansa kohde, joka yhteiskunnassa hyväksytään rahaksi. Viime kädessä kyse on moninkertaisesta uskomusjärjestelmästä. Esimerkiksi euroalueella setelit ja kolikot ovat talousjärjestelmän kannalta rahaa sen vuoksi, että olemme valmiit myymään esimerkiksi meille kuuluvia hyödykkeitä seteleitä ja kolikoita vastaan, koska uskomme muidenkin arvostavan seteleitä ja kolikoita siinä määrin, että he ovat valmiit tarjoamaan meille tavaroita ja palveluita niitä vastaan.

Tunnetuimmatkin originaalit virtuaalivaluutat ovat toimineet varsin heikosti todellisina maksuvälineinä. Vaikka sopijakumppanit voivat määrittää maksutavan haluamallaan tavalla, esimerkiksi bitcoinin tai etherin varaan rakentuvat maksujärjestelyt ovat edelleen suhteellisen harvinaisia. Oma lukunsa ovat toki ne järjestelyt, jotka on toteutettu lohkoketjuympäristössä tai muuten sellaisessa digitaalisessa ympäristössä, johon lohkoketjupohjainen maksaminen sopii luontevasti. Esimerkiksi voidaan ajatella vaikkapa Ethereum-järjestelmässä toteutettua sovellusta, jossa edellytetään myös maksutoimintoja ja joka on tekniseltään toteutukseltaan sellainen, että maksun tulee tapahtua juuri ethereiden avulla.

Se, että esimerkiksi nykymuotoinen bitcoin voisi muodostua tavanomaiseksi maksuvälineeksi esimerkiksi päivittäistavarakaupassa, tuntuu verraten epätodennäköiseltä. Maksujen käsittely ei yksinkertaisesti tapahdu vaaditulla nopeudella, ja Bitcoin-järjestelmä joutuisi hankaluuksiin jo tapahtumien valtavan määrän vuoksi. Tähän on tosin kehitetty jo erilaisia teknisiä ratkaisuja, ja esimerkiksi Lightning Network-protokollan käyttö mahdollistaa nopeamman maksujen käsittelyn ja sujuvamman maksamisen. Lightning Network -protokollaan perustuva lompakko on käytössä esimerkiksi El Salvadorissa, jossa bitcoin on hyväksytty viralliseksi maksuvälineeksi.

Hitausongelmat voivat siis olla ratkaistavissa teknisin innovaatioin. On myös hyvä panna merkille, että esimerkiksi Ethereum-järjestelmä on merkittävästi Bitcoin-järjestelmää nopeampi toiminnoissaan etenkin pitkään suunnitellussa, syksyllä 2022 toteutetussa *The Merge* -päivityksessä (aiemmin Ethereum 2.0) omaksutun *proof-of-stake*-konsensusmekanismin ansiosta (ns. osakkuusvarmennus). Jäljelle jää kuitenkin kysymys, miksi kuluttajat ja elinkeinonharjoittajat ylipäätään haluaisivat ottaa käyttöön bitcoinin, etherin tai jonkin muun sen tapaisen virtuaalivaluutan varaan rakentuvan järjestelmän myös se huomioon ottaen, millaisia sähköisiä maksujärjestelmiä muuten on käytössä.

Niin bitcoinin kuin muiden rakenteellisesti sitä vastaavien originaalien virtuaalivaluuttojen arvo on historiallisesti katsoen heitellyt paljon, mikä hankaloittaa niiden käyttöä yleisenä maksuvälineenä. On kuitenkin erilaisia keinoja pyrkiä vakauttamaan arvoa. Parhaaksi käydään paljon keskustelua erilaisista vakautetuista virtuaalivaluutoista (englanniksi *stablecoin*). Toisin kuin esimerkiksi bitcoin, erilaiset stablecoinit tyypillisesti henkilöityvät tiettyihin toimijoihin. Stablecoina voidaan pyrkiä vakauttamaan esimerkiksi suhteessa yhteen tai useampaan laillisena maksuvälineenä käytettävään valuuttaan kuten dollariin, muihin varallisuuden muotoihin, erilaisiin hyödykkeisiin tai raaka-aineisiin ja myös kaikenlaisiin eri vaihtoehtojen kombinaatioihin. Kyse voisi olla esimerkiksi siitä, että stablecoinien omistajille tarjottaisiin vaihtoehto vaihtaa tietty määrä johonkin hyödykkeeseen, jolloin stablecoinin hinta tähän hyödykkeeseen nähden pysyisi vakiona.

Esimerkiksi omaisuutta toiselle luovutettaessa on periaatteessa mahdollista arvottaa omaisuutta pelkästään siltä kannalta, mikä on omaisuuden arvo jollain virtuaalivaluutalla määritettynä. Eri valtioissa on kuitenkin lukuisia oikeudellisia rakenteita (kuten kirjanpito- ja verolainsäädäntöä), jotka ainakin jollain tavalla pakottavat määrittämään hinnat lainsäädännössä tunnustetun rahan, kuten euron, avulla. Vaikka jotain yksityistä virtuaalivaluuttoa ryhdyttäisiin käyttämään laajamittaisesti maksuvälineenä arkielämässä, kyse ei välttämättä olisi sellaisesta käytämisestä, joka syrjäyttäisi virallisen valuutan mukaisen hintamekanismin markkinoilla. Hinnat voisivat siis edelleen määräytyä esimerkiksi eurojen ja dollareiden perusteella siten, että käytettäessä virtuaalista valuuttaa maksuvälineenä tähdättäisiin siihen, että virtuaalisen valuutan arvo vastaa sitä euro- tai dollarimäärää, johon hinta on määritelty. Tämä vastaisi valuutan käyttäjän näkökulmasta nykyisellään tilannetta, jossa useilla maksukorteilla on mahdollista maksaa vieraassa valuutassa, vaikka omalla tilillä olisi vain euroja. Tässä tapauksessa maksuvälittäjä tilittää myyjälle tietyn määrän vaadittua valuuttaa ja poistaa muuntokurssin kautta vaaditun määrän euroja käyttäjän tililtä.

Julkisvallalla on verraten suuri intressi ohjata virtuaalisten valuuttojen käyttöä maksuvälineenä. Nykymuotoisissa yhteiskunnissa yksi hyvin tärkeä talouteen vaikuttamisen keino on rahapolitiikka, jonka harjoittaminen on tyypillisesti uskottu keskuspankeille. Monet virtuaalivaluuttoja kannattavat henkilöt pitävät julkisvallan vaikutusmahdollisuuksien vähenemistä hyvänäkin asiana ja mahdollisesti vakautta luovana seikkana, mutta ainakin tällä hetkellä vaikuttaa siltä, että useimmat valtiot eivät noin vain halua luopua niillä olevasta vallasta vaikuttaa talousjärjestelmään rahajärjestelmän välityksellä. Jos yksityiset virtuaalivaluutat osataan esimerkiksi euroalueella kytkeä lainsäädännön avulla sopivalla tavalla euroääräisiin seteleihin ja kolikoihin sekä näiden varaan rakentuviin muihin maksujärjestelmiin, myös rahapolitiikan harjoittamisen edellytykset voidaan säilyttää

samalla kun annetaan mahdollisuus lohkoketjupohjaisille maksujärjestelmien innovaatioille.

## 2.4 Saantomuodot

Bitcoinin ja sitä vastaavien virtuaalivaluuttojen ilmaantumisen myötä on syntynyt uudenlaisia objekteja, joita voidaan omistaa siinä kuin esimerkiksi irtaimia esineitä. Kun ei ole mitään keinoa erottaa valuuttayksiköitä toisistaan, edellä jaksossa 2.1 esitetyn mukaisesti tuntuu luonteelta lähteä siitä, että tiettyyn osoitteen tai tiliin kytketyt varat muodostavat yhden objektin. Seuraavassa tarkastellaan lähemmin sitä, kuinka henkilö voi saada omistukseensa tällaisia digitaalisia varoja. Vertailukohtana käsitellään toistuvasti aineelliseen esineeseen kohdistuvan omistusoikeuden saamista, jotta saataisiin esitellyksi ne opit, joiden näkökulmasta on perusteltua tarkastella myös virtuaalivaluutoista ja yleisemminkin digitaalisessa muodossa olevasta varallisuudesta koostuvien objektien omistusta.

Tosiseikkoja, jotka synnyttävät jollekulle omistusoikeuden, kutsutaan kotimaisessa varallisuus oikeudessa vakiintuneesti *saannoksi*. Tavallisin perusta omistajanvaihdokselle on luovutus eli se, että henkilöstä tulee omistaja hänen hyväksyen annetun luovutusta tarkoittavan tahdonilmaisun perusteella. Tällaisessa luovutussaannossa voi olla kyse esimerkiksi kaupasta, vaihdosta tai lahjasta. Luovutuksen käsite ei rajoitu ainoastaan omistusoikeuteen, vaan luovutuksen (tai siirron) kohteena voi olla myös esimerkiksi saamisoikeus tai jokin immateriaalioikeus kuten tekijänoikeus. Myös luovutussaannon tai yleensä saannon käsitettä käytetään usein laajassa merkityksessä siten, että saannoista puhuminen ei rajoitu ainoastaan omistusoikeuden saamiseen.

Myös originaalista virtuaalivaluutasta kuten bitcoinista koostuvien objektien omistus edellyttää jonkin saannon tunnusmerkkien täyttymistä. Käytännössä tärkein tilanne lienee se, että omistajaksi tuleminen perustuu toisen henkilön antamaan tahdonilmaisuun. Tarkastellaan esimerkiksi tilannetta, jossa A ja B neuvottelevat B:n omistaman irtaimen esineen kaupasta ja jossa B haluaisi saada maksuksi 10 bitcoinia. Yhteisymmärrys saavutetaan, ja B antaa A:lle tiedoksi osoitteen, jonne A voi siirtää vaaditut varat. A:lla sattuu olemaan yhdessä osoitteessa tasan 10 bitcoinia, jotka A siirtää B:n tilille. A tekee siirron siinä tarkoituksessa, että A menettää oikeutensa siirrettyihin varoihin. Toisaalta A tarkoittaa, että kyseessä olevat 10 bitcoinia kuuluvat B:lle. Jos B:n tilillä sattuu olemaan siirron hetkellä entuudestaan hänelle kuuluvia bitcoineja, A:n tarkoitus merkitsee tarkkaan ottaen sitä, että A:n siirtämät 10 bitcoinia muodostavat yhdessä B:n tilillä jo olevien bitcoinien kanssa kokonaisuuden, joka kuuluu yksin B:lle. Oletetaan kuitenkin yksinkertaisuuden vuoksi, että B:n tilillä ei siirron tapahtuessa ole muita bitcoineja.

Esimerkkitapauksessa on selvää, että B:llä on saantoperuste niihin bitcoineihin, jotka A siirsi B:n ilmoittamaan osoitteeseen. Arvio aineellisen normiston mukaisesta oikeustilasta olisi olennaisesti toisenlainen, jos joku henkilö olisi esimerkiksi erehdyksessä siirtänyt varoja B:n tilille. Ajatellaan vaikkapa tilannetta, jossa C:n on tarkoitus siirtää 10 bitcoinia erälle toiselle omalle tililleen. Erehdyksessä käy kuitenkin niin, että hän siirtää varat B:n osoitteeseen. Oletetaan nytkin yksinkertaisuuden vuoksi, että B:n tilillä ei ole laisinkaan bitcoineja tuolla hetkellä.

Viimeksi mainitussa tilanteessa olisi ainakin kotimaisen oikeuden näkökulmasta perusteltua katsoa, että B:n tilillä olevat varat kuuluvat aineellisessa mielessä C:lle, vaikka B tosiasiallisesti kykenee määräämään varoista. Toinen asia on, että C ei käytännössä voi ottaa yhteyttä B:hen ja vaatia tältä varojen palauttamista, jos C ei tiedä B:n henkilöllisyyttä. Aineellisen normiston kannalta hyvin tärkeää on, että C:n oikeus sitoo myös B:n velkojia. Jos B esimerkiksi asetetaan konkurssiin, C voi vaatia varojen itselleen palauttamista. Tämä johtuu siitä, että konkurssiin asettamisen myötä syntyvään konkurssipesään voi yleensä kuulua vain konkurssivelalliselle kuuluvaa omaisuutta. Konkurssilain (120/2004; KonkurssiL) 5:6:ssä säädetään sivullisen omaisuudesta vielä erikseen:

Velallisen hallinnassa oleva sivullisen omaisuus, joka voidaan erottaa velallisen omaisuudesta, ei kuulu konkurssipesään. Sivullisen omaisuus on luovutettava omistajalle tai tämän määräämälle sellaisin ehdoin, joiden täyttämistä konkurssipesällä on oikeus vaatia.

Myös bitcoinien kaltainen virtuaalinen varallisuus voi epäilyksettä olla omaisuutta konkurssilaisissa tarkoitetulla tavalla, joten konkurssipesän varoihin saattaa sisältyä myös virtuaalista varallisuutta. Esimerkkitapauksessa B:n tilillä oleva 10 bitcoinin varallisuuserä kuuluu kuitenkin sivulliselle eli C:lle niin, että C voi vaatia konkurssipesää siirtämään varat takaisin C:n tosiasialliseen määräysvaltaan. Tilanne olisi olennaisesti hankalampi muun muassa siinä tapauksessa, että B:n tilillä olisi ollut 5 bitcoinia siirron tapahtuessa. Tällöin jouduttaisiin kysymään, täytyykö KonkurssiL 5:6:ssä asetettu vaatimus siitä, että sivullisen omaisuus voidaan erottaa velallisen omaisuudesta.

Sääntelyä tulkittaessa tulee tietysti ottaa huomioon myös lainvalmistelutöissä esitetty. Hallituksen esityksen HE 26/2003 vp mukaan velallisen ja sivullisen omaisuus menettävät yksilöitävyytensä, jos ne sekoittuvat toisiinsa (s. 74). Tämän jälkeen lausutaan seuraavasti:

Sekoittuminen voi tapahtua monin eri tavoin. Sivullisen omaisuus on voitu liittää osaksi velallisen omaisuutta tai kysymyksessä voi olla esine, jota ei voi erottaa velallisen muusta samanlaisesta omaisuudesta. Erityisesti rahavarojen osalta kysymys yksilöitävyydestä voi olla käytännössä merkityksellinen. Jos velallinen ei ole pitänyt sivullisen varoja tämän lukuun erillään muista varoistaan, varat eivät ole yleensä erotettavissa velallisen muista varoista. Joissakin tapauksissa esimerkiksi

sivullisen velallisen pankkitilille maksamat varat voivat kuitenkin olla yksilöitävissä.

Säännös esitöineen täytyy ottaa vakavasti, vaikka siihen saattaa sisältyä tietynlainen periaatteellinen hahmotusongelma osassa sekoittumistapauksia. Esimerkiksi öljyerien tai bitcoinien sekoittumisen jälkeen ei liene lainkaan aiheellista puhua sivullisen ja velallisen omaisuudesta samaan tapaan kuin ennen sekoittumista, sillä alkuperäiset omistuksen kohteet ovat oikeastaan lakanneet sekoittumisen myötä. Tämän tyyppisissä sekoittumistapauksissa on yleisesti ottaen tärkeämpää kysyä myös yhteisomistuksen mahdollisuus huomioon ottaen, kenelle sekoittumisen myötä syntynyt kokonaisuus kuuluu. Esimerkiksi voidaan ajatella tilannetta, jossa kaksi samanlaatuista öljyerää sekoittuu toisiinsa. Oikeuskirjallisuudessa on usein puollettu kantaa, jonka mukaan tämän kaltaisessa tilanteessa voisi syntyä yhteisomistussuhde. Jos esimerkiksi A:lle kuuluva 500 litran öljyerä sekoittuu B:lle kuuluvaan 500 litran öljyerään, lähtökohtana voitaisiin pitää, että syntynyt 1 000 litran öljyerä kuuluu A:n ja B:n yhteiseen omistukseen suhteessa 1:1. Mikäli B asetettaisiin konkurssiin B:n pitäessä hallinnassaan A:lle ja B:lle kuuluvaa öljyerää, yhteisomistussuhteen puitteissa voisi päättyä luontevasti muun muassa siihen, että A voisi vaatia konkurssipesältäkin yhteisomistussuhteen lakauttamista eli käytännössä öljyerän jakamista kahteen 500 litran öljyerään. Vastava ratkaisu voisi ainakin joillain edellytyksillä tulla kyseeseen myös esimerkiksi pankkirahan, arvo-osuuksien ja virtuaalisen varallisuuden yhteydessä.

Yhteisomistussuhteen syntyminen ei kuitenkaan saa merkittävää tukea oikeuskäytännöstä. Korkeimman oikeuden viimeaikaisten kannanottojen (ks. etenkin KKO 2020:51, KKO 2021:36 ja KKO 2022:46) perusteella vaikuttaa päinvastoin siltä, että ainakin pankkitilille siirretyistä varoista tulee sekoittumisen myötä tilinhaltijalle kuuluvia varoja. Tilivarojen sekoittuminen lienee ymmärretty niin, että sekoittuminen on käsillä esimerkiksi silloin, kun 5 000 euron saldoa osoittavalle tilille tehdään 5 000 euron tilisiirto. Vaikka oikeuskäytännössä on myös tulokinnanvaraisuuksia, vaikuttaa siltä, että korkein oikeus on mieltänyt sekoittumisen saantoperusteeksi, jonka myös sekoittumisen myötä syntynyt kokonaisuus kuuluu tilinhaltijalle. Voitaneen olettaa (ks. myös KKO 2020:64), että tämä sekoittumissääntö koskettaa myös bitcoineja ja muita sen kaltaisia virtuaalivaluuttayksiköitä silloin, kun jokin taho yksin hallitsee sitä yksityistä avainta, jota tarvitaan osoitteessa olevista varoista määräämiseen.

Virtuaalisen valuutan luovutus voi tapahtua oikeudelliselta kannalta, vaikka tietokannassa itsessään ei tapahtuisi minkäänlaista muutosta. Ajatellaan vaikkapa tilannetta, jossa A:lla on tietystä osoitteesta omistuksessaan 10 bitcoinia. Oletetaan, että A haluaa lahjoittaa kaikki nämä bitcoinit B:lle. A laatii tätä tarkoitusta ilmentävän lahjakirjan, jonka hän antaa B:lle selittäen tarkoituksensa.



Myös viimeksi mainitussa tapauksessa voidaan puhua luovutuksesta ainakin silloin, kun tapahtumia tarkastellaan kotimaisen oikeuden kannalta. Lahjoitusta voidaan myös pitää pätevästi toteutettuna siitä riippumatta, katsotaanko lahjanlupauslain (625/1947; LahjaL) soveltuvan myös kyseessä olevaan lahjoitukseen. Sääöksessä asetetut pätevän lahjan edellytykset nimittäin täyttyvät. LahjaL 1.1 §:ssä on säädetty:

Irtaimen omaisuuden lahjoittamista koskeva, lupaus olkoon, niin kauaa kuin lahjoitusta ei ole täytetty, vaikutukseton, jollei lupaus ole tehty velkakirjassa tai muussa asiakirjassa, joka on annettu lahjan saajalle, tai elleivät asianhaarat lupaus tehtäessä osoita, että se oli tarkoitettu tulemaan yleisön tietoon.

Esimerkkimme A oli siis toteuttanut lahjoituksen asiakirjassa, joka oli annettu lahjansaajalle. Se, soveltuuko lahjanlupauslaki tarkastellun kaltaiseen lahjoitukseen, ei kuitenkaan ole täysin selvää. Lahjanlupauslaissa on kerrottu varsin yksityiskohtaisesti erilaisten omaisuuslajien osalta, kuinka lahjoituksen täyttäminen tapahtuu. Esimerkiksi LahjaL 2 §:ssä säädetyn nojalla rahan tai tavaran lahjoitusta ei ole täytetty, jos lahjan saaja ei ole saanut haltuunsa sitä, mitä on luvattu. Bitcoinin kaltaisista virtuaalivaluutoista koostuvien omaisuuserien lahjoittamiseen ei ole otettu kantaa.

Virtuaalista varallisuutta voi saada omistukseensa muillakin tavoilla kuin luovutuksella. Palataan hahmottamisen helpottamiseksi omistusoikeuden pariin. Eri-laisia saantomuotoja ryhmiteltäessä on usein lähdetty siitä, että toisistaan voidaan erottaa alkuperäiset, johdannaiset ja kumoavat saannot. Alkuperäiselle saannolle ominaista on, että henkilöstä tulee omistaja tilanteessa, jossa esineellä ei ole edeltävää omistajaa. Kyse voi olla esimerkiksi ilman omistajaa olevan esineen omaksi ottamisesta valtaukseksi kutsutun saantomuodon puitteissa. Johdannaissaanto viittaa tilanteeseen, jossa esineellä on entuudestaan omistaja ja jossa omistusoikeus ainoastaan siirtyy toiselle. Luovutussaannot lukeutuvat omistajanvaihdossaantoihin samoin kuin muun muassa perhe- ja jäämistöoikeudelliset saannot. Kumoavat saannot puolestaan ilmenevät tilanteissa, joissa esineellä sinänsä on edeltävä omistaja mutta jossa uuden omistajan oikeus ei perustu edeltäjän oikeuteen samaan tapaan kuin johdannaisissa saannoissa.

Kaikki omistusoikeuden saamista koskevat saantomuodot eivät sovellu originaalista virtuaalivaluutasta koostuvaan omaisuuteen. Selvää on kuitenkin, että saantoperusteena voi olla esimerkiksi perimys. Jos esimerkiksi 10 bitcoinia omistava A kuolee, kyse epäilemättä on sellaisesta omaisuudesta, joka siirtyy muille henkilöille perintökaaressa (40/1965) tarkemmin säädetyllä tavalla. Virtuaalisesta varallisuudesta voidaan määrätä myös testamentilla. Tältä osin on syytä panna merkille, että perintökaaressa edellytetään tiettyjen muotomääräysten noudattamista.

Käytännössä hyvin yleinen tapa saada virtuaalista varallisuutta on louhiminen (englanniksi *mining*), jossa palkitaan lohkon luomiseen osallistuneita tahoja virtuaalisella valuutalla. Tällainen ominaisuus on sisäänrakennettuna esimerkiksi Bitcoin-järjestelmässä ja monissa muissa järjestelmissä, joissa konsensusmekanismina on *proof-of-work*. Bitcoinien lukumäärä lisääntyy tällä haavaa koko ajan tämän ominaisuuden vuoksi, vaikka palkkion määrä hiljalleen laskeekin. Vaikka bitcoinien enimmäismääräksi on määritetty 21 miljoonaa, tämä enimmäismäärä tulee vastaan vasta vuonna 2100, joten protokollan muuttamiseen tai muihin järjestelmän uudistamista koskeviin toimenpiteisiin on vielä runsaasti aikaa.

Louhimista saatetaan luonnehtia erityistyyppiseksi alkuperäiseksi saannoksi. Voitaneen sanoa, että se muodostaa luovutuksen ohella tärkeimmän saantotyypin esimerkiksi bitcoinin kaltaisten originaalien virtuaalivaluuttojen yhteydessä. Päivitetystä Ethereum-järjestelmässä, jossa konsensusmekanismina on syyskuusta 2022 lähtien ollut *proof-of-stake*, virtuaalista varallisuutta voi ansaita menettelyllä, jota kutsutaan englanniksi termeillä *minting* ja *forging*. Termiä louhiminen käytetään tosin usein laajassa merkityksessä siten, että se kattaa myös *proof-of-stake*-konsensusmekanismiin, jossa merkitystä annetaan louhijoiden omistusuosuudelle virtuaalivaluutan yhteenlasketusta kokonaismäärästä.

## 2.5 Virtuaalivaluutan luovutus ja velkojasuoja

Kun jokin varallisuus oikeus luovutetaan toiselle, luovutus yleensä saa kotimaisen oikeuden mukaan itsessään aikaan sen, että luovutus sitoo myös luovuttajan velkojia. Tällainen varallisuus oikeus ei enää kuulu luovuttajalle siten, että sitä voitaisiin käyttää hänen velkojensa maksamiseen ulosotossa. Ulosottokaaren (705/2007) 4:9.1:ssä säädetään nimenomaisesti, että sivulliselle kuuluvaa omaisuutta ei saa ulosmitata. Kyse ei myöskään ole konkurssipesään kuuluvasta omaisuudesta. Velallisen hallinnassa oleva sivullisen omaisuus ei KonkurssiL 5:6:n mukaan kuulu konkurssipesään, kunhan se voidaan erottaa velallisen omaisuudesta.

Joskus luovutus kuitenkin sitoo luovuttajan velkojia vain tiettyjen edellytysten vallitessa. Esimerkiksi velkakirjalain (622/1947; VKL) 22.1 §:ssä säädetään, että juoksevan velkakirjan luovutus ei ole luovuttajan velkojia sitova, ellei se, jolle luovutus on tapahtunut, ole saanut velkakirjaa haltuunsa. Juoksevia velkakirjoja ovat VKL 11.1 §:n mukaan haltijalle sekä nimetylle henkilölle tai hänen määräämälleen asetetut velkakirjat. Haltijalle asetettuna pidetään myös velkakirjaa, josta ei käy ilmi kenelle maksu on suoritettava.

Esimerkiksi bitcoinien ja muiden vastaavien objektien tai näistä objekteista koostuvien erien luovutuksen sitovuuteen luovuttajan velkojiin nähden ei ole otettu nimenomaisesti kantaa kotimaisessa lainsäädännössä. Oikeustilassa on näin ollen väistämättä jonkin verran epäselvyyttä. Lähdetessä tarkastelemaan lähemmin

aihepiiriä on syytä ottaa huomioon, että luovutus voidaan toteuttaa eri tavoin. Sen lisäksi, että A saattaa yksinkertaisesti siirtää virtuaalista varallisuutta määräysvallassaan olevasta osoitteesta toiseen osoitteeseen, A voi esimerkiksi antaa B:lle asiakirjan, jonka mukaan tietyssä osoitteessa olevat varat kuuluvat osin tai kokonaisuudessaan B:lle.

Jos luovutus ei itsessään riitä tuottamaan sitovuutta luovuttajan velkojiin nähden, herää kysymys, mitä kaikkea sitovuus edellyttää. Tarkastellaan esimerkiksi tilannetta, jossa tietyssä osoitteessa olevat 10 bitcoinia kuuluvat A:lle, joka ainoana henkilönä tuntee osoitteeseen liittyvän yksityisen avaimen. A:lla on melko paljon euromääräistä velkaa B:lle, joka on valmis vapauttamaan A:n tämän velasta bitcoineja vastaan. Näin päädytään siihen, että B vapauttaa A:n tämän velasta sitä vastaan, että A luovuttaa erillisellä asiakirjalla kyseisessä osoitteessa olevat 10 bitcoinia A:lle. Lisäksi A antaa B:lle osoitteeseen liittyvän yksityisen avaimen, jota koskeva tieto jää myös hänelle itselleen.

Vaikka B on saanut itselleen yksityisen avaimen, myös A:lla on tosiasiallisesti mahdollisuus määrätä luovuttamista bitcoineista, vaikka kyse onkin luovutuksen perusteella B:lle kuuluvista bitcoineista. Tällaisen mahdollisuuden olemassaolo luultavasti merkitsisi esimerkin kaltaisissa olosuhteissa sitä, ettei luovutus sitoisi luovuttajan velkojia, mikäli oikeusjärjestyksessä pidettäisiin lähtökohtana, ettei luovutus itsessään riitä tuottamaan sitovuutta velkojiin nähden. Jos sen sijaan A olisi tehokkaasti hävittänyt itseltään tiedon yksityisestä avaimesta, asia saattaisi olla toisin. Tämä on kuitenkin epävarmaa, sillä kyse olisi näytöllisesti hyvin epäselvästä asiasta. Velkojien intressien vuoksi voitaisiin puoltaa kantaa, jonka mukaan kyseessä olevat varat pitäisi siirtää jollekin toiselle tilille tai ainakin aloittaa siirtoprosessi. Tällöin ongelma siirtyy tosin toisaalle, sillä vaikka kyseessä olisi alun perin B:n määräysvallassa oleva tili, B saattaisi antaa A:lle tähän tiliin liittyvän yksityisen avaimen.

Ei voidakaan pitää täysin selvänä oikeutemme mukaan, mitä kaikkea luovutuksen sitovuus edellyttäisi, jos luovutus itsessään ei riitä tuottamaan sitovuutta. Tästä epäselvyydestä huolimatta voidaan kuitenkin puoltaa kantaa, jonka mukaan *luovutus itsessään ei riitä tuottamaan sitovuutta*. Originaalista virtuaalivaluutasta kuten bitcoineista koostuvat omaisuuserät ovat luonteeltaan sellaisia, että niiden osalta on luontevaa noudattaa VKL 22.1 §:stä ja siihen liittyvistä säännöksistä ilmeneviä yleisiä arvopaperioikeudellisia periaatteita. Todettakoon vielä, että lahjanlupaussalissa on omaa sääntelyään siinä, millaisin edellytyksin lahjoitus sitoo lahjoittajan velkojia. Täyttämätön lahjoitus ei LahjaL 1.2 §:n nojalla sido lahjoittajan velkojia. Jos luovutuksen yleensä katsottaisiin itsessään sitovan luovuttajan velkojia, olisi varsin merkittävää painetta tulkita lahjanlupaussalain sääntelyä siten, että lahjaksi tapahtunut luovutus sitoo vain täytetyksi tulemisen perusteella – mitä tämä täyttäminen tarkkaan ottaen sitten merkitseekään. Toisaalta lahjanlupaussalain voidaan

katsoa soveltuvan siinäkin tapauksessa, että virtuaalivaluutan luovutus yleisesti ottaen määräytyy muun muassa VKL 22.1 §:stä ilmenevien periaatteiden mukaisesti.

Otetaan seuraavaksi tarkasteltavaksi ne tilanteet, joissa siirretään tosiasiallisesti varoja teknisessä järjestelmässä ilman näitä toimia edeltävää muulla tavalla toteutettua oikeudellista luovutusta. A esimerkiksi siirtää tietyssä osoitteessa olevat 10 bitcoinia B:n ilmoittamaan osoitteeseen ilman, että B:llä ennen siirtoa olisi mitään oikeutta juuri kyseessä oleviin bitcoineihin. Kysymykseksi jää, mitä tarkkaan ottaen vaaditaan, että luovutus sitoisi A:n velkojia. Menettely muistuttaa siinä määrin tavanomaista pankkirahalla maksamista, että tilisiirron sitovuus muodostaa mielenkiintoisen vertailukohdan. Maksupalvelulain (290/2010) 81 §:n mukaan maksu sitoo maksajan velkojia ja muita sivullisia, kun maksunsaajan palveluntarjoaja on saanut tarvittavat tiedot maksutapahtuman rahamäärän maksamiseksi maksunsaajan maksutilille ja 1) maksutapahtuman rahamäärä on maksettu maksunsaajan palveluntarjoajan tilille tai 2) maksunsaajan palveluntarjoajan asettamat maksutapahtuman katetta koskevat ehdot ovat muutoin täyttyneet. Maksu sitoo sivullisia kuitenkin aina, kun maksutapahtuman rahamäärä on maksettu maksunsaajan maksutilille.

Bitcoinin ja sitä vastaavien virtuaalisten valuuttojen siirto ei toteudu samoin kuin pankkirahan siirto, koska kyse on periaatteellisesti erilaisista järjestelmistä. Tiettyjä vastaavuuksia voidaan sen sijaan havaita. Virtuaalisen valuutan siirto etenee normaalisti järjestyksessä 1) elektroninen allekirjoitus, 2) vahvistaminen ja 3) lohkokoon kirjaaminen. Sitovuuteen luovuttajan velkojia vastaan riittää epäilemättä se, että transaktio on kirjattu lohkokoon. Riittäväksi saatettaisiin kuitenkin katsoa jo elektroninen allekirjoitus sillä edellytyksellä, että transaktio kuitenkin lopulta kirjataan lohkokoon. Tämä saatettaisiin itse asiassa asettaa velkojasuojan edellytykseksi silloinkin, kun osoitteesta siirretään varoja, jotka on jo luovutettu teknisen siirronsaajan omistukseen esimerkiksi erillisellä lahja- tai kauppakirjalla.

## 2.6 Toiselle kuuluvan virtuaalivaluutan luovutus

Kun omaisuutta luovutetaan, luovuttaja on yleensä omistaja itse. Luovutustahdonilmaisun saattaa kuitenkin antaa myös henkilö, joka ei ole omistaja ja jolla ei muutenkaan ole kelpoisuutta luovutukseen. Tällöin on luonnollisesti lähtökohdana, että omistajanvaihdos ei tapahdu luovutustahdonilmaisun perusteella samoin kuin yleensä. Käytännössä kaikissa oikeusjärjestyksissä on kuitenkin sääntelyä, jonka nojalla luovutuksensaaja voi ainakin joissain tilanteissa tulla omistajaksi erityisten vilpittömän mielen suojaa koskevien oppien perusteella. Tällaisten oppien vallitessa tietynlaiseen tosiseikastoon, johon kuuluu luovutuksen ohella

vähintään luovutuksensaajan vilpittömässä mielessä toimiminen, kytkeytyy ”oikean” omistajan oikeuden lakkaaminen ja luovutuksensaajan omistuksen alkaminen.

Oikeudettomat luovutukset ovat mahdollisia myös originaalien virtuaalivaluuttojen yhteydessä. Tarkastellaan vaikkapa tilannetta, jossa A:lla on omistuksessaan 10 bitcoinia eräessä A:n määräysvallassa olevassa osoitteessa. Nyt voi käydä esimerkiksi niin, että B onnistuu selvittämään A:n yksityisen avaimen ja siirtämään bitcoinit juuri hankkimaansa osoitteeseen. Jos B saman tien siirtää bitcoinit esimerkiksi C:lle velkojensa maksuksi tai pelkästään kertoo C:lle esimerkiksi suullisesti luovuttavansa kyseessä olevat varat C:n omistukseen, ainakin kotimaisessa oikeudessa on hyvät perusteet katsoa, että B on määrännyt oikeudettomasti A:lle kuuluneesta omaisuudesta. Vastaavalla tavalla voidaan suhtautua esimerkiksi tilanteeseen, jossa A on itse erehdyksessä siirtänyt bitcoinit B:n osoitteeseen tilanteessa, jossa A:n oli tarkoitus siirtää bitcoinit toiseen määräysvallassaan olevaan osoitteeseen.

Kotimaisessa lainsäädännössä ei ole nimenomaisesti otettu kantaa bitcoineista tai niiden kaltaisista virtuaalisen valuutan yksiköistä koostuvien omaisuuserien oikeudettomaan luovutukseen. On kuitenkin melko paljon sääntelyä, josta voidaan lähteä hakemaan analogista johtoa. Esimerkiksi arvo-osuustileistä annetun lain (827/1991; ATL) 26 §:ssä lähdetään siitä, että arvo-osuustilille kirjattu saanto ja arvo-osuuteen kohdistuva arvo-osuustilille kirjattu oikeus saa etusijan suhteessa saantoon ja oikeuteen, jota ei ole kirjattu tilille. Jos samaan arvo-osuuteen kohdistuu keskenään ristiriidassa olevia oikeuksia, aikaisemmin arvo-osuustilille kirjattu oikeus saa etusijan myöhemmin kirjattuun nähden. Aiemmin syntynyt saanto tai oikeus saa kuitenkin etusijan myöhempään nähden, jos 1) myöhempi saanto tai oikeus perustuu ositukseen tai perintöön, oikeushenkilön sulautumiseen, jakautumiseen tai purkautumiseen taikka yhteisen omaisuuden jakoon tai 2) myöhempään saantoon tai oikeuteen vetoava saannon hetkellä tai oikeuden saadessaan taikka hänen saantoaan tai oikeuttaan tilille kirjattaessa tiesi tai hänen piti tietää aikaisemmasta saannosta tai oikeudesta. ATL 27 § koskee puolestaan tilannetta, jossa arvo-osuuden tai siihen kohdistuvan oikeuden on luovuttanut joku, jolla arvo-osuustilin kirjausten mukaan oli siihen oikeus. Saajan oikeutta ei säännöksen mukaan estä se, ettei luovuttajalla ollut oikeutta määrätä arvo-osuudesta, paitsi jos saaja saannon hetkellä tai oikeuden saadessaan taikka hänen saantoaan tai oikeuttaan tilille kirjattaessa tiesi tai hänen piti tietää siitä.

Varteenotettavalta vaihtoehdolta näyttää, että bitcoinien ja niitä vastaavien virtuaalivaluuttayksiköiden luovutuksensaajalla olisi mahdollisuus tulla omistajaksi vilpittömän mielen suojan perusteella vastaavassa laajuudessa kuin arvo-osuuk-sienkin luovutuksensaajalla. Aivan selvää ei kuitenkaan ole, mitä kaikkea vilpit-

töman mielen suoja edellyttää. Tulkintaongelmat ovat samantapaisia kuin edellisessä jaksossa. Riittävänä voitaneen varmuudella pitää sitä, että virtuaalinen valuutta on siirretty luovutuksensaajan osoitteeseen ja että luovutuksensaaja toimii perustellussa vilpittömässä mielessä vielä silloin, kun varat saapuvat hänen määrättäväkseen.

Käytännössä ongelmaksi voi koitua, että oikea omistaja A ei kykene tunnistamaan luovutuksensaajaa C, ja myös B saattaa jäädä tuntemattomaksi. Tällöin A:n oikeudet helposti jäävät toteutumatta.

Se, että vilpittömässä mielessä toiminutta luovutuksensaajaa todella suojattaisiin samassa laajuudessa kuin arvo-osuuksien luovutuksensaajaa, ei ole itsestään selvää. Esimerkiksi tavanomaisten irtainten esineiden vaihdannassa tunnetaan tilanteita, joissa vilpittömän mielen suoja ei voi saada. Esimerkiksi rikoslain voimaannapamisesta annetun asetuksen (39B/1889; RVA) 11 § koskee tilannetta, jossa esine on viety entiseltä haltijalta ”näpistämisen, varkauden, ryöstön tahi kiristämisen kautta”. Tämän säännöksen soveltuessa luovutuksensaaja ei voi saada itselleen vilpittömän mielen suojaa. Esimerkiksi juoksevien velkakirjojen luovutuksensaaja on kuitenkin paremmassa asemassa, sillä RVA 11 §:ään nähden etusijalla on VKL 14 §, jonka nojalla juoksevan velkakirjan luovutuksensaajaa suojataan käytännössä yhtä tehokkaasti kuin arvo-osuuden luovutuksensaajaa. Kun pohditaan vilpittömän mielen suojaamista bitcoinin ja muiden sen kaltaisten virtuaalivaluuttojen yhteydessä, kysymys on oikeastaan siitä, voidaanko luovutuksensaajan eduksi tukeutua VKL 14 §:stä, arvo-osuustililaista sekä eräistä muista samansuuntaisista säännöksistä johdettaviin arvopaperioikeudellisiin periaatteisiin.

## 2.7 Säilytystä sisältävät palvelut

Originaalien virtuaalivaluuttojen ympärille on rakentunut monenlaista palvelutoimintaa, ja usein palveluun sisältyy säilytystä asiakkaiden lukuun joko pääasiallisena tai vähintään täydentävänä elementtinä. Keskeinen palveluja koskeva kotimainen säädös on laki virtuaalivaluutan tarjoajista, joka edellä jaksossa 2.2 todetun mukaisesti ulottaa vaikutuksensa myös lohkoketjupohjaisiin virtuaalivaluuttoihin ja jossa virtuaalivaluuttaan liittyvällä palvelulla tarkoitetaan virtuaalivaluutan liikkeeseenlaskua, virtuaalivaluutan vaihtopalvelua ja lompakkopalvelun tarjoamista (VvTL 2.1 §:n 6 kohta). Säilytystä ilmenee etenkin kahdessa viimeksi mainitussa.

Virtuaalivaluutan vaihtopalvelulla tarkoitetaan säädöksessä luonnollista henkilöä tai oikeushenkilöä, joka liike- tai ammattitoimintana a) vaihtaa virtuaalivaluuttaa palveluna lailliseksi maksuvälineeksi tai toiseksi virtuaalivaluutaksi, b) vaihtaa virtuaalivaluuttaa palveluna muuksi hyödykkeeksi tai muun hyödykkeen virtuaalivaluutaksi tai c) ylläpitää markkinapaikkaa, jossa sen asiakkaat voivat harjoittaa

kohdissa a) ja b) tarkoitettua toimintaa (VvTL 2.1 §:n 4 kohta). Säilytys mainitaan nimenomaisesti lompakkopalvelun tarjoajan määritelmässä; kyse on luonnollisesta henkilöstä tai oikeushenkilöstä, joka pitää virtuaalivaluuttaa hallussa toisen lukuun tai tarjoaa sen siirtoa taikka säilytystä (VvTL 2.1 §:n 5 kohta).

Siihen, mitä säilytys tarkkaan ottaen merkitsee eri palvelujen yhteydessä, ei ole yksiselitteistä vastausta. Esimerkiksi bitcoinien osalta kyse voi yksinkertaisimmillaan olla siitä, että palveluntarjoaja pitää huolta asiakkaan yksityisestä avaimesta tarjoten samalla lompakkopalvelua. Asiakkaalla on siis tällöin samoin kuin yleensäkin lohkoketjujärjestelmässä hänelle yksilöityvä osoite, johon voidaan myös siirtää varoja tavalliseen tapaan. Osoitteita voi tietysti olla myös useita. Kun asiakas haluaa itse siirtää bitcoineja, hän turvautuu palveluntarjoajan tarjoamaan lompakkoon, johon hän pääsee käsiksi palveluntarjoajan tunnistautumisjärjestelmän avulla. Mitään estettä ei sinänsä ole sille, että asiakas voi määrätä omaisuudestaan muutenkin olettaen, että hänellä on myös yksityinen avain tiedossaan.

Kun asiakkaan yksityiset avaimet ovat palveluntarjoajalla, asiakas muistuttaa tietyissä suhteissa tavanomaisen pankin asiakasta. Asiakas tyypillisesti operoi palveluntarjoajan tunnistautumisjärjestelmän avulla, ja jos hän esimerkiksi kadottaa tarvittavat tunnukset, hän voi olla yhteyksissä palveluntarjoajaan samaan tapaan kuin pankkiin. Palveluntarjoajan olemassaolo on omiaan helpottamaan myös asiakkaan omaisten asemaa asiakkaan poismenon jälkeen. Jos palveluntarjoaja vain on tiedossa, omaiset ja testamentinsaajat voivat päästä käsiksi virtuaalivaluuttoihin silloinkin, kun kuolleen jäljiltä ei löydy mitään tunnuksia. Jos esimerkiksi bitcoineja suoraan omistava ja itse hallinnoiva henkilö ei eläessään varaudu kuolemansa jälkeisiin tapahtumiin, saattaa käydä niin, etteivät jälkeläiset pääse käsiksi virtuaalivaluuttoihin tai saa edes tietoa lohkoketjupohjaisen varallisuuden olemassaolosta.

Siitä, että virtuaalivaluutat ovat palveluntarjoajan tosiasiallisessa määräysvallassa, koituu toisaalta myös erilaisia riskejä. Palveluntarjoajat ovat esimerkiksi suosittuja kohteita hakkerointiyrityksille. Toisinaan tällaiset yritykset ovat tuottaneet myös tulosta, vaikka riskien vähentämiseen on erilaisia keinoja. Yksityisiä avaimia voidaan esimerkiksi säilyttää erillisillä muistilaitteilla, jotka eivät ole jatkuvasti yhteydessä julkiseen tietoverkkoon. Tällaisen ns. kylmäsäilytyksen (*cold storage*) ohella ja rinnalla voidaan myös noudattaa yhtä useamman yksityisen avaimen järjestelmää (*multisig*-säilytys), joka osaltaan vaikeuttaa hakkerointia.

Myös asiakkaat voivat tehostaa turvaansa *cold storage* -menetelmillä ja useamman yksityisen avaimen käytöllä, ja monet omaan osaamiseensa luottavat henkilöt tyytyvätkin omatoimiseen säilytykseen. Vaikka palveluntarjoaja joutuisi vastuuseen asiakkaisiinsa nähden hakkerointitapauksessa sopimus oikeuden yleisten oppien perusteella, korvausvelvollisuus saattaa olla laiha lohdutus, mikäli palveluntarjo-

ajalla ei ole riittävästi varojen korvausten maksamiseen. Käytännössä on kuitenkin myös tilanteita, joissa asiakkaan on hankala toimia täysin omatoimisesti. Monet markkinapaikat käytännössä edellyttävät sitä, että originaalit virtuaalivaluutat ovat ainakin jossain laajuudessa palveluntarjoajan tosiasiallisessa määräysvallassa. Myös sellaisia toimintamalleja, joissa yksityiset avaimet voidaan pitää omissa käsissä, on toisaalta pyritty kehittämään. Markkinapaikkoihin liittyviä riskejä voidaan vähentää niinkin, että markkinapaikan määräysvallassa pidetään esimerkiksi bitcoineja kulloinkin vain lyhyen aikaa ja ainoastaan siinä laajuudessa, kuin tiedossa olevat lähitulevaisuuden vaihtotarpeet edellyttävät.

Jos jokaisella palveluntarjoajan asiakkaalla on tälle yksilöityvä osoite tai useampiakin osoitteita, saavutetaan varsin selkeä perusrakenne. Kyse voi toisaalta olla myös verraten työläästä ja monimutkaisesta rakenteesta. Ainakin palveluntarjoajan näkökulmasta kiinnostavaksi vaihtoehdoksi voi nousta järjestelmä, jossa eri asiakkaille kuuluvia originaaleja virtuaalivaluuttoja säilytetään yhdessä osoitteessa. Teoriassa voi tosin ajatella myös järjestelmää, jossa asiakkaiden oikeudet eivät lainkaan kohdistu tiettyihin varoihin ja jossa palveluntarjoaja on vain ”velkaa” asiakkaalle samaan tapaan kuin pankki on asiakkailleen velkaa sen summan, jota asiakkaan pankkitilillä oleva saldo osoittaa.

Yhteissäilytys saattaa hidastaa asiakkaan mahdollisuuksia määrätä haluamallaan tavalla originaaleista virtuaalivaluutoista. Toisaalta yhteissäilytys voi yksinkertaistaa toimintoja ja vähentää myös lohkoketjuun tehtävien muutosten määrää.

Oikeudelliselta kannalta keskeiseksi kysymykseksi nousee, millaiset sinänsä mahdolliset säilytysjärjestelmät ovat hyväksyttäviä myös lainsäädännön näkökulmasta. Keskeinen kotimainen säännös tässä suhteessa on asiakasvarojen säilyttämistä pykäläotsikkonsa mukaisesti koskeva VvTL 11 §, jonka 1 momentti kuuluu seuraavasti:

Virtuaalivaluutan tarjoajan on suojattava palvelunkäyttäjiltä tai toiselta palveluntarjoajalta virtuaalivaluuttojen vaihtamiseksi vastaanotetut varat ja virtuaalivaluutat. Varoilla tarkoitetaan käteistä, tilille kirjattua raha-arvoa ja sähköistä rahaa.

Säännöksen ensimmäisessä virkkeessä oleva määre ”virtuaalivaluuttojen vaihtamiseksi vastaanotetut” tuntuisi sanamuodon perusteella viittaavan säännöksessä määriteltujen varojen eli käteisen, tilille kirjatun raha-arvon (pankkirahan) ja sähköisen rahan ohella myös virtuaalivaluuttoihin. Joudutaan kuitenkin kysymään, voidaanko määre ymmärtää kirjaimellisesti. VvTL 11.1 § koskee yleisesti virtuaalivaluutan tarjoajia, eivätkä virtuaalivaluutan tarjoajista annetun lain mukaiset palvelut rajoitu virtuaalivaluuttojen vaihtamiseen. Sääntelyn yleistavoitteiden näkökulmasta tuntuisi aiheelliselta tulkita määrettä ”virtuaalivaluuttojen vaihtamiseksi vastaanotetut” sanamuotoa laajemmin. Suojaamisvelvollisuus koskisi tosin vain sellaisia virtuaalivaluuttoja ja muita varoja, joita voidaan pitää ”asiakasvaroina”.



Virtuaalivaluutan tarjoajan pitää VvTL 11.2 §:n mukaan säilyttää 1 momentissa tarkoitetut varat niin, ettei ole vaaraa niiden sekoittumisesta toisen palvelun käyttäjän, palveluntarjoajan tai sen omiin varoihin. Tämä sääntely kohdistuu siis ainoastaan käteiseen, tilille kirjattuun raha-arvoon ja sähköiseen rahaan. Varat pitää tallettaa tilille keskuspankkiin, talletuspankkiin tai muussa valtiossa toimiluvan saaneeseen talletusten vastaanottamiseen oikeutettuun luottolaitokseen taikka vähäriskisiin ja helposti rahaksi muutettaviin arvopapereihin tai muihin sijoituskohteisiin. Tämä pätee kuitenkin vain, jos varoja ei ole siirretty varojen vastaanottamista seuraavana työpäivänä. Säännöksen mukaan Finanssivalvonta antaa määräykset siitä, milloin arvopaperia tai muuta sijoituskohdetta voidaan pitää vähäriskisenä ja helposti rahaksi muutettavana.

Lakitekstin perusteella ei ole selvä, mitä kaikkea VvTL 11.1 §:n mukaiseen suojaamiseen sisältyy. Säännöksen perusteluissa on kuitenkin kerrottu (HE 167/2018 vp s. 89):

Kun virtuaalivaluutan tarjoaja vastaanottaa virtuaalivaluuttoja, ne on vastaavasti säilytettävä luotettavalla tavalla erillään muiden asiakkaiden virtuaalivaluutoista esimerkiksi erillisessä virtuaalisessa lompakossa. Tämä ei tarkoittaisi sitä, että jokaiselle käyttäjälle olisi avattava ja hallinnoitava erillistä lompakkopalvelua, vaan kunkin asiakkaan virtuaalivaluutat on pystyttävä luotettavasti erottelemaan muiden asiakkaiden virtuaalivaluutoista esimerkiksi kirjanpidollisesti.

Lakitekstistä ja esitöistä ei saada suoraan vastausta siihen, voidaanko asiakkaan virtuaalivaluuttoja pitää VvTL 11.1 §:n mukaisesti suojattuna silloinkin, kun palveluntarjoaja tietoisesti säilyttää samoissa osoitteissa niin omiaan kuin asiakkaiden virtuaalivaluuttoja. Oikeuskirjallisuudessa Jon Hautamäki, Max Atallah ja Karri Koskikare ovat tulkinneet teoksessaan *Virtuaalivaluutan tarjoaminen – käsi-kirja virtuaalivaluuttalain soveltamiseen* (Edita 2019; luku 11 Asiakasvarojen säilyttäminen) sääntelyä siten, että lain vaatimaan suojaamiseen riittää, että asiakkaille kuuluvat virtuaalivaluutat voidaan erottaa kirjanpidollisesti, vaikka asiakkaiden ja yritysten varoja olisikin samalla tilillä. Tämä riittää kirjoittajien mukaan myös käteisen, tilille kirjatun raha-arvon ja sähköisen rahan yhteydessä. Asiakasvarojen kirjanpidollinen eriyttäminen tarkoittaa heille sitä, että ”asiakasvarat ovat muiden varojen kanssa samalla tilillä (ts. pankkitili) siten, että ne kuitenkin kirjanpidossa on merkitty asiakasvaroiksi” (s. 97).

Voidaanko sääntelyä todella tulkita mainitulla tavalla, on kyseenalaista. Erikseen tulee kysyä myös, millaiset menettelyt vastaavat kirjanpitolaista (1336/1997) johtuvia vaatimuksia. Tämä kysymys jätetään kuitenkin tällä kertaa vain maininnan varaan.

Kun lainsäädännössä otetaan kantaa asiakasvarojen säilytykseen, yleensä vaaditaan menettelyä, jonka myötä asiakkaat varmasti saavat tehokasta suojaa erilai-

sissa insolvenssimenettelyissä. Jos asiakkaille kuuluvia virtuaalivaluuttoja ja rahavaroja säilytetään samoilla tileillä kuin palveluntarjoajan omia varoja, ei voida pitää ainakaan selvänä sitä, että asiakkailla olisi velkoja sitovia oikeuksia esimerkiksi palveluntarjoajan konkurssissa. Kuten edellä jaksossa 2.4 esitettiin, uudemman oikeuskäytännön perusteella vaikuttaa jopa verraten todennäköiseltä, että virtuaalivaluuttojen katsottaisiin kuuluvan siviilioikeudelliselta kannalta palveluntarjoajalle välittömästi sekoittumisen perusteella. Virtuaalivaluutan tarjoajista annetussa laissa ei ole erityissääntelyä, jonka perusteella asiakkaat olisivat suojattuja esimerkiksi palveluntarjoajan konkurssissa. Kiinnostavan vertailukohdan tosin muodostaa laki arvopaperitileistä (750/2012), jonka 11.1 §:ssä lähdetään siitä, että säilyttäjän tilinhaltijoidensa lukuun hallitsevat arvopaperit eivät kuulu säilyttäjän konkurssipesään eikä niitä voida ulosmitata säilyttäjän velasta. Arvopaperitililaissa olevan erityissääntelyn ansiosta asiakkaat ovat joissain suhteissa paremmassa asemassa kuin siinä tapauksessa, että esimerkiksi säilyttäjän konkurssia arvioitaisiin puhtaasti yleisten oppien eli ennen muuta KonkurssiL 5:6:n ympärille rakentuneen tulkintatradition näkökulmasta. Tässä yhteydessä ei kuitenkaan ole mahdollista tarkastella yksityiskohtaisesti tilinhaltijoiden oikeusasemaa arvopaperitililain järjestelmässä eikä edes sitä, kuinka arvopaperien säilyttäminen tulee tarkkaan ottaen järjestää.

Virtuaalivaluutan tarjoajista annetussa laissa ei säädetä nimenomaisesti siitä, että virtuaalivaluutan tarjoajan täytyisi pitää itselleen kuuluvat virtuaalivaluutat erossa asiakkaille kuuluvista virtuaalivaluutoista. Jos tällaista erilläänpitovelvollisuutta olisi tarkoitettu, voitaisiin ajatella, että tämä olisi tuotu selvästi esiin sääntelyssä. Vertailun vuoksi voidaan mainita, että esimerkiksi asianajajan on asianajajista annetun lain (496/1958) 5.3 §:n mukaan pidettävä päämiehilleen kuuluvat raha- ja muut varat erillään omista varoistaan. Tämä sääntely koskee epäilemättä myös virtuaalivaluuttoja.

Toisaalta on ajateltavissa, että erilläänpitovelvollisuuden asettavat lukuisat säännökset ilmentävät yleistä periaatetta, jonka mukaan asiakasvarat tulee pitää erillään liike- ja ammatinharjoittajan omista varoista. Varojen erilläänpitoa on yleensä edellytetty lainsäädännössä ennen muuta asiakkaiden insolvenssisuojan vuoksi. Esimerkiksi hallituksen esityksen HE 199/1996 vp mukaan varojen erillisuus on tärkeää muun muassa toimeksiantajan suojaamiseksi toimeksisaajan velkojia vastaan (s. 16): ”Jos varoja ei asianmukaisesti säilytetä erillään, on olemassa riski, että ne ulosmitataan toimeksisaajan velasta tai että niiden katsotaan kuuluvan toimeksisaajan konkurssipesään.” Lausumat liittyvät saatavien perinnästä annetun lain (513/1999) 11 §:ään (”Asiakasvarat”), jonka mukaan varat, jotka toimeksisaaja on perinyt velkojan lukuun, on pidettävä erillään toimeksisaajan omista varoista ja talletettava pankkitilille tai säilytettävä muulla luotettavalla tavalla.

Tilannetta mutkistaa osaltaan, että virtuaalivaluuttojen tarjoajista annetussa laissa tarkoitetut virtuaalivaluutat saattavat olla myös sijoituspalvelulain (747/2012) 1:14:ssä (1069/2017) tarkoitettuja rahoitusvälineitä ja että virtuaalivaluutan tarjoajan toiminnassa saattaa olla kyse lain 15 §:ssä (1069/2017) määritellystä sijoituspalvelusta tai sijoitustoiminnasta. Koska sijoituspalvelulaki soveltuu liiketoimintaan, jossa tarjotaan sijoituspalvelua tai harjoitetaan sijoitustoimintaa (1 §, 1069/2017), joudutaan pohtimaan sijoituspalvelulain ja virtuaalivaluutan tarjoajista annetun lain keskinäistä suhdetta. Sijoituspalvelulain 9 luvussa on nimittäin sääntelyä asiakasvarojen säilyttämisestä ja muusta käsittelystä. Luvussa on lukuisia pykäläitä, joissa ei välttämättä aina puhuta asiakasvaroista täysin samassa merkityksessä. Sijoituspalvelulain 9:1:ssä (1069/2017, ”Asiakasvarojen säilyttäminen”) lähdetään siitä, että sijoituspalveluyrityksen on järjestettävä sen hallintaan luovutettujen asiakkaan rahoitusvälineiden ja rahavarojen (asiakasvarat) säilyttäminen ja käsittely luotettavalla tavalla.

Sijoituspalvelulain 9:1.2:n mukaan sijoituspalveluyrityksen on ”asiakasvarojen säilyttämisessä ja käsittelystä erityisesti huolehdittava siitä, että sijoituspalveluyrityksen varat pidetään selkeästi erillään asiakasvaroista ja luottolaitoksia lukuun ottamatta estettävä rahavarojen käyttäminen sijoituspalveluyrityksen omaan lukuun”. Sääntelyä voitaneen myös 9:1.3 huomioon ottaen tulkita siten, ettei kirjanpidollinen eriyttäminen riitä silloin, kun kyse on sääntelyssä tarkoitetuista asiakasvaroista. Tuo pykälän 3 momentti nimittäin kuuluu seuraavasti: ”Sijoituspalveluyrityksen on pidettävä luotettavasti kirjaa asiakasvaroista siten, että kunkin asiakkaan asiakasvarat ovat riittävästi eriteltyinä muiden asiakkaiden varoista.” Kirjanpidollinen eriyttäminen on siis ilmeisesti osoitettu riittäväksi siltä osin kuin kyse on asiakkaille kuuluvien varojen erottamisesta tilanteessa, jossa esimerkiksi pankkitilillä on vain asiakkaille kuuluvia varoja.

Vaikka laissa virtuaalivaluutan tarjoajista ei ole nimenomaisesti säädetty velvollisuudesta pitää eri henkilöille kuuluvat virtuaalivaluutat erillään toisistaan, VvTL 11.1 §:ssä puhutaan kuitenkin virtuaalivaluuttojen ja muiden varojen suojaamisesta. Kirjoituksessa Janne Kaisto – Eelis Paukku: *Virtuaalivaluutat, niihin liittyvät palvelut ja asiakasvarojen säilyttäminen* (Liikejuridiikka 3/2022 s. 8–44) on tulkittu kyseessä olevaa tulkinnanvaraista säännöstä siten, että virtuaalivaluuttojen suojaamiseen sisältyy myös, että virtuaalivaluutat säilytetään erillään virtuaalivaluutan tarjoajille kuuluvista virtuaalivaluutoista. Tämä koskee ennen muuta bitcoinia ja muita sen kaltaisia virtuaalivaluuttoja, jotka voivat sekoittua samaan tapaan kuin pankkiraha. Asiakkaille kuuluvien virtuaalivaluuttojen yhteissäilytys sen sijaan on sallittua, koska tällaiseen yhteissäilytykseen ei ainakaan yleisesti ottaen sisälly vastaavanlaista riskiä insolvenssisuojan menettämisestä.

Finanssivalvonta voi VvTL 11.4 §:n mukaan antaa tarkempia määräyksiä asiakasvarojen säilyttämisestä ja suojaamisesta. Määräykset ja ohjeet 4/2019, Virtuaalivaluutan tarjoajat, sisältää tällaisia määräyksiä. Näistä määräyksistä, myös annetut ohjeet huomioon ottaen, syntyy vaikutelma, jonka mukaan asiakasvarojen kirjanpidollista eriyttämistä olisi saatettu pitää riittävänä. Erillistä asiakasvarojen tiliä ei nimenomaisesti edellytetä edes rahavarojen osalta, ja toisaalta esimerkiksi kohdassa 16 olevassa määräyksessä todetaan:

Valvottavan on pidettävä kirjaa omista varoistaan ja asiakasvaroistaan. Valvottavan on varmistettava kirjanpidon eheys, saatavuus ja luottamuksellisuus. Tietojärjestelmiin on rakennettava kontrollit, jotka mahdollistavat kirjanpidon ja säilytyksessä olevien varojen täsmäytyksen.

Finanssivalvonnan lähtökohtana on ollut, että asiakasvaroihin kuuluvien virtuaalivaluuttojen säilyttäminen ja suojaaminen tarkoittavat yleensä yksityisten salausavainten luotettavaa säilyttämistä ja suojaamista (kohta 25). Määräyksissä ja ohjeissa 4/2019 on useita määräyksiä, jotka konkretisoivat luotettavaa säilyttämistä ja suojaamista. Esimerkiksi kohdassa 28 olevan määräyksen mukaan asiakasvaroihin kuuluvista virtuaalivaluutoista saa olla säilytyksessä julkiseen tietoverkkoon kytketyssä järjestelmässä vain sellainen määrä, jonka menettämisen valvottava pystyy riskiarvion perusteella kattamaan. Toiseksi esimerkiksi käy kohdan 34 määräys, jonka mukaan tietojärjestelmien varmuuskopiot ja mahdollinen tietojenkäsittelyn varakeskus tulee sijoittaa niin kauas varsinaisesta tietojenkäsittelykeskuksesta, että tiedot ja niiden varmistukset eivät voi tuhoutua samanaikaisesti.

Ei voida pitää täysin selvänä sitä, kuinka Finanssivalvonta on tulkinnut asiakasvarojen säilyttämistä koskevaa sääntelyä. Verkkouutisessa 20.12.2022 (21/2022), otsikoltaan *Virtuaalivaluuttamarkkinoilla epävarmuutta – Finanssivalvonta selvittää suomalaisten tarjoajien yhteyttä ongelmiin joutuneisiin toimijoihin*, kirjoitetaan muun muassa, että asiakasvarojen suojaamisvelvollisuus ”tarkoittaa asiakkaiden varojen suojaamista muun muassa yhtiön omalta konkurssilta” ja että ”[v]irtuaalivaluutan tarjoajan tulee järjestää asiakasvarojen hallintansa siten, ettei mahdollisen konkurssin myötä asiakasvaroja kuuluisi konkurssipesään”. Jos asiakasvaroja ei säilytetä erillään virtuaalivaluutan tarjoajan omista varoista, on verraten suuri riski siitä, että asiakasvaroilta puuttuu tarkoitettu konkurssisuoja. Verkkouutisessa mainittu epävarmuus virtuaalivaluuttamarkkinoilla liittyy eräiden kansainvälisten toimijoiden ongelmiin, joita on käsitelty julkisuudessa ympäri maailman. Esimerkiksi konkurssiin päätyneet yhtiöt nimeltään Celcius Network LLC ja FTX Trading Ltd tulivat vuoden 2022 aikana tutuiksi talousuutisia seuraaville.

## 2.8 Virtuaalivaluutat ja verotus

Bitcoinin, etherin ja muiden vastaavien virtuaalisten valuuttojen luovutuksiin liittyy useita vero-oikeuden kannalta relevantteja kysymyksiä. Esimerkiksi käy EU:n tuomioistuimessa käsitelty tapaus ECLI:EU:C:2015:718 (C-264/14, Skatteverket v. David Hedqvist), jossa otettiin kantaa arvonlisäverodirektiivin 112/2006/EY tulkintaan. Tapaus lähti liikkeelle siitä, että David Hedqvist -niminen henkilö halusi tarjota yrityksen kautta bitcoin-valuutan ja perinteisen valuutan välistä vaihtopalvelua eli toisin sanoen bitcoin-valuutan ostoa ja myyntiä. Hedqvist pyysi ennen toiminnan aloittamista Ruotsissa keskusverolautakunnalta ennakkotietoa siitä, pitikö bitcoinien ostosta ja myynnistä maksaa arvonlisäveroa. Ruotsin verohallinto valitti keskusverolautakunnan verovapautuksen mukaisesta päätöksestä kansalliseen tuomioistuimeen, joka puolestaan pyysi ennakkoratkaisua EU:n tuomioistuimelta.

EU:n tuomioistuin ratkaisi asian Hedqvistin haluamalla tavalla. Kyseessä olevan kaltaiset toimet sinänsä katsottiin sellaisiksi liiketoimiksi, jotka kuuluivat arvonlisäverodirektiivin alaisuuteen eli joista tuli suorittaa arvonlisäveroa. EU:n tuomioistuin kuitenkin katsoi, että kyse oli arvonlisäverodirektiivin 135 artiklan 1 kohdan e alakohdan nojalla arvonlisäverosta vapautetuista liiketoimista. Tuon alakohdan mukaan jäsenvaltioiden tuli vapauttaa verosta ”liiketoimet, mukaan lukien välitys, jotka koskevat valuuttaa sekä laillisina maksuvälineinä käytettäviä seteleitä ja kolikoita, lukuun ottamatta keräilykolikoita ja -seteleitä eli kulta-, hopea- ja muita metallikolikoita ja seteleitä, joita ei tavallisesti käytetä laillisina maksuvälineinä tai jotka ovat numismaattisesti arvokkaita kolikoita”. Ratkaisun tueksi esitettiin useita lausumia, joihin on viitattu verraten usein jälkikäteen yleisemmissäkin merkityksissä. EU:n tuomioistuin muun muassa katsoi, että ”bitcoin-valuutta on sopimukseen perustuva maksuväline” ja että on riidatonta ”ettei virtuaalisella bitcoin-valuutalla ole muuta tarkoitusta kuin käyttö maksuvälineenä ja että tietyt toimijat hyväksyvät sen maksuvälineenä”.

Edellä mainitun ratkaisun yleisempää merkitystä pohdittaessa tulee ottaa huomioon, että siinä otettiin suoranaisesti kantaa vain tiettyihin arvonlisäverodirektiivin tulkintaongelmiin. Oma kysymyksensä on esimerkiksi, mitä kotimaisessa tuloverolaissa (1535/1992; TVL) oleva sääntely merkitsee bitcoinien ja muiden vastaavien virtuaalivaluuttayksikköjen luovutuksesta saadun voiton kannalta. TVL 32 §:n mukaan veronalaista pääomatuloa on omaisuuden tuotto, omaisuuden luovutuksesta saatu voitto ja muu sellainen tulo, jota varallisuuden voidaan katsoa kerryttäneen. Omaisuuden luovutuksesta saatu voitto on TVL 45.1 §:n mukaan veronalaista pääomatuloa siten kuin tuloverolain 2 luvussa säädetään. Omaisuuden luovutuksesta saadun voiton määrä lasketaan TVL 46.1 §:n nojalla yleensä siten, että luovutushinnasta vähennetään omaisuuden hankintamenon poistamatta olevan osan ja voiton hankkimisesta olleiden menojen yhteismäärä. Muun

verovelvollisen kuin yhteisön tai avoimen yhtiön taikka kommandiittiyhtiön saamista luovutushinnasta vähennettävä määrä on kuitenkin aina vähintään 20 prosenttia ja, jos luovutettu omaisuus on ollut luovuttajalla vähintään 10 vuoden ajan, vähintään 40 prosenttia luovutushinnasta (ns. hankintameno-olettama). Eräitä verovapaita pääomatuloja koskevan TVL 53 §:n mukaan veronalaista tuloa ei ole muun muassa luonnolliselle henkilölle tai kuolinpesälle muuhun kuin tulonhankkimistoimintaan liittyvien valuuttakurssivoittojen yhteismäärä enintään 500 euroon asti vuodessa.

Monet virtuaalivaluuttoja ostanee ja myyneet henkilöt ovat saaneet huomattavia voittoja, koska esimerkiksi bitcoinin ja etherin arvo on noussut valtavasti monina ajanjaksoina. Jos virtuaalivaluutan luovutuksesta saatu voitto katsotaan omaisuuden luovutukseksi tuloverolain järjestelmässä eikä muuksi pääomatuloksi, tulee huomioon ottaa myös TVL 46.1 §:ssä oleva sääntely. Korkein hallinto-oikeus otti kysymykseen kantaa tapauksessa KHO 2019:42, jossa A oli pyytänyt keskusverolautakunnalta ennakkoratkaisua seuraavaan kysymykseen: jos A myi omistamaansa ether-virtuaalivaluuttaa, katsottiinko luovutus TVL 45.1 §:ssä tarkoitetuksi omaisuuden luovutukseksi, johon sovellettiin TVL 46.1 §:n luovutusvoiton laskemista koskevaa sääntelyä siten, että hakijan veronalaisen voiton määrä laskettiin vähentämällä luovutushinnasta todellinen hankintameno ja voiton hankkimisesta aiheutuneet menot tai niitä korkeampi hankintameno-olettama?

Keskusverolautakunta katsoi ennakkoratkaisussaan, että luovutusta ei voinut katsoa TVL 45.1 §:ssä tarkoitetuksi omaisuuden luovutukseksi. Syntynyt tulo oli sen sijaan muuta pääomatuloa. Korkein hallinto-oikeus päätyi kuitenkin sille kannalle, että luovutusta oli pidettävä TVL 45.1 §:ssä tarkoitettuna omaisuuden luovuttamisena, johon TVL 46.1 §:ssä olevat luovutusvoiton laskemista koskevat säännökset soveltuivat. Tuloverolaissa oleva omaisuuden käsite ymmärrettiin sen verran laajaksi, että se kattoi myös ether-virtuaalivaluutan. Vastaavalla tavalla tulee epäilemättä suhtautua myös bitcoiniin ja muihin vastaaviin virtuaalivaluuttoihin, joten kansallisen tuloverotuksen näkökulmasta edes maksuvälineeksi tarkoitettujen virtuaalisen varallisuuden muotojen yhteydessä ei ole kyse TVL 53 §:ssä tarkoitettusta valuuttakurssivoitosta tai TVL 32 §:ssä tarkoitettusta muusta pääomatulosta kuin luovutusvoitosta.

Ratkaisu KHO 2019:42 ja edellä tarkasteltu EU:n tuomioistuimen ratkaisu eivät suoranaisesti ole ristiriidassa jo sen vuoksi, että niissä tarkasteltiin erilaisia kysymyksiä. Korkein hallinto-oikeus totesi nimenomaisesti oman kantansa:

Koska asiassa on kyse tuloverotuksesta, jota säännellään kansallisella tasolla ja jota ei ole Euroopan unionissa harmonisoitu arvonlisäverotuksen tavoin, tilannetta ei ole arvioitava toisin myöskään sen tähden, että Euroopan unionin tuo-

mioistuun on asiassa C-264/14, Skatteverket v. David Hedqvist, antamassaan tuomiossa katsonut, että virtuaalinen Bitcoin-valuutta on sopimukseen perustuva maksuväline.

Korkein hallinto-oikeus toteaa eräässä kohtaa ratkaisun KHO 2019:42 perustelua, että etheriä ”voidaan käyttää sekä vaihdon välineenä että sijoituskohteena”. Ilmeistä onkin, että etheriin ja moniin muihin virtuaalisiin valuuttoihin on ainakin takavuosina ryhdytty juuri sijoitusmielessä. Kuten edellä jaksossa 2.3 on esitetty, tunnetuimmatkin virtuaalivaluutat ovat itse asiassa toimineet varsin heikosti todellisina maksuvälineinä. Korkein hallinto-oikeus ei EU-tuomioistuimen tavoin painota sitä rakenteellista lähtökohtaa, että virtuaalisen valuutan ainoa käyttötarkoitus on toimia maksuvälineenä. Tapauksessa KHO 2019:42 voitiin pitää selvitettyinä, että etheriden arvon nousuun luottanut A oli ostanut etheriä sijoitustarkoituksessa. Korkeimman hallinto-oikeuden kantaa voidaan kaiken kaikkiaan pitää perusteltuna.

Moni henkilö saa merkittäviä lisätuloja lohkoketjun konsensusmekanismin edellyttämiin toimintoihin osallistumalla. Esimerkiksi voidaan ajatella Bitcoin-järjestelmän taustalla olevan *proof-of-work*-mekanismin mukaista louhintaa. Verotuksen näkökulmasta yksi tulkintakysymys koskettaa saatujen tulojen luonnehdintaa tuloverolain näkökulmasta eli ennen muuta siitä, onko kyse pääomatulosta vai ansiotulosta. Tuloverolain järjestelmässä TVL 61 §:n mukaan ansiotuloa on muu tulo kuin tuloverolain 2 luvussa tarkoitettu pääomatulo, jota puolestaan tyypillisesti saadaan omaisuuden tuottona, omaisuuden luovutuksesta saatuna voittona ja muuna sellaisena tulona, jota varallisuuden voidaan katsoa kerryttäneen (TVL 32 §).

Verohallinto lähtee ohjeessaan *Virtuaalivaluuttojen verotus* (annettu 22.1.2020) siitä, että louhimisesta saatu tulo ei ole tuloverolaissa tarkoitettua varallisuuden kerryttämää tuloa silloin, kun kyse on *proof-of-work*-konsensusmekanismista (jakso 2.5.1 Proof of work -protokolla). Kyse on näin ollen ansiotulosta. Sen sijaan *proof-of-stake*-mekanismeissa saatu tulo on pääomatuloa, koska tässä tapauksessa ”kyse on olemassa olevaan varallisuuteen eli aiemmin omistettuun virtuaalivaluuttaan suoraan perustuvasta tulosta” (jakso 2.5.2 Proof of stake -protokolla). Verohallinto on lähtenyt siitä, että *proof-of-stake*-mekanismeissa uusien virtuaalivaluuttojen saanto perustuu ”jo olemassa olevan virtuaalivaluutan määrän lukitsemiseen hetkeksi verkon käyttöön”.

Se, että louhimisesta saatu tulo on katsottu pääomatuloksi *proof-of-stake*-konsensusmekanismin yhteydessä, vaikuttaa perustellulta. Sen sijaan *proof-of-work*-mekanismiin liittyvä näkemys on kritisoitavissa. Esille voidaan nostaa erityisesti se, että louhimisesta saatava tulo edellyttää laitteistoa ja että monet tarjoavat ja hankkivatkin laskentatehoa juuri siinä tarkoituksessa, että he jatkuvan toiminnan

myötä saavuttaisivat suhteellisen tasaista tuloa louhimisesta. Oikeuskirjallisuudessa Kristian Keskitalo on artikkelissaan *Virtuaalivaluutan louhiminen: ansio- vai pääomatuloa?* (Edilex 2022/7) suhtautunut kriittisesti verohallinnon ohjeeseen ja verrannut *proof-of-work*-konsensusmekanismin mukaista louhintapalkkiota korvaukseen siitä, että ajoneuvo annetaan toisen henkilön käyttöön. Molemmissa tapauksissa on hänen mukaansa loppujen lopuksi kyse omaisuuteen perustuvasta tulosta eli pääomatulosta. Toisaalta voidaan myös esittää vastakkainen näkemys siitä, että laitteistoa käytetään vain työkaluna, jolla tuotetaan palvelua muille virtuaalivaluutan käyttäjille.



## 3 ÄLYSOPIMUKSET JA SOPIMUSOIKEUS

### 3.1 Älyopimukset pääpiirteissään

Lohkoketjuun voidaan sijoittaa ohjelmia tai sovelluksia, joilla voi olla mitä erilaisimpia toiminnallisuuksia. Kyse voi olla esimerkiksi siitä, että tietynlaisen viestin ohjelmalle lähettäminen aktivoi jonkin toiminnon. Tällaisia lohkaketjussa toimivia ohjelmia kutsutaan varsin yleisesti älyopimuksiksi siitä riippumatta, millaisesta ohjelmasta on kysymys. Älyopimukset luetaan usein lohkaketjuteknologian kehitysvaiheeksi 2.0 lähdetessä siitä, että virtuaalivaluutat bitcoin etunässä merkitsevät kehitysvaihetta 1.0.

Joitain alustoja suunniteltaessa on pidetty vahvasti silmällä älyopimusten tekemistä. Tunnetuin näistä alustoista on Ethereum, jossa erotetaan kaksi tilityyppiä eli ulkoiset tilit ja sopimustilit. Ulkoisesta tilistä (englanniksi *external account* tai *externally owned account* eli EOA) voidaan määrätä yksityisen avaimen samaan tapaan kuin bitcoin-tilistä. Sopimustilit (englanniksi *contract account* eli CA) puolestaan toimivat niihin sijoitetun ohjelman mukaisesti.

Kun älyopimus ymmärretään edellä kerrotulla tavalla, se tulee erottaa sellaisista juristeille tutuista sopimuksista, joita käsitellään sopimusoikeudeksi kutsutulla oikeudenalalla. Älyopimukset ovat kuitenkin kiinnostava ilmiö myös oikeudellisten sopimusjärjestelyjen ja sopimusoikeuden kannalta. Ajatellaan esimerkiksi tilannetta, jossa A lupaa tehdä B:lle rahasuorituksen sen jälkeen, kun B on tehnyt tietyn palvelun A:n hyväksi. Vaikka B tekisi palvelun, voi käydä niin, ettei A tee lupaamaansa suoritusta joko halun tai kyvyn puuttumisen vuoksi. Tällaisen riskin olemassaolo voi omalta osaltaan vaikuttaa B:n päätöksentekoon niin, ettei B edes halua tehdä A:n kanssa sopimusta, jossa B velvoittautuisi palveluun ja A myöhemmin tehtävään rahasuoritukseen.

Tarkastellun kaltaisessa tilanteessa on lukuisia keinoja, joilla voidaan etukäteen pyrkiä vähentämään B:n asemassa olevan henkilön riskejä. Yksi mahdollinen tapa on turvautua älyopimukseen. Esimerkiksi Ethereum-järjestelmään voidaan sijoittaa ohjelma, joka automaattisesti toimittaa tietyn määrän ethereitä B:lle siinä tapauksessa, että ohjelma on saanut tiedon palvelun toteutumisesta.

Älyopimusten avulla voidaan siis automatisaation avulla vähentää perinteisiä *sopimusten täyttämiseen* liittyviä ongelmia. Tämä koskee luonnollisesti vain sellaisia asioita, jotka ovat lohkaketjuun sijoitetun ohjelman määräysvallassa. Esimerkki oli tässä mielessä selkeä, sillä sopimustilien määräysvallassa voi olla ethereitä, joista älyopimukset pystyvät määräämään. On hyvä panna merkille, että esimerkiksi A:n ja B:n piti lisäksi päästä yhteisymmärrykseen siitä, että B saa palvelun tekemisen jälkeen juuri ethereitä. Jotta ohjelma myös voisi toimittaa etherit B:lle, A:n tulisi järjestää riittävästi ethereitä sopimustilille.

Lohkoketjussa olevat tietokoneohjelmat eivät tarkkaile maailman tapahtumia siten kuin ihmiset, mutta nekin voivat silti saada tietoa ulkomaailman tapahtumista. Sellaista tahoja, jolta älysovimus voi saada tietoa, kutsutaan yleensä *oraakkeliksi*. Esimerkissä ei kuvattu tarkemmin oraakkelia, vaan tältä osin tyydyttiin sanomaan, että ohjelma oli saanut tiedon palvelun toteutumisesta. Jos esimerkiksi A ja B haluaisivat turvautua älysovimukseen, heidän tulisi ratkaista hyvin tarkasti myös kysymys siitä, kuinka ohjelma saa tiedon palvelun toteutumisesta.

### 3.2 Lohkoketjuun sijoitettu ohjelma – oikeushenkilö?

Kun lohkaketjuun sijoitetut ohjelmat tekevät erilaisia asioita, on monesti luonteva kohdella ohjelmia ikään kuin subjekteina. Esimerkiksi edellisessä jaksossa onkin puhuttu siitä, että älysovimus siirtäisi virtuaalista varallisuutta ja että älysovimus myös saisi tietoa. Erikseen tulee kuitenkin kysyä, voidaanko älysovimuksia pitää oikeudellisesti *oikeuskelpoisina* siinä mielessä, että niillä voisi olla oikeuksia ja velvollisuuksia. Oikeudellisessa ajattelussa lähdetään niin meillä kuin muuallakin yleensä siinä, että oikeussubjektit ovat luonnollisia henkilöitä eli ihmisiä tai oikeushenkilöitä. Tästä dikotomiasta liikkeelle lähdettäessä kysymys on siitä, voiko lohkaketjuun sijoitettu ohjelma olla oikeushenkilö, sillä ihmisestä ei tietenkään ole kysymys.

Valtioissa tyypillisesti tunnustetaan niin kotimaisia kuin ulkomaisia oikeushenkilöitä. Monet oikeushenkilötyypit ovat sellaisia, että ne tunnetaan osapuulleen samanlaisina kaikkialla. Esimerkiksi kotimaisessa osakeyhtiölaissa (624/2006; OYL) tarkoitettu osakeyhtiö tunnetaan maailmanlaajuisesti. Osakeyhtiö on OYL 1:2.1:n mukaan osakkeenomistajistaan erillinen oikeushenkilö, joka syntyy rekisteröimisellä. Niin meillä kuin muualla pätee myös hyvin tärkeä yleinen lähtökohta, jonka mukaan osakkeenomistajat eivät henkilökohtaisesti vastaa yhtiön velvoitteista.

Maapallolla tuskin on valtiota, jossa oikeushenkilön katsottaisiin syntyvän pelkästään sillä perusteella, että lohkaketjuun sijoitetaan ohjelma. Monilla foorumeilla keskustellaan kuitenkin siitä, tulisiko älysovimukset joillain edellytyksillä tunnustaa omanlaiseksi oikeushenkilöiden tyypiksi. Erityisen paljon on keskusteltu sellaisista projektiluontoisista älysovimuksista tai älysovimusten kokonaisuuksista, joita voidaan kutsua nimityksellä *Decentralized Autonomous Organization* eli DAO.

Älysovimuksia ja DAO:ja koskeva keskustelu liittyy laajempaan diskurssiin siitä, missä määrin viimeaikainen teknologinen kehitys tulisi ottaa huomioon arvioitaessa perinteisiä käsityksiä oikeushenkilöistä. Tässä yhteydessä voidaan mainita ainakin tekoäly ja robotiikka. Euroopan parlamenttikin on ottanut aihepiiriin kantaa päätöslauselmassaan 16. helmikuuta 2017 suosituksista komissiolle robotiikkaa koskevista yksityisoikeudellisista säännöistä. Aihepiiri, joka on tärkeä

muun muassa vahingonkorvauksen kannalta, jakaa mielipiteitä. Myös yleiseltä kannalta lukemisen arvoisena voidaan pitää vuonna 2019 julkaistua EU-raporttia *Liability for Artificial Intelligence and other emerging digital technologies* (European Commission 2019, Report from the Expert Group on Liability and New Technologies – New Technologies Formation), jossa suhtaudutaan varsin kriittisesti oikeudellisen henkilöllisyyden (*legal personality*) myöntämiseen uusille digitaalisille teknologioille.

Jos esimerkiksi DAO:t ollaan valmiita hyväksymään oikeushenkilöiksi jollain aiemmin tuntemattomalla tavalla, tarvitaan huolellista ja seikkaperäistä sääntelyä. Joissain valtioissa on jo otettu askelia tähän suuntaan. Esimerkiksi voidaan mainita Malta, jota monesti kutsutaan ”lohkaketjusaareksi”. Maltalla luotiin jo vuoden 2018 loppupuolella järjestelmä, joka antaa mahdollisuuden muun muassa DAO:jen ja älysovimusten määräaikaiseen sertifiointiin. Keskeisen *Innovative Technology Arrangements and Services Act* -säädöksen mukaisen, varsin raskaan menettelyn myötä voidaan saavuttaa sertifiointi, joka muun muassa antaa luotettavuutta kyseessä olevalle teknologiselle innovaatiolle.

### 3.3 Soveltuvasta sääntelystä

Valtaosassa sopimustilanteista voidaan ilman ongelmia tunnistaa, minkä oikeusjärjestyksen alaisuuteen sopimus kuuluu. Myös soveltuva lainsäädäntö on monesti helposti tunnistettavissa. Jos esimerkiksi Suomessa asuvat yksityishenkilöt A ja B sopivat Suomessa sijaitsevan irtaimen esineen kaupasta, liikkeelle voidaan epäilemättä lähteä kotimaisen kauppalaain (355/1987) soveltumisesta. Yhtä selvältä näyttää muun muassa kotimaisen varallisuus oikeudellisista oikeustoimista annetun lain (228/1929; OikTL) eli oikeustoimilain soveltuminen.

Sopimusjärjestelyllä saattaa kuitenkin olla sellaisia liityntöjä yhtä useampaan valtioon, ettei olekaan ainakaan heti ensi katsomalta selvää, minkä valtion oikeusjärjestyksen näkökulmasta erilaisia oikeudellisia kysymyksiä tulee tarkastella. Sopijakumppanit voivat esimerkiksi asua eri maissa, ja sopimus saattaa koskettaa omaisuutta, joka sijaitsee jossain aivan muualla. Mahdollista on sekin, että samassa tai eri maassa asuvat sopijakumppanit haluaisivat itse määrittää esimerkiksi sen, minkä valtion lain näkökulmasta tulee tarkastella ainakin joitakin oikeudellisia kysymyksiä.

Kussakin oikeusjärjestyksessä on *kansainväliseksi yksityisoikeudeksi* kutsuttu oikeudenala, jonka perusteella soveltuva sääntely määräytyy. EU-valtioissa tulee huomioon ottaa myös EU-tasoinen sääntely. Sopimusoikeuden näkökulmasta tärkein yksittäinen säädös lienee Euroopan parlamentin ja neuvoston asetus (EY) 593/2008, annettu 17 päivänä kesäkuuta 2008, sopimusvelvoitteisiin sovellettavasta laista eli Rooma I -asetus, jonka perusteella määräytyy sopimusvelvoitteisiin

soveltuva laki siviili- ja kauppaoikeuden alalla. Kaiken kattava asetus ei kuitenkaan ole, vaan jotkin kysymykset on jätetty asetuksen soveltamisalan ulkopuolelle.

Myös älysopimusten käyttämisen yhteydessä voi aktualisoitua kysymys soveltuvasta oikeusjärjestyksestä. Rooma I -asetuksessa on asetettu lähtökohdaksi *valinnanvapaus*. Sopimukseen sovelletaan 3 artiklan mukaan pääsääntöisesti sen maan lakia, jonka osapuolet ovat valinneet. Jos valintaa ei ole tehty nimenomaisesti, sen pitää käydä selvästi ilmi sopimusehdoista tai tapaukseen liittyvistä olosuhteista. Valinnanvapaudella on kuitenkin myös erinäisiä rajoitteita. Jos esimerkiksi kaikki muut lakiviittauksen ajankohtana tilanteeseen liittyvät seikat liittyvät toiseen maahan kuin siihen, jonka laki on valittu, osapuolten tekemä valinta ei rajoita niiden kyseisen toisen maan lain säännösten soveltamista, joista ei voida sopimuksin poiketa.

Älysopimukseen turvautuvat sopijakumppanit voivat siis yleensä sopia siitä, minkä maan lakia (oikeudelliseen) sopimukseen sovelletaan. Mikäli valinnanvapautta ei ole käytetty, soveltuva laki määräytyy toisin kriteerein. Rooma I -asetus sisältää tässä suhteessa lukuisia sääntöjä. Esimerkiksi irtaimen tavaran kauppasopimukseen sovelletaan yleensä sen maan lakia, jossa myyjän asuinpaikka on.

Lohkoketjuja tarkasteltaessa on monesti nostettu esille, että soveltuvan lain tunnistaminen voi olla hankalaa tai mahdotontakin. Tällaiset pelot vaikuttavat liioitelluilta ainakin sopimusoikeuden näkökulmasta, sillä kansainvälisen yksityisoikeuden oppien perusteella myös hankaliin kysymyksiin löytyy ratkaisu. Sitä ei käy kiistäminen, että erilaisia tulkintaongelmia saattaa ilmetä. Yksi lohkaketjuihin läheisesti liittyvä tulkintaongelma koskettaa esimerkiksi Rooma I -asetuksen 1 artiklan 2 kohtaa, jossa on lueteltu seikkoja, jotka eivät kuulu asetuksen soveltamisalaan. Kyseisen kohdan d alakohdassa on mainittu ”velvoitteet, jotka johtuvat vekseleistä, sekeistä tai nimennäisvelkakirjoista taikka muista juoksevista arvopapereista, siltä osin kuin tällaisiin muihin juokseviin arvopapereihin liittyvät velvoitteet johtuvat niiden siirtokelpoisuudesta”. Voi olla hankala sanoa, tuleeko jotain lohkaketjupohjaista virtuaalisen varallisuuden muotoa pitää kohdassa tarkoitettuna arvopaperina. Uusiin teknologioihin liittyy yleisestikin ottaen helposti erilaisia tulkintaongelmia, koska kansainvälisen yksityisoikeuden opit ovat monessa suhteessa kehittyneet ilman huomion kiinnittämistä digitaalisen maailman tapahtumiin.

### 3.4 Älysopimus sopimuksen täytäntöönpanon välineenä

Sopimuksia tehtäessä synnytetään usein velvoitteita, jotka on tarkoitus panna täytäntöön myöhemmin. Siihen, tehdäänkö suoritus todella, sisältyy tällaisessa tilanteessa riskejä. Oikeusjärjestyksissä on tyypillisesti oikeusnormeja, joiden perusteella suorituksen tekemättä jättämisellä voi olla erilaisia seurauksia. Monet

näistä seurauksista ovat sitä luontoa, että niiden käytännön toteuttaminen edellyttää viranomaisten apua. Esimerkiksi tuomioistuinmenettelyt ovat puolestaan usein kalliita ja aikaa kuluttavia.

Jotkin sopimustilanteet ovat luonteeltaan sellaisia, että sopimuksen täytäntöönpanoon liittyviä riskejä kyetään vähentämään automatisoinnilla. Kuten edellä jaksossa 3.1 on jo kerrottu, lohkoketjuun sijoitettu älysopimus saattaa olla varteenotettava vaihtoehto. Ohjelmointi vaatii kuitenkin erityisosaamista, jota sopijakumppaneilla ei välttämättä ole. Jos sopijakumppanit tästä huolimatta haluavat tehdä älysopimuksen, heidän tulee turvautua ulkopuoliseen apuun tai vähintään jonkun toisen aikaisemmin laatimaan ohjelmaan ja ohjeisiin siitä, kuinka ohjelma sijoitetaan lohkoketjuun.

Älysopimusten mahdollistama automaattinen täytäntöönpano on omiaan vähentämään tuomioistuinriitujen määrää, mutta älysopimukseen ei toisaalta saa kohdistaa liiallisia odotuksia tässä suhteessa. Ajatellaan esimerkiksi tilannetta, jossa A ja B tekevät kirjallisesti sopimuksen, jonka täytäntöönpano uskotaan tietyn osin älysopimukselle. Voi käydä esimerkiksi niin, että ohjelman laatimisessa tapahtuu virhe, jonka vuoksi ohjelma ei toimi asianomaisten tarkoittamalla tavalla. Lopputuloksena on, että vaikka ohjelman piti tiettyjen edellytysten täytyttyessä tehdä yhtä, se tekikin toista.

Sopimuksia tehtäessä on mahdollista varautua eri tavoin siihen, että älysopimuksessa on ohjelmointivirhe tai että ohjelma ei muuten toimi sopijakumppanien tarkoittamalla tavalla. Täysin mahdollista on kuitenkin sekin, että sopijakumppanit eivät etukäteen ole huomanneet varautua erheellisesti toimivaan ohjelmaan. Koska ohjelma saattaa toimia yhden sopijakumppanin eduksi ja toisaalta toisen haitaksi, osapuolten välille saattaa syntyä riitaa siitä, kuinka asiassa tulee menetellä. Jos esimerkkinä A:n ja B:n välille syntyy riitaa, asia saattaa päätyä myös tuomioistuimen käsiteltäväksi.

Älysopimukset eivät yleensä voine syrjäyttää niitä edeltävää oikeudellista sopimusta siten, että osapuolten olisi tyytyminen älysopimuksen toimintaan, tekipä ohjelma mitä tahansa. Kysymys on kuitenkin hankalampi, jos osapuolet ovat nimenomaisesti halunneet antaa älysopimukselle tällaisen aseman. Joudutaan nimittäin kysymään, eikö ainakin lähtökohtana voisi olla, että sopijakumppanit voisivat etukäteen luopua mahdollisista oikeuksistaan. Ei voidakaan sulkea pois sitä vaihtoehtoa, että ainakin joissain tilanteissa aiemmin solmitun oikeudellisen sopimuksen osapuolet olisivat voineet sitoutua älysopimukseen ja sen tuottamiin lopputuloksiin.

Tuomioistuinriidat ovat mahdollisia, vaikka älysopimus itsessään toimisi juuri siten kuin pitääkin. Esimerkiksi voidaan ajatella tilannetta, jossa A:n ja B:n välistä oikeudellista sopimusta rasittaa jokin pätemättömyysperuste. A on esimerkiksi

harjoittanut pakkoa tai petollista viettelyä B:hen nähden. Mahdollista on luonnollisesti sekä, että jos B:n esimerkiksi piti tehdä jokin palvelus A:n hyväksi, tässä palvelussa paljastuu myöhemmin merkittävä virhe. Ei voida ajatella, että älysopimukseen turvautuminen itsessään tekisi A:n ja B:n välisen oikeudellisen sopimuksen immuuniksi esimerkiksi pätemättömyyttä tai suoritusvirheitä koskevalle sääntelylle.

Kun sopimuksen täytäntöönpano halutaan osin tai kokonaan uskoa älysopimukselle, sopijakumppanit ovat käytännössä pakotettuja miettimään verraten tarkasti omia tarkoituksiperiään. Muuten on nimittäin hankala laatia näitä tarkoituksiperiä vastaavaa ohjelmaakaan. Älysopimusten yleistymisen saattaa käytännössä johtaa aiempaa tarkempaan sopimuksentekoon, mitä voitaneen pitää hyvänä asiana olettaen, että tämä ei johda merkittävästi kohonneisiin transaktiokustannuksiin. Jos kuitenkin sopijakumppanit haluavat jonkin kysymyksen ratkeavan esimerkiksi kohtuuden, hyvän tavan tai kunniallisuuden kaltaisen joustavan kriteerin perusteella, älysopimuksen tekeminen käytännössä sulkeutunee pois sen vuoksi, ettei ainakaan tällä hetkellä ole mahdollista esittää sopijakumppanien tarkoituksiperiä asianmukaisella tavalla koodimuodossa.

### 3.5 Tarjouksen tekeminen lohkoketjuun sijoitetun ohjelman avulla

Sopimuksia tehdään usein siten, että tarjoukseen annetaan hyväksyvä vastaus. Tällainen tarjous-vastaus-malli tunnetaan osapuulleen kaikissa oikeusjärjestyksissä samoin ne keskeiset kysymyksenasettelut, jotka liittyvät tilanteisiin, joissa sopimuksen muodostavat tahdonilmaisut on tarkoitus antaa eriaikaisesti. Keskeinen kotimainen säädös kyseessä olevan sopimuksentekomekanismin kannalta on oikeustoimilaki, jonka 1 luvussa säädetään sopimuksen tekemisestä. OikTL 1.1 §:n lähtökohta on: ”Tarjous sopimuksen tekemisestä ja sellaiseen tarjoukseen annettu vastaus sitovat tarjouksen tekijää ja vastauksen antajaa sen mukaan, kuin jäljempänä tässä luvussa säädetään.” Oikeustoimilain 1 luvun sääntelyn merkitystä arvioitaessa tulee huomioon ottaa, että luvun säännökset eivät OikTL 1.2 §:n mukaan ”koske määrämuotoisia sopimuksia eivätkä myöskään sopimuksia, joiden päättämiseen vaaditaan suorituksen toimittamista toiselle sopimuspuolelle”. Lisäksi säännökset ovat ”muuten voimassa vain, mikäli tarjouksesta tai vastauksesta tahi kauppa- tai muusta tavasta ei muuta johdu”.

Eri maissa on käyty keskustelua siitä, voiko ohjelman sijoittaminen lohkoketjuun konstituoida tarjouksen tekemistä. Varsin usein tähän kysymykseen on vastattu myöntävästi. Seuraavassa tarkastellaan lähemmin oikeustoimilain 1 luvussa tarkoitettua tarjouksen tunnusmerkistön täyttymistä.

Tarjous voidaan oikeustoimilain 1 luvun järjestelmässä ymmärtää tahdonilmaisuksi, joka edellyttää hyväksyntää. Myös se huomioon ottaen, että oikeustoimilaki on laki *varallisuus oikeudellisista* oikeustoimista, tahdonilmaisulla tulee olla riittävä varallisuus oikeudellinen liityntä. Esimerkiksi voidaan ajatella tilannetta, jossa A on valmis ottamaan itselleen rahasuoritusvelvoitteen, mikäli B luovuttaa tietyn irtaimen esineen A:n omistukseen. A voi tällöin lähettää B:lle esimerkiksi sähköpostin, jossa kerrotaan, että A lupautuu maksamaan B:lle 100 euroa, mikäli B luovuttaa A:lle omistusoikeuden esineeseen X, jonka A haluaa itselleen.

Varallisuus oikeudellisia tahdonilmaisuja voidaan toteuttaa usein eri tavoin kuten puheen, erilaisten asiakirjojen tai eleiden perusteella. Esimerkiksi pään nyökkäys voi sopivissa olosuhteissa merkitä käyttäytymistä, joka voidaan tulkita esimerkiksi rahasuoritukseen velvoittautumiseksi tai omistusoikeuden luovutukseksi. Myös ohjelman sijoittaminen lohkoketjuun voidaan käsittää yhdeksi mahdolliseksi tahdonilmaisun toteuttamisen tavaksi. Henkilö saattaa siis tarkoittaa tiettyjen oikeusvaikutusten synnyttämistä varallisuus oikeudellisen oikeustoimen tekemisellä siten, että hän ilmaisee tahtonsa sijoittamalla tarkoitusta ilmentävän ohjelman lohkoketjuun.

Myös tarjous eli hyväksyntää edellyttävä tahdonilmaisuus voidaan toteuttaa usein eri tavoin. Sama koskee myös hyväksyvää vastausta, joskin tarjouksesta tai vastaasta voi seurata, että vastaus pitää toteuttaa tietyllä tavalla. Oikeustoimilaista käy nimenomaisesti ilmi sekin, että tarjous voidaan tehdä edellyttämättä siihen nimenomaista vastausta (OikTL 8 §).

Myös ohjelman lohkoketjuun asettaminen saattaa konstituoida hyväksyntää edellyttävän varallisuus oikeudellisen tahdonilmaisun. Mikäli kyse sinänsä on oikeustoimilain 1 luvun alaisuuteen kuuluvasta järjestelystä (OikTL 1.2 §), tällaista tahdonilmaisua voitaneen pitää luvussa tarkoitettuna tarjouksena. Tulkintaongelmaksi voi tosin osoittautua se, onko kyse juuri varallisuus oikeudellisesta tahdonilmaisusta. Tarjouksessa edellytetty hyväksyntä saattaa olla esimerkiksi originaalin virtuaalivaluutan siirto, jota voidaan itsessään pitää varallisuus oikeudellisena oikeustoimena. Virtuaalisen valuutan siirtoa lohkoketjuun sijoitetulle ohjelmalle voidaan nykytietämyksen perusteella pitää varsin tyyppisenä tapana tarjouksen hyväksymiselle.

Tarjouksen tunnusmerkistön täyttymisestä seuraa oikeustoimilain 1 luvussa olevan sääntelyn soveltuminen. Lohkoketjuympäristössä voi olla verraten suuri merkitys sillä, että OikTL 1.2 §:n nojalla luvun sääntely on tahdonvaraista. Tästä seuraa erityisen suuri valta tarjouksen tekijälle, sillä tarjouksen tekijä on aloitteen tekijänä tietyllä tavalla tilanteen herra. Mitä seikkaperäisemmästä tarjouksesta on kyse, sitä vähemmän merkitystä on oikeustoimilain 1 luvussa olevalla sääntelyllä.

Kun tarjous toteutetaan lohkoketjuun sijoitettavalla ohjelmalla, tarjous on monesti itsessään sellainen, että oikeustoimilaissa olevalla sääntelyllä ei edes voi olla samaa merkitystä kuin esimerkiksi kirjeitse toteutetun tarjouksen yhteydessä.

Oikeustoimilain 1 luvussa olevan sääntelyn merkitystä pohdittaessa tulee ottaa huomioon myös mahdollinen laajempi konteksti. Esimerkiksi voidaan ajatella tilannetta, jossa A ja B neuvottelevat jostain lohkoketjuun liittyvästä sopimusjärjestelystä. Neuvottelut päättyvät siihen, että A kertoo harkitsevansa tarjouksen tekemistä lohkoketjuun sijoitettavan ohjelman muodossa. A voi jo tässä vaiheessa kertoa B:lle, että tarjouksen hyväksyminen edellyttää, että B luovuttaa viimeistään tietyn päivänä aikana riittävän määrän varoja ohjelmalle. A voi vieläpä tähdentää, että tämä määräaika pätee siinäkin tapauksessa, että A toteuttaisi ohjelman niin, että ohjelmalle varat voisi luovuttaa vieläpä kerrotun päivän jälkeenkin.

Jos A myöhemmin toteuttaisi tarjouksen ohjelman avulla kertomallaan tavalla, tarjouksen voimassaoloajan voidaan katsoa määräytyvän A:n suullisesti kertoman perusteella. Oletetaan seuraavaksi, että B ilmoittaa A:lle suullisesti heti ohjelman havaittuaan, että hän hylkää A:n tekemän tarjouksen. Vaikuttaa siltä, että B ei tämän hylkäämisen jälkeen voisi hyväksyä tarjousta sen enempää kuin siinäkin tapauksessa, että B haluaisi hylätä tarjouksen A:n suullisesti antaman määräajan päättymisen jälkeen. Tarjouksen hylkäämistä koskevan OikTL 5 §:n mukaan hylätty tarjous on nimittäin rauennut, vaikka ”aika, jonka se muuten olisi ollut voimassa, ei ole mennyt umpeen”.

Esimerkkimme B saattaa tarjouksen hylkäämisestä huolimatta muuttaa myöhemmin mieltään ja siirtää varoja A:n lohkoketjuun sijoittamalle ohjelmalle. Koska tarjous on kuitenkin menettänyt voimassaolonsa, oikeudellista sopimusta ei aineellisessa mielessä ole syntynyt. Lopputuloksena saattaa olla, että asianosaiset päätyvät selvittämään välejään tuomioistuimessa. A saattaa suhtautua torjuvasti sopimuksen syntymiseen esimerkiksi siitä syystä, että A oli hylkäämisen tapahtumisen jälkeen sopeuttanut omia toimintojaan sen varaan, ettei sopimusta synny tarjouksen perusteella.

Koska edellä on tarkasteltu oikeustoimilain 1 luvun alaisuuteen kuuluvan tarjouksen tekemistä lohkoketjuun sijoitetun ohjelman avulla, huomioon ei ole otettu määrämuotoa edellyttäviä sopimuksia. Vaikka sopimuksen muodostavat tahdonilmaisut voidaan kotimaisessa oikeudessa toteuttaa yleensä vapaamuotoisesti, oikeudessamme tunnetaan myös erilaisia muotosäännöksiä. Siitä riippuen, mitä lainsäädännössä ilmoitetun muodon laiminlyömisestä seuraa, toisistaan voidaan erottaa varsinaiset, epävarsinaiset ja ohjesisällölliset muotosäännökset. Kyse voi olla esimerkiksi lainkohdasta, jonka mukaan sopimuksen pätevyys edellyttää kirjallista muotoa ja mahdollisesti myös osapuolten allekirjoituksia.



Jos määrämuodon vaatimukseen ei sisälly tahdonilmaisujen samanaikaisuuden vaatimusta, myös määrämuotoinen sopimus saattaa saada alkunsa hyväksyntää edellyttävästä tahdonilmaisusta. Ainakaan niissä tilanteissa, joissa on kyse varsinaisesta muutosäännöksestä, oikeustoimilain 1 luvussa oleva sääntely ei sovellu ainakaan suoranaisesti.

Jos sopimus on lain mukaan tehtävä kirjallisesti, vaatimuksen voi sähköisen viestinnän palveluista annetun lain (917/2014) 181.1 §:n mukaan täyttää myös sellainen sähköinen sopimus, jonka sisältöä ei voida yksipuolisesti muuttaa ja joka säilyy osapuolten saatavilla. Sääntely liittyy sähköistä kaupankäyntiä koskevan direktiivin (2000/31/EY) 9 artiklan 1 kohtaan, jonka mukaan jäsenvaltioiden on huolehdittava siitä, että ”niiden oikeusjärjestelmässä annetaan mahdollisuus sopimusten tekemiseen sähköisessä muodossa”. Jos tarjous edellyttää lainsäädännön mukaan kirjallista muotoa, myös lohkoketjuun sijoitettu ohjelma saattaa näin ollen riittää vaatimuksen täyttämiseen. Sähköisen viestinnän palveluista annetun lain 181.1 §:ssä todetaan vielä, että jos sopimus on lain mukaan allekirjoitettava, sovitaan mitä sähköisistä allekirjoituksista erikseen säädetään.

Sähköistä kaupankäyntiä koskevassa direktiivissä on lueteltu useita sopimustyyppöjä, joiden osalta jäsenvaltioiden ei tarvitse antaa mahdollisuutta sähköiseen muotoon. Sähköisen viestinnän palveluista annetun lain 181.3 §:n mukaan 181.1 §:ssä säädetty ei sovellu kiinteistön kauppaa tai muuta luovutusta koskevaan sopimukseen eikä perhe- tai jäämistöoikeudelliseen sopimukseen. Kirjallista muotoa vaaditaan esimerkiksi silloin, kun kyse on perinnönjakoa koskevasta sopimuksesta, ositusopimuksesta tai avioehtosopimuksesta. Kiinteistön kauppa voidaan tehdä perinteiseen tapaan kirjallisesti tai Maanmittauslaitoksen ylläpitämässä sähköisessä kaupankäyntijärjestelmässä.

## 4 ICO JA TOKENIT

### 4.1 Initial Coin Offering (ICO) pääpiirteissään

Yhdeltä tai useammalta taholta kerätään usein varoja niin, että varojen luovuttaja saa jotain vastinetta panoksestaan. Lohkoketjuteknologia saattaa tarjota tämän kaltaisiin tilanteisiin käyttökelpoisen teknisen alustan etenkin silloin, kun varoja halutaan kerätä yleisöltä. Olivatpa tarkoitusperät mitkä tahansa, melkein kuka tahansa voi melko vaivattomasti laskea liikkeelle erilaisia *tokeneita* eli *rahakkeita*. Listautumisannin käsitettä (englanniksi *Initial Public Offering* eli IPO) mukaillen virtuaalivaluuttojen yhteydessä käytetään nykyään vakiintuneesti ilmausta *Initial Coin Offering* eli ICO, jonka alaisuuteen on laskettu ennen muuta erilaiset joukkorahoituksen muodot.

Rahakkeilla voi olla mitä erilaisimpia tarkoitusperiä ja käyttötapoja. Toisinaan myös bitcoin ja muut siihen rinnastuvat originaalit virtuaalivaluutat luetaan rahakkeiden alaisuuteen, mutta tämä ei ole mikään käsitteellinen välttämättömyys. Mahdollista on sekin, että jonkin jo olemassa olevan lohkoketjusovelluksen puitteissa lasketaan liikkeelle rahakkeita, joilla ei itsessään ole mitään substanssiarvoa siinä muodossa, että ne synnyttäisivät joitain oikeuksia johonkin reaali maailman hyödykkeeseen tai ylipäättään saisivat aikaan sellaisia oikeusasemia, joiden yhteydessä voitaisiin puhua yhteen tai useampaan tahoon kohdistuvasta oikeudesta. Liikkeelle laskijan tarkoituksena on voinut olla yksinkertaisesti, että rahakkeita voidaan näin haluttaessa käyttää maksuvälineenä esimerkiksi bitcoinien ja etheriden tapaan.

Toisaalta rahake voi ilmentää jotain vanhastaan tunnettua oikeutta tai etuutta. Ajatellaan esimerkiksi tilannetta, jossa A tarvitsee lainavaroja. A voi tällöin menetellä esimerkiksi siten, että hän ottaa vastaan euromääräistä luottoa useilta eri tahoilta antaen näille vastineeksi rahakkeita lupauksin, että hän myöhemmin maksaa jokaista yksittäistä rahaketta vastaan 100 euroa. Voidaan sanoa, että A on ottanut itselleen maksuvelvoitteita siten, että velvoitteiden mukaisten suoritusten tekeminen on kytketty A:n liikkeelle laskemiin tokeneihin. A on itse asiassa käyttänyt lohkoketjuympäristöä hyväkseen luodakseen rahakkeita, jotka merkitykseltään vastaavat perinteisiä fyysisiä asiakirjoja, joihin suoritusvelvollisuus on kytketty. A voi näin halutessaan pyrkiä automatisoimaan toimintoja älysopimusten avulla, mutta välttämätöntä tämä ei ole.

Rahakkeet toteutetaan useimmiten siten, että niitä voidaan siirtää käytössä olevan lohkoketjujärjestelmän puitteissa. Kyse ei sinänsä ole mistään teknisestä välttämättömyydestä, ja käytännössä tunnetaankin myös lohkoketjun näkökulmasta siirtokelvottomia rahakkeita (*soulbound tokens*). Tekninen siirtokelvottomuus ei sinänsä tarkoita automaattisesti sitä, että myös rahakkeen edustama oikeus tai

etuus olisi siirtokelvoton niin, ettei sitä voitaisi siirtää pätevästi toiselle lohkoketjujärjestelmän ulkopuolisilla menettelyillä. Siirtokelvottomat tokenit voivat toisaalta liittyä luontevasti myös sellaisiin tilanteisiin, joissa tokenin edustamat oikeudet tai etuudet ovat luonteeltaan henkilökohtaisia eli tiettyyn henkilöön sidottuja. Esimerkiksi äänestysoikeus saattaa olla tällainen oikeus tai etuus.

Käsitteen ICO alaisuuteen voidaan lukea niin erilaisia ilmiöitä, että systemaattisen kuvan luominen erilaisista variaatioista ei ole helppoa. Valtaosa erilaisista järjestelyistä on toteutettu Ethereum-ympäristössä. Monesti kyse on ikävä kyllä ollut etupäässä huijauksista tai vähintään epärealistisista hankkeista, jotka eivät ole johtaneet haluttuihin lopputuloksiin ainakaan hyväuskoisten rahakkeita hankkineiden näkökulmasta. Tästä huolimatta vuonna 2013 alkaneen ICO-ilmion puitteissa on kyetty keräämään valtavasti varoja siten, että suurimmat yksittäiset ICO:t ovat jo itsessään olleet arvoltaan miljardeja euroissa tai dollareissa mitattuna.

Lukuisissa valtioissa ja myös EU:ssa harkitaan paraikaa ICO-järjestelyihin kohdistuvia lainsäädäntötoimia, ja jotkin valtiot ovat jo ehtineet antaa lainsäädäntöä, jossa on otettu kantaa ainakin tietyn tyyppisiin ICO-järjestelyihin. Jossain määrin voidaan itse asiassa tunnistaa tietynlaisia valtioiden välistä kilpailua. Jotkin valtiot ovat yleisesti ottaen halunneet luoda lohkoketjuteknologialle suotuista sääntelykehikkoa, joka voisi omaltaan osaltaan olla houkuttamassa alan kehitystä ja yrityksiä kyseisiin valtioihin. Esimerkiksi Malta toteutti jo vuonna 2018 kolmen säädöksen (*Virtual Financial Assets Act*, *Malta Digital Innovation Authority Act* ja *Innovative Technology Arrangements and Services Act*) kokonaisuuden, jonka tarkoitus oli profiloida Maltaa uusille teknologioille otollisena valtiona ja erityisesti ”lohkoketjusaarena”. Myös EU on ehtinyt antaa aihepiirin kannalta relevanttia sääntelyä, ja lähitulevaisuudessa voidaan odottaa lisää EU-tason lainsäädäntötoimia, jotka yhtenäistävät oikeustilaa EU-alueella.

## 4.2 Perusteita rahakkeista tekniseltä ja oikeudelliselta kannalta

Rahakkeet luodaan tavallisesti jollain yleisellä lohkoketjualustalla älysopimusta hyväksi käyttäen. Tavallisin alusta on Ethereum, jota silmällä pitäen on kehitetty koko joukko ns. rahakestandardeja (*Token standards*), joihin älysopimuksia tehtäessä voidaan turvautua. Tunnetuimpia lienevät ERC-20 ja ERC-721, joissa molemmissa on lukuisia erilaisia toiminnallisuuksia. Näiden kahden standardin perusero liittyy jaotteluun *fungiibeli* / *ei-fungiibeli*. Jos älysopimuksen halutaan luovan toisistaan yksilöllisesti erottuvia rahakkeita, ERC-721 on käytännössä yleisin standardi tähän tarkoitukseen. Rahakkeita kuvataan yleisesti lyhenteellä NFT, joka tulee englannin sanoista *non-fungible token*. Mikäli halutaan luoda fungiibeilitä rahakkeita, ERC-20 on sopiva ja käytännössä yleisin vaihtoehto.

Rahakestandarit tyypillisesti mahdollistavat rahakkeiden siirron muiden toiminnallisuuksien ohella. NFT:t toimivat yleensä siten, että älysovimuksessa on ikään kuin taulukko, joka kertoo, mihin osoitteeseen liittyy mahdollisuus määrätä kustakin yksilöllisestä rahakkeesta. Se henkilö, joka tietää osoitteeseen liittyvän yksityisen avaimen, voi siirtää rahakkeen toiselle. Fungüibelit rahakkeet saattavat sen sijaan toimia esimerkiksi siten, että älysovimus määrittää rahakkeiden kokonaismäärän siten, että tietystä osoitteesta voidaan määrätä rahakkeista enintään kirjattujen transaktioiden perusteella määräytyvän kokonaismäärän verran. Määrät voivat olla jaollisia haluttuun desimaaliin asti, tai sitten rahakkeet on voitu laatia vaikka sellaisiksi, että niistä voidaan määrätä vain kokonaislukuina. Tekniseltä kannalta on hyvä panna merkille, että standardin ERC-20 oletus on 18 desimaalia ja että Ethereum-järjestelmässä tavallaan operoidaan pienimmillä yksiköillä siten, että käyttäjän näkökulmasta yksi kokonainen yksikkö ERC-20 standardin mukaista rahaketta jäsenyy kertolaskuksi yksi kertaa kymmenen potenssiin kahdeksantoista. Standardin mukaisen oletuksen käyttämistä voidaan pitää suositeltavana yhteensopivuuden varmistamiseksi, koska oletusta noudatetaan useissa sovelluksissa.

Jaottelulla fungüibeli / ei-fungüibeli on merkitystä myös oikeudellisesti. Esimerkiksi voidaan ajatella sekoittumisproblematiikkaa, jota tarkasteltiin edellä luvussa 2 originaalien virtuaalivaluuttojen, kuten bitcoinin, osalta. NFT:t eivät voi sekoittua keskenään samoin kuin fungüibelit rahakkeet siinä mielessä, että ne joissain olosuhteissa menettäisivät ”esineellisen” yksilöllisyytensä.

Olipa kyse millaisesta rahakkeesta tahansa, yksittäisiä rahakkeita tai tiettyyn osoitteeseen kytkettyä kokonaismäärää voidaan pitää omistuksen kohteeksi kelpaavina objekteina. Erikseen tulee kysyä kuitenkin sitä, kytkeytyykö rahakkeen omistukseen joitain muitakin oikeusvaikutuksia. Edellä jaksossa 4.1 on jo mainittu se, että A voi luvata tehdä maksusuorituksen euroissa niille henkilöille, jotka tietyllä hetkellä omistavat jonkun tokenin. Tällaiset saamisoikeudet ovat tarkastellussa suhteessa verraten ongelmattomia, koska rahakkeille löytyy luontevia vertailukohtia perinteisistä fyysisistä asiakirjoista. Asetelma ei muutu olennaisesti toiseksi, vaikka A olisi järjestänyt tokenin haltijalle tulevan suorituksen jonkin älysovimuksen avulla siten, että älysovimus suorittaa esimerkiksi tietyn määrän ethereitä siihen osoitteeseen, jolle token tietyllä hetkellä on rekisteröity.

Rahakkeita voidaan kuitenkin pyrkiä käyttämään jonkin oikeuden edustajana myös luonteeltaan toisenlaisissa tilanteissa. Osakeyhtiön yhtiöjärjestykseen saatetaan esimerkiksi ottaa kohta, jonka mukaan yhtiön osakkeet kuuluvat tiettyjen rahakkeiden haltijoille. Irtaimen tai kiinteän esineen omistaja saattaa puolestaan luoda älysovimuksella tokenin kertoen niin älysovimuksessa itsessään kuin eri-

laisilla lohkaketjun ulkopuolisilla tiedotustoimilla, että kyseisen tokenin ja esi-  
neen omistus kytkeytyvät toisiinsa: se, joka omistaa tokenin, omistaa myös ky-  
seessä olevan esineen.

Kaikissa viimeksi mainituissa tilanteissa joudutaan kysymään, onko tarkoitetut  
oikeusvaikutukset mahdollista saada aikaiseksi ilman lainsäädännöstä erityisesti  
saatavaa tukea. Esimerkiksi kiinteän esineen omistuksen osalta on helppo todeta,  
että ainakaan Suomen nykyisin voimassa olevassa oikeudessa ei käytännössä ole  
mahdollista tokenisoida kiinteistön omistusta. Tämä johtuu jo siitä, että kiinteis-  
tön omistusoikeuden luovutusta ei voida toteuttaa vapaamuotoisesti. Keskeinen  
säädös on tässä suhteessa maakaari (540/1994; MK), jonka ensimmäisessä osassa  
säädetään kiinteistön saannosta. Kiinteistön kauppa (MK 2:1) tulee tehdä joko  
erityisessä sähköisessä kaupankäyntijärjestelmässä tai kirjallisesti tiettyä muotoa  
noudattaen. Kuten maakaaren 4 luvussa tarkemmin säädetään, määrämuotoa tu-  
lee noudattaa myös vaihdon, lahjan ja muun maakaareissa tarkoitetun luovutuk-  
sen (ks. myös MK 1:1) yhteydessä.

Jos omistusoikeuden luovutus voidaan toteuttaa pätevästi myös vapaamuotoi-  
sesti, esineen omistaja voi epäilemättä saada rahakkeen avulla aikaiseksi sen, että  
omistusoikeus siirtyy häneltä sille henkilölle, joka saa tokenin omistukseensa. Il-  
man erityislainsäädäntöä ei kuitenkaan päästä siihen, että esimerkiksi tavanomai-  
seen irtaimen esineeseen liittyvät säännöt menettäisivät merkityksensä. Esimer-  
kiksi voidaan ajatella tilannetta, jossa irtain esine jää aiemman omistajansa hal-  
tuun ja jossa tämä myy esineen sivulliselle väittäen, että esine edelleen kuuluu  
hänelle. Aiempi omistaja siis salaa tokenin luovutuksen kautta toteutetun esineen  
omistusoikeuden luovutuksen. Irtaimen esineen myöhempi ostaja voi saada täl-  
laisessa tilanteessa vilpittömän mielen suojaa samoin kuin yleensäkin irtaimen  
esineen kaksoisluovutustilanteissa. Mahdollisuus vilpittömän mielen suojaan voi-  
daan käytännössä ehkäistä esimerkiksi siten, että tokenisoidun irtaimen esineen  
hallinta uskotaan jollekin luotettavalla ulkopuoliselle taholle, jolloin muiden ta-  
hojen on hankala saada aikaiseksi vilpittömän mielen suojaan oikeuttavaa luovu-  
tusta.

Irtaimen esineen ostaja tai muu luovutuksensaaja ei RVA 11 §:n vuoksi voi saada  
vilpittömän mielen suojaa muun muassa silloin, kun kyse on oikealta omistajalta  
varastetusta esineestä. Luovutuksensaajien kannalta edullista olisi tämän vuoksi,  
jos heillä olisi mahdollisuus varmistua siitä, että luovutuksen toteuttava taho to-  
della omistaa esineen. Rahakkeet voivat olla tässä suhteessa yksi kätevä käytän-  
nöllinen keino. Esimerkiksi arvokkaiden tuotteiden valmistaja saattaa omaksua  
rutiininomaisesti menettelyn, jossa jokaista tuotetta vastaa rahake, joka luovute-  
taan samalla kertaa itse tuotteen omistusoikeuden kera. Henkilö, joka myöhem-  
min väittää itseään tuotteen omistajaksi, verraten suurella todennäköisyydellä on-

kin omistaja, mikäli hänellä tuotteen hallinnan ohella on tuotteeseen kytketty rahake tosiasiallisessa määräysvallassaan. Rahakkeiden avulla voidaan varmistua samalla kertaa myös tuotteen autenttisuudesta eli siitä, että kyse on juuri kyseessä olevan valmistajan tekemästä tuotteesta eikä tuoteväärennyksestä.

Erikseen tulee kysyä, onko rahakkeen hankinnan kautta irtaimen esineen omistukseensa saanut henkilö sidottu rahakkeeseen siten, että hän voi määrätä esineestä vain tokenin luovutuksen kautta. Voi käydä esimerkiksi niin, että tokenin ja esineen omistaja haluaisi myydä esineen ulkopuoliselle tavanomaiseen tapaan. Kyseessä oleva ulkopuolinen saattaa olla henkilö, joka ei osallistu eikä haluakaan osallistua lohkoketjupohjaisiin järjestelmiin vaan tahtoo, että kaupasta sovitaan suullisesti tai tavanomaisella kauppakirjalla. Ainakin ensi katsannossa tuntuisi siltä, että esineen omistajalla täytyy olla mahdollisuus määrätä omistuksensa kohteesta muutenkin kuin rahakkeiden luovutuksen kautta.

Koska myös tokenia voidaan toisaalta pitää omana kohteenaan, erikseen on tarkasteltava siihen liittyviä kysymyksiä. Jos ajatellaan esimerkiksi rahakkeen siirtoa, vastattavaksi voi tulla muun muassa se, millaisten edellytysten vallitessa rahakkeen siirto sitoo luovuttajan velkojia. Oma kysymyksensä on, kuinka tulee suhtautua tilanteeseen, jossa luovutetaan oikeudetta toiselle kuuluvia rahakkeita. Näiden kysymysten tarkastelussa saattaa olla aiheellista noudattaa arvopaperioikeudellisia periaatteita (ks. myös edellä jaksot 2.5 ja 2.6), vaikka tokenisaation kohteena olisi esimerkiksi omistusoikeus tavanomaiseen irtaimeen esineeseen. Oikeustilaa ei kuitenkaan voida pitää selvänä.

Kuten edellä jo tuli mainittua, saamisoikeuden kytkeminen rahakkeeseen on ongelmatonta ainakin siinä mielessä, että rahakkeelle löytyy luontevia vertailukohtia perinteisistä fyysisistä asiakirjoista. Erikseen tulee kuitenkin kysyä, kuinka esimerkiksi siirtotilanteisiin liittyviin oikeudellisiin kysymyksiin vastataan. Niissä tilanteissa, joissa rahake ilmentää saamisoikeutta liikkeeseen laskijaa kohtaan, siirtokelpoisuudesta koituu muun ohella myös monia velallisen ja velkojan väliseen suhteeseen liittyviä kysymyksiä. Seuraavassa tarkastellaan suuntaa antavasti näitä kysymyksiä. Käsittely rajoittuu niihin tilanteisiin, joissa rahake on muun kuin aineellisesti siihen oikeutetun hallussa. Tällaiseen asetelmaan saatetaan päätyä esimerkiksi siten, että joku henkilö on menestyksekkään tietomurron seurauksena onnistunut siirtämään toiselle kuuluvia rahakkeita itselleen. Aihepiiriä tarkastellaan kotimaisen oikeuden näkökulmasta, eikä huomiota kiinnitetä kansainvälisen yksityisoikeuden alaisuuteen kuuluviin kysymyksiin. Käytännössä voi aiheutua suuriakin tulkintaongelmia pohdittaessa, minkä valtion sääntely tulee sovellettavaksi erilaisissa riitajutuissa.

Konkretisoidaan aihepiiriä esimerkin avulla. Oletetaan, että B:llä on määräysvallassaan NFT-muotoinen rahake, jota vastaan A on lupautunut maksamaan 100 euroa. C saa teräaseella uhaten aikaiseksi sen, että B pakotettuna siirtää rahakkeen

C:lle. Tämän jälkeen A maksaa 100 euroa C:lle, jonka määräysvallassa olevaan osoitteeseen rahake kuuluu. Herää muun muassa kysymys, voiko A vapautua C:lle tehdyllä suorituksella maksuvelvoitteestaan.

Esimerkissä on kuvattu ongelmatilanne, joka ei suinkaan ole rahakespesifi. Vastaavanlaisia ongelmia voi aktualisoitua esimerkiksi fyysisten velkakirjojen käytön yhteydessä. Ajatellaan vertailun vuoksi tilannetta, jossa A antaa B:lle velvoittautumistarkoituksessa asiakirjan, jonka mukaan A velvoittautuu maksamaan 100 euroa kyseessä olevan asiakirjan haltijalle. Kyse on VKL 11 §:ssä tarkoitettusta haltijavelkakirjasta, joka luokitellaan velkakirjalain järjestelmässä juoksevaksi velkakirjaksi samoin kuin sellaiset velkakirjat, jotka on asetettu nimetylle henkilölle tai tämän määräämälle. Juoksevat velkakirjat ovat arvopapereita siinä mielessä, että kyse on asiakirjasta, jonka hallinta on siitä ilmenevän oikeuden käyttämisen välttämätön edellytys.

Saamisoikeutta ilmentävä rahake laskettaneen yleensä liikkeelle tarkoitusperein, jotka vastaavat juoksevan velkakirjan liikkeelle laskijan tarkoituspieriä. Kyse ei kuitenkaan ole mistään välttämättömyydestä. Jos palataan fyysisiin velkakirjoihin, velkakirjalaisissa tunnetaan myös tavalliset velkakirjat eli nimetylle henkilölle asetetut velkakirjat. Tällaiset velkakirjat eivät ole arvopapereita sen enempää kuin esimerkiksi sopimusasiakirjat, jotka ilmentävät osapuolten toisilleen antamia lupauksia.

Velkakirjalaisissa on otettu kantaa myös siihen, voiko velallinen vapautua velvoitteestaan myös silloin, kun suoritus tapahtuu muulle kuin siihen oikeutetulle. Ratkaisut riippuvat merkittävästi siitä, minkä tyyppisestä velkakirjasta on kyse. Jos kyse on esimerkiksi haltijavelkakirjasta, velallista suojataan varsin tehokkaasti. VKL 19.1 § koskee tilannetta, jossa haltijavelkakirja on maksettu sille, jonka hallussa se oli, mutta sitten käy ilmi, ettei hän ollutkaan oikeutettu vastaanottamaan maksua. Säännöksen mukaan suoritus on kuitenkin pätevä, paitsi milloin velallinen tiesi tai hänen olisi pitänyt tietää maksun joutuvan väärälle henkilölle. Voidaan sanoa, että velvoitteesta vapautuva velallinen saa osakseen maksusuoja.

Kotimaisessa lainsäädännössä ei ole nimenomaisesti otettu kantaa lohkoketju-pohjaisiin rahakkeisiin liittyviin maksusuojaongelmiin. Jos edellä mainitussa rahake-esimerkissä suorituksen tekeminen on kytketty rahakkeeseen perinteiseen juoksevaan velkakirjaan rinnastuvalla tavalla, lienee aiheellista katsoa velkakirjalaisista ilmenevien periaatteiden mukaisesti, että A voi vapautua velvoitteestaan B:hen nähden suorittamalla 100 euroa C:n hallussa olevaa tokenia vastaan. Myös monet muut velkakirjalain haltijavelkakirjoja tai yleisesti ottaen juoksevia velkakirjoja koskevat säännökset soveltunevat analogisesti. Jos C esimerkiksi luovuttaa tokenin D:lle, D lienee oikeutettu saantosuojaan VKL 14 §:stä ilmenevien periaatteiden mukaisesti. Niin maksusuoja kuin saantosuoja koskevissa kysymyksissä voidaan johtoa hakea myös arvo-osuustililaisista olevasta sääntelystä,

jossa pääosin noudatellaan samansuuntaisia sääntöjä kuin fyysisten arvopapereiden järjestelmässä.

Velkakirjalain järjestelmässä juoksevan velkakirjan liikkeelle laskeneen tahon velvoitteesta vapautuminen edellyttää, että velallinen tekee maksun perustellussa vilpittömässä mielessä. Tämä vaikuttaisiärkevältä lähtökohdalta myös tässä tarkastellussa tapauksessa. Voi esimerkiksi käydä niin, että B ottaa ennen suoritusta yhteyttä A:han kertoen uskottavasti C:n menettelystä. Jos A tästä huolimatta tekee suorituksen C:lle, hän ei olekaan oikeutettu VKL 19.1 §:n mukaiseen vilpittömän mielen suojaan.

Tilanne mutkistuu, jos A on automatisoinut takaisinmaksun esimerkiksi lohkoketjuun sijoitetulla älysojimuksella. Kyse voi olla esimerkiksi siitä, että ohjelma tekee automaattisesti tokenin haltijalle maksun tietyllä hetkellä. Jotta tämä varmasti olisi mahdollista teknisesti, muutetaan esimerkkiä niin, että jokainen token oikeuttaa eurojen sijasta tiettyyn määrään ethereitä. Oletetaan, että B ottaa yhteyttä A:han heti pakon lakkaamisen jälkeen ja kertoo tapahtuneesta. Jos A:lla ei kuitenkaan ole mahdollisuuksia vaikuttaa ohjelman toimintaan ja ohjelma automaattisesti siirtää ethereitä C:lle, herää kysymys, onko A vapaa kaikista vastuista B:hen nähden.

Viimeksi mainittua kysymystä tarkasteltaessa tulee lähteä liikkeelle siitä, kuinka järjestely alun perin toteutettiin. A saattoi tuoda kaikella mahdollisella selvyydellä esille, että takaisinmaksu on automatisoitu ja että lohkoketjuun sijoitettu ohjelma siirtää ethereitä täysin A:sta riippumatta. Tällöin voidaan liikkeelle lähteä siitä, että B:n asemassa olevan henkilön täytyy hyväksyä, että A on vapaa vastuistaan, kunhan ohjelma toimii tarkoitettulla tavalla. Huomioon täytyy kuitenkin ottaa myös, että tahdonvapautta on rajoitettu esimerkiksi kuluttajien eduksi ja että niin Suomessa kuin lukuisissa muissakin maissa tunnetaan mahdollisuus sovitteluun kohtuussyistä. Jotta esimerkkitapaukseen voisi antaa vastauksen riittävällä luotettavuudella, tarvittaisiin tarkempaa tosiseikastokuvausta. Joissain olosuhteissa vaatimuksena voisi esimerkiksi olla, että A:n asemassa olevan henkilön täytyy toteuttaa älysojimus niin, että älysojimuksen ohjelmaan voidaan tarvittaessa puuttua myös jälkikäteen kohtuuttomien oikeudenmenetysten estämiseksi.

Lohkoketjupohjaisille rahakkeille voidaan kaiken kaikkiaan keksiä mitä erilaisempia käyttötarkoituksia, ja rahakkeiden omistukseen on myös mahdollista kytkeä erilaisia oikeusvaikutuksia. Viimeisten vuosien aikana käytännöllisestikin merkittäväksi ovat nousseet erilaiset taide-NFT:t, joihin on kiinnitetty runsaasti huomiota myös julkisessa keskustelussa. Aihepiiriin palataan luvussa 6, jossa käsitellään lohkoketjuja immateriaalioikeuksien näkökulmasta. Jotta taide-NFT-ilmioistä saisi oikeanlaisen kuvan, tarvitaan tiettyjä perustietoja immateriaalioikeuksista ja ennen muuta tekijänoikeudesta subjektiivisena oikeutena.



Käytännössäkin tärkeänä ominaisuutena voidaan pitää sitä, että tokenisointi voi koskea myös määräosaista yhteisomistusta. Esimerkiksi arvokkaan maalauksen omistava A saattaa luoda vaikkapa standardia ERC-20 käyttäen 100 tokenia sillä ajatuksella, että kyseessä oleva esine kuuluu määräosaisin yhteisomistuksen tokenien omistajalle siinä suhteessa kuin kukin omistaa tokeneita. Henkilölle, joka omistaa vaikkapa 10 tokenia, kuuluu yksi kymmenesosa esineen omistuksesta. Vastaavalla tavalla voidaan järjestää myös muiden kohteiden omistus, eli määräosaisen tokenisoinnin mahdollisuus ei tietenkään koske ainoastaan irtainten esineiden omistusoikeutta. Määräosainen yhteisomistus saatetaan mahdollistaa myös NFT-pohjaisesti, ja erilaiset ns. pilkotut rahakkeet (*fractional NFT*), joissa NFT on pilkottu toisistaan erottuviin pienempiin osasiin, ovat saaneet osakseen verratan paljon huomiota viime aikoina.

Lohkoketjuteknologia sisältää käteviä mahdollisuuksia järjestää yhteisomistukseen monesti liittyviä käytännön toimintoja. Esimerkiksi kotimaisessa eräistä yhteisomistussuhteista annetussa laissa (180/1958) eli yhteisomistuslaissa lähdetään siitä, että yhteisomistajalla on oikeus toisia yhteisomistajia kuulematta luovuttaa osuutensa ja muutenkin siitä määrätä, samoin kuin myös käyttää yhteistä esinettä hyväkseen sellaisella tavalla, että hänen toimenpiteensä eivät loukkaa muiden yhteisomistajien vastaavia etuja ja oikeuksia (3 §). Toisin tulee sen sijaan suhtautua oikeustoimeen tai toimenpiteeseen, joka koskee esinettä kokonaisuudessaan. Tällaisiin oikeustoimiin tai toimenpiteisiin ei lähtökohtaisesti saa ryhtyä ilman kaikkien yhteisomistajien suostumusta (4 §). Lohkoketjuteknologian puitteissa saatetaan turvautua esimerkiksi *multisig*-lompakkoon, jossa transaktion toteuttaminen edellyttää yhtä useampaa yksityistä avainta. Yhteisomistuslaki soveltuu lain 1 §:n mukaan paitsi yhteisesti omistettuun kiinteistöön, irtaimeen esineeseen tai muuhun tavaraan, soveltuvin kohdin myös osakkeeseen, osuustodistukseen, obligaatioon tai muuhun sellaiseen arvopaperiin.

### 4.3 Sijoittamista koskeva sääntely

Monet henkilöt hankkivat itselleen ICO:ssa tarjottuja rahakkeita yksinkertaistusti sanottuna rikastumisen toivossa. Kyse voi olla esimerkiksi järjestelystä, jossa tokenit tavalla tai toisella tuottavat oikeuden jostain toiminnasta syntyviin tuottoihin. Joku saattaa pitää toimintaa niin lupaavana, että haluaa osallistua siihen sijoittajana. Joku toinen saattaa sen sijaan ryhtyä järjestelyyn luottaen etupäässä siihen, että rahakkeiden arvo tulee myöhemmin nousemaan merkittävästi sen vuoksi, että niille löytyy paljon ostohalukkaita. Olivatpa syyt mitkä tahansa, monet ICO:t ymmärretään etupäässä sijoituskohteiksi, mikä herättää kysymyksen sijoitustoimintaa koskevan sääntelyn soveltumisesta ja merkityksestä.

Nykymuotoiseen talousjärjestelmään kuuluu olennaisena osana sijoittaminen, jossa erilaiset tahot alkaen kotitalouksien kaltaisista pientalouksista aina megaluokan institutionaalisiin sijoittajiin etsivät jatkuvasti sijoituskohteita varoilleen. Sijoitusprofiileissa kuten suhtautumisessa riskiin voi olla eroja, mutta kaikki sijoittajat pyrkivät lopulta kartuttamaan varallisuusasemaansa tai ainakin ylläpitämään sitä. Erilaisia sijoituskohteita on valtava määrä. Sijoitustarkoituksessa voidaan hankkia esimerkiksi saamisoikeuksia, pörssissä listattujen tai muiden osakeyhtiöiden osakkeita, kiinteistöjä tai raaka-aineita. Tällaisiin kohteisiin voidaan monesti sijoittaa myös epäsuorasti eli välillisesti kuten hankkimalla osuuksia rahastosta, jotka tyypillisesti noudattavat etukäteen kerrottua sijoitusstrategiaa.

Merkittävä osa sijoittamisesta tapahtuu käytännössä kaikille avoimilla markkinoilla. Esimerkiksi julkisesti noteeratut osakeyhtiöt voivat järjestää osakeanteja, joihin periaatteessa kaikilla on mahdollisuus osallistua. Tämän tyyppisessä tilanteessa on niin liikkeellelaskijan, sijoittajien kuin koko yhteiskunnan kannalta tärkeää, että sijoittajat voivat parhaalla mahdollisella tavalla arvioida sijoittamiseen liittyviä riskejä ja hyötyjä.

Lukuisissa valtioissa on kiinnitetty erityistä huomiota arvopaperimarkkinoiden tehokkaaseen ja luotettavaan toimintaan. Tässä suhteessa keskeisellä sijalla on lainsäädäntö, jossa eri tavoin pyritään tukemaan sijoittajien luottamusta markkinoiden toimintaan, varmistamaan tasapuolisuus sekä ehkäisemään väärinkäytöksiä. Kun esimerkiksi pörssinoteerattu osakeyhtiö toteuttaa osakeannin, sen tulee huolehtia siitä, että sijoittajille annetaan riittävästi tietoja harkitun sijoituspäätöksen tekemistä varten. Erilaiset tiedonantovelvollisuudet pätevät monesti myös liikkeelle laskun jälkeen, mistä konkreettiseksi esimerkiksi käyvät pörssiyhtiöiden tilinpäätökset ja osavuosikatsaukset.

Arvopaperimarkkinoista säädetään esimerkiksi EU-alueella varsin kattavasti. Tärkein yksittäinen kotimainen säädös lienee arvopaperimarkkinalaki (746/2012; AML), joka samoin kuin muutkin kansalliset arvopaperimarkkinaoikeutta koskevat säädökset perustuu vahvasti EU-sääntelyyn. Jotkin EU-tasoiset säädökset soveltuvat lisäksi suoraan myös Suomessa. Arvopaperimarkkinalaissa säädetään AML 1:1.1:n mukaan arvopaperien yleiseen liikkeeseen saattamisesta, tiedonantovelvollisuudesta arvopaperimarkkinoilla, julkisista ostotarjouksista, arvopaperimarkkinoiden väärinkäytön estämisestä ja valvonnasta. Laki koskee etupäässä kotimaisia arvopaperimarkkinoita, mutta se soveltuu laissa tarkemmin kuvatuissa tilanteissa myös muualla kuin Suomessa tapahtuvaan toimintaan.

Arvopaperimarkkinalaissa asetetaan lukuisia velvollisuuksia etenkin liikkeeseenlaskijalle, jolla AML 2:3:n mukaan tarkoitetaan suomalaista ja ulkomaista yhteisöä, joka on laskenut liikkeeseen arvopaperin. Se, mitä arvopaperilla tarkoitetaan arvopaperimarkkinalaissa, on puolestaan oma kysymyksensä. AML 2:1.1:n mu-

kaan arvopaperilla tarkoitetaan ”sellaista arvopaperia, joka on vaihdantakelpoinen ja joka on saatettu tai saatetaan yleiseen liikkeeseen useiden samansisältöisistä oikeuksista annettujen arvopaperien kanssa”. Lainkohdan mukaan tällainen voi olla esimerkiksi

- 1) osakeyhtiön osake ja muun yhteisön vastaava osuus sekä tällaisesta oikeudesta annettu talletustodistus;
- 2) joukkovelkakirja tai muu velkasitoumus sekä tällaisesta oikeudesta annettu talletustodistus;
- 3) muu arvopaperi, joka oikeuttaa hankkimaan tai myymään 1 tai 2 kohdassa tarkoitettua arvopaperin, taikka arvopaperi, jonka perusteella voi saada arvopaperin, valuutan, koron tai tuoton, hyödykkeen taikka muun indeksin tai arvon perusteella määräytyvän käteissuorituksen; tai
- 4) sijoitusrahastolaissa (48/1999) tarkoitettu rahasto-osuus tai muu siihen rinnastettava yhteissijoitusyrityksen osuus.

Yksikään ICO ei toteudu ilman, että se voidaan kytkeä johonkin toimijaan. Kyse ei välttämättä ole suoraan jostain luonnollisesta henkilöstä tai yleisesti tunnustetusta oikeushenkilöstä. Onhan ajateltavissa, että järjestelyn toteuttajana on esimerkiksi jokin enemmän tai vähemmän itsenäiseen päätöksentekoon pystyvä teknologinen innovaatio. Ainakin toistaiseksi voidaan kuitenkin lähteä siitä, että toteuttajana on yleisesti tunnustettu subjekti. Huomioon tulee ottaa myös, että vaikka esimerkiksi jokin DAO voitaisiin teknisesti katsoa ICO:n toteuttajaksi, DAO:n taustoja riittävän kauaksi selvittäessä päädytään luonnollisiin henkilöihin ja yleisesti tunnustettuihin oikeushenkilöihin.

Vaikuttaa melko selvältä, että ICO-järjestelyn aloittanut yhteisö saattaa olla arvopaperimarkkina-alaissa tarkoitettu liikkeeseenlaskija. Jos asia on näin, liikkeeseenlaskijalla on koko joukko erilaisia velvollisuuksia. Esimerkiksi voidaan ajatella kieltoa menetellä hyvän arvopaperimarkkinatavan vastaisesti ja velvollisuutta julkaista arvopapereita koskeva esite niissä tilanteissa, joissa ei päde mikään poikkeus esitteen julkaisemisvelvollisuudesta. Esitteestä säädetään kotimaisen arvopaperimarkkinain 3 luvussa ja erityisesti ns. esiteasetuksessa eli Euroopan parlamentin ja neuvoston asetuksessa (EU) 2017/1129, annettu 14 päivänä kesäkuuta 2017, arvopapereiden yleisölle tarjoamisen tai kaupankäynnin kohteeksi säännellyllä markkinalla ottamisen yhteydessä julkaistavasta esitteestä ja direktiivin 2003/71/EY kumoamisesta. Vaikka erilaiset ns. *white paper* -dokumentit ovatkin tyypillisiä ICO:jen yhteydessä, toinen kysymys on, vastaavatko ne kaikkiin soveltuvasta lainsäädännöstä johtuviin vaatimuksiin.

Kysymys siitä, onko ICO-järjestelyn aloittaja liikkeeseenlaskija, riippuu olennaisesti siitä, millaisista rahakkeista on kyse. Oikeudellinen luokittelu on osoittautunut hankalaksi monessa käytännön tilanteessa. EU-tasolla aihepiiriä voidaan lähestyä muun muassa siltä kannalta, kuinka Euroopan parlamentin ja neuvoston

direktiivi 2014/65/EU, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta määrittelee keskeiset käsitteet kuten *siirtokelpoisen arvopaperin*. Direktiivin 4 artiklan 1 kohdan 44 alakohdan mukaan siirtokelpoisilla arvopapereilla tarkoitetaan sellaisia arvopaperilajeja maksuvälineitä lukuun ottamatta, jotka ovat vaihdantakelpoisia pääomamarkkinoilla, kuten

- a) yhtiöiden osakkeita ja muita arvopapereita, jotka vastaavat yhtiöiden, henkilöyhtiöiden ja muiden yhteisöjen osakkeita, sekä osaketalletustodistuksia;
- b) joukkovelkakirjoja tai muita arvopaperistettuja velan muotoja, mukaan lukien tällaisia arvopapereita koskevat talletustodistukset;
- c) kaikkia muita arvopapereita, jotka oikeuttavat hankkimaan tai myymään edellä mainitun kaltaisia siirtokelpoisia arvopapereita tai jotka edellyttävät käteissuoritusta, joka määräytyy siirtokelpoisten arvopapereiden, valuuttojen, korkojen tai tuottojen, hyödykkeiden taikka muiden indeksien tai mittareiden perusteella.

Siirtokelpoiset arvopaperit lukeutuvat laajempaan rahoitusvälineiden luokkaan. Rahoitusvälineillä tarkoitetaan direktiivin 2014/65/EU 4 artiklan 1 kohdan 15 alakohdan mukaan liitteessä I olevassa C osassa eriteltyjä välineitä. Määritelmään on hiljattain lisätty tarkennus ”mukaan lukien hajautetun tilikirjan teknologiaa käyttäen liikkeeseen lasketut välineet”. Vaikka jonkin ICO:n yhteydessä ei laskettaisi liikkeelle siirtokelpoisia arvopapereita, kyse saattaa kuitenkin olla rahoitusvälineestä jollain muulla liitteessä kerrotulla perusteella. Liitteessä I olevassa C osassa on yhteensä 11 kohtaa.

Monet ICO-järjestelyt ovat haastavia nykyisen sääntelykehikon näkökulmasta. Aina ei ole helppo sanoa, onko kyse esimerkiksi direktiivin 2014/65/EU näkökulmasta siirtokelpoisesta arvopaperista tai muunlaisesta rahoitusvälineestä. Oikeustilassa on epäselvyyttä, ja EU:n sisämarkkinoiden toimintaa hankaloittaa, että yksittäiset jäsenvaltiot ovat omatoimisesti lähteneet kehittämään sääntelyään. Sellaisen liikkeeseenlaskijan, joka haluaa toimia koko EU:n alueella, tulee ainakin periaatteessa perehtyä erikseen jokaisessa jäsenvaltiossa pätevään sääntelyyn. Olosuhteet ovat muodostuneet sellaisiksi, että Euroopan unionin toiminnasta annetun sopimuksen 114 artiklassa kerrotut edellytykset ovat käsillä. Tämän artiklan nojalla EU:n toimielimillä on toimivalta antaa sisämarkkinoiden toteuttamista ja toimintaa koskevia säännöksiä jäsenvaltioiden lainsäädännön lähentämiseksi.

Lähiainakoina on odotettavissa merkittäviä EU-tason lainsäädäntötoimia, joissa käsitellään suoraan tai välillisesti myös erilaisten ICO-järjestelyjen toteuttamista. Komissio julkaisi 24.9.2020 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi kryptovarojen markkinoinnista ja direktiivin (EU) 2019/1937 muuttamisesta (COM(2020) 593). Ehdotus oli osa laajempaa digitaalisen rahoituksen toimenpidepakettia, johon sisältyi myös uusi digitaalisen rahoituksen strategia

(COM(2020) 591), ehdotus DLT-teknologiaan perustuvien markkinainfrastruktuurien pilottijärjestelmästä (COM(2020) 594), ehdotus rahoitusalan digitaalisesta häiriönsietokyvystä (COM(2020) 595) ja ehdotus tiettyjen rahoituspalveluja koskevien EU:n sääntöjen selkeyttämiseksi tai muuttamiseksi (COM(2020) 596).

Digitaalisen rahoituksen toimenpidepaketissa sekä nimenomaisesti tunnustetaan hajautetun tilikirjan teknologian olemassaolo että annetaan siihen liittyvää sääntelyä. Toimenpidepaketin mukaiset lainsäädäntötoimet on monelta osin saatu jo päätökseen. Esimerkiksi käy tämän teoksen 1.1 jaksossa mainittu Euroopan parlamentin ja neuvoston asetus (EU) 2022/858, annettu 30 päivänä toukokuuta 2022, hajautetun tilikirjan teknologiaan perustuvien markkinainfrastruktuurien pilottijärjestelmästä ja asetusten (EU) N:o 600/2014 ja (EU) N:o 909/2014 sekä direktiivin 2014/65/EU muuttamisesta. Juuri tämän asetuksen 18 artiklaan perustuu se, että direktiivin 2014/65/EU 4 artiklan 1 kohdan 15 alakohdassa nykyään mainitaan nimenomaisesti hajautetun tilikirjan teknologiaa liikkeeseen lasketut välineet. Asetuksen (EU) 2022/858 avulla halutaan ennen muuta edistää teknisiä ja liiketaloudellisia innovaatioita luomalla oikeudellinen kehikko, joka mahdollistaa tiettyjen DLT-pohjaisten markkinainfrastruktuurien väliaikaisen vapauttamisen joistain lainsäädännöstä muuten johtuvista vaatimuksista. Digitaaliseen toimenpidepakettiin liittyvät myös Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2556, annettu 14 päivänä joulukuuta 2022, direktiivien 2009/65/EY, 2009/138/EY, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 ja (EU) 2016/2341 muuttamisesta finanssialan digitaalisen häiriönsietokyvyn osalta.

Komission ehdottamaa asetusta kryptovarojen markkinoista ja direktiivin (EU) 2019/1937 muuttamisesta (myöhemmin MiCA-asetus) ei kuitenkaan ole vielä saatu aikaiseksi. Kyse on verraten tärkeästä säädöksestä myös sijoittamisen kannalta. Komission ehdottaman mukaan asetus koskee varsin laajasti erilaisia kryptovaroja, joilla ehdotuksen 3 artiklan 1 kohdan 2 alakohdan mukaan tarkoitetaan digitaalista arvon tai oikeuksien kirjausta, joka voidaan siirtää ja tallentaa sähköisesti käyttäen hajautetun tilikirjan teknologiaa tai vastaavaa teknologiaa. Ehdotetun 1 alakohdan mukaan hajautetun tilikirjan teknologialla eli DLT-teknologialla puolestaan tarkoitetaan teknologiaa, joka tukee salattujen tietojen hajautettua tallentamista.

Asetusehdotus muodostaa varsin mittavan kokonaisuuden, jonka yksityiskohtaiseen tarkasteluun ei tässä yhteydessä ole mahdollisuuksia. Komission ehdotuksen mukaisen 1 artiklan mukaan asetuksessa vahvistetaan yhdenmukaiset vaatimukset seuraavien seikkojen osalta:

- (a) kryptovarojen liikkeeseenlaskua ja kaupankäynnin kohteeksi ottamista koskevat läpinäkyvyys- ja julkisuusvaatimukset;
- (b) kryptovarapalvelun tarjoajien, referenssivaratokenien liikkeeseenlaskijoiden ja sähköisen rahan tokenien liikkeeseenlaskijoiden toimilupien myöntäminen ja valvonta;
- (c) referenssivaratokenien liikkeeseenlaskijoiden, sähköisen rahan tokenien liikkeeseenlaskijoiden ja kryptovarapalvelujen tarjoajien toiminta, organisaatio ja hallinto;
- (d) kryptovarojen liikkeeseenlaskua, kauppaa, vaihtoa ja säilytystä koskevat kuluttajansuojasäännöt;
- (e) toimenpiteet, joilla estetään markkinoiden väärinkäyttö kryptovarojen markkinoiden luotettavuuden varmistamiseksi.

Myös palvelun tarjoajien asiakkaiden suoja mainittaneen lopullisessa 1 artiklassa, mutta yleisesti ottaen 1 artikla toteutunee suurelta osin komission ehdottaman mukaisesti. Tällä hetkellä on käynnissä tavalliseen lainsäätämisyjärjestykseen kuuluva Euroopan parlamentin ja neuvoston vuoropuhelu (SEUT 294 artikla), ja lokakuussa 2022 valmistui kompromissiehdotus asetuksesta. Seuraavassa lähdetään kuitenkin yksinkertaisuuden vuoksi komission ehdotuksesta. Viittauksia kompromissiehdotukseen tehdään vain valikoidusti silloin, kun tämä näyttää erityisen tarpeelliselta ehdotettuun sääntelyyn tehtyjen muutosten vuoksi.

Komission ehdottamassa asetuksessa on yhteensä yhdeksän osastoa, joissa käsitellään muun muassa muita kryptovaroja kuin referenssivaratokeneita tai sähköisen rahan tokeneita (II osasto), referenssivaratokeneita (III osasto) ja sähköisen rahan tokeneita (IV osasto). Ilmeistä on, että globaalisti toimivat stablecoinit ja niitä koskevat suunnitelmat ovat nopeuttaneet komission toimia. Referenssivaratokenilla tarkoitetaan asetusehdotuksen 3 artiklan 1 kohdan 3 alakohdan mukaan kryptovaratyyppiä, ”jonka arvo pyritään vakauttamaan siten, että sen referenssinä on useiden laillisenä maksuvälineenä käytettävien fiat-valuuttojen arvo, yksi tai useampi hyödyke tai yksi tai useampi kryptovara tai tällaisten varojen yhdistelmä”. Sähköisen rahan token puolestaan viittaa kryptovaratyyppiin, ”jota on pääasiallisesti tarkoitus käyttää vaihdantavälineenä ja jonka arvo pyritään vakauttamaan siten, että sen referenssinä on laillisenä maksuvälineenä käytettävän fiat-valuutan arvo” (4 alakohta).

Sähköisen rahan tokenit liittyvät läheisesti direktiivissä 2009/110/EY tarkoitettuun sähköiseen rahaan. Tässä direktiivissä tarkoitetaan sähköisellä rahalla 2 ar-

tiklan 2 kohdan mukaan ”sähköisesti tai magneettisesti tallennettua rahallista arvoa, joka ilmenee liikkeeseenlaskijaan kohdistuvana saatavana, joka on laskettu liikkeeseen vastaanotettuja varoja vastaan direktiivin 2007/64/EY 4 artiklan 5 kohdassa määriteltyjä maksutapahtumia varten ja jonka muu luonnollinen henkilö tai oikeushenkilö kuin sähköisen rahan liikkeeseenlaskija itse ottaa vastaan”. MiCA-asetusehdotuksessa on paljon sääntelyä, jolla olisi etusija suhteessa direktiivissä 2009/110/EY olevaan sääntelyyn. Toisaalta sähköisen rahan tokenien haltijoille olisi annettava tällaisten sähköisen rahan tokenien liikkeeseenlaskijaan kohdistuva saatava, mikä lisää luottamusta sähköisen rahan tokeneihin. Asetusehdotuksen 44 artiklassa todetaan vielä nimenomaisesti sekin, että kaikki sähköisen rahan tokenit, jotka eivät anna kaikille haltijoille saatavaa, olisivat kiellettyjä.

MiCA-asetusta sovellettaisiin komission ehdotuksen 2 artiklan 1 kohdan mukaan henkilöihin, jotka osallistuvat kryptovarojen liikkeeseenlaskuun tai tarjoavat kryptovarapalveluja unionissa. Artikla sisältää kuitenkin myös suuren määrän erilaisia poikkeuksia.

Komission tarkoituksena ei ole erityisesti suosia DLT-teknologiaa jonkin toisen teknologian kustannuksella. Tämä näkyy muun muassa siinä, että ehdotettua MiCA-asetusta ei sen 2 artiklan 2 kohdan a alakohdan mukaan sovellettaisi kryptovaroihin, joita pidetään direktiivin 2014/65/EU 4 artiklan 1 kohdan 15 alakohdassa määriteltyinä rahoitusvälineinä.

Lokakuun 2022 kompromissiehdotuksessa on useita muutoksia ja lisäyksiä komission ehdotukseen verrattuna. Kiinnostavimpiin lukeutuu se, että 2 artiklaan ehdotetaan kohtaa, jossa säädettäisiin seuraava rajoitus soveltamisalaan: ”This Regulation does not apply to crypto-assets that are unique and not fungible with other crypto-assets.”

Ainutlaatuisuus (*unique*) ja ei-fungiibeli (*not fungible*) lienee erotettu käsitteellisesti toisistaan niin, että asetuksen soveltumattomuus edellyttäisi kummankin edellytyksen täyttymistä. Kompromissiehdotuksen perusteluista käy ilmi, että silmällä on pidetty muun muassa digitaalista taidetta ja kokoelmia. Erikseen mainitaan myös palveluita ja fyysisiä varallisuusarvoja edustavat kryptovarot. Asetuksen soveltamisalan ulkopuolelle halutaan sulkea kohteet, joiden tosiasiallinen merkitys ja taloudellinen merkitys määräytyy yksittäisten kohteiden erityispiirteiden perusteella.

Kompromissiehdotuksen perustelujen mukaan ainutlaatuisten ja ei-fungiibelien kryptovarojen murto-osia ei tulisi pitää uniikkeina ja ei-fungiibeleina. Se, että kryptovaroja lasketaan liikkeelle NFT-muodossa suurina sarjoina tai kokoelmana, viittaa fungiibeliin luonteeseen. Asetuksen tulisi perustelujen mukaan soveltua myös kryptovaroihin, jotka vaikuttavat ainutlaatuksilta ja ei-fungiibeleiltä,

mutta joita niiden tosiasiallisten piirteiden tai näiden ja tosiasiallisen käytön yhdistelmän perusteella voidaan pitää joko fungibileina tai ei-ainutlaatuisina.

#### 4.4 Hyödykerahakkeet (utility tokens)

ICO:n toteuttajana on monesti yritys, joka tarjoaa tai ainakin aikoo tarjota jotain tuotetta tai palvelua asiakkailleen. Rahakkeiden tarkoituksena voi olla tällöin esimerkiksi se, että rahake tuottaa oikeuden tuotteeseen tai palveluun. Rahake eli siihen liittyvä oikeus saattaa olla myös siirtokelpoinen. Monesti rahake ei heti tuota oikeutta tuotteeseen ja palveluun, mikä voi johtua esimerkiksi siitä, että tuotteet ja palvelut on tarkoitus kehittää ICO:n avulla kerättyjen varojen avulla. Tämän tyyppiseen tilanteeseen liittyy helposti se, että ICO:ssa hankitut rahakkeet tavallaan aliarvostetaan suhteessa vastikkeena tarjottavien tuotteiden ja palveluiden arvoon.

Mainitun kaltaisia rahakkeita voidaan kutsua hyödykerahakkeiksi tai -tokeneiksi, englanniksi *utility token*. Jos rahake on siirtokelpoinen, joudutaan kysymään, kuinka siirtoon liittyviin varallisuusoikeudellisiin kysymyksiin tulee vastata. Oikeudelliselta kannalta kyse voi olla esimerkiksi saamisoikeudesta, joka on kytketty rahakkeeseen perinteistä fyysistä arvopaperia vastaavalla tavalla. Ongelmana voi olla esimerkiksi se, millaisin edellytyksin oikeuden luovutus sitoo luovuttajan velkoja. Saamisoikeuksien yhteydessä vastausta vaatii myös kysymys siitä, vapautuuko velallinen velvoitteestaan silloinkin, kun hän tekee suorituksen muulle kuin siihen aineelliselta kannalta oikeutetulle. Virheellisten yleistävien päätelmien välttämiseksi kutakin kysymystä tulee tarkastella omana ongelmanaan, mutta ainakin ensi katsannossa tuntuisi luontevalta noudattaa vastaavia sääntöjä kuin niissä tilanteissa, joissa tuotteeseen tai palveluun oikeuttava saamisoikeus on kytketty fyysiseen asiakirjaan. Ainakin Suomessa oikeustilan arviointia mutkistaa, että kaikki tällaisiin fyysisiin asiakirjoihin liittyvät säännöt eivät ole täysin selviä. Analogia-apua on toisaalta luonteva hakea myös arvo-osuustilailaisissa omaksumista ratkaisuisista.

Hyödykerahakkeen hankkiva henkilö ei välttämättä ole niinkään kiinnostunut jostain rahakkeeseen liittyvästä tuotteesta kuin siitä, että hän olettaa rahakkeen arvon nousevan. Mahdollista on myös sekin, että rahake tuottaa joitain muita oikeuksia kuin yksinkertaisen oikeuden johonkin tuotteeseen tai palveluun. Kyse saattaa kaikkiaan olla tilanteesta, jossa hyödykerahakkeita yleisesti ottaen hankitaan etupäässä sijoitustarkoituksessa. Tällöin herää kysymys, onko kyse sijoittamista koskevan sääntelyn alaisuuteen kuuluvasta menettelystä. Myös viranomaiset eri puolilla maailmaa ovat joutuneet vastatusten tämän ongelman kanssa, ja niin USA:ssa toimiva Securities and Exchange Commission (SEC) kuin eurooppalainen European Securities and Markets Authority (ESMA) ovat enenevästi



kiinnittäneet huomiota hyödykerahakkeisiin ja niiden erilaisiin variaatioihin sijoittamisen ja arvopaperimarkkinoiden näkökulmasta.

Edellisessä jaksossa tarkastellun ehdotetun MiCA-asetuksen eli kryptovarojen markkinoita ja direktiivin (EU) 2019/1937 muuttamista koskevan komission asetusehdotuksen näkökulmasta hyödykerahakkeissa on kyse muusta kryptovarausta kuin referenssivaratokenista tai sähköisen rahan tokenista. Ehdotuksen 4 artiklan 1 kohdan mukaan mainittujen ryhmien ulkopuolelle jääviä kryptovaroja ei saisi tarjota yleisölle tai hakea tällaisten kryptovarojen ottamista kaupankäynnin kohteeksi kryptovarojen kauppapaikassa, jollei liikkeeseenlaskija

- (a) ole oikeushenkilö;
- (b) ole laatinut kyseisiä kryptovaroja koskevaa kryptovaran kuvausta 5 artiklan mukaisesti;
- (c) ole antanut kyseistä kryptovaran kuvausta tiedoksi 7 artiklan mukaisesti;
- (d) ole julkaissut kyseistä kryptovaran kuvausta 8 artiklan mukaisesti;
- (e) täytä 13 artiklassa vahvistettuja vaatimuksia.

Pääsääntöisesti kaikkien vaatimusten olisi täyttyttävä. Mainitun kohdan b–d alakohtia ei kuitenkaan sovellettaisi aina. Näin kävisi 4 artiklan kohdan 2 mukaan, jos

- (a) kryptovarot tarjotaan ilmaiseksi;
- (b) kryptovarot luodaan automaattisesti louhimalla vastineeksi DL-tekniikan ylläpidosta tai liiketoiminnan validoinnista;
- (c) kryptovarot ovat ainutlaatuisia eivätkä ne ole korvattavissa muilla kryptovaroilla;
- (d) kryptovaroja tarjotaan alle 150 luonnolliselle henkilölle tai oikeushenkilölle jäsenvaltiota kohden, ja kyseiset henkilöt toimivat omaan lukuunsa;
- (e) kryptovarojen yleisölle tarjoamisen yhteenlasketut vastikkeet unionissa 12 kuukauden aikana ovat enintään 1 000 000 euroa tai vastaava määrä muussa valuutassa tai kryptovaroina, tai
- (f) kryptovarojen tarjoaminen yleisölle on kohdettu ainoastaan kokeneille sijoittajille, ja kryptovaroja voivat pitää hallussa ainoastaan tällaiset kokeneet sijoittajat.

Jos kyse on palvelua koskevasta hyödyketokenista, joka ei vielä ole toiminnassa, kryptovaran kuvauksessa kuvaillun yleisölle tarjoamisen kesto saisi 4 artiklan 3 kohdan mukaan olla enintään 12 kuukautta. Hyödyketokenilla tarkoitetaan asetusehdotuksen 3 artiklan 1 kohdan 5 alakohdan mukaan ”kryptovaratyyppiä, jonka tarkoituksena on tarjota digitaalinen oikeus DLT-tekniikan kautta saatavilla olevaan tavaraan tai palveluun ja jonka ainoastaan kyseisen tokenin liikkeeseenlaskija hyväksyy”.

MiCA-asetusehdotuksessa on määritetty varsin tarkkaan ne tiedot, jotka olisi sisällytettävä kryptovaran kuvaukseen. Ehdotuksen 5 artiklan nojalla edellytettiin muun ohella yksityiskohtaista kuvausta kryptovaroihin liittyvistä oikeuksista

ja velvollisuuksista sekä näiden oikeuksien käyttämiseen liittyvistä menettelyistä ja ehdoista. Tällaisten tietojen ilmoittaminen ei sinänsä tarkoita sitä, että kyse varmasti olisi kaikin puolin hyväksyttävästä järjestelystä myös esimerkiksi kuluttajansuojaa koskeva sääntely ja yleiset periaatteet huomioon ottaen. Kuluttajien turvaa parantaisi asetusehdotuksessa myös se, että kuluttajilla lähtökohtaisesti olisi 14 kalenteripäivää voimassa oleva peruuttamisoikeus siten kuin asetuksen 12 artiklassa tarkemmin säädettäisiin.

Erilaiset hyödykerahakkeisiin liittyvät ICO-järjestelyt ovat helposti sen luontoisia, että niitä tulee arvioida myös kuluttajansuojaa koskevan sääntelyn kannalta. Esimerkiksi kotimainen kuluttajansuojalaki (38/1978; KSL) koskee KSL 1:1.1:n mukaan kulutushyödykkeiden tarjontaa, myyntiä ja muuta markkinointia elinkeinonharjoittajilta kuluttajille. Laki soveltuu myös, kun elinkeinonharjoittaja välittää hyödykkeitä kuluttajille. Kulutushyödykkeellä tarkoitetaan KSL 1:3:n mukaan ”tavaroita, palveluksia sekä muita hyödykkeitä ja etuuksia, joita tarjotaan luonnollisille henkilöille tai joita tällaiset henkilöt olennaisessa määrässä hankkivat yksityistä talouttaan varten”.

Kuluttajansuojalain sääntely sisältää monenlaista kuluttajalle edullista sääntelyä, joka suurelta osin pohjautuu EU-tason direktiiveihin. Kuluttajansuojalain järjestelmässä tunnetaan myös kollektiivinen kuluttajansuoja.

Hyödyketokeneita tarkasteltaessa ei yleisesti ottaen tule hämääntyä uudesta teknisestä ympäristöstä. Monesti ICO:n yhteydessä liikkeelle lasketulle tokenille löytyy vastine fyysisestä maailmasta. Esimerkiksi jo pitkät ajat on toteutettu palveluja siten, että vastiketta vastaan on annettu fyysisiä lippuja, joita on tarkoitus käyttää palvelua lunastettaessa. Esimerkiksi voidaan ajatella elokuvateatterissa käyntiä. Varsin usein hyödyketoken kuvastaa jotain aiemmin jo tunnettua oikeutta, joka ainoastaan joiltain osin toteutetaan uudella tavalla uudessa teknisessä ympäristössä.

Muiden kryptovarojen kuin referenssivaratokenien tai sähköisen rahan tokenien liikkeeseenlaskijoiden olisi komission ehdottaman MiCA-asetuksen 7 artiklan 2 kohdan mukaan annettava kryptovaran kuvaus ja 6 artiklassa tarkoitettu markkinointiaineisto tiedoksi kotijäsenvaltionsa toimivaltaiselle viranomaiselle vähintään 20 työpäivää ennen kryptovaran kuvauksen julkistamista. Viranomainen voisi tällöin käyttää 82 artiklan 1 kohdassa säädettyjä valtuuksia, joita on verraten paljon. Toimivaltainen viranomainen voisi jopa kieltää kryptovarapalvelun tarjoamisen. Kryptovaran kuvauksessa tulisi selittää, miksi kryptovarot eivät ole direktiivissä 2014/65/EU määriteltyjä rahoitusvälineitä tai strukturoituja talletuksia, direktiivissä 2009/110/EY määriteltyä sähköistä rahaa ja direktiivissä 2014/49/EU määriteltyjä talletuksia.

Asetusehdotuksen 4 artikla siihen liittyvine artikloineen merkitsisi kaikkiaan melko mittavia velvollisuuksia liikkeeseenlaskijalle silloin, kun käsillä ei olisi 4 artiklan 2 kohdassa tarkoitettua poikkeusta. Lokakuun 2022 kompromissiehdotus on pääosin vaikutuksiltaan samansuuntainen, vaikka ehdotuksessa onkin muokattu kohtalaisesti 4 artiklaa ja muitakin II osaston artikloja. Kompromissiehdotuksessa 4 artikla koskee otsikkonsa (*Offers of crypto-assets, other than asset-referenced tokens or e-money tokens, to the public*) mukaisesti muiden kryptovarojen yleisölle tarjoamista. Uudessa 4a artiklassa (*Admission of crypto-assets, other than asset-referenced tokens or e-money tokens, to trading on a trading platform for crypto-assets*) puolestaan otetaan erikseen kantaa kryptovarojen kauppapaikkoihin.

#### **4.5 Laki virtuaalivaluutan tarjoajista liikkeeseenlaskijan kanalta**

Virtuaalivaluutan tarjoajalla tarkoitetaan virtuaalivaluutan tarjoajista annetussa laissa myös virtuaalivaluutan liikkeeseenlaskijaa eli luonnollista henkilöä tai oikeushenkilöä, joka laskee virtuaalivaluutan liikkeelle. Sitä, että sääntely ulottaa vaikutuksensa myös liikkeeseenlaskijaan, ei vaadita EU-sääntelyssä. Hallituksen esityksessä ratkaisua perusteltiin virtuaalivaluuttaan liittyvillä riskeillä ja väärinkäytöksillä (HE 167/2018 vp s. 84). Tässä yhteydessä mainittiin nimenomaisesti myös ICO: ”Erityisesti väärinkäytöksiä on havaittu niin sanottujen Initial Coin Offeringin (ICO) yhteydessä, jossa liikkeeseenlaskija kuvaa virtuaalivaluutan ominaisuuksia, käyttötarkoitusta ja liikkeeseenlaskun ehtoja.”

Virtuaalivaluutan tarjoajista annetussa laissa tarkoitettu virtuaalivaluutta saattaa olla myös arvopaperimarkkinalainsäädännön alainen rahoitusväline. Tämä mahdollisuus käy nimenomaisesti ilmi markkinointia koskevasta VvTL 12 §:stä, jonka 4 momentin mukaan virtuaalivaluuttaan sovelletaan myös arvopaperimarkkinalakia, jos kyse on siinä tarkoitettusta rahoitusvälineestä. Tässä yhteydessä ei ole mahdollisuuksia tarkastella lähemmin, millaisia tulkintaongelmia voi syntyä niissä tilanteissa, joissa rahoitusvälineen tunnusmerkistö täyttyy. Seuraavassa pidetään silmällä vain virtuaalivaluutan tarjoajista annettua lakia siitä näkökulmasta, millaisiin liikkeeseenlaskuihin siinä oleva sääntely tarkkaan ottaen soveltuu.

Ei ole täysin selvää, kuinka laajasti laki virtuaalivaluutan tarjoajista soveltuu ICO:n toteuttajiin. Vaatimuksena on epäilemättä, että käsillä on säädöksessä tarkoitettu virtuaalivaluutta. Kuten edellä on jo tuotu esille, virtuaalivaluutalla tarkoitetaan VvTL 2.1 §:n 1 kohdan mukaan digitaalisessa muodossa olevaa arvoa, jota keskuspankki tai muu viranomainen ei ole laskenut liikkeeseen ja joka ei ole laillinen maksuväline, jota henkilö voi käyttää maksuvälineenä, ja joka voidaan siirtää, tallentaa ja vaihtaa sähköisesti.

Virtuaalivaluutan tunnusmerkistöä ei ole kytketty lohkoketjuteknologiaan, joka kuitenkin on yksi mahdollisuus. Kotimaisessa hallituksen esityksessä kerrotaan, että virtuaalivaluutalla ”voi olla liikkeeseenlaskija tai se voi perustua hajautettuun järjestelmään, kuten Bitcoinin taustalla olevaan lohkoketjuteknologiaan” (s. 84). Tämä lausuma vaikuttaisi viittaavan siihen, että liikkeeseenlaskijaa ei olisi lohkoketjupohjaisten ratkaisujen yhteydessä. On kuitenkin verraten epätodennäköistä, että lausumalla olisi tarkoitettu näin kategorista käytettävään teknologiaan liittyvää rajausta.

Laissa olevaan virtuaalivaluutan tunnusmerkistöön kuuluu, että kyseessä on digitaalisessa muodossa oleva arvo, ”jota henkilö voi käyttää maksuvälineenä”. Hallituksen esityksessä todetaan tältä osin, että osapuolet voivat sopia virtuaalivaluutan hyväksymisestä maksuvälineenä, vaikka se ei ole laillinen maksuväline (s. 84). Tunnusmerkkiin sisältyy vastaavanlaisia tulkintaongelmia kuin direktiivissä (EU) 2018/843 käytettyyn ilmaisuun ”luonnolliset henkilöt tai oikeushenkilöt hyväksyvät vaihdantavälineenä”, jonka tulkinta todettiin jaksossa 2.2 yllättävänkin ongelmalliseksi. Koska laki virtuaalivaluutan tarjoajista kattaa myös liikkeeseenlaskijat, kotimaisella tulkintaongelmalla on vielä suurempi asiallinen ja käytännöllinen merkitys kuin direktiiviin liittyvällä tulkintaongelmalla. Tulkintaongelmat kytkeytyvät luonnollisesti toisiinsa siten, että kotimaisen säädöksen 2 §:ää tulkittaessa tulee ottaa huomioon, kuinka direktiiviä tulkitaan vastaavassa suhteessa.

Esimerkiksi hyödykerahake rinnastuu yksinkertaisimmillaan perinteiseen fyysiseen lippuun, jota vastaan voi saada joitain palveluita. Esimerkiksi perinteistä elokuvalippua tuntuisi verraten oudolta pitää maksuvälineenä sen vuoksi, että lipun näyttämällä pääsee näytökseen, jota varten lippu on ostettu. Samaten tuntuisi oudolta pitää sitä maksuvälineenä sen vuoksi, että joku toinen saattaa olla esimerkiksi valmis vapauttamaan lipun haltijan tämän 10 euron velasta lipun luovuttamista vastaan. Jos mahdollisuus käyttää jotain siirtokelpoista objektia sijais-suorituksena olisi maksuvälineen tunnusmerkki, maksuvälineitä voisivat olla myös esimerkiksi taideteokset, polkupyörät ja valtamerialukset.

Lakia virtuaalivaluutan tarjoajista voidaan kritisoida ainakin epäselvyydestä, vaikka epäselvyys juontuu jo direktiivistä (EU) 2018/843. Esimerkiksi Markus Rahkola on kiinnittänyt kirjoittamassaan *Katsauksessa lohkoketjuteknologioiden hyödyntämiseen Suomessa* (Eduskunnan tulevaisuusvaliokunnan julkaisu 1/2019) huomiota virtuaalivaluutan tunnusmerkistöön laissa ja siihen, mitä hallituksen esityksessä on kerrottu maksuvälineenä käyttämisestä (s. 51). Rahkolan sanoin:

Jos rahakkeella voi olla arvoa, jolla voi saada suoritettua palveluita lohkoketjun sisällä, onko se lainmukainen maksuväline? Epäselvä lainsäädäntö ja siihen liittyvät valvontamaksut sekä käytännöt estävät käytännössä suurelta osin hajautettu-

jen arvonluontiverkoston muodostumisen Suomeen lisäämällä yritysten tai verohallinnon hallinnollista taakkaa erilaisten automatisoitujen digitaalisten palveluiden verotusarvon tai käyttöarvon määrittämisessä. Käytännössä tämä tarkoittaisi sitä, että esimerkiksi automatisoidussa digitaalisessa prosessissa käytettäville palvelurahakkeille tulisi laskea euromääräinen arvo jatkuvasti. Tämä voi johtaa epäselvään tilanteeseen esimerkiksi virtuaalirahakkeita palveluissa hyödyntäville yrityksille, sen suhteen, pitääkö heidän rekisteröityä Finanssivalvonnan ylläpitämään virtuaalivaluutan tarjoajarekisteriin.

Vaikuttaa siltä, että Finanssivalvonta, joka valvoo virtuaalivaluutan tarjoajista annetun lain noudattamista, ymmärtää virtuaalivaluutan käsitteen varsin laajasti. Ainakin voidaan todeta, että Finanssivalvonta lähtee omilla verkkosivuillaan ([www.finanssivalvonta.fi/kuluttajansuoja/virtuaalivaluutat](http://www.finanssivalvonta.fi/kuluttajansuoja/virtuaalivaluutat)) siitä, että ICO on yksi tapa toteuttaa uuden virtuaalivaluutan liikkeeselasku. Virtuaalivaluutat jaetaan samalla karkeasti kolmeen luokkaan huomautuksin, että myös hybridimallit ovat mahdollisia. Pääluokkina erotetaan toisistaan 1) maksuvälineen kaltaiset virtuaalivaluutat, 2) tietyn hyödykkeen maksamiseen käyvät virtuaalivaluutat ja 3) rahoitusvälineiksi luettavat virtuaalivaluutat.

## 5 TIETOSUOJALAINSÄÄDÄNTÖ

### 5.1 Lähtökohtia

Euroopan unionin perusoikeuskirjan 8 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan, ja sama todetaan myös Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklassa. Keskeinen säädös henkilötietojen suojan kannalta EU-alueella on Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta. Tämä *yleisenä tietosuojasetuksena* tai englanninkielisestä nimikkeestä *General Data Protection Regulation* juontuvalla lyhenteellä GDPR tunnettu asetus tuli muodollisesti voimaan 24.5.2016 ja sovellettavaksi 25.5.2018 lukien. Yleinen tietosuojasetus toi mukanaan monia uudistuksia, joskin useat siitä ilmenevät sääntelyratkaisut vastaavat olennaisin osin tietosuojasetuksen antamisen yhteydessä kumottua ns. *henkilötietodirektiiviä* eli Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

Vaikka yleinen tietosuojasetus on asetuksena suoraan voimassa kaikissa EU-maissa, jäsenvaltioilla on eräiltä osin mahdollisuus täydentää ja täsmentää tietosuojasetuksen sääntelyä kansallisella lainsäädännöllä, ja voimassa on myös runsaasti erityislainsäädäntöä. Yleisen tietosuojasetuksen ohella eurooppalaisen tietosuojalainsäädännön kehikkoon kuuluu muun muassa ns. *rikosasioiden tietosuojadirektiivi* eli Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta. *Tietosuojaunionin omissa toimielimissä, elimissä ja laitoksissa* koskee asetus Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta.

Laajempaa kansainvälistä merkitystä on ollut myös Euroopan neuvoston tietosuoja koskevalla yleissopimuksella (1981, ETS 108), johon myös kaikki EU:n jäsenvaltiot ovat liittyneet. Jo melko lailla vanhentunut yleissopimus uudistettiin yhtäaikaaisesti yleisen tietosuojasetuksen valmistelun kanssa, joskaan vuonna

2018 allekirjoituksille avattu modernisoitu sopimusversio ”108+” (CETS 223) ei ole vielä tullut kansainvälisoikeudellisesti voimaan. Seuraavassa lohkoketjujärjestelmiin liittyviä tietosuojavelvoitteita tarkastellaan ensisijaisesti yleisen tietosuojasetuksen kannalta, ja kansalliseen täydentävään sääntelyyn tai sen mahdollisuuksiin viitataan vain eräissä yksittäisissä kohdissa. Erityislainsäädäntöä tai kansainvälisoikeudellisia instrumentteja ei käsitellä lähemmin.

*Henkilötiedoilla* tarkoitetaan tietosuojasetuksen 4 artiklan 1 kohdan mukaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Kyse on kaiken kaikkiaan huomattavan laajasta määritelmästä. Tyypillisiä henkilötietoja ovat esimerkiksi nimi, erilaiset osoitteet, puhelinnumero ja tiedot sairauksista. Lohkoketjuja pohdittaessa on ajateltu varsin yleisesti, että järjestelmässä tunnistena toimivassa käyttäjän *julkisessa avaimessa* voi olla kyse henkilötiedosta. Koska yleinen tietosuojasetus koskee vain luonnolliseen henkilöön liittyviä tietoja, esimerkiksi osakeyhtiöihin tai muihin oikeushenkilöihin liittyvien tietojen käsittely jää asetuksen soveltamisalan ulkopuolelle. Sitä luonnollista henkilöä, johon liittyviä henkilötietoja käsitellään, kutsutaan tietosuojasetuksessa *rekisteröidyksi*, vaikka käsiteltävät tiedot eivät sinänsä muodostaisikaan rekisteriä.

Myös *henkilötietojen käsittely* ymmärretään varsin laajasti: asetuksen 4 artiklan 2 kohdan mukaan sillä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. Käsittely kattaa siis kaikenlaiset toimenpiteet läpi henkilötietojen koko elinkaaren.

Yleinen tietosuojasetus on luonteeltaan *teknologianeutraali*, vaikka juuri teknologisen – erityisesti tietotekniikan – kehityksen myötä tehostuneet tavat käsitellä tietoa ovat luoneet tarpeen tietosuojasetuksen tapaiselle sääntelylle. Tietosuojasetusta sovelletaan sen 2 artiklan 1 kohdan mukaan osittain tai kokonaan automaattiseen henkilötietojen käsittelyyn sekä myös käsittelyyn muussa kuin automaattisessa muodossa, silloin kun henkilötiedot muodostavat rekisterin osan tai niiden on tarkoitus muodostaa rekisterin osa. Asetusta ei kuitenkaan sovelleta aivan kaikkeen henkilötietojen käsittelyyn: yksi 2 artiklan 2 kohdassa säädetyistä poikkeuksista on sellainen henkilötietojen käsittely, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa. Poikkeusta tulkitaan varsin suppeasti, mutta se voi silti olla relevantti myös lohkoketjujen kontekstissa.

On myös huomattava, että aivan kaikki tavalla tai toisella henkilöihin tai henkilöryhmiin laajasti ymmärrettynä liittyvät tiedot eivät ole tietosuoja-asetuksessa tarkoitettuja henkilötietoja. Asetuksen johdanto-osan 26 perustelukappaleessa todetaan nimenomaisesti, että asetus ei koske *anonyymien tietojen* käsittelyä. Kyse voi olla tiedosta, joka ei lainkaan liity tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Toisaalta kyse voi olla laajassa mielessä henkilötiedon luonteen alkujaan omanneesta tiedosta, jolta on kuitenkin myöhemmin poistettu tunnistettavuus niin, ettei rekisteröidyn tunnistaminen ole enää mahdollista. Esimerkiksi tilasto- ja tutkimusympäristöissä käytetään usein anonyymejä tietoja.

Käsiteltävien tietojen anonymisoinnista siis seuraa, ettei tietosuoja-asetus enää sovellu tietojen jatkokäsittelyyn, mikä saattaa olla tavoiteltava lopputulos niin lohkoketjuympäristössä kuin yleisemminkin. Henkilötiedon määritelmässä olen-naista on, että tällainen tieto liittyy *tunnistettavissa* olevaan henkilöön. Jo mainitussa johdanto-osan 26 perustelukappaleessa todetaan tunnistettavuuteen liit-tyen seuraavaa:

Jotta voidaan määrittää, onko luonnollinen henkilö tunnistettavissa, olisi otettava huomioon kaikki keinot, joita joko rekisterinpitäjä tai muu henkilö voi kohtuullisen todennäköisesti käyttää mainitun luonnollisen henkilön tunnistamiseen suo-raan tai välillisesti, kuten kyseisen henkilön erottaminen muista. Jotta voidaan varmistaa, voidaanko keinoja kohtuullisen todennäköisesti käyttää luonnollisen henkilön tunnistamiseen, olisi otettava huomioon kaikki objektiiviset tekijät, ku-ten tunnistamisesta aiheutuvat kulut ja tunnistamiseen tarvittava aika sekä käsit-telyajankohtana käytettävissä oleva teknologia ja tekninen kehitys.

Kuten todettua, yleinen tietosuoja-asetus antaa tietyiltä osin mahdollisuuden ase-tuksen sääntelyn täydentämiseen tai täsmentämiseen kansallisella tasolla, ja se suoranaisesti edellyttääkin jäsenvaltioilta lainsäädäntötoimia esimerkiksi *tietosuo-javiranomaisten* toiminnan järjestämiseksi. Suomessa keskeinen säädös tässä suh-teessa on tietosuojalaki (1050/2018), jossa on toteutettu erinäisiä kansallisia rat-kaisuja tietosuoja-asetuksen sallimissa rajoissa. Tietosuojalain soveltamisala esi-merkiksi on määritetty jonkin verran tietosuoja-asetusta laajemmaksi. Samalla on säädetty myös siitä, että yleinen tietosuoja-asetuskin soveltuu laajemmalti kuin asetuksen 2 artiklassa kerrotaan. Tietosuojalain mukaan tietosuoja-asetus sovel-tuu liki kokonaisuudessaan myös sellaiseen henkilötietojen käsittelyyn, joka suo-ritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön so-veltamisalaan, tai jota jäsenvaltiot suorittavat toteuttaessaan Euroopan unionista tehdyn sopimuksen V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa. Täl-laiset tilanteet on siis tietosuoja-asetuksessa itsessään suljettu asetuksen soveltu-misen ulkopuolelle.

Tietosuoja-asetuksella on verraten laaja *alueellinen soveltamisala*. Asetus soveltuu 3 artiklan mukaan ensinnäkin henkilötietojen käsittelyyn, jota suoritetaan unionin



alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei. Toiseksi asetus soveltuu unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittautunut unioniin, jos käsittely liittyy a) tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionissa riippumatta siitä, edellytetäänkö rekisteröidyltä maksua; tai b) näiden rekisteröityjen käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa. Kolmanneksi asetusta sovelletaan henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä ei ole sijoittautunut unioniin vaan toimii paikassa, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla.

Laajan maantieteellisen soveltamisalan lisäksi rajat ylittävissä käsittelytilanteissa – jollaisia erilaisiin lohkoketjusovelluksiin epäilemättä liittyy – on syytä havaita asetuksen V luvun sääntely *henkilötietojen siirroista kolmansiin maihin* tai kansainvälisille järjestöille. Alueelliseen soveltamisalaan, EU-alueen ulkopuolelle suuntautuvia siirtoja koskevaan sääntelyyn ja näiden mahdollisiin leikkauspisteisiin liittyviin tulkintaongelmiin ei tässä perusesityksessä pystytä lähemmin perehtymään. Lohkoketjujärjestelmissä suoritettavaan henkilötietojen käsittelyyn liittyviä velvoitteita tarkastellaan jäljempänä lähtien siitä oletuksesta, että käsittelystä vastaavat tahot ovat velvollisia noudattamaan yleisen tietosuoja-asetuksen sääntelyä.

## 5.2 Rekisterinpitäjät ja henkilötietojen käsittelijät

Tietosuoja-asetuksen järjestelmässä henkilötietojen käsittelystä vastuussa olevat tahot jaetaan kahteen kategoriaan. Asetuksen mukaisessa henkilötietojen käsittelyssä tärkein rooli on *rekisterinpitäjällä*, jolla tarkoitetaan tietosuoja-asetuksen 4 artiklan 7 kohdan mukaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Määritelmän yhteydessä todetaan vielä, että jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. Tämä tarkoittaa käytännössä sitä, että rekisterinpitäjä voi syntyä myös lain nojalla.

Toisin kuin asetuksen englanninkielisessä versiossa käytetty termi *controller*, suomenkielinen termi rekisterinpitäjä ei kovinkaan selkeästi tuo ilmi sitä, että roolille tunnusomaista on laaja määräysvalta henkilötietojen käsittelyn suhteen. Termi on myös rekisterinpitoon viittaavana vanhahtava, eikä tietosuoja-asetuksen soveltamisen kannalta ole ratkaisevaa, muodostavatko tietoteknisillä laitteilla ja tietojärjestelmissä käsiteltävät henkilötiedot rekisterin. Rekisterinpitäjä vastaa laa-

jasti siitä, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta riippumatta siitä, suorittaako rekisterinpitäjä käsittelytoimenpiteet kokonaan itse vai onko niiden suorittaminen joltain osin ulkoistettu.

Rekisterinpitäjä voikin turvautua henkilötietojen käsittelytoiminnassa ulkopuoliseen apuun. *Henkilötietojen käsittelijällä* tarkoitetaan 4 artiklan 8 kohdan mukaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Myös henkilötietojen käsittelijä vastaa suorittamiensa käsittelytoimien osalta tietosuoja-asetuksen mukaisten velvoitteiden noudattamisesta. Henkilötietojen käsittelijän vastuun ulottuvuutta määrittää rekisterinpitäjän ja henkilötietojen käsittelijän välinen tietojenkäsittelysopimus, jollaista edellytetään ja jonka sisällöstä säädetään tarkemmin tietosuoja-asetuksen 28 artiklassa.

Vastuun kohdentumisen ja jakautumisen sekä rekisteröityjen oikeuksien toteutumisen kannalta erityisen tärkeää on tunnistaa se taho, joka kussakin käsittelytilanteessa toimii rekisterinpitäjän roolissa. Tähän liittyy yksi tietosuojalainsäädännön ja lohkokejuteknologian perusjännitteistä. Jonkin verran yksinkertaistetusti voidaan väittää, että eurooppalainen tietosuojalainsäädäntö rakentuu oletukselle keskitetystä järjestelmästä, jossa yksi selkeästi erotettavissa oleva keskustaho käyttää määräysvaltaa käsittelyn suhteen ja määrittää sen tarkoitukset, laajuuden ja keinot. Lohkoketjuteknologialle tyypillinen hajautettu järjestelmä on tietynlaisessa ideologisessa ristiriidassa tämän lähtökohdan kanssa, mikä tekee tietosuoja-asetuksen mukaisten roolien tunnistamisen haastavaksi.

Täysin yhteensovittamaton tämä ristiriita ei välttämättä ole. Sen lisäksi, että tietosuoja-asetuksen järjestelmässä henkilötietojen käsittelijöitä voi tuki olla useita, asetuksessa tunnustetaan nimenomaisesti, että myös rekisterinpitäjiä voi olla useampia. Niissä tilanteissa, joissa vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, on 26 artiklan mukaan kyse *yhteisrekisterinpitäjistä*.

Lohkoketjuympäristössä voi helpostikin käydä niin, että lohkokejtuun osallinen taho on tietosuojalainsäädännön näkökulmasta rekisterinpitäjä ja/tai henkilötietojen käsittelijä. Muun muassa Euroopan parlamentti on kiinnittänyt asiaan huomiota 13.12.2018 antamassaan päätöslauselmassa *Lohkoketju: tulevaisuuteen suuntautuva kaupapolitiikka*. Päätöslauselmassa on lukuisia tietosuojaan liittyviä mainintoja, ja parlamentti painottaa kohdassa 23, että ”lohkoketjujen käyttäjät voivat toimia samalla sekä rekisterinpitäjinä, kun ne syöttävät järjestelmään henkilötietoja, ja henkilötietojen käsittelijöinä, sillä käyttäjien koneelle tallentuu täydellinen kopio rekisteristä”.

Sillä, että jokin lohkoketjuteknologian avulla toteutettavaan toimintaan osallistuva taho katsotaan rekisterinpitäjäksi, on monenlaisia seurauksia. Koska rekisterinpitäjän rooli tuo mukanaan lukuisia velvollisuuksia ja vastuita, lohkoketjuun osallistuvilla saattaa olla intressi pyrkiä toteuttamaan järjestely siten, etteivät ne joutuisi rekisterinpitäjän asemaan. Rekisterinpitäjyyden kohdentumiseen voidaan vaikuttaa toiminnan tosiasiallista järjestämistä koskevilla sopimusjärjestelyillä, ja yhteisrekisterinpitäjyyden sijaan osapuolet voivat esimerkiksi perustaa yhdessä uuden oikeushenkilön ja pyrkiä järjestämään toiminnan siten, että kyseinen oikeushenkilö määrittää yksin käsittelyn tarkoitukset ja keinot ja toimii siten (ainoana) rekisterinpitäjänä. Tietosuoja-asetuksen vastuurooleihin liittyviä käsitteitä tulkitaan kuitenkin funktionaalisesti, eikä osapuolten ole asiaa koskevin sopimusmääräyksin mahdollista sulkea pois rekisterinpitäjän asemaa sellaisessa tilanteessa, jossa kyseessä oleva taho tosiasiallisesti täyttää rekisterinpitäjän määritelmän eli kykenee päättämään henkilötietojen käsittelyn tarkoituksista ja keinoista.

Jos rekisterinpitäjyyttä ei ole tehokkaasti keskitetty yhdelle taholle, sopimuksilla voidaan ja tulee määrätä vastuun ja tehtävien jakamisesta yhteisrekisterinpitäjien kesken. Tietosuoja-asetuksen 26 artiklan mukaan yhteisrekisterinpitäjien on määriteltävä keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualueet. Järjestelystä eli esimerkiksi yhteisrekisterinpitäjien välisestä, keskeisiltä osiltaan rekisteröityjen saataville saatetusta sopimuksesta on käytävä asianmukaisesti ilmi tahojen todelliset roolit ja suhteet rekisteröityihin nähden. Rekisteröityjä varten voidaan myös nimetä yhteinen yhteyspiste. Yhteisrekisterinpitäjien riskinhallinnan näkökulmasta on kuitenkin syytä huomata, ettei tällainen järjestely rajoita rekisteröidyn mahdollisuuksia käyttää tietosuoja-asetuksen mukaisia oikeuksiaan suhteessa mihin tahansa yhteisrekisterinpitäjästä taikka yhteisrekisterinpitäjän vahingonkorvausvastuuta suhteessa henkilöön, joka on kärsinyt vahinkoa henkilötietojensa lainvastaisen käsittelyn seurauksena.

Koska lohkoketjuteknologia ja erilaiset siihen perustuvat sovellukset muodostavat varsin heterogeenisen kokonaisuuden, kysymystä rekisterinpitäjän tai henkilötietojen käsittelijän tunnusmerkistön täyttymisestä tulee käsitellä eritellysti ja kunkin tilanteen erityispiirteet huomioiden. Kattava esitys kaikista erilaisten lohkoketjusovellusten ja -järjestelmien yhteydessä mahdollisesti kyseeseen tulevista skenaarioista ei ole tässä yhteydessä mahdollinen, mutta seuraavassa tarkastellaan lähemmin rekisterinpitäjän määritelmän täyttymistä muutamassa perustilanteessa.

*Yksityisessä ja suljetussa lohkoketjujärjestelmässä* vastuiden ja roolien määrittely on jossain määrin yksinkertaisempaa kuin julkisissa ja avoimissa lohkoketjuissa. Esimerkiksi jos ryhmä pankkeja tai vakuutusyhtiöitä luo suljetun lohkoketjujärjestelmän asiakkaitaan koskevien tietojen käsittelyyn (esimerkiksi tarkoituksessa

täyttää lain vaatimukset asiakkaan tuntemisesta), voivat ne päättää, että yksi järjestelmään osallisista yrityksistä toimii rekisterinpitäjänä ja käyttää päätösvaltaa käsittelyn tarkoituksista ja keinoista. Vaihtoehtoisesti osallistujatahot voivat perustaa tätä tarkoitusta varten erillisen yhteisyrityksen tai muun oikeushenkilön. Jos muut järjestelmän osalliset tai yhteisyrityksen perustajat tällöin toimivat esimerkiksi transaktioita validoivina louhijoina, ovat ne lähtökohtaisesti henkilötietojen käsittelijän asemassa, ja niiden tulee tehdä rekisterinpitäjän kanssa henkilötietojen käsittelyä koskeva sopimus, jossa vastuuroolit määritellään. Jos mitään osallistujatahoista ei ole valittu ainoaksi rekisterinpitäjäksi tai jos rekisterinpitäjäksi ei perusteta erillistä oikeushenkilöä, kaikkia järjestelmään osallistuvia pankkeja tai vakuutusyhtiöitä on todennäköisesti pidettävä yhteisrekisterinpitäjinä, koska ne ovat valinneet käyttää lohkoketjuteknologiaa omien laillisten velvoitteidensa täyttämiseen liittyvään henkilötietojen käsittelyyn.

Epävarmuutta oikeustilaan luo suljetuissakin järjestelmissä kuitenkin se, että rekisterinpitäjyyden käsitettä arvioidaan toiminnallisin perustein eikä muodollisesti. Niinpä mikä tahansa rekisterinpitäjyyttä koskeva ilmoitus, sopimus tai edes uuden oikeushenkilön perustaminen eivät sinänsä estä sitä, että osallistujat myöhemmin todetaankin yhteisrekisterinpitäjiksi esimerkiksi tietosuojaviranomaisen valvonta- tai sanktioratkaisun taikka vahingonkorvausoikeudenkäynnin yhteydessä.

Bitcoinin kaltaisessa *julkisessa ja avoimessa lohkoketjujärjestelmässä* roolien määrittely on haastavampaa, koska lähtökohtaisesti kuka tahansa voi liittyä järjestelmään. Eräänä näkemyksenä on esitetty, että kuka tahansa, joka suorittaa tällaisessa järjestelmässä transaktioita ja kirjaa niiden yhteydessä henkilötietoja lohkoihin olisi tulkittavissa rekisterinpitäjäksi näiden tietojen osalta. Olennaista olisi siis se, että osallistujalla on kirjoitusoikeus lohkoketjuun ja hän voi siten lähettää transaktioita muiden järjestelmään osallisten validoitavaksi. Esimerkiksi bitcoin-siirtoja tekevät yksityishenkilöt eivät kuitenkaan välttämättä olisi rekisterinpitäjiä, jos nämä siirrot liittyisivät puhtaasti heidän omiin henkilökohtaisiin tai kotitaloutta koskeviin asioihinsa, kuten palveluista maksamiseen kuluttajan asemassa. Tällöin kyse ei olisi ainakaan heidän osaltaan tietosuoja-asetuksen soveltamisalaan kuuluvasta toiminnasta. Jos bitcoin-maksut sen sijaan liittyvät elinkeinon harjoittamiseen tai kaupalliseen toimintaan, myös yksityishenkilö voisi saada rekisterinpitäjän aseman. Toisaalta tietosuoja-asetuksen soveltamisalan ns. kotitalouspoikkeusta on Euroopan unionin tuomioistuimen ratkaisuihin nojautuen tulkittu myös tiukemmin. Oikeuskäytännön mukaan toiminnan yksityistä luonnetta koskevan testin lisäksi on huomioitava myös se, kuinka laajalle joukolle käsiteltävät tiedot julkistetaan. Koska bitcoin-transaktiot ovat lähtökohtaisesti julkisia ja kuka tahansa pystyy tarkastelemaan niitä esimerkiksi *block explorer* -palveluiden

avulla, ei kotitalouspoikkeus tämän tulkinnan mukaan voisi tulla lainkaan sovellettavaksi bitcoin-maksuihin, koska maksuihin liittyviä tietoja lohkoketjuun kirjattaessa henkilötietoja julkistetaan rajoittamattomalle henkilökoukolle.

Bitcoin-maksuja luonnollisille henkilöille suorittava tai niitä heiltä vastaanottava yritys tai muu oikeushenkilö sen sijaan olisi lähtökohtaisesti aina (yhteis)rekisterinpitäjä näiden transaktioiden yhteydessä käsiteltävien henkilötietojen osalta. Sen sijaan oikeushenkilöiden välisessä bitcoin-liikenteessä ei välttämättä lainkaan käsitellä henkilötietoja, jos sen enempää lähettäjän kuin vastaanottajankaan tunnistena toimiva julkinen avain eli bitcoin-osoite ei ole yhdistettävissä edes teoreettisesti tunnistettavissa olevaan luonnolliseen henkilöön.

Bitcoin-louhijoita tai muita avoimessa lohkoketjujärjestelmässä transaktioita validoivia toimijoita ei yleisen käsityksen mukaan ole lähtökohtaisesti pidettävä rekisterinpitäjinä. Vaikka louhijoilla on valtaa käsittelyn teknisistä ratkaisuksista päättämässä, ne eivät itse määritä, mitä henkilötietoja ne käsittelevät ja mihin tarkoituksiin, vaan ne suorittavat tehtäviään siten kuin transaktioita validoitavaksi lähettävät käyttäjät edellyttävät. Koska transaktioiden yhteydessä käsiteltäviin ja lohkoon kirjattaviin tietoihin sisältyy tyypillisesti henkilötietoja, louhijoita voitaneen ainakin jossain olosuhteissa pitää henkilötietojen käsitelijöinä. Lisäksi roolien määrittelyssä on huomioitava, että esimerkiksi Bitcoin-järjestelmässä transaktioiden validointiin osallistuu useita erilaisia toimijoita. Kryptografisten laskentatoimitusten ratkaisemiseen keskittyvien louhijoiden ohella järjestelmään kuuluu erityyppisiä solmuja eli noodeja, jotka pitävät yllä joko osittaista tai täydellistä kopiota Bitcoin-lohkoketjutietokannasta. Koska tietokantaan sisältyy henkilötietoja, tekee sen tallentaminen palvelimelle noodin ylläpitäjistä vähintään henkilötietojen käsitelijän aiemmin mainitussa Euroopan parlamentin päätöslauselmassa esitettyä kantaa vastaavasti.

Jos transaktioita validoivien louhijoiden ja tietokantakopioita ylläpitävien noodien ylläpitäjät tulkitaan henkilötietojen käsitelijöiksi, ongelmaksi muodostuu se, että rekisterinpitäjän ja henkilötietojen käsitelijän tulisi järjestää suhteensa ja vastuunsa henkilötietojen käsittelyä koskevalla sopimuksella. Tämä on kuitenkin käytännössä mahdotonta tilanteessa, jossa kukin transaktioita suorittava järjestelmän osallistuja on omalta osaltaan rekisterinpitäjä. Lisäksi perustellusti voidaan esittää myös sellainen tulkintavaihtoehto, että noodit eivät tietoja muille verkon osallisille lähettäessään tai omaan tietokantakopioonsa tallentaessaan käsittele tietoja pelkästään transaktioita suorittavien käyttäjien lukuun, vaan ne käsittelevät henkilötietoja myös toteuttaakseen omaa tarkoitustaan eli verkon toimintaan osallistumiseksi. Näin tulkiten myös ne voisivat saada rekisterinpitäjän aseman.

Lohkoketjujärjestelmiin liittyy edellä mainittujen lisäksi muitakin toimijatahoja, jotka voivat olosuhteista riippuen saada (yhteis)rekisterinpitäjän tai henkilötietojen käsittelijän aseman. Tällaisia voivat olla esimerkiksi lohkaketjualueen tai -ekosysteemin tekniset ylläpitäjät sekä alueen tai yksittäisten älysovimusten luomiseen osallistuvat ohjelmistokehittäjät. Erityisesti viimeksi mainittujen osalta henkilötietojen käsittelijän rooli on näistä vaihtoehdoista todennäköisempi, ja rekisterinpitäjäyys voinee syntyä vain erityisissä olosuhteissa.

Koska lohkaketjusovelluksiin liittyvät tietosuojasetuksen asemamäärittelyt eivät ole yksiselitteisiä ja ne riippuvat myös kunkin lohkaketjusovelluksen laadusta ja toiminnasta, saattavat lohkaketjuun eri tavoin ryhtyneet tahot joutua rekisterinpitäjiksi tai käsittelijöiksi ilman, että ne ovat tiedostaneet tätä mahdollisuutta. Esimerkiksi tietosuojasetuksen 26 artiklassa edellytetyn yhteisrekisterinpitäjien välisen järjestelyn puuttuminen ei tarkoita sitä, etteikö toimijaa voitaisi pitää rekisterinpitäjänä tai asettaa vastuuseen asetuksen mukaisten velvollisuuksien noudattamatta jättämisestä. Vastaavasti asetuksen 28 artiklassa edellytetyn tietojenkäsittelysopimuksen puuttuminen ei estä sitä, että henkilötietoja rekisterinpitäjän lukuun tosiasiallisesti käsittelevää tahoa pidettäisiin henkilötietojen käsittelijänä. Koska monien tietosuojavelvoitteiden täyttäminen edellyttää etukäteistä suunnittelua ja ennen käsittelyn aloittamista toteutettavia toimenpiteitä, tarkoittaa puute tai virhe roolin tunnistamisessa usein sitä, että henkilötietojen käsittely ei ole asetuksen mukaista. Siksi lohkaketjujärjestelmää suunnittelevan tai sellaiseen osallistumista harkitsevan tahon on aina syytä tarkoin analysoida kyseisen lohkaketjujärjestelmän ominaisuuksia ja omaa suunniteltua toimintaansa tietosuojasetuksen näkökulmasta.

Edellä kuvatun perusteella tietosuojasetuksen mukaisten vastuuroolien tunnistamista ja järjestämistä erilaisissa lohkaketjujärjestelmissä voidaan yleisesti luonnehtia varsin haastavaksi ja samalla myös ongelmalliseksi. Oikeudellinen epävarmuus vastuuroolien määrittelyn sekä muiden jäljempänä käsiteltävien tulkinnallisesti epäselvien kysymysten suhteen voikin muodostaa potentiaalisesti varsin merkittävän esteen tai hidasteen lohkaketjuteknologian hyödyntämiselle ja uusille lohkaketjuperustaisille innovaatioille Euroopan unionissa. Toisaalta lohkaketjuteknologian hyödyntämiseen voi liittyä myös merkittäviä rekisteröidyn oikeuksiin kohdistuvia riskejä, jolloin tietynasteista varovaisuutta uuden teknologian kehittämisessä ja käyttöönotossa voidaan perustella paitsi liiketaloudellisilla vahingonkorvaus- ja sanktoriskeillä, myös perus- ja ihmisoikeuksien turvaamisella.

Jos ja kun erilaisia lohkaketjuteknologiaan perustuvia sovelluksia kuitenkin halutaan ottaa käyttöön teknologian tarjoamien hyötyjen vuoksi, vastuutahojen määrittelyn ongelmista riippumatta sekä rekisterinpitäjiin, käsittelijöihin että rekisteröityihin kohdistuvia taloudellisia, oikeudellisia ja muita riskejä kannattaa

luonnollisesti pyrkiä minimoimaan. Niinpä kaikessa henkilötietojen käsittelytoiminnassa tulee joka tapauksessa kiinnittää erityistä huomiota siihen, että siinä noudatetaan ns. *tietosuojaperiaatteita* mahdollisimman hyvin, varaudutaan toteuttamaan erilaisia *rekisteröidyn oikeuksia* ja huolehditaan henkilötietojen käsittelyn *turvallisuudesta* tarkoituksenmukaisin ja riittävin keinoin. Seuraavissa alaluvuissa perehdytään hieman lähemmin näihin aihepiireihin.

### 5.3 Tietosuojaperiaatteet ja käsittelyn oikeusperusteet

Tietosuojasetuksen 5 artiklassa säädetään useista periaatteista, jotka määrittävät yleisesti henkilötietojen käsittelyä ja jotka on huomioitava kaikessa henkilötietojen käsittelytoiminnassa. Artiklan 1 kohdassa mainitut, henkilötietojen käsittelyä koskevat periaatteet ovat:

- a) lainmukaisuus, asianmukaisuus ja läpinäkyvyys
- b) käyttötarkoitussidonnaisuus
- c) tietojen minimointi
- d) täsmällisyys
- e) säilytyksen rajoittaminen
- f) eheys ja luottamuksellisuus.

Ensimmäisessä alakohdassa mainittu *lainmukaisuus* tarkoittaa etupäässä sitä, että henkilötietojen käsittelylle on oltava jokin asetuksessa määritelty oikeusperuste. Tietosuojasetuksen 6 artiklassa määritellään *yleiset käsittelyperusteet*. Käsittelyn perusteista tietyissä erityisilanteissa säädetään myös asetuksen 9–11 artikloissa. Täydentävää sääntelyä on myös kansallisella tasolla, Suomessa tietosuojalain 2 luvussa ja erityislaeissa.

Yleisiä käsittelyperusteita luetellaan 6 artiklan 1 kohdassa yhteensä kuusi:

- a) rekisteröidyn suostumus
- b) sopimuksen täytäntöönpano
- c) rekisterinpitäjän lakisääteisen velvoitteen noudattaminen
- d) rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen
- e) yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen
- f) rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttaminen.

Luettelo on tyhjentävä, joskin rekisterinpitäjän lakisääteistä velvoitetta sekä yleistä etua tai julkisen vallan käyttöä koskevat perusteet ovat varsin avoimia, ja niissä tarkoitettun käsittelyn perustasta voidaan säätää tarkemmin sekä EU-oikeudessa että kansallisella tasolla. Joka tapauksessa vähintään yhden 6 artiklassa luetelluista perusteluista on sovellettava, jotta käsittely olisi lainmukaista. Tiettyyn

käsittelytoimintaan voi samanaikaisesti soveltua useampikin kuin yksi käsittelyperuste.

Osa käsittelyperusteista on omiaan soveltumaan erilaisiin lohkoketjusovelluksiin paremmin kuin toiset. Kun osapuolten väliset sopimusvelvoitteet toteutetaan lohkoketjujärjestelmän avulla, *sopimuksen täytäntöönpanoa* koskeva peruste on usein luonteva vaihtoehto ainakin tietojen välittömälle käsittelylle. Lohkoketjusovellusten kannalta relevantti *lakisääteinen velvollisuus* voi taas olla esimerkiksi palveluntarjoajan velvollisuus tuntea asiakkaansa, jonka noudattaminen voi vaatia lohkoketjutransaktioita suorittavien tahojen yksilöimiseen ja tunnistamiseen tarvittavien henkilötietojen käsittelemistä (joskaan ei välttämättä näiden tietojen tallentamista kokonaisuudessaan lohkoketjuun). Toisaalta lohkoketjuteknologialla voidaan toteuttaa myös esimerkiksi perinteisten pankkipalveluiden asiakkaiden tuntemisvelvollisuutta koskeva hajautettu, usean pankin yhteinen tietokanta.

Rekisterinpitäjän ja kolmannen tahon *oikeutettua etua* koskevan perusteen kannalta huomionarvoista on, että käsittelyn nojaaminen tähän perusteeseen vaatii oikeutetun edun olemassaolon lisäksi sen arviointia, ovatko rekisteröidyn perusoikeudet kyseisessä käsittelytilanteessa painavampia kuin rekisterinpitäjän/kolmannen osapuolen edut, joita käsittelyllä pyritään turvaamaan. Jos rekisteröidyn oikeudet punnitaan painavammiksi, käsittely ei ole sallittua. Tätä ns. *tasapainotestiä* koskevan Euroopan unionin tuomioistuimen tulkintakäytännön mukaan rekisteröidyn oikeudet ovat lähtökohtaisesti etusijalla rekisterinpitäjän tai kolmannen osapuolen yksinomaan taloudellisiin etuihin nähden, eli kyse on rekisteröidyn hyväksi painotetusta punninnasta. Punninnassa huomioon on otettava myös rekisteröidyn ja rekisterinpitäjän välinen suhde ja se, voiko rekisteröity kyseisessä tilanteessa odottaa tietojaan käsiteltävän. Toisaalta oikeutettu etu on sekä lohkoketjusovelluksissa että yleisestikin varsin houkutteleva käsittelyperuste, koska se on perusteena joustava ja monikäyttöinen. Oikeutettu etu voi soveltua käsittelyperusteeksi riippumatta siitä, onko osapuolten välillä olemassa sopimussuhdetta vai ei, eikä kyseeseen tulevien etujen luonnetta ole enemmälti rajattu.

*Suostumuksen* käyttöön ainoana käsittelyperusteena lohkoketjusovelluksessa liittyy merkittäviä riskejä, erityisesti koska tietosuoja-asetuksen 7 artiklan 3 kohdan mukaan rekisteröity voi perua suostumuksensa milloin vain, ja peruutuksen jälkeen henkilötietoja ei enää saa käsitellä, ellei jotain muuta perustetta ole olemassa. Jos suostumusta kuitenkin käytetään käsittelyperusteena, tulee kyseessä olla 4 artiklan 11 kohdan suostumuksen määritelmän täyttävä vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu. Jäljempänä mainittuja erityisiä henkilötietoryhmiä käsiteltäessä suostumuksen tulee vielä olla lisäksi nimenomainen. Lisäksi 7 artiklassa säädetään esimerkiksi siitä, miten suostumuksen antamista koskeva pyyntö on esitettävä, ja huomioon on syytä ottaa myös se, mitä



johdanto-osan 42–43 perustelukappaleissa todetaan erityisesti suostumuksen va-paaehtoisuuden arvioinnista.

Tietosuoja-asetuksen 6 artiklassa luetelluista perusteista elintärkeiden etujen suo-jaaminen ja yleistä etua koskeva tehtävän suorittaminen tai julkisen vallan käyt-täminen eivät tyypillisesti sovellu ainakaan tavanomaisimpiin lohkoketjusovel-luksiin, eikä näistä jälkimmäinen sovellu lainkaan yksityisen sektorin toimintaan. Toisaalta näihinkin perusteisiin nojaavassa henkilötietojen käsittelyssä voidaan sinänsä hyödyntää monia erilaisia teknologioita – lohkoketjut mukaan luettuna.

Tietosuoja-asetus kieltää lähtökohtaisesti ns. *erityisten henkilötietoryhmien* käsittelyn. Tällaisia (aiemmassa tietosuojalainsäädännössä *arkaluonteisiksi* nimitettyjä) tietoja ovat 9 artiklan 1 kohdan mukaan tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys. Lisäksi kiellettyä on geneettisten tai biometrinen tietojen käsittely hen-kilön yksiselitteistä tunnistamista varten ja terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely. Jos lohkoketjuun halutaan tallentaa tällaisia tietoja, 6 artiklan mukaisen käsittelyperusteen olemassaolon lisäksi jonkin 9 artiklassa 2 tai 3 koh-dassa mainitun poikkeusperusteen tulee täytyä. Artikla sallii poikkeuksista sää-tämisen myös kansallisessa laissa.

Lainmukaisuuden ohella myös muut 5 artiklassa tarkoitetut periaatteet on huo-mioitava kaikessa henkilötietojen käsittelyssä ja siten myös lohkoketjusovelluk-sissa, joissa käsitellään henkilötietoja. Mainitun artiklan 1 kohdan a alakohdassa edellytetään lainmukaisuuden lisäksi sitä, että käsittely on muutoinkin asianmu-kaista ja rekisteröidyn kannalta läpinäkyvää. Läpinäkyvyyden periaatetta konkre-tisoidaan asetuksen III luvun rekisteröidyn oikeuksia koskevissa säännöksissä (erityisesti 12–15 artiklat). Läpinäkyvyyden periaatteesta tai siihen liittyvistä sään-nöksistä ei voi suoraan johtaa yleistä velvollisuutta kertoa rekisteröidyille siitä, että heidän tietojaan käsitellään lohkoketjussa. Asetuksen johdanto-osan 39 pe-rustelukappaleen mukaan rekisteröidyille on kylläkin tiedotettava muun muassa siitä, minkälaisia riskejä käsittelyyn voi liittyä. Koska nämä riskit voivat johtua lohkoketjuteknologian ominaisuuksista, on myös käsittelyn teknisistä perusrat-kaisuista kertominen usein (ellei jopa aina) tarpeen. Lisäksi myöhempänä esitel-tävän käyttötarkoitussidonnaisuuden periaatteen ja siihen sisältyvän tarkoituksen määrittelemisen kannalta on olennaista, että rekisteröidyille kerrotaan sekä välit-tömästi lohkoketjutransaktion toteuttamiseen liittyvästä henkilötietojen käsitte-lystä että tietojen myöhemmästä käsittelytarpeesta, joka ajankohtaistuu, kun loh-koketjuun myöhemmin lisätään uusia lohkoja. Huomionarvoista on myös se, että rekisteröidyille annettavan informaation tulisi olla helposti saatavilla olevassa ja

ymmärrettävässä muodossa, mikä tarkoittaa sitä, ettei hyvin teknisluonteinen dokumentaatio lohkoketjusovelluksen toiminnasta välttämättä riitä (ainakaan yksinään) täyttämään tietosuoja-asetuksen läpinäkyvyys- ja tiedonantovelvoitteita.

Jo sivuttuun käyttötarkoitussidonnaisuuden periaatteeseen sisältyy kaksi osaa: ensinnäkin henkilötiedot tulee kerätä tiettyä, nimenomaista ja laillista tarkoitusta varten, ja toiseksi niitä ei saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Käyttötarkoitussidonnaisuus ei siten estä henkilötietojen tallentamista lohkoketjuun, kunhan tietojen käsittelylle on olemassa peruste ja käsittelyn tarkoitus nimetään. Periaate voi sen sijaan rajoittaa lohkoketjuun tallennettujen tietojen myöhempää käyttöä, johon lohkoketjujärjestelmää suunniteltaessa tai tietoja tallennettaessa ei ole varauduttu.

Tämä ei kuitenkaan tarkoita, että tällainen myöhempi käyttö olisi automaattisesti kiellettyä, vaan alkuperäisen ja uuden tarkoituksen yhteensopivuus on arvioitava tapauskohtaisesti. Kuten aiemman henkilötietodirektiivin 29 artiklan mukainen työryhmä (WP 29) on tuonut ilmi asiaa koskevassa lausunnossaan *Opinion 03/2013 on purpose limitation* (WP 203), tässä analyysissä voidaan huomioida ainakin tietojen keräämisen tarkoituksen ja uuden käyttötarkoituksen suhde, tietojen keräämisen olosuhteet ja rekisteröidyn perusteltavissa olevat odotukset niiden käytöstä, kyseessä olevien tietojen luonne ja jatkokäsittelyn vaikutus rekisteröityyn sekä rekisterinpitäjän toimenpiteet käsittelyn asianmukaisuuden varmistamiseksi ja rekisteröityyn kohdistuvien haittavaikutusten ehkäisemiseksi. Yhteensopivuuden arviointi kytkeytyy myös muihin periaatteisiin: siihen vaikuttavat ainakin käsittelyn asianmukaisuus ja läpinäkyvyys ja erityisesti se, minkälaista informaatiota rekisteröidyille alun perin on käyttötarkoituksista annettu. On yleensäkin tärkeää havaita, että tietosuojaperiaatteet ovat monin paikoin toistensa kanssa limittäisiä ja päällekkäisiä, ja niitä on tulkittava kokonaisuutena eli yhdessä toistensa kanssa.

Lohkoketjuteknologian ja eri tietosuojaperiaatteiden yhteensopivuuden aste vaihtelee huomattavasti. Siinä missä lohkoketjuteknologia luontevasti tukee käsiteltävien tietojen eheyden varmistamista eli ehkäisee tietojen häviämistä, tuhoutumista tai vahingoittumista, ovat lohkoketjujen perusominaisuudet – kuten lohkoketjuun tallennettujen tietojen lähtökohtainen pysyvyys ja niiden replikoituminen hajautetussa verkostossa eri noodeihin – jännitteessä ainakin tietojen säilytyksen rajoittamista koskevan periaatteen kanssa. Tämä periaate ei kylläkään edellytä tietojen täydellistä poistamista minkään kiinteän aikarajan puitteissa, mutta sen noudattamiseksi järjestelmä tulisi suunnitella siten, että lohkoketjuun tallennettujen tietojen yhteys tunnistettavissa oleviin luonnollisiin henkilöihin pystytään katkaisemaan, jos tietojenkäsittelyn tarkoitus ei edellytä tietojen pysyvää säilyttämistä tunnistamisen mahdollistavassa muodossa. Säilytyksen rajoittamiseen läheisesti liittyvä tietojen minimoinnin periaate on niin ikään jännitteessä

lohkoketjuteknologian ominaisuuksien kanssa. Tämäkin periaate on kuitenkin sidottu vahvasti henkilötietojen käsittelyn tarkoitukseen, joten sen huomioiminen puoltaa lohkokeitusovellusten näkökulmasta ensisijaisesti sitä, ettei lohkoketjuun tule alun perinkään tallentaa järjestelmän tarkoituksen ja toiminnan kannalta epäolennaisia henkilötietoja, ja lohkoketjuun tallennettavien tietojen tulee mahdollisuuksien mukaan olla anonymisoidussa tai pseudonymisoidussa muodossa.

Täsmällisyyden periaate koskee tietojen laatua ja ajankohtaisuutta, ja se velvoittaa toteuttamaan kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Koska lohkoketjuun tallennettavat tiedot voidaan yleensä käytännössä päivittää lisäämällä ketjuun uutta tietoa, periaate ei ole ainaakaan täysin yhtensovittamattomassa ristiriidassa lohkoketjuille ominaisen tiedon pysyvyyden kanssa, vaikka näiden välillä jonkinasteinen jännite onkin. Tämäkin periaate konkretisoituu rekisteröidyn oikeuksia koskevissa säännöksissä eli seuraavassa alaluvussa käsiteltävissä tietosuoja-asetuksen 16 ja 17 artikloissa, jotka koskevat oikeutta tiedon oikaisemiseen ja poistamiseen.

Tietosuoja-asetuksen 5 artiklan 2 kohdassa määrätään niin sanotusta osoitusvelvollisuudesta ja sen kohdentumisesta. Siitä, että kaikkia edellä mainittuja periaatteita noudatetaan ja tämä pystytään myös osoittamaan, vastaa nimenomaisesti rekisterinpitäjä, vaikka itse periaatteet soveltuvat myös henkilötietojen käsittelijän suorittamiin käsittelytoimiin. Osoitusvelvollisuudenkin kannalta tärkeää on siis sen tunnistaminen, kuka tai ketkä lohkoketjujärjestelmään osallistuvista ovat rekisterinpitäjiä. Käytännössä osoitusvelvollisuutta voidaan toteuttaa käsittelytoiminnan ja siihen liittyvien järjestelyjen huolellisella ja jatkuvalla dokumentoinnilla. Käsittelytoiminnan täsmällisessä dokumentoinnissa lohkoketjujen toimintamekaniikasta aikaleimoinen ja kryptografisine varmistus- ja suojakeinoineen voi olla apuakin.

Tietosuojaperiaatteiden merkitys tietosuoja-asetuksen järjestelmässä on kaiken kaikkiaan suuri, ja henkilötietojen käsittelyyn osallisten on syytä ottaa ne vakavasti. Periaatteita on noudatettava kaikessa henkilötietojen käsittelyssä ja ne vaikuttavat kattavasti asetuksen ja siihen sisältyvien täsmällisempien, periaatteita konkretisoivien säännöksiä tulkintaan ja soveltamiseen. Periaatteiden asema näkyy myös tietosuoja-asetuksen seuraamusjärjestelmässä, sillä niiden rikkomisesta voidaan määrätä 83 artiklan mukaan hallinnollinen seuraamusmaksu, jonka suuruus on enintään 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Tähän korkeampaan sanktiokategoriaan kuuluvat periaatteiden rikkomisen ohella muun muassa seuraavaksi käsiteltävien rekisteröidyn oikeuksien loukkaukset.

## 5.4 Rekisteröidyn oikeudet

Tietosuoja-asetuksen II luvussa säädetään erilaisista rekisteröidyn oikeuksista. Seuraavassa tarkastellaan valikoituja oikeuksia lohkoketjujen näkökulmasta. Lähtöoletuksena on, että käsillä on lohkoketjusovellus, johon yleinen tietosuoja-asetus sinänsä soveltuu. Lähemmän tarkastelun kohteeksi otetaan vain kolme lohkoketjuteknologian näkökulmasta erityisen kiinnostavalta – ja samalla ongelmalliselta – näyttävää rekisteröidyn oikeutta: oikeus *tietojen oikaisemiseen* (16 artikla), oikeus *tietojen poistamiseen* (17 artikla) ja *automatoituihin yksittäispäätöksiin* liittyvät rekisteröidyn oikeudet (22 artikla). Vaikka 15 artiklassa tarkoitettulla oikeudella saada pääsy tietoihin on tärkeä rooli mainittujen ja muidenkin oikeuksien käytön mahdollistajana, ei seuraavassa käsitellä sitä lähemmin, koska se soveltuu periaatteessa samalla tavalla riippumatta siitä, onko henkilötiedot tallennettu lohkoketjuun vai muuta tekniikkaa tai tallennusallustaa käyttäen. Huomautettakoon tosin, että myös 15 artiklassa tarkoitettujen oikeuden käyttämistä ja toteuttamista voi silti tosiasiallisesti hankaloittaa epäselvä vastuuroolien määrittely hajautetussa järjestelmässä.

Rekisteröidyllä on tietosuoja-asetuksen 16 artiklan mukaan oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheutonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Rekisteröidyllä saattaa olla myös oikeus saada puutteelliset henkilötiedot täydennettyä, mutta täydennysoikeutta arvioidaan suhteessa tietojen käsittelyn tarkoituksiin, eikä rekisteröidyllä siis ole ehdotonta oikeutta tehdä mitä tahansa lisäyksiä tietoihinsa. Todetusti rekisterinpitäjällä on asetuksen nojalla muutenkin velvollisuus huolehtia henkilötietojen oikeellisuudesta, sillä jo 5 artiklan 1 kohdan d alakohdan mukaan henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Täsmällisyyttä koskevassa periaatesäännöksessä edellytetään kaikkia mahdollisia kohtuullisia toimenpiteitä sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Asetuksen 16 artiklassa tarkoitettu oikeus vaatia oikaisua onkin ennen kaikkea keino, jolla rekisteröity voi konkreettisesti vaikuttaa häntä itseään koskevien, rekisterinpitäjän käsittelemien tietojen laatuun.

Jos henkilötietoa säilytetään lohkossa, herää kysymys, seuraako yleisestä tietosuoja-asetuksesta, että lohkoa pitäisi voida muuttaa jälkikäteen. Vaikka tämä on sinänsä teknisesti mahdollista ja erityisesti suljetuissa ja yksityisissä lohkoketjuissa usein myös käytännössä toteutettavissa, kyse on kuitenkin ainakin tietyllä tapaa lohkoketjuideologian vastaisesta ratkaisusta. Vaikka erilaiset konsensusmekanismi mahdollistavat jo nykyään myöhemmät muutokset, monet lohkoketjusovellukset rakentuvat sen lähtökohdan varaan, että muutoksia ei pitäisi tapahtua. Eri-

tyisesti julkisissa ja avoimissa lohkoketjuissa yksittäiset toimijat eivät mahdollisesta tietosuojaoikeudellisesta rekisterinpitäjätalouksesta huolimatta tyypillisesti ole sellaisessa asemassa, että muutosten tekeminen lainkaan onnistuisi.

Tarvetta muuttaa lohkoketjua voitaisiin pyrkiä välttämään sillä, että henkilötietoja ei itsessään sijoitettaisi lohkoketjuun, vaan lohkoketjuun tallennettaisiin ainoastaan viittaus toisaalla säilytettävään henkilötietoon (ns. *off-chain*-tallennus). Tällainen ratkaisu toteuttaisi osaltaan tietojen minimoinnin ja säilytyksen rajoittamisen periaatteita sekä niitä osaltaan täydentävää, tietosuoja-asetuksen 25 artiklasta ilmenevää velvoitetta huomioida tietosuoja henkilötietojen käsittelyyn käytettävien järjestelmien suunnittelussa (*sisäänrakennettu ja oletusarvoinen tietosuoja*). Toisaalta tällaisessa järjestelmässä menetettäisiin osa lohkoketjuteknologian tuottamista eduista juuri siksi, että ketjun ulkopuolelle tallennettua tietoa voidaan poistaa tai muokata jälkikäteen lohkoketjun konsensusmekanismista poikkeavassa menettelyssä (vaikka muutokset voidaankin sinänsä havaita, jos ketjuun sijoitettu, pysyvä viittaus on toteutettu kryptografisen tiivistefunktion avulla). Luottamusta ketjun ulkopuolelle tallennettavaan dataan ja sitä hallinnoivaan tahoon olisi siksi tarpeen turvata muillakin keinoilla. Lisäksi on huomattava, että lohkoketjuun on välttämätöntä tallentaa transaktioiden yhteydessä lohkoketjuympäristössä tunnistettavia toimivia julkisia avaimia, joita voidaan pitää ainakin joissakin olosuhteissa henkilötietoina. Myös lohkoketjuun *off-chain*-tallentamisen yhteydessä sisällytetyt, viitteinä toimivat tiivistetiedot voivat ainakin teoriassa olla tapauskohtaisesti yhdistettävissä luonnollisiin henkilöihin ja siten henkilötietoja, vaikka viitattut tiedot myöhemmin poistettaisiinkin. *Off-chain*-tallennuksella voidaan siis minimoida ketjuun tallennettavien henkilötietojen määrää, mutta ei yleensä välttää kokonaan henkilötietojen tallentamista lohkoketjuun.

Tietosuoja-asetuksen 16 artiklan sääntelyä ei kuitenkaan tarvitse välttämättä ymmärtää siten, että lohkoketjuun jo sisällytettyihin lohkoketjuun olisi pakko tehdä muutoksia. Saattaisi nimittäin riittää, että lohkoketjuun lisättävä uusi lohko sisältäisi tietosuoja-asetuksen edellyttämät korjaukset ja täsmennykset. Asetuksen 16 artiklassa nimenomaisesti mainitaan myös ”oikeus saada *puutteelliset* henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys” (korostus tässä). Artiklan sanamuoto ei kuitenkaan vastaa suoraan siihen, onko lohkoketjuissa luontevasti toteutettavissa oleva, uuden tiedon lisäämisellä suoritettava täydentäminen hyväksyttävä keino myös *epätarkkojen* tai *virheellisten* tietojen oikaisuun. Jotta säännöksen tarkoitus toteutuu, olennaista on vähintäänkin varmistaa se, ettei lohkoketjuun jäävä virheellinen tieto enää voi tulla aktiivisen käsittelyn kohteeksi ja esimerkiksi vaikuttaa rekisteröidyn oikeuksia tai velvollisuuksia koskevaan päätöksentekoon.

Tietojen oikaisemista koskevan oikeuden ohella rekisteröidyillä on tietosuoja-asetuksen 17 artiklan mukaan oikeus tietojen poistamiseen eli ”oikeus tulla unohdetuksi”. Kyse ei ole ehdottomasta oikeudesta, vaan jotta rekisterinpitäjä olisi velvollinen poistamaan henkilötiedot, tulee jonkin artiklan 1 kohdassa luetelluista perusteista täytyä. Poistamisoikeus on lähtökohtaisesti olemassa, jos

- a) henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin;
- b) rekisteröity peruuttaa suostumuksensa, johon käsittely on perustunut 6 artiklan 1 kohdan a alakohdan tai 9 artiklan 2 kohdan 2 alakohdan mukaisesti, eikä käsittelyyn ole muuta laillista perustetta;
- c) rekisteröity vastustaa käsittelyä 21 artiklan 1 kohdan nojalla eikä käsittelyyn ole olemassa perusteltua syytä tai rekisteröity vastustaa käsittelyä 21 artiklan 2 kohdan nojalla;
- d) henkilötietoja on käsitelty lainvastaisesti;
- e) henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi;
- f) henkilötiedot on kerätty 8 artiklan 1 kohdassa tarkoitettun tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.

Poistamisperusteet eivät juurikaan itsessään rajoita henkilötietojen käsittelyä, vaan useat niistä soveltuvat sellaisiin tilanteisiin, joissa henkilötietoja ei asetuksen mukaan muutenkaan saisi käsitellä. Myös edellä käsitellyt tietosuojaperiaatteet (erityisesti säilytyksen rajoittaminen, lainmukaisuus, tietojen minimointi ja käytötarkoitussidonnaisuus) edellyttävät, ettei henkilötietoja käsitellä enää sen jälkeen, kun ne eivät ole tarpeen (a alakohta), tai kun käsittelylle ei ole enää laillista perustetta (b alakohta). Henkilötietojen lainvastainen käsittely taas on – luonnollisesti – kiellettyä poistamisoikeudesta riippumatta, ja d alakohta onkin ymmärrettävä hyvin yleisluontoiseksi perusteeksi. Sanamuoto ”on käsitelty” tarkoittaa, että rekisteröity voi vaatia tietojen poistamista myös silloin, kun tietoja on *aiemmin* käsitelty lainvastaisesti, vaikka kyseisellä hetkellä käsittelyyn sinänsä olisikin laillinen peruste. Lisäksi rekisteröidylle on haluttu antaa erityinen mahdollisuus puuttua sinänsä lainmukaiseenkin käsittelyyn silloin, kun käsittely perustuu rekisterinpitäjän oikeutettuun etuun (c alakohta) tai kun hän on antanut suostumuksensa tietoyhteiskunnan palvelujen tarjoamisen yhteydessä ollessaan alaikäinen (f alakohta). Artiklan pääasiallinen merkitys on siis kuitenkin se, että se tekee tietojen poistamisesta 1 kohdassa mainituissa tapauksissa rekisteröidyn subjektiivisen oikeuden, jonka toteuttamista hän voi tehokkaasti vaatia tarvittaessa myös tuomioistuimessa.

Jos tiedot on poistettava, tämän tulee tapahtua ilman aiheetonta viivytystä. Oikeutta tulla unohdetuksi vahvistaa osaltaan siihen liittyvä ilmoitusvelvollisuus,

josta säädetään 17 artiklan 2 kohdassa. Jos rekisterinpitäjä on julkistanut henkilötiedot ja poistamisoikeus on olemassa, sen tulee ilmoittaa muille näitä henkilötietoja käsitteleville rekisterinpitäjille siitä, että rekisteröity on pyytänyt poistamaan näihin henkilötietoihin liittyvät linkit tai näiden henkilötietojen jäljennökset tai kopiot. Ilmoittamisvelvollisuus ei kuitenkaan ole ehdoton eikä rekisterinpitäjä ole vastuussa siitä, että toiset rekisterinpitäjät todella poistavat tiedot. Rekisterinpitäjän vastuulla on ainoastaan kohtuullisten toimenpiteiden toteuttaminen asiasta ilmoittamiseksi, ja tähän liittyvässä arvioinnissa huomioidaan artiklan sanamuodon mukaan käytettävissä oleva teknologia ja toteuttamiskustannukset. Hajautetussa lohkaketjujärjestelmässä uudet lohkot replikoituvat lähtökohtaisesti automaattisesti eri nooidien tietokantakopioihin, ja tätä ominaisuutta voitaneen hyödyntää myös 17 artiklan 2 kohdan mukaisen ilmoittamisvelvollisuuden automatisoinnissa. Käytetystä tietojen poistamistekniikasta riippuen tämä ei kuitenkaan aina riitä tarkoituksenmukaisen lopputuloksen saavuttamiseen, ja muutkin toimenpiteet voivat olla tarpeen.

Oikeus tulla unohdetuksi ei ole aivan niin vahva oikeus kuin edellä lausutun perusteella voisi kuvitella. Tietosuoja-asetuksen 17 artiklan 3 kohdan mukaan sen enempää 1 kuin 2 kohtaa ei nimittäin sovelleta, jos käsittely on tarpeen

- a) sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi;
- b) rekisterinpitäjään sovellettavaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisäätöisen velvoitteen noudattamiseksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten;
- c) kansanterveyteen liittyvää yleistä etua koskevista syistä 9 artiklan 2 kohdan h ja i alakohdan sekä 9 artiklan 3 kohdan mukaisesti;
- d) yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti, jos 1 kohdassa tarkoitettu oikeus todennäköisesti estää kyseisen käsittelyn tai vaikeuttaa sitä suuresti; tai
- e) oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Teoriassa mikä vain 3 kohdassa luetelluista poistamisoikeutta rajoittavista perusteista voi tulla kyseeseen myös erilaisissa lohkaketjujärjestelmissä. Toisaalta poistamisvelvollisuuden toteuttamisesta ei vapauta pelkästään se, että jokin tietojenkäsittelytoimi on päätetty järjestää lohkaketjuteknologian avulla.

Yleisestikin merkittävä avoin tulkintakysymys on, mitä 17 artiklassa tarkalleen ottaen tarkoitetaan tietojen poistamisella. Vaatiiko oikeuden toteuttaminen aina tietojen lopullista ja täydellistä hävittämistä ja tuhoamista kaikista mahdollisista lähteistä ja kopioista, vai voiko riittää, että tiedot merkitään poistetuiksi tai rekisterinpitäjä estää niiden jatkokäsittelyn teknisillä keinoilla, vaikka tietoja ei suora-

naisesti hävitettä tietokannasta tai varmuuskopioista? Tietoteknisessä toimintaympäristössä datan tehokas ja lopullinen hävittäminen ei nimittäin aina ole teknisesti aivan yksinkertainen toimenpide, vaan muun muassa käytetyistä menetelmistä ja tallennusvälineen tyypistä riippuen ”poistettu” data saattaa olla eri keinoilla ja työkaluilla palautettavissa tarkasteltavaksi. Poistamisen merkitykseen tai keinoihin ei oteta kantaa itse asetuksessa eikä sen johdanto-osan perustelukappaleissa. Euroopan unionin tuomioistuimen oikeuskäytännöstä on löydettävissä tukea sekä ehdottomalle tuhoamisvelvollisuudelle (ECLI:EU:C:2017:994, C-434/16, Peter Nowak v. DPC) että joustavammalle, rekisterinpitäjän tosiasialliset toimintamahdollisuudet ja käytetyn tekniikan ominaispiirteet huomioivalle tulkintavaihtoehdolle (ECLI:EU:C:2014:317, C-131/12, Google Spain v. AEPD ja Mario Costeja González). Tapaukset eivät koskeneet nimenomaisesti lohkoketjusovelluksia.

Jos rekisteröidyllä on oikeus tietojen poistamiseen, lohkoketjuympäristössä joudutaan tekemisiin niiden ongelmien kanssa, joita sivuttiin jo edellä käsiteltäessä oikeutta tietojen oikaisemiseen. Tietojen täydellinen tuhoaminen on käytännössä haastavaa ja ongelmallista erityisesti julkisissa ja avoimissa lohkoketjujärjestelmissä. Lisäksi on syytä huomata, että jos lohkoketjusovelluksessa hyödynnetään esimerkiksi Ethereumin tapaista valmista alustaa tai ekosysteemiä, yksittäistä sovellusta suunniteltaessa ja rakennettaessa ollaan sidottuja alustatason teknisiin ratkaisuihin. Sovellusta voi tämänkin vuoksi olla vaikeaa tai mahdotonta toteuttaa siten, että sen toiminnan kannalta tarpeelliset henkilötiedot voitaisiin tarvittaessa myöhemmin hävittää lohkoketjusta.

Poistamisen käsitettä joustavasti tulkittaessa poistaminen voitaisiin katsoa asianmukaisesti toteutetuksi ilman, että lohkoketjuun jo liitettyihin lohkoihin kirjattuja tietoja tarvitsisi muokata tai hävittää. Tällöinkin jo lohkoketjusovellusta suunniteltaessa on syytä harkita ja suunnitella, miten poistamisoikeus voidaan toteuttaa mahdollisimman tehokkaasti ja rekisteröityyn kohdistuvat riskit minimoiden. Yksi vaihtoehto voisi olla lohkoketjuun tallennettavien henkilötietojen vahva kryptografinen salaaminen, jolloin tietojen jatkokäsittely voitaisiin myöhemmin varsin tehokkaasti estää hävittämällä salauksen purkamisen mahdollistava salausavain. Tämä tosin edellyttäisi sitä, että kutakin henkilöä koskevat tiedot salattaisiin eri salausavaimella, jotta yhden henkilön tietojen poistamisoikeuden toteuttaminen salausavaimen hävittämisellä ei vaikuttaisi muiden rekisteröityjen henkilötietoihin. Jos lohkoketjuun tallennettavat tiedot liittyvät muuhun henkilöön kuin transaktion suorittajaan, vaatii tämä siis ylimääräistä salauskerrosta juuri kyseiseen henkilöön yhdistettävällä salausavaimella. Lisäksi mallin toteuttaminen vaatii sitä, että salausavainten hallintaan kiinnitetään huomiota ja poistamisoikeutta toteutettaessa pystytään varmistamaan, ettei kyseisen tiedon purkamisen mahdollistava avain jää minkään järjestelmään osallisen tahon haltuun niin, että tämä



taho edelleen pystyisi purkamaan salauksen ja jatkamaan tietojen käsittelyä. Käsiteltävien henkilötietojen tyypeistä ja lohkoketjusovelluksen tarkoituksesta riippuen tällainen salaukseen perustuva poistamismalli ei välttämättä ole kaikissa tilanteissa lainkaan käytökelpoinen poistamisoikeuden toteuttamiseen.

Toinen poistamisoikeuden toteuttamista edesauttava malli voisi olla edellä mainittu henkilötietojen *off-chain*-tallentaminen tai se, että ainakin ketjussa olevat tiedot luonnollisiin henkilöihin yhdistävät tunnisteet tai muut vastaavat tunnistamisen mahdollistavat lisätiedot säilytettäisiin ketjun ulkopuolella. Tällöin lohkoissa olevat tiedot ja tietosarjat olisivat itsessään *pseudonymisoituja*, eli niiden yhdistämiseksi tiettyyn rekisteröityyn tarvittaisiin muualla säilytettäviä lisätietoja. Pseudonymisointi on tietosuoja-asetuksen veloitteiden toteuttamista edesauttava ja käsittelyyn liittyviä riskejä vähentävä toimenpide, mutta pseudonymisoidut tiedot ovat tietosuoja-asetuksen näkökulmasta edelleen henkilötietoja. Jos tunnistettavuus poistetaan kokonaan ja peruuttamattomasti, kyse on anonyymeistä tiedoista, joiden käsittely ei enää kuulu lainkaan asetuksen alaan. Jos lohkoketjuun tallennettujen tietojen tunnistettavuus voidaan poistaa ja tiedot sitä kautta anonyymisoida, tämän toimenpiteen voitaisiin katsoa toteuttavan myös 17 artiklan mukaisen poistamisoikeuden.

Ongelmaksi saattaa kuitenkin muodostua se, että on hyvin tulkinnanvaraista, milloin tiedot todella ovat anonyymejä. Ensisijaisten tunnisteiden hävittämisestä huolimatta tiedot voivat niiden sisällöstä ja käytettävissä olevista muista tietoinaistoista, tiedonkäsittelytekniikoista ja profiloitimenetelmistä riippuen tosiasiallisesti olla edelleen yhdistettävissä tunnistettavissa oleviin luonnollisiin henkilöihin. Tietosuoja-asetuksen johdanto-osan 26 perustelukappaleen mukaan määriteltäessä sitä, onko luonnollinen henkilö tunnistettavissa, olisi otettava huomioon kaikki keinot, joita joko rekisterinpitäjä tai muu henkilö voi kohtuullisen todennäköisesti käyttää mainitun luonnollisen henkilön tunnistamiseen suoraan tai välillisesti, kuten kyseisen henkilön erottaminen muista. Käytännössä anonyymiyden arviointi on hyvin tapauskohtaista, ja tilanne voi myös muuttua ajan myötä siten, että aiemmin anonyymeinä pidetyt tiedot pystytäänkin tulevaisuudessa jälleen vaivatta yhdistämään rekisteröityihin.

Edellä päähuomio on ollut siinä, mitä tietosuoja-asetus merkitsee lohkoketjuun merkittyjen tietojen kannalta. Huomioon tulee kuitenkin ottaa myös, että vaadittujen muutosten tekeminen tai tietojen poistaminen edellyttää luonteeltaan menettelyllistä varautumista. Joudutaan esimerkiksi kysymään, keneen rekisteröidyn on otettava yhteyttä, jos hän haluaa tietoja poistettavan. Jollain tavalla tulee varmistua siitäkin, että kyse on kaikin puolin asianmukaisesta pyynnöstä mukaan lukien se, että pyynnön esittäjänä on tähän oikeutettu henkilö eikä joku muu.

Rekisteröidyillä tulee olla myös riittävät mahdollisuudet saada tiedot häntä koskevista henkilötiedoista. Kaikki nämä ovat sen tyyppisiä asioita, joista rekisterinpitäjän tulee tietosuoja-asetuksen mukaan huolehtiakin.

Ainakin ensi katsannossa näyttäisi siltä, että yksityisten ja suljettujen lohkoketjujen yhteydessä on olennaisesti paremmat edellytykset täyttää tietosuoja-asetuksen 17 artiklassa tai yleensä tietosuoja-asetuksessa asetetut vaatimukset. Toinen asia on, koetaanko vaatimukset kaikesta huolimatta niin hankaliksi, että henkilötietoja ei haluta tallentaa lohkoketjuun, mikäli tämä ei ole välttämätöntä.

Jakson loppuksi on aiheellista tarkastella tietosuoja-asetuksen 22 artiklaa, jossa käsitellään automatisoituja yksittäispäätöksiä. Rekisteröidyillä on artiklan 1 kohdan mukaan oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.

Jos lohkoketjuun on sijoitettu autonomisesti toimiva ohjelma eli älysopimus, herää kysymys, tekeekö ohjelma päätöksiä edellä mainitussa säännöksessä tarkoitettulla tavalla. Tuntuu melko selvältä, että ainakin jotkin ohjelmat tekevät tällaisia päätöksiä kokonaan automaattisen käsittelyn perusteella. Tällöin ollaan 22 artiklan 1 kohdassa asetetun kiellon piirissä, jos päätöksellä on rekisteröityä koskevia oikeusvaikutuksia tai se vaikuttaa häneen vastaavalla tavalla merkittävästi. Myös tämä edellytys täyttyy monien älysopimusten yhteydessä, vaikka älysopimusten moninaisten luonteen vuoksi on epäilemättä myös sellaisia lohkoketjuun sijoitettavia ohjelmia, joiden osalta edellytys jää täyttymättä.

Kyseessä oleva kielto ei kuitenkaan ole ehdoton. Tietosuoja-asetuksen 22 artiklan 2 kohdan mukaan 1 kohtaa ei sovelleta, jos päätös

- a) on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten;
- b) on hyväksytty rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa vahvistetaan myös asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi; tai
- c) perustuu rekisteröidyn nimenomaiseen suostumukseen.

Ensimmäinen poikkeus eli a alakohta voi soveltua ainoastaan silloin, kun kyse on rekisteröidyn ja rekisterinpitäjän välisestä sopimuksesta. Lohkoketjusovelluksissa voi kuitenkin ilmetä myös asetelma, jossa rekisterinpitäjäksi katsottava taho ei ole sopimusosapuolena. Vaikka poikkeus sinänsä soveltuisi kyseessä olevaan älysopimukseen, huomioon tulee ottaa myös 22 artiklan 3 kohta, jonka nojalla rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi. Tämä koskee kohdan mukaan vähintään oikeutta vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö, sekä oikeutta esittää kantansa ja riitauttaa päätös,

mikä voi olla ongelmallista pelkästään täysin automatisoituun päätöksentekoon ja lohkaketjun avulla tapahtuvaan ohjelmalliseen täytäntöönpanoon nojaavien älysopimusten hyväksyttävyyden kannalta. Tietojen käsittelyä luonnollisen henkilön toimesta koskeva vaatimus on kuitenkin sen laatuinen, että se voi täyttyä suhteellisen helpostikin siitä riippuen, kuinka sääntelyä lopulta tulkitaan.

Lohkoketjuun sijoitettujen älysopimusten osalta ei ole annettu b alakohdassa tarkoitettua EU-tason sääntelyä. Koska b alakohta mahdollistaa automaattista päätöksentekoa koskevista säännöistä poikkeamisen myös kansallisen lainsäädännön nojalla, EU:n jäsenvaltiot voisivat pyrkiä hankkimaan itselleen kilpailuetua lohkaketjuliiketoiminnan houkutteluun luomalla älysopimuksia koskevaa ja niiden käyttöä edistävää erityislainsäädäntöä. Jäsenvaltioille onkin jätetty varsin paljon päätösvaltaa 22 artiklan todellisen kattavuuden ja merkityksen määrittämisessä. Huomionarvoista on, että 2 kohdan b alakohdan mukaisessa tilanteessa sovellettavaksi ei tule edellä mainittu saman artiklan 3 kohta. Niinpä vaikka myös kansallisessa laissa tulee vahvistaa asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi, ainakaan artiklan sananmuodon valossa tällaiseen lakiin ei ole välttämätöntä sisällyttää 22 artiklan 3 kohdassa erikseen mainittuja vähimmäistoimenpiteitä (eli rekisteröidyn oikeutta vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö ja oikeutta esittää kantansa ja riitauttaa päätös).

Kolmas poikkeusperuste on 22 artiklan 2 kohdan c alakohdan mukaan se, että päätös perustuu rekisteröidyn nimenomaiseen suostumukseen. Tällainen suostumus on ainakin periaatteessa helppoa hankkia silloin, kun sopijakumppanit ovat tekemisissä keskenään ennen ohjelman sijoittamista lohkaketjuun. Toisaalta on ilmiselvästi myös tilanteita, joissa suostumuksen vaatimus jää helposti täyttymättä. Älysopimukseen turvautumista hankaloittaa lisäksi, että c alakohta on 22 artiklan 3 kohdan kannalta samassa asemassa kuin a alakohta. Rekisteröidyllä on siten aina muun muassa mahdollisuus vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö.

Yleisesti ottaen edellä mainittujen rekisteröidyn oikeuksien toteuttamiseen liittyy samankaltaisia tulkinnanvaraisuuksia ja epävarmuutta oikeustilasta kuin henkilö-tietojen käsittelyn vastuuroolien määrittelyyn. Selkeitä, nimenomaisesti lohkaketjuteknologiaa koskevia linjauksia Euroopan unionin tuomioistuimelta ei tois-taiseksi ole. Eurooppalaisista tietosuojaviranomaisista koostuva Euroopan tietosuojaneuvosto ei sekään ole antanut lohkaketjuteknologiaa koskevia ohjeita tai suosituksia, ja yksittäisten tietosuojaviranomaisten kannanotot ja ohjeistukset eivät ole olleet kovinkaan yhtenäisiä. Rekisteröidyn eri oikeuksien toteuttamista lohkaketjujärjestelmissä (kuten myös muita tässä teoksessa käsiteltyjä tietosuojaan liittyviä aihepiirejä) on pyritty jossain määrin tätä esitystä laajemmin selven-

tämään esimerkiksi Michèle Finckin laatimassa, Euroopan parlamentin tutkimuspalvelun vuonna 2019 julkaisemassa *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* -tutkimuksessa. Erilaiset lohkoketjuteknologiaan ja tietosuojalainsäädäntöön, erityisesti vastuurooleihin ja rekisteröidyn oikeuksiin, liittyvät tulkintakysymykset ovat luonnollisesti olleet viime vuosina myös oikeustieteilijöiden mielenkiinnon kohteena, ja aiheesta on julkaistu lukuisia tieteellisiä artikkeleita. Tästä huolimatta oikeustila on edelleen kaikkiaan selvennyksen tarpeessa.

## 5.5 Henkilötietojen käsittelyn turvallisuus

Kyber- ja tietoturvallisuus ovat nykyisessä tietoverkkoihin monin tavoin kytkeytyneessä ja niistä riippuvaisessa verkkoyhteiskunnassa keskeisiä vaatimuksia käytännössä millä tahansa toimintasektorilla. Myös ja erityisesti henkilötietoja käsiteltäessä on välttämätöntä varautua erilaisiin turvallisuushäikiin, jotka voivat vaikuttaa käsiteltävien tietojen eheyteen ja luottamuksellisuuteen taikka haitata niiden käsittelyä. Tietoturva voidaankin määritellä esimerkiksi järjestelyiksi, joilla pyritään varmistamaan tiedon *eheys, luottamuksellisuus* ja *saatavuus*. Eheys voidaan vuorostaan määritellä tiedon yhtäpitävyydeksi alkuperäisen tiedon kanssa eli muuttumattomuudeksi. Luottamuksellisuus viittaa siihen, että tiedot ovat vain oikeutettujen henkilöiden käytettävissä eivätkä sivulliset voi saada niitä käsiinsä. Saatavuus puolestaan tarkoittaa, että tieto on häiriöttä hyödynnettävissä haluttuna aikana eli silloin, kun sitä tarvitaan.

Tietoturvauhat voivat puolestaan olla luonteeltaan monenlaisia ja -tasoisia. Kyse voi olla esimerkiksi verkossa ammattimaisesti toimivien rikollisryhmittymien tai muiden ulkopuolisten hyökkääjien toteuttamista tietomurroista, haittaohjelmista, palvelunestohyökkäyksistä taikka ohjelmointivirheiden, teknisten häiriöiden tai virheellisten manuaalisten käsittelytoimien vaikutuksista tietoon ja niiden käsittelyyn käytettävien järjestelmien toimintaan.

Tietosuojalainsäädännön näkökulmasta tietoturva on yksi tietosuojan toteuttamisen keino. Tietosuoja-asetuksessa mainittuihin yleisiin tietosuojaperiaatteisiin kuuluu henkilötietojen eheys ja luottamuksellisuus: asetuksen 5 artiklan 1 kohdan f alakohdan mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. Tätä periaatetta konkretisoidaan käsittelyn turvallisuutta koskevassa 32 artiklassa, jossa rekisterinpitäjä ja henkilötietojen käsittelijä veloitetaan toteuttamaan käsittelyyn liittyvää riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Riittävän turvalli-

suustason arviointi on siis riskiperusteista, ja vaadittavat toimenpiteet tulee artiklan mukaan suhteuttaa saatavilla olevaan tekniikkaan ja toteuttamiskustannuksiin. Artiklassa mainitaan eräinä mahdollisina toimenpiteinä ensisijaisesti luottamuksellisuutta (ja osin eheyttä) tukevat henkilötietojen pseudonymisointi ja salaus. Toisaalta artiklassa viitataan myös esimerkiksi kykyyn taata käsittelyjärjestelmien ja palveluiden jatkuvan luottamuksellisuuden ja eheyden ohella myös niiden käytettävyys ja vikasietoisuus.

Merkittävänä tietoturvallisuuden kytkettyinä uutuutena tietosuoja-asetuksessa voidaan pitää 33 ja 34 artikloista ilmenevää ilmoittamisvelvollisuutta tilanteissa, joissa tietoturvaloukkauksen seurauksena on käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Tällaisen ns. *henkilötietojen tietoturvaloukkauksen* tapahtuttua rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä sekä tietosuojaviranomaiselle että rekisteröidyille, joiden oikeuksille ja vapauksille loukkaus todennäköisesti aiheuttaa korkean riskin. Tietosuojaviranomaiselle ilmoitus on tehtävä lähtökohtaisesti 72 tunnin kuluessa loukkauksen ilmitulosta. Artikloihin sisältyy myös poikkeuksia ilmoittamisvelvollisuudesta.

Sekä 32 artiklan tietoturvatoinenpiteiden että 33–34 artiklojen mukaisten ilmoitusten laiminlyönnistä voi seurata vahingonkorvausvastuun ohella asetuksen 83 artiklassa tarkoitettu hallinnollinen seuraamusmaksu, jonka suuruus voi olla enintään 10 000 000 euroa, tai jos kyseessä on yritys, kaksi prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Tosin jos samalla on rikottu 5 artiklan 1 kohdan f alakohdan mukaista henkilötietojen eheyden ja luottamuksellisuuden periaatetta – kuten kyseisen periaatteen ja 32 artiklan läheisen suhteen vuoksi tyypillistä on – sakon enimmäismäärä voi olla tuplasti suurempi.

Lohkoketjujen näkökulmasta turvallisuusvelvoitteet ovat moniulotteisia, ja riskiperustaisesta sääntelytavasta johtuen tietosuojalainsäädännön vaatimien tietoturvatoinenpiteiden laatu ja määrä voivat vaihdella merkittävästikin. Tietosuoja-asetus ei siis sisällä yksityiskohtaisia listoja tai taulukkoja siitä, minkälaisia tietoturvatoinenpiteitä missäkin tilanteessa vaaditaan. Turvallisuusvelvoitteiden tasoa arvioidaan ensisijaisesti henkilötietojen käsittelyyn liittyvien riskien perusteella, ja niinpä vaadittavat toimenpiteet riippuvat suuresti siitä, miten paljon ja minkälaisia henkilötietoja lohkoketjusovelluksessa käsitellään. Riskiarvioinnissa tulee 32 artiklan 2 kohdan mukaan erityisesti huomioida riskit, jotka aktualisoituvat käsiteltävien henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn seurauksena. Jos käsittely kohdistuu erityisiin henkilötietoryhmiin, käsit-

tely on erityisen laajamittaista tai tietojen vahingoittuminen tai päätyminen väärin käsiin muutoin voisi aiheuttaa erityistä vahinkoa rekisteröidyille, nostaa tämä tietoturvalta vaadittavaa tasoa.

Viimeksi mainituissa tilanteissa aktivoituu tyypillisesti myös tietosuoja-asetuksen 35 artiklan mukainen velvollisuus suorittaa nimenomainen tietosuoja koskeva vaikutustenarviointi (*data protection impact assessment* eli DPIA) jo ennen käsittelyn aloittamista. Vaikutustenarviointi on usein muutenkin tarpeen ennen kuin tietoja aletaan käsitellä lohkoketjujärjestelmien avulla, koska lohkoketjujen toimintamekaniikka saattaa vaikeuttaa jälkikäteisiä muutos- ja korjaustoimenpiteitä ja koska lohkoketjuille tyypilliseen pysyväisluonteiseen tiedon tallentamiseen ja älysojimuksilla automatisoituun päätöksentekoon liittyy merkittäviä riskejä tietosuoja-lainsäädännön mukaisten rekisteröityjen oikeuksien näkökulmasta. Tietosuoja-asetuksen 35 artiklan mukainen vaikutustenarviointi ei rajoitu pelkästään tietoturvasuuskysymyksiin, mutta sen tulee sisältää muun ohella suunnitellut toimenpiteet rekisteröidyn oikeuksia ja vapauksia koskeviin riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet.

Lähtökohtaisesti tietosuoja-asetuksen tietoturvasuvelvoitteiden näkökulmasta merkitystä ei sinänsä ole sillä, miltä osin tietoja tallennetaan lohkoketjuun ja miltä osin sen ulkopuolelle – tietoturvasta on huolehdittava joka tapauksessa sekä teknisillä että organisatorisilla keinoilla. Lohkoketjujen hyödyntäminen on toki jo itsessään yksi keino suojata tietojen eheyttä, sillä lohkoketjujen perusajatuksenahan on varmistaa kryptografisin keinoin, ettei ketjuun tallennettuja lohkoja jälkikäteen voida muokata ja että kaikista muutoksista vähintäänkin jää jälki. Lisäksi lohkoketjujen hajautettu luonne voi olla omiaan parantamaan ketjuun tallennettujen tietojen saatavuutta ja järjestelmän häiriönsietokykyä (*resilienssiä*), kun esimerkiksi yksittäisen tietojenkäsittelyyn osallistuvan solmun tai lounhijan putoaminen pois toiminnasta vaikkapa palvelunestohyökkäyksen seurauksena ei yleensä vaikuta laajemmin koko lohkoketjujärjestelmän toimintaan.

Vaikka lohkoketjujärjestelmillä on siis lähtökohtaisesti tietoturvasuuta tukevia ominaisuuksia, lohkoketjujalustojen ja -sovellusten koodissa voi olla erilaisia haavoittuvuuksia, jotka voivat mahdollistaa myös ei-toivotut muutokset lohkoketjuun. Toisaalta järjestelmän ominaisuudet voivat johtaa ketjuun tallennettujen tietojen pysyvään käyttökeltvottomuuteen esimerkiksi salausavainten häviämisen myötä. Pelkkä lohkoketjun hyödyntäminen ei siten itsessään riitä henkilötietoihin kohdistuvien tietoturva vaatimusten täyttämiseen, vaan kyse on kokonaisvaltaisesta ja tapauskohtaisesta arvioinnista.

Etenkin henkilötietojen luottamuksellisuuden varmistaminen lohkoketjuissa vaatii erityistä, järjestelmän tyyppin ja tietojen käsittelyn tarkoitukset ja tarpeet huomioivaa etukäteissuunnittelua. Lähtökohtana tulee olla, että henkilötiedot ovat hajautetussa järjestelmässä vain sellaisten tahojen saatavilla ja käsiteltävissä,

jotka todella kyseisiä tietoja tarvitsevat. Erityisesti jos kyse on julkisesta ja avoimesta lohkoketjusta, johon kenellä tahansa on pääsy, lohkoihin tallennettavat henkilötiedot on lähtökohtaisesti pseudonymisoitava tai salattava, jollei niiden ole erityisestä syystä tarpeen olla kaikkien saatavilla. Salausalgoritmien tulee olla matemaattisesti vahvoja ja luotettaviksi tiedettyjä ja salausavainten riittävän pitkiä laskentavoimaan perustuvien hyökkäysten ehkäisemiseksi. Myös salausavainten ja pääsyoikeuksien hallinnointitapoihin on kiinnitettävä huomiota.

Vaikka tietosuoja-asetuksessa tietoturvallisuustoimenpiteet sidotaan nimenomaisesti *uusimpaan* tekniikkaan, käytännössä pitkäaikaiseen käyttöön tarkoitettuja lohkoketjusovelluksia suunniteltaessa on syytä pyrkiä ennakoivuuteen ja myös tulevaisuuteen suuntautuvaan tietoturvallisuustoimien mitoittamiseen, koska perustavanlaatuisen tietoturvaratkaisujen muutoksia voi olla hankala toteuttaa jälkikäteen.

Yksi tulevaisuuden tekniseen kehitykseen kytkeytyvä ongelma on se, että vaikka nykyään lohkoketjujen perustoiminnassa, kryptovaluuttajärjestelmissä ja henkilötietojen salaamisessa hyödynnettävät salausratkaisut ovat matemaattisesti niin vahvoja, etteivät puhtaasti laskentatehoon perustuvat hyökkäykset ole tällä hetkellä toteuttamiskelpoisia, tilanne voi muuttua dramaattisesti esimerkiksi *kvanttietokoneiden* kehityksen myötä. Näiden tarjoaman laskentatehojen merkittävän kasvun myötä lohkoketjuteknologian pohjana olevien epäsymmetristen salaus-ten murtaminen voi nimittäin tulla mahdolliseksi. Nykyiset lohkoketjujärjestelmät perustuvat edellä jo ilmi käyneeseen tapaan julkisen ja yksityisen avaimen käyttöön. Nämä avaimet liittyvät toisiinsa, ja julkinen avain on matemaattisesti yksinkertaista selvittää yksityisen avaimen perusteella. Järjestelmän toiminnan taakana on se, että yksityisen avaimen selvittäminen julkisen avaimen perusteella on sen sijaan käytännössä mahdotonta nykyisillä laskentatehoilla. Teoriassa se voisi kuitenkin onnistua jo vuonna 1994 julkaistua Shorin algoritmia käyttäen riittävän tehokkaalla kvanttietokoneella.

Toisaalta myös entistä vahvempia salaustekniikoita kehitetään jatkuvasti, ja jo vuosikymmenten ajan on pyritty kehittämään nimenomaisesti erilaisia kvanttilaskennan kestäviä salausratkaisuja (*post-quantum cryptography*). Kvanttifysiikkaa voidaan hyödyntää myös uudenaikaisissa salausjärjestelmissä, ja kvanttilaskennan pitäisikin olla ihanteellisessa tilanteessa teoreettisesti mahdottomia murtaa laskennallisesti.

Tässä luvussa tietoturvallisuuskysymyksiä on lähestytty erityisesti tietosuojalainsäädännön näkökulmasta, joka painottuu etenkin henkilötietojen luottamuksellisuuden ja eheyteen. Huomattava on silti myös, että laajemmin lohkoketjusovellusten tai -järjestelmien taikka niiden avulla harjoitettavan liiketoiminnan näkökulmasta myös käsiteltävien tietojen saatavuuden ja toisaalta muunkin datan kuin

henkilötietojen suojaaminen voi olla ensiarvoisen tärkeää. Korkea tietoturvallisuuden taso on nykypäivänä perusedellytys yhteiskunnalliselle ja taloudelliselle toiminnalle tietoverkoissa ja niiden ulkopuolellakin. Samalla se on välttämätöntä luonnollisten henkilöiden monien perus- ja ihmisoikeuksien, esimerkiksi omaisuuden suojan ja henkilökohtaisen turvallisuuden, turvaamiseksi. Niinpä lohkoketjujärjestelmissäkin tietoturvariskit kohdistuvat paitsi henkilötietojen suojaan ja yksityisyyteen, myös moniin muihin tärkeisiin yleisiin ja yksityisiin intresseihin.

EU-tasolla tietoturvallisuutta yleisesti on edistetty ja edistetään lähivuosina useilla säädöksillä, esimerkiksi Euroopan parlamentin ja neuvoston asetuksella (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintäteknikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (*kyberturvallisuusasetus*), Euroopan parlamentin ja neuvoston direktiivillä (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (*NIS 2 -direktiivi*) sekä ehdotuksella asetukseksi digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvavaatimuksista ja asetuksen (EU) 2019/1020 muuttamisesta (COM(2022) 454, ns. *kyberkestävyyssäädös*). Tämä tietoturvallisuutta koskeva EU-sääntely voi joiltain osin olla relevanttia myös lohkoketjuihin liittyvissä tilanteissa, mutta mainituissa säädöksissä ei ole lohkoketjuteknologiaan liittyviä erityissäännöksiä.



## 6 IMMATERIAALIOIKEUDELLISIA NÄKÖKOHTIA

### 6.1 Lohkoketju ja tekijänoikeus

Tekijänoikeuden (*copyright*) käsite tunnetaan käytännössä globaalisti. Kotimaisessa tekijänoikeuslaissa (404/1961; TekL) lähdetään siitä, että kirjallisen tai taiteellisen teoksen luojalla on tekijänoikeus teokseen. Valtiot ovat perinteisesti tehneet pitkään yhteistyötä tekijänoikeuskysymyksissä, minkä vuoksi tekijänoikeuden yleiset lähtökohdat ovat samantapaiset useilla alueilla. Euroopan unionin jäsenvaltioissa oikeustilaa yhtenäistää se, että myös EU-tasolla on otettu kantaa moniin tekijänoikeuden kannalta relevantteihin kysymyksiin. Suomi on osallisena useissa kansainvälisissä sopimuksissa ja tehnyt perinteisesti läheistä yhteistyötä muiden Pohjoismaiden kanssa.

Lohkoketjuteknologiaan ja sen mahdollistamiin sovelluksiin liittyy lukuisia tekijänoikeuden kannalta kiinnostavia kysymyksiä. Alkajaisiksi voidaan todeta, että myös lohkoketjuehittäjä saattaa luoda teoksen, joka voi olla tekijänoikeuden kohteena. Kyse voi olla esimerkiksi tietokoneohjelmasta, joka siis myös kelpaa teokseksi. Esimerkiksi TekL 1.2 §:stä käy nimenomaisesti ilmi, että myös tietokoneohjelmaa pidetään kirjallisena teoksena. Sen lisäksi, että tekijänoikeus saattaa suojata lohkoketjua, on myös mahdollista käyttää lohkoketjuteknologiaa suojaamaan tekijänoikeuden suojaamia teoksia.

Tekijänoikeus tyypillisesti syntyy kussakin oikeusjärjestyksessä suoraan lain nojalla, eikä esimerkiksi Suomessa ole viranomaisten ylläpitämää tekijänoikeusrekisteriä. Tekijälle edulliset ratkaisut suojan syntymisen osalta omaksuttiin jo vuoden 1886 Bernin yleissopimuksessa, jota voidaan edelleen pitää tärkeimpänä yleissopimuksena tekijänoikeuden alalla.

Jotta kyse ylipäätään olisi tekijänoikeuden suojaamasta teoksesta, tietynlaisen teoskynnyksen tulee täytyä. Tietokoneohjelmien osalta tulee EU-alueella ottaa muun ohella huomioon Euroopan parlamentin ja neuvoston direktiivi 2009/24/EY, annettu 23 päivänä huhtikuuta 2009, tietokoneohjelmien oikeudellisesta suojasta, jossa painotetaan *omaperäisyyden* merkitystä. Direktiivin 1 artiklan 3 kohdassa todetaan: ”Tietokoneohjelmaa suojataan, jos se on omaperäinen siinä merkityksessä, että se on tekijänsä henkinen luomus. Muita arviointiperusteita ei saa soveltaa arvioitaessa, suojataanko ohjelmaa.” Myös tietokanta voi olla tekijänoikeussuojan piirissä, ja Euroopan parlamentin ja neuvoston direktiivi 96/9/EY, annettu 11 päivänä maaliskuuta 1996, tietokantojen oikeudellisesta suojasta sisältää omaperäisyyden osalta vastaavanlaista sääntelyä kuin direktiivi 2009/24/EY. Kansallista teoskynnystä koskevaa sääntelyä ei muutettu tämän direktiivin vuoksi, joten myös kansallisen tekijänoikeuslain 1 §:n mukaisen

teoskynnyksen voidaan olettaa vastaavan näiden direktiivien sisältöä ainakin tässä yhteydessä.

Tekijänoikeus tuottaa tekijälleen useita erilaisia oikeuksia. Toisistaan voidaan erottaa *taloudelliset* ja *moraaliset* oikeudet. Taloudellisten oikeuksien ytimessä on TekL 2 §:n nojalla tekijän lähtökohtaisesti yksinomainen oikeus määrätä teoksesta valmistamalla siitä kappaleita tai saattamalla se yleisön saataviin. Tekijä voi kuitenkin hyödyntää oikeuttaan myös esimerkiksi siirtämällä tekijänoikeuden toiselle tai antamalla jonkinlaisen lisenssin eli käyttöluvan. Tekijä voi TekL 3 §:n mukaan luopua myös moraalisisista oikeuksistaan, mutta kuitenkin vain, jos kyseessä on laadultaan ja laajuudeltaan rajoitettu teoksen käyttäminen. Moraalisiin oikeuksiin lukeutuu muun muassa tekijän ilmoittaminen ja kielto muuttaa teosta tekijää loukkaavalla tavalla.

Tekijänoikeuden syntymekanismista koituu erinäisiä käytännön hankaluuksia kuten toisinaan vaikeus tunnistaa, kenelle kuuluu tekijänoikeus johonkin teokseen. Lohkoketjuteknologia tarjoaa kätevän keinon jakaa tietoa teoksista sekä niitä koskevista oikeuksista. Lohkoketjupohjainen rekisteri, joka voisi syntyä puhtaasti vapaaehtoisuuden pohjalta, saattaisi siis tuoda oikeudellista selvyttä siihen, kenellä on oikeus määrätä teoksesta tai jollain tavalla ryhtyä siihen. Rekisteriin voitaisiin viedä tiedot myös tekijänoikeuden siirtymisestä ja lisensseistä.

Tekijänoikeus ja kaikki muutkin immateriaalioikeudet ovat suhteellisia ja niitä on rajoitettu muiden intressien vuoksi. Esimerkiksi kotimaisen tekijänoikeuslain 2 luvussa on säädetty useista rajoituksista. Teoksesta voi esimerkiksi olla sallittua valmistaa kappaleita. Esimerkiksi julkistettujen teosten osalta on TekL 12 §:n nojalla lähtökohtana, että jokainen saa valmistaa teoksesta muutaman kappaleen yksityistä käyttöään varten. Tekijänoikeus on pääsääntöisesti voimassa siihen saakka, että 70 vuotta on kulunut tekijän kuolinvuodesta (TekL 43 §). Koska tekijällä ei ole täydellistä hallintaa teokseen, hänellä on tarve valvoa ja kontrolloida sen käyttöä suojatakseen laillisia oikeuksiaan.

Lohkoketjuteknologia voi toimia myös tekijänoikeuden suojaamisessa ja tekijän oikeuksien toteuttamisessa. Lohkoketjuteknologia tarjoaa tekijänoikeuden haltijalle yhden lisäkeinon saattaa teos yleisön saataville. Koska teokset viime kädessä ovat aineettomia kohteita, ne ovat yleensä digitalisoitavissa. Pääsy ja lisensointi teokseen saatetaan toteuttaa älysovimuksia hyväksi käyttäen, ja lohkoketjujärjestelmässä voidaan toteuttaa myös maksujärjestelyjä. Lohkoketju onkin herättänyt kiinnostusta tekijänoikeuksien digitaalisen hallinnoinnin (*digital rights management* eli DRM) näkökulmasta. Lohkoketjuteknologiassa nähdään potentiaalia esimerkiksi sen jälkikäteiseen todentamiseen, kuka on alun perin luonut teoksen, koska lohkoketjuun jää aikamerkintä teoksen luomisesta ilman, että tätä voidaan muuttaa jälkeenpäin. Lohkoketju mahdollistaa myös erilaiset ratkaisut, joissa tekijän tiedot ja tieto tekijänoikeudesta kulkevat digitaalisen teoksen mukana, jolloin sitä

käyttävien on mahdollista seurata materiaalin tekijänoikeuksia ja siten välttyä tahattomilta tekijänoikeusrikkomuksilta.

Tekijänoikeutta ei aina kunnioiteta, ja teosta saatetaan esimerkiksi levittää ilman asianmukaista oikeutusta. Kyse on käytännössä merkittävästä ongelmasta, johon on kiinnitetty huomiota useilla eri foorumeilla. Lohkoketjupohjaiset sovellukset saattavat tarjota ainakin osaratkaisun ongelmaan, ja esimerkiksi tietokoneohjelmien luvattoman kopioinnin ja käyttämisen havaitsemiseksi on esitetty lohkoketjun varassa toimivia järjestelmiä. Lohkoketjut on nähty hyödyllisiksi myös tuotevääreännösten vastaisessa taistelussa. Esimerkiksi Euroopan unionin teollisoikeuksien virasto (englanniksi *European Union Intellectual Property Office* eli EUIPO) on osoittanut tässä suhteessa kiinnostusta lohkoketjuteknologiaan. EUIPO seuraa muiden tehtäviensä ohella muun muassa niin teollis- kuin tekijänoikeuksien loukkauksia.

## 6.2 Tekijänoikeus ja tokenisoitu taide

Erilaiset taide-NFT:t ovat yleistyneet viime vuosina, mihin on kiinnitetty huomiota myös julkisessa keskustelussa. Taiteeseen kytkeytyvistä rahakkeista on voitu maksaa jopa miljoonia euroja. Vaikka hinta olisi joissain tapauksissa tarkoituksellisesti keinoteltu korkeaksi, kyse on kaiken kaikkiaan merkittävästä ja vakavasti otettavasta markkinasta. On arvioitu, että taiteeseen liittyviä ei-fungibeileita tokeneita ostettiin ja myytiin 2,3 miljardin euron edestä vuonna 2021.

Tokenisoidulla taiteella laajasti ymmärrettynä on monia liittymäkohtia immateriaalioikeuksiin kuten tekijänoikeuteen ja tavaramerkkiin. Seuraavassa tarkastellaan aihepiiriä lähemmin tekijänoikeuden näkökulmasta. Tarkastelu perustuu suurelta osin niihin havaintoihin, joita on tehty Euroopan parlamentin tilaamassa ja lokakuussa 2022 valmistuneessa tutkimuksessa *Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art*, joka on vapaasti luettavissa Euroopan parlamentin nettisivuilla. Päähuomio on kotimaisessa tekijänoikeuslaissa, joka monessa tärkeässä suhteessa tosin perustuu EU-tason direktiiveihin, joita etupäässä on pidetty silmällä EU-parlamentin julkaisemassa raportissa.

Lohkoketjuteknologia mahdollistaa lukuisia erilaisia taide-NFT:n toteutuksia. Yleensä turvaudutaan valmiisiin alustoihin kuten Ethereumiin, joka on tällä hetkellä tokenisoidun taiteen tavallisin alusta. Yleisin tekninen standardi on puolestaan ERC-721, jota on tarkasteltu tämän teoksen jaksossa 4.2 yleiseltä kannalta. Kyse on siis valmiista standardista, johon voidaan turvautua älysopimuksia tehtäessä. Taiteenkin kannalta kiinnostavana piirteenä voidaan pitää sitä, että älysopimuksen luoma *tokenID* on mahdollista toteuttaa niinkin, että rahake voidaan sen itsensä sisältämän tiedon perusteella esittää esimerkiksi kuvana sopivan ohjelman avulla. Älysopimuksen osoite yhdessä älysopimuksen luoman tokenID:n

kanssa erottaa älysopimuksen luoman NFT:n kaikista muista non-fungiabeleistä tokeneista. Älysopimus on keskeisessä asemassa, sillä tokenID on vain luku, joka saa merkityksensä sen luoneen älysopimuksen kontekstissa.

Kuten edellä jaksossa 4.2 todettiin, irtaimen omistus lukeutuu seikkoihin, jotka on mahdollista tokenisoida. Koska myös maalausten ja veistosten kaltaiset taideesineet ovat irtaimia esineitä, niiden omistus voidaan tokenisoida samoin kuin muidenkin irtainten esineiden omistus. Perustapauksessa yksi token edustaa yhtä taideteosta. Ainakin erityisten arvokkaiden taide-esineiden yhteydessä voi toisaalta olla tarkoituksenmukaista tehdä älysopimus, joka mahdollistaa taide-esineen omistuksen määräosissa. Määräosiin oikeuttavat tokenit voivat tällöin olla NFT-muotoisia, mutta kyse voi sinänsä olla myös fungiabeleistä rahakkeista.

Fyysisen taideteoksen omistaja voi näin halutessaan tokenisoida teoskappaleen omistuksen. Erityisongelmia kuitenkin syntyy, jos teokseen kohdistuu voimassa oleva tekijänoikeus. Kaikella taiteella ei ole tekijänoikeutta jo sen iäkkyyden vuoksi. Voimassaoloajan suhteen on pääsääntönä, että tekijänoikeus on voimassa, kunnes 70 vuotta on kulunut tekijän kuolinvuodesta (TekL 43 §). Tekijä on myös saattanut luopua oikeuksistaan, joskin moraalisisista oikeuksista (TekL 3 §) luopuminen käy päinsä vain, mikäli kysymyksessä on laadultaan ja laajuudeltaan rajoitettu teoksen käyttäminen. Maailmalla on kaiken kaikkiaan valtava määrä taidetta, joka on joko yleiseen käyttöön asetettua tai vapautunutta (ns. *public domain*).

Jos teokseen kohdistuu tekijänoikeus eikä teoskappaleen omistajalla ole tekijänoikeuteen kuuluvia taloudellisia oikeuksia, tokenisointiin saattaa sisältyä tekijänoikeuden loukkauksia. Esimerkiksi teoskappaleiden valmistaminen, joka lähtökohtaisesti kuuluu yksinomaan tekijänoikeuden haltijalle, ymmärretään varsin laajasti. TekL 2.2 §:n mukaan kappaleen valmistamisena pidetään sen valmistamista kokonaan tai osittain, suoraan tai välillisesti, tilapäisesti tai pysyvästi sekä millä keinolla ja missä muodossa tahansa. Kappaleen valmistamisena pidetään myös teoksen siirtämistä laitteeseen, jolla se voidaan toisintaa.

Koska lohkoketjuteknologiassa on perimmältään kyse tiedon hajautetusta varastoinnista, se soveltuu ainakin periaatteessa erityisen hyvin digitaaliseen taiteeseen. Voidaanhan lohkoketjuun tallentaa kuvia, videoita, ääntä ja mitä tahansa digitaaliseen muotoon siirrettävää sisältöä. Käytännössä merkittäviä rajoituksia on kuitenkin koitunut kustannuksista. Mitä suuremmasta määrästä tietoa on kysymys, sitä kalliimmaksi lohkoketjuun tallentaminen muodostuu. Tavalliseksi menettelytavaksi tokenisoidun taiteen yhteydessä onkin muotoutunut se, että lohkoketjuun (eli älysopimukseen esimerkiksi standardin ERC-721 valmiita ominaisuuksia hyväksi käyttäen) sijoitetaan vain osoitin (*pointer*), jolla pääsee NFT-metadatan sisältävään tiedostoon. Metadata sisältää tavallisesti taiteilijan ja teoksen nimen sekä lyhyen kuvauksen. Lisäksi metadatatassa on varsinaisen teoksen lähde, joka

käytännössä on teoksen sijainnin kertova URL-osoite. Tällaisen *Off-Chain NFT:n* (vrt. *On-Chain NFT*) ongelmana on tosin se, että tiedon pysyvyydestä ja muuttumattomuudesta ei ole vastaavia takeita kuin siinä tapauksessa, että kopio taideteoksesta on lohkoketjussa. Niin metadata kuin varsinaisen teoksen lähde saattavat käytännössä kadota kokonaan. Riskejä voidaan vähentää tallentamalla tietoa mahdollisimman luotettavasti kuten IPFS-järjestelmää (*InterPlanetary File System*) hyväksi käyttäen sekä omaksumalla menetelmiä, joiden avulla voidaan tunnistaa taideteoksesta kopion sisältävän tiedoston muuttumattomuus. Tiedostosta voidaan ottaa esimerkiksi hash-arvo ja sisällyttää tämä arvo myös NFT:ään, mikä mahdollistaa sen varmistamisen, että NFT todella viittaa alkuperäiseen tiedostoon.

Valtaosa nykypäivän NFT-taiteesta koskettaa digitaalisia taideteoksia, joille ei ole vastinetta reaalielämässä. Monet taiteilijat ovat havainneet, että lohkoketjuteknologia mahdollistaa tietynlaisen alkuperäisyyden ja ainutkertaisuuden toteamisen siten, että tietyt digitaaliset kappaleet erottuvat muista sinänsä vastaavanlaisista kappaleista. Tämä puolestaan on omiaan herättämään keräilijöiden kiinnostuksen. Lukuisat tahot ovat valmiita maksamaan merkittäviä summia siitä, että juuri heillä on tietyn teoksen ”alkuperäiskappale” tai vähintään tietyllä numerolla varustettu kappale tilanteessa, jossa samasta teoksesta on tehty yhdellä kertaa useita digitaalisia kopioita. Digitaalisen taiteen ongelmana on ollut aiemmin, että on voinut olla erittäin hankala tunnistaa alkuperäistä taidekappaletta, koska digitaaliset kopiot eivät itsessään poikkea toisistaan. Kehitteillä olevat virtuaalitodellisuudet (*metaverse* tai *metaversumi*) voivat entuudestaan lisätä keräilijöiden halukkuutta ryhtyä NFT-pohjaiseen taiteeseen.

Taiteilijoiden ja keräilijöiden kiinnostusta selittänee osaltaan sekin, että lohkoketjuteknologia mahdollistaa kätevän perustan omistajanvaihdoksille ja samalla myös kaupankäynnille digitaalisella taiteella. Kaiken kaikkiaan NFT mahdollistaa taidemaailmassa vaihdannan, jossa tietty kopio saa alkuperäisen statuksen ja samalla myös rahallisen arvon. Taiteilijoiden kannalta kätevänä piirteenä voidaan pitää myös sitä, että lohkoketjuteknologian puitteissa on verraten helppo järjestää taiteilijalle jälleenmyyntikorvaus eli korvaus teoksen myöhemmistä kaupoista. Käytännössä esiintyykin älysovimuksia, joita käytettäessä taiteilija automaattisesti saa tietyn prosenttiosuuden kauppahinnasta.

Älysovimuksessa määritetyn prosenttiosuuden ei tarvitse vastata suuruudeltaan tekijänoikeuslain 2 b luvussa säädettyä jälleenmyyntikorvausta, eikä taiteilija myöskään ole sidottu lakisääteisiin edellytyksiin. Tekijänoikeuslain 26 i §:n mukaan kuvataiteen teoksen tekijällä on oikeus saada korvaus kaikesta kuvataiteen teoksen jälleenmyynnistä, johon osallistuu myyjänä, ostajana tai välittäjänä taide-markkinoiden ammattilainen. Jälleenmyyntikorvaus on 5 prosenttia siitä osasta kuvataiteen teoksen myyntihintaa, joka on enintään 50 000 euroa. Prosenttiosuus

pienenee myyntihinnan noustessa siten, että se on esimerkiksi 3 prosenttia siitä osasta myyntihintaa, joka on yli 50 000 euroa mutta enintään 200 000 euroa. Jälleenmyyntikorvaus lasketaan arvonlisäverottomasta myyntihinnasta. Jos myyntihinta on arvonlisäverottomana enintään 255 euroa, oikeutta jälleenmyyntikorvaukseen ei ole. Korvaus voi olla enintään 12 500 euroa.

Jälleenmyyntikorvaus perustuu Euroopan parlamentin ja neuvoston direktiiviin 2001/84/EY, annettu 27 päivänä syyskuuta 2001, alkuperäisen taideteoksen tekijän oikeudesta jälleenmyyntikorvaukseen, jota EU-parlamentin tutkimuksessa *Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art* on tulkittu NFT-kontekstissa siten, että NFT:n myynnin yhteydessä ei yleensä ole kyse jälleenmyyntikorvauksen alaisesta kaupasta (s. 39–40). Direktiivin johdanto-osan 2 perustelukappaleen mukaan oikeus jälleenmyyntikorvaukseen koskee varsinaista teosta eli sitä ilmaisuvälinettä, johon suojattu teos sisältyy. Vaikka digitaalinenkin taide voi sinänsä oikeuttaa jälleenmyyntikorvaukseen, raportin kirjoittajien (Katharina Garbers-von Boehm, Helena Haag, Katharina Gruber) mukaan tämä edellyttää sellaista fyysistä tallennusta, jota ei voida tunnistaa NFT:n luomisen ja myymisen yhteydessä. NFT:n myynti koskettaa myös vain NFT:tä digitaalisena tietojoukkona. Lisäksi tutkimuksessa pidetään taiteilijalle edullista tulkintaa tarpeettomana siinä mielessä, että taiteilijalla on älysopimuksen kautta mahdollisuus itse määrittää haluamansa kaltainen jälleenmyyntikorvaus.

Direktiivissä 2001/84/EY pidetään alkuperäisinä taideteoksina myös direktiivin alaan kuuluvien taideteosten kopioita, jotka taiteilija on itse tehnyt tai jotka on tehty hänen luvallaan ja joita on rajoitettu määrä (2 artiklan 2 kohta). TekL 26 i §:n 4 momentin mukaan oikeus saada korvaus jälleenmyynnistä syntyy, kun tekijä tai hänen oikeudenomistajansa on myynyt tai muutoin pysyvästi luovuttanut kuvataiteen teoksen tai tekijän itsensä tekemiä tai hänen luvallaan tehtyjä kuvataiteen teoksen kappaleita, joita on rajoitettu määrä. Oikeus lakisääteiseen jälleenmyyntikorvaukseen myös tavanomaisen NFT-kaupan yhteydessä ei tuntuisi mitenkään perusteettomalta myös se huomioon ottaen, että NFT:n kaupan yhteydessä ostaja saattaa saada myös jonkin fyysisen tallennuslaitteen, johon digitaalinen taideteos on tallennettu. Oikeus jälleenmyyntikorvaukseen yleisten edellytysten täytyessä tuntuu myös ilmeiseltä silloin, kun fyysisen kuvataiteen teoksen kauppa on toteutettu NFT-muodossa.

Oikeus jälleenmyyntikorvaukseen on TekL 26 i §:n 6 momentin mukaan henkilökohtainen, eikä tekijä voi luovuttaa sitä kolmannelle tai luopua siitä. Vaikka tekijä olisi toteuttanut itse tokenisoinnin siten, että hän ei saa korvausta myöhemmistä luovutuksista, kyse ei ole tehokkaasta luopumisesta. Jälleenmyyntikorvaus siis syntyy lakisääteisten edellytysten täytyessä. Mikäli tekijä toisaalta saa

älysopimuksen perusteella vähintään lakisäätteistä vastaavan jälleenmyyntikorvauksen, hänellä ei tämän lisäksi voine olla oikeutta lakisäätteiseen jälleenmyyntikorvaukseen.

Digitaalisen taiteen harjoittajat ja muutkin taiteilijat voivat käytännössä hyödyntää lohkoketjuteknologiaa ilman merkittävää teknistä osaamista. On esimerkiksi lukuisia melko helppokäyttöisiä markkinapaikkoja (kuten opensea.io, rarible.com ja manifold.xyz), joiden kautta taiteilija voi tokenisoida taidettaan ja tarjota sitä myytäväksi. Markkinapaikka luo halutun kaltaiset taide-NFT:t tai suuremmat kokoelmat, mikä käytännössä voi merkitä uuden älysopimuksen tekemistä tai jonkun jo olemassa olevan älysopimuksen hyödyntämistä. Erillisen älysopimuksen tekeminen ei ole niin työlästä ja kallista kuin ensi katsannossa voisi kuvitella sen vuoksi, että älysopimus voi hyödyntää lohkoketjuun jo sijoitettuja älysopimuksia siten, että älysopimus siihen koodatulla tavalla perii toisen älysopimuksen ominaisuuksia. Tämä lyhentää olennaisesti ohjelman pituutta. Olipa tekninen toteutus mikä tahansa, markkinapaikat usein kysyvät erikseen myös jälleenmyyntikorvauksesta.

Markkinapaikkoja on paljon, ja uusia syntyy liki päivittäin. Markkinapaikalla toimittaessa on tärkeä ymmärtää, mitä kulloinkin tapahtuu. Joillekin markkinapaikoille voi esimerkiksi ladata teoksia niin, että niistä luodaan NFT vasta ostohetkellä. Tällaiset odotustilassa olevat tokenit (*lazy mint*) ovat yksi kätevä keino vähentää kustannuksia ja samalla lisätä markkinapaikan houkuttavuutta taiteilijoiden kannalta.

Rajanveto fyysisten taideteosten ja digitaalisen taiteen välillä ei ole tarkkarajainen, sillä fyysisistä taideteoksista saatetaan laatia myös digitaalisia versioita, joihin tokenit oikeuttavat. Tällaisia menettelyjä on ilmennyt myös käytännössä. Lohkoketjuteknologian avulla samalla teoksella voi tavallaan luoda taloudellista arvoa useita kertoja. Samaan tokeniin voidaan kytkeä myös samaan aikaan niin fyysisen kuin digitaalisen teoskappaleen omistus.

Tokenisoitu taide on kaiken kaikkiaan sen verran uusi ilmiö, ettei siihen juurikaan ole ehditty ottaa kantaa lainsäädännössä. Suomessa yksi tulkintaongelma koskettaa virtuaalivaluutan tarjoajista annetun lain soveltumista. Odotettavissa oleva MiCA-asetus ei muuttane olennaisesti oikeustilaa, sillä edellä jaksossa 4.3 käsitellyn lokakuun 2022 kompromissiehdotuksen 2 artiklassa on kohta, jonka mukaan asetusta ei sovelleta kryptovaroihin, jotka ovat uniikkeja ja ei-fungibeilejä muiden kryptovarojen kanssa. Tätä kohtaa valmisteltaessa on pidetty nimenomaisesti silmällä myös digitaalista taidetta ja kokoelmia. Kyseessä oleva soveltamisalaa koskeva rajoitus ei voine yleensä soveltua, jos liikkeelle on laskettu lukuisia tokeita, jotka yksittäin tuottavat oikeuden ainoastaan pieneen määrääosaan teoskappaleen omistuksesta. Samoin voinee käydä siinäkin tapauksessa, että samasta taideteoksesta on tehty useita digitaalisia kopioita ja niitä vastaavia rahakkeita.

Kunhan teoksen yleiset edellytykset täyttyvät, tekijä saa tekijänoikeuden myös digitaaliseen taiteeseen. Tekijänoikeuden loukkausten kannalta ongelmattomia ovat tilanteet, joissa tekijä itse heti teoksen luotuaan ryhtyy tarjoamaan kappaleen tai kappaleita NFT-muodossa. Ilman tekijänoikeuden haltijan lupaa tämä ei kuitenkaan käy yleensä päinsä. Jotta taide-NFT saataisiin aikaiseksi ja myyntiin, vaaditaan käytännössä sellaisia toimia, jotka helposti konstituoivat TekL 2 §:n mukaista valmistamista tai yleisölle saattamista. Kyse ei ole kotimaisen oikeuden erityispiirteistä, sillä valmistamista ja yleisölle saattamista koskeva tekijänoikeuslain sääntely pohjautuu suurelta osin kansainvälisiin sopimuksiin ja EU-tasoiseen sääntelyyn kuten Euroopan parlamentin ja neuvoston direktiiviin 2001/29/EY, annettu 22 päivänä toukokuuta 2001, tekijänoikeuden ja lähioikeuksien tiettyjen piirteiden yhdenmukaistamisesta tietoyhteiskunnassa. Tämän direktiivin 2 artiklassa säännellään kappaleen valmistamista koskevasta oikeudesta sekä 3 artiklassa oikeudesta välittää yleisölle teoksia ja oikeudesta saattaa muu aineisto yleisön saataviin.

Digitaalinen taideteos tallennetaan yleensä internetiin yhteydessä olevaan kohteeseen siten, että lohkoketjuun sijoitetaan kustannussyistä mahdollisimmin vähän tietoa. Taideteoksen tallentaminen on TekL 2 §:n mukaista valmistamista, joten luvaton menettely tässä suhteessa merkitsee tekijänoikeuden loukkausta. Sen sijaan kyse ei välttämättä ole siitä, että kohde olisi samalla myös saatettu yleisön saataviin tavalla, johon tekijänoikeuden haltijalla lähtökohtaisesti on yksinomainen oikeus. Esimerkiksi URL-tallennettuun työhön pääsee käsiksi vain tarkan osoitteen tietämisen perusteella, ja osoite voidaan tallentaa suojatussakin muodossa.

Kun taide-NFT on luotu, sitä tyypillisesti tarjotaan myytäväksi jollain markkinapaikalla, mikä useimmiten edellyttää kuvaa NFT:n edustamasta teoksesta. Tämä merkitsee yleensä niin TekL 2 §:ssä tarkoitettua valmistamista kuin teoksen yleisön saataville saattamista. Kyse ei kuitenkaan välttämättä ole tekijänoikeuden loukkauksesta. Taideteoksen, joka kuuluu kokoelmaan tai pannaan näytteille taikka tarjotaan myytäväksi, saa TekL 25 a §:n 1 momentin mukaan kuvata näyttelyä tai myyntiä koskevaan tiedotukseen taikka painamalla, valokopioimalla tai muulla vastaavalla menetelmällä valmistettuun luetteloon. Ei ole selvä, kuinka sääntelyä tulee tulkita NFT-ympäristössä huomioon ottaen myös se, että on lukuisia erilaisia tokenisoinnin muotoja.

Erilaiset tekijänoikeuden loukkaukset ovat tällä haavaa melko tavallisia. Tokenisoinnin suorittanut taho saattaa jopa esiintyä taiteilijana, vaikka tämä ei pidä paikkaansa. Tällä hetkellä etsitäänkin keinoja, joilla taide-NFT:n ostanut voisi varmistua siitä, että taiteilija itse on toteuttanut tokenisoinnin tai että tokenisoinnille on ollut ainakin taiteilijan lupa. Verraten monelle ostajalle lienee tärkeää se, että token on peräisin juuri taiteilijalta itseltään, koska tämä on omiaan vaikuttamaan



rahakkeen arvoon. Fyysisten taideteosten yhteydessä arvokkaana saatetaan pitää sitäkin, että rahakkeen tai rahakkeiden liikkeeseenlaskijana toimii joku arvostettu taho kuten kansainvälisesti tunnettu museo, joka omistaa kyseessä olevan fyysisen taideteoksen. Jotkut museot ovatkin havainneet mahdollisuuden lisätuloihin tekemällä ikivanhoista taide-esineistä tai niiden osista digitaalisia kopioita, joita on myyty NFT-muodossa.

Tekijänoikeuden loukkaukset saattavat jäädä havaitsematta, ja monesti on hankala löytää niitä tahoja, jotka tekijänoikeutta ovat loukanneet. Koska markkinapaikoilla on käytännössä suuri merkitys niin NFT:iden luomisen kuin kauppojen kannalta, markkinapaikkojen vastuuttaminen on yksi tapa ehkäistä väärinkäytöksiä. Monet markkinapaikat tosin toimivat DAO-pohjaisesti, eikä aina ole helppo löytää niitä tahoja, jotka viime kädessä ovat oikeudellisesti vastuussa markkinapaikan toiminnasta.

Keskustelua voidaan käydä siitä, voidaanko markkinapaikkoja pitää Euroopan parlamentin ja neuvoston direktiivissä (EU) 2019/790, annettu 17 päivänä huhtikuuta 2019, tekijänoikeudesta ja lähioikeuksista digitaalisilla sisämarkkinoilla ja direktiivien 96/9/EY ja 2001/29/EY muuttamisesta tarkoitettuina verkkosisällönjakopalvelujen tarjoajina. Direktiivin 2 artiklan 6 kohdan mukaan tällaisella toimijalla tarkoitetaan sellaisen tietoyhteiskunnan palvelun tarjoajaa, jonka päätarkoituksena tai yhtenä päätarkoituksena on säilyttää suuri määrä käyttäjiensä palveluun lataamia tekijänoikeudella suojattuja teoksia tai muuta suojattua aineistoa, jotka palvelu organisoii ja joita se promotoi voitontavoittelua varten, ja antaa yleisölle pääsy niihin. Artiklassa osoitetaan kuitenkin myös useita poikkeuksia, joista yksi koskee verkossa toimivia markkinapaikkoja. Jos NFT-taiteen markkinapaikkojen katsottaisiin kuuluvan sääntelyn piiriin, tällä olisi suuri merkitys erityisesti direktiivin 17 artiklan vuoksi. Tässä artiklassa lähdetään siitä, että jäsenvaltioiden on säädettävä, että ”verkkosisällönjakopalvelujen tarjoaja suorittaa tässä direktiivissä tarkoitettun yleisölle välittämisen tai yleisön saataviin saattamisen, kun se antaa yleisölle pääsyn käyttäjiensä palveluun lataamiin tekijänoikeudella suojattuihin teoksiin tai muuhun suojattuun aineistoon” (17 artiklan 1 kohta). Verkkosisällönjakopalvelun tarjoajien on käytännössä hankittava oikeudenhaltijoilta tähän lupa uhalla, että muuten ne saattavat joutua vastuuseen tekijänoikeuden loukkauksesta.

Henkilö, joka saa taide-NFT:n itselleen esimerkiksi kaupan perusteella, ei lähtökohtaisesti saa itselleen tekijänoikeutta teokseen. TekL 27.2 §:ssä todetaan nimellisesti, että kappaleen luovutukseen ei sisälly tekijänoikeuden luovutus. Lähtökohta on tässä suhteessa sama niin digitaalisen taiteen kuin reaali maailmassa ilmenevien teoskappaleiden yhteydessä. Jos ajatellaan esimerkiksi tiettyä maalausta, on tärkeä erottaa kyseiseen maalaukseen kohdistuva omistusoikeus teokseen kohdistuvasta tekijänoikeudesta. Teoskappaleeseen kohdistuvasta

omistuksesta koituu tosin tiettyjä etuja myös tekijänoikeuslain kannalta. Esimerkiksi TekL 20 §:ssä säädetään teoskappaleen näyttämisestä tilanteessa, jossa teoksen kappale on tekijän suostumuksella myyty tai muutoin pysyvästi luovutettu. Säännöksen mukaan kappaletta saadaan tällöin käyttää teoksen näyttämiseen julkisesti.

Taiteilija voi omistamansa teoskappaleen luovutuksen yhteydessä luovuttaa myös tekijänoikeutensa, ja sama koskee muitakin tahoja, jotka omistavat niin teoksen kuin teoskappaleen. Taiteilijan seuraajien osalta tulee kuitenkin ottaa huomioon TekL 28 §:ssä olevat rajoitukset. Ellei toisin ole sovittu, ei se, jolle tekijänoikeus on luovutettu, saa muuttaa teosta eikä luovuttaa oikeutta toiselle. Jos oikeus kuitenkin kuuluu liikkeelle, sen saa luovuttaa yhdessä liikkeen tai sen osan kanssa.

Erikseen voidaan tietysti sopia siitä, että teoskappaleen luovutuksensaaja saa itselleen myös tekijänoikeuden teokseen olettaen, että teoskappaleen luovuttajalla on oikeus määrätä myös tekijänoikeudesta. Sopiminen voi käytännössä tapahtua usein eri tavoin samoin kuin sopiminen yleensä. Jos kaupanteko tapahtuu jollain valmiilla markkinapaikalla, huomioon tulee ottaa myös markkinapaikan mahdollisesti tarjoamat vakioehdot. Niin taide-NFT:iden ostajien kuin myyjien kannattaa perehtyä huolella siihen, millaisia oikeusvaikutuksia taide-NFT:n luovutukseen liittyy myös tekijänoikeuden kannalta silloin, kun kauppa tehdään markkinapaikalla tiettyjen valintojen puitteissa.

Tekijänoikeus on ilmiönä paljon vanhempi kuin NFT-muotoinen taide. On paljon vanhoja sopimuksia, joissa tekijä on jollain tavalla määrännyt tekijälle kuuluvista taloudellisista oikeuksista toisten hyväksi. Tekijä on esimerkiksi voinut luovuttaa toiselle taloudelliset oikeudet pidättäen kuitenkin jotkin oikeudet itsellään. Jos sopimusta tehtäessä ei ole kiinnitetty lainkaan huomiota tokenisointiin, tulkin ongelmia voi koitua esimerkiksi siitä, kenellä on oikeus tehdä fyysisestä taideteoksesta NFT ja tarjota sitä kenen tahansa ostettavaksi. Tällaisia riitoja on ilmennyt myös käytännössä.

### 6.3 Lohkoketjupatentit

Patentti on käytännössä tärkein erilaisista *teollisoikeuksista*, joihin luetaan myös muun muassa tavaramerkit ja mallioikeus. Siinä missä tekijänoikeus kohdistuu teokseen, patentin kohteena on keksintö. Aivan mikä tahansa keksintö ei kuitenkaan oikeuta patenttiin. Esimerkiksi kotimaisessa patenttilaissa (550/1967; PatenttiL) lähtökohtana on sen 1.1 §:n mukaan:

Joka on tehnyt mihin tekniikan alaan tahansa liittyvän keksinnön, jota voidaan käyttää teollisesti, tai se, jolle keksijän oikeus on siirtynyt, voi hakemuksesta saada patentin keksintöön ja siten yksinoikeuden sen ammattimaiseen hyödyntämiseen sen mukaan kuin tässä laissa säädetään.

Myös keksintöihin liittyvän sääntelyn alalla on tehty pitkään kansainvälistä yhteistyötä, ja patentteihin on otettu kantaa myös EU-tasolla. Muun muassa sisämarkkinoiden tehokas toiminta edellyttää ainakin periaatteessa, että jäsenvaltiot tekevät yhteistyötä. Jo Euroopan unionin toiminnasta tehdyn sopimuksen 118 artiklan 1 kohdassa on todettu, että sisämarkkinoiden toteuttamisen tai toiminnan yhteydessä toteutettaviin toimenpiteisiin olisi kuuluttava yhdenmukaisen patenttisuojan luominen kaikkialla unionissa sekä unionin laajuisten keskitettyjen luvananto-, yhteensovittamis- ja valvontajärjestelmien muodostaminen.

Samoin kuin tekijän, myös keksijän täytyy olla luonnollinen henkilö. Tekijänoikeudesta poiketen patenttia tulee hakea, ja patentit rekisteröidään. Suomessa patenttihakemus tehdään Patentti- ja rekisterihallitukselle (PRH), joka yleensä toimii kansallisena patenttiviranomaisena. Patenttihakemus voidaan tehdä myös Euroopan patenttivarastolle, joka myöntää patenteja Euroopan patenttisopimuksen mukaisesti. Euroopan patenttisopimus, joka on EU:sta riippumaton sopimus, on yleissopimus, joka alun perin tehtiin vuonna 1973. Yleissopimuksen päämerkitys on keskitetyssä hakumenettelyssä, sillä patentin oikeusvaikutukset riippuvat kansallisesta sääntelystä niissä maissa, joissa patentti on saatettu voimaan. Sopimuksella on kuitenkin myös aineelliseen yhdenmukaistamiseen liittyviä tarkoituksia, joita EU-tasolla edistää myös muun muassa Euroopan parlamentin ja neuvoston asetus (EU) N:o 1257/2012, annettu 17 päivänä joulukuuta 2012, yhtenäisen patenttisuojan luomiseksi toteutettavasta tiiviimmästä yhteistyöstä.

Lohkoketjuteknologiaan tavalla tai toisella liittyvät patenttihakemukset ovat lisääntyneet merkittävästi viime vuosina eri puolilla maailmaa, ja joitain patenttihakemuksia on hyväksyttykin. Tietokoneohjelmien osalta huomioon tulee kuitenkin ottaa, että niin Suomessa kuin yleensäkin Euroopassa on perinteisesti lähdetty siitä, että tietokoneohjelmien suoja toteutuu tekijänoikeuden kautta. Tällä on ilmentymänsä myös kotimaisissa patenttilaissa. PatenttiL 1.2 §:n 3 kohdan nojalla keksinnöksi ei katsota pelkästään ”suunnitelmaa, sääntöä tai menetelmää älyllistä toimintaa, peliä tai liiketoimintaa varten taikka tietokoneohjelmaa”.

Patenttilain sanamuoto saattaa antaa jonkin verran harhaanjohtavan kuvan tosiasiallisesta tilanteesta. Myös Euroopan patenttisopimuksen 52 artiklan 2 kappaleesta käy ilmi, että suunnitelmia, sääntöjä tai menetelmiä älyllistä toimintaa, peliä tai liiketoimintaa varten ja tietokoneohjelmia ei pidetä keksintöinä. Artiklan 3 kappaleen mukaan 2 kappaleen määräykset ovat kuitenkin ”esteenä patentin myöntämiselle siinä mainittujen kohteiden tai toimintojen osalta vain siinä määrin, kuin eurooppapatenttia koskeva hakemus tai eurooppapatentti liittyy noihin kohteisiin tai toimintoihin sinänsä”.

Niin eurooppapatentteja kuin kansallisia patentteja myönnetään käytännössä myös tietokoneohjelmilla toteutetuille keksinnöille. Tälle ratkaisulle on ollut tiettyä kansainvälistä painetta, koska esimerkiksi USA:ssa on perinteisesti suhtauduttu myönteisemmin tietokoneohjelmien ja myös erilaisten liiketoimintamenetelmien patentoimiseen. Yleisten keksinnön edellytysten tulee kuitenkin täyttyä, ja huomioon tulee lisäksi ottaa, että lainsäädännön yleisen lähtökohdan mukaisesti tietokoneohjelmat eivät ole keksintöjä. PRH:n omassa *Patenttikäsikirja*-ohjejulkaisussa (Heinäkuu 2022, jakso E.7.3 Tietokoneohjelmia koskevat patenttivaatimukset) lähtökohta on seuraava: ”Jos tietokoneohjelmalla toteutettu keksintö omaa teknisen luonteen, ts. se saa tietokoneessa suoritettuna aikaan teknisen vaikutuksen, joka on enemmän kuin mikä ilmenee tavanomaisessa tietojenkäsittelyssä mitä tahansa tietokoneohjelmaa suoritettaessa, on se patentoitavissa.” Mahdollisuus patenttiin ei tarkoita sitä, ettei tietokoneohjelma itsessään voisi samalla kuulua myös tekijänoikeussuojan piiriin.

Monet lohkoketjuteknologian osat ovat jo yleisessä tiedossa ja käytössä niin, ettei kukaan voi enää saada niihin patenttia uutuusarvon puuttumisen vuoksi. Patentti nimittäin myönnetään esimerkiksi PatenttiL 2.1 §:n mukaan ainoastaan keksintöön, ”joka on uusi siihen verrattuna, mikä on tullut tunnetuksi ennen patenttihakemuksen tekemispäivää, ja lisäksi olennaisesti eroaa siitä”. Parannukset ja lisäykset voivat kuitenkin olla patentoitavissa keksintöinä. Huomioon tulee ottaa myös, että tietokonepohjaiset liiketoimintamenetelmätkin saattavat olla patentoitavissa keksintöinä, jos ne omaavat riittävän teknisen luonteen. Liiketoimintamenetelmiin itsessään liittyy siis samoja ongelmia kuin tietokoneohjelmiin. Myös patenttihakemusten voimakkaasti kasvaneen lukumäärän vuoksi on epäilty, että tulevaisuudessa saattaa syntyä sellaisia lohkoketjuliittännäisiä patenttisotia, joita on aiemmin saatu nähdä esimerkiksi matkapuhelinten valmistajien välillä.

Patentin merkitys on sen synnyttämässä yksinoikeudessa. Kotimaisen patenttilain kannalta keskeinen säännös on tässä suhteessa PatenttiL 3 §, joka sisältää yksityiskohtaista sääntelyä yksinoikeuden sisällöstä. Kukaan ei esimerkiksi saa ilman patentinhaltijan lupaa käyttää hyväksi keksintöä käyttämällä patentoitua menetelmää. Patenttisuojan laajuus riippuu patenttivaatimuksista (PatenttiL 39 §), jotka tulee ilmoittaa jo patenttihakemuksessa. Kansallista patenttihakemusta koskevassa PatenttiL 8 §:ssä lähdetään tältä osin siitä, että hakemuksen tulee sisältää ”keksinnön selitys, tarvittaessa piirustuksineen, sekä täsmällisesti ilmaistuna se, mitä patentilla halutaan suojata”. Patentista tulee suorittaa vuosimaksu, ja myönnetty patentti voidaan PatenttiL 40 §:n mukaan pitää voimassa, kunnes 20 vuotta on kulunut patenttihakemuksen tekemispäivästä. Patentinhaltija voi luovuttaa oi-

keutensa toiselle tai perustaa lisenssejä, ja patentin toiselle siirtymisestä tai käyttöluvan luovuttamisesta tehdään pyynnöstä merkintä patenttirekisteriin (PatenttiL 44.1 §).

## 7 LOPUKSI

Lohkoketjuilla ja lohkoketjusovelluksilla on oma oikeudellinen viitekehyksensä, joka suurelta osin perustuu sellaiseen sääntelyyn, jossa ei erityisesti ole otettu huomioon juuri lohkoketjuteknologiaa. Käsillä olevassa teoksessa on tarkasteltu vain tiettyjä oikeudellisesti relevantteja kysymyksiä. Lukijalle lienee käynyt selväksi, että oikeustilaa voidaan monessa suhteessa pitää melko tulkinnanvaraisena. Lainsäädännön, oikeuskäytännön ja myös oikeustieteellisen keskustelun lisääntymisen myötä opitaan kuitenkin koko ajan paremmin tunnistamaan relevantteja kysymyksiä ja ratkaisemaan ne tarkoituksenmukaisesti.

Lohkoketjuteknologiaan liittyy koko joukko oikeudellisia kysymyksiä, joihin ei nykytiedon valossa antaa varmoja vastauksia. Tähän nähden ei olekaan yllättävää, että monet aihepiiriä koskevat kirjoitukset sisältävät nimenomaisen vastuuvapausilmoituksen. Myös tämän teoksen esipuheessa huomautettiin, että kirjoittajat eivät vastaa materiaalissa mahdollisesti olevista virheistä, puutteista tai epätarkkuuksista.

Aihepiiristä kiinnostuneiden on syytä pyrkiä mahdollisimman laaja-alaiseen perehtymiseen eli käytännössä lukemaan mahdollisimman useiden kirjoittajien tekstejä. Myös kriittisyys on tärkeää siitä riippumatta, luetaanko esimerkiksi oppikirjoja, tieteellisiä teoksia tai artikkeleita taikka erilaisia viranomaisten laatimia tekstejä.

Eri puolilla maailmaa luodaan enenevässä määrin lainsäädäntöä, jota annettaessa on vähintään tosiasiallisesti pidetty silmällä lohkoketjuja ja lohkoketjusovelluksia. Tällaista lainsäädäntöä on annettu myös EU:ssa, ja lainsäädäntötoimia on odotettavissa tulevaisuudessakin. Yksi kiinnostavimmista hankkeista on MiCA-asetus eli asetus kryptovarojen markkinoista ja direktiivin (EU) 2019/1937 muuttamisesta, joka annettaneen lähiaikoina. Asetus tulee tuomaan moniin kysymyksiin selvyyttä omalla soveltumisalueellaan, joskin myös erilaisia tulkintaongelmia voidaan pitää ilmeisinä samoin kuin yleensäkin uuden lainsäädännön yhteydessä.