DIGITAALISEN DISRUPTION VAIKUTUKSIA SISÄISEEN TARKASTUKSEEN: CASE LOHKOKETJUT

Jyväskylän yliopisto
Kauppakorkeakoulu

Pro gradu -tutkielma

2022

Tekijät: Eetu Havia, Jere Selin
Oppiaine: Laskentatoimi
Ohjaaja: Antti Rautiainen

JYVÄSKYLÄN YLIOPISTO

TIIVISTELMÄ

Tekijä
Eetu Havia ja Jere Selin

Työn nimi
Digitaalisen disruption vaikutuksia sisäiseen tarkastukseen: case lohkoketjut

Oppiaine	Työn laji
Laskentatoimi	Pro gradu -tutkielma
Aika (pvm.)	Sivumäärä
4.5.2022	126

Tiivistelmä – Abstract

Lohkoketjuteknologiaa on alettu tutkia uudenlaisena tapana tallentaa ja jakaa tietoa organisaatioiden käyttämissä tietojärjestelmissä. Lisäksi kyseinen teknologia on synnyttänyt täysin uuden kryptovaroiksi kutsutun omaisuusluokan. Lohkoketjuteknologian aiheuttaman muutoksen tietojärjestelmiin on ennakoitu olevan luonteeltaan disruptiivista, sen tapahtuessa ensin vähitellen ja sitten yhtäkkiä, aiheuttaen äkillisiä muutoksia organisaatioiden riskiympäristöön.

Sisäisille tarkastajille on ehdotettu nykyistä suurempaa roolia sekä yleisesti disruptiiviisiin innovaatioihin varautumisessa että erityisesti lohkoketjuteknologian käyttöönottoprosesseissa. Tämän tutkielman tavoite on selvittää suomalaisten sisäisten tarkastajien valmiuksia, kokemuksia ja odotuksia koskien lohkoketjuteknologian käyttöä sekä kryptovarojen käytön mahdollisia vaikutuksia organisaatioiden riskiympäristöön.

Tutkielman teoreettinen viitekehys rakentuu sekä sisäisen tarkastuksen objektiivisuuden ja arvonluonnin tarkastelusta digitalisaation aikakaudella että lohkoketjuteknologian ja lohkoketjupohjaisten sovellusten esittelystä. Tutkielman empiirinen aineisto koostuu sekä kvantitatiivisesta että kvalitatiivisesta aineistosta. Kvantitatiivinen aineisto kerättiin suomalaisille sisäisille tarkastajille suunnattuna verkkokyselynä (n=68). Kvalitatiivista aineistoa varten haastateltiin sähköpostitse kuuden eri asiantuntijaorganisaation edustajia, jotka käsittelevät kryptovaroja.

Tutkimustulosten perusteella lohkoketjuteknologia näkyy toistaiseksi melko vähän suomalaisten sisäisten tarkastajien työtehtävissä, eivätkä sisäiset tarkastajat usko lohkoketjuteknologian nousevan merkittäväksi osaksi työtehtäviä ainakaan lyhyellä aikavälillä. Sisäisten tarkastajien kokema osaaminen ja kiinnostus koskien lohkoketjuteknologiaa oli myös keskimäärin vähäistä. Kryptovarojen liiketoiminnalliseen hyödyntämiseen liittyvät havaitut riskitekijät koskivat hinnan volatiliteettia ja markkinoiden toimivuutta, ulkoisten sidosryhmien suhtautumista, teknologiaosaamista ja käytettävyyttä sekä lainsäädäntöä.

Asiasanat
lohkoketju, sisäinen tarkastus, kryptovara, digitaalinen disruptio

Säilytyspaikka Jyväskylän yliopiston kirjasto

SISÄLLYS

KUVIOT

TAULUKOT

1. JOHDANTO

1.1 Yleistä

Lohkoketjuteknologia (blockchain technology) ja kyseiseen teknologiaan pohjautuvat kryptovarat (crypto assets), kuten kryptovaluutat ja ei-lajiesinemäiset tokenit (NFT) ovat kasvattaneet suosiotaan viimeisten vuosien aikana. Käytön nopeasta kasvusta syntyvät verkostovaikutukset sekä lohkoketjuteknologia uutena teknologisena innovaationa ovat saaneet niin tutkijat kuin kaupalliset toimijatkin pohtimaan eri liiketoimintaprosessien uudelleenorganisointia lohkoketjuteknologiaa hyödyntäen. Lohkoketjuteknologian ja kryptovarojen käytön yleistyminen on ollut niin nopeaa ja laaja-alaista useilla eri toimialoilla, että muutosta on kuvailtu luonteeltaan malliesimerkiksi disruptiivisesta innovaatiosta (Frizzo-Barker ym. 2020). Lohkoketjuteknologian sekä kryptovarojen käytön kasvua onkin verrattu jo internetin nopeaan yleistymiseen 1990-luvun lopulla (Casey & Vigna 2018; Ito, Narula & Ali 2017). Internetin tapaan, lohkoketjuteknologian on ajateltu muodostavan uudentyyppisen liiketoiminnallisen sekä vuorovaikutuksellisen perustan tuleville uusille innovaatioille (Frizzo-Barker ym. 2020).

Kuten internetin yleistyminen, myös lohkoketjuteknologia ja kryptovarat voivat tuoda mukanaan sekä monia mahdollisuuksia että uhkia organisaatioille, joihin vastaaminen voi edellyttää organisaatioissa toimivilta laskentatoimen erityisasiantuntijoilta ponnisteluja kaaoksen välttämiseksi. Monet laskentatoimen erityisasiantuntijat, kuten sisäiset tarkastajat, tuntevat organisaatioiden ydintoiminnot sekä riskiympäristön, joten heidän ammattitaitonsa tehokas hyödyntämin voi osoittautua tärkeäksi elementiksi lohkoketjuteknologian jalkauttamisessa. Lohkoketjuteknologian ja kryptovarojen ajatellaan vaikuttavan organisaatioiden riskiympäristöön kahdella merkittävällä tavalla, joista toinen koskee lohkoketjuteknologian hyödyntämistä osana riskienhallintaa ja toinen puolestaan lohkoketjuteknologian ja kryptovarojen nopeasta yleistymisestä aiheutuvia riskejä. Erityistä huolta riskienhallinnan näkökulmasta ovat herättäneet ajatukset siitä, että internetin yleistymisen tapaan, lohkoketjuteknologian

tai kryptovarojen omaksuminen osaksi liiketoimintoja ei tule välttämättä olemaan organisaation itsensä päätettävissä, jolloin puutteellinen varautuminen voi asettaa organisaation hankalaan asemaan. (Burns, Steele, Cohen & Ramamoorti 2020; Kloch & Little 2019.)

Lohkoketjuteknologiaa koskevan osaamisen kouluttaminen sisäisille tarkastajille on nähty mahdollisena keinona varautua lohkoketjuteknologiapohjaisten sovellusten nopeaan yleistymiseen. Toisaalta sisäiset tarkastajat voisivat osallistua myös lohkoketjuteknologian potentiaalisten käyttökohteiden kartoittamiseen. Rooney, Aiken ja Rooney (2017) ovatkin ehdottaneet sisäisten tarkastajien laajempaa osallistuttamista lohkoketjuteknologiaan siirtymisen päätös- ja käyttöönottoprosesseihin. Näissä tapauksissa sisäisten tarkastajien roolina olisi toimiminen hallinto-, riski- ja valvontaympäristön arvioitsijana sekä neuvonantajana, joka tuntee hyvin organisaation ydintoiminnot (Rooney ym. 2017).

Sisäisen tarkastuksen varautuminen ennalta ja osallistuminen lohkoketjuteknologian käyttöönottoprosessiin voidaan nähdä organisaatiolle arvoa tuottavana toimintona (Lineros 2021). Toisaalta aiheeseen liittyy laajempi sisäisen tarkastuksen luonnetta koskeva kysymys siitä, missä määrin neuvonantajana toimiminen ja sisäisen tarkastuksen konsultoiva ote vaikuttavat objektiivisuuden säilymiseen, jota pidetään yhtenä sisäisen tarkastuksen kulmakivenä. Esimerkiksi Roussy ja Rodrigue (2018) ovat esittäneet objektiivisuuden vaarantuvan, mikäli sisäinen tarkastus työskentelee liian tiiviisti johdon kanssa. Toisaalta Basden, Torcasi, Mack ja Kristall (2017) kyselyn mukaan monet sidosryhmät odottaisivat sisäisen tarkastuksen tuottavan nykyistä enemmän arvoa samalla, kun ”ketterästi” toimiva ja osallistuva sisäinen tarkastus koetaan sidosryhmien kannalta lisäarvoa tuottavana toimintona. (Basden ym. 2017.) Myös Seagon (2015) on todennut, että sisäinen tarkastus voisi ydintoimintojen tuntemisen ansiosta toimia organisaation ”katalysaattorina” parantaen liiketoimintaprosessien tehokkuutta ja suorituskykyä tarjoamalla esimerkiksi suosituksia dataanalyysiin ja arviointiin perustuen.

Huolimatta eri koulukuntien suhtautumisesta sisäisen tarkastuksen objektiivisuuteen liittyviin kysymyksiin, sisäisten tarkastajien tutustumista lohkoketjuteknologiaan suositellaan joka tapauksessa, jotta sisäisen tarkastus pystyisi vähintäänkin säilyttämään kyvykkyytensä riskienhallinnan kolmantena puolustusmuurina (Kloch & Little 2019). Lohkoketjuteknologia voi tarjota sisäiselle tarkastukselle myös mielenkiintoisia työkaluja riskienhallintaan esimerkiksi älysopimusten, hajautettuihin oraakkeleihin perustuvien kontrollien, sekä muiden lohkoketjuteknologian muuttumattomuutta ja läpinäkyvyyttä hyödyntävien järjestelmien avulla (Burns ym. 2020; Lineros 2021). Alles ja Gray (2020) kuitenkin muistuttavat artikkelissaan, ettei lohkoketjujen ja sen sovellusten käyttäminen poista tarvetta sisäiselle tarkastukselle. Heidän mukaansa se voi muuttaa tarkastusten luonnetta jossain määrin, mutta se ei poista itsessään käyttäjien väärinkäytösriskejä, ja voi aiheuttaa myös uudenlaisia riskejä, joita nykyisissä järjestelmissä ei ole kohdattu. Lineros (2021) nostaa artikkelissaan esiin, että lohkoketjujen käyttöön liittyy muun muassa uusia IT-hallintoon liit-

tyviä haasteita, joiden huomioiminen sisäisessä tarkastuksessa on kriittistä. Hänen mukaansa IT-hallintoon liittyvien haasteiden sivuuttaminen, voi johtaa sisäisen tarkastuksen ja organisaation johdon epäonnistumiseen, joka pettää sidosryhmien odotukset. Monet haasteista liittyvät Linerosin (2021) mukaan toisaalta sisäisten tarkastajien osaamiseen ja toisaalta reagoivaan eikä ennakoivaan lähestymistapaan uusien järjestelmien käyttöönotossa.

Lohkoketjupohjaiset järjestelmät ovat tällä hetkellä monin paikoin vasta kehitysvaiheessa, mutta esimerkiksi Cai (2019) on esittänyt, että olisi tärkeää saada jo varhaisessa vaiheessa laskentatoimen asiantuntijoita mukaan kehittämään uusia käyttökohteita lohkoketjuteknologialle. Ongelmaksi on kuitenkin muodostunut osaamiskuilu laskentatoimen asiantuntijoiden ja lohkoketjukehittäjien välille, jonka ylipääsemiseksi molemmat osapuolet tarvitsisivat enemmän toisiltaan tukea. (Cai 2019.) Ymmärrys lohkoketjuteknologiaa kohtaan on näyttäytynyt ongelmana myös sisäisten tarkastajien keskuudessa, jossa laskentatoimen tausta on korostunut ja IT-taustaisia henkilöitä on alalla niukasti (Lineros 2021). Sisäisten tarkastajien kansainvälisen yhteistyöjärjestö IIA:n (The Institute of Internal Auditors) jäsenilleen suunnattuun kyselyyn vastanneista selvä enemmistö (65,3 %) arvioikin lohkoketjuteknologian kokeilun suurimmaksi esteeksi yleisen ymmärryksen puutteen lohkoketjuteknologiaa kohtaan (Kloch & Little 2019).

Kryptovaroja ja lohkoketjuteknologiaa on tutkittu toistaiseksi hyvin vähän sisäisen tarkastuksen näkökulmasta. Roussy ja Perron (2018) ovat tunnistaneet kirjallisuuskatsauksessaan aiheeseen liittyvän tutkimuskirjallisuuden olevan erittäin vähäistä ehdottaen tätä erääksi tulevaisuuden tutkimussuunnista. Myös Kotb, Elbardan ja Halabi (2020) ovat esittäneet, että lohkoketjuteknologian vaikutuksia sisäisen tarkastuksen tulevaisuuteen tulisi selvittää laajemmin. Suomalaista aineistoa hyödyntäviä tutkimuksia tai opinnäytetöitä lohkoketjuteknologiasta tai kryptovaroista ei ole laadittu sisäisen tarkastuksen näkökulmasta lainkaan.

1.2 Tutkimuksen tavoitteet, rajoitteet ja tutkimuskysymys

Teknologian kehittyminen avaa uusia mahdollisuuksia tutkimukselle, mutta toisaalta vaatii teknologian käyttäjiltä ja laskentatoimen ammattilaisilta osaamista toimia jatkuvasti muuttuvassa toimintaympäristössä. Uusien teknologioiden ilmaantuminen voi aiheuttaa muutospaineita laskentatoimen ammattilaisten osaamistarpeisiin, mutta toisaalta myös korostaa ammatillisen skeptisyyden tärkeyttä uuden teknologian hyötyjen arvioinnissa. Aiemmissa kansainvälisissä julkaisuissa on havaittu sisäisten tarkastajien tuntevan vielä heikosti lohkoketjuteknologiaa ja sen mahdollisuuksia (Cai 2019; Lineros 2021; Kloch & Little 2019). Tämän tiedon valossa voitaisiin olettaa, että lohkoketjuteknologia ja kryptovarat ovat myös suomalaisille sisäisille tarkastajille vielä kohtuu uusia asioita. Tutkimuksessa on kaksi teemaa, joista ensimmäinen keskittyy siihen, miten lohkoketjuteknologia näkyy sisäisessä tarkastuksessa Suo-

messa vuonna 2022 ja mitä odotuksia sisäisillä tarkastajilla on lohkoketjuteknologiaan liittyen. Toisena teemana puolestaan selvitetään millaisen riskiympäristön organisaatiot kohtaavat Suomessa niiden ottaessa käyttöön kryptovaroja. Eli selvitetään millaisia haasteita sisäisessä valvonnassa ja tarkastuksessa joudutaan huomioimaan, mikäli kryptovaroja otettaisiin käyttöön.

Tutkimuskysymysten ensimmäiset neljä kysymystä liittyvät ensimmäiseen pääteemaan ja viides tutkimuskysymys liittyy riskiympäristön muutokseen. Tutkimuskysymyksemme ovat:

1. Kuinka paljon lohkoketjut näkyvät sisäisten tarkastajien nykyhetken työssä?
2. Uskovatko sisäiset tarkastajat lohkoketjujen käytön yleistyvän tulevaisuudessa ja vaikuttaako se sisäiseen tarkastukseen?
3. Kuinka hyvin sisäiset tarkastajat osaavat/osaisivat käsitellä työssään lohkoketjuja ja mitkä tekijät selittävät osaamista?
4. Kuinka kiinnostuneita sisäiset tarkastajat ovat lohkoketjuteknologiasta ja mitkä tekijät selittävät kiinnostusta?
5. Millaisia riskejä kryptovarojen käyttö voi aiheuttaa organisaatiolle Suomessa?

Tutkimuksessa suoritettiin sekä kysely että haastatteluita. Kysely toteutettiin yhteistyössä Sisäiset tarkastajat ry:n kanssa. Kysely lähetettiin koko yhdistyksen jäsenistölle yhdistyksen sähköpostilistan kautta, jonka lisäksi sataan sisäiseen tarkastajaan oltiin myös suoraan yhteydessä. Kyselyn vastaukset analysoitiin tilastollisin menetelmin ja kyselyaineiston avulla vastataan tutkimuskysymyksiin 1–4. Tutkimuskysymystä viisi varten suoritettiin asiantuntijahaastatteluita. Haastateltavat työskentelevät kaikki johtoasemassa kukin erilaisissa organisaatioissa, jotka toimivat kryptovaluuttojen parissa. Tarkemmin menetelmiä ja aineistoa on avattu luvussa viisi.

Tutkimuksen rajoituksista lukijan on hyvä tiedostaa, että lohkoketjuissa kulkevia varallisuuseriä ja lohkoketjuja ylipäätään koskeva sanasto ei ole vielä kehittynyt kovin monimuotoiseksi ja ristiriitaista luokittelua tapahtuu paljon eri viranomaistoimijoiden sekä lähteiden välillä. Tässä tutkimuksessa on jouduttu soveltamaan nykyisiä käsitteitä ja muun muassa kääntämään sellaisia termejä, joille ei ole vastinetta suomen kielessä. Sekä käännösten että muuten vakiintumattomien termien osalta on pyritty käyttämään mahdollisimman hyvin asiaa kuvaavaa termiä.

1.3 Keskeiset käsitteet

Sisäinen tarkastus on objektiivista ja riippumatonta arviointi-, varmistus- sekä konsultointitoimintaa. Sisäisen tarkastuksen rooli on tuottaa lisäarvoa organisaatioille ja parantaa niiden toimintaa tukemalla tavoitteiden saavuttamisessa sekä tarjoamalla järjestelmällisen lähestymistavan valvonta-,

riskienhallinta-, sekä hallinto- ja johtamisprosessien tehokkuuden arviointiin ja kehittämiseen. (Sisäiset tarkastajat ry 2022a.)

Disruptiivinen innovaatio kuvaa uutta ja usein teknologista innovaatiota, joka mahdollistaa vähäiset resurssit omaavalle organisaatiolle kyvyn haastaa alan vakiintuneet toimijat. Teoria perustuu siihen, että alan vakiintuneet toimijat keskittyvät usein liiaksi palvelemaan vain nykyisten tuottavimpien ydinasiakkaiden tarpeita, eikä markkinoille saapuvia uusia innovaatioita jalkauteta mukaan toimintaan, mikäli ne eivät vastaa suoranaisesti näiden ydinasiakkaiden tarpeisiin. Alan pienemmät toimijat voivat kuitenkin omaksua nämä uudet innovaatiot osaksi toimintaansa, mikäli ne tuovat arvoa heidän mahdollisesti kapeammalle asiakassegmentillensä. Mikäli innovaatio osoittautuu todella toimivaksi, niin jossain vaiheessa myös vakiintuneiden toimijoiden ydinasiakkaat haluavat siirtyä käyttämään kyseistä innovaatiota, jolloin ne hylkäävät alan vakiintuneiden toimijoiden ratkaisut aiheuttaen *disruptiota* toimialan markkinoilla. (Bower & Christensen 1995.)

Lohkoketju on joukko tapahtumatietoja sisältäviä lohkoja, jotka yhdistyvät toisiinsa kryptografian avulla muodostaen ”ketjun”. Lohkoketju toteutetaan käytännössä listana tai lokina transaktioista, jotka jaetaan verkoston kesken ja tämän perusteella koostetaan tietokanta. Jokainen uusi lohko sisältää tiivistelmän aiemmista lohkoista ja jokaisen verkoston jäsenen on mahdollista tarkistaa jokainen uusi lohko ennen lohkon hyväksymistä ja lisäämistä osaksi lohkoketjua. Tämän on katsottu tekevän tapahtumahistorian väärentämisen lähes mahdottomaksi. *Lohkoketjuteknologian* synnyttämä innovaatio onkin kyky taata tietojen tarkkuus ja turvallisuus ilman, että tarvittaisiin luotettavaa kolmatta osapuolta pitämään huolta järjestelmän toiminnasta. (Hayes 2022.)

Lohkoketjujärjestelmä voi olla käytännössä lähes mikä vain tietojärjestelmä, joka käyttää pohjana lohkoketjuteknologiaa. Järjestelmän loppukäyttäjä ei välttämättä edes tiedä käyttävänsä lohkoketjujen päällä toimivaa järjestelmää, vaan se on enemmänkin taustalla toimiva alusta, jonka päälle on rakennettu käyttöliittymä. (Hayes 2022.)

Tokenisointi tarkoittaa varallisuuserän omistusoikeuden siirtämistä lohkoketjujärjestelmään siten, että lohkoketjujärjestelmässä käsiteltävä *tokeni* (poletti) edustaa omistusoikeutta kyseiseen varallisuuserään (Dutta 2020, 79).

Kryptovara on kryptografisesti suojattu esitys digitaalisesta arvosta tai sopimuksesta, jota voidaan siirrellä ja tallentaa sähköisesti, sekä käydä kauppaa julkisilla markkinoilla. Kryptovarojen toiminta perustuu lohkoketjuteknologiaan. (*HMRC* 2021.)

Lajiesinemäisyydellä tarkoitetaan kryptovarojen kontekstissa sitä, että kryptovarana toimiva esitys on korvattavissa päikseen toisella samansisältöisellä esityksellä. Lajiesinemäisyyden vastakohta on *ei-lajiesinemäisyys*, joka tarkoitta sitä, että jokainen esitys on uniikki eikä näin ollen suoraan korvattavissa toisella esityksellä. (Tanninen 2021.) Yksinkertaistettuna *kryptovaluutat* edustavat lajiesinemäisiä kryptovaroja, kun taas *NFT*-tokenit ovat ei-lajiesinemäisiä kryptovaroja.

1.4 Tutkielman rakenne

Rakenteeltaan tutkielma koostuu johdannosta, teoriaosasta, tutkimusosasta ja johtopäätöksistä. Johdannossa esitetään tutkimuksen tausta, tavoitteet, tutkimuskysymys sekä määritellään lyhyesti keskeiset käsitteet. Johdantoa seuraa teoriaosuus, joka pohjautuu tutkittavaa asiaa käsittävään kirjallisuuteen, tutkimukseen sekä tieteellisiin artikkeleihin. Tutkimuksen teoriaosa koostuu kahdesta eri pääteemasta.

Teoriaosan ensimmäisessä osassa esitellään sisäisen tarkastuksen perusperiaatteet. Lisäksi tarkastellaan sisäistä tarkastusta arvoa tuottavana toimintona sekä sitä, millaisista tekijöistä tämä arvo voi koostua. Teoriaosassa perehdytään myös uusien innovaatioiden, erityisesti IT-teknologioiden, mahdollisiin vaikutuksiin sisäisessä tarkastuksessa. Tarkastelun kohteena on erityisesti se, kuinka sisäinen tarkastus voi toisaalta varautua uusien innovaatioiden aiheuttamiin mahdollisiin haasteisiin, mutta toisaalta myös käyttää niitä hyväksi toiminnan kehittämisessä.

Teoriaosan toisessa osuudessa keskitytään esittelemään lohkoketjuteknologiaa ja kryptovarojen teoreettista taustaa sekä teknologisista että liiketoiminnallisista näkökulmista. Tämän teoriaosan tarkoituksena on havainnollistaa syitä sille, miksi ja miten organisaatiot voivat päätyä käyttämään lohkoketjuteknologiaa tai kryptovaroja tulevaisuudessa, vaikka ajatus näiden käytöstä tuntuisi toistaiseksi vielä vieraalta. Toisen osion lopussa esitellään vielä tarkemmin lohkoketjuteknologian erityispiirteitä sisäisessä tarkastuksessa sekä keinoja, joilla sisäinen tarkastus voi hallita lohkoketjuteknologian käyttöön liittyviä tunnistettuja riskejä. Teoriaosion tarkoituksena on luoda lukijalle riittävä kuva tutkittavasta aiheesta, sekä luoda viitekehys ennen varsinaista empiiristä tutkimusta.

Tutkimusosa koostuu luvuista neljä ja viisi. Tutkielman neljännessä pääluvussa esitellään tutkimusaineiston keräämistapa sekä perustellaan valitut aineistonkeruu sekä -analysointimenetelmät. Viidennessä luvussa esitellään saadut tulokset. Kuudennessa luvussa vastataan tutkimuskysymyksiin, esitetään johtopäätökset sekä arvioidaan tutkimuksen luotettavuutta ja esitetään mahdollisia jatkotutkimusaiheita.

2. SISÄINEN TARKASTUS

2.1 Johdanto

Organisaation sisäiset tarkastuskontrollit voidaan jakaa valvontaan ja tarkastukseen. Organisaatioiden johdolla on vastuu järjestää tehokas sisäinen valvonta. Sisäinen tarkastus toimii valvontavastuun täyttämisessä ylimmän johdon kumppanina. Sillä tulee olla riippumaton asema organisaatiossa, joka mahdollistaa objektiivisten varmennus- ja konsultointipalveluiden tuottamisen, joiden tavoitteena on kehittää ja parantaa organisaation toimintatapoja. Toimiva sisäinen tarkastus auttaa yritysjohtoa turvaamaan raportoinnin luotettavuutta, noudattamaan lakeja ja ohjeistuksia sekä tarkastelemaan toimintojen tehokkuutta ja tuloksellisuutta. (Niemi 2018; Ratsula 2017.)

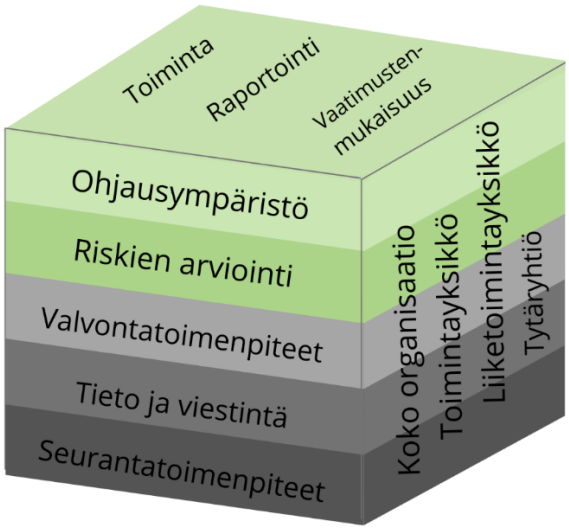
Sisäinen valvonta puolestaan on jatkuvaa ohjausta ja valvontaa, ei siis varsinaista tarkistamista. Sen sijaan se on osa johtamis- ja hallinnonseurantajärjestelmää, jolla pyritään samaan kohtuullinen varmuus, että organisaation toiminnoista, raportoinnista sekä vaatimuksenmukaisuudesta annetut tavoitteet täyttyvät. Käytännössä sisäinen valvonta koostuu useista organisaation eri tasoilla tapahtuvista toimista. Nämä toimet käsittävät esimerkiksi erilaiset hyväksymisvaltuudet, työtehtävien jaon ja käytössä olevien järjestelmien sisältämät kontrollit. (Ratsula 2017.)

Termeinä sisäinen tarkastus ja valvonta voivat mennä helposti sekaisin osittain samankaltaisten tavoitteiden ja tehtävien vuoksi, mutta kiteytettynä erona on, että sisäisestä valvonnasta vastaa organisaation toimiva johto, kun taas sisäinen tarkastus vastaa sisäisen valvonnan arvioinnista. Huomionarvoista on myös se, että sisäinen tarkastus ei voi hoitaa itse tai toimeenpanna sisäisen valvonnan toteuttamista, koska tämä vaarantaisi tarkastusten objektiivisuuden ja riippumattomuuden. Sen sijaan yksittäisiä seurantatoimenpiteitä voivat hoi-

taa myös sisäiset tarkastajat, kunhan tämä ei vaaranna objektiivisuutta tai riippumattomuutta. (Niemi 2018.)

2.1.1 Sisäinen valvonta – COSO-malli

Sisäistä tarkastusta tai valvonnan toimenpiteiden varmennusta ei ole mielekästä suorittaa, mikäli sisäistä valvontaa ei ole ensin järjestetty huolellisesti. Tehokkaan sisäisen valvonnan järjestämisen avuksi on tuotettu yleisesti tunnettu COSO-viitekehys. Viitekehyksen mukaan sisäinen valvonta koostuu viidestä toisiinsa liittyvästä osatekijästä, jotka ovat aina suhteessa toisiinsa. Nämä tekijät ovat esitetty alla olevan kuvion 1 ”etuseinällä”. (COSO 2013; Niemi 2018.)



Kuvio 1: ”COSO-kuutio” (Sisäiset tarkastajat ry 2022b)

COSO-malli jakaa sisäisen valvonnan tavoitteet kolmeen luokkaan. Toiminnan tavoitteet, kuten suoritustavoitteet ja organisaation omaisuuden turvaaminen petoksilta, keskittyvät liiketoiminnan vaikuttavuuteen ja tehokkuuteen. Raportoinnin tavoitteet, mukaan lukien sekä sisäinen että ulkoinen talousraportointi sekä ei-taloudellinen raportointi, liittyvät organisaation raportointitapojen läpinäkyvyyteen, oikea-aikaisuuteen ja luotettavuuteen. Vaatimustenmukaisuutta koskevat tavoitteet ovat puolestaan sisäisen valvonnan tavoitteita, jotka perustuvat niiden lakien ja määräysten noudattamiseen, joita organisaation on noudatettava. (COSO 2013; Ratsula 2017.) Mallin kolmannella akselilla ovat puolestaan eri liiketoimintatasot muistuttamassa, että valvontaa tulee suorittaa kaikilla eri tasoilla (COSO 2013).

COSO-malli tarjoaa siis viitekehyksen tai mallinnuksen siitä, mitä kaikkea sisäinen valvonta pitää sisällään. COSO-kuution hyödyntämisen helpottamiseksi on laadittu vielä 17 perusperiaatetta tarkasteltavista asioista, joiden perusteella valvonta koostetaan. (COSO 2013.) Eli kuten edellä esitetystä mallista käy ilmi, sisäinen valvonta kattaa käytännössä koko organisaation ja on osa joh-

tamis- ja hallinnonseurantajärjestelmää. Tämän valvonnan tavoitteena on luoda käytänteitä ja valvoa, että muun muassa organisaation toiminnoista, raportoinnista ja vaatimuksenmukaisuudesta annetut tavoitteet täyttyvät.

2.1.2 Sisäinen tarkastus

Toisin kuin esimerkiksi tilintarkastuksen, ei sisäisen tarkastuksen järjestämisestä yrityksissä säädetä tarkasti lailla, mutta osakeyhtiölaissa kuitenkin viitataan pörssiyhtiöiden ja muiden yleisen edun kannalta merkittävien yhtiöiden hallitusten velvoitteeseen kiinnittää erityistä huomiota muun muassa sisäisen tarkastuksen tehokkuuteen (Osakeyhtiölaki 6:16.2 §). Edellä mainitun velvoitteen täyttämiseksi julkisesti noteeratussa tai muussa yleisen edun kannalta merkittävässä yhtiössä täytyy siis järjestää myös sisäinen tarkastus. Myös esimerkiksi vakuutussektorilla toimivilla yhtiöillä tulee lain mukaan olla sisäinen tarkastaja, joka arvioi yhtiön sisäisen valvonnan ja muun hallinnon riittävyyttä ja tehokkuutta (Vakuutusyhtiölaki 6:15 §). Muille yritystoimijoille sisäisen tarkastuksen järjestäminen puolestaan vaikuttaa täysin vapaaehtoiselta, mutta se ei tietenkään poista tarkastajan tuomia hyötyjä muissakaan organisaatioissa.

Sisäisten tarkastajien tarpeellisuutta on perusteltu muun muassa niin sanotulla agenttiongelmalla. Tällaiset ongelmat nousevat esiin etenkin sellaisissa yrityksissä, joiden omistus ja johto on hajautunut. Lyhyesti selitettynä agenttiongelmassa on kyse siitä, että johtohenkilöt pyrkivät maksimoimaan omaa etuaan omistajien edun kustannuksella ja omistaja tarvitsee sen vuoksi kolmannen osapuolen tarkkailemaan johtoa. Sisäinen tarkastus voidaankin nähdä kolmantena osapuolena ja tarkastuksilla on todistettavasti saatu pienennettyä agenttiongelmaa. (Adams 1994.)

Sisäisen valvonnan järjestämistä ja toimintaa valvovat siis sisäiset tarkastajat. Tarkastajat voivat olla joko organisaation sisäisiä työntekijöitä tai tarkastus on mahdollista ostaa myös ulkoiselta palveluntarjoajalta. Tarkastusten tavoitteena on tuottaa organisaation johdon ja omistajien sisäiseen käyttöön riippumatonta tietoa organisaation riskienhallinnasta, valvonnasta sekä hallinto- ja johtamisprosesseista. Tarkastuksilla on tavoitteena myös estää ja havaita tehottomuuksia sekä väärinkäytöksiä, jotka voisivat hankaloittaa organisaation tavoitteiden saavuttamista. Tarkastajien työnkuvaan voi kuulua myös organisaation neuvonta ja kouluttaminen erilaisten hyvien toimintatapojen löytämiseksi. (Niemi 2018.)

Sisäistä tarkastusta ohjaavat kansainväliset ammattistandardit. Ammattina sisäinen tarkastus on melko vanha, sillä sisäisiä tarkastajia on ollut ainakin 1900 luvun alkupuolelta saakka. Sisäistä tarkastusta koskevia vaatimuksia ja standardeja on muutettu ajan myötä vastaamaan kehittyviin tarpeisiin. Tarkastajien työnkuva on muuttunut alkuaikojen ”vahtikoirasta” yhä enemmän konsultoivaan rooliin. (Chambers & Odar 2015; Roussy & Perron 2018). Sisäisten tarkastajien kansainvälisen yhteistyöjärjestö IIA:n (The Institute of Internal Auditors) laatimien ammattistandardien tavoitteena on määrittää niin sanottu minimitaso, jonka mukaan sisäisten tarkastajien tulisi toimia tehtävissään. Nämä standardit koostuvat kolmesta pääosasta. Ensimmäinen osa ovat ominaisuus-

standardit. Tämä osa koskee sisäistä tarkastusta hoitavien toimijoiden ominaispiirteitä. Toinen osa koostuu toteutustapastandardeista, jotka puolestaan määrittävät laatuvaatimukset ja kuvaavat tehtävien luonteen. Tehtävistä suoriutumista voidaan arvioida näiden laatustandardien mukaan. Kolmas osa koostuu puolestaan soveltamisstandardeista, joissa syvennetään ominaisuus- ja toteutustapastandardeja sekä tarkennetaan muun muassa konsultointi-, arviointi- ja varmistustehtäviä koskevia vaatimuksia. (IIA 2016; Sisäiset tarkastajat ry 2022b.)

Sisäisen tarkastuksen tehtävät ovat muuttuneet 2000- luvun aikana pelkästä tarkastustoiminnasta yhä enemmän konsultoivaan rooliin. Sisäisten tarkastajien tehtäviin kuuluvatkin nykyään varsinaisten tarkastusten tai varmennusten teon lisäksi muun muassa johdon avustaminen tehokkaan sisäisen valvonnan rakentamisessa ja muut konsultoivat tehtävät. (Chambers & Odar 2015; Roussy & Perron 2018.) Muuttuneesta tehtäväkuvauksesta huolimatta sisäisten tarkastajien tulee pysyä huolehtimaan myös konsultointitehtävissään siitä, ettei objektiivisuus tai riippuvuus kärsi. Sisäinen tarkastaja voi esimerkiksi avustaa johtoa riskienhallintaprosessien käyttöönotossa tai kehittämisessä, mutta sisäisen tarkastajan tulee pidättäytyä ottamasta johdolle kuuluvaa vastuuta varsinaisessa riskien hallinnassa tai prosessien täytäntöönpanossa (IIA 2120.C3 2016).

2.2 Sisäinen tarkastus arvoa tuottavana toimintona

Sisäisen tarkastuksen tulisi määritelmänsä mukaan olla arvoa tuottava toiminto, mutta vaikuttaisi sille, että sisäisen tarkastuksen tuottama arvo koostuu hieman erilaisista tekijöistä eri organisaatioissa. Muun muassa Jiang, Messier ja Wood (2020) mukaan perinteisen talousraportoinnin varmentamisen lisäksi sisäisellä tarkastuksella on mahdollisuus tuottaa organisaatiolle lisäarvoa tarjoamalla tietoa ja näkökulmia, joita organisaation johdossa voidaan käyttää operatiivisten ja strategisten päätösten tukena. Kuitenkaan aina organisaatioissa ei välttämättä ole tarvetta tällaisille näkökulmille ja niissä tapauksissa sisäisen tarkastuksen olisi kyettävä tuottamaan lisäarvoa muilla tavoin.

Andersonin (2003) mukaan sisäisen tarkastuksen arvonluontia arvioitaessa tulisi lähteä liikkeelle siitä, että määritellään asiakas tai sidosryhmä, jolle lisäarvoa pyritään tuottamaan. Mahdollisia sidosryhmiä ovat esimerkiksi organisaation johto, tilintarkastajat, omistajat, tavarantoimittajat sekä viranomaiset. Sisäisen tarkastuksen tuottama arvo eri sidosryhmille vaihtelee kunkin sidosryhmän tarpeista riippuen. Esimerkiksi tilintarkastajat voivat katsoa sisäisen tarkastuksen olevan osa organisaation omaa sisäistä valvontaa ja toimiva sisäinen valvonta ja -tarkastus voivat helpottaa tilintarkastajan työtä. Tavarantoimittajat ja asiakkaat puolestaan voivat odottaa sisäisen tarkastuksen varmistavan, että rajapinnat, joissa liikkuu heidän tietojaan ovat turvallisia. Toisinaan eri sidosryhmien odotukset ja tarpeet ovat ristiriidassa käytössä olevien resurssien kanssa ja toisaalta jopa sisäisten tarkastajien tehtävien kanssa. Selkeimmin sidosryhmienväliset, osittain ristiriitaiset tarpeet nousevat esiin Andersonin mukaan tarkasteltaessa tarkastusvaliokunnan tai hallituksen odotuksia suhteessa

toimivan johdon odotuksiin. Hallitus sekä tarkastusvaliokunta odottavat sisäisen tarkastuksen tarjoavan varmennuksen siitä, että sisäinen valvonta on riittävää, johtajien toimittamat tiedot ovat luotettavia sekä organisaatio toimii noudattaen lakeja ja määräyksiä. Operatiivinen johto puolestaan voi odottaa sisäisen tarkastuksen auttavan tehokkuuteen ja suorituskykyyn vaikuttavien kohteiden havainnoinnissa ja muotoilussa. Toisin sanottuna operatiivinen johto voi odottaa sisäisen tarkastuksen toimivan muutosagenttina, kun taas tarkastusvaliokunta ja hallitus odottavat sisäisen tarkastuksen parantavan informaation laatua. Sisäisen tarkastuksen luoma arvo voi siis riippua siitä, minkä sidosryhmän tarpeista asiaa tarkastellaan. (Anderson 2003.)

Myös Roth (2003) pitää tärkeänä sidosryhmien ja heidän tarpeidensa tunnistamista. Vuonna 2003 sisäiset tarkastajat näkivät kyselyn mukaan työssään tulevaisuudessa tärkeiksi ja nouseviksi suuntauksiksi muun muassa konsultoinnin, riskien hallinnan, tietokoneavusteisen auditoinnin, kyberturvallisuuden, sisäisen valvonnan yksiköiden kouluttamisen sekä jatkuvan tarkkailun ja varmentamisen. Sisäiset tarkastajat uskovat, että keskittymällä näihin edellä mainittuihin teemoihin he myös tuottavat arvoa organisaatiolle, jossa he toimivat. Kuitenkin Roth nostaa artikkelissaan esiin lisäarvon tuottamisen vaikean mitattavuuden sekä vaihtelevat määritelmät siitä, mikä todella tuottaa lisäarvoa. Toiset sisäiset tarkastajat korostavat vaatimuksenmukaisuustarkastuksia, kun taas toiset mieltävät lisäarvoa syntyvän johdon tukemisesta liiketoiminnan kehittämisessä. Vaihtelevat näkökulmat ovatkin todennäköisesti riippuvaisia organisaatiosta ja siitä, mitä sisäisiltä tarkastajilta odotetaan kyseisessä organisaatiossa. Vaikka lisäarvoa tuottava toiminta vaihtelee luonteeltaan eri organisaatioissa, on Rothin mukaan olemassa joitakin yleisiä tekijöitä, joita voidaan soveltaa kaikkialla. Näitä tekijöitä ovat sisäisen tarkastajan syvällinen tuntemus muun muassa organisaatiosta, kulttuurista, avaintoimijoista ja kilpailuympäristöstä. Lisäksi rohkeus innovoida odottamattomilla tavoilla, sekä luovuus mukauttaa uusia innovaatioita yrityksen tarpeisiin voivat auttaa ylittämään sidosryhmien odotukset. (Roth 2003.)

Puolestaan Seagon (2015) mukaan sisäisen tarkastajan tuottama arvo koostuu kolmesta osatekijästä, joita ovat; varmentajana toimiminen, objektiivisuus sekä syvä tietämys organisaatiosta. Sisäinen tarkastus antaa varmuuden hallinnosta, riskienhallinnasta ja kontrolleista auttaakseen organisaatiota saavuttamaan sen strategiset, operationaaliset, taloudelliset sekä valvonnalliset tavoitteet. Syvän organisaation ymmärryksen avulla sisäinen tarkastus voi toimia myös niin sanottuna ”katalysaattorina”, joka voi parantaa tehokkuutta ja suorituskykyä tarjoamalla suosituksia, jotka perustuvat liiketoimintaprosessien ja datan analyyseihin ja arviointiin. Objektiivisuus näkökulmasta tarkasteltuna sisäinen tarkastus voi puolestaan tuottaa arvoa hallintoelimille ja ylimmälle johdolle toimimalla objektiivisena riippumattomana neuvonnan lähteenä. (Seago 2015.)

Sisäisille tarkastajille laaditun kattavan kansainvälisen kyselyn, johon vastasi hieman vajaa 15 000 tarkastajaa, mukaan lähes kaikki sisäiset tarkastajat pitävät yhtenä tärkeimmistä arvoa tuottavista toiminnoista sisäisen valvonnan

riittävyyden ja tehokkuuden varmistamista. Muina tärkeimpinä arvoa tuottavina toimina sisäiset tarkastajat näkivät liiketoimintakohteiden parannusehdotukset, riskinhallintaprosessien varmistamisen sekä säännösten noudattamisen varmistamisen. Sisäisten tarkastajien omissa vastauksissa siis korostuivat varmentajana toimimisen näkökulma, kun taas asiantuntijarooli sekä objektiivisen neuvonantajan rooli nousivat harvemmin esiin. (Seago 2015.)

Kuten Aderson (2003) ja Roth (2003) myös Seago (2015) nostaa julkaisussaan esiin sisäisen tarkastuksen tarpeen tunnistaa sidosryhmät ja niiden odotukset. Seagon (2015) mukaan sisäisen tarkastuksen tulisikin aivan ensiksi tunnistaa ne odotukset, jotka sille on asetettu. Ilman odotusten tunnistamista on hyvin haastavaa myöskään vastata näihin odotuksiin. Odotusten tunnistamisen jälkeen olisi syytä luoda mittarit, joilla voidaan arvioida odotusten täyttymistä ja aloittaa mittaaminen. Lopuksi tulokset raportoidaan sidosryhmille ja vähintään kerran vuodessa tarkastetaan sidosryhmien odotukset ja tarpeet uudestaan, jotta jatkossakin pystytään tuottamaan arvoa sidosryhmille. (Seago 2015.)

Kuten edellä on todettu, on sisäisellä tarkastuksella erilaisia rooleja ja eri sidosryhmien odotukset vaihtelevat. Basden ym. (2017) raportin mukaan monet keskeiset sidosryhmät odottavat sisäisten tarkastajien tuottavan enemmän lisäarvoa kuin sisäinen tarkastus oli pystynyt tuottamaan vuoden 2017 aikana. Vain 44 % kaikista vastaajista oli sitä mieltä, että sisäisen tarkastus tuottaa merkittävää arvoa. Toisaalta samaan aikaan niissä organisaatioissa, joissa on käytössä ”ketterä” (agile) sisäinen tarkastus oli sidosryhmien tyytyväisyysaste 88 %. (Basden ym. 2017.) Havaintoa, joko lisäarvoa tuottamattomasta tai heikosti lisäarvoa tuottavasta sisäisestä tarkastuksesta, voidaan pitää D’Onza, Selim, Melville ja Allegrini (2015) tutkimuksen perusteella huolestuttavana. D’Onza, ym. korostavat, että lisäarvontuottamiskyky on erittäin tärkeää sisäiselle tarkastukselle, sillä tarve sisäiselle tarkastukselle perustuu nimenomaan sen kykyyn tuottaa lisäarvoa organisaatiolle. Lisäarvoa tuottamattomalla sisäisellä tarkastuksella uhkana on tuottaa enemmän kustannuksia kuin hyötyjä.

Basden ym. (2017) sekä Kotb, Elbardan ja Halabi (2020) raporttien mukaan vaikuttaisi sille, että nopeasti muuttuvassa liiketoimintaympäristössä, joissa esiintyy lukuisia disruptiivisia tekijöitä, ketterä sisäinen tarkastus tuottaa sidosryhmille huomattavasti enemmän arvoa kuin muunlainen sisäinen tarkastus. Raportin mukaan ketterät sisäiset tarkastajat osallistuivat huomattavasti muita sisäisiä tarkastajia useammin organisaation toimintaympäristön muutosten aiheuttamien häiriöiden kartoittamiseen, hallitsemiseen ja häiriöihin vastaamiseen.

Ketterässä sisäisessä tarkastuksessa lähtökohtana on, että tarkastuksen toiminnot katsovat tulevaisuuteen ennakoiden tulevia murroksia sekä niihin liittyviä tarpeita. Tällainen sisäinen tarkastus toimii integroidusti yhdessä organisaation muiden toimintojen kanssa. Ennakoiva asenne ja toiminta tiiviissä yhteistyössä organisaation muiden toimintojen kanssa mahdollistaa sisäiselle tarkastukselle muun muassa johdon apuna toimimisen, sillä silloin heillä on ajantasaisin tieto siitä, mitä on edessä ja miten kulloinenkin asia voitaisiin ratkaista. Toisaalta ketterään sisäiseen tarkastukseen kuuluu myös muuntautumis-

tai sopeutumiskyky. Sopeutumiskykyinen sisäinen tarkastus reagoi kohdattuihin disruptiivisiin muutoksiin nopeasti ja osaa tarvittaessa kohdistaa tarkastuksen resurssit suhteessa muuttuvaan ympäristöön. (Basden ym. 2017.)

Integroidusti johdon kanssa tiiviisti yhdessä toimivasta sisäisestä tarkastuksesta on esitetty myös kritiikkiä. Muun muassa Roussy ja Rodrigue (2018) nostavat artikkelissaan esiin objektiivisuuden voivan vaarantua kyseisessä menettelyssä. Artikkelissa nostetaan esiin mahdollisuus, ettei johdon kanssa tiiviisti työskentelevä sisäinen tarkastus välttämättä kiinnitä tarpeeksi huomiota johdon toimien arviointiin ja varmentamiseen, sillä he työskentelevät niin sanotusti liian lähellä johtoa. Sisäisten tarkastajien tiivis työskentely johdon kanssa voi johtaa myös siihen, ettei tarkastusvaliokunta saa kaikkea tarvitsemaansa tietoa tarkistaakseen johdon toimia. (Roussy & Rodrigue 2018.)

Toisaalta sisäisen tarkastuksen ketteryyden ja tiiviin yhteistyön johdon kanssa voidaan siis olettaa samaan aikaan tuottavan lisäarvoa ja toisaalta voivan aiheuttaa haasteita sisäisen tarkastuksen objektiivisuudelle ja vaikeuttaa toisten sidosryhmien arviointityötä. Suomessa tehdyissä sisäisten tarkastajien haastatteluissa on havaittu Sintosen (2017) mukaan, että ”monesti sisäinen tarkastuksen työ ja osallistuminen alkavat vasta kun muutos on tapahtunut, uusi toimintamalli kehitetty ja implementoitu. Kun sisäinen tarkastus ei ole tarpeeksi kiinteästi mukana uuden liiketoimintamallin kehitysvaiheessa, tarpeellinen osaaminen jää kertymättä tai se kertyy takapainotteisesti.” Vaikuttaisi siis sille, että Suomessa ei ollut ainakaan vielä 2017 mennessä siirrytty laajasti niin sanottuun ketterään sisäiseen tarkastamiseen, vaan toimintaympäristön muutokset tulevat sisäisille tarkastajille niin sanotusti yllättäen ja tarkastuksen toiminta on enemmän reaktiivista kuin ennakoivaa.

Yhteenvetona sisäisen tarkastuksen arvoa tuottavista toimista voidaan todeta, että sisäisen tarkastuksen tuottama arvo vaihtelee sen mukaan, mistä näkökulmasta ja missä organisaatiossa asiaa tarkastellaan. Sisäisillä tarkastajilla on oma näkemys toimista, jotka tuottavat heidän organisaatiolleen lisäarvoa, kun taas eri sidosryhmillä on omat näkemyksensä. Sisäinen tarkastaja joutuukin työssään puntaroimaan sitä, mikä sidosryhmä on merkittävin vai ovatko kaikki yhtä arvokkaita ja toimimaan siten, että sekä ammatillinen ohjeistus että sidosryhmien odotukset täyttyvät parhaalla mahdollisella tavalla.

2.2.1 Sisäisen tarkastus ja IT-teknologia

Teknologian käyttö auditointiprosesseissa jatkaa kasvuaan, mutta Cangemin (2016) mukaan parantamisen varaa olisi yhä. Hän ehdottaa, että sisäisten tarkastajien tulisi käyttää teknologiaa parantaakseen sisäisen tarkastuksen tehokkuutta ja tuottaakseen siten organisaatiolleen enemmän arvoa. Samaan aikaan uusien teknologioiden vaikutukset ovat olleet paradoksaalisia. Toisaalta kehittyvät teknologiat ovat luoneet vaikeammin tarkastettavan järjestelmän. Toisaalta tarkastajat ovat kuitenkin onnistuneet käyttämään uusia teknologioita tarkastuksen välineinä ja siten teknologia on myös muovannut prosesseja tehokkaammiksi. (Cangem 2016.)

Vuonna 2015 toteutetun kansainvälisen kyselyn mukaan sisäisistä tarkastajista IT-taustaisia oli vastaajista vain 10 %, kun taas esimerkiksi laskentatoimen taustalla toimivia sisäisiä tarkastajia oli 60 %. Vähäinen IT-osaajien määrä voi aiheuttaa sisäisen tarkastuksen osastoille haasteita teknologiaan liittyvissä tai teknologiaosaamista vaativissa työtehtävissä. Raportin mukaan osaamisvajeita voi esiintyä niin käytössä olevien järjestelmien kuin uusien järjestelmien kohdalla. Etenkin uusien teknologioiden käyttöönottoprosesseissa sisäisellä tarkastuksella voi olla keskeinen rooli. Se voi osallistua uuden teknologian arviointiprosessin alkuvaiheisiin ja antaa ohjeita sen riskeistä ja valvontavaatimuksista. Sisäinen tarkastus voi toimia työryhmän osana määrittämässä uuden teknologian aiheuttamia lisäriskejä tai joissain tapauksissa riskien pienenemistä. (Flora & Rai 2015.)

Toisaalta uusien teknologioiden ymmärtäminen riittävällä tasolla voi vaatia kehittyneitä IT- taitoja, jotta sisäinen tarkastus voisi edistää prosessien laatua käyttöönoton aikana. Edellä esitetyn mukaisesti osaamisessa voi kuitenkin esiintyä puutteita. Ratkaisuksi tähän Lineros (2021) huomauttaa, että joissakin tapauksissa sisäisen tarkastuksen yksikkö voi kehittää joitain näistä taidoista sisäisesti ja mikäli osastolla ei ole kuitenkaan sisäisiä resursseja riittävään sisäiseen IT-tarkastukseen, ulkopuolisten erikoiskonsulttien käyttö on sallittua.

Floran ja Rain (2015) tapaan myös Lineros (2021) korostaa sisäisen tarkastuksen roolia uusien järjestelmien käyttöönotossa. Hänen mukaansa sisäisen tarkastuksen osallistuminen IT-järjestelmien käyttöönottoon sekä hallintoon voi muodostaa tärkeän osan tehokkaan järjestelmän turvallisuutta, saatavuutta, luotettavuutta ja luottamuksellisuutta (Lineros 2021). Sisäisen tarkastuksen piiriin kuuluu myös arvioida, miten uudet teknologiat sopivat yhteen liiketoiminnallisten tavoitteiden kanssa, sekä mitä lisäriskejä teknologian käyttöön liittyy (COSO 2017; IIA 2016). Sisäisellä tarkastuksella on myös tärkeä rooli IT-hallinnossa (IT-Governance), koska se pystyy arvioimaan koko organisaatioon vaikuttavia organisaatioiden välisiä, kuin myös sisäisiäkin riskejä (Lineros 2021). IT-hallinnon osalta IIA:n standardi 2110.A2 sanoo, että sisäisen tarkastuksen tulisi arvioida, millainen IT-hallinto tukee organisaation tavoitteita. Tiivis osallistuminen IT-hallinnon ohjaamiseen konsultoimalla tai muilla tavoin voi kuitenkin aiheuttaa ongelmia objektiivisen tarkkailun ja varmentamisen näkökulmista. Sisäisen tarkastuksen olisikin kyettävä erottamaan konsultointi- ja varmennuspalveluiden tuottaminen toisistaan niin, ettei objektiivisuus kärsi. Käytännössä tämä tarkoittaa, että samat henkilöt eivät saisi tuottaa ensin konsultointipalveluja ja sen jälkeen varmentaa samoja tehtäviä, vaan näissä rooleissa tulisi toimia eri henkilöiden tai sisäisen tarkastuksen eri osastojen. (COSO 2017; IIA 2016.)

COSO:n (2013) toimintaperiaatteen mukaisesti sisäinen tarkastus on viimeinen sisäinen ”puolustuslinja”, joka edustaa viimeistä mahdollisuutta tunnistaa uuden teknologian mahdollisesti haitalliset vaikutukset. Tämän toimintaperiaatteen mukaan sisäisten tarkastajien on tunnistettava ja arvioitava muutokset, jotka voivat merkittävästi uhata sisäisen valvonnan rakenteita ja aiheuttaa vahinkoa organisaatiolle (COSO 2013). Lisäksi sisäisten tarkastajien tehtä-

vänä on ennakoida kehittyvien teknologioiden vaikutuksia ja tiedottaa niistä säännöllisesti johdolle (Lineros 2021).

2.2.2 Disruptiiviset innovaatiot sisäisessä tarkastuksessa

Disruptiivisen innovaation käsitteen ovat esitelleet ensimmäisen kerran Bower & Christensen (1995). He pohtivat julkaisussaan miksi ja miten eri toimialojen johtavat organisaatiot päätyvät usein tulemaan syrjäytetyiksi toimialan käydessä läpi teknologisia uudistuksia. Julkaisun pääsanoma on, että disruptiiviset innovaatiot ilmestyvät vakiintuneiden toimijoiden näkökulmasta usein yllättäen siksi, että niihin varautumisen ei ole ajateltu olevan kannattavaa organisaation ydinasiakkaiden palvelemista tietyllä hetkellä. Toisin sanoen, organisaatioilla on alttius keskittyä toiminnassaan nykyisten ydinasiakkaiden käyttäytymiseen niin paljon, että ydinasiakkaiden käyttäytymisen muuttumiseen varautuminen uuden (disruptiivisen) innovaation seurauksena jää usein liian vähälle huomiolle. (Bower & Christensen 1995.)

Uusia teknologisia innovaatioita tehdään jatkuvasti, mutta on povattu, että tällä hetkellä käynnissä olisi uusi ”teollinen vallankumous”. Teollisuus 4.0 on Saksassa vuonna 2011 esitelty konsepti tulevaisuuden teollisuudesta, joka hyödyntää uusia internetin mahdollistamia teknologioita (Drath & Horch 2014). Teollisuus 4.0:n on kuvattu pitävän sisällään useiden digitaalisten disruptiota aiheuttavien teknologioiden eksponentiaalista yleistymistä, joiden on arveltu muuttavan perustavanlaatuisesti tuotanto-, johtamis- ja hallintojärjestelmiä. Tämän muutoksen merkittäviksi arvioiduista yhteiskunnallisista vaikutuksista johtuen muun muassa Maailman talousfoorumi on alkanut käyttämään konseptista myös nimitystä ”neljäs teollinen vallankumous”. (Schwab 2016.)

Teollisuus 4.0:n tapauksessa disruptiiviset innovaatiot pohjautuvat digitaalisiin teknologioihin, joiden odotetaan johtavan toimintojen automatisointiin sekä digitaalisen ja fyysisen toimintaympäristön rajoja hämärtävien kyberfyysisten toimintaympäristöjen syntymiseen (Drath & Horch 2014; Schwab 2016). Deloitte (2018) on esittänyt, kuinka organisaatiot ovat käymässä läpi tiedon käsittelyn kolmivaiheista siirtymää kohti teollisuus 4.0 kontekstissa esitettyä toimintojen digitalisoitumista ja automaatiota. Ensimmäinen siirtymä on ollut järjestelmäintegraatio, jonka aikana organisaatiot ovat liittäneet eri järjestelmät toisiinsa sujuvoittaakseen tiedonkulkua. Tämän jälkeen seuraavassa siirtymässä on tapahtunut tiedon analysoinnin kehittyminen, joka on johtanut tilastollisten mallien tunnistamiseen ja tiedon visualisointiin. Tällä hetkellä Deloitte näkee useiden organisaatioiden olevan kolmannessa, automatisoinnin vaiheeksi kutsutussa siirtymässä, jossa toimintoja aletaan suunnittelemaan uusiksi ohjelmistorobotiikan avulla. Tulevaisuudessa odotetaan tapahtuvan siirtyminen jatkuvan integraation menetelmiin, joissa muun muassa koneoppimisen avulla pyritään automatisoimaan virheiden tunnistaminen tiedonsaannin muuttuessa reaaliaikaiseksi. (Deloitte 2018.)

Teollisuus 4.0:n ajatellaan siis koostuvan joukosta disruptiivisia innovaatioita. Nämä innovaatiot voivat muovata perinteisiä toimialoja ja muuttaa työtehtävien luonnetta. Muuttuva teknologia ja maailma asettavat myös sisäiselle tar-

kastukselle tarpeen uudistua ja kehittyä. Toistaiseksi sisäisen tarkastuksen näkökulmasta muun muassa big dataa, tekoälyä, sekä lohkoketjuteknologiaa ja kryptovaroja käsittelevää tutkimuskirjallisuutta on kuitenkin hyvin rajallisesti tarjolla (Roussy & Perron 2018). Samaan aikaan disruptiivisina pidettyjen innovaatioiden hyödyntämisen organisaatioissa ennakoidaan olevan tulevaisuudessa yhä yleisempää, jolloin myös sisäiset tarkastajat kohtaavat näitä työssään yhä useamin.

Sisäisten tarkastajien kansainvälinen yhteistyöjärjestö IIA:n raportissa Christ, Eulerich ja Wood (2019) tuovat esille, kuinka disruptiiviset teknologiainnovaatiot lisäävät usein yritysten kilpailuetua, mutta aiheuttavat mahdollisesti myös tuntemattomia riskejä. Monissa julkaisuissa esitetään (Christ ym. 2019; Lineros 2021; Liu 2020; Popchev, Radeva & Velichkova 2021), että sisäisillä tarkastajilla pitäisi, tai ainakin voisi olla rooli luotettavina neuvonantajina organisaation ottaessa käyttöön uusia teknologioita ja tunnistaessa näiden teknologioiden käyttöön liittyviä riskejä. Toisaalta mahdolliseksi ongelmaksi voi kuitenkin muodostua sisäisten tarkastajien puutteelliset tietotekniset valmiudet kyseessä olevaa uutta teknologiaa kohtaan (Christ ym. 2019; Lineros 2021).

Deloitte (2018) tunnistaa teollisuus 4.0:n sisäisille tarkastajille aiheuttamiin haasteisiin vastaukseksi kolme teemaa, joiden välillä sisäisten tarkastajien tulisi tasapainotella vastatakseen sisäiselle tarkastukselle asetettuihin vaatimuksiin. Nämä teemat ovat: perinteisen varmuuden tarjoaminen, neuvonantajana toimiminen ja tulevaisuuden riskien ennakoiminen sekä niihin valmistautuminen. Christ ym (2019) kuvailevat raportissaan vielä yksityiskohtaisemmin sisäisen tarkastuksen parhaita käytänteitä käsitellä disruptiivisia innovaatioita tarkastustyössä. Nämä käytänteet on luokiteltu haastatteluiden perusteella kuuteen kohtaan, jotka ovat:

1. Sisäisen tarkastuksen tulisi pystyä osallistumaan päätöksentekoon prosessin varhaisessa vaiheessa. Erityisesti uuden innovaation käyttöönottoa pohtiessa tulisi sisäistä tarkastusta käyttää mahdollisten riskien ja uusien valvontamekanismien tunnistamisessa.

2. Sisäisen tarkastuksen ja muun uuden innovaation käyttöönottoon osallistuvan henkilöstön välinen tehokas viestintä. Sisäiset tarkastajat voivat auttaa organisaatioita ”epäonnistumaan nopeasti” tarkoittaen sitä, että innovaation mahdollinen toimimattomuus olisi hyvä havaita mahdollisimman nopeasti.

3. Uusien innovaatioiden käyttöönotossa korostuu vahvan hallintotavan rooli. Asiantuntiahaastatteluiden mukaan organisaatioissa yksittäiset tahot, kuten tiimit ja yksiköt, sortuvat helposti innovoimaan huomioimatta koko organisaation strategiaa.

4. Sisäisen tarkastuksen tulisi osallistua organisaation riskienhallintaan tarkoittaen sitä, että sisäisen tarkastuksen tulisi olla jatkuvasti tietoinen or-

ganisaation ajamista ja pohtimista uusista innovaatioista osatakseen valmistautua niiden käsittelyyn tarkastuksessa.

5. Sisäisen tarkastuksen tulisi pystyä olemaan itsessään innovatiivinen. Sisäisten tarkastajien tulisi toimia riskienhallinnan asiantuntijoina, jotka ovat tietoisia uusista innovaatioista ja pyrkivät tutustumaan niihin ennen kuin itse organisaatio aloittaa kyseisten innovaatioiden kartoittamisen.

6. Kun organisaatio lopulta päätyy uudistumaan ja ottamaan uusia innovaatioita käyttöön, tulisi pitää huolta siitä, että sisäisellä tarkastuksella on riittävät taidot vastata uudistuneen ympäristön asettamiin vaatimuksiin. (Christ ym. 2019.)

Käytännössä disruptiivisten innovaatioiden käyttöönotossa on kyse uuden IT-teknologian käyttöönotosta. Niimpä Christin ym. (2019) korostamat tekijät toistuvat samankaltaisina myös muissa IT-teknologian käyttöönottoprosesseissa. Floran ja Rain (2015) ehdottavat uusien teknologioiden käyttöönotossa sisäisen tarkastuksen tehtäviksi, että sisäisen tarkastuksen tulisi selvittää, onko organisaatiolla jo olemassa tiimi, joka arvioi uusia IT-teknologioita. Onko organisaatiolla prosesseja uusien teknologioiden arvioimiseksi? Miten organisaatio tunnistaa uusien teknologioiden aiheuttamat riskit? Lisäksi pitäisi olla perillä siitä, mitä sellaisia hankkeita organisaatiossa on meneillään, joissa uutta teknologiaa ollaan ottamassa käyttöön. Kun selvitys on tehty, sisäisen tarkastuksen tehtäviksi jää Floran ja Rain mukaan ymmärtää ja pitää silmällä uusia projekteja, joissa uutta teknologiaa voidaan ottaa käyttöön, sekä selvittää uusien teknologioiden riskikohteet. Tärkeässä roolissa on myös vuorovaikutus IT-teknologiatiimin kanssa, jotta sisäisellä tarkastuksella olisi ajantasainen ymmärrys strategiasta ja perusteista uusien teknologioiden käyttöönottamiseksi. (Flora & Rai 2015.)

Ehkä suurimpana erona Floran ja Rain (2015) julkaisussaan listaamiin uuden teknologian käyttöönoton vaiheisiin Christ ym. (2019) painottavat raportissaan, että sisäinen tarkastus voisi ottaa näitä disruptiivisina pidettyjä innovaatioita käyttöön jo ennen tarkastamaansa organisaatiota. Tämä mahdollistaisi sisäisille tarkastajille toimimisen asiantuntijana yrityksen suorittamassa käyttöönottoprosessissa. Heidän mukaansa innovaatioiden käyttöönotto sisäisen tarkastuksen omissa toiminnoissa voisi auttaa myös kehittämään mielikuvaa sisäisistä tarkastajista innovatiivisina asiantuntijoina. Vaikka Christ ym. nostavat raportissaan esiin vahvasti sisäisten tarkastajien kasvavan IT-osaamisen tarpeen, pitävät he kuitenkin tärkeimpinä sisäisten tarkastajien ominaisuuksina disruptiivisten innovaatioiden kannalta uteliaisuutta sekä halua osallistua tutkimaan näitä uusia innovaatioita. (Christ ym. 2019.) Uteliaisuus ja halu oppia voivatkin olla merkittävässä roolissa, sillä lopulta ainakin koettua osaamista voi kartuttaa nopeastikin. Gomaa, Gomaa ja Stampone (2019) ovat nostaneet tutkimuksessaan esiin, että koettu lohkoketjuosaaminen on niin sisäisillä tarkastajilla kuin laskentatoimen ammattilaisilla yleisesti heikkoa. Heidän mukaansa osaa-

mista on kuitenkin mahdollista kehittää yksinkertaisten harjoitteiden avulla nopeasti ja merkittävästi.

2.3 Audit 4.0

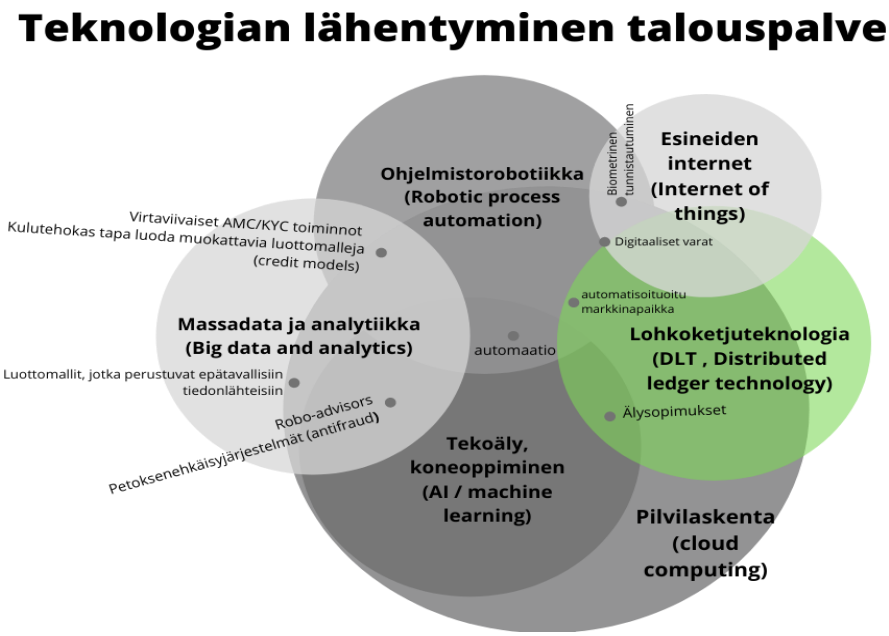
Teollisuus 4.0:n kontekstissa ajateltavan tiedon reaaliaikaisuuden ja luotettavuuden parantumisen odotetaan vaikuttavan myös sisäisen tarkastuksen toimintoihin erityisesti jatkuvan seurannan (continuous auditing) myötä (Burns ym. 2020; Rooney ym. 2017). Vaikka esimerkiksi sisäiset tarkastajat ovat pyrkineet luomaan jatkuvan seurannan ekosysteemejä Christ ym. (2019) mukaan jo vuosikymmeniä, niin kyseisen teeman ajatellaan kuitenkin vaikuttavan disruptiivisesti sisäisen tarkastuksen toimintoihin analysointityökalujen ja teknologian kehittyessä (Christ ym. 2019). Sekä sisäistä että ulkoisen tarkastusta koskien onkin jo esitelty tulevaisuuden konsepti nimeltä Audit 4.0, joka pohjautuu teollisuus 4.0:n kontekstin teknologian mahdollistamiin uusiin tapoihin kehittää organisaatioiden valvontaprosesseja reaaliaikaisiksi. Erityisesti esineiden internetin, kyberfyysisten järjestelmien ja älykkään tuotannon odotetaan mahdollistavan data-analytiikan tehokkaamman käyttämisen visualisointia ja mallintamista hyödyntävillä tavoilla. (Dai & Vasarhelyi 2017.)

Tiedon visualisointiin ja mallintamiseen perustuvaa data-analytiikkaa käytetään sisäisille tarkastajille suunnatun kyselyn perusteella jo nyt suhteellisen laajasti organisaatioiden toiminnoissa, mutta käytön odotetaan yleistyvän myös itse sisäisessä tarkastuksessa tulevaisuudessa (Christ ym. 2019). Dai ja Vasarhelyi (2017) ovat puhuneet tiedon mallintamisen ja erityisesti visualisoinnin yhteydessä ”peilimaailmoista” (mirror worlds), jolla he tarkoittavat fyysisten esineiden ja prosessien mallintamista reaaliajassa päivittyviksi digitaalisiksi kaksosiksi (digital twin). Tämän konseptin idea on se, että digitaalisten kaksosten avulla voitaisiin sekä valvoa reaaliaikaisesti että myös optimoida simulointien avulla fyysisesti tapahtuvia prosesseja. Lisäksi muun muassa Weingärtner (2019) odottaa esineiden internetin yleistymisen johtavan siihen, ettei digitaalisten kaksosten soveltaminen jää vain passiivisen seurannan tasolle, vaan niiden avulla luodaan vuorovaikutteisia yhteyksiä. Näissä yhteyksissä kulkevat komennot voivat vaikuttaa samanaikaisesti sekä digitaaliseen että fyysiseen ulottuvuuteen mahdollistaen uudenlaisia tapoja hyödyntää tekoälyä ja simulointia sekä koneiden keskinäistä kommunikointia (Weingärtner 2019).

Jatkuvan seurannan järjestäminen sekä kyberfyysisten systeemien käyttäminen asettavat uusia vaatimuksia tietoa tuottavien ja käsittelevien järjestelmien tietoturvan ja läpinäkyvyyden suhteen. Lohkoketjuteknologiaa pidetään yhtenä mahdollisena ratkaisuna, jonka uskotaan voivan onnistua vastaamaan teollisuus 4.0:n ja audit 4:0:n konteksteissa miellettyjen sovellusten reaaliaikaisen tiedon tarpeeseen tietoturvaominaisuuksiltaan luotettavana ja läpinäkyvänä teknologiana (Bueno, Morais, Fernandes, Righi & Alberti 2020; Javaid, Haleem,

Pratap Singh, Khan & Suman 2021; Nascimento, Pólvora & Lourenço 2018; Weingärtner 2019). Weingärtner (2019) on myös painottanut, kuinka luottamuksen rooli tulee painottumaan siirryttäessä virtuaalisiin ympäristöihin, joissa asiat eivät ole aina sitä miltä näyttävät. Hän on esittänytkin lohkoketjuteknologian mahdollistamaa tokenisointia keinoksi kasvattaa luottamusta koskien esimerkiksi virtuaalisissa ekosysteemeissä käytettävää identiteettiä, oikeuksia ja asioiden aitoutta. (Weingärtner 2019.)

Edellä esitetyistä seikoista johtuen lohkoketjuteknologian odotetaan myös olevan mahdollisesti tärkeässä asemassa tulevaisuuden taloushallinnossa. Lohkoketjuteknologian mahdollista roolia teknologisena ratkaisuna useissa tulevaisuuden talouspalveluissa on havainnollistettu Singerin (2020) toimesta kuvion 2 mukaisesti.



Kuvio 2: Teknologian lähentyminen talouspalveluissa (Singer 2020).

Kuviosta 2 voidaan havainnoida, kuinka lohkoketjuteknologian uskotaan vaikuttavan esimerkiksi tekoälyn, esineiden internetin ja ohjelmistorobotiikan sovelluksiin. Nascimenton ym. (2018) Euroopan komission yhteiselle tutkimuskeskukselle laaditussa raportissa on esitettykin lohkoketjuteknologian olevan merkittävässä roolissa teollisuus 4.0:n uudessa ekonomiassa koskien muun muassa: datan käsittelyä, kyberturvallisuutta, toimitusketjuja, resurssienhallintaa, Web 3.0:aa ja tuotannon seurantaa.

Myös Burns ym. (2020) ovat ennakoineet lohkoketjuteknologian vaikuttavan tekoälyn, esineiden internetin ja datan analysointia koskeviin tulevaisuuden sovelluksiin myös sisäisen ja ulkoisen tarkastuksen kontekstissa. He ovat esittäneet, kuinka lohkoketjuteknologian mahdollistama jatkuva tarkastus sekä luotettavampi tiedonsaanti voisivat johtaa luotettavampaan sisäisen tarkastuk-

sen ympäristöön, joka voisi lisätä luottamusta ulkoisissa tarkastajissa ja mahdollistaa syvemmän yhteistyön sisäisen ja ulkoisen tarkastuksen välillä. Tästä seurauksena Burns ym. pitävätkin tulevaisuuteen suuntautuvan toiminnan näkökulmasta tärkeänä, että sisäiset tarkastajat oppisivat ymmärtämään paremmin lohkoketjuteknologiaa mahdollisten soveltamiskohteiden löytämiseksi. (Burns ym. 2020.) Sisäisten tarkastajien lohkoketjuteknologian tuntemuksesta voidaan ajatella olevan hyötyä myös mahdollisissa kohtaamisissa nopeasti suosiota kasvattavien kryptovarojen kanssa (Kloch & Little 2019). Lohkoketjuteknologian voidaankin ajatella vaikuttavan sisäisen tarkastuksen tulevaisuuteen mahdollisesti sekä sisäisen tarkastuksen prosesseja itsessään muuttavana teknologiana että synnyttämällä uudenlaisia tarkastuskohteita muun muassa kryptovarojen muodossa.

Seuraavassa luvussa 3. esitellään ensin lohkoketjuteknologian teknologista toimintaa sekä hyödynnettävyyttä erityisesti kirjanpidollisissa, mutta myös muissa tietojen kirjaamista ja tallentamista koskevissa sovelluksissa. Tämän jälkeen luvussa esitellään tokenisointia ja kryptovaroja sekä näiden teemojen ympärille rakentuneiden sovellusten, kuten hajautetun finanssiteknologian (DeFi), ei-lajiesinemäisten tokenien (NFT) ja Salamaverkon (Lightning Network) toimintaa ja mahdollisia riskejä sisäisessä tarkastuksessa arvioitavaksi. Kappaleen lopuksi esitellään vielä, miten lohkoketjuteknologian odotetaan vaikuttavan sisäiseen tarkastukseen.

3. LOHKOKETJUT

3.1 Lohkoketjuteknologia

Lohkoketjuteknologiaa voidaan pitää teknologisena ratkaisuna digitaalisen hajautetun tietokannan tai tilikirjan yläpitämiseksi, mistä johtuen lohkoketjuteknologiaa voidaan joissakin tapauksissa kutsua myös hajautetun tilikirjan teknologiaksi (Distributed Ledger Technology, DLT) (Bashir 2017, 53; Bullmann, Klemm & Pinna. 2019; Mattila, Laikari, Markkanen, Koulu & Jia 2019). Lohkoketjuteknologian toiminta perustuu hajautetun moniversiohallinnan eli konsensuksen mahdollistamiseen tietojärjestelmässä ilman keskusjohtoista toiminnan kontrollointia. Käytännössä tämä tarkoittaa sitä, että toisilleen tuntemattomat tahot voivat tehdä vapaasti muokkauksia järjestelmään yhtä aikaa valvonnan tapahtuessa joukkoistettuna kaikkien järjestelmää käyttävien tahojen toimesta. Mikäli muokkaukset ovat ristiriidassa toisiinsa nähden, niin järjestelmän sääntöjen mukainen muokkaus hyväksytään vallitsevaksi totuudeksi. (Mattila ym. 2019.) Käytännön sovelluksissa lohkoketjuteknologialla on pyritty poistamaan tarve kolmansien osapuolten varmistustoiminnoille välitystä koskevissa sovelluksissa (Grassi, Lanfranchi, Faes & Renga 2022; Zetzsche, Arner & Buckley 2020). Lohkoketjuteknologian hyödyntämistä on kuitenkin alettu tutkia myös muun kaltaisissa hajautettujen tilikirjojen sovelluksissa, joskin tämän tutkimusalan on kuvattu olevan vasta varhaisessa vaiheessa (Cai 2019; Faccia & Petratos 2021; Ibañez, Bayer & Tasca 2021).

Vaikka lohkoketjuteknologiaa koskevaa keskustelua voi leimata usein uusille innovaatioille ominainen ”hype”, niin tästä huolimatta olisi hyvä tiedostaa, että ilmiön taustalla on myös tunnistettuja ongelmia, joita pyritään ratkaisemaan lohkoketjuteknologian avulla. Näitä ovat esimerkiksi aikaa vievät, kalliit ja kuitenkin inhimillisille virheille alttiit tilintarkastusmenettelyt (Cai 2019; Maiti, Kotliarob & Lipatnikov 2021), perinteisten rahoitusjärjestelmien välityspalkkiot ja hitaus (Grassi ym 2022; Schär 2021), varallisuuden kalliista arvottamis-

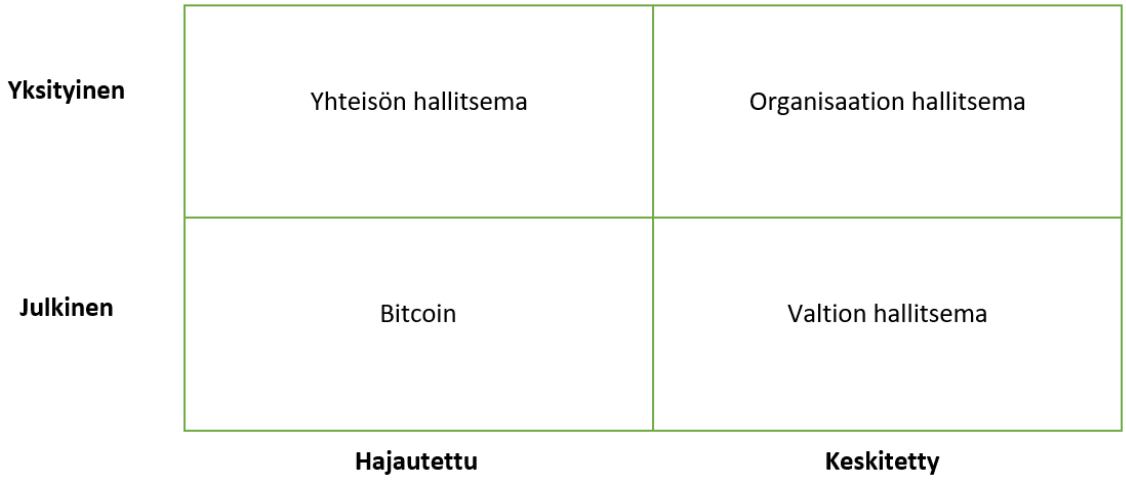
prosesseista johtuva tehottomuus (Popescu 2021), virtuaalisissa ympäristöissä esiintyvä luottamuspula sekä digitaalisten asioiden aitouden ja omistajuuden todentaminen (Weingärtner 2019), älysopimusten käytön teknologinen mahdollistaminen (Bashir 2017; Dutta 2020), mikromaksujen teknologinen mahdollistaminen (Robert, Kubler & Ghatpande 2020), fiat-valuuttojen rahapoliittiset valuviat (Selgin 2015), rahoitusjärjestelmän läpinäkymättömyydestä johtuvat järjestelmäriskit (Ito ym. 2017) sekä sensuroimattomien ja esteettömien pankkipalveluiden mahdollistaminen (Zetzsche ym. 2020).

Esimerkiksi Casey ja Vigna (2018) sekä Ito ym. (2017) ovat verranneet kryptovarojen ja lohkoketjuteknologian viime vuosien kehitystä internetin yleistymiseen 1990-luvulla. Casey ja Vigna (2018) ovat myös todenneet, että koska 1990-luvun internetbuumista muistetaan yleensä vain IT-kuplan puhkeaminen, niin tämän varjoon jää usein buumin mahdollistama resurssien hakeutuminen alalle, joka kuplan puhkeamisesta huolimatta johti merkittäviin innovaatioihin. Lohkoketjuteknologian kehittämisessä nähdäänkin tapahtuvan nyt samankaltaista resurssien hakeutumista alan innovointiprosesseihin, jonka uskotaan myös johtavan pitkäaikaiseen kehitystyöhön (Casey ja Vigna 2018; Ito ym. 2017).

Lohkoketjuteknologian odotetaan yleistyvän merkittävästi tulevien vuosien aikana. Markkinatutkimuksia suorittavan yhtiön Research and Markets (2021) raportin mukaan lohkoketjumarkkinan odotetaan kasvavan 68,4 % keskimääräistä vuosivauhtia 67,4 miljardiin dollariin vuoteen 2026 mennessä. Kasvua ajaviksi voimiksi raportti esittää suuryritysten kiinnostuksen lohkoketjusovellusten hyödyntämiseen koskien: älysopimuksia, toimitusketjujen hallintaa, maksujärjestelmiä, lojaliteetti- ja palkitsemisohjelmia sekä vaatimustenmukaisuutta (compliance). Pk-yritysten kiinnostuksen raportti esittää suuntautuvan manuaalisten ja puoliautomaattisten perustoimintojen, kuten laskutuksen, varastonhallinnan ja palkanlaskennan tehostamiseen, jonka lisäksi lohkoketjuteknologia voi raportin mukaan auttaa alentamaan pk-yrityksien markkinoille tulon korkeita kustannuksia, mikäli kustannukset johtuvat kolmansien osapuolten välitystoiminnasta. (Research and Markets 2021.)

Lohkoketjujärjestelmien hyödyntämät lohkoketjuteknologiat voidaan jakaa julkisiin ja yksityisiin lohkoketjuihin sekä näiden hybrideihin, jonka lisäksi lohkoketjujärjestelmiä voidaan luokitella myös järjestelmähallinnon hajautuneisuuden perusteella (Bashir 2017, 53-54; O'Leary 2017). Julkisilla lohkoketjuilla tarkoitetaan kaikille avointa lohkoketjua, jota ei omista kukaan ja johon kuka tahansa voi liittyä ilman erillistä lupaa. Useita kryptovaluuttajärjestelmiä, kuten Bitcoin-protokollaa voidaan pitää esimerkkinä julkisesta lohkoketjusta. Yksityisen lohkoketjun voidaan puolestaan ajatella olevan vastakohta julkiselle lohkoketjulle, jonka omistaa jokin tietty taho ja johon liittyminen voi olla luvanvaraista. (O'Leary 2017.) Lohkoketjujärjestelmien hajautuneisuudella tarkoitetaan sitä, kuinka hajautetusti tai keskitetysti järjestelmässä suoritettavat oikeudet jakau-

tuvat ja päätöksenteko määräytyy. Yksityiset lohkoketjujärjestelmät ovat tyypillisesti keskitetympiä, kun taas julkiset lohkoketjujärjestelmät hajautetumpia ratkaisuja, joskin esimerkiksi Mattila ym. (2019) ovat todenneet, ettei lohkoketjujärjestelmän hajautuneisuuden määrittämiseen ole vielä olemassa yleispätevää menetelmää. Kuviossa 3 on esitetty O'Learya (2017) mukaillen lohkoketjujärjestelmien erilaiset päätyypit ja esimerkit siitä, millaisissa tilanteissa näitä voitaisiin käyttää.



Kuvio 3: Lohkoketjujärjestelmien päätyypit (O'Leary 2017.)

Kuviosta 3 käy ilmi, millaisia variaatioita lohkoketjujärjestelmät voivat edustaa ottaen huomioon sekä julkisuutta että hajautuneisuutta koskevat ulottuvuudet. Bitcoin sekä monet muut kryptovarat edustavat julkisia ja hajautettuja lohkoketjujärjestelmiä, mutta sekä järjestelmän ylläpitoa keskittämällä että pääsyoikeutta rajoittamalla voidaan pyrkiä luomaan tietyn yhteisön, organisaation tai valtiollisen toimijan tarpeita vastaavia lohkoketjujärjestelmiä. Lisäksi O'Leary (2017) on esittänyt organisaatioiden olevan kasvavissa määrin kiinnostuneita pilvipohjaisten lohkoketjujärjestelmien hyödyntämisestä siinä missä esimerkiksi kryptovarat toimivat usein vertaisverkkoina. Mattila ym. (2019) ovat myös todenneet, että yritysten mahdollisesti suosimat yksityiset lohkoketjujärjestelmät voivat poiketa alkuperäisestä lohkoketjuteknologian toteutuksesta niin paljon, että ne kannattaisi käsitteellistää hajautetuiksi tilikirjoiksi tai DLT-järjestelmiksi lohkoketjujärjestelmien sijaan.

Kuten aiemmin todettua, lohkoketjuteknologiaa koskevan keskustelun on havaittu ajoittain kärsivän ylenpalttisesta teknologian hehkuttamisesta. Lohkoketjuteknologiasta keskusteltaessa tulisi pitää mielessä, että kyseessä on neutraali teknologia, jonka tarkoitus oli alun perin ratkaista Bysanttilaisen kenraalin ongelmana tunnettu peliteoreettinen haaste koskien hajautettujen tietojärjestelmien toimintaa. Lohkoketjuteknologian hyödynnettävyyttä tutkittaessa tulisikin keskittyä tarkastelemaan sitä, missä määrin edellä kuvatun ongelman ratkaisu voisi tuoda lisäarvoa muihin käyttötarkoituksiin. (Coyne ja McMickle 2017.)

3.1.1 Bysanttilaisen kenraalin ongelma

Avoimien hajautettujen tietojärjestelmien toimintaan liittyi ennen lohkoketjuteknologian keksimistä merkittävä haaste koskien haitallisten toimijoiden hyökkäyksiä järjestelmää vastaan (Bashir 2017, 37-39). Bysanttilaisen kenraalin ongelma on Lamport, Shostak & Pease (1982) kehittämä analogia, jolla kuvataan päätöksentekomekanismin toimintaa vikasietoisessa tietokonejärjestelmässä. Bysanttilaisen kenraalin ongelma perustuu kuvitelmaan tilanteesta, jossa joukko armeijan kenraaleja yrittää saavuttaa enemmistön yhteisymmärryksen joko hyökätä tai vetäytyä. Tilannetta kuitenkin vaikeuttaa merkittävästi se, että kenraalit voivat kommunikoida toisilleen vain sanansaattajien välityksellä ja kuka tahansa kenraali voi olla petturi. Tästä johtuen kenraalien on keksittävä tapa muodostaa yhteisymmärrys riippumatta siitä, että kaikkiin osapuoliin ei voi luottaa. (Lamport ym. 1982.)

Bysanttilaisen kenraalin ongelma omaksuttiin yleisesti myös peliteoreettiseksi lähtökohdaksi hajautettujen tietojärjestelmien kehittämiseen (Dutta 2020, 46). Hajautettujen tietojärjestelmien kontekstissa kenraalilla tarkoitetaan noodia ja sanansaattajalla noodien välistä yhteydenpitokanavaa. Tieto siitä, että osa noodeista voi olla haitallisia toimijoita aiheuttaa sen, ettei lähtökohtaisesti yhteenkään noodiin voi luottaa ilman yleistä yhteisymmärryksen synnyttävää mekanismia. Maailman ensimmäisenä kryptovaluuttana pidetyn bitcoinin käyttämä työtodistemekanismi oli ensimmäinen käytännön sovellus, jonka avulla yhteisymmärrys eli konsensus onnistuttiin saavuttamaan avoimessa hajautetussa tietojärjestelmässä. Bitcoinin tapauksessa konsensuksen saavuttaminen mahdollisti ratkaisun kaksinkertaisen kulutuksen ongelmaan (Double-Spending Problem), mikä tarkoitti sitä, ettei valuuttana toimivaa rahaketta voinut kopioida ja käyttää useaan kertaan. (Bashir 2017, 12; Coyne & McMickle 2017.)

Coyne ja McMickle (2017) ovat todenneet konsensusmekanismien ja lohkoketjuteknologian ratkaisevan Bysanttilaisen kenraalin ongelman onnistuneesti kryptovarojen kontekstissa, mutta he ovat kuitenkin suhtautuneet kriittisesti tämän ongelman ratkaisemisen tuottamaan lisäarvoon luonteeltaan keskitetymmissä sekä yksityisemmissä tietojärjestelmissä, kuten organisaatioiden kirjanpitojärjestelmissä. Toisaalta esimerkiksi Cai (2019) on ehdottanut, että lohkoketjuteknologian yhdistäminen kolminkertaisen kirjanpidon konseptiin voisi tuoda huomattavaa lisäarvoa myös kirjanpitojärjestelmiin. Tätä näkökulmaa tarkastellaan luvussa 3.2.

3.1.2 Konsensus-mekanismit

Koska lohkoketjuteknologia perustuu hajautettuun moniversionhallintaan, täytyy järjestelmään osallistuvien tahojen pystyä muodostamaan konsensus koskien tapahtumien sääntöjenmukaisuuden varmistamista sekä varmistettujen tapahtumien järjestystä (Burns ym. 2020). Konsensuksen saavuttamiseksi on kehitetty erilaisia konsensusalgoritmeja, joista yleisimmin käytetyt ovat työto-

distejärjestelmä (Proof-of-Work, PoW) ja varantotodistejärjestelmä (Proof-of-Stake, PoS) (Dutta 2020, 44).

Työtodistejärjestelmä perustuu todistukseen siitä, että lohkoketjujärjestelmää ylläpitävän noodin on täytynyt tehdä resursseja kuluttavaa ”työtä” päästäkseen ehdottamaan uusinta lohkoa lohkoketjuun. Käytännössä työllä tarkoitetaan tietokoneen laskentatehon käyttämistä satunnaislukujen arvaamiseen kilvan muiden noodien kanssa. Tätä toimintaa kutsutaan louhinnaksi. (Antonopoulos 2014.) Varantodistejärjestelmä perustuu työn tekemisen sijaan todistukseen siitä, että uusinta lohkoa ehdottavalla noodilla on tarpeeksi pääomaa sidottuna järjestelmään. Tämän seurauksena noodien insentiivin voidaan rationaalisesti ajatella tukevan järjestelmän sovittua toimintaa. Noodien on täytynyt esimerkiksi tallettaa varoja järjestelmään niin paljon, että teoriassa ajateltuna kaikki noodien yrittämät hyökkäykset järjestelmää kohtaan tuottaisivat hyökkääjälle aina tappion. (Bashir 2017, 29; Dutta 2020, 53–55.)

Kuten edellä esitettiin, sekä työtodistejärjestelmä että varantotodistejärjestelmä pohjautuvat sellaisten insentiivien luomiseen, että järjestelmää ylläpitävät tahot hyötyisivät kaikissa tilanteissa vain järjestelmän toiminnan turvaamisesta. Konsensusalgoritmien perimmäinen idea onkin joukkoistaa kaikki lohkoketjujärjestelmän ylläpitäjät vahtimaan tapahtumien kulkua, minkä voidaan ajatella takaavan korkeammalla todennäköisyydellä tapahtumien oikeellisuuden, verrattuna luonteeltaan keskitetymmin valvottaviin järjestelmiin (Burns ym. 2020). Tästä huolimatta tulisi kuitenkin myös muistaa, että konsensusalgoritmit eivät itsessään takaa lohkoketjujärjestelmän turvallisuutta, sillä konsensuksen muodostuminen on aina pohjimmiltaan sosiaalinen toimenpide (Mattila ym. 2019).

Toimiva konsensusalgoritmi pohjautuukin riittävien sosiaalisten kannustinmekanismien synnyttämiseen. Kryptovarojen kohdalla kannustinmekanismit pohjautuvat työtodistejärjestelmässä louhijoiden tienaamiin uusiin kryptorahakkeisiin ja varantotodistejärjestelmässä talletetuilla kryptorahakkeilla eli ”steikkauksella” (staking) ansaittaviin korkotuloihin (Burns ym. 2020; Dutta 2020). Nämä mallit ovat osoittaneet toimivuutensa kryptovarajärjestelmissä, mutta esimerkiksi yksityisten lohkoketjujärjestelmien kohdalla huonosti suunniteltu konsensusmekanismi voi altistaa järjestelmän ”51 % hyökkäyksenä” tunnetulle riskille, jossa hyökkääjä saa hetkellisen ylivallan järjestelmässä mahdollistaen esimerkiksi vanhojen tapahtumien muuttamisen jälkikäteen (Burns ym 2020). Tästä johtuen käytettävän konsensusalgoritmin toiminnalle ehdotetaan asetettavaksi kontrolleja, joiden testaamisella voidaan varmentaa, että konsensusalgoritmi sopii lohkoketjujärjestelmän käyttötarkoitukseen ja toimii sovitun mukaisesti (Burns ym 2020; Kloch & Little 2019).

3.1.3 Tapahtuman suorittaminen lohkoketjussa

Kuten jo aikaisemmin on tullut todettua, lohkoketjut ovat pohjimmiltaan järjestelmässä suoritettavista tapahtumista tiliä pitäviä tilikirjoja ja tietokantoja, joi-

den todellisuus varmistetaan verkoston jatkuvalla konsensuksella järjestelmän tilasta. Lohkoketjussa suoritettavan tapahtuman vaiheet ovat Bashiria (2017, 49–51) mukaillen:

1. Käyttäjä pyytää tapahtuman suorittamista. Pyyntö toteutetaan yksityisellä avaimella tehtävällä allekirjoituksella.
2. Pyyntö tapahtuman suorittamisesta lähetetään kaikille muille noodeille, jotka vahvistavat tapahtuman ennalta määrättyjen sääntöjen mukaisesti.
3. Tapahtuman vahvistamisen jälkeen tapahtuma katsotaan toteutuneeksi ja se sisällytetään seuraavaksi muodostuvaan lohkoon.
4. Uusi lohko muodostuu ja se lisätään hyväksymisen jälkeen lohkoketjuun.
5. Jokainen kyseisen lohkon jälkeen syntyvä uusi lohko vahvistaa vanhempien lohkojen tapahtumien toteutumisen. Teoreettisesti on ajateltavissa, että transaktio muodostuu sitä lopullisemmaksi, mitä enemmän uusia lohkoja luodaan lohkoketjuun. (Bashir 2017, 49–51.)

3.1.4 Älysopimukset

Internetin ja tietokoneiden yleistyminen sekä kryptografian kehittyminen johtivat 1990-luvun lopulla ajatukseen kolmansien osapuolten tarpeen vähentämisestä sähköisessä kaupankäynnissä. Szabo (1997) esitteli jo tuolloin ajatuksen sopimusehtoja automaattisesti toteuttavasta tietokoneistetusta tapahtumaprotokollasta, jota hän kutsui älysopimukseksi (smart contract). Älysopimusten tarkoituksena oli poistaa inhimillisyyteen liittyviä petosriskejä sekä vähentää transaktioiden toteuttamisesta aiheutuvia kustannuksia mahdollistaen pienet mikromaksut. (Szabo 1997.) Siinä missä Szabon alkuperäinen ajatus älysopimuksista jäi lopulta konseptin tasolle, niin lohkoketjuteknologian kehittymisen jälkeen havaittiin nopeasti, että lohkoketjupohjaiset alustat tarjoavat hyvän lähtökohdan ohjelmoitaville älysopimuksille.

Käsitteellisesti älysopimusten on esitetty olevan toimintasäännöistä koostuvia autonomisesti toimivia komponentteja, jotka suorittavat ehtojen täyttyessä sovitun tapahtuman automaattisesti (Coyne & McMickle 2017; Grassi ym. 2022; Schär 2021). Älysopimusten toiminnan on kuvailtukin sisältävän turvallisuuden ja pysäyttämättömyyden elementtejä (Bashir 2017, 46–48). Konkreettisesti älysopimukset ovat omia autonomisia osoitteita lohkoketjujärjestelmissä, joihin voidaan tallettaa järjestelmässä liikuteltavia varallisuuseriä, ja jotka jakavat nämä erät uudelleen tiettyjen ehtojen täyttyessä, ehtojen määräämällä tavalla. Tyypillisesti, mikäli ehdot jäävät täyttymättä, on älysopimus ohjelmoitu palauttamaan varat takaisin tallettajille tietyn ajan kuluttua. (Dutta 2020, 62; Schär 2021). Älysopimukset koostuvat pohjimmiltaan ”jos/kun-niin”-säännöstöstä, joita voidaan hyödyntää tehokkaasti, mikäli ennakkoehtojen täyttyminen kyetään määrittämään (Dutta 2020, 62–63). Tällä tarkoitetaan sitä, että sopimusehtojen täyttymistä täytyy pystyä valvomaan luotettavalla tavalla, etteivät osa-

puolet voi lähettää vääriä signaaleja ehtojen täyttymisestä (Dutta 2020; Weingärtner 2019).

Älysopimusten käyttöön liittyy näkemyseroja sen suhteen, kuinka automaattisia älysopimusten tulisi olla. Osa tutkijoista on sitä mieltä, että täysin automaattisesti toimivan älysopimuksen sijaan niiden olisi parempi olla vain automatisoitavissa olevia, mutta manuaalisen syötön mahdollistavia kokonaisuuksia, kun taas osan mielestä manuaalisen syötön mahdollisuus pilaa koko älysopimuksen toimintaidean. Tietynlaista kompromissia näihin näkökulmiin voidaan yrittää hakea käyttämällä oraakkeleita, joiden avulla voidaan hakea tietoja ulkoisten palveluntarjoajien syötteistä tai esimerkiksi esineiden internettiin kytketyistä laitteista. (Bashir 2017, 231–233.) Ongelmaksi voi kuitenkin tässäkin tapauksessa syntyä luottamus tietoa tarjoavaa tahoa kohtaan, jonka lisäksi yksittäinen tiedontarjoaja, kuten esimerkiksi tietty laite, voi olla altis manipuloinnille (Weingärtner 2019). Näiden huolien tunnistaminen onkin johtanut hajautettujen oraakkelien (decentralised oracles) ja näihin pohjautuvien oraakkelijärjestelmien kehittymiseen, joiden avulla pyritään varmistamaan ulkoisen tiedon aitous käyttämällä hyödyksi useita tietolähteitä ja muodostamalla konsensus kaikesta saatavilla olevasta tiedosta (Bashir 2017, 231-233; Schär 2021; Weingärtner 2019).

Hajautettujen oraakkelijärjestelmien tarkoitus on toimia luotettavan tiedon tarjoajana, jota muiden lohkoketjujen älysopimuksia käyttävät sovellukset voivat hyödyntää. Hajautettu oraakkelijärjestelmä voidaan ohjelmoida hakemaan ja yhdistelemään tietoa useista ulkoisista tietolähteistä sekä mahdollisimman luotettavina pidetyistä järjestelmistä, kuten vaikkapa tietyn organisaation omasta yksityisestä lohkoketjujärjestelmästä ja luomaan näistä tiedoista konsensus (Bashir 2017 231-233; Weingärtner 2019). Oraakkelien ja älysopimusten käyttöä voitaisiin mahdollisesti hyödyntää tulevaisuudessa myös sisäisen tarkastuksen ja valvonnan toimenpiteissä erityisesti eri lohkoketjujärjestelmät ylittävien transaktioiden seurannassa. Toistaiseksi teknologia on kuitenkin niin kehitysvaiheessa, että lohkoketjujärjestelmien toimintaa tulisi lähtökohtaisesti lähestyä valvonnan ja järjestelmätarkastuksen perinteisesti hyväksi havaittujen keinojen näkökulmasta käsin (Dutta 2020, 263).

Älysopimukset siis mahdollistavat lohkoketjujen ja kryptovarojen ohjelmoitavuuden, minkä avulla voidaan toteuttaa hajautetusti monia sellaisia toimintoja, jotka ovat ennen vaatineet toimiakseen jonkun keskitetyn tahon aktiivista toimintojen hallinnointia. Älysopimusten mielikuvituksellinen hyödyntäminen onkin johtanut hajautettujen applikaatioiden (decentralized apps, dapps) ja hajautettujen autonomisten organisaatioiden (decentralized autonomous organization, DAO) kehittymiseen, jotka ovat muodostaneet esimerkiksi anonyymien käyttäjien jatkuvan demokraattisen äänestyksen perusteella ohjautuvia applikaatioita ja virtuaalisia organisaatioita. (Bashir 2017, 234–235.)

3.2 Lohkoketjuteknologian integroituminen tietojärjestelmiin

Lohkoketjujen voidaan ajatella olevan yksinkertaisuudessaan sähköistä kirjanpitoa, jossa valvonta tapahtuu reaaliaikaisesti kaikkien järjestelmää käyttävien tahojen toimesta. Lohkoketjuteknologian soveltamista onkin alettu tutkimaan varsinkin sellaisissa tietojärjestelmissä, joihin kuuluu oleellisena osana tapahtumien seurantaa tai kirjanpitoa. Myös lohkoketjupohjaisten älysopimusten hyödyntäminen perinteisten tietojärjestelmien automatisoimisessa on herättänyt laajalti keskustelua. (Cai 2019; Coyne & McMickle 2017; Mattila ym. 2019.) Frizzo-Barker ym. (2020) systemaattisen kirjallisuuskatsauksen perusteella lohkoketjuteknologiaa koskevasta tutkimus keskittyy tällä hetkellä erityisesti finanssialan sovelluksiin (31% tutkimuksista), mutta lakia ja hallintoa (Law & Governance) (22% tutkimuksista) sekä kirjanpitoa (Accounting & Record-keeping) (9% tutkimuksista) koskevat teemat näyttäytyvät myös merkittävinä aiheina lohkoketjuteknologiaa koskevissa julkaisuissa (Frizzo-Barker ym. 2020). Lohkoketjuteknologiasta ovat kiinnostuneet myös kaikki ”Big four”-tilintarkastusyhtiöt, jotka ovat investoineet lohkoketjuteknologian hyödyntämiseen taloushallinnon tietojärjestelmissä (Alles & Gray 2020). Burns ym. (2020) ovat esittäneet lohkoketjuteknologian laajemman yleistymisen organisaatioiden käyttämissä tietojärjestelmissä vaikuttavan merkittävästi sisäisen valvonnan järjestämiseen sekä sisäiseen tarkastukseen. Saman suuntaisia ajatuksia ovat esittäneet myös Kloch & Little (2019) todeten lohkoketjuteknologian vaikuttavan tulevaisuudessa sisäisen tarkastuksen asemaan riskienhallinnan kolmantena puolustuslinjana.

Lohkoketjuteknologian on uskottu disruptoivan perinteisiä keskitetysti hallinnoituja taloushallinnon tietojärjestelmiä, minkä on ajateltu uhkaavaan vakiintuneita alan ohjelmistoyhtiöitä. Ohjelmistovalmistaja SAP:in lohkoketjuasiantuntija onkin todennut lohkoketjuteknologian olevan aidosti potentiaalinen uhka monille ohjelmistovalmistajille uskoen kuitenkin, että lohkoketjujen yleistymisestä huolimatta kysyntää tulee olemaan ohjelmistovalmistajien tapauskohtaisia järjestelyjä koskevalle ammattiosaamiselle myös tulevaisuudessa. (Morris 2018.) SAP:in lisäksi myös monet muut tunnetut yritysohjelmistojen valmistavat, kuten Oracle, Microsoft ja IBM ovatkin jo kehittäneet omia pilvipohjaisia BaaS (Blockchain as a Service) -lohkoketjualustoja, joissa heidän asiakkaansa voivat kokeilla lohkoketjuteknologian käyttöä ilman tarvetta suurille investoinneille (Mattila ym. 2019).

Myös suomalaisissa organisaatioissa tiedetään olevan käynnissä useampia sekä julkisen että yksityisen sektorin kokeiluja lohkoketjuteknologian integroimisesta osaksi liiketoimintaa. Esimerkiksi Arla (2018) ja S-ryhmä (2018) ovat molemmat käynnistäneet pilottihankkeet lohkoketjuteknologian hyödyntämisestä toimitusketjuissa. Toimitusketjujen lisäksi lohkoketjuteknologiaa on pyritty hyödyntämään markkinapaikkojen rakentamiseen. Nokia (2021) on avannut lohkoketjupohjaisen markkinapaikan datakaupalle ja Asiakastieto, Nordea, OP

ryhmä, Privanet ja Tieto (2018) ovat yhdessä kehittäneet lohkoketjupohjaista listaamattomien osakkeiden markkinapaikkaa. Myöskin julkisella sektorilla esimerkiksi Kela (2019) on kehittänyt digitaalisena maksusitoumuksena toimivaa lohkoketjupohjaista ”älyrahaketta”.

3.2.1 Lohkoketjujärjestelmissä käsiteltävät varallisuuserät

Lohkoketjuteknologian mahdollisia käyttötarkoituksia pohdittaessa tulisi pystyä ymmärtämään, minkälaisiin ongelmiin lohkoketjuteknologia voisi mahdollisesti tarjota ratkaisuja. Toisaalta myöskään kryptovaroja koskevia osaamisvaateita ei pidä unohtaa. Lohkoketjujärjestelmätyyppien sekä järjestelmissä esiintyvien varallisuuserien tuntemista voidaan pitää tärkeänä seikkana lohkoketjuteknologian soveltuvuuden arvioimisessa, sekä kohdatessa näissä esiintyviä varoja. Sen lisäksi, että lohkoketjujärjestelmät voivat itsessään poiketa toisistaan luvussa ollen enimmissä määrin joko yksityisiä tai julkisia sekä hajautettuja tai keskitettyjä, niin myös lohkoketjujärjestelmässä esiintyviä varallisuuseriä voidaan luokitella eri omaisuuksien perusteella.

Lohkoketjujärjestelmissä esiintyvät varallisuuserät voidaan jakaa yleisellä tasolla Allesin & Grayn (2020) mukaan natiivisti digitaalisiin varoihin ja digitaalisiin kaksosiin (digital twin) sillä perusteella, kuinka varallisuuserä tai esitys varallisuuserästä on muodostunut lohkoketjujärjestelmään. Käytännössä saman suuntaisen jaon ovat tehneet myös Ibañez ym. (2021) sekä Faccia ja Petratos (2021) esittäen, että lohkoketjujärjestelmissä esiintyvät varallisuuserät ovat joko natiivisti digitaalisia kryptovaroja tai fyysisten varojen digitaalisia ilmentymiä kuvaavia tokeneita. Pohjimmiltaan jako perustuu ajatukseen siitä, sisältääkö lohkoketjujärjestelmä tapahtumien kirjanpidon lisäksi myös varsinaisen arvonsiirtotapahtuman. Natiivi digitaalisten kryptovarojen tapauksessa arvo siirtyy tosiasiallisesti lohkoketjujärjestelmän sisällä, kun taas tokenien tapauksessa lohkoketjujärjestelmä toimii enemmänkin kirjanpidollisena välineenä (Faccia & Petratos 2021).

3.2.2 Tokenisointi

Tokenisoinnilla (tokenization) tai poletisoinnilla tarkoitetaan lohkoketjujen yhteydessä varallisuuserän omistusoikeuden siirtämistä lohkoketjujärjestelmään siten, että lohkoketjujärjestelmässä käsiteltävä tokeni edustaa omistusoikeutta tähän varallisuuserään (Dutta 2020, 79; Schär 2021). Osin vastaavasta finanssialan toimenpiteestä käytetään termiä arvopaperistaminen (securitization) (Dutta 2020, 102).

Monien vaikeasti siirreltävien tai jaettavien omaisuusluokkien, kuten esimerkiksi arvometallien kauppaa on perinteisesti päädytty käymään omistusoikeutta koskevilla asiakirjoilla, jotka ovat voineet oikeuttaa omistuksen joko koko kohde-etuuteen tai sen osaan. Kohde-etuuksia koskevat asiakirjat on todentanut ja myöntänyt yleensä jokin kolmantena osapuolena toimiva keskitetty

taho, kuten valtion virasto tai kaupallinen välittäjä. Digitalisoitumisen myötä nämä asiakirjat ovat alkaneet muuttua enenevissä määrin sähköisessä muodossa oleviksi omistusoikeuksiksi nopeuttaen sekä helpottaen osto- ja myyntiprosesseja. (Dutta 2020.)

Vaikka perinteiset asiakirjat ovatkin digitalisoituneet, niin kaupantekoprosessissa voidaan edelleen tarvita kolmatta osapuolta varmistamaan kauppojen toteutuminen sekä kauppakirjojen aitous, mikä voi hidastaa kaupantekoprosessia. Tokenisoinnin ajatellaan poistavan kokonaan tämän tarpeen jokaisen kaupan todentamisesta kolmannelta osapuolelta, koska osapuolet voivat luottaa omistusoikeuden edustavan aitoa kohde-etuutta, mikäli se on edustanut tätä aikaisemmissakin lohkoketjussa suoritetuissa transaktioissa. Kun kolmatta osapuolta ei tarvita varmistamaan transaktioita, niin kohde-etuudella on mahdollista käydä kauppaa milloin tahansa ja ilman varmistuksesta aiheutuvia välityspalkkioita. (Dutta 2020, 80–81.) Tokenisoinnin ajatellaankin tehostavan hinnanmuodostusta lisäämällä kaupankäynnin mahdollisuuksia ja vähentäen näin ollen arvonmääritysprosessien kustannuksia. Esimerkiksi finanssialan toimijoilla on jo olemassa useita keinoja arvostaa omaisuutta, mutta prosesseihin käytettävät ulkopuoliset tilintarkastajat ja luottoluokittajat voivat nostaa arvonmääritysprosessin kustannuksia tehden jatkuvasta käypään arvoon arvostamisesta taloudellisesti kannattamatonta. (Popescu 2021.)

Tokenisoinnin kautta on syntynyt uusia innovatiivisia sovelluksia, joissa tokenisointia on alettu hyödyntämään esimerkiksi kiinteistöjen, taiteen, arvometallien ja osakkeiden omistusoikeuksien kaupankäynnissä (Alles & Gray 2020; Dutta 2020). Lisäksi tokenisoinnin myötä on kehittynyt uudenlaisia tapoja monetisoida esimerkiksi digitaalista sisällöntuotantoa. Tokenisointia hyödyntävistä sovelluksista suosiota ovat erityisesti kasvattaneet luvussa 3.4 esitellyt NFT-teokset sekä luvussa 3.5.5 käsitellyt DeFi-sovellukset. Weingärtnerin (2019) mukaan myös esineiden internetin yleistymisen uskotaan lisäävän uusia käyttötarkoituksia tokenisoinnille. Erityisesti sellaiset digitaaliset kaksoset, jotka voivat toimia kahdensuuntaisessa vuorovaikutuksessa fyysiseen edustamaansa asiaan nähden, voivat tarvita tokenisointia varmistamaan asioiden omistajuuden sekä fyysisessä että digitaalisessa ympäristössä jo pelkästään turvallisuussyistä (Weingärtner 2019).

Tokenisointi voi olla helppo tapa järjestää vaikkapa kaupankäynti periaatteessa mistä tahansa kohteesta, mutta tokenisointia voi myös varjostaa monet arvopaperistamiselle tutut riskit. Esimerkiksi Dutta (2020, 102) on todennut, että tällä hetkellä suosiota kasvattavalla tokenisoinnilla ja vuoden 2008 finanssikriisiin johtaneella monimutkaisella arvopaperistamisella on havaittavissa joitakin yhtäläisyyksiä (Dutta 2020, 102). Lisäksi tokenien edustamien kohde-etuuksiin laatuun ja edustettavuuteen voi liittyä riskejä, jotka voivat aiheutua tokenisointiprosessissa. Alles ja Gray (2020) kuvaavat tätä tokenisointiprosessissa esiintyvää laatuongelmaa ”ensimmäisen mailin ongelmaksi”.

3.2.3 Lohkoketjupohjainen kolminkertainen kirjanpito

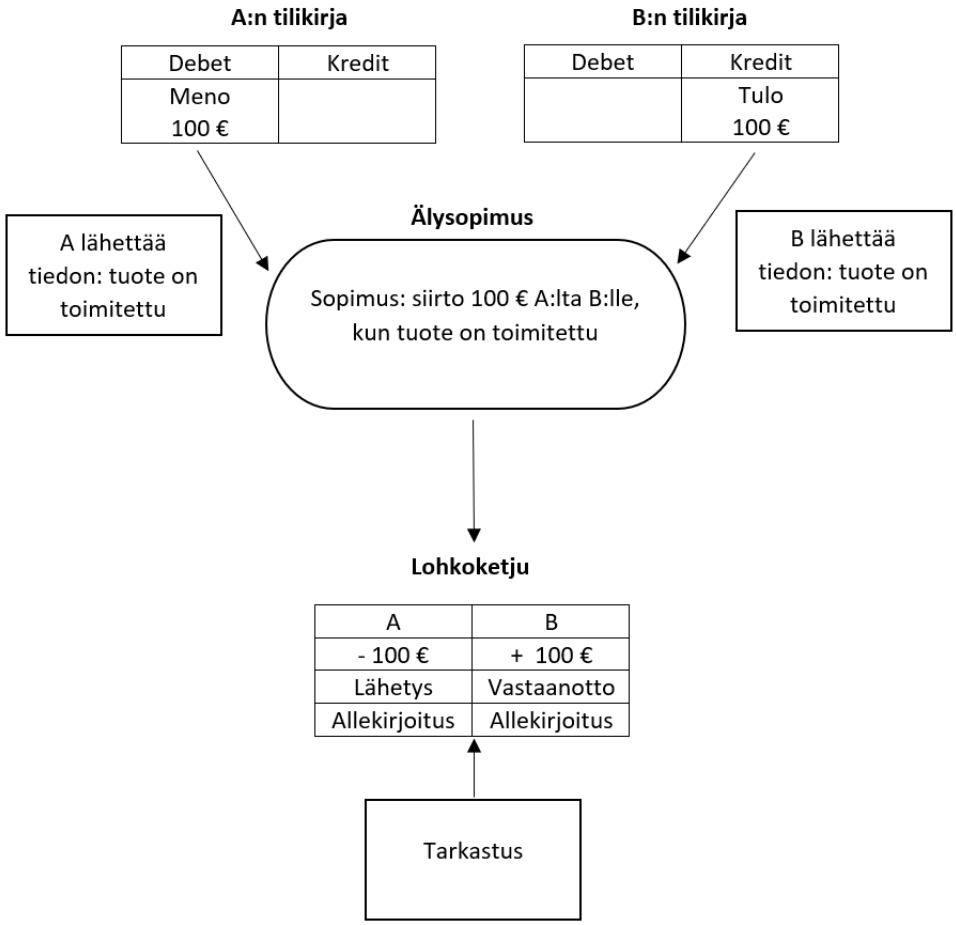
Nykyisillä organisaatioiden käyttämillä kirjanpitojärjestelmillä on pitkät juuret kirjanpidon historiallisessa kehittymisessä, jonka pyrkimyksenä on ajansaatossa ollut tarjota yhteiskunnille mahdollisuus muodostaa luottamus koskien omistussuhteita ja velkoja. Kirjanpito onkin kehittynyt alkukantaisesta yhdenkertaisesta kirjanpidosta nykyään käytettävään kahdenkertaiseen kirjanpitoon luottamuksen parantamiseksi eri sidosryhmien välillä. Kirjanpitoon käytettävät teknologiat ovat jatkaneet kehittymistään erityisesti tietokoneiden kehittymisen myötä, joita kirjanpitäjät ovatkin olleet hyödyntämässä heti ensimmäisten joukossa. (Smith 2021.)

Casey ja Vigna (2018) uskovat lohkoketjuteknologian olevan mahdollisesti yhtä mullistavalla tavalla luottamusta kasvattava keksintö, kuin kahdenkertaisen kirjanpidon kehittyminen, joka heidän mukaansa nosti luottamuksen pankkiireita ja maksunvälittäjiä kohtaan mahdollistaen puitteet kapitalismin nousulle. He kuitenkin näkevät kahdenkertaisessa kirjanpidossa olevan luottamusta heikentäviä ja kustannuksia aiheuttavia valuvikoja, joita lohkoketjuteknologia voisi mahdollisesti pystyä vähentämään poistamalla ainakin osittain tarpeen ulkopuolisille ja keskitetyille luottamuksen takaajilta. (Casey & Vigna 2018.)

Lohkoketjuteknologian yhteydessä onkin alettu puhumaan Griggin (2005) esittämästä kolminkertaisen kirjanpidon konseptista, joka perustuisi kryptografisesti suojattujen kuittien ja organisaation oman sisäisen virtuaalivaluutan hyödyntämiseen kirjanpidossa. Griggin mukaan organisaation ei pitäisi olla ainoa tapahtumista kirjaa pitävä taho, vaan kirjanpidosta tulisi tehdä julkisempaa agenttiongelmien torjumiseksi. Kryptografisen kuitin ja organisaation sisäisen virtuaalivaluutan avulla olisi hänen mukaansa mahdollista saavuttaa sellainen läpinäkyvyys ja tapahtumien muuttumattomuus, että esimerkiksi Enronin tapaisia kirjanpitoa ja tilintarkastusta koskevia skandaaleja ei pääsisi tapahtumaan. Kyseisessä konseptissa kahdenkertaisen kirjanpidon lisäksi tapahtumien kryptografisesti suojatut kuitit ehdotettiin tallennettaviksi kolmanteen, tapahtumien osapuolten välillä yhteisesti jaettuun, tilikirjaan. Kryptografisesti suojattujen kuittien muuttumattomuus ja yhteisesti jaetun tilikirjan tarkoitus olisi taata se, etteivät osapuolet pystyisi tekemään todellisuudesta poikkeavia kirjauksia omiin kirjanpitoihinsa tai muuttamaan näitä kirjauksia jälkikäteen. (Grigg 2005.)

Griggin (2005) esittämä konsepti tarjosi uuden lähestymistavan kirjanpitoon, mutta se jätti käytännön tasolla avoimia kysymyksiä koskien sitä, kuka lopulta vastaisi tästä kolmannesta tilikirjasta. Cai (2019) on ehdottanut hajautetusti ylläpidettävän lohkoketjujärjestelmän sopivan työkaluksi tämän kolmannen tilikirjan toteuttamiseksi. (Cai 2019.) Lohkoketjupohjaisessa kolminkertaisessa kirjanpidossa kahdenkertaisen kirjanpidon debet- ja kredit-puolten kirjausten lisäksi kirjaukset yhdistyisivät siis myös niin kutsutun ”trebit”-puolen eli lohkoketjuun tallentuvien kirjausten avulla (Cai 2019; Maiti ym. 2021). Tämän uskotaan voivan lisätä läpinäkyvyyttä, tiedon eheyttä sekä lohkoketjun mahdollistaman tiedon reaaliaikaisuuden ansiosta parempia mahdollisuuksia esimerkiksi jatkuvan seurannan järjestämiseen (Centobelli, Cerchione, Del Vec-

chio, Oropallo & Secundo 2021; Faccia & Petratos 2021). Lisäksi lohkoketjujen ohjelmoitavuus älysopimusten avulla voi tuoda uusia mahdollisuuksia tehokkaampien kontrollien asettamiseen eri tietojärjestelmiin (Cai 2019; Centobelli ym. 2021; Faccia & Petratos 2021). Kuviossa 4 esitetään Cain (2019) alkuperäisiä kuvioita mukaileva esimerkki älysopimusta hyödyntävästä lohkoketjupohjaisesta kolminkertaisesta kirjanpidosta.



Kuvio 4: Kolminkertaisen kirjanpidon järjestelmä (Cai 2019)

Cain (2019) mukaan lohkoketjupohjainen kolminkertainen kirjanpito voisi vähentää merkittävästi sisäisiä petoksia ja parantaa kirjanpidon tehokkuuden myötä myös organisaation operatiivista tehokkuutta. Laskentatoimen asiantuntijoiden ja lohkoketjusovellusten kehittäjien välinen kuilu on kuitenkin aiheuttanut hänen mukaansa sen, etteivät laskentatoimen asiantuntijat täysin ymmärrä lohkoketjuteknologian potentiaalia esimerkiksi kirjanpidossa. Toisaalta lohkoketjusovellusten kehittäjät tarvitsisivat laskentatoimen asiantuntijoiden tukea sopivien ratkaisujen kehittämiseksi. (Cai 2019.)

Lohkoketjuteknologian hyödyntämistä onkin alettu tutkimaan toiminnanohjausjärjestelmissä (Enterprice Resource Planning, ERP) ja laskentatoimen tietojärjestelmissä (Accounting Information System, AIS). Sarwar ym. (2021) ovat tutkineet lohkoketjuteknologian yhdistämistä perinteisiin tietokantoihin. Tä-

män avulla voitaisiin ratkaista julkisten lohkoketjujärjestelmien skaalautuvuutta koskevia ongelmia. Heidän mukaansa monista julkisista lohkoketjujärjestelmistä poiketen, organisaatioiden lohkoketjujärjestelmät eivät tarvitsisi tuhansia noodeja varmistamaan kaikkia toimintoja. (Sarwar ym. 2021.) Myös O'Leary (2017) on esittänyt, että lohkoketjuteknologian ja perinteisten tietokantojen pilvipohjaiset hybridiratkaisut voisivat lisätä sekä läpinäkyvyyttä että turvallisuutta olematta kuitenkaan organisaation näkökulmasta liian raskaita käytettäviksi (O'Leary 2017). Faccia ja Petratos (2021) näkevät lohkoketjuteknologian soveltuvan mahdollisesti suoraan organisaatioiden perinteisiin ERP- ja AIS-järjestelmiin integroitavaksi, minkä lisäksi he ovat nostaneet esille tärkeän näkökulman lohkoketjupohjaisten sovellusten, kuten DeFi:n, laajenemisesta osaksi yhä useampien organisaatioiden liiketoimintaa. Tämä laajeneminen voisi heidän mukaansa tuoda järjestelmäintegraatiota koskevia hyötyjä lohkoketjuteknologian hyödyntämiseen laajemmin myös organisaation muissa tietojärjestelmissä. (Faccia & Petratos 2021.)

3.2.4 Lohkoketjuteknologian hyödyntämistä koskeva kritiikki

Uusille teknologioille tyypilliseen tapaan myös lohkoketjuteknologian ominaisuuksia voidaan herkästi liioitella sekä esittää ratkaisuksi sellaisiin ongelmiin, joihin kyseinen teknologia ei varsinaisesti tuo ratkaisua. Kryptovaluutta Ethereumin perustajiin lukeutuva Vitalik Buterin on kuvannut lohkoketjujärjestelmien kärsivän trilemmasta (blockchain trilemma) hajautettavuuden, turvallisuuden ja skaalautuvuuden välillä, sillä vain kahta näistä elementeistä on mahdollista priorisoida samanaikaisesti. Käytännössä lohkoketjujärjestelmän laaja hajautettavuus ja turvallisuus tukevat usein toisiaan, mutta laaja hajautus asettaa samalla rajoitteita järjestelmän nopeudelle eli skaalautuvuudelle. Monet julkiset lohkoketjujärjestelmät ovatkin päätyneet priorisoimaan hajautettavuutta ja turvallisuutta varsinaisessa lohkoketjujärjestelmässä, minkä lisäksi skaalautuvuutta on pyritty parantamaan niin sanottujen toisen kerroksen (layer 2) ratkaisujen, kuten myöhemmin luvussa 3.5.2.2 esiteltävän Salamaverkon avulla. (Swyftx Learn 2022.)

Lohkoketjujen trilemmaan pohjautuvan ongelman turvallisuuden ja hajautettavuuden välillä ovat havainneet myös muun muassa Coyne ja McMickle (2017) tutkiessaan lohkoketjuteknologian hyödynnettävyyttä perinteisissä tietojärjestelmissä, kuten ERP- ja AIS-järjestelmissä. He ovatkin arvioineet, ettei lohkoketjuteknologian ratkaisu Bysanttilaisen kenraalin ongelmaan tuo itsessään lisäarvoa näihin järjestelmiin kolmesta syystä, joita ovat:

1. *Luottamuksellisuus*. Organisaatiot haluavat salata yksityiskohtaisia tietoja, minkä vuoksi ne eivät halua käyttää julkisia lohkoketjuja. Yksityisten lohkoketjujen avulla tiedot voidaan kyllä salata ulkopuolisilta tahoilta, mutta tämä taas johtaa seuraavassa kohdassa esitettyyn ongelmaan.

2. *51 % hyökkäys.* Organisaatiolla voi olla kyky manipuloida yksityisiä luvanvaraisia lohkoketjuja takautuvasti, jolloin tämän tyyppiset lohkoket-

jujärjestelmät eivät tosiasiallisesti takaa tietojen eheyttä ja muuttumattomuutta.

3. *Rajoitettu tapahtumien varmentaminen.* Lohkoketjuteknologia kehitettiin alun alkaen varsinaista varojen siirtoa varten, eikä varojen siirron kirjanpitoa varten. Lohkoketjun ensisijainen tehtävä on estää kahdenkertainen kulutus, mutta tämä toiminto ei ole riittävä varmennusmekanismi kirjanpidollisesti. Lohkoketju ei itsessään estä esimerkiksi varojen väärinkäytöksiä, virheellistä mittausta tai kelvollisien tapahtumien määrittämistä muusta kuin kahdenkertaisen kulutuksen näkökulmasta. (Coyne & McMickle 2017.)

Coynen ja McMicklen (2017) kuvaamat seikat hahmottavat lohkoketjujen hyödyntämisen paradoksaalisuutta koskien lohkoketjujen läpinäkyvyyttä. Läpinäkyvyys voi joukkoistaa tapahtumien jatkuvan seurannan järjestelmää käyttävän yhteisön avulla, mutta organisaatioiden näkökulmasta liian suuri läpinäkyvyys ei kuitenkaan ole toivottavaa. He pitävätkin lohkoketjuteknologiaa hyödyllisenä natiivisti digitaalisten kryptovarojen sekä älysopimusten osalta, joissa kirjanpidon lisäksi myös varsinainen arvon siirto tapahtuu lohkoketjussa. Pelkässä kirjanpidossa he eivät kuitenkaan näe lohkoketjuteknologian tuovan lisäarvoa keskitettyjä tietokantoja hyödyntäviin perinteisiin järjestelmiin nähden. (Coyne & McMickle 2017.) Cai (2019) on kuitenkin esittänyt, että Coynen ja McMicklen (2017) huomiot rajoittuvat lohkoketjuteknologian tarkasteluun kahdenkertaisen kirjanpidon kontekstissa, jonka lisäksi hänen mukaansa Coynen ja McMicklen väittämät ovat osin vanhentuneita lohkoketjupohjaisten sovellusten kehittymisen myötä. Cai uskoo yksityisten luvanvaraisten lohkoketjujen sopivan kirjanpitojärjestelmien teknologiseksi ratkaisuksi siirryttäessä kolminkertaiseen kirjanpidon kontekstiin, minkä avulla Coynen ja McMicklen esittämät ongelmakohdat 2 ja 3 voitaisiin ratkaista. (Cai 2019.)

Edellä esitettyjen ongelmakohtien ja kritiikin lisäksi lohkoketjuteknologian toiminnan luonteeseen voi liittyä joitakin harhaluuloja koskien tapahtumien muuttumattomuutta ja pysyvyyttä, mikäli ei ymmärretä, että konsensuksen määräytyminen lohkoketjujärjestelmässä on pohjimmiltaan sosiaalinen eikä teknologinen tapahtuma. Esimerkiksi Mattila ym. (2019) ovat haastaneet käsityksen lohkoketjuteknologian lupaamasta tietojen muuttumattomuudesta vedoten siihen, että muuttumattomuus perustuu konsensuksen ylläpitoon järjestelmässä noudatettavista säännöistä, mikä taas perustuu sosiaaliseen yhteisymmärrykseen. Mikään ei kuitenkaan suoranaisesti estä järjestelmän käyttäjiä esimerkiksi muuttamasta noudatettavia sääntöjä. Vaikka riski konsensuspohjaisesta yllättävästä sääntöjen muuttamisesta mielletäänkin yleensä keskitetympien ja yksityisten lohkoketjujärjestelmien ongelmaksi, niin myös hajautetuissa ja julkisissa lohkoketjujärjestelmissä näin on tapahtunut. (Mattila ym. 2019.) Yhtenä tunnetuimpana esimerkkinä voitaneen pitää kryptovaluutta Ethereumin käyttäjien konsensuspohjaista päätöstä palauttaa hakkerin anastamat varat takaisin hakkeroinnin uhriksi joutuneille sijoittajille (Castillo 2016; Mattila ym. 2019).

3.3 Kryptovarat

Kryptovaroilla tarkoitetaan kryptografiaa hyväksikäyttävää toteutusta digitaalisesti esitetystä arvosta tai sopimuksesta. Euroopan keskuspankki (2019) määrittelee kryptovarat uudentyyppiseksi kryptografiaa hyödyntäväksi digitaaliseksi varallisuusmuodoksi, joka ei edusta taloudellisia velvoitteita tai vaatimuksia millekään tunnistetulle taholle (EKP 2019). Kryptovaroille on kuvattu yhteisiksi piirteiksi siirrettävyys, tallennettavuus sekä sähköisen kaupankäynnin mahdollisuus (HMRC 2021). Myös Suomen Finanssivalvonta (2019b) on esittänyt toimivien markkinoiden olevan edellytys kryptovara määritelmän käytölle (Finanssivalvonta 2019b).

Kryptovarat hyödyntävät lohkoketjuteknologiaa esimerkiksi digitaalisen varallisuuden omistusoikeuden osoittamisessa, sekä myös uudenlaisten valtiottomien rahajärjestelmien rakentamiseen. Näiden rahajärjestelmien toimintaan liittyy myös uudenlaisia DeFi-sovelluksia, jotka hyödyntävät lohkoketjuteknologian mahdollistamaa tokenisointia mitä mielikuvituksellisempien asioiden arvopaperistamiseen (Dutta 2020, 102)

Monet saattavatkin tuntea monet kryptovarat paremmin termillä kryptovaluutta, mutta esimerkiksi Suomen Pankissa neuvontajana toimiva Grym (2018) on todennut, että koska kryptovaluutat eivät täytä virallisen rahan määritelmää tai ole todellinen vaihtoehto viralliselle rahalle, niin niistä tulisikin puhua termillä kryptovara (Grym 2018). Tämä näkökulma on toisaalta tullut aiheelliseksi myös sellaisten ”krypto-sovellusten” kehittyessä, jotka eivät lähtökohtaisesti pyri toimimaan valuuttana, kuten termi kryptovaluutta saattaa antaa ymmärtää. Kryptovarojen luokan voidaankin ajatella koostuvan tällä hetkellä kryptovaluuttojen ryhmästä sekä suhteellisen uudesta NFT-tokenien ryhmästä, jotka molemmat voivat tapauskohtaisesti täyttää edellä mainitut määritelmät kryptovarasta.

3.3.1 Yksityinen ja julkinen avain

Kryptovarojen toiminta perustuu julkisen avaimen salaus -nimiseen kryptografiseen menetelmään, jossa avainparin avulla salataan ja todennetaan lähetettävät tietosisällöt. Julkisen avaimen salaus rakentuu julkisen avaimen ja yksityisen avaimen yhdistelmästä, jossa julkinen avain tehdään julkiseksi tietosisällön vastaanottamista varten ja lähetettävä tietosisältö salataan yksityisen avaimen avulla. (Bashir 2017, 92–93; HMRC 2021.)

Yksityinen avain on satunnaisesti luotu numerosarja, jonka käyttäjän tulee pitää vain omana tietonaan. Yksityistä avainta voitaisiin ajatella salasanana, jolla vastaanotettua tietosisältöä pystyy käsittelemään. Käytännössä kryptovarojen tapauksessa yksityistä avainta käytetään transaktioiden valtuuttamiseen, jossa valtuutetaan julkisessa osoitteessa sijaitsevien kryptovarojen lähettäminen toiseen osoitteeseen. (HMRC 2021.)

Julkinen avain muodostetaan matemaattisella toimenpiteellä yksityisestä avaimesta, jolloin julkinen ja yksityinen avain muodostavat kryptografisen parin. Julkinen avain julkaistaan julkiseksi, jolloin toinen käyttäjä pystyy lähettämään kyseisen julkisen avaimen omistavalle taholle salatun tietosisällön. (Bashir 2017, 92–93.) Julkinen avain tai jossain tapauksissa julkisesta avaimesta generoitu erillinen osoite, tallentuu lohkoketjuun, jolloin jokainen lohkoketjuun osallistuva taho pystyy näkemään transaktioiden kulun kyseisiin osoitteisiin (HMRC 2021). Julkiseen osoitteeseen saapuneita transaktioita pystyy käsittelemään vain sellainen taho, joka pitää hallussaan kyseisen julkisen osoitteen yksityistä avainta. Julkisen avaimen salausta hyödyntävän kryptovaran käyttäjien onkin erityisen tärkeää tiedostaa, että yksityisen avaimen katoaminen johtaa siihen, ettei julkisessa osoitteessa olevilla kryptovaroilla ole mahdollista suorittaa transaktioita. (HMRC 2021.)

Yksityisen avaimen turvallista säilyttämistä on pyritty helpottamaan niin sanotuilla lompakkosovelluksilla, joiden tarkoitus on parantaa kryptovarojen käyttäjäkokemusta. Käytännössä lompakon voidaan ajatella olevan graafinen käyttöliittymä säilytettävän kryptovaran lohkoketjuun ja varojen hallinnointiin. (Hyppänen 2021.)

3.3.2 Lompakko

Kryptovarojen kontekstissa lompakoksi kutsutaan paikkaa, jossa käyttäjä säilyttää kryptovaroja sisältävän osoitteen yksityistä avainta. Lompakkotyypit voidaan jakaa karkeasti kahteen eri päätyyppiin, joita ovat internet-yhteydessä toimiva online-lompakko ja internettiin kytkemätön offline-lompakko. (Burns ym. 2020; HMRC 2021). Näiden päätyyppien lisäksi on olemassa myös niin kutsuttu moniallekirjoituslompakko (multisignature), jota voidaan hyödyntää sekä online- että offline-lompakoiden yhteydessä (BitPay 2022; Burns ym. 2020). Eri lompakkotyypit voivat sisältää toisistaan eroavia riskitekijöitä, jotka tulisi osata ottaa huomioon sisäistä valvontaa suunniteltaessa sekä sisäisessä tarkastuksessa (Burns ym. 2020).

Online-lompakolla tai kuumalompakolla tarkoitetaan sitä, että yksityistä ja julkista avainta säilytetään paikassa, joka on yhteydessä internettiin. Online-lompakot voidaan jakaa edelleen käyttäjän omaan online-lompakkoon, kuten älypuhelimen käyttöön lompakkona, ja palveluntarjoajien online-lompakkoihin. Tyypillisiä palveluntarjoajien online-lompakoita ovat esimerkiksi kryptovaluuttapörsseissä käytettävät lompakot. (HMRC 2021.) Erityisesti palveluntarjoajien online-lompakoiden hyötyjen voidaan ajatella perustuvan helppokäyttöisyyteen sekä, varsinkin kokemattomampien käyttäjien ollessa kyseessä, säilytyksen ja siirtojen ulkoistamiseen asiantuntijalle. Online-lompakon käyttöä voidaankin monelta osin verrata perinteisten pankkipalveluiden käyttämiseen, kuitenkin sillä erotuksella, että online-lompakoita tarjoavat tahot eivät toistaiseksi kuulu välttämättä yhtä kattavan viranomaissääntelyn piiriin, kuin perinteiset pankit.

Offline-lompakolla tai kylmälompakolla tarkoitetaan yksityisen ja julkisen avaimen säilyttämistä paikassa, joka ei ole yhteydessä internettiin (HMRC 2021; Burns ym. 2020). Offline-lompakkona voidaan käyttää esimerkiksi kyseiseen

käyttötarkoitukseen kehitettyä laitteistoa, kuten USB-muistitikkua (HMRC 2021). Avaimet voidaan myös tallentaa yksinkertaisesti paperilapulle tai kaivertamalla esimerkiksi metallilevyyn tekstin säilymisen parantamiseksi. Offline-lompakoiden merkittävänä etuna voidaan pitää niiden vaikeampaa hakkeroitavuutta verrattuna jatkuvassa internetyhteydessä oleviin online-lompakoihin (Hyppänen 2021). Offline-lompakoiden tapauksessa vastuu siirtyy kuitenkin kokonaan käyttäjälle, jonka tekemä virhe voi johtaa pahimmassa tapauksessa säilytettyjen kryptovarojen menettämiseen pysyvästi.

Kryptovaralompakot ovat yleensä lähtökohtaisesti yhden allekirjoituksen vaativia lompakoita, mutta etenkin organisaatioiden näkökulmasta tällainen lompakko voi aiheuttaa esimerkiksi avainhenkilöriskin sen suhteen, kenelle annettaan valtuutus hallita kyseistä lompakkoa. Yksi suosittu tapa hallita avainhenkilöriskiä on moniallekirjoituslompakko, jolloin lompakossa olevien varojen hallinta edellyttää useamman yksityisen avaimen yhteistyötä. Tällöin julkiset avaimet voidaan jakaa eri henkilöille ja asettaa raja sille, kuinka monen henkilön valtuutus tarvitaan transaktion toteuttamiseen. (BitPay 2022; Burns ym. 2020.)

3.4 Ei-lajiesinemäiset tokenit (NFT)

Termi NFT tulee lyhennelmänä englannin kielen sanoista “non-fungible token”, joka voidaan suomentaa ei-lajiesinemäiseksi tokeniksi (Tanninen 2021). Kyseisen termin voisi myös ymmärtää kuvaavan Popescun (2021) mukaan digitaalisessa muodossa olevaa yksilöivää aitoustodistusta tai Karin (2021) suomalaisen oikeustieteen käyttämästä käsitteestä "erityisesine” johtamaa termiä ”erityistunniste”, jonka avulla tietty teos, kuten kuva tai video, voidaan yksilöidä digitaalisessa ympäristössä.

NFT-teknologiaa voidaan pitää yhtenä tokenisoinnin muotona, jossa lohkoketjuteknologiaa hyödynnetään omistusoikeuksia esittävien tokenien kirjanpitoon (Popescu 2021). NFT-tokenit toimivat teknisesti hyvin samalla tavalla kuin kryptovaluutat eroten kuitenkin vaihdettavuudeltaan kryptovaluuttojen ollessa ei-lajiesinemäisyyden sijaan lajiesinemäisiä. Lajiesinemäisyydellä tarkoitetaan sitä, etteivät tokenit ole eroteltavissa toisistaan, vaan ne ovat tasa-arvoisesti vaihdettavia päikseen. NFT-tokenit edustavat kuitenkin ei-lajiesinemäisiä tokeneita, joka tarkoittaa, että kyseiset tokenit ovatkin eroteltavissa toisistaan jonkin ominaisuuden perusteella. (Tanninen 2021; Popescu 2021.)

NFT-teknologia on alkanut kehittyä vasta aivan viime vuosien aikana eikä esimerkiksi lainsäädännössä ole vielä ehditty ottaa kunnolla kantaa NFT-teoksien juridiseen sääntelyyn. Kari (2021) on kritisoinut NFT-oikeuksien heikkoa juridista asemaa nykyisessä tekijänoikeuslainsäädännössä, sillä NFT-oikeuden omistaminen ei yleensä lähtökohtaisesti tarkoita juridisesti tekijänoikeuksien omistamista. Kaikkonen ja Wang (2021) kuitenkin painottavat, että nykyisestä heikosta oikeudellisesta asemasta huolimatta ei tule kiistää, etteikö

itse NFT-teknologialla olisi potentiaalia tuoda uusia mahdollisuuksia aineettomien oikeuksien kaupankäyntiin sekä omistusketjujen varmentamiseen. NFT-teknologiaa voisi olla heidän mukaansa mahdollista käyttää patenttien ja tavaramerkkien, sekä muiden rekisteröityjen immateriaalioikeuksien esittämisessä, mutta tätä voidaan pitää enemmänkin juridisena sopimusasiana, kuin itse teknologiaan liittyvänä seikkana. (Kaikkonen & Wang 2021.)

Teknologisesta näkökulmasta NFT-teknologian on arveltu tuovan lisäarvoa erityisesti älysopimusten mahdollistamien uudenlaisten teostyyppien sekä kompensaatiomallien avulla. Lohkoketjuun ohjelmoitavat älysopimukset mahdollistavat esimerkiksi transaktioperusteisten ehtojen luomisen omistettavaan kohteeseen, jolloin vaikkapa kohteen ominaisuudet voisivat muuttua transaktioiden myötä tai alkuperäinen valmistaja voisi saada korvauksia kaupan jälkeen myös myöhemmin tapahtuvista transaktioista. (Kaikkonen & Wang 2021; Popescu 2021.) Popescu on myös puhunut artikkelissaan NFT-teknologian roolista tulevaisuuden ”arvon internetissä”, joka tunnetaan käsitteenä laajasti myös nimillä Web 3.0 tai Web3 (Popescu 2021).

Arvon internetin ajatellaan muodostuvan ”Proof-Of-Asset” (PoA) -protokollaa käyttävästä ekosysteemistä, jossa digitaalisille asioille voidaan määrittää tokenisoinnin avulla omistajuus (Popescu 2021). Ethereum Foundation -säätiö (2022) on määrittänyt keskeisimmät erot, joita NFT-teknologia voisi tuoda verrattuna nykyiseen internetin ”Web2”-ekosysteemiin. Nämä erot esitellään taulukossa 1.

Taulukko 1: Keskeisimmät erot Web3 ja Web2 välillä (Ethereum Foundation 2022.)

NFT-teknologiaa hyödyntävä Web3	**Nykyinen käytössä oleva Web2**
Jokainen digitaalinen asia on digitaalisesti ainutlaatuinen ja kopioimaton.	Digitaalisesta asiasta tehtyä kopiota ei pystytä erottamaan alkuperäisestä, joten digitaaliset asiat ovat helposti kopioitavissa.
Jokaisella digitaalisella asialla on omistaja, joka voidaan todentaa julkisesta lohkoketjusta.	Digitaalisten asioiden omistajuus tallennetaan keskitettyjen tahojen hallitsemille palvelimille, joiden sanaan on luotettava todentamisessa.
Erityyppisillä NFT-tuotteilla toteutetut transaktiot ovat keskenään yhteensopivia käytetyn järjestelmän sisällä. Esimerkiksi konserttilipun voi vaihtaa päikseen taideteokseen.	Jokaiselle digitaaliselle tuotetyypille rakennetaan oma infrastruktuuri, jossa kaupankäynti on mahdollista vain kyseisellä tuotetyypillä.
Sisällöntuottaja myy teoksiaan globaalilla markkinalla ilman rajoitteita tai riippuvuutta tietystä palveluntarjoajasta.	Sisällöntuottaja on käyttämästään alustasta riippuvainen esimerkiksi jakelun, käyttöehtojen ja maakohtaisten rajoitusten suhteen.
Sisällöntuottaja voi säilyttää omistusoikeuden teokseensa myös myyntitapahtuman jälkeen ja saada jälleenmyyntikorvauksia älysopimusten avulla.	Keskitetyn alustan tarjoava instituutio hallitsee omistusoikeuksia ja vie suuren osan myyntikorvauksista.
Digitaalisia tuotteita voidaan käyttää täysin uusilla tavoilla esimerkiksi lainan vakuutena hajautetun finanssiteknologian (DeFi) sovelluksissa.	

Vaikka edellä esitellyt kuvaukset sisällöntuottajasta voidaan nykypäiväisessä kontekstissa mieltää erityisesti luovia aloja koskeviin ammatinharjoittajiin, kuten taiteilijoihin, niin arvon internetin konseptissa tällä tarkoitetaan jokaista kyseiseen ekosysteemiin liittynyttä tahoa, jotka pyrkivät tuottamaan monetisoitavissa olevaa arvoa ennalta määrittelemättömällä tavalla. Arvon internetin ja Web3:n voidaankin ajatella olevan osa laajempaa, esimerkiksi sisältötaloudeksi (creator economy) suomennettua konseptia, joka perustuu ajatukseen tuotoksen tasapuolisemmasta jakautumisesta tuotoksen synnyttäjän ja tämän käyttämän alustasovelluksen omistajien välillä (Cimaglia 2022; Singer 2020).

3.5 Kryptovaluutat

Kryptovaluutat ovat nousseet ennennäkemättömän nopeasti maailmanlaajuiseksi omaisuusluokaksi, kun yhä useammat sijoittajat, pörssilistatut yritykset ja jopa valtiot ovat alkaneet osoittaa mielenkiintoa kyseistä omaisuusluokkaa kohtaan. Siinä missä kryptovaluuttojen käyttäjämäärän arvioiminen oli vielä muutamia vuosia sitten haastavaa johtuen käyttäjien anonymiteetistä, niin suurimpien kryptovaluuttavälittäjien viimeaikainen siirtyminen asiakkaan tuntemista ja rahanpesua koskevan viranomaissääntelyn piiriin on mahdollistanut kryptovaluuttojen käyttäjämäärien tarkemman arvioinnin. Maailman suurimpiin kryptovaluuttavälittäjiin kuuluva Coinbase (2021) on ilmoittanut käyttäjikseen noin 73 miljoonaa varmennettua yksityiskäyttäjää, sekä noin 10 000 yrityksen nimiin rekisteröityä käyttäjätiliä alustallaan (Coinbase 2021). Kaiken kaikkiaan kryptovaluuttojen käyttäjiä on arvioitu olevan globaalisti noin 295 miljoonaa tahoa (Hon, Wang, Bolger, Wu & Zhou 2022). Suurin osa kryptovaluuttojen käyttäjistä koostuu bitcoinin käyttäjistä, joita on arvioitu olevan 176 miljoona tahoa. Toiseksi eniten käyttäjiä on Ethereumin käyttämällä valuutalla etherillä, jonka käyttäjiksi on tunnistettu noin 23 miljoonaa tahoa. Kryptovaluuttojen käyttäjämääriä tarkasteltaessa erityisen huomionarvoisena seikkana voidaan pitää vuoden 2021 aikana tapahtunutta kryptovaluuttojen käyttäjämäärän nousua 106 miljoonasta käyttäjästä 295 miljoonaan käyttäjään. (Hon ym. 2022.)

Kryptovaluutat ovat alkaneet herättää kiinnostusta myös Suomessa etenkin nuorten keskuudessa. LähiTapiolan (2021) kyselyn perusteella 14 % vastanneista oli harkinnut sijoittamista kryptovaluuttoihin. Nuorten joukossa osuus oli kuitenkin huomattavasti suurempi, sillä 15–25-vuotiaista vastaajista 34 % kertoi harkinneensa kryptovaluuttoihin sijoittamista. (LähiTapiola 2021.) Yrityksien näkökulmasta kryptovaluuttojen suosion kasvaminen yksityishenkilöiden keskuudessa voikin tarjota houkuttelevia liiketoimintamahdollisuuksia tulevaisuudessa, mikä puolestaan voi ajaa yhä useampia yrityksiä pohtimaan kryptovaluuttojen hyödyntämismahdollisuuksia.

Forrester Consulting ja Bitpayn (2020) yhteistyössä toteutetun tutkimuksen mukaan myyjille, jotka mahdollistivat kryptovaluuttamaksut asiakkailleen, koitui merkittäviä taloudellisia hyötyjä kryptovaluuttojen käyttöönotosta. Tutkimuksen mukaan 40 % kryptovaluutoilla maksavista asiakkaista oli kokonaan yrityksen uusia asiakkaita, minkä lisäksi kryptovaluutoilla maksavien asiakkaiden ostosten keskisumma oli kaksi kertaa suurempi kuin perinteisillä luottokorteilla maksavien asiakkaiden tekemien ostosten keskisumma. (Forrester Consulting & Bitpay 2020.) Luottokorttiyhtiö Visan (2021) pk-yrityksille suunnatussa kyselytutkimuksessa paljastuikin, että 24 % vastaajista aikoo hyväksyä kryptovaluuttoja maksuvaihtoehdoksi vuoden 2022 aikana (Visa 2021). Myös ICT-alan konsultointiyritys Gartner (2021) on arvioinut, että 20 % suuryrityksistä tulee käyttämään kryptovaluuttoja vuoteen 2024 mennessä joko maksuvälineenä, arvon säilyttäjänä tai DeFi:n mahdollistamien ratkaisujen vuoksi (Gartner 2021).

3.5.1 Synteettinen hyödykeraha

Valtion ja rahan keskinäinen suhde sekä rahapolitiikan keskusjohtoisuus ovat synnyttäneet näkemyseroja eri taloustieteen koulukuntien keskuudessa jo vuosikymmeniä. Keskustelun taustalla ovat olleet huolet poliittisten intressien aiheuttamista haittavaikutuksista sekä rahapolitiikan optimoinnin vaikeudesta, jotka ovat johtaneet hahmotelmiin yksityisistä toisiaan vastaan kilpailevista rahajärjestelmistä (Hayek 1990.) Myös keskuspankkien korvaamista tietokoneohjelmalla on ehdotettu historian saatossa (Friedman 1999).

Suomessa on tällä hetkellä käytössä virallisena rahajärjestelmänä eurojärjestelmä, jonka käytettävänä valuuttana toimii euro, joka on luonteeltaan fiat-valuuttaa. Termi ”fiat” juontaa juurensa latinan kielen verbiin ”facere”, joka voidaan suomentaa ”olkoon”. Fiat-valuutta on valuuttaa, jonka arvoa ei ole taattu liikkeellelaskijan toimesta millään konkreettisella hyödykkeellä, vaan arvo muodostuu uskomuksen sekä verkostovaikutuksen kautta. (Kauko 2020.) Fiat-valuutan vastakohtana voidaan pitää hyödykerahaa, jonka arvo on sidottu johonkin hyödykkeeseen, kuten kultaan. Esimerkiksi kultakolikkojen sisältämällä kullalla on itsessään arvoa riippumatta kolikkojen sovitusta nimellisarvosta. (Selgin 2015.)

Fiat-valuutan sekä hyödykerahan lisäksi nykypäivänä ajatellaan olevan olemassa myös kolmas valuuttaryhmä nimeltään synteettinen hyödykeraha (synthetic commodity money), jota kryptovaluutat edustavat. Kryptovaluutat ovat siis rahahyödykkeitä, jotka jakavat osin sekä fiat-valuutan että hyödykerahan ominaisuuksia. Tämä tarkoittaa sitä, että fiat-valuuttojen tavoin kryptovaluutoillakaan ei ole välttämättä sisäistä hyödykkeeseen perustuvaa arvoa, mutta hyödykkeiden tapaan ne ovat kuitenkin usein luonteeltaan niukkoja. (Selgin 2015.)

Vuonna 2007 alkanut finanssikriisi nosti taloustieteilijöiden kiistelyn rahan luonteesta, sekä keskuspankkien rahapolitiikasta vahvasti esille. Osa oli sitä mieltä, että koko kriisiä ei olisi tapahtunut niin suuressa mittakaavassa, mikäli keskuspankit eivät olisi yrittäneet elvyttää taloutta löysällä rahapolitiikalla, kun

taas toisten mielestä keskuspankkien harjoittaman rahapolitiikan ansiosta kriisi saatiin päättymään nopeasti (Constâncio 2017). Samansuuntainen keskustelu on myös jatkunut koronapandemian aikana keskuspankkien harjoittaessa historiallisen löysää rahapolitiikkaa, joka on johtanut globaalilla tasolla fiat-valuuttojen inflaation nopeaan ja huolestuttavaan kasvuun (Lacalle 2021). Heikentyvä luottamus fiat-valuuttoja sekä keskusjohtoista rahapolitiikkaa kohtaan ovatkin voineet olla yksi selittävä tekijä kryptovaluuttojen käytön kasvulle, mikä on huomioitu myös perinteisessä finanssimaailmassa. Esimerkiksi makrotalousasiantuntija Pozsar (2022) totesi Credit Suissen sijoittajakirjeessä, ettei raha tule olemaan enää entisensä ennustaen kryptovaluutta bitcoinin mahdollisesti hyötyvän tilanteesta.

3.5.2 Bitcoin

Maailman ensimmäisenä kryptovaluuttana pidetty bitcoin aloitti toimintansa vuonna 2009, jolloin pseudonyymia Satoshi Nakamoto käyttävä henkilö tai ryhmittymä käynnisti Bitcoin-verkon toiminnan luomalla lohkoketjun ensimmäisen lohkon eli alkulohkon. Bitcoinin avainideana oli kehittää vertaisverkossa toimiva raha, joka ei tarvitse pankkeja tai muitakaan maksuvälittäjiä välikädeksi käyttäjien välisiin transaktioihin. Teknologisesti bitcoin yhdisteli useita kryptografisia menetelmiä, kuten Merkle-puuta, hash-funktiota, julkisen avaimen salausta sekä digitaalista allekirjoitusta yhdeksi toimivaksi kokonaisuudeksi. (Antonopoulos 2014.) Bitcoinia edelsi useampikin aikaisempi yritys luoda yksityinen digitaalinen valuutta. Tunnetuimpia bitcoinia edeltäviä konsepteja ovat vuonna 1998 kehitetty b-money ja 2005 esitelty BitGold (Bashir 2017, 41-42).

Bitcoin luotiin rahajärjestelmäksi, jonka tarkoitus oli yhdistää ennalta määritelty rahapolitiikka internetin mahdollistamaan yksityisyyteen, verkostoominaisuuksiin sekä digitaalisuuteen. Bitcoinin rahapolitiikasta tehtiin poliittisista päätöksistä riippumatonta sekä hyvin ennakoitavaa. Tämä toteutettiin rajoittamalla bitcoinien enimmäislukumäärä 21 miljoonaan kappaleeseen ja säätämällä uusien bitcoinien muodostama inflaatio puoliintuvaksi 210 000 lohkon, eli noin neljän vuoden välein. Viimeisen uuden bitcoinin on arvioitu muodostuvan vuonna 2140, jonka jälkeen kaikki 21 miljoonaa bitcoinia tulevat olemaan vapaasti kierrossa. (Antonopoulos 2014, 1–2.)

3.5.2.1 Louhinta

Bitcoin-järjestelmää hyökkäyksiltä suojaava voima on työtodiste–konsensusmekanismi, joka perustuu verkon ylläpitäjien louhinnaksi kutsuttuun toimintoon. Louhinnalla tarkoitetaan tietokoneen laskentatehon käyttämistä matemaattiseen prosessointiin, jonka avulla luodaan uusia transaktiotietoja sisältäviä lohkoja lohkoketjuun. Louhinnan tarkoituksena on muodostaa suoja bitcoinin lohkoketjulle sekä laskentatehon että energiankulutuksen avulla. Mikäli jokin haitallinen toimija yrittäisi hyökätä Bitcoin-järjestelmää vastaan yrit-

täen muuttaa lohkoketjun sisältämiä kirjauksia, niin onnistuakseen hänen täytyisi saavuttaa enemmistö bitcoin-louhijoiden yhteenlasketusta laskentatehosta (51 % hyökkäys), mikä edellyttäisi niin valtavaa määrää sekä laskentatietokoneiden omistamista että energian kulutusta, että tämän uhan todennäköisyyttä pidetään käytännössä olemattomana. (Antonopoulos 2014.)

Louhijoiden insentiivi suorittaa louhintaa perustuu louhinnasta jaettavaan louhintapalkkioon, eli uusiin bitcoineihin sekä transaktiomaksuun. Lohkoketjun ollessa ruuhkautunut transaktioiden määrästä, transaktiota on mahdollista saada nopeutettua antamalla ”tippiä” louhijoilla, jolloin louhija voi priorisoida transaktioita tippien perusteella. (Antonopoulos 2014, 175.) Transaktiomaksun on mahdollista luoda louhijoille insentiivi jatkaa Bitcoin-järjestelmän suojaamista louhinnan avulla senkin jälkeen, kun viimeinen uusi bitcoin on saatu luotua.

Yksinkertaistettuna louhintaa suoritetaan käytännössä arvaamalla satunnaislukuja tietystä lukuavaruudesta, jonka koko muuttuu tietyin aikavälein sen mukaan, kuinka paljon laskentatehoa käytetään lukujen arvaamiseen. Tätä mekanismia kutsutaan louhinnan vaikeusasteeksi, joka on ohjelmoitu muuttumaan 2016 louhitun lohkon välein siten, että uusia lohkoja syntyisi tulevaisuudessa keskimäärin noin 10 minuutin välein riippumatta siitä, kuinka paljon louhijat käyttävät laskentatehoa louhimiseen. (Kroll, Dabey & Felten 2013.) Tästä johtuen voidaan myös kyseenalaistaa tietyin aikavälein huomiota saavat väitteet, joissa bitcoin-transaktion kerrotaan kuluttavan tietyn verran energiaa. Bitcoin-järjestelmän energiankulutus nimittäin syntyy edellä kuvatun mukaisesti järjestelmän turvaamisesta eikä niinkään transaktioiden suorittamisesta.

3.5.2.2 Salamaverkko

Bitcoin-järjestelmän päälohkoketjussa käsitellään tällä hetkellä karkeasti noin 250 000–350 000 transaktiota päivässä (Blockchain.com 2021). Bitcoinin päälohkoketjun kapasiteetin ollessa rajallinen, on bitcoinin maksujärjestelmän skaalautuvuutta kritisoitu useaan otteeseen viimeisten vuosien aikana. Voidaan kuitenkin ajatella, että bitcoinin päälohkoketjua ei ole tarkoitettu päivittäisten maksujen suorittamiseen, vaan toimimaan vasta lopullisena maksujen selvitysjärjestelmänä. Bitcoin-järjestelmän maksujen prosessointikykyä onkin jo alettu skaalaamaan niin kutsuttujen toisen kerroksen ratkaisujen, kuten Salamaverkon avulla.

Salamaverkko on Bitcoin-järjestelmän päälohkoketjuun liittynyt, mutta siitä kokonaan erillinen ohjelmisto, jolla pyritään siirtämään yksittäiset pienet transaktiot pois kuormittamasta päälohkoketjua siten, että transaktiot netotetaan tietyllä aikavälillä ennen lopullista transaktioiden kirjaamista päälohkoketjuun (Poon & Dryja 2016). Salamaverkko hyödyntää älysopimuksia sekä moniallekirjoituslompakkoa luodakseen turvallisen maksukanavan käyttäjien välille, jonka sisällä voi toteuttaa transaktioita suurella volyymilla sekä välittömästi ilman kolmansia osapuolia. Salamaverkon maksukanavassa on mahdollista to-

teuttaa mikromaksuja pienimillään vain 0,00000001 bitcoinilla, joka vastaa tutkimuksen tekohetken kurssilla 0,00036 euroa. (Lightning.network 2022.)

Mikromaksujen mahdollisuus sekä nopea transaktioiden toteuttaminen on ajanut organisaatioita hyödyntämään Salamaverkon toimintoja. Zap Solutions-niminen yritys on rakentanut Salamaverkon varaan toimivan sovelluksen nimeltä Strike, jonka avulla käyttäjät voivat lähettää globaaleja maksuja käytännössä ilman siirtokustannuksia. Esimerkiksi yhteisöpalvelu Twitter on mahdollistanut sovelluksessaan pienten bitcoin-maksujen lähettämisen käyttäjätilien välillä Striken mikromaksu-palvelun kautta. (Mallers 2021.)

Salamaverkon hyödyntämisen vodaan ajatella olevan tulevaisuudessa varteenotettava vaihtoehto ulkomaanmaksujen välittämiseen haastaen nykyisiä maksuvälityspalveluita sekä etenkin kehittyviin maihin suunnatuksi maksupalveluksi. Kehittyneiden maiden näkökulmasta digitalisaation jatkumisen myötä myös mikromaksujen hyödyntäminen voi kasvaa tulevaisuudessa, mihin Salamaverkko tarjoaa tällä hetkellä kyvykkään ratkaisun. Esimerkiksi Robert ym. (2020) ovat osoittaneet, että Salamaverkko voisi sopia teknologiseksi ratkaisuksi esineiden internetin (IoT) ekosysteemien vaatimien mikromaksutapahtumien toteutukseen. Salamaverkon toimintaan voi kuitenkin vielä liittyä anonymiteettiin sekä maksukanavien keskittymiseen liittyviä riskejä, jotka tulisi osata huomioida Salamaverkon laajemmassa käytössä (Tikhomirov, Moreno-Sanchez & Maffei 2020).

3.5.3 Vaihtoehtovaluutat

Bitcoinin ollessa avoimen lähdekoodin projekti, monet toimijat päättivät kopioida ja alkaa jatkokehittämään Bitcoin-protokollan koodia, jonka seurauksena alkoi syntyä niin kutsuttuja altcoineja eli vaihtoehtovaluuttoja bitcoinille. Vaihtoehtovaluuttoja tarkoittava termi "altcoin" on lyhennelmä englannin kielen sanoista "alternative" ja "coin" tarkoittaen määritelmällisesti kaikkia muita kryptovaluuttoja paitsi bitcoinia. (Bashir 2017, 186.)

Sekä termiä kryptovaluutta että termiä vaihtoehtovaluutta voidaan kuitenkin pitää tietyssä mielessä liian yksinkertaisina termeinä kuvaamaan kaikkia kryptovaluuttaprojekteja. Suomenkielisiä kryptovaluuttaoppaita tuottava Bitcoinkeskus (2019) onkin todennut termin kryptovaluutta olevan liian epämääräinen kuvaamaan kaikkia tällä hetkellä olemassa olevia kryptovaluuttoja, koska ne voivat poiketa toisistaan käyttötarkoituksen osalta merkittävästi. Bitcoinkeskus jakaa kryptovaluutat käyttötarkoituksen mukaisesti kolmeen eri alaluokkaan, joita ovat: valuutat, tokenit ja sovellusalustat.

Valuuttakategoriaan kuuluvilla kryptovaluutoilla on oma lohkoketjujärjestelmänsä, jonka ansiosta ne pystyvät toimimaan itsenäisinä valuuttajärjestelminä. Toisin sanoen valuuttakategorian kryptovaluutat muodostavat itsessään kokonaisen raha- ja maksujärjestelmän, joka pystyy operoimaan ilman ulkopuolisten ohjelmien tukea. Tokenit ovat valuuttakategoriaan kuuluvia kryp-

tovaluuttoja kevyempiä ratkaisuja, joiden tarkoitus on toimia vain tietyn sovelluksen sisällä tapahtuvissa transaktioissa, eivätkä ne muodosta itsessään kokonaista rahajärjestelmää. Sovellusalustoiksi luokitellut kryptovaluutat eroavat merkittävästi edellä esitellyistä valuutta- ja tokeni-kategorioiden kryptovaluutoista, sillä sovellusalustat eivät pyri ensisijaisesti toimimaan valuuttoina, vaan käyttöjärjestelmänä tai ohjelmointialustana muille sovelluksille. (Bitcoinkeskus 2019.)

3.5.4 Vakaavaluutat

Vakaavaluutalla tarkoitetaan kryptovaluuttaa, joka on suunniteltu minimoimaan arvonvaihtelu kyseisessä valuutassa. Euroopan keskuspankki määrittelee vakaavaluutan digitaalisessa muodossa olevaksi arvoyksiköksi, joka ei ole muodoltaan mikään toistaiseksi tunnettu virallinen valuutta, mutta joka erilaisten vakautustyökalujen avulla pyrkii minimoimaan arvon vaihtelua suhteessa sellaiseen viralliseen valuuttaan, jota vakaavaluutan arvoyksikkö pyrkii edustamaan. (Bullmann ym. 2019.) Vakaavaluuttoja käytetään varsinkin DeFi-ekosysteemeissä virallisten valuuttojen korvikkeena.

Vakaavaluutat voidaan jakaa vakautusmekanismin toimintaperiaatteen mukaisesti kolmeen eri luokkaan, joita ovat: virallisilla valuutoilla suoritettuihin takauksiin pohjautuvat vakaavaluutat, kryptovaluutoilla suoritettuihin takauksiin pohjautuvat vakaavaluutat sekä algoritmeihin perustuvat vakaavaluutat. Vakaavaluutan vakausmekanismi voi vaikuttaa merkittävästi vakaavaluutan kykyyn säilyttää arvonsa erilaisissa markkinatilanteissa. (Bullmann ym. 2019.)

Virallisten valuuttojen takauksiin pohjautuvilla vakaavaluutoilla tarkoitetaan vakaavaluuttaa, jonka liikkeellelaskija on lupautunut pitämään vähintään vastaavan määrän virallisessa valuutassa mitattavia varoja säilytyksessä, kuin mitä vakaavaluuttaa on laskettu liikkeelle. Huomionarvoista on, että liikkeellelaskijan säilytyksessä pitämät varat voivat koostua myös muista instrumenteista kuin käteisestä, kuten esimerkiksi korkopapereista. (Bullmann ym. 2019.) Tästä johtuen takauksiin pohjautuva vakaavaluutta voi olla altis luottamuspulasta johtuville markkinareaktioille, mikäli markkinaosapuolet alkavat epäilemään liikkeellelaskija halussa olevien takauksien todellista arvoa (Bullmann ym. 2019; Moore 2020).

Kryptovaluutta pohjaisiin takauksiin perustuvat vakaavaluutat ottavat vastaan virallisten valuuttojen sijasta jotain kryptovaraa takauksiksi. Tämän tyyppiset vakaavaluutat toimivat usein hajautettujen sovellusten tai hajautettujen autonomisten organisaatioiden pohjalta hyödyntäen älysopimuksia tarvittavista takauksista huolehtimiseen. Koska takaukset suoritetaan julkisessa lohkoketjussa, on takauksien määrä ja laatu myös jatkuvasti todennettavissa lisäten tietynlaista luottamusta toimintaan. (Bullmann ym. 2019.)

Algoritmeihin pohjautuvien vakaavaluuttojen toiminta perustuu peliteoreettiseen markkinamekanismiin, jolloin vakaavaluutta ei tarvitse takauksia pitääkseen valuutan arvon tasaisena. Algoritmeihin pohjautuvat vakaavaluutat edustavat teoriassa mahdollisesti lupaavinta innovaatiota vakaavaluuttojen kannalta, joita monet keskuspankitkin ovat tutkineet. Vaikka kyseiset vakaavaluutat toimivat suurimman osan ajasta hyvin, niin toistaiseksi ne eivät ole kuitenkaan käytännössä onnistuneet lunastamaan lupauksiaan markkinashokeissa. (Bullmann ym. 2019.)

Vaikka vakaavaluuttojen käyttäminen voi varsinkin seuraavaksi esiteltävän hajautetun finanssiteknologian ekosysteemissä tuntua houkuttelevalta ratkaisulta nopean liikuteltavuuden ja alhaisten siirtomaksujen vuoksi, niin vakaavaluuttojen käyttöön voi liittyä useita tunnistettuja riskejä koskien rahanpesua, asiakkaan tuntemista koskevan lainsäädännön laiminlyömistä sekä vakaavaluuttojen reservien auditoitavuutta, joka voi muodostua todelliseksi riskiksi viimeistään markkinashokeissa. (Moore 2020).

3.5.5 Hajautettu finanssiteknologia (DeFi)

Termi DeFi on lyhennelmä englannin kielen sanoista “decentralized finance”, jolla tarkoitetaan hajautettuja finanssiteknologiaa (Zetzsche ym. 2020; Grassi ym. 2022). DeFi:ä ei ole toistaiseksi juuri määritelty juridisesti, mutta DeFi-sovellusten on havaittu noudattavan vähintään yhtä tai useampaa seuraavista ominaisuuksista: hajautettu toimintaympäristö, lohkoketjuteknologian käyttäminen, älysopimusten hyödyntäminen, transaktioiden mahdollistaminen ilman välittäjiä ja sensuroimattomien pankkitoimintojen mahdollistaminen (Zetzsche ym. 2020).

DeFi-sovellusten toiminta perustuu lohkoketjuteknologian mahdollistamiin hajautettuihin selvityskerroksiin (settlement layer), joiden avulla on pyritty parantamaan sekä perinteisten rahoitusinstrumenttien läpinäkyvyyttä, että luomaan myös uudenlaisia instrumentteja, kuten autonomiset likviditeettipoolit, pikalainat ja vakaavaluutat (Schär 2021). Tämänhetkiset DeFi-sovellukset ovat rakennettu enimmäkseen älysopimukset mahdollistavan Ethereum-sovellusalustan varaan, joka puolestaan on luonut merkittäviä skaalautuvuutta koskevia verkostovaikutuksia rakennettaville sovelluksille (Grassi ym. 2022; Schär 2021). DeFi-sovellusten toimintaan liittyy myös läheisesti tokenisointi, jonka avulla lisätään resursseja, kuten vaikkapa tiettyjä oikeuksia lohkoketjuun siirreltäväksi (Schär 2021).

DeFi-sovellusten hyödyt painottuvat perinteisiä rahoitusjärjestelmiä nopeampiin ja halvempiin transaktioihin, lohkoketjujen läpinäkyvyyteen, anonymiteetin suomaan esteettömyyteen sekä erityisesti verkostovaikutusten myötä syntyvään skaalautuvuuteen (Grassi ym. 2022; Schär 2021). Schär onkin kuvannut DeFi-sovellusten kehittämistä Lego-palikoilla rakentamiseksi, joka mahdollistaa mielikuvituksellisten yhteyksien luomisen uusilla skaalautuvilla tavoilla (Schär 2021).

Edellä kuvatuista hyödyistä huolimatta, DeFi-sovelluksiin liittyen on tunnistettu useampia riskikohteita koskien esimerkiksi älysopimusten toimintaa, käytön turvallisuutta sekä ulkoisen tietolähteen varmentamista. Hajautetuksi väitettyjen DeFi-sovellusten toimintoja saatetaan myös todellisuudessa ohjailla keskitetysti järjestelmävalvojien erityisoikeuksien avulla, mikä voi kyseenalaistaa sovelluksen todellisen hajautuneisuuden luonteen. (Schär 2021.) Lisäksi esimerkiksi DeFi-solvelluksissa käytetystä tokenisoinnista puhuttaessa olisi hyvä keskustella täysin vapaiden finanssimarkkinoiden tuomista systeemiriskeistä, kun yksityishenkilöiden on mahdollista päästä osallistumaan sellaisiin rahoitustuotteisiin ja markkinoihin, joilla perinteisesti on toiminut vain asiantuntijaroolin omaavia henkilöitä (Dutta 2020 102).

Vaikka DeFi-sovellukset rakentuvatkin usein pelkkien älysopimusten varaan toimiakseen ilman välittäjiä, niin edellä mainituista riskeistä johtuen DeFi-sovellusten käyttö edellyttää kuitenkin toimenpiteitä sisäisessä tarkastuksessa. DeFi-sovellusten tarkastaminen saattaa aiheuttaa uusia osaamistarpeita sisäiselle tarkastukselle, sillä sovellusten toimintaa varmentavien tarkastajien olisi kyettävä jossain määrin ymmärtämään koodia sekä algoritmien teknistä toimintaa älysopimusten taustalla (Burns ym. 2020; Grassi ym. 2022).

3.6 Kryptovarat osana liiketoimintaa

Kryptovarojen yleistyessä yhä useammat yritykset voivat ajautua pohtimaan kryptovaroihin tutustumista ja mahdollisen kokeilun aloittamista. Esimerkiksi DeFi:n avulla yrityksellä voi olla mahdollisuus päästä käsiksi uudenlaisiin rahoitusmahdollisuuksiin, kun taas NFT-teknologia voi auttaa tuotteistamaan täysin uudenlaisia digitaalisia tuotteita ja palveluita sekä saavuttamaan uusia asiakasryhmiä. Deloitte (2021) on nostanut raportissaan esille myös organisaatioiden kiinnostuksen valmistautua teknologisesti keskuspankkivaluuttojen (Central Bank Digital Currency) mahdolliseen kehittymiseen tulevaisuudessa.

Suomalaisten organisaatioiden näkökulmasta yhtenä merkittävänä haasteena kryptovaroihin tutustumiselle on pidetty pankkien negatiivista suhtautumista kryptovaluuttoihin. Vuonna 2018 uutisoitiin, kuinka suomalaiset pankit sulkivat Suomen suurimman kryptovaluuttapörssin pankkitilit vedoten viranomaisvaateisiin rahan alkuperän selvittämisestä sekä asiakkaiden tunnistamisesta (Leppänen 2018). Vuonna 2019 asiaan saatiin kuitenkin merkittävä muutos, kun laki virtuaalivaluutan tarjoajista (572/2019) astui voimaan. Laissa säädetään virtuaalivaluutan tarjoajan: luotettavuudesta (7 §), asiakasvarojen säilyttämisestä (11 §) ja asiakkaan tuntemisesta (13 §). Lain voimaanastumisen jälkeen Finanssivalvonta myönsi toimintaluvan takaavan rekisteröinnin viidellä suomalaiselle kryptovaluuttatoimijalle (Finanssivalvonta 2019). Laki virtuaalivaluutan tarjoajista ja Finanssivalvonnan rekisteri ovat olleet askel eteenpäin siinä mielessä, että asiakkaan tuntemista ja rahanpesun estämistä koskeva lainsäädäntö on helpottanut tiukemmin säädeltyjen pankkien mahdollisuutta toimia yhteistyössä suomalaisten kryptovaroja käyttävien organisaatioiden kanssa.

Lohkoketjuteknologian ja kryptovarojen käytön yleistyessä organisaatiot voivat kohdata haasteita sekä teknologian integroinnissa osaksi olemassa olevia järjestelmiä ja käytänteitä että sääntely-ympäristön muuttuessa jatkuvasti. Lohkoketjupohjaisten sovellusten huono integroiminen organisaation toimintoihin voi johtaa esimerkiksi huonoon asiakaskokemukseen ja lakien noudattamatta jättämiseen. Kryptovarojen suhteen vallitsevan lainsäädännön tunteminen koskien verotusta, tietosuojaa, talousraportointia sekä muita mahdollisia asetuksia koskien onkin välttämätöntä ja voi vaatia myös sisäiseltä tarkastukselta ponnisteluja lainsäädännön kehittyessä myös valtiokohtaisesti. (Burns ym. 2020.)

3.6.1 Kryptovarat kirjanpidossa

Suomen kirjanpitolaki ei tunne erikseen kryptovaroja omaisuusluokkana, mutta kirjanpitolaista on kryptovarojen osalta sovellettavissa ohjeistus vertaisvaluuttojen ja kryptovaluuttojen käsittelyyn kirjanpidossa. Yritykset ovat Suomessa velvoitettuja pitämään kirjanpitoa liiketapahtumistaan. Tällaisia liiketapahtumia ovat KPL 2:1 § (1997) mukaan; tulot, menot, rahoitustapahtumat sekä niiden oikaisu- ja siirtoerät. Kirjanpitolautakunnan (1895/2012) lausunnon mukaan vertaisvaluutan käyttäminen ei vaikuta tähän kirjanpitovelvoitteeseen, vaan myös vertaisvaluutoilla suoritetut liiketapahtumat kuuluvat normaalin kirjanpitovelvoitteen piiriin.

Vertaisvaluuttoja tai kryptovaluuttoja ei voida pitää virallisena rahana, jonka vuoksi kirjanpidollisesti näitä varoja ei voida lukea ”rahoihin ja pankkisaamisiin” (KILA 1895/2012). Sen sijaan kryptovaluutat tulee kirjanpitolautakunnan mukaan merkitä joko rahoitus- tai vaihto-omaisuudeksi käyttötarkoituksesta riippuen. Mikäli kryptovaluutat ovat hankittu aktiivista kaupankäyntiä varten ne luokitellaan vaihto-omaisuudeksi. Kun taas mikäli kryptovaluutat ovat hankittu joko pitkäaikaiseen säilyttämiseen tai on vastaanotettu maksuja kryptovaluuttoina muuttamatta niitä viralliseen valuuttaan, luokitellaan nämä erät rahoitusomaisuuteen. Omaisuuserän luokittelulla on merkitystä etenkin erän arvostuksen kannalta. (KPL 1997; KILA 1895/2012.) Tilinpäätöksen liitetiedoissa tulee KPL 3:2.1 § (1997) mukaisesti antaa tarvittavat tiedot kryptovaluuttojen arvostusmenetelmistä ja periaatteista. Lisäksi tiedon ollessa olennaista ja merkittävää tulee liitetiedoissa ilmoittaa kryptovaluuttojen kokonaismäärä. (KILA 1895/2012.)

Kotimaisen kirjanpitokäytännön lisäksi IFRS-standardeista on laadittu kansainvälisiä ohjeita kryptovaluuttojen kirjanpidolliseen käsittelyyn. IFRS-komitean (2019) mukaan, mikäli kryptovaluuttaa ei ole hankittu jälleenmyymistarkoituksessa ne tulisi luokitella kirjanpidossa aina IAS 38:n mukaisesti aineettomiin hyödykkeisiin, kun taas mikäli virtuaalivaluutat ovat hankittu jälleenmyyntitarkoituksessa tulisi tätä erää käsitellä IAS 2 standardin mukaisesti vaihto-omaisuutena. Sen sijaan IFRS-komitea on päätynyt päätelmään, jossa kryptovaluuttoja ei voida luokitella (IFRS 32 mukaan) rahoitusomaisuuteen. Pääsyynä on, että heidän mukaansa kryptovaluuttojen ei voida katsoa olevan rahaa. Perusteena tälle on, että vaikka joitain kryptovaluuttoja voidaan käyttää vastikkeena tietyistä tavaroista tai palveluista, IFRS-komitea ei ole tietoinen mistään

kryptovaluutasta, jota käytettäisiin vaihtovälineenä ja rahayksikkönä tavaroiden tai palvelujen hinnoittelussa siinä määrin, että se olisi kaikkien liiketoimien arvostusperuste ja kirjattaisiin myös tilinpäätökseen. Näin ollen IFRS-komitea päätteli, että kryptovaluuttoja ei voida pitää myöskään rahoitusomaisuutena. (IFRS 2019.)

Asia kuitenkin vaikuttaisi olevan käytännössä monimutkaisempi ja monisyisempi kuin IFRS-komitean 2019 linjaus antaa ymmärtää. IFRS-standardeja ei ole luotu kryptovaluuttoja silmällä pitäen, joten IFRS-standardit ja niiden perusteella tehdyt tulkinnat ovat hieman kankeita kryptovaluuttoja käsiteltäessä. IFRS-standardeihin ja niiden tulkintaan onkin odotettavissa tarkennuksia lähivuosina. Muun muassa European Financial Reporting Advisory Group (EFRAG) on kritisoinut IFRS-komitean linjausta. Kritiikin kohteena ovat esimerkiksi se, että kaikki kryptovaluutat ovat niputettu yhteen, vaikka kryptovaluuttojen ominaisuudet ja käyttökohteet vaihtelevat laajasti. Heidän mukaansa tämä tulisi huomioida omaisuuserän määrittelyssä. Lisäksi tiukka linjaus rahasta ja rahoitusomaisuuteen kuuluvista eristä saavat kritiikkiä (EFRAG 2020).

Myös EU:n rahanpesudirektiivissä (EU 2018/84) on päädytty erilaiseen tulkintaan kryptovaluutoista ja rahanpesudirektiivin mukaan kryptovaluuttoja ei tulisi pitää niinkään aineettomina hyödykkeinä vaan ennemmin rahana. Rahanpesudirektiivissä (EU 2018/84) virtuaalivaluutta on määritelty seuraavasti: ”Virtuaalivaluutat ovat digitaalisia arvonkantajia, jotka eivät ole keskuspankin tai viranomaisen liikkeeseen laskemia ja joita ei välttämättä ole kytketty paperirahaan, mutta jotka luonnolliset henkilöt tai oikeushenkilöt hyväksyvät maksuvälineinä ja joita voi siirtää, varastoida tai myydä sähköisesti”. Voitaneenkin olettaa, että eri tahojen tulkinnat tulevat vielä muuttumaan ja tarkentumaan sitä mukaa kun kryptovaluutat ja niiden käyttö yleistyvät tai muuttuvat. Kirjanpidon lisäksi myös kryptovarojen verotuskäytännöt vaihtelevat maakohtaisesti. Suomessa verohallinto on laatinut ohjeen kryptovarojen verotukseen liittyvistä tekijöistä. Verohallinnon ohjeessa Virtuaalivaluuttojen verotus (2020) kuvataan nykyisen verolain soveltamisesta kryptovaroille. Tarkemmin Suomalaista kryptovaluuttojen verotusta on esitelty liitteessä 1.

3.6.2 Yleisiä tunnistettuja riskejä

Kryptovarojen sekä lohkoketjujen käyttöön voi liittyä useita tunnistettuja riskejä. Laskentatoimen näkökulmasta näitä riskejä koskevaa tutkimusta on tehty lähinnä kryptovaluuttojen osalta ja tilintarkastusnäkökulmasta, mutta havaituista (audit risk) tarkastusriskeistä monet voivat olla relevantteja myös sisäisen tarkastuksen näkökulmasta. Toiset riskeistä liittyvät yritysten sisäisiin- ja toiset ulkoisiin haasteisiin. Esimerkiksi Dyball ja Seethamraju (2021) havaitsivat tutkimuksessaan, että tilintarkastajien keskuudessa vallitsee yleinen käsitys siitä, että kryptovaluuttoja tai lohkoketjuteknologiaa hyödyntävät asiakkaat ovat riskialttiimpia kuin muut asiakkaat ja että (inherent) luontaiset ja (control risks) valvontariskit lisääntyvät tarkastustoimeksiannoissa ”lohkoketjuasiakkaiden” kanssa. Nämä käsitykset liittyvät ensisijaisesti siihen, että lohkoketjusovellusten kirjanpidosta ja teknisistä standardeista ei vallitse yksimielisyyttä. Heidän mu-

kaansa yksimielisyyden puute heikentääkin lohkoketjualustojen käytön tuomia etuja, kuten näiden alustojen tietojen eheyttä ja validointia. Lisäksi heidän tutkimuksensa mukaan tilintarkastusyrityksillä ei ole vielä kykyä varmistaa lohkoketjutransaktioita, mikä osaltaan vaikuttaa havaitsemisriskiin. (Dyball & Seethamraju 2021.) Puolestaan Harrast, Mcgilsky ja Sun (2021) kuvaavat artikkelissaan Kanadan tilintarkastajainstituutin (CPAC 2018) esiin nostamia mahdollisia ongelmakohtia. Kanadan tilintarkastajainstituutti on havainnut yhdeksän pääkohdetta, joita tilintarkastajien tulisi ottaa huomioon suunnitellessaan toimeksiantoja tai arvioitaessa onko tarkastajalla riittävä tietotaito toimeksiannon suorittamiseen. Näitä riskejä ovat;

1. ”Yhteisö päättää käyttää kryptovaluuttapörssiä, jolla ei ole tehokasta valvontaa yhteisön puolesta tekemiin transaktioihin tai yhteisön tileillä oleviin kryptovaluuttasaldoihin.
2. Yhteisöllä on kryptovaluuttalompakko, jota ei ole otettu huomioon.
3. Entiteetti menettää yksityisen avaimen, eikä siksi voi enää käyttää siihen liittyvää kryptovaluuttaa.
4. Luvaton osapuoli saa pääsyn entiteetin yksityiseen avaimeen ja varastaa entiteetin kryptovaluutan.
5. Entiteetti antaa vääriä tietoja yksityisen avaimen omistuksesta ja siten uudelleen sidotun kryptovaluutan omistajuudesta.
6. Entiteetti lähettää kryptovaluutan väärään osoitteeseen, eikä kryptovaluuttaa voida palauttaa.
7. Yhteisö tekee ja kirjaa kryptovaluuttatapahtuman sellaisen lähipiirin kanssa, jota ei voida tunnistaa lohkoketjutransaktioiden osapuolten anonymiteetin vuoksi.
8. Kryptovaluuttatransaktioiden käsittelyssä on merkittäviä viiveitä jakson lopussa.
9. Tapahtumat tai olosuhteet vaikeuttavat sen arvon määrittämistä, jolla kryptovaluutta tulisi kirjata taloudellisissa raporteissa.” (CPAC 2018.)

Edellä mainittujen riskitekijöiden vaikuttavuutta ja toimintariskin määrää on arvioitu Harrast ym. (2021) tutkimuksessa haastattelemalla tilintarkastajia ja muita laskentatoimen ammattilaisia. Tutkimuksessa on haettu vastauksia sekä riskin todennäköisyyteen että vaikuttavuuteen. Näiden tekijöiden summasta on puolestaan muodostettu niin sanottu toimintariski tai toiminnan luonteesta johtuva riski (inherent risk). Tulosten mukaan asiantuntijat pitävät kaikista todennäköisimpinä riskeinä kohtia yksi, yhdeksän ja seitsemän. Sen sijaan asiantuntijat arvioivat isoimman riskin liittyvän kohtiin, yksi, neljä ja kolme. Suurin toimintariski vaikuttaisi tulosten perusteella liittyvän ulkoisen palveluntarjoajan tai kryptovaluuttapörssin valintaan. Asiantuntijat korostavatkin haastatteluissaan, että mikäli organisaatio päätyy käyttämään ulkoista palveluntarjoajaa joko kryptovaluuttasijoituksiin tai kryptovaluutan säilyttämiseen, tulee palveluntarjoajan valintaan kiinnittää tarkasti huomiota. Tärkeitä tekijöitä ovat muun muassa kattavien raporttien saatavuus, sekä toimijan turvallisuus. Turvalli-

suusriski liittyy myös kahteen toisiksi suurimman toimintariskin omaaviin tekijöihin, joita ovat kohdat neljä ja kolme. Kryptovaluuttalompakon suojausavaimen joutuminen vääriin käsiin, joko hakkeroitavissa olevan avaimen tai avaimen huolettoman säilytystavan vuoksi, voivat johtaa varojen peruuttamattomaan menetykseen. Myös kryptovaluuttojen arvostaminen oikein talousraportoinnissa nähdään asiantuntijoiden keskuudessa haastavaksi tekijäksi ja sen kokonaistoimintariski on tilintarkastuksen näkökulmasta lähes yhtä suuri kuin kryptovaluutan menettämiseen liittyvät riskitekijät. (Harrast ym. 2021)

Harrast ym. (2021) havaitsivat asiantuntijoille laaditussa kyselyssään lisäksi, että sellaiset asiantuntijat, joilla on omakohtaista kokemusta kryptovaluutoista joko henkilökohtaisessa elämässä tai töiden puolesta, suhtautuivat kryptovaluuttoihin liittyvien riskien todennäköisyyteen vähemmän huolissaan, kuin sellaiset asiantuntijat, joille kryptovaluutat olivat tuntemattomampia. Muissa tutkimuksissa havaitut riskitekijät liittyvät edellä mainittujen lisäksi muun muassa kryptovaluuttojen voimakkaaseen volatiliteettiin sekä toimintaympäristön muuttuvaan regulaatioon (Vincent & Wilkins 2019).

Ulkoisen palveluntarjoajan käyttäminen varojen säilyttämiseen voi olla myös Vincent:in ja Wilkins:in (2019) mukaan haastavaa riskien arvioinnin näkökulmasta. Kolmansien osapuolien tarjoama puutteellinen informaatio siitä miten se säilyttää varoja, aiheuttaa riskiä. Riski liittyy esimerkiksi siihen, että asiakas luulee omistavansa kolmannen osapuolen palvelussa kryptovaluuttaa, mutta tosiasiassa omistaakin vain tietyn kokoisen oikeuden palveluntarjoajan omistamaan ja hallinnoimaan kryptovaluuttavarantoon. Toisaalta huomionarvoista voi olla myös se, onko omistus erillään muista palveluntarjoajan varoista vai käsitteleekö palveluntarjoaja niitä keskitetysti yhtenä eränä. Mikäli omistajana on tosiasiallisesti kolmas osapuoli ja/tai varat ovat keskitetty palveluntarjoajan tilille, aiheuttaa tämä toimijasta itsestään riippumattoman riskin, sillä palveluntarjoajan ajautuessa vaikeuksiin esimerkiksi verkkohyökkäyksen tai maksukyvyttömyyden vuoksi on mahdollista, että oikeuden käyttäminen varoihin ei enää onnistukaan ja varat menetetään. (Vincent & Wilkins 2019.)

Toisaalta varojen säilyttämiseen ilman palveluntarjoajia liittyy myös monia riskikohtia niin sisäisen- kuin tilintarkastuksenkin näkökulmasta. Säilyttäminen omassa kryptovaluuttalompakossa vaatii jonkin verran osaamista ja asiaan paneutumista niin teknologisen osaamisen kuin myös osaamista esimerkiksi salausavaimien säilytystavasta ja lompakossa olevien varojen hallitsemisesta. Tilintarkastusnäkökulmasta ongelmallista voi olla esimerkiksi varojen todellisen omistamisen todentaminen, varmistuminen kaikista käytössä olevista lompakoista ja toisaalta varmistuminen riittävistä sisäisistä valvontatoimenpiteistä. (Dyball & Seethamraju 2021; Harrast ym. 2021; Vincent & Wilkins 2019.) Sisäisellä valvonnalla ja toisaalta -tarkastuksella tulisikin siis varmistaa ja ennaltaehkäistä, ettei tilintarkastajien havaitsemat riskikohdat pääse realisoitumaan.

Edellä esitellyissä riskeissä keskitytään paljon kryptovaroja koskeviin riskeihin. Kuitenkin muissakin lohkoketjujärjestelmissä esiintyy erilaisia riskejä. Osa riskeistä liittyy itse teknologiaan ja osa enemmänkin sen käyttämiseen liittyviin tekijöihin. Lohkoketjujärjestelmissä esiintyviä yleisiä riskejä ovat muun

muassa riski 51% hyökkäykseen, korkea energian kulutus, vaikeudet integroida järjestelmiä keskenään, puutteet teknologiaa koskevista standardeista, järjestelmien monimutkaisuus, puutteellinen osaaminen, datan turvallisuus ja todenmukaisuus sekä älysopimusten haavoittuvuudet (Prewett, Prescott & Philips 2020). Lohkoketjuteknologian teknologiaan liittyviä riskejä on esitelty myös luvussa 3.2.4

3.6.3 Lohkoketjujen sisäinen valvonta

Lohkoketjupohjaisten sovellusten yleistyessä organisaatioille voi tulla ajankohtaiseksi pohtia, kuinka sisäinen valvonta ja tarvittavat kontrollit pystytään järjestämään uuden teknologian vaatimuksia vastaaviksi. Lohkoketjupohjaiset sovellukset voivat itsessään edistää monia riskienhallintaa koskevia seikkoja, kuten parantaa toiminnan luotettavuutta ja reagointikykyä. Lisäksi älysopimusten hyödyntäminen uudenlaisissa kontrolleissa voi muuttaa perustavanlaatuisesti sisäisen valvonnan toimintaympäristöä. Tästä huolimatta lohkoketjuteknologia voi aiheuttaa uusia vaikeasti tunnistettavia riskejä, joihin tulisi kuitenkin pyrkiä varautumaan mahdollisimman tehokkaalla tavalla. (Burns ym. 2020.)

Lohkoketjupohjaisia sovelluksia taloushallinnon näkökulmasta tutkiva Accounting Blockchain Coalition on kehittänyt neuvoa-antavan viitekehyksen työkaluksi sisäisen valvonnan järjestämisestä koskien lohkoketjupohjaisten kryptovarojen käyttöä. Viitekehys on muodostettu jakamalla kryptovarojen käyttöä koskevat prosessit kahteen osa-alueeseen; transaktioiden toteuttamiseen ja protokollatason toiminnan tuntemiseen (due dilligence). Transaktioiden toteuttamisella viitataan transaktioiden toteuttamista ja valtuuttamista koskeviin seikkoihin, kun taas protokollatason tuntemuksella tarkoitetaan kryptovaran hyödyntämän järjestelmän toimintojen tuntemista. (Pierre 2019.)

Moore (2020) tarkentaa kuinka transaktioiden toteutuksen ja valtuutuksen huomioitavat kohdat voidaan jakaa viitekehyksen puitteissa tarkemmin: lompakkotyypin valintaan, moniallekirjoituslompakon hyödyntämiseen, henkilöiden valtuuttamiseen sekä tietyssä kauppapaikassa, kuten kryptovaluuttapörssissä, sijaitsevan käyttäjätilin hallintaan. Protokollatason tuntemus puolestaan koostuu mahdollisen testiverkon (testnet) hyödyntämisestä pilotointivaiheessa, kryptovarojen toiminnan tuntemuksesta sekä hyödynnettävissä olevien lompakoiden tuntemuksesta. Viitekehyksen mukaan näiden molempien osa-alueiden edellä esitettyjen alakohtiin liittyvien riskien tunnistamisessa tulisi ottaa huomioon seuraavaksi esiteltävät osiot. (Moore 2020.)

3.6.3.1 Toiminnan luonteesta aiheutuva riski

Toiminnan luonteesta aiheutuvilla riskeillä tarkoitetaan toiminnan luonnollisia riskejä, joille organisaatio altistuu, mikäli toimenpiteitä riskien hallitsemiseksi ei suoriteta (Pierre 2019). Tällaisiksi riskeiksi voidaan mieltää transaktioiden toteuttamisen ja valtuutuksen näkökulmasta esimerkiksi osapuolten salainen yhteistyö (collusion) ja kolmannen osapuolen tarjoamien palveluiden luotettavuus. Protokollatason tuntemuksen osalta riskit voivat kohdistua kryptovaran toiminnan tarkastettavuuteen ja ilmoitettujen sääntöjen noudattamiseen erityisesti

sellaisen kryptovaran tapauksessa, joka edustaa tokenisoinnin kautta jotain reaalimaailman kohde-etuutta. (Moore 2020.)

3.6.3.2 Uhat ja haavoittuvuudet

Uhilla ja haavoittuvuuksilla tarkoitetaan toiminnan luonteesta aiheutuvien riskien mahdollista konkreettista ilmaantuvuutta. Esimerkiksi salainen yhteistyö voi näyttäytyä useamman henkilön yhteistyönä siirtää organisaatiolle kuuluvia kryptovaroja heidän henkilökohtaiseen omistukseensa ja ilmoitettujen sääntöjen noudattamatta jättäminen voi johtaa siihen, ettei reaalimaailman kohde-etuutta edustava kryptovara ole todellisuudessa taattu tällä kohde-etuudella. (Moore 2020.)

3.6.3.3 Todennäköisyys ja vaikutukset

Todennäköisyydellä ja vaikuttavuudella tarkoitetaan edellä kuvattujen uhkien ja haavoittuvuuksien todennäköisyyksien sekä ilmaantuessaan mahdollisen kokonaisvaikutuksen merkittävyyttä organisaation näkökulmasta tarkasteltuna. Viitekehyksessä sekä uhkien todennäköisyys että uhan realisoitumisen vaikutukset ovat molemmat jaettu erikseen arvioitaviksi asteikolla matalaksi, keskiverroksi ja korkeaksi. (Moore 2020.)

3.6.3.4 Sisäisen valvonnan järjestäminen

Viitekehyksen kontekstissa sisäisen valvonnan järjestämisellä tarkoitetaan edellä esiteltyjen osioiden arvioinnin perusteella suositeltavien kontrollimekanismien käyttöönottoa, joiden tarkoituksena on vähentää toiminnan luonteesta aiheutuvia uhkia ja haavoittuvuuksia organisaatiossa. Kryptovarojen käyttöä koskevan sisäisen valvonnan järjestämisen tulisi siis alkaa kryptovarojen käytön luontaisten riskien ja näiden riskien aiheuttamien uhkien tunnistamisella, minkä jälkeen tulisi siirtyä tapauskohtaisesti määrittämään uhkien todennäköisyydet ja mahdolliset vaikutukset niiden realisoituessa. Uhkien todennäköisyyksien ja mahdollisten vaikutuksien määrittämisen jälkeen voidaan pyrkiä asettamaan kontrollit näiden uhkien realisoitumisen estämiseksi kustannustehokkaalla tavalla. (Moore 2020.)

3.7 Lohkoketjujärjestelmät sisäisessä tarkastuksessa

Lohkoketjut ovat niin sisäisen kuin ulkoisenkin tarkastuksen näkökulmasta vielä hyvin uusia ja vähän tunnettuja tarkastuskohteita. Onkin esitetty olevan todennäköistä, että kaikkia sisäiselle tarkastukselle merkityksellisiä teemoja tai ongelmakohtia ei ole vielä havaittu tai pystytty ennakoimaan. (Kloch & Little 2019; Ozeran, Gura, Gura & Taras 2020.) Sisäisen valvonnan ja tarkastuksen näkökulmasta lohkoketjuja ja kryptovaroja koskevat yleiset standardit tai toimintamallit ovat vielä enimmäkseen kehitysvaiheessa, mutta COSO (Burns ym. 2020) sekä Accounting Blockchain coalition (Moore 2020) tarjoavat jo alustavan viitekehyksen lohkoketjuihin liittyvän sisäisen valvonnan järjestämisestä. Sen sijaan sisäisen tarkastuksen standardeihin ei ole ainakaan vielä tehty lohkoket-

juja koskevia lisäyksiä tai tarkennuksia. Sisäisen tarkastuksen näkökulmasta lohkoketjuteknologia ja sen mukanaan tuomat sovellukset näyttäytyvätkin uutena teknologisena haasteena. Tilanne ei ole sinällään uusi, sillä nopeasti digitalisoituvassa ympäristössä sisäisen tarkastuksen henkilöstö on joutunut ja joutuu kohtaamaan muitakin uudenlaisia disruptiivisina pidettyjä teknologiota. Lohkoketjuteknologiaa voidaan ajatella uutena järjestelmänä, jossa on joitakin fundamentaalisia eroja, mutta myös paljon samaa, kuin perinteisissä keskitetysti hallinnoiduissa järjestelmissä.

On esitetty, että lohkoketjujärjestelmillä voi olla potentiaalia mahdollistaa lukuisia uusia digitaalisia ratkaisuja moniin organisaatioiden kohtaamiin haasteisiin. Vaikka vallitsee kasvava yksimielisyys siitä, että lohkoketjut voivat tarjota merkittävää arvoa organisaatioille, on silti suoritettava arviointia sen varmistamiseksi, että tällaiset sovellukset ja järjestelmät ovat paras valinta tietyn tavoitteen saavuttamiseksi. Toisin sanottuna lohkoketjut eivät välttämättä ole paras ratkaisu läheskään kaikkiin käyttötarkoituksiin. Organisaation onkin kyettävä sisäisesti määrittämään, että lohkoketjujärjestelmä hoitaa luvatun tehtävän lisäksi tehtävänsä järkevän ja tehokkaan hallinnon mukaisesti. On myös esitetty, että tässä päätösprosessissa ja käyttöönottoprosessissa sisäisten tarkastajien roolina voisi olla toimiminen hallinto-, riski- ja valvontaympäristön arvioitsijana ja toisaalta neuvonantajana, joka tuntee liiketoiminnan sekä organisaation sisäiset toimintamallit. (Lineros 2021; Rooney ym. 2017.)

Linerosin (2021) mukaan lohkoketjujen muodostama dynaaminen ympäristö edellyttää, että sisäiset tarkastajat antavat ennakoivaa ohjausta. Näiden ennaltaehkäisevien toimien ja vastausten avulla voidaan vähentää lohkoketjujen aiheuttamia uhkia ja optimoida etuja. Lohkoketjujen yleistyminen tarjoaakin monella tapaa ainutlaatuisen mahdollisuuden sisäisen tarkastuksen ammattilaisille osoittaa merkityksensä, koska lohkoketjujen käytön käytänteet ovat vielä kehittymässä ja yritykset vasta opettelevat, mitkä sisäisen valvonnan keinot tarjoavat parhaan tasapainon kyberturvallisuuden, luottamuksellisuuden ja toimivuuden välillä. Tässä käyttöönotto- ja oppimisprosessissa sisäiset tarkastajat voivat luoda organisaatiolleen lisäarvoa omalla asiantuntijuudellaan. Linerosin mukaan myös sisäisen tarkastuksen uskottavuus ja arvo paranevat, kun tarkastajat ovat ennakoivia, tarjoavat uusia näkemyksiä ja huomioivat tulevaisuuden vaikutuksia. Näin ollen sisäisen tarkastuksen laatimat ennakoivat ohjeet, joissa käsitellään lohkoketjuongelmia, kuten kapasiteetin suunnittelua, yksityisen avaimen suojausta, luottamuksellisuutta, salausta ja ennaltaehkäiseviä laki- ja sääntelysopimuksia, tuottavat organisaatiolle arvoa (Lineros 2021).

Puolestaan Rooneyn ym. (2017) mukaan sisäisen tarkastuksen osastojen tulisi alkaa valmistautua jo ennakolta mahdolliseen tulevaisuudessa tapahtuvaan lohkoketjujärjestelmän käyttöönottoon kouluttamalla ainakin osalle sisäisistä tarkastajista lohkoketjuteknologian keskeisimpiä asioita. He perustelevat valmistautumisen tärkeyttä sisäisten tarkastajien asiantuntija- ja tarkastusroolilla organisaatiossa. Jotta sisäiset tarkastajat voisivat antaa objektiivisen varmuuden ja näkemyksen hallinnon, riskienhallinnan ja sisäisen valvonnan prosessien riittävyydestä ja tehokkuudesta lohkoketjuja hyödyntävissä ympäristöissä, on

sisäisten tarkastajien ensin ymmärrettävä, mitä heitä pyydetään käsittelemään. (Rooney ym. 2017.)

Organiaation ottaessa käyttöön tai kehittäessä lohkoketjupohjaista omaa järjestelmää, suositellaan yrityksen heti alkumetreiltä ottavan mukaan organisaation sisäinen tarkastaja. Kaikissa järjestelmissä on oltava riittävä hallinto, riskienhallinta ja valvonta, ja on paljon helpompaa rakentaa ne heti alusta alkaen kuin jälkiasennuttaa ne ongelman havaitsemisen jälkeen. Siispä asiantunteva sisäinen tarkastaja voi auttaa välttämään kalliit ja hankalat järjestelmän jälkiasennukset. (Lineros 2021; Rooney ym. 2017.)

Sisäisen tarkastuksen näkökulmasta merkittävimmät tunnistetut erot lohkoketjuteknologiaa hyödyntävän hajautetun kirjausjärjestelmän ja keskitetysti hallinnoidun kirjausjärjestelmän välillä voidaan jakaa Rooney ym. (2017) mukaan kolmeen teemaan, joita ovat: tiedon saatavuus, yhteistyön korostuva merkitys eri toimijoiden välillä ja ymmärrys siitä, että tietyt perinteiset sisäisen tarkastuksen toiminnot voivat olla tarpeettomia uudessa teknologisessa ympäristössä, jolloin tarkastuksen painopisteen tulisi muuttua.

3.7.1 Tiedon saatavuus

Tiedon saatavuudella Rooney ym. (2017) tarkoittavat sitä, että sisäisellä tarkastuksella on oltava pääsy lohkoketjuissa kulkevaan informaatioon. Pääsyn lisäksi sisäisen tarkastuksen on pystyttävä varmistamaan tiedon oikeellisuus. (Rooney ym. 2017.) Myös Alles ja Gray (2020) korostavat tutkimuksessaan lohkoketjuissa kulkevan tiedon oikeellisuuden varmentamista sekä toisaalta tiedon saatavuutta.

Toisaalta lohkoketjuun perustuva järjestelmä voi mahdollistaa tiedon jatkuvan reaaliaikaisen analysoinnin, joka voi parantaa tiedon luotettavuutta. Huomionarvoista on kuitenkin muistaa, ettei ajantasainenkaan tieto ole aina virheetöntä. Reaaliaikaisen tiedon tarkasteleminen voi vaatia erilaisia tietoteknisiä valmiuksia ja sisäisen tarkastajan tulee ymmärtää tarkastettavan lohkoketjun toimintaperiaate riittävissä määrin (Lineros 2021; Rooney ym. 2017).

Tiedon reaaliaikainen saatavuus voi Liun (2020) mukaan vaatia lohkoketjuteknologian hyödyntämisen lisäksi nykyistä parempia internetyhteyksiä, jotta tiedon päivittyminen lohkoketjuun voi tapahtua täysin viiveettä. Hyvä tiedon saatavuus on tärkeää myös data-analyysin mahdollistajana. Liu nostaa esiin, että sisäisen tarkastuksen tulisi kohdentaa varmennustoimenpiteitä lohkoketjuissa kulkevaan dataan. Käytännön työvaiheita varmennukseen liittyen ovat datan kerääminen lohkoketjusta, tietojen käsittely sekä analysointi ja toimenpiteiden suorittaminen auditointidatan analyysiraportin perusteella. Reaaliaikaisen tiedon saatavuuden ja toisaalta älysopimusten avulla sisäiseen valvontaan sekä -tarkastukseen voi olla mahdollisuus luoda myös järjestelmiä, jotka poimivat automaattisesti epäilyttävät tiedot heti kun ne on kirjattu lohkoketjuun. Tällöin valvonta automatisoituu ja varmennuksia voidaan suorittaa kohdennetummin. (Liu 2020.)

Tiedon saatavuudesta puhuttaessa on huomattava myös, ettei kaikki lohkoketjut toimi keskenään samalla tavalla. Muun muassa konsensusmekanismit ja lohkoketjun yksityisyyden taso voivat vaikuttaa lohkoketjun toimintalogiikkaan ja tiedon saatavuuteen. Lohkoketjujen eri toimintaperiaatteita avataan tarkemmin luvussa 3.1.

3.7.2 Yhteistyön korostuva merkitys

Yhteistyön korostuvalla merkityksellä tarkoitetaan yhteistyötä eri organisaatioiden tai organisaatiotasojen välillä tilanteissa, joissa lohkoketjujärjestelmä on julkisen käytön sijaan yksityisessä käytössä vain tietyllä rajatulla joukolla (Rooney ym. 2017). Esimerkiksi tunnetuimmat kryptovaluutat ovat yleensä julkisia lohkoketjujärjestelmiä, mutta on myös mahdollista, että yritys päätyy käyttämään yksityistä lohkoketjujärjestelmää toiminnassaan (Lineros 2021). Yksityiset lohkoketjujärjestelmät voivat tulla kyseeseen esimerkiksi sellaisilla organisaatioilla, joiden toimitusketjut ovat pitkiä tai raaka-aineiden ja tuotteiden matkaa tahdotaan valvoa tarkasti. Esimerkiksi lääketeollisuudessa ja elintarviketeollisuudessa onkin jo otettu testaukseen tai käyttöön tällaisia sisäisiä lohkoketjuteknologian päällä toimivia järjestelmiä, jotka mahdollistavat muun muassa nykyisiä järjestelmiä nopeamman ja tehokkaamman tuotteiden seurannan. (Deloitte 2019; Hayes 2022.)

Rooneyn ym. (2017) mukaan tällaisissa yksityisissä lohkoketjuissa tulisi löytää eri sidosryhmien ja sidosryhmien sisäisten tarkastajien välille yhteisymmärrys toimintatavoista. Yhteisten toimintatapojen löytäminen puolestaan vaatii aina kommunikaatiota sidosryhmien kesken.

Toisaalta yhteistyön merkitys voi korostua myös silloin kun esimerkiksi toimitusketjuissa perinteistä ei hajautettua järjestelmää käyttävät kaikki toimitusketjun jäsenet. Eli pelkkä teknologiapäivitys perinteisestä järjestelmästä lohkoketjujärjestelmään ei välttämättä vaikuta yhteistyön merkitykseen. Sen sijaan järjestelmän käyttötarkoitus ja käyttötapa vaikuttavat yhteistyön merkityksen mahdolliseen korostumiseen. (Alles & Gray 2020.)

3.7.3 Tarkastuksen painopisteen muuttuminen

Sisäisen tarkastuksen tietyt rutiininomaiset toiminnot voivat Rooneym ym. (2017) mukaan osoittautua tarpeettomiksi uusissa lohkoketjuihin perustuvissa toimintaympäristöissä. Rooney ym. tuovat esille esimerkkinä sen, että lohkoketjujärjestelmien kohdalla ei tarvitse enää sovittaa yhteen eri kirjaamisjärjestelmien eroja, kuten keskitettyjen järjestelmien tapauksissa, vaan lohkoketjusta on nähtävissä reaaliajassa yksi ainoa totuus, joka näyttäytyy samana kaikille lohkoketjun osapuolille. (Rooney ym. 2017.)

Klochin ja Littlen (2019) tuottaman tutkimusraportin mukaan sisäisen tarkastuksen painopistettä olisi siirrettävä enemmän lohkoketjujen yksittäisten osien toiminnan varmistamiseen ja sisäisten tarkastajien henkilökohtaista osaamista eri lohkoketjujen toimintalogiikoista tulisi parantaa. Raportin mu-

kaan uusissa järjestelmissä sisäisen tarkastuksen tulisi erityisesti hallita käyttöoikeuksien ja salausavaimien validointi, älysopimusten toiminnallisuuksien vahvistaminen, sekä lohkoketjun käyttämän suojauksen varmentaminen. (Kloch & Little 2019.)

Puolestaan Linersonin (2021) mukaan säännöllinen näytteenotto ja perinteiset arvioinnit eivät enää riitä. Lohkoketjujen, etenkin suljettujen lohkoketjujen, pitkälle automatisoitu luonne johtaa hänen mukaansa siihen, että skaalautuvia analyyttisiä työkaluja tarvitaan jatkuvaan verkon valvontaan ja tietojen eheyden varmistamiseen (Lineros 2021). Myös Liu (2020) nostaa artikkelissaan esiin näkökulman, jonka mukaan lohkoketjujen mahdollistamat automatisoinnit vaativat sisäisiltä tarkastajilta uudenlaisia työkaluja ja tehtävien painotusta. Hänen mukaansa automaation ansiosta sisäiset tarkastajat voisivat lohkoketjujärjestelmissä keskittyä ennemmin riskien ennaltaehkäisyyn ja tehokkuuden parantamiseen kuin ongelmien etsimiseen. (Liu 2020.)

Voidaankin ajatella, että lohkoketjuja hyödyntävät järjestelmät voivat vähentää sisäisten tarkastuksien rutiininomaista työtaakkaa ja siirtää tarkastuksien painopistettä enemmän eri lohkoketjuteknologioiden riskien kartoittamiseen. Lohkoketjuteknologia voi myös mahdollistaa reaaliaikaisen tarkastamisen, joka voi puolestaan tuoda yritykselle arvoa esimerkiksi riskien reaaliaikaisen havainnoinnin kautta.

Toisaalta Klochin ja Littlen (2019) sekä osin myös Linerosin (2021) julkaisuissa korostettua näkökulmaa tarkastuspainopisteen siirtymisestä enemmän järjestelmän ja sen ominaisuuksien tekniseen tarkasteluun voidaan myös haastaa. Alles ja Gray (2020) esittävätkin tutkimuksessaan, että järjestelmän tarkastaminen itsessään on kyllä merkityksellistä, mutta lopulta paljon merkityksellisempää on huolehtia, että järjestelmään syötetyt tiedot ovat paikkansa pitäviä. Heidän mukaansa ajatus tämän uudenlaisen järjestelmän teknisen tarkastuksen isosta merkityksestä onkin osittain liioiteltua. Näkökulman sanotaan juontavan juurensa ainakin osittain suurten tilintarkastusorganisaatioiden tuottamista raporteista, jotka korostavat järjestelmän teknisen tarkastuksen merkitystä (Alles & Gray 2020). Käytännössä nämä samat organisaatiot sitten tarjoavat suosittelemiaan palveluita sellaisille muille yrityksille, joiden omat valmiudet eivät riitä järjestelmien tekniseen tarkastamiseen.

3.8 Sisäisen tarkastuksen keinot lohkoketjujen aiheuttamien riskien hallintaan

Lohkoketjuteknologiaan perustuvien teknologioiden tuomat haasteet sisäisen valvonnan ja -tarkastuksen sekä riskienhallinnan näkökulmasta ovat alkaneet nousta esille alan ammattilaisten, kuten suurien tilintarkastusyhtiöiden, keskuudessa. Kuitenkin akateemista kirjallisuutta on aiheesta vielä hyvin vähän.

Linerosin (2021) mukaan yrityksen implementoidessa käyttöön lohkoketjuteknologiaa voidaan hyödyntää sisäisen tarkistuksen ja -valvonnan keinoja

riskien hallitsemiseksi. Sisäisen tarkastus voi keskittyä esimerkiksi konsultoimaan ja opastamaan hyvistä toimintatavoista, ja taas toisaalta tehtäviin voi kuulua myös muun muassa arviointia valittujen kontrollimenetelmien soveltuvuudesta ja riittävyydestä (Lineros 2021). Sisäisen tarkastuksen keinot lohkoketjutegnologian käytön aiheuttamien riskien hallitsemiseksi voidaan jakaa Rooneyn ym. (2017) sekä Klochin ja Littlen (2019) julkaisujen mukaan kolmeen pääteemaan, joita ovat hallinto, riskienhallinta ja kontrollit.

3.8.1 Hallinto

Hallinnolla tarkoitetaan sisäisen tarkastuksen yhteydessä organisaation suorituskyvystä vastaamista, etiikan sekä yrityksen arvojen toteutumisesta huolehtimista sekä riskienhallinnan järjestämistä (Rooney ym. 2017). IIA esittää asetuksessaan 2110, että sisäisen tarkastuksen tulisi arvioida seuraavia sisäisen valvonnan hallintoprosesseja:

1. Yrityksen määrittelemien arvojen ja etiikan noudattaminen.
2. Yrityksen tehokkaan suorituskyvyn ja vastuullisuuden toteutumisen varmistaminen.
3. Riskienhallinnan ja kontrollijärjestelmien järjestäminen asianmukaisesti.
4. Sujuvan viestinnän varmistaminen ulkoisten ja sisäisten tarkastajien sekä yhtiön hallituksen ja johdon välillä.

Lisäyksenä edellä mainittuihin hallintoprosesseihin IIA esittää vielä tarkentavina asetuksina 2110.A1 ja 2110.A2, että yrityksen etiikkaan liittyvien tavoitteiden toteuttamisen tehokkuutta sekä tietoteknisen hallinnon kykyä tukea yrityksen strategiaa ja tavoitteita tulisi myös arvioida sisäisissä tarkastuksissa. (IIA 2016.)

Käytännössä lohkoketjupohjaisiin varallisuuseriin liittyvällä hallinnoinnilla voidaan tarkoittaa esimerkiksi yksityisiin avaimiin liittyviä turvallisuusohjeita, vakiomuotoisten toimintojen määrittelyä, menettelytapoja käyttöoikeuksien lisäämiseen ja poistamiseen sekä erilaisten varmistusalgoritmien luomista (Kloch & Little 2019). Toisaalta IIA:n (2016) asetuksen perusteella lohkoketjuteknologian hallinnointiin voi kuulua myös esimerkiksi varmistuminen siitä, että teknologian käyttö tukee organisaation suorituskykyä ja kontrollit ovat järjestetty asianmukaisesti. Myös Liu (2020) painottaa artikkelissaan vahvan IT-hallinnon tärkeyttä lohkoketjuja käytettäessä. Hänen mukaansa se toimii teknologian käytön perustana ja auttaa määrittämään järjestelmän teknisiä vaatimuksia.

3.8.2 Riskienhallinta

Riskienhallinnalla tarkoitetaan kaikkia sellaisia toimenpiteitä, joiden tarkoitus on tunnistaa, arvioida ja pyrkiä hallitsemaan sellaisia riskejä, jotka voivat vaikuttaa yrityksen tavoitteiden saavuttamiseen. Riskienhallintaprosessi sisältää muun muassa yrityksen riskinsietokyvyn ymmärtämisen, petosriskiarvioinnin suorittamisen sekä teknologiariskien kartoittamisen. (Rooney ym. 2017.)

IIA on säätänyt riskienhallintaa koskevasta ohjeistuksesta asetuksessa 2120, kohdat 1–4, sekä asetuksessa 2120.A1, kohdat 5–8. Asetuksien mukaan riskienhallintaprosessi sisältää arvioinnin seuraavista seikoista:

1. Yrityksen tavoitteet ovat perusteltuja yrityksen mission kannalta.
2. Yritys tunnistaa merkittävimmät riskit ja arvioi niitä.
3. Yritys valitsee sopivat keinot hallita riskejä ja valitut keinot ovat perusteltuja yrityksen riskinottohalukkuuden näkökulmasta.
4. Kaikki olennaiset tiedot riskeistä ja niiden hallinnasta kerätään ja välitetään oikeaan aikaan yrityksen sisällä henkilökunnalle, johdolle sekä hallitukselle.
5. Taloudellisten ja operatiivisten tietojen luotettavuuden varmistaminen.
6. Operatiivisten toimintojen tehokkuuden sekä vaikuttavuuden arviointi.
7. Yrityksen omaisuuden turvaamiseen käytettävien mekanismien määrittäminen.
8. Kaiken lainsäädännön, määräysten, sopimusten ja sovittujen menettelytapojen noudattaminen. (IIA 2016.)

Käytännössä lohkoketjujen ja kryptovarojen riskienhallintaan kuuluu siis monia asioita ja lohkoketjujen monipuolisten teknologiaratkaisujen sekä käyttötarkoitusten vuoksi, myös siitä aiheutuvat riskit voivat vaihdella. Yleisiä lohkoketjuihin liittyvissä riskeissä huomioitavia asioita ovat esimerkiksi yksityisen avaimen säilytystapa ja turvallisuus, älysopimusten valvonta koodivirheiden ja peukaloinnin varalta ja järjestelmien virheettömän vuorovaikutuksen varmistaminen. (Kloch & Little 2019.) Liu (2020) puolestaan nostaa esiin huomioon otettavista riskeistä muun muassa ”51 % hyökkäyksen” ja juridiset epäselvyydet esimerkiksi älysopimuksia koskien. Toisaalta myös esimerkiksi kryptovaroja koskeva muuttuva lainsäädäntö voi sekin aiheuttaa käyttäjäorganisaatiolleen riskejä, jotka on hyvä huomioida.

3.8.3 Kontrollit

Kontrollit ovat yrityksen käyttämiä konkreettisia valvontamekanismeja, jotka auttavat vähentämään sekä hallitsemaan mahdollisia riskejä (Rooney ym. 2017). IIA:n asetuksen 2130 mukaan sisäisen tarkastuksen tulisi auttaa yritystä ylläpitämään sekä kehittämään tehokkaita kontrolleja. Asetuksessa 2130.A täsmennetään, että erityisesti riskienhallinnan kohtien 1,5,6,7 & 8 osalta tulisi arvioida kontrollien ja valvonnan riittävyyttä suhteessa mahdollisiin riskeihin (IIA 2016). Käytännön hallintakohteita voivat olla esimerkiksi; järjestelmään pääsyn hallinta, oikeuksien antaminen käyttäjille sekä järjestelmän ylläpitoon liittyvät kontrollit (Kloch & Little 2019).

Kloch ja Little (2019) nostavat raportissaan esiin tärkeäksi, että data, datan säilyttäminen sekä pääsy dataan on järjestetty huolella ja näitä koskevat kontrollit sekä tarkastuskäytännöt ovat kunnossa. Dataan liittyvinä huomioina he nostavat esiin muun muassa datan koostamisen lohkoihin tietoturvallisella tavalla sekä järjestelmään yhteydessä olevien rajapintojen tarkastamisen. Lohko-

ketjuissa on tyypillistä, että lohkoketjun pääkirja on hajautettu ja tallennettu useisiin ”solmuihin” (nodes), joka pienentää riskiä koko järjestelmän ajautumisesta ongelmatilaan, jossa tietoihin ei päästä syystä tai toisesta käsiksi. Kuitenkin tarkastajan on huomioitava myös odottamattomien katastrofien mahdollisuus ja datan säilyttämisessä täytyy arvioida riittääkö lohkoketjun hajautetun järjestelmän tuoma toimintavarmuus. Pääsyssä järjestelmiin ja dataan tulee arvioida puolestaan muun muassa, onko käyttöoikeudet jaettu perustellusti tai onko yleinen tietoturvallisuus järjestetty riittävällä tasolla. (Kloch & Little 2019.)

Lohkoketjuissa kulkevaan dataan liittyviä kysymyksiä on pohtinut myös Liu (2020). Hänen mukaansa sisäisten tarkastajien tulisi olla tietoisia siitä, että lohkoketjuteknologia voi edellyttää nykyisiä järjestelmiä tehokkaampia internet yhteyksiä ja toisaalta enemmän tallennustilaa. Nopeampia yhteyksiä vaaditaan jatkuvaan järjestelmän ajantasaiseen synkronointiin ja lohkoketjuissa lohko lohkolta kasvava tietomäärä asettaa omat vaatimuksensa järjestelmää ylläpitävien solmujen tallennustilalle. (Liu 2020.)

3.8.4 Kritiikkiä tekniseen tarkastukseen liittyvästä näkökulmasta

Edellä esitetyistä haasteista etenkin Kloch & Little (2019) korostavat omassa raportissaan tietoteknisiä ominaisuuksia ja haasteita, joita sisäiset tarkastajat tulevat kohtaamaan tarkastaessaan lohkoketjujärjestelmiä. Myös muissa tutkimuksissa, sekä raporteissa tuntuu olevan hyvin yleistä korostaa itse järjestelmän tarkastamista (esim. Deloitte 2019; Lee, Fiedler & Mautz 2018). Esimerkiksi järjestelmän tarkastuskohteet, joita Lee ym. (2018) suosittavat artikkelissaan sisäisille tarkastajille, sisältävät erittäin paljon käytännössä IT- tarkastukseen liittyviä työtehtäviä. Järjestelmän tekninen toiminta onkin varmasti tärkeää, mutta herää kysymys onko se kaikista tärkein osa-alue vai pitäisikö sisäisten tarkastajien kuitenkin keskittyä ennemmin muihin osa-alueisiin.

Alles ja Gray (2020) ovat päätyneet tutkimuksessaan muista poikkeavaan tulkintaan siitä, mihin sisäisten tarkastajien tulisi keskittyä lohkoketjujärjestelmien tarkastamisessa. Heidän mukaansa voisi olla syytä palata perusteisiin sen sijaan että keskitytään tarkastamaan järjestelmän teknistä toimivuutta. Käytännössä on nimittäin havaittu, että oikein laaditut lohkoketjujärjestelmät toimivat niin kuin pitääkin, mutta sen sijaan käyttäjät tekevät virheitä ja väärinkäytöksiä. Esimerkiksi joissain yrityksissä lääkkeiden valmistus- ja toimitusketjujen tehostamiseen ja laadun valvontaan on otettu käyttöön lohkoketjupohjaisia järjestelmiä. Käytännössä teknisesti täysin oikein toimivalla lohkoketjujärjestelmällä ei kuitenkaan artikkelin esimerkkitapauksessa saatu parannettua lääkkeiden laatuongelmia. Ongelmien taustalla ei nimittäin ollut järjestelmävirheet vaan se, että tuottajapuoli ei toiminut eettisesti vaan syötti järjestelmään virheellisesti raportteja, joiden mukaan tehtaalla kaikki on erinomaisessa kunnossa, kun taas todellisuudessa tehtailla oli muun muassa paljon erilaisia hygieniapuutteita. (Alles & Gray 2020.)

Käytännössä lohkoketjujärjestelmä ei siis itsessään takaa parempaa kontrolliympäristöä vaan järjestelmästä riippumatta tulee huomioida ja estää mah-

dolliset väärinkäytöstapaukset. Allesin ja Grayn (2020) mukaan lohkoketjupohjaisissa järjestelmissä väärinkäytösten ennaltaehkäisy voi olla jopa perinteisiä järjestelmiä tärkeämpää, sillä lähtökohtaisesti kaikki mitä lohkoketjuun on lisätty, on siellä pysyvästi, eli virhekirjauksien seuraus on pysyvämpi kuin perinteisissä järjestelmissä, joissa kirjauksia ja merkintöjä voidaan jälkikäteen muokata tai poistaa.

Tietojärjestelmän teknisen tarkastamisen sijaan Alles ja Gray (2020) pitävät tärkeänä, että sisäisessä tarkastuksessa kiinnitetään huomiota tekijöihin järjestelmän taustalla. Heidän mukaansa ongelmia syntyy, kun lohkoketjujärjestelmään syötetyt tiedot eivät vastaa todellisuutta. Sisäisen valvonnan tehtävänä olisikin luoda soveltuvat kontrollit, joiden avulla pystytään varmistumaan siitä, että järjestelmään syötetyt tiedot ovat paikkansa pitäviä, jolloin sisäisen tarkastuksen tehtäväksi jäisi näiden kontrollien varmentaminen. (Alles & Gray 2020.)

Myös Popchev ym. (2021) ovat päätyneet kritisoimaan Klochin ja Littlen (2019) julkaisussa vahvasti esiin tuomaa tietojärjestelmän tarkastamiseen liittyvää näkökulmaa. Heidän mukaansa sisäisen tarkastajan suorittama tietojärjestelmän yksityiskohtainen tarkastaminen ei ole realistinen ajatus, vaan järjestelmän teknologisesta tarkastamisesta vastaavat IT-henkilöt. Sen sijaan sisäisen tarkastuksen tehtäviin lohkoketjuteknologiaa käyttöönotettaessa kuuluvat heidän mukaansa varmistaa, että käyttöönoton johtaminen, riskienhallinta ja valvonta ovat järjestetty asianmukaisesti. Popchev ym. (2021) huomauttavat kuitenkin, että vaikka tietojärjestelmien tarkastaminen ei olisikaan varsinaisesti sisäisen tarkastuksen tehtävä, tulee sisäisillä tarkastajilla olla riittävä ymmärrys uudesta teknologiasta, jotta he pystyvät suorittamaan muita siihen liittyviä tehtäviä koskien muun muassa riskienhallintaa ja kontrollien sekä hallinnon arviointia.

4. AINEISTO JA MENETELMÄ

4.1 Aineisto

Tutkimuksessa pyrittiin selvittämään suomalaisten sisäisten tarkastajien valmiuksia, kokemuksia ja odotuksia koskien lohkoketjuteknologian käyttöä sekä kryptovarojen käytön mahdollisia vaikutuksia organisaatioiden riskiympäristöön. Tutkimuksen empiirinen aineisto koostuu sekä kvantitatiivisesta että kvalitatiivisesta tutkimusaineistosta. Määrällinen aineisto kerättiin sisäisille tarkastajille suunnattuna verkkokyselynä Webropol 3.0 -ohjelmistolla luodun kyselylomakkeena avulla. Tutkimuksen kvalitatiivinen eli laadullinen aineisto muodostettiin sähköpostihaastatteluiden avulla. Laadullinen aineisto koostuu kuuden kryptovaroista kokemuksia omaavien suomalaisten organisaatioiden edustajien kommenteista.

Sisäisille tarkastajille suunnatun kyselylomakkeen suunnittelussa pyrittiin ottamaan huomioon varsinaiset tutkimuskysymykset ja tutkimuksen teoriaosuus siten, että kyselylomakkeeseen vastaaminen olisi kuitenkin mahdollisimman helppoa ja ymmärrettävää eikä vastaamiseen tarvitsisi aikaisempaa tuntemusta lohkoketjuteknologiasta. Kysely toteutettiin anonyymisti eikä vastauksia voida yhdistää vastaajiin. Kyselyn avulla pyrittiin tavoittamaan mahdollisimman monta suomalaista sisäisen tarkastuksen parissa työskentelevää henkilöä, ja kysely suoritettiin Suomen sisäiset tarkastajat ry:n avustuksella. Suomen sisäiset tarkastajat ry on jäsenenä sisäisten tarkastajien maailmanlaajuisessa kattojärjestössä The Institute of Internal Auditors (IIA), sekä The European Confederation of Institute of Internal Auditing (ECIIA) -yhteenliittymässä. Yhdistys on ilmoittanut jäsenmääräkseen runsaat 600 jäsentä, joka muodostaa tutkimuksen perusjoukon. (Sisäiset tarkastajat ry 2022c.)

Kyselyyn kerättiin vastauksia aikavälillä 01.-31.03.2022. Sisäiset tarkastajat ry julkaisi 01.03.2022 sivustollaan saatekirjeen ja linkin verkkokyselyyn, jonka lisäksi tieto kyselystä lähetettiin uutiskirjeen yhteydessä Sisäiset tarkastajat ry:n jäsenille. Osallistumisesta lähetettiin uutiskirjeiden ohessa muistutukset kaksi viikkoa kyselyn alkamisen jälkeen, sekä vielä kaksi päivää ennen kyselyn sul-

keutumista. Kyselyyn vastasi ensimmäisen kolmen viikon aikana yhteensä 29 vastaajaa. Matalan vastaajamäärän vuoksi kysely päätettiin lähettää myös LinkedIn-sovelluksen Sales Navigator-ohjelmalla yhteensä sadalle sellaiselle henkilölle, jonka ilmoitettu tehtävänimike sisälsi nimikkeen ”sisäinen tarkastaja” tai ”internal auditor”. Edellä mainittujen hakutermien lisäksi haussa käytettiin maantieteellistä rajausta, jonka avulla haku rajattiin koskemaan vain Suomessa työskenteleviä henkilöitä. Näiden keinojen avulla vastauksia saatiin kyselyyn yhteensä 68 kappaletta. Saatu otos kattaa noin 11 % perusjoukosta. Kysely avattiin yhteensä 131 kertaa, joten kyselyn efektiivinen vastausprosentti oli 52 %.

Kyselylomake rakennettiin tutkimuskysymyksien sekä tutkimuksen teoriaosuudessa esiteltyjen teemojen ympärille. Näitä teemoja olivat: kiinnostus, uusien teknologioiden tuntemus, koettu osaaminen, sisäisen tarkastuksen yleinen rooli, tulevaisuuden odotukset sekä lohkoketjuteknologian ja kryptovarojen omaksumisen aste. Lisäksi kyselylomakkeen taustamuuttujia kuvaava osio koostui työkokemuksesta, työnantajasektorista sekä demografisista tekijöistä, kuten ikä ja sukupuoli.

Kyselyyn vastasi laajasti eri taustaisia sisäisiä tarkastajia ja sisäisen tarkastuksen johtajia. Vastaajista noin 66 % työskenteli yksityisellä sektorilla ja julkisella sektorilla noin 24 %. Sisäiset tarkastajat ry:n (2022) mukaan järjestön jäsenistä noin 60 % edustaa yksityistä sektoria ja 20 % julkista sektoria, joten aineiston voidaan ajatella kuvaavan ainakin tämän jakauman suhteen kohtuullisen hyvin perusjoukkoa. Vastaajat olivat iältään suurimmaksi osaksi 31–50-vuotiaita, kuten taulukosta 2 käy ilmi.

Taulukko 2: Vastaajien ikä ja sukupuoli

			Sukupuoli			
			Nainen	Mies	En halua vastata	yht.
Ikä	Alle 30	n	4	0	0	4
		%	100,0%	0,0%	0,0%	100,0%
	31-40	n	6	22	1	29
		%	20,7%	75,9%	3,4%	100,0%
	41-50	n	13	13	0	26
		%	50,0%	50,0%	0,0%	100,0%
	Yli 50	n	2	7	0	9
		%	22,2%	77,8%	0,0%	100,0%
	yht.	n	25	42	1	68
		%	36,8%	61,8%	1,5%	100,0%

Suurin osa vastaajista oli työskennellyt sisäisenä tarkastajana taulukon 3 mukaisesti alle 10 vuotta, joskin vastaukset jakautuivat kohtuullisen tasaisesti aina 20 kokemusvuoteen asti. Kyselylomakkeessa vastaajaa pyydettiin ilmoittamaan tehtävänimikkeensä avoimella kysymyksellä, jonka jälkeen tehtävänimikkeet luokiteltiin viiteen eri luokkaan saapuneiden vastauksien perusteella. Vastaa-

jien joukossa oli useita eri tehtävänimikkeitä, mutta sisäiseksi tarkastajaksi ja sisäisen tarkastuksen johtajaksi luokiteltavat nimikkeet muodostivat enemmistön. Muut-luokka sisältää laajasti eri tehtävänimikkeitä, kuten: johtaja, pankkitarkastaja, ylitarkastaja ja tarkastaja.

Taulukko 3: Vastaajan tehtävänimike ja työkokemus sisäisenä tarkastajana

			Tehtävänimike					
			Sisäinen tarkastaja	Sisäisen tarkastuksen johtaja	IT-tarkastaja	Konsultti	Muut	yht.
Kokemus sisäisenä tarkastajana	Alle 5 vuotta	n	10	4	1	1	4	20
		%	50,0%	20,0%	5,0%	5,0%	20,0%	100,0%
	6-10 vuotta	n	5	5	1	4	2	17
		%	29,4%	29,4%	5,9%	23,5%	11,8%	100,0%
	11-15 vuotta	n	10	4	0	0	2	16
		%	62,5%	25,0%	0,0%	0,0%	12,5%	100,0%
	16-20 vuotta	n	3	4	0	0	4	11
		%	27,3%	36,4%	0,0%	0,0%	36,4%	100,0%
	Yli 20 vuotta	n	2	1	0	0	1	4
		%	50,0%	25,0%	0,0%	0,0%	25,0%	100,0%
	yht.	n	30	18	2	5	13	68
		%	44,1%	26,5%	2,9%	7,4%	19,1%	100,0%

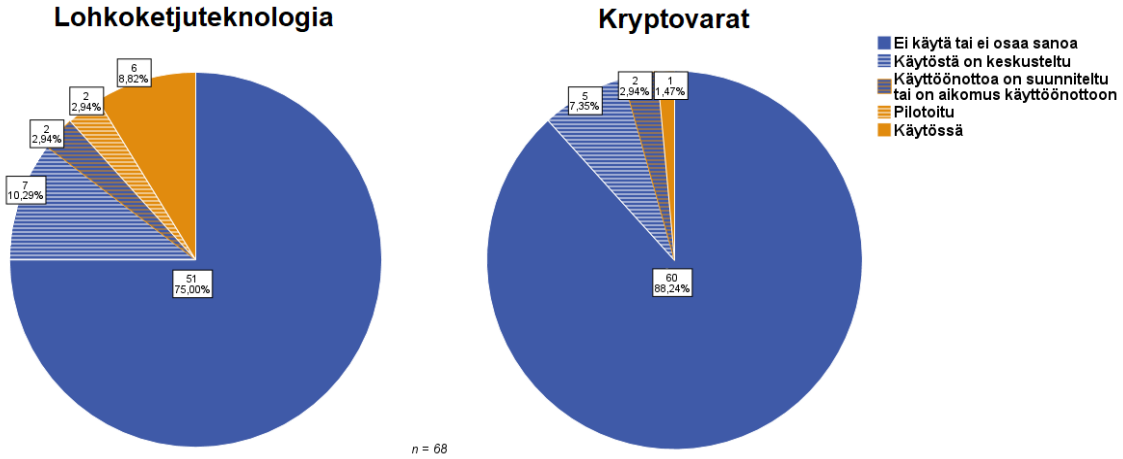
Tehtävänimikkeen lisäksi vastaajan toimiala oli kyselylomakkeen toinen avoin kysymys. Vastaajien ilmoittamat toimialat luokiteltiin taulukko 4:n mukaisesti viiteen eri toimialaluokkaan. Peräti neljäsosa vastaajista ilmoitti työskentelevänsä rahoitus- ja/tai vakuutustoimialalla. Myös teollisuus ja julkishallinto nousivat edustuksellaan huomionarvoisiksi toimialoiksi vastausten ryhmittelyssä. Muut-luokassa esiintyviä toimialoja ovat esimerkiksi: media-ala, vapaa-ajan palvelut, kaupan ala ja elintarvikeala.

Kaikista 68 vastaajasta yhteensä kuusi vastaajaa ilmoitti edustamansa organisaation jo käyttävän lohkoketjuteknologiaa osana liiketoimintaa. Lohkoketjuteknologiaa jo käyttävien organisaatioiden lisäksi kaksi vastaajaa kertoi heidän edustaman organisaation pilotoineen lohkoketjuteknologian käyttöä ja kahden vastaajan mukaan lohkoketjuteknologian käyttöönottoa oli jo suunniteltu. Lisäksi seitsemän vastaajaa vielä ilmoitti, että heidän organisaatioissansa oli käyty keskustelua lohkoketjuteknologian hyödyntämisestä. Sen sijaan 51 eli kolme neljäsosaa vastaajista kertoi, ettei heidän edustamissaan organisaatioissa ole käsitelty lohkoketjuteknologian käyttämistä millään tasolla tai he eivät olleet ainakaan tästä tietoisia. Taulukon 4 mukaisesti lohkoketjuteknologiaa oli käsitelty melko paljon rahoitus- ja vakuutustoiminnan toimialalla. Lisäksi lohkoketjuteknologiaa oli käsitelty vastaajien organisaatioissa suhteellisesti paljon tilintarkastusta- ja konsultointipalveluita koskevalla toimialalla, joskin kyseistä toimialaa koskeva havaintomäärä oli hyvin pieni.

Taulukko 4: Lohkoketjuteknologian käsittely aiheena vastaajien toimialoittain

			Lohkoketjuteknologian käsittely aiheena		
			Aihetta ei ole käsitelty	Aihetta on käsitelty	yht.
Toimiala	Rahoitus- ja vakuutustoiminta	n	8	9	17
		%	47,1%	52,9%	100,0%
	Teollisuus	n	15	1	16
		%	93,8%	6,3%	100,0%
	Julkishallinto	n	11	0	11
		%	100,0%	0,0%	100,0%
	Teknologia	n	3	1	4
		%	75,0%	25,0%	100,0%
	Tilintarkastus- ja konsultointipalvelut	n	1	4	5
		%	20,0%	80,0%	100,0%
	Muut	n	13	2	15
		%	86,7%	13,3%	100,0%
	yht.	n	51	17	68
		%	75,0%	25,0%	100,0%

Lohkoketjuteknologian käyttö oli vastausten perusteella laajempaa kuin kryptovarojen käyttö. Vain yksi vastaaja ilmoitti hänen edustamansa organisaation jo käyttävän kryptovaroja, kun 60 (88 %) vastaajista ilmoitti, ettei heidän edustamissaan organisaatioissa ole edes keskusteltu kryptovarojen käytöstä tai he eivät ole ainakaan siitä tietoisia. Vastauksia voidaan pitää odotuksien mukaisina, sillä toisinkuin pk-yrityksissä, isoissa Suomalaisissa organisaatioissa ei ole yhtäkään toimijaa, joka olisi ainakaan avoimesti ilmoittanut käyttävänsä tai omistavansa kryptovaroja. Sekä lohkoketjuteknologian että kryptovarojen käytön laajuutta vastaajien organisaatioissa on havainnollistettu tarkemmin kuviossa 5.



Kuvio 5: Lohkoketjuteknologian ja kryptovarojen käytön laajuus

Tutkimuksen laadullista osiota varten haastateltiin kryptovaluuttaasiantuntijoita. Haastattelut kohdistettiin alan asiantuntijoille sisäisten tarkastajien sijaan, sillä aiheesta tarpeeksi kokemusta omaavia sisäisiä tarkastajia olisi ollut erittäin haastava löytää. Kryptovaluuttojen parissa toimivien organisaatioiden edustajien voitiin myös olettaa olevan tietoisia käyttöön liittyvistä riskitekijöistä, joten he sopivat tämän teeman asiantuntijoiksi.

Laadullinen aineisto koostuu yhteensä kuuden suomalaisen organisaation edustajan sähköpostihaastatteluista, joissa käsiteltiin kryptovarojen liiketoiminnalliseen käyttöön liittyviä riskitekijöitä ja käyttöä rajoittavia haasteita. Yhteyttä otettiin yhteensä yhdeksään asiantuntijaorganisaatioon, jotka ovat julkisesti ilmaisseet käyttävänsä tai tarjoavansa kryptovaluuttoihin liittyviä palveluita. Nämä organisaatiot valikoituivat yhteydenoton kohteiksi, koska niillä voitiin olettaa olevan syvällistä asiantuntijuutta tutkittavasta aiheesta. Haastateltaville ilmoitettiin, että vastauksia tullaan hyödyntämään tutkimuskäytössä ja tuloksia käsitellään anonyymisti. Yhdeksästä yhteydenotosta kuusi johti haastatteluun. Vastaajat toimivat organisaatioissaan erilaisissa johtotehtävissä. Organisaatiotasolla luokiteltuna vastauksia saatiin kryptovaluuttojen palveluntarjoajalta, kryptovaluuttoja hyödyntävästä verkkokaupasta, kahdesta kryptovarojen käsittelyyn erikoistuneesta tilitoimistosta sekä kryptovaluuttojen asiantuntijayrityksestä ja -yhteisöstä.

4.2 Menetelmät

Tutkimuksessa hyödynnettiin sekä laadullista että määrällisiä menetelmiä, joten kyseessä on niin sanottu mixed methods tutkimus. Laadullisten ja määrällisten menetelmien yhdistämisellä voidaan pyrkiä yhdistämään menetelmien parhaat puolet, ja mahdollistaa näin monitahoisten tutkimuskysymyksien tarkastelu (Vaivio & Sirén 2010).

Tutkimuksen määrällisenä aineistonkeruumenetelmänä toimi verkkokysely, sillä sen avulla oli mahdollisuus tavoittaa huomattavasti useampia kohdehenkilöitä, kuin pelkästään haastattelemalla olisi ollut mahdollista, ja saada näin kattavampi kuva tutkittavan aiheen tilasta Suomessa. Haastatteluilla puolestaan pyrittiin syventämään ymmärrystä ja löytämään tekijöitä, joita ei olisi määrällisin menetelmin ollut mahdollista tutkia. Koska kyseessä on ennalta hyvin vähän tutkittu aihe, sisältää tutkimus kartoittavalle tai kuvailevalle tutkimukselle tyypillisiä piirteitä, mutta aineiston avulla on pyritty myös tekemään selittäviä tulkintoja.

Kartoittavan tai kuvailevan tutkimuksen perusteella voidaan muun muassa etsiä uusia näkökulmia ja löytää asian keskeisiä teemoja, luokkia ja tyypittelyjä, joita puolestaan voidaan hyödyntää jatkotutkimuksissa. (Metsämuuronen 2011, 55; Vilkka 2007, 20.) Määrälliseksi aineistonkeruumenetelmäksi valikoitui kysely, sillä valmista aineistoa ei ole saatavilla, ja vakiomuotoisten haastattelujen pitäminen kymmenille, jopa sadoille, sisäisille tarkastajille olisi mahdottomuus tutkimukseen käytettävien resurssien näkökulmasta. Toisaalta pienelle

joukolle suoritettujen teemahaastattelujen tuloksia ei olisi mahdollista kvantifioida ja ensimmäisiin tutkimuskysymyksiin vastaaminen olisi näin haastavaa.

Kysely on aineistonkeruutapa, jossa kysymysten muoto on standardoitu ja eroaa lomakehaastatteluista lähinnä siten, että vastaaja itse lukee ja vastaa kysymykseen (Vilkka 2007, 28). Käytännössä haastattelijan puuttumisen vuoksi kyselyn vastaaja ei voi tehdä tarvittaessa tarkentavia kysymyksiä mitä jollakin kysymyksellä tarkoitetaan, joten kyselyn laatimisessa tulee olla erityisen huolellinen. Tutkijan onkin määriteltävä käsitteet sekä kysymykset sellaisiksi, että kaikki vastaajat ymmärtävät kysymykset samalla tavalla, jotta niistä saatuja vastauksia voidaan mitata. (Vilkka 2007, 36–37.) Kysymysten laadinnassa pyrittiin edellä mainittujen asioiden lisäksi huomioimaan vastaajien oletetusti erilaiset osaamistasot niin, että vastaaminen ei edellytä aikaisempaa asian tuntemusta. Kyselyn kysymykset ovat liitteessä 2.

Kyselyn vastausvaihtoehdoissa hyödynnettiin Likertin viisi portaista asteikkoa, jossa vastaaja arvioi asiaa asteikolla täysin erimieltä, osittain erimieltä, ei samaa eikä eri mieltä, osittain samaa mieltä ja täysin samaa mieltä. Tämä asteikko on ordinaali- eli järjestysasteikollinen. Vaikka asteikko ei ole tarkasti tarkasteltuna jatkuva, se on erittäin käytetty ja yleensä ”tarpeeksi jatkuva” jatkuvuutta vaativien välimatka-asteikoille kehitettyjen tilastollisten menetelmien käyttämiseen (Metsämuuronen 2011, 71).

Aineiston avoimien kysymysten luokitteluun käytettiin Microsoft Officen Exceliä ja aineiston analysointi tapahtui IBM SPSS 28 ohjelmiston avulla. Ensin aineistolle suoritettiin normaalijakaumatarkastuksia Kolmogorov-Smirnovin testillä sekä tarkastelemalla huipukkuuksia ja vinoutta, jotta tiedetään, voidaanko käyttää vapaammin tilastollisia menetelmiä, vai täytyykö käyttää epäparametrisiä testejä. Testeissä havaittiin, että erittäin moni muuttuja osoittautui epänormaalisti jakautuneeksi. Seuraavaksi tarkasteltiin, johtuvatko epänormaalit jakaumat yksittäisistä outliereista. Epänormaalisuus vaikuttaisi kuitenkin johtuvan monissa tapauksissa siitä, että vastaukset ovat hajautuneet joko hyvin voimakkaasti vinoon tai sitten niin sanotusti kyllä-ei tapauksiin, jossa neutraaleja keskivälin vastauksia on hyvin vähän, jolloin huipukkuus on voimakkaasti negatiivinen. Normaalijakaumaoletuksen toteutumattomuus puhuu epäparametristen testien käytön puolesta. Monissa normaalijakaumaa edellyttävissäkin testeissä vaikuttaisi kuitenkin olevan tiettyjä poikkeussääntöjä, kuten riittävä otoskoko, joiden täyttyessä jakauman normaalisuus vaatimuksista voidaan joustaa (Tähtinen, Laakkonen & Broberg 2020).

Seuraavassa vaiheessa muuttujista muodostettiin erilaisia summamuuttujia. Summamuuttujien muodostamisessa käytettiin tukena eksploratiivista faktorianalyysia sekä Cronbachin alfaa. Faktorianalyysin avulla luokiteltiin muuttujia tiettyihin ryhmiin ja Cronbachin alfan avulla laskettiin kunkin muodostetun summamuuttujan reliabiliteetti. Summamuuttujien avulla muodostettiin mittarit disruptiivisten teknologioiden yleisestä tuntemisesta ja koetusta osaamisesta. Disruptiivisten teknologioiden tuntemista kuvaavan mittarin Cronbachin alfa on 0,914 ja osaamista kuvaavan mittarin alfa 0,951. Molempien mittarien reliabiliteetti on siis oikein hyvä ja ylittää selkeästi arvon 0,6, jota on

pidetty alfan miniminä (Metsämuuronen 2011, 77-78; Tähtinen ym. 2020, 86-87). Osaamista kuvaavan mittarin muodostus on esitetty luvussa 5.4. Uusien teknologioiden tuntemista kuvaava summamuuttuja puolestaan muodostettiin yhdistämällä kyselyn (liitteessä 2) osion kaksi kaikki kysymykset yhdeksi uudeksi summamuuttujaksi.

Aineiston analysoinnissa käytettiin Spearmanin korrelaatiokerrointa, Mann-Whitneyn U testiä ja regressioanalyysiä. Spearmanin korrelaatiokertoimen käyttöön päädyttiin siksi, että se ei ole niin herkkä poikkeaville arvoille tai muuttujan epänormaalisuudelle kuin Pearsonin korrelaatiokerroin (de Winter, Gosling & Potter 2016). Mann-Whitneyn U testi valittiin menetelmäksi samasta syystä, tämä testi ei edellytä muuttujien normaalijakaumaa toisin kuin Studentin t-testi (Tähtinen ym. 2020, 134-136).

Lineaarinen regressioanalyysi sisältää erilaisia oletuksia ja ehtoja, joiden täyttyessä sitä voidaan käyttää. Esimerkiksi havaintojen on oltava toisistaan riippumattomia, selittävissä muuttujissa ei saa esiintyä multikollineaarisuutta ja residuaalien tulee noudattaa normaalijakaumaa (Tähtinen ym. 2020, 195–202). Multikollineaarisuutta tarkasteltiin VIF ja Tolerance arvojen avulla, jotka myös näkyvät liitteissä olevissa regressioanalyysien tulosteissa. Arvojen raja-arvoista on hieman erilaisia näkemyksiä eri lähteissä. Shresthan (2020) mukaan yli yhden oleva VIF arvo kertoo, että muuttujien välillä esiintyy korrelaatiota. Arvon jäädessä kuitenkin alle viiden voidaan multikollineaarisuutta pitää niin vähäisenä, ettei se estä menetelmän käyttöä tai vaadi jatkotarkasteluita (Shrestha 2020). Havaintojen keskinäistä riippumattomuutta, eli virhetermien keskinäistä korreloimattomuutta mitattiin Durbin-Watsonin testillä. Arvojen ollessa lähellä arvoa kaksi, voidaan todeta, ettei haitallista määrää autokollineaarisuutta esiinny (Savin & White 1977). Residuaalien normaalijakaumat testattiin Kolmogorov-Smirnovin testillä ja testin tulosten mukaan tutkimuksen regressioanalyysien residuaalit noudattavat normaalijakaumaa.

Viimeistä tutkimuskysymystä varten suoritettiin sähköpostihaastatteluja. Sähköpostihaastattelussa haastattelu tapahtuu menetelmän nimen mukaisesti sähköpostin välityksellä. Etuina perinteisiin haastatteluihin verrattuna on muun muassa sen kustannus- ja ajankäytöllinen tehokkuus, sillä haastateltava voi vastata kysymyksiin silloin kun hänellä on aikaa ja haastattelijalle ei synny esimerkiksi matkakuluja live-haastatteluihin matkustamisesta. Toisaalta vastaajien sanattomia reaktioita ja esimerkiksi äänenpainoja on mahdotonta tulkita sähköpostin perusteella. Uhkana on myös, että kaikki ne asiat jotka, olisivat kasvotusten nousseet esiin eivät tule käsitellyiksi, mikäli vastaajan motivaatio on alhainen viestien kirjoittamiseen. Toisaalta kirjalliset vastaukset keskittyvät usein hyvin asiaan, ovat informatiivisia ja voivat joissain tapauksissa tarjota jopa enemmän tietoa, mitä perinteisellä haastattelulla on mahdollista saavuttaa. Sähköpostihaastatteluilla on siis omat etunsa ja heikkoutensa. (Meho 2006.)

Tässä tutkimuksessa sähköpostihaastattelua oli tarkoitus käyttää pohjaaineistona, jonka tietoja olisi voitu vielä syventää tavallisilla haastatteluilla. Sähköpostihaastatteluiden avulla saadut vastaukset olivat kuitenkin niin kattavia, että jo pelkistä sähköpostivastauksista koostuvan aineiston perusteella oli

mahdollista suorittaa laadullista tulkintaa tutkimuksen kannalta riittävällä laajuudella. Laadullisen tekstiaineiston käsittely aloitettiin teemoittelemalla systemaattisen taulukoinnin avulla aineisto havaittuihin teemoihin, jonka jälkeen teemat ryhmiteltiin neljäksi luokaksi. Teemoittelun avulla aineisto, kuten tekstimassa, voidaan järjestää havaittujen yhtenevien teemojen mukaiseen järjestykseen. Teemojen systemaattista taulukointia pidetään myös yhtenä yleisesti suositeltuna toimenpiteenä laadullisen aineiston käsittelyssä, joka voi auttaa määrittämään yhdistäviä tekijöitä kullekin teemalle. (Saaranen-Kauppinen & Puusniekka 2006.)

5. TUTKIMUKSEN TULOKSET

5.1 Yleistä

Tässä luvussa vastataan tutkimuksen alussa esitettyihin tutkimuskysymyksiin. Kysymyksiin 1–4 vastataan määrällisen aineiston avulla ja kysymykseen viisi laadullisen aineiston pohjalta. Tutkimuskysymykset ovat:

1. Kuinka paljon lohkoketjut näkyvät sisäisten tarkastajien nykyhetken työssä?
2. Uskovatko sisäiset tarkastajat lohkoketjujen käytön yleistyvän tulevaisuudessa ja vaikuttaako se sisäiseen tarkastukseen?
3. Kuinka hyvin sisäiset tarkastajat osaavat/osaisivat käsitellä työssään lohkoketjuja ja mitkä tekijät selittävät osaamista?
4. Kuinka kiinnostuneita sisäiset tarkastajat ovat lohkoketjuteknologiasta ja mitkä tekijät selittävät kiinnostusta?
5. Millaisia riskejä kryptovarojen käyttö voi aiheuttaa organisaatioille Suomessa?

Tulokset on koostettu niin, että ensiksi tarkastellaan voiko lohkoketjuteknologiaan liittyvät työtehtävät ylipäätään kuulua sisäisen tarkastuksen tehtäväkenttään. Sen jälkeen tulokset käsitellään samassa järjestyksessä, missä tutkimuskysymykset ovat esitetty.

5.2 Tulokset

Kyselyssä varmistettiin näkevätkö sisäiset tarkastajat lohkoketjuihin ja niiden tarkastamiseen liittyvien tehtävien kuuluvan ylipäätään sisäisen tarkastuksen tehtäviin. Vastaajien selvä enemmistö näki, että sisäiset tarkastajat voivat osallistua muun muassa lohkoketjujen käyttöönottoon tai riskikohteiden kartoitta-

miseen. Sen sijaan kysymyksen ”lohkoketjujen varmentaminen kuuluu sisäisten tarkastajien työtehtäviin” vastaukset painottuivat neutraalin ei samaa eikä eri mieltä vastauksen ympärille, kuten taulukosta 5 havaitaan.

Taulukko 5: Miten sisäiset tarkastajat voivat osallistua

	Mediaani	Keskiarvo	Keskihajonta
Sisäisillä tarkastajilla voi olla rooli lohkoketjujärjestelmien käyttöönotossa	4	3,529	1,113
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa	4	3,706	1,008
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän riskikohteiden löytämisessä	4	4,074	,779
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän valvonnan rakentamisessa	4	3,794	1,016
Lohkoketjujen varmentaminen kuuluu sisäisten tarkastajien työtehtäviin	3	2,985	1,029

Taulukon 5 vastausten perusteella voidaan päätellä, että sisäisten tarkastajien työnkuvaan voi liittyä myös lohkoketjujärjestelmiin liittyviä tehtäviä.

Seuraavaksi tarkasteltiin kuinka paljon sisäiset tarkastajat ovat jo kohdanneet lohkoketjuja työssään. Vastausten perusteella lohkoketjuteknologia ja kryptovarat ovat näkyneet toistaiseksi hyvin vähän sisäisten tarkastajien työssä. Kyselyyn vastanneiden sisäisten tarkastajien organisaatioissa oli joka neljännessä keskusteltu lohkoketjuteknologian käyttömahdollisuuksista ja noin joka kymmenennen vastaajan organisaatio käyttää lohkoketjuihin pohjautuvia sovelluksia tai järjestelmiä. Vastanneista sisäisistä tarkastajista vain yksi (~1,5 %) oli täysin samaa mieltä, että hän on jo tarvinnut lohkoketjuosaamista työssään ja kuusi (~8,8 %) vastaajista oli osittain samaa mieltä. Kaikki vastaajat, jotka kokivat tarvinneensa jompaakumpaa osaamista työskentelevät sellaisessa organisaatiossa, jossa on vähintään keskusteltu lohkoketjujen käyttömahdollisuuksista. Sen sijaan se, että organisaatio käyttää lohkoketjupohjaisia järjestelmiä, ei aineiston mukaan ole vaatinut kaikilta tällaisten organisaatioiden sisäisiltä tarkastajilta lohkoketjuosaamista. Niissä organisaatioissa, jotka käyttävät lohkoketjuteknologiaa, puolet vastaajista oli tarvinnut lohkoketjuosaamista ainakin jonkin verran.

Enimmäkseen kokemusta kuvaavat vastaukset keskittyvät kuitenkin voimakkaasti asteikon negatiivisen puolelle ja tulosten valossa suurin osa sisäisistä tarkastajista ei ole tarvinnut lainkaan osaamista lohkoketjuihin tai kryptovaroihin liittyen.

Taulukko 6: Työhön vaadittu lohkoketjuosaaminen

	Keskiarvo	Mediaani	Keskihajonta
Olen tarvinnut kryptovaluuttoihin tai NFT:hen liittyvää osaamista työssäni	1,427	1,000	,903
Olen tarvinnut lohkoketjuteknologiaan liittyvää osaamista työssäni	1,485	1,000	,999

Aikaisemman teoriatiedon valossa (esim. Basden ym. 2017; Lineros 2021) sisäisten tarkastajien rooli ja osallistumisen aste esimerkiksi uusien teknologioiden käyttöönottoon vaihtelee eri organisaatioissa. Varhaista osallistumista teknologioiden käyttöönottoon on pidetty osana ketterää sisäisen tarkastuksen toimintatapaa ja ketterän sisäisen tarkastuksen on todettu tuottavan organisaatioilleen enemmän lisäarvoa kuin perinteinen sisäinen tarkastus (Basden ym. 2017; Kotb ym. 2020). Tässä tutkimuksessa oltiin kiinnostuneita, voisiko tällä osallistumisen asteella olla merkitystä lohkoketjuihin suhtautumiseen. Tulosten mukaan käytännöt vaihtelevat, mutta monien vastaajien organisaatiossa sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa. Sen sijaan itse päätösprosessiin osallistuvia on hyvin vähän.

Taulukko 7: Osallistuminen uusien teknologioiden käyttöönottoon

	Keskiarvo	Mediaani	Keskihajonta
Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönoton päätösprosessiin	2	2	1,037
Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa	3,25	4	1,418

Spearmanin korrelaation avulla voidaan havaita, että osallistuminen varhaisessa vaiheessa korreloi positiivisesti, ja tilastollisesti merkitsevästi, lohkoketjuosaamisen sekä uusien teknologioiden tuntemuksen kanssa. Sen sijaan kiinnostuksen ja varhaisen osallistumisen välillä ei löydetty tilastollisesti merkitsevää yhteyttä. Varhainen osallistuminen teknologioiden käyttöönottoon korreloi myös positiivisesti tulevaisuuden odotusten kanssa, kuten taulukosta 8 havaitaan.

Taulukko 8: Korrelaatiot – Varhaisen vaiheen osallistumisen yhteys muihin muuttujiin

	Spearmanin rho	P (2-suuntainen merkitsevyys)	95% luottamuväli (2-suuntainen)	
			Alaraja	Yläraja
Osaamisen mittari	,532	<,001	,330	,688
Olen tarvinnut lohkoketjuteknologiaan liittyvää osaamista työssäni	,509	<,001	,302	,671
Olen kiinnostunut lohkoketjuteknologiasta	,092	,456	-,157	,330
Olen kiinnostunut kryptovaluutoista tai NFT:stä	,188	,124	-,060	,414
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana	,408	<,001	,181	,594
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana	,330	,006	,093	,532
Uusien teknologioiden tuntemus	,244	,045	-,001	,462

Vahvinta korrelaatio on osaamisen kanssa ja toisaalta sen kanssa, että lohkoketjuosaamista on tarvittu jo käytännössä. Eli tulosten mukaan, mitä vahvemmin sisäinen tarkastus osallistuu uusien teknologioiden käyttöönottoon, sitä parempaa myös lohkoketjuosaaminen on. Aineiston pienen koon vuoksi on kuitenkin hyvä huomata, että vaikka tilastollinen merkitsevyys löytyy edellä esitetyistä muuttujista, korrelaation luottamusvälit 95 % mukaan laskettuna jäävät laajoiksi. Esimerkiksi varhaisen vaiheen osallistumisen ja osaamisen välisen korrelaation luottamusväli on Spss:n Bootstrap toiminnolla laskettuna ,330–,688. Koko korrelaatiomatriisi on esitetty liitteessä 3.

5.3 Lohkoketjut ja sisäinen tarkastus tulevaisuudessa

Tulevaisuuden näkymistä voidaan karkeasti todeta, että sisäiset tarkastajat eivät usko yleisesti lohkoketjujen vaikuttavan heidän työhönsä ainakaan viiden vuoden aikavälillä. Sen sijaan, kun tarkasteluun otetaan kymmenen vuoden aikaikkuna, nähdään vaikutukset hieman todennäköisempänä, tosin vastaukset painottuvat edelleen neutraalin ”ei samaa eikä erimieltä” vastaus vaihtoehdon tienoille. Tulevaisuuden näkymissä on havaittavissa pientä negatiivista suhtau-

tumista lohkoketjuteknologiaan. Sen nähdään ennemmin vaikeuttavan ja lisäävän sisäisten tarkastajien työmäärää kuin helpottavan työtä.

Taulukko 9: Tulevaisuuden odotukset

	Keskiarvo	Mediaani	Keskihajonta
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana	2,485	2	,906
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana	3,250	3	,920
Lohkoketjuteknologia tulee vähentämään sisäisten tarkastajien työmäärää	2,721	3	,709
Lohkoketjuteknologia tulee lisäämään sisäisten tarkastajien työmäärää	3,235	3	,775
Lohkoketjuteknologia tulee vaikeuttamaan sisäisten tarkastajien työtä	3,191	3	,580
Lohkoketjuteknologia tulee helpottamaan sisäisten tarkastajien työtä	2,779	3	,730
Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa	3,514	3,5	,872

Koska lohkoketjuteknologian voidaan olettaa, aiempien tulosten ja tutkimusten (ks. esim. Kloch & Little 2019; Lineros 2021) valossa, olevan sisäisille tarkastajille vielä melko uusi asia, päätettiin tarkastella, onko kokemuksella merkitystä tulevaisuuden odotuksiin. Jaottelussa käytettiin jakoa niihin, joiden organisaatiossa on vähintään keskusteltu lohkoketjuteknologian käytöstä ja muihin vastaajiin. Menetelmänä käytettiin Mann-Whitneyn U testiä, sillä normaalijakaumaoletus ei toteudu kaikkien muuttujien osalta ja toisaalta otoskoko on pieni.

Sellaisten sisäisten tarkastajien vastaukset, joiden organisaatiossa on vähintään keskusteltu lohkoketjuteknologian käytöstä, poikkeavat monin paikoin tilastollisesti merkitsevästi muiden vastaajien vastauksista. Alla olevassa taulukossa 10 on kuvattu testin tuloksia.

Taulukko 10: Lohkoketjukeskustelun vaikutukset tulevaisuuden odotuksiin

Onko vähintään keskusteltu lohkoketjujen käytöstä. K/E	KA. Kyllä Ei	Mann-Whitney U	Z	p	r
Sisäisiä tarkastajia tarvitaan tulevaisuudessa enemmän	3,000 3,080	430,00	-,294	,769	0,036
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana	3,444 2,140	107,00	-5,123	<,001	0,621
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana	3,944 3,000	195,00	-3,792	<,001	0,460
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän IT-osaamista	4,611 4,320	341,00	-1,704	,088	0,207
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista lohkoketjuista	3,889 3,160	212,50	-3,562	<,001	0,432
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä	3,778 2,740	162,50	-4,194	<,001	0,509
Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa	4,056 3,320	233,50	-3,189	,001	0,387
Uskon, että organisaatiomme on osaamisvalmiuksien puolesta valmis ottamaan käyttöön lohkoketjuteknologiaa	3,667 2,380	185,50	-3,844	<,001	0,466
Lohkoketjupohjaisten järjestelmien parissa työskentely ei aiheuta/aiheuttaisi minulle stressiä	3,833 2,940	264,50	-2,696	,007	0,327
Lohkoketjuteknologia tulee helpottamaan sisäisten tarkastajien työtä	2,833 2,760	430,00	-,313	,755	0,038
Lohkoketjuteknologia tulee vaikeuttamaan sisäisten tarkastajien työtä	3,444 3,100	312,50	-2,332	,020	0,283
Lohkoketjuteknologia tulee lisäämään sisäisten tarkastajien työmäärää	3,444 3,160	340,00	-1,664	,096	0,202
Lohkoketjuteknologia tulee vähentämään sisäisten tarkastajien työmäärää	2,722 2,720	422,00	-,459	,646	0,056

KA=keskiarvo, r=efektikoko

Tuloksista havaitaan, että ryhmien väliset keskiarvot poikkeavat monissa muuttujissa tilastollisesti toisistaan. Yleisenä havaintona voidaan todeta, että

kyllä vastanneet sisäiset tarkastajat uskovat enemmän lohkoketjujen yleistymiseen ja siihen, että sisäisiltä tarkastajilta tullaan tarvitsemaan enemmän sekä kryptovara- että lohkoketjuosaamista. Sen sijaan yleiseen IT-osaamisen tarpeeseen tai väittämään, että lohkoketjuteknologia tulee helpottamaan sisäisten tarkastajien työtä ei löydetty tilastollisesti merkitsevää eroa. Kaikista suurimmat efektikoot olivat sillä, uskooko lohkoketjuteknologian vaikuttavan paljon työhön seuraavan viiden vuoden aikana (r=,621) ja väittämällä ”Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä” (r=,509). Näiden molempien väittämien efektikoko indikoi suurta vaikutusta (>,5 suuri vaikutus; >,3 kohtalainen vaikutus; >,1 pienivaikutus (Tähtinen ym. 2020, 45)).

Lohkoketjujen uskottuja tulevaisuuden vaikutuksia sisäisen tarkastuksen työhön tutkittiin myös regressioanalyysin avulla. Kyselyssä selvitettiin kuinka paljon sisäiset tarkastajat uskovat lohkoketjujen vaikuttavan sisäisten tarkastajien työhön seuraavan viiden ja kymmenen vuoden aikana. Kuten taulukosta 11 käy ilmi, sisäiset tarkastajat eivät yleisesti näe kovin todennäköisenä, että lohkoketjuteknologia vaikuttaisi heidän työhönsä seuraavan viiden vuoden aikana. Kymmenen vuoden aikaikkunaa tarkasteltaessa yhä useampi pitää vaikutusta kuitenkin mahdollisena. He, joilla on jo jonkinlaista kokemusta lohkoketjuteknologiasta, pitivät vaikutuksia kuitenkin todennäköisempänä kuin muut vastaajat. Tekijöitä, jotka vaikuttavat tulevaisuuden odotuksiin mitattiin askeltavan lineaarisen regressioanalyysin avulla. Sekä viiden vuoden, että kymmenen vuoden aikajännettä tarkasteltiin erikseen. Jaottelun tarkoituksena oli selvittää miten selittävät tekijät muuttuvat aikavälin kasvaessa.

Taulukko 11: Lohkoketjujen yleistymistä sisäisessä tarkastuksessa selittävät tekijät: 5 vuotta

Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan 5 vuoden aikana	Keskivirhe	β	t	p	R^2 muutos
Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan	,096	,187	1,952	,050	,450
Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia	,107	,424	3,978	,000	,073
Uskon, että organisaatiomme on osaamisvalmiuksien puolesta valmis ottamaan käyttöön lohkoketjuteknologiaa	,085	,287	3,371	,001	,048
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa	,097	-,200	-2,072	,042	,027

Korjattu R^2=,572, β=regressiokerroin, F(4,63)=23,413; p<,001, Durbin Wattson=2,427

Taulukossa 11 on esitetty muun muassa selittävien muuttujien kertoimet, selitysasteet ja merkitsevyysarvot. Liitteessä 4 on esitetty tämän regressioanalyysin alkuperäiset tulosteet. Mallin oikaistu kokonaisselitysaste on 57 % ja kaikki selittävien muuttujien kertoimet ovat tilastollisesti merkitseviä. Parhaaksi selittäjäksi osoittautui väite ”Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia” (β = ,424; p < ,001). Selittävissä muuttujissa kaksi muuta positiivisen kertoimen omaavaa muuttujaa vaikuttaisivat liittyvän organisaation tuottamasta ”paineesta” kertoviin tekijöihin. Muista poiketen väitteen ”sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa” regressiokerroin on negatiivinen. Siispä suhtautuminen negatiivisesti edellä mainittuun muuttujaan selittää positiivista vastausta selitettävässä muuttujassa.

Taulukko 12: Lohkoketjujen yleistymistä sisäisessä tarkastuksessa selittävät tekijät: 10 vuotta

Uskon Lohkoketjuteknologian vaikuttavan sisäisen tarkastuksen työhön paljon seuraavan 10 vuoden aikana	Keskivirhe	β_s	t	p	R^2 muutos
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä	,090	,443	4,806	,000	,449
Ikä	,087	-,294	-3,892	,000	,107
Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa	,099	,325	3,483	,001	,062
Lohkoketjuteknologia tulee lisäämään sisäisten tarkastajien työmäärää	,088	,192	2,588	,012	,037

Korjattu R^2=,632, β_s=standardoituregressiokerroin, F(4,63)=29,751; p<,001, Durbin Watson=2,298

Kun tarkastelujaksoa kasvatettiin kymmeneen vuoteen, muuttuivat myös selittäjät. Korjattu selitysaste (63 %) on tässä regressioanalyysissä hieman parempi kuin vastaavassa viiden vuoden mallissa. Analyysin mukaan iän regressiokerroin on negatiivinen, joka tarkoittaa käytännössä sitä, että nuoremmat vastaajat pitävät vanhempia vastaajia todennäköisempänä lohkoketjujen vaikuttavan paljon sisäiseen tarkastukseen kymmenen vuoden sisällä. Muut standardoidut regressiokertoimet ovat positiivisia ja näin ollen positiivinen suhtautuminen näihin selittäjiin johtaa positiivisempaan suhtautumiseen myös selitettävässä muuttujassa. Ehkä hieman yllättävästi, suurimman regressiokertoimen (β_s=,443; p<,001) omasi väittämä sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä, kun taas vastaava kysymys, jossa selvitettiin tarvetta tulevaisuuden osaamiselle lohkoketjujärjestelmistä ei noussut lainkaan malliin mukaan. Taulukossa 12 on esitetty muista taulukoista poiketen standardoitu regressiokerroin standardoimattoman sijaan, sillä ikämuuttuja ei toimi samalla

Likertin asteikolla muiden muuttujien kanssa. Regressioanalyysin tulosteet löytyvät liitteestä 5.

Taulukoista 11 ja 12 havaitaan, että yksikään selittävistä muuttujista ei esiinny molemmissa malleissa. Viiden vuoden aikavälillä selittävät tekijät ovat ehkä hieman konkreettisempia ja liittyvät kenties siihen, että työnantajaorganisaatio harkitsee tai on ottamassa lohkoketjujärjestelmiä käyttöönsä. Sen sijaan kymmenen vuoden tarkastelujakson selitettävää muuttujaa tarkasteltaessa esiin ei nouse organisaation vaikutus ainakaan selkeästi.

5.4 Lohkoketjuosaaminen sisäisten tarkastajien keskuudessa

Yleinen osaaminen ja tietämys lohkoketjujärjestelmistä ja kryptovaroista on tulosten mukaan melko heikkoa. Aihe vaikuttaa olevan numeerisen datan perusteella suurimmalle osalle sisäisiä tarkastajia vielä melko tuntematon. Koettua osaamista kartoitettiin useiden kysymysten avulla ja näiden kysymysten perusteella muodostettiin summamuuttuja ”osaamisen mittari”.

Taulukko 13: Osaamisen summamuuttuja

Muuttuja	Summa-muuttuja	Cronbachin alfa
Osaan/osaisin varmentaa lohkoketjujärjestelmiä Osaan/osaisin tunnistaa lohkoketjujärjestelmien riskikohteet Osaan/osaisin antaa konsultaatiota lohkoketjujärjestelmien kontrollien luomisessa Osaan/osaisin auttaa lohkoketjujärjestelmien sisäisen valvonnan järjestämisessä	Osaamisen mittari	0,951

Osaamisen mittarin keskiarvon (2,301) sekä mediaanin (2) jäädessä alhaiseksi, voidaan ajatella myös osaamisen tason olevan alhainen. Sellaisissa organisaatioissa, jotka ovat jo vähintään keskustelleet lohkoketjujen käyttömahdollisuuksista, vastaajien osaaminen on tilastollisesti merkitsevästi parempaa kuin muissa organisaatioissa $U(66)=92$, $Z=-5{,}019$, $p<{,}001$, $r=0{,}618$. Vastaajien osaamisen mittarin keskiarvo ”keskustelleissa organisaatioissa” oli 3,6806 kun muissa organisaatioissa osaamisen keskiarvo jäi tasolle 1,815.

Osaamista selittäviä tekijöitä tarkasteltiin askeltavan lineaarisen regressioanalyysin avulla. Analyysin tulokset ovat esitelty taulukossa 14.

Taulukko 14: Osaamista selittävät tekijät

Osaamisen mittari	Keskivirhe	β	t	p	R^2 muutos
Tiedän kuinka lohkoketjun rakenne vaikuttaa lohkoketjujärjestelmän riskeihin	,083	,453	5,423	,000	,603
Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa	,054	,257	4,764	,000	,144
Tunnen kryptovaluuttoja koskevan keskeisen lainsäädännön	,082	,231	2,827	,006	,022
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän IT-osaamista	,128	-,361	-2,821	,006	,021
Lohkoketjuteknologia on merkityksellistä työni kannalta	,091	,187	2,062	,043	,013

Korjattu R^2=,788, β=regressiokerroin, F(5,62)=50,942; p<,001, Durbin Wattson 1,960

Selittävät muuttujat selittävät 79 % osaamisen mittarin muutoksesta. Kaikki selittävien muuttujien kertoimet ovat tilastollisesti merkitseviä. Voimakkaimmiksi selittäjiksi nousivat ”Tiedän kuinka lohkoketjun rakenne vaikuttaa lohkoketjujärjestelmän riskeihin” (β=,453; p<,000) ja ”Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa” (β=,257; p<,000). Kaikkien muiden paitsi väittämän ”Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän IT-osaamista” (β=-,361; p=,006) regressiokertoimet ovat positiivisia. Edellä mainitun väittämän kerroin kertoo, että negatiivinen suhtautuminen selittävään muuttujaan johtaa positiiviseen suhtautumiseen selitettävässä muuttujassa. Osaamiseen liittyvän regressioanalyysin tulosteet ovat liitteessä 6.

5.5 Sisäisten tarkastajien kiinnostus lohkoketjuteknologiaan

Sisäiset tarkastajat ovat tulosten mukaan yleisesti kiinnostuneita uusista IT-teknologioista. Tarkastajien yleinen kiinnostus lohkoketjuteknologiaa sekä kryptovaroja kohtaan ovat kuitenkin hieman vähäisempää, kuten taulukosta 15 havaitaan.

Taulukko 15: Kiinnostuneisuus uusista teknologioista

	Keskiarvo	Mediaani	Keskihajonta
Olen kiinnostunut uusista IT-teknologioista	4,103	4	,866
Olen kiinnostunut lohkoketjuteknologiasta	3,162	3	1,016
Olen kiinnostunut kryptovaluutoista tai NFT:stä	2,853	3	1,225
Uskon lohkoketjuteknologian käyttämisen (esim. tietojärjestelmissä) voivan luoda lisäarvoa organisaatiolle	3,250	3	,780
Uskon kryptovaluuttojen tai NFT:n käytön voivan luoda lisäarvoa organisaatiolle	2,603	2,5	,900
Uskon lohkoketjuteknologian ratkaisevan nykyisten järjestelmien ongelmia	3,000	3	,810

Kiinnostusta selittäviä tekijöitä tutkittiin lineaarisen regressioanalyysin avulla. Analyysin tulokset ovat esitetty taulukossa 16.

Taulukko 16: Lohkoketjuteknologia kiinnostusta selittävät tekijät

Olen kiinnostunut lohkoketjuteknologiasta	Keskivirhe	β	t	p	R^2 muutos
Olen kiinnostunut kryptovaluutoista tai NFT:stä	,061	,448	7,353	,000	,657
Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan	,059	,263	4,487	,000	,090
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa	,060	-,216	-3,616	,001	,042
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista lohkoketjuista	,090	,265	2,952	,004	,030
Olen kiinnostunut uusista IT-teknologioista	,076	,180	2,373	,021	,015

Korjattu R^2= ,821, β=regressiokerroin, F(5,62)= 62,322; p<0,001, Durbin Wattson= 2,302

Selittävät muuttujat selittävät 82 % selitettävän muuttujan vaihtelusta. Selkeästi vahvin lohkoketjuteknologia kiinnostusta selittävä muuttuja on kiinostuneisuus kryptovaroista (β=,448; p<,001). Kiinnostus yleisesti uusista IT-teknologioista selittää sekin osaltaan kiinnostusta lohkoketjuteknologioihin, mutta sen regressiokerroin jää huomattavasti alhaisemmaksi (β=,180; p=0,21). Malliin nousi mukaan myös hieman yllättävä selittävä muuttuja ”Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa”, jonka regressiokerroin on negatiivinen (β=-,216; p=,001). Suhtautuminen muuttujaan negatiivisesti johtaa mallin mukaan kiinnostukseen lohkoketjuista. Muiden selittävien

muuttujien kertoimet ovat positiivisia, joten positiivinen suhtautuminen muuttujaan selittää positiivisesti kiinnostusta. Alkuperäiset regressioanalyysin tulosteet ovat liitteessä 7.

5.6 Kryptovarojen käytön tunnistetut riskit ja haasteet suomalaisissa organisaatioissa

Kryptovaluuttojen käytöstä aiheutuvia riskejä kysyttiin kuudelta kryptovaluuttojen kanssa tekemisissä olleiden organisaatioiden edustajilta. Organisaation edustajasta käytetty lyhenne ja organisaation toimiala ovat esitetty taulukossa 17. Asiantuntijaorganisaatioiden edustajien vastaukset koskien kryptovaluuttojen käytön mahdollisia riskejä ja haasteita teemoiteltiin sekä luokiteltiin neljään riskikategoriaan. Nämä riskikategoriat olivat vastausten perusteella: hinnan volatiliteetti ja markkinat, ulkoisten sidosryhmien suhtautuminen, osaaminen ja käytettävyys sekä lainsäädäntö.

Taulukko 17: Vastaajien perustiedot

Lyhenne:	Toimiala:
Henkilö A1	Kryptovaluuttojen palveluntarjoaja
Henkilö A2	Verkkokauppa
Henkilö B1	Tilitoimisto
Henkilö B2	Tilitoimisto
Henkilö C1	Asiantuntijayritys
Henkilö C2	Asiantuntijayhteisö

5.6.1 Hinnan volatiliteetti ja markkinat

Sekä henkilöiden A1 että B2 vastauksissa nousi esiin kryptovaluuttojen hinnanvaihteluista aiheutuvat riskit ja ainakin osittainen epäily markkinoiden toimivuutta kohtaan. Henkilö B2 esitti kryptovaluuttojen hinnan volatiliteetin aiheuttavan liiketoiminnallista riskiä valuuttariskin muodossa, koska veronkanto ja pankkien pitkien lainasopimuksien takaisinmaksun tapahtuvat yleensä euromääräisinä.

> B2: ” Volatiliteetti on suurin haaste. Kryptot eivät ainakaan tässä vaiheessa toimi arvon säilyttäjinä riittävän luotettavasti, että ne toisivat ennustettavuutta ja vähentäisivät liiketoimintaan liittyviä riskejä -- Veronkanto tapahtuu ainakin toistaiseksi euroissa eli niiden tilitys vaatii yrityksiä pitämään myös merkittävää eurokassaa -- tuohon veronkantoon vielä lisäyksenä myös pankkien kanssa sovitut pitkät lainasopimukset (takaisinmaksu euroissa).”

Kryptovaluuttojen tapauksessa luvussa 3.5 esitellyt vakaavaluutat ovat pyrkineet ratkaisemaan volatiliteettiin liittyviä haasteita. Vakaavaluuttojen käyttö koetaan kuitenkin vielä riskialttiiksi regulaation puutteen vuoksi.

> B2: ” Toki tässä voi ajatella myös stablecoineja, mutta niiden osalta taas haasteena on regulaation puute.”

Toisaalta henkilö A1 esitti, että vakaavaluuttojen käyttö korkotulojen kerryttämiseen olisi kuitenkin yksi suosittu kryptovaluuttoja koskeva trendi tällä hetkellä.

> A1: ”Nyt eletään aika erilaista vaihetta ja esimerkiksi maksamisen käyttötapaus ei ehkä olekaan niin relevantti kuin suojan ja hajautuksen hakeminen bitcoinin avulla tai tuottoa vakaakolikoille maksettavilla "korkotuotoilla".

Henkilö A1 nosti esiin myös kryptovaluuttamarkkinoiden sirpaleisuuden, jolla hän tarkoitti yleisesti esiintyvää huolta siitä, mistä kauppapaikalta saa parhaimman hinnan ja mihin palveluntarjoajiin voi ylipäätään luottaa. Lisäksi henkilö A1 kertoi, että monet ammattimaiset toimijat pelkäävät edelleen kryptovaluuttamarkkinoiden markkinamanipulaatiota.

5.6.2 Ulkoisten sidosryhmien suhtautuminen

Ulkoisten sidosryhmien negatiivinen suhtautuminen kryptovarojen käyttöä kohtaan nousi esiin lähes kaikkien vastaajien vastauksissa. Eniten huolta aiheutti suomalaisten finanssialan toimijoiden, kuten talletuspankkien ja maksulaitosten negatiivinen suhtautuminen kryptovaluuttoja käyttäviin yrityksiin. Henkilöt A1, B1 ja C1 kertoivat kryptovaluuttojen käytön aiheuttaneen muutamissa tapauksissa yritysten pankkitilien sulkemisen pankin toimesta tai estävän tilien avaamisen. He kommentoivat asiaa seuraavasti:

> A1: ”Pankista voi olla myös vaikea saada yritykselle pankkipalveluita, jos kryptot on jollain tavoin vahvasti näkyvillä. Pankit eivät uskalla ottaa "riskejä", koska eivät näe bitcoinissa ja kryptoissa muuta kuin negatiivisia puolia -- Yrittäjän tehtävänä ei voi olla se, että koulutetaan ja vakuutetaan pankki avaamaan peruspankkipalvelut, jos ja kun liiketoiminta on muutoin täysin laillista, mutta kryptot nyt vain syystä tai toisesta homman ytimessä tai näkyvästi esillä.”

> B1: ”Jos uusi yritys ilmoittaa pankkitiliä avatessa toimivansa kryptojen parissa niin tili tuskin avautuu. Tilejä myös suljetaan, jos kotiutuksessa käytetään suoraa siirtoa markkinapaikasta. Tilit kestävät, kun käytetään kotimaisia FIVA:n luvallisia toimijoita.”

> C1: ”Pankeilla on käytännössä valta tehdä ihan mitä haluaa ja kryptovaluutat näyttävät ainakin toistaiseksi olevan tie ongelmiin. Jotain kertoo se, että suomalainen FINANSSIVALVONNAN LISENSOIMA northcrypto.com käyttää latvialaista pankkia asiakasvaroihin.”

> C2: ”Lähinnä käytännön asioista haasteena saattaa olla yrityksen pankkitili ja sen avaaminen/ylläpitämien, mikäli on rahaliikennettä pankista kryptopörsseihin.”

Henkilö C1 kuitenkin myös täsmensi, että yritystilin avaaminen on nykyään mahdollista Finanssivalvonnan lisensoimiin suomalaisiin kryptovaluuttapörsseihin.

> C1: ”Suomalaisiin kauppapaikkoihin saa avattua yritystilin ja sieltä saa ulos kaikki tarvittavat raportit. Myös kryptovaluuttojen vastaanottoon on olemassa kolmannen osapuolen palveluita, jos ei halua ottaa kryptoja vastaan omaan lompakkoon.”

Henkilöt A1 ja C2 nostivat esille myös mahdollisten rahoittajien negatiivisen suhtautumisen kryptovaluuttojen käyttöä kohtaan. Henkilö C2 totesi, ettei kryptovaluutoille anneta vakuusarvoa, kun taas henkilö A1 kertoi, etteivät suomalaiset rahoittajat arvosta krypto-ekosysteemien, kuten DeFi:n käyttöä, mistä johtuen näiden käyttöön keskittyvät yritykset joutuvat hakemaan rahoituksen ulkomailta. Lisäksi henkilö A1 kertoi bitcoinin käyttöä koskevien ESG- ja vastuullisuuskysymysten voivan aiheuttaa haasteita.

5.6.3 Osaaminen ja käytettävyys

Vastauksissa painottui laajasti kryptovaluuttojen käyttöä koskevien standardien puuttuminen ja yleinen osaamattomuus kryptovaluuttojen käsittelyssä. Sekä henkilöt A1 että A2 arvioivat kryptovaluuttojen oikeaoppisen säilyttämisen olevan monelle yritykselle haasteellista, koska kyseistä prosessia ei ole yleisesti standardisoitu.

> A2: ”Teknisesti ei ole mitään käytännön esteitä ostaa ja pitää bitcoinia, mutta yleiset toimintatavat puuttuvat; mistä on turvallista ostaa, missä sitä säilytetään, kenellä on pääsy varoihin jne. Itsellä ei ainakaan ole tiedossa mitään alan standardia, joka on niin helppo ja selkeä, että päättäjän olisi helppo tehdä osto.”

Henkilön A1 mukaan monet ulkoistavatkin tästä johtuen kryptovaluuttojen säilytyksen usein ulkoiselle palveluntarjoajalle.

> A1: ”Epätietoisuus siitä, miten bitcoinia ja kryptoja säilytetään oikeaoppisesti, jonka ajatellaan olevan äärimmäisen vaikeaa ja hankalaa verrattuna säilytykseen vain vaihtopaikoilla tai kryptovaluuttapörsseissä.”

Toisaalta henkilö A2 kertoi, että alan palveluntarjoajat kärsivät luottamuspulasta, jonka vuoksi niitä ei uskalleta käyttää.

> A2: ”Tietämättömyyden myötä, myös käytännön luottamus alan palveluntarjoajiin on heikkoa. Esimerkiksi pankkialalla työskentelevä tuttavani ei uskaltanut käyttää (suomalainen palveluntarjoaja) ja muiden palveluita luottamuspulan vuoksi.”

Henkilö A1 arvioikin, että yksi epävarmuutta synnyttävä tekijä voi olla vertaistuen puute, koska esimerkiksi monet kryptovaluuttoihin sijoittaneet suomalaiset yritykset eivät juuri tuo asiaa julkisuuteen.

5.6.4 **Lainsäädän**tö

Vastauksissa nousi esiin useita lainsäädännöllisiä riskejä koskien verotusta, kirjanpitoa, asiakkaan tuntemista (KYC), rahanpesun estämistä (AML) ja tietosuoja-asetuksia (GDPR). Kryptovaluuttojen verotus koettiin erityisen työlääksi ja aikaa vieväksi. Myös verotuksen epäselvyys koskien spesifisempien kryptosovellusten toimintaa aiheutti huolta. Henkilöt B1, A2 ja C1 kommentoivat kryptovaluuttojen verotusta seuraavasti:

> B1: ”Kryptovaluuttaparin vaihdannassa realisoituva luovutusvoitto- tai tappio sekä sen laskenta on työlästä, joten se tuottaa ongelmia. Tämä taas tulee päätöksestä Helsingin HAO 18/0426/3.”

> A2: ”Verotuksen epäselvyys ja aggressiivisuus. Esimerkiksi Striken rakentaman teknologian hyödyntäminen Suomessa maksuliikenteessä epäilyttää itseä. Jos menet kauppaan ja ostat 2 eurolla kahvin 2 euroa vaihtuu bitcoiniksi, joka siirtyy Bitcoin-verkossa kauppiaalle ja vaihtuu takaisin 2 euroksi. Erona normaalin oli, että raha liikkui ilman välikäsiä, kauppias saa rahansa välittömästi (vrt. Visan 30 päivään) ja lähes 0 % kuluilla (vrt. 2,9 % kulut). Suomessa regulaation epäselvyys ja verotuksen aggressiivisuus rajoittaa tällaisen rakentamista, koska epäilyt herää esimerkiksi siitä, että pitäisikö kuluttajan ilmoittaa kaikki transaktiot bitcoiniin ja siitä takaisin euroihin, vaikka tähän kuluu alle 1 sekunti ja kuluttaja ei itse tiedä käyttäneensä Bitcoin-maksuverkkoa ylipäätään.”

> C1: ”Kryptovaluuttojen käyttö maksuvälineenä ei ole järkevää verotuksen puolesta Suomessa eikä missään muuallakaan, jos et ole El Salvadorissa. Koska jokainen myynti euroiksi on verotettava tapahtuma, niin valuuttana käyttö on kallista ja työlästä puuhaa.”

Myös kirjanpidon käytänteet koskien kryptovaluuttoja olivat molempien kryptovaluuttoja toiminnassaan käyttävien yritysten edustajien mielestä epäselviä.

> A1: ”…epätietoisuus verotus- ja kirjanpitokäytännöistä, koska alan ammattilaisillakaan ei välttämättä ole kovin paljon tietoa. Muun muassa raportointi on edelleen vaihtelevaa ja luotettavaa tietoa voi olla hankala hankkia.”

> A2: ”…monia askarruttaa kirjanpito ja "vakiintuneet käytännöt" siihen liittyen.”

Verotuksen ja kirjanpidon haasteiden lisäksi henkilö A2 nosti esille ongelmia koskien KYC-, AML- ja GDPR-asetuksia.

> A2: ”…toiminta kryptovaluutoilla on osoittautunut erittäin vaikeaksi: Maksupalveluntarjoajat joutuvat säilyttämään asiakastiedon (ml. henkilötiedot + public key) jokaisesta ostoksesta 5 vuotta. Verkkokauppa ei esimerkiksi pysty vastaamaan GDPR:n vaatimuksiin, sillä KYC ja AML ylikirjoittavat GDPR:n. Yleisesti nämä asettavat ku-

> luttajat suureen vaaraan … Bitcoin on alun perin tehty edistämään digitaalista kaupankäyntiä kryptaamalla ostajan ja myyjän, jolla pyritään välttämään esim. identiteetti- ja luottokorttivarkaudet. Regulaatio kuitenkin paljastaa nämä ja tekevät kuluttajasta hyvin haavoittuvaisen."

Edellä esitetyt yksityisyyttä koskevat ongelmat liittyvät siis siihen, että esimerkiksi bitcoin on luonteeltaan julkinen tilikirja, joka kuitenkin takaa anonymiteetin avulla käyttäjien yksityisyyden. Kuitenkin kun toimintaan liitetään mukaan asiakkaan tunnistusta koskevia vaatimuksia, kuten henkilötietojen säilyttäminen, niin näiden tietojen yhdistäminen julkisen tilikirjan mahdollistamaan seurantaan voivat yhdessä heikentää käyttäjän yksityisyyttä. Toisaalta KYC- ja AML-asetuksilla on tärkeä tehtävä rikollisen toiminnan, kuten rahanpesun ehkäisemisessä, mistä johtuen ongelmaan on pyritty ratkaisemaan erilaisten kompromissien avulla löytämättä kuitenkaan yleisesti kaikkia osapuolia tyydyttävää ratkaisua.

5.6.5 Koetut ja arvioidut hyödyt

Vaikka vastaajia pyydettiin tutkimuskysymykseen perustuen ensisijaisesti arvioimaan kryptovaluuttojen käyttöä koskevia riskejä ja mahdollisia haasteita suomalaisten organisaatioiden näkökulmasta, niin moni vastaaja nosti esiin myös kryptovaluuttojen käytön positiivisia puolia. Nämä nostot päätettiin myös raportoida tutkimuksen yhteydessä, sillä ne voivat auttaa hahmottamaan kryptovaluuttojen käyttökohteita juuri suomalaisten organisaatioiden näkökulmasta tarkasteltuna. Kommentit koskivat pääosin sekä kryptovaluuttojen käyttöä maksujärjestelmänä että inflaatiosuojana. Henkilö B2 esitti, että kryptovaluutat voivat tuoda etuja mantereiden väliseen maksuliikenteeseen.

> B2: "…maksuvälineenä voisi olla tosi paljon hyötyjä, jos maksuliikennettä on esim. mantereiden välillä."

Henkilö A2 näki maksuliikenteen hyötyvän mahdollisesti bitcoinin Salamaverkosta, jonka lisäksi hän piti bitcoinia mahdollisena suojana inflaatiota vastaan.

> A2: "Objektiivisesti ja jälkiviisaana ajateltuna, jokaisen talousjohtajan pitäisi tutustua bitcoiniin, sillä noussut inflaatiovauhti ja bitcoinin hinnan nousu alleviivaavat bitcoinin arvolupausta -- Lightning verkkoa ei hyödynnetä vielä laajalti. Tässä on tulossa varmasti isoja edistysaskeleita Taproot-päivityksen myötä sekä infrastruktuurin kehittyessä (esim. Strike)."

Lisäksi henkilöt C1 ja A1 nostivat esille kokemuspohjaiset näkökulmat kryptovaluuttojen käytön hyödyistä uusien asiakasryhmien houkuttelemisessa.

> C1: "Suurin kysymys on kuitenkin se, että miksi edes haluaisit luopua tuottavasta assetista kuten bitcoin ja ennemmin jättää tilillesi euroja ... Bitcoinilla maksamissa on tolkkua tällä hetkellä esim. tilanteissa, joissa voisit ostaa auton, asunnon tai vastaavan suoraan bitcoineilla eli hintaluokka kymmeniä, satoja tuhansia tai miljoonia euroja. Maailmalla on ollut useita uutisia siitä, että ihmiset ovat kotiuttaneet pörsseistä

> suuria summia pankkiin juuri esim. asunnon ostoa varten. Sen jälkeen pankki on todennut, että tämä on likaista rahaa etkä saa sillä lainaa tai uhataan tilin sulkemista. Vaikka olisikin todistusaineisto kaikista kaupoista. Tällaisissa tilanteissa voi olla siis järkeä maksaa suoraan kryptovaluutoilla ja ostaja voi jopa pyytää sitä. Tietyllä sektorilla toimiva yritys voi siis nyt ja tulevaisuudessa hyötyä siitä, jos hyväksyy bitcoinit."

> A1: "Toisaalta bitcoinilla ja kryptoilla on lukuisia myönteisiä puolia, joista olemme sekä itse hyötyneet että joista asiakkaamme hyötyvät, muun muassa uusien asiakas- ja käyttäjäryhmien houkuttelu."

Vastaava näkökulma on esitetty myös teoriaosan luvussa 3.5, jossa kerrottiin, kuinka kryptovaluutoilla maksavien asiakkaiden ostosten keskisumma oli huomattavasti suurempi kuin perinteisillä luottokorteilla maksavien asiakkaiden tekemien ostosten keskisumma. Henkilön C1 ajatus pankkien ohittamisesta suoralla kryptovaluutta-transaktioilla voi tuntua arveluttavalta toiminnalta. Merkitystä voisi kuitenkin ajatella olevan sillä, perustuuko pankkien käyttäytyminen todellisuudessa regulaatioon vai asenneilmastoon, mikäli maksaja pystyisi kuitenkin esittämään kaikki lakeihin perustuvat tarvittavat tositteet varojen alkuperästä.

5.6.6 Yhteenveto

Yhteenvetona kaikista vastauksista voitaneen todeta, että kryptovarojen käyttö voi vaikuttaa organisaation riskiympäristöön erityisesti lainsäädännön ja teknologisen osaamisen, mutta myös ulkoisten sidosryhmien suhtautumisen kautta. Lainsäädännön osalta kryptovarojen muuttuvat verotus- ja kirjanpitokäytännöt tuntuvat aiheuttavan edelleen alan vakiintuneillekin toimijoille epätietoisuuttaa. Globaalilla tasolla tulkinnat eroavat luvussa 3.6 esiteltyyn tapaan sekä sen suhteen tulisiko kryptovaluuttoja käsitellä rahoitusomaisuutena vai aineettomana pääomana että toisaalta sen suhteen tulisiko kaikkia kryptovaluuttoja tai kryptovaroja edes käsitellä samanlaisena omaisuuseränä, koska niiden toiminta voi erota fundamentaalisesti merkittävästi toisistaan. Vastaajien keskuudessa kryptovaluutoilla nähdään kuitenkin olevan suotuisia käyttökohteita nykyisten maksujärjestelmien tehostamisessa, mahdollisena pidemmän aikavälin inflaatiosuojana sekä toisaalta myös eräänlaisena brändityökaluna. Kaikki vastaukset kryptovaluuttojen käyttöä koskevista riskeistä sekä haasteista ovat esitetty tiivistetysti taulukossa 18.

Taulukko 18: Yhteenveto tulosten teemoittelusta

Hinnan volatiliteetti & markkinat	**Ulkoisten sidosryhmien suhtautuminen**	**Osaaminen & käytettävyys**	**Lainsäädäntö**
A1 & B2: Lyhyen aikavälin kurssivaihtelusta aiheutuva valuuttariski	A1, A2, B1, C1 & C2: Perinteiset finanssialan toimijat, kuten pankit suhtautuvat negatiivisesti	A1, A2 & C2: Yleinen tietämättömyys ja osaamisen puute	B1: Kryptovaluuttaparin vaihdannassa realisoituvan luovutusvoiton- tai tappion laskeminen on työlästä
B2: Verot ja lainat täytyy maksaa euroissa	C2: Kryptovaluutoille ei anneta vakuusarvoa	A1 & A2: Alan palveluntarjoajiin ei luoteta	A1 & A2: Kirjanpitoa ja verotusta koskeva ohjeistus on epäselvää
B2: Liiketoiminnan ohuen katteen suhde suureen volatiliteettiin	B1 & C1: Yritysten pankkitilejä on suljettu, kun varoja on siirretty kryptopörssistä takaisin pankkitilille	A1 & A2: Yleiset standardit puuttuvat koskien ostamista, säilyttämistä ja pääsyä varoihin	B1, A2 & C1: Valuuttana käyttäminen kallista ja työlästä johtuen aggressiivisesta verotuksesta
A1: Markkinoiden ja markkinadatan sirpaleisuus sekä pelko markkinamanipulaatiosta	A1: Bitcoinia koskevat ESG- ja muut vastuullisuuskysymykset	A2: Käyttöliittymät eivät ole vielä kovinkaan kehittyneitä	A2: KYC-, AML- ja GDPR-säännösten toteuttaminen on haastavaa

6. JOHTOPÄÄTÖKSET JA ARVIOINTI

6.1 Yhteenveto

Tutkimuksen lähtökohdat rakentuivat lohkoketjuteknologian tunnistamisesta mahdollisesti disruptiiviseksi innovaatioiksi sekä sen pohtimisesta, kuinka organisaatiot pystyisivät varautumaan lohkoketjuteknologiaan pohjautuvien sovellusten, kuten kryptovarojen, mahdolliseen yleistymiseen. Aikaisemman teorian perusteella muodostui päätelmä, että sisäisen tarkastuksen olisi mahdollista olla organisaatioiden käyttämä tukitoiminto, joka pystyisi auttamaan organisaatioita uusien disruptiivisten teknologioiden käyttöönotossa ja riskien hallinnassa (Christ ym. 2019; Lineros 2021). Myös esimerkiksi Rooney ym. (2017) olivat ehdottaneet erityisesti sisäisten tarkastajien osallistuttamista organisaatioiden lohkoketjuteknologiaan siirtymisen päätös- ja käyttöönottoprosesseihin. Lohkoketjuteknologian tutkimista sisäisen tarkastuksen kontekstissa voitiin pitää mielenkiintoisena teemana myös siksi, että lohkoketjuteknologian käytön yleistymisen on odotettu vaikuttavan sisäisten tarkastajien tulevaisuuden työtehtäviin kahdesta suunnasta. Lohkoketjuteknologiaa voidaan mahdollisesti käyttää tehokkaampien sisäisten kontrollien ja riskienhallintamenetelmien kehittämiseen, mutta toisaalta lohkoketjupohjaiset sovellukset voivat muuttaa organisaation riskiympäristöä myös negatiivisempaan suuntaan varsinkin, mikäli sovelluksien hyödyntämää teknologiaa ei ymmärretä kunnolla (Alles & Gray 2020; Burns ym. 2020; Kloch & Little 2019). Lohkoketjuteknologian ja sisäisen tarkastuksen yhteyksiä on tutkittu aikaisemmin hyvin rajallisesti niin Suomessa kuin globaalillakin tasolla. Olemassa olevaa kirjallisuutta vaikutti kuitenkin yhdistävän huoli siitä, onko sisäinen tarkastus tarpeeksi valmistautunut lohkoketjuteknologian ja kryptovarojen käytön yleistymiseen (Burns ym. 2020; Kloch & Little 2019; Lineros 2021; Rooney ym. 2017). Lisäksi aihetta läheltä sivuavissa teemoissa huolta ovat aiheuttaneet sisäisen tarkastuksen yleinen valmistautuminen disruptiviisten teknologioiden yleistymiseen sekä sisäisten tarkastajien IT-osaaminen (Cangemi 2016; Christ ym. 2019; Flora & Rai 2015; Kotb ym. 2020).

Tutkimuksen yhtenä tavoitteena oli selvittää lohkoketjuteknologian tämänhetkinen asema suomalaisten sisäisten tarkastajien työtehtävissä ja asettaa näin lähtökohdat teeman syvemmälle tarkastelulle. Sisäisille tarkastajille suunnatusta verkkokyselystä kävi ilmi, että vain joka neljännessä organisaatiossa oli vähintään keskusteltu lohkoketjuteknologian käyttömahdollisuuksista. Eli suurimman osan työyhteisöissä ei ole vielä edes keskusteltu lohkoketjuteknologian käytöstä, eivätkä sisäiset tarkastajat olleet täten juuri tarvinneet aiheeseen liittyvää osaamista työssään. Niissäkin neljänneksessä organisaatioita, joissa lohkoketjuteknologiaa oli aiheena käsitelty, sisäiset tarkastajat eivät keskimäärin olleet kokeneet tarvitsevansa lohkoketjuja koskevaa osaamista. Kyselyn tulosten mukaan Suomalaiset sisäiset tarkastajat ovat toistaiseksi kohdanneet vähemmän lohkoketjuteknologiaa työssään kuin sisäiset tarkastajat ovat kansainvälisesti kohdanneet. Kansainvälisen IIA:n 2018 sisäisille tarkastajille suunnatussa kyselyssä vastaajista 76,6 % ilmoitti, etteivät he olleet käyttäneet lohkoketjuteknologiaa edustamissaan organisaatioissa (Kloch & Little 2019), kun tässä tutkimuksessa vain noin joka kymmenes kertoi heidän organisaationsa käyttävän lohkoketjuteknologiaa.

Kyselyn perusteella niissä organisaatioissa, joissa lohkoketjuteknologiasta oli vähintään keskusteltu, vastaajat kokivat lohkoketjuteknologiaa koskevan osaamisensa olevan korkeammalla tasolla kuin organisaatioissa, joissa aiheesta ei ollut edes keskusteltu. Ero oli tuloksissa merkitsevä. Keskimääräisesti sisäiset tarkastajat kokivat lohkoketjuteknologiaa koskevan osaamisensa olevan kuitenkin melko heikkoa. Tilastollisesti merkitsevä ero näiden kahden ryhmän välillä voi kertoa toisaalta todellisesta osaamiserosta, mutta ainakin periaatteessa eron voisi aiheuttaa myös se, että aihe voi olla täysin tuntematon heille, joiden organisaatiossa ei ole käsitelty aihetta. Täysin tuntematonta aihetta koskevaa osaamista voi olla haastavaa arvioida. Niinpä aiheesta vähintään keskustelleiden kokema parempi osaaminen voi kieliä myös siitä, että he tietävät millaista osaamista heiltä vaaditaan ja kokevat täyttävänsä nämä vaatimukset, kun taas he, jotka eivät tunne aihetta eivätkä osaamisvaatimuksia arvioivat osaamistaan alakanttiin. Samankaltaisia havaintoja ovat esittäneet esimerkiksi Harrast ym. (2021), jotka havaitsivat, että ne asiantuntijat, joille kryptovarat ovat tutumpia suhtautuivat niiden aiheuttamiin riskeihin huolettomammin kuin sellaiset vastaajat, joilla ei ole kokemusta aihepiiristä. Gomaa ym. (2019) puolestaan havaitsivat tutkimuksessaan, että jo lyhyt opetus tai kokemus lohkoketjuista parantaa merkitsevästi vastaajien koettua osaamista. Näin ollen melko isoltakin vaikuttava osaamisero voi ainakin teoriassa kaventua nopeastikin, kunhan asia on vastaajille yhtä tuttu. Joka tapauksessa enemmistön kokema heikko osaaminen on linjassa aiemman IIA:n kansainvälisen kyselyn kanssa. Samassa kyselyssä havaittiin myös, että ymmärryksen ja osaamisen puute ovat suurimpana esteenä lohkoketjuteknologian kokeilulle (Kloch & Little 2019).

Mikäli lohkoketjuteknologiaan pohjautuvat sovellukset osoittautuvat käytännössä disruptiivisiksi teknologioiksi, joiden käyttö laajenee merkittävästi tulevaisuudessa, niin osaamisen ollessa heikkoa, voi sisäisen tarkastus kohdata haasteita tilanteeseen sopeutumisessa. Heiltä kuitenkin odotetaan osaamista

myös uusien teknologioiden osalta. Nimittäin IIA:n (2016) sisäisten tarkastajien pätevyyttä käsittelevä standardi 1210 velvoittaa, että sisäisellä tarkastuksella tulisi olla vähintään kollektiivisella tasolla tarvittavat tiedot, taidot ja mahdolliset muut pätevyydet ammatillisten velvoitteiden hoitamiseen myös IT-järjestelmiä koskien. Myös Popchev ym. (2021) ovat todenneet, että vaikka IT-tarkastus ei kuuluisikaan kaikkien sisäisten tarkastajien työtehtäviin, niin kaikilla sisäisillä tarkastajilla tulisi kuitenkin olla riittävä ymmärrys organisaation käyttämästä teknologiasta.

Aikaisemmissa tutkimuksissa esimerkiksi Basden ym. (2017) ja Kotb ym. (2020) on kuvanneet ”ketterän” sisäisen tarkastuksen osallistuvan muita useammin disruptiivisten innovaatioiden vaikutuksien kartoittamiseen, hallitsemiseen sekä käyttöönottoprosessiin. Lisäksi Kotb ym. (2020) painottavat että disruptiivisiin teknologioihin vastaaminen vaatii sisäiseltä tarkastukselta varhaista ja ennakoivaa osallistumista. Mielenkiintoisena huomiona tämän tutkimuksen tuloksista nousikin esille sisäisen tarkastuksen varhaisen osallistumisen merkitys lohkoketjuteknologia-osaamista selittävänä tekijänä. Tulosten perusteella uusien teknologioiden käyttöönottoon varhaisessa vaiheessa osallistuvat sisäiset tarkastajat omaavat muita parempaa osaamista lohkoketjuteknologiasta. Toisaalta osallistuminen varhaisessa vaiheessa korreloi positiivisesti myös yleisesti uusien teknologioiden tuntemuksen kanssa. Eli tuloksista voidaan tulkita, että varhaisessa vaiheessa uusien teknologioiden käyttöönottoon osallistuvilla sisäisillä tarkastajilla on yleisesti muita tarkastajia paremmat teknologiavalmiudet koskien uusia teknologioita. Sen sijaan osallistumisella varhaisessa vaiheessa uusien teknologioiden käyttöönottoon ja kiinnostuksella lohkoketjusovelluksiin ei löytynyt yhteyttä, vaan kiinnostusta selittävät muut tekijät.

Kaiken kaikkiaan vastaajat olivat melko kiinnostuneita uusista IT-teknologioista. Sen sijaan kiinnostus juuri lohkoketjuteknologiaa kohtaan oli keskinkertaista. Tuloksista kävi ilmi, että kryptovaroja koskeva kiinnostus selittää voimakkaasti myös yleisempää kiinnostusta lohkoketjuteknologiaa kohtaan. Muita kiinnostusta selittäviä tekijöitä olivat muun muassa myös työyhteisön vaatimus tutustua kyseiseen teknologiaan ja vastaajien oma uskomus, että osaamista tarvitaan tulevaisuudessa.

Sisäisten tarkastajien tulevaisuuden odotukset vaihtelivat. Usko siihen, että lohkoketjuteknologia tulee vaikuttamaan sisäiseen tarkastukseen voimakkaasti, oli vähäistä, mutta mitä pidemmäksi tarkasteluväli otettiin, sitä todennäköisempänä he pitivät lohkoketjuteknologian vaikutuksia. Tutkimuksessa tarkasteltiin sitä mitkä tekijät vaikuttavat tulevaisuuden odotuksiin viiden ja kymmenen vuoden sisällä. Viiden vuoden aikajänteellä organisaation vaikutukset näkyivät selittävissä tekijöissä, kun taas kymmenen vuoden aikajänteellä selittäjinä korostuivat muun muassa henkilökohtainen uskomus, että sisäiset tarkastajat tarvitsevat enemmän osaamista kryptovaroista ja vastaajien ikä. Lohkoketjuteknologian arveltiin yleisesti ennemmin vaikeuttavan kuin helpottavan sisäisten tarkastajien työtä tulevaisuudessa. Erot olivat kuitenkin pieniä, ja tulokseen on voinut vaikuttaa sama ilmiö kuin koettuun osaamiseen, eli uuden ja tuntemattoman asian vaikutuksiin voidaan suhtautua epäilevästi.

Kryptovarojen osalta tutkimuksessa havaittiin, että kryptovarojen käyttö voi vaikuttaa organisaation riskiympäristöön erityisesti lainsäädännön, teknologisen osaamisen, hinnan volatiliteetin sekä sidosryhmien suhtautumisen kautta. Vastaukset olivat yhteneviä esimerkiksi Vincentin ja Wilkinsin (2019) havaintojen kanssa, joiden mukaan kryptovaluuttojen käyttöä koskevat riskitekijät liittyvät tekniseen osaamiseen, kryptovaluuttojen hinnan voimakkaaseen volatiliteettiin sekä toimintaympäristön muuttuvaan regulaatioon. Vastauksista kävikin vahvasti ilmi, että jopa alan vakiintuneemmat toimijat kärsivät edelleen kryptovaluuttojen regulaatiota, erityisesti verotusta ja kirjanpitoa, koskevista epäselvyyksistä. Dyball ja Seethamraju (2021) ovatkin esittäneet, että kryptovaluuttoja käyttäviä organisaatioita leimaavat käsitykset riskialttiudesta ja valvontariskien korostumisesta johtuvat enemmänkin toimintaa ohjaavien standardien puutteesta kuin kryptovaluuttoja käyttävien organisaatioiden omasta toiminnasta. Nämä käsitykset voivat kuitenkin olla vaikuttavia osatekijöitä joidenkin ulkoisten sidosryhmien negatiivisessa suhtautumisessa kryptovarojen käyttöä kohtaan.

Ulkoisten sidosryhmien negatiivista suhtautumista kryptovarojen käyttöön voidaan pitää mielenkiintoisena havaintona, jota on käsitelty vain vähän aikaisemmissa tutkimuksissa. Pankkien negatiivinen suhtautuminen nähtiin yhtenä kryptovarojen käytön riskitekijänä. Pankkien negatiivisen suhtautumisen korostuminen voinee johtua osittain siitä, että suomalaisissa organisaatioissa kryptovarojen käyttö vaikuttaa rajautuvan suurimmaksi osaksi suuryrityksiä heikomman neuvotteluvoiman omaaviin pk-yrityksiin. Pk-yritysten pankkitilejä on kenties helpompaa yksipuolisesti sulkea ja todeta että asiakkaan on etsittävä toinen palveluntarjoaja, kun taas suuryrityksillä voi olla neuvotteluvoimaa asiassa. Vaikka Suomessa kryptovarojen käyttö suuryrityksissä ei vaikuta olevan ainakaan vielä tätä päivää, globaalilla tasolla tarkasteltuna yhä useammat suuretkin organisaatiot ovat alkaneet jo sisällyttää kryptovarojen käyttöä osaksi liiketoimintoja.

Lohkoketjuteknologian ja kryptovarojen käytön yleistyessä myös suuremmat suomalaiset organisaatiot joutuvat pohtimaan, millä tavoilla näiden innovaatioiden käytön yleistyminen saattaa vaikuttaa organisaation riskiympäristöön. Riskiympäristön kartoittamisessa voi painottua organisaatioiden laskentatoimen asiantuntijoiden sekä erityisesti varmentavien tukitoimintojen, kuten sisäisen tarkastuksen, rooli riskienhallinnan asiantuntijana. Tämän takia sisäisten tarkastajien voisi olla hyvä tutustua lohkoketjuteknologian ja kryptovarojen toimintaan vähintään ennaltaehkäisevästi jo ennen heidän edustamansa organisaation päätöstä teknologian käyttöönotosta.

Yhteenvetona voidaan todeta, että aikaisemman kirjallisuuden perusteella lohkoketjusovelluksia pidetään luonteeltaan disruptiivisina. Käytännössä vaikuttaisi kuitenkin siltä, että Suomessa lohkoketjujen leviäminen organisaatioiden käyttöön on vielä hyvin alkutekijöissä. Näin ollen innovaatiosta on toistaiseksi mahdotonta sanoa, tuleeko se olemaan todella niin disruptiivinen kuin on ennakoitu. Kuitenkin uusien teknologioiden sivuuttaminen vähäpätöisinä voi olla vahingollista ja onkin hyvä muistaa, että toimialoja mullistavat disrup-

tiiviset innovaatiot eivät ilmesty yllättäen siksi, ettei niiden olemassaolosta ole oltu tietoisia, vaan enemmänkin siksi, että niihin varautumista ei ole koettu tarpeeksi tärkeänä (Bower ja Christensen 1995).

6.2 Tutkimuksen luotettavuus

Tutkimuksia arvioidaan useimmiten validiteetin ja reliabiliteetin näkökulmista. Validiteetilla tarkoitetaan sitä, miten hyvin tutkimus mittaa tutkittavaa ilmiöitä, eli tutkiiko tutkimus sitä, mitä luvattiin – eli oliko se pätevä. Reliabiliteetti puolestaan viittaa siihen, miten toistettavia tutkimuksen tulokset ovat. Tässä luvussa pyritään esittämään lyhyesti tämän tutkimuksen luotettavuus hyödyntäen tätä pääjakoa.

Tässä tutkimuksessa kyselyn vastausmäärä jäi melko pieneksi ja aiheuttaa näin ollen omia rajoitteitaan johtopäätöksien tekoon ja tulosten yleistämiseen. Vastauksia saatiin yhteensä vain 68 kappaletta, joten tuloksia ei voida yleistää luotettavasti koskemaan koko perusjoukkoa. Sen sijaan tilastollisilla menetelmillä saavutetut tulokset kuvaavat tämän otoksen vastaajia. Tuloksia voidaan pitää kuitenkin suuntaa antavina arvioitaessa koko perusjoukkoa. Koska kysely perustui vapaaehtoisuuteen ja kokonaisvastausmäärä jäi alhaiseksi, on mahdollista, että vastauksissa korostuvat suhteessa enemmän sellaisten henkilöiden vastaukset, jotka ovat aiheesta muutenkin kiinnostuneita, kun taas sellaiset henkilöt, joille aihe on tuntemattomampi ovat voineet jättää sen vuoksi vastaamatta kyselyyn. Vastaajien taustatekijät jakautuivat paikoin hieman epätasaisesti, vajaa kolmannes vastaajista oli työskennellyt alle viisi vuotta sisäisen tarkastuksen tehtävissä, kun taas yli 20 vuotta työskennelleiden osuus jäi kuuteen prosenttiin. Kuitenkaan taustatekijöiden perusteella ei otos ole voimakkaasti vinoutunut vaan vastaajien jakautuminen kuvaa melko hyvin perusjoukkoa.

Kyselyn tulosten luotettavuuteen vaikuttaa oleellisesti myös kysymysten selkeys ja se, että vastaajat ovat ymmärtäneet kysymykset samalla tavoin. Kyselylomake pyrittiin laatimaan niin, että kysymykset ovat yksiselitteisiä ja vastaaminen ei vaadi ennakko-osaamista. Lopullista kyselylomaketta testattiin kahdella koevastaajalla ennen kyselyn lähettämistä, jotta varmistuttaisiin kysymysten ymmärrettävyydestä ja selkeydestä. Ennen kyselyn tulosten varsinaista analysointia vastaukset käytiin läpi ja tarkistettiin ettei aineistossa esiinny selkeitä epäjohdonmukaisuuksia. Tämän jälkeen siirryttiin varsinaiseen aineiston käsittelyyn, jossa muun muassa aluksi testattiin muuttujien normaalijakautuneisuutta ja valittiin menetelmät aineistolle sopivaksi. Tilastollisten menetelmien käytössä varmistettiin, että aineisto täyttää menetelmän käytön ehdot.

Laadullisen osion luotettavuuteen vaikuttavia tekijöitä voi olla tässä tutkimuksessa muun muassa sähköpostihaastatteluiden käyttö perinteisten haastatteluiden sijaan. Kuitenkin tällä tavoin tavoitettiin suurin osa suomalaisista asiantuntijaorganisaatioista, jotka toimivat avoimesti kryptovarojen parissa. Vastauksissa toistuivat vahvasti samat asiat ja teemat, joten tuloksien voidaan katsoa olevan kattavat. Tuloksia tulkittaessa on kuitenkin hyvä huomata, että

vastaajat ovat oman alansa asiantuntijoita, eivät sisäisiä tarkastajia. Tutkimuskysymyksen kannalta olisi ollut mielenkiintoista haastatella myös sisäistä tarkastajaa, jolla on kokemusta aiheesta. Se ei kuitenkaan ollut mahdollista sillä tällaisia tarkastajia on erittäin vähän, eikä käytössä olevin resurssein ollut mahdollisuutta tällaista tarkastajaa löytää haastateltavaksi.

6.3 Jatkotutkimusaiheet

Lohkoketjuteknologiaa koskeva tutkimus keskittyy tällä hetkellä pitkälti lohkoketjuteknologian mahdollisten käyttökohteiden kartoittamiseen. Tutkimukset vaikuttaisivat keskittyvän erityisesti finanssialan sovelluksiin, mutta myös taloushallintoa koskevia sovelluskohteita, kuten kirjanpitoa ja toimitusketjuja koskeva tutkimus on korostuneessa asemassa lohkoketjuteknologiaa käsittelevissä julkaisuissa. Lohkoketjuteknologian laajempi hyödyntäminen eri taloushallinnon sovelluksissa voi johtaa uusien paradigmojen muodostumiseen useissa kirjanpitoa jollakin tapaa sivuavissa työtehtävissä, kuten sisäisessä ja ulkoisessa tarkastuksessa. Nykyisessä tutkimuksessa painottuu erityisesti niin sisäisten tarkastajien kuin myös kaikkien laskentatoimen erityisasiantuntijoiden IT-taitojen tärkeys lohkoketjuteknologiaa koskevissa ammatillisissa valmiuksissa. Erityisesti yksityiskohtaisempiin taitoihin keskittyvää tutkimusta ei kuitenkaan ole juuri tarjolla. Jatkotutkimuskohteiksi voidaankin ehdottaa sekä tarkempaa lohkoketjuteknologian käytön vaatimien erityistaitojen selvittämistä että selvittämistä keinoista, joilla nämä taidot olisi opetettavissa tehokkaasti kaikille lohkoketjuteknologian parissa työskenteleville laskentatoimen asiantuntijoille.

Toinen mielenkiintoinen konseptuaalinen jatkotutkimusaihe olisi sisäisen tarkastuksen hyödyntäminen yhtenä solmuna eli noodina organisaation tai organisaatioiden välisen konsortion lohkoketjujärjestelmässä. Monissa varsinkin keskitetymmissä lohkoketjujärjestelmissä noodit nimittäin käytännössä hoitavat monia sisäisille tarkastajille ominaisia tehtäviä. Tätä aihetta on hieman jo tutkittu ulkoisen tarkastuksen näkökulmasta siten, että tilintarkastusta suorittava taho toimisi lohkoketjujärjestelmän yhtenä noodina ja järjestelmän auditointi tapahtuisi reaaliaikaisesti ympäri tilikauden. Sisäisen tarkastuksen kohdalla tätä aihetta koskevaa tutkimusta ei vaikuttaisi kuitenkaan löytyvän vielä laisinkaan.

Kryptovarojen suhteen monet erityisesti suomalaisten organisaatioiden kokemat nykyiset koetut ongelmat vaikuttaisivat johtuvan epäselvyyksistä lainsäätäjän, kryptovaluuttoja käyttävän organisaation sekä tätä tiukemmin säädeltyjen finanssialan toimijoiden välillä. Kryptovarojen jalkautuessa laajempaan käyttöön, jatkotutkimusaiheeksi voitaisiin ehdottaa sen selvittämistä, millaisilla järjestelyillä, koskien muun muassa KYC-, AML- ja GDPR-vaatimuksia, nämä kaikki kolme osapuolta pystyisivät toimimaan tehokkaammin yhdessä lisäarvoa kaikille tuottavilla tavoilla. Yleisemminkin voidaan todeta, että sekä lohkoketjuteknologian että kryptovarojen käyttöön ei ole olemassa vielä yleisesti hyödynnettäviä standardeja, joita sisäiset tarkastajat sekä laajemminkin talous-

hallinnon ammattilaiset voisivat hyödyntää. Näiden standardien kehitystä koskevaan tutkimukseen kaivattaisiin sekä lohkoketjukehittäjien että laskentatoimen erityisasiantuntijoiden poikkitieteellistä yhteistyötä.

LÄHTEET

Adams, M. B. (1994). Agency Theory and the Internal Audit. Managerial Auditing Journal, 9(8), 8–12. https://doi.org/10.1108/02686909410071133

Alles, M., & Gray, G. L. (2020). "The first mile problem": Deriving an endogenous demand for auditing in blockchain-based business processes. International Journal of Accounting Information Systems, 38, 100465. https://doi.org/10.1016/j.accinf.2020.100465

Anderson, U. (2003). Assurance and Consulting services. Chapter 4. 1. painos. Internal Audit Research Foundation.

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 1. painos. O'Reilly Media, Inc.

Arla. (2018). Arla Maitoketju, maidontuotannon lohkoketju — Tarinoita Sipoosta. https://www.arla.fi/artikkelit/arla-maitoketju-lapivalaisee-maidon-valmistusketjun/

Basden, K., Torcasi, S., Mack, D., & Kristall, M. (2017). State of the Internal Audit Profession Study. Staying the course toward True North: Navigating disruption. PricewaterhouseCoopers. https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/2017_State_of_the_Internal_Audit_Profession_Study.pdf

Bashir, I. (2017). Mastering Blockchain. 1. painos. Packt Publishing Ltd.

Bitcoinkeskus. (2020). Ethereumin haastajat platform-kisassa. Bitcoinkeskus. https://bitcoinkeskus.com/ethereumin-haastajat-platform-kisassa/

BitPay. (2022). What is a Multisignature (Multisig) or Shared Wallet? BitPay Support. https://support.bitpay.com/hc/en-us/articles/360032618692-What-is-a-Multisignature-Multisig-or-Shared-Wallet-

Blockchain.com. (2021). Confirmed Transactions Per Day. Blockchain.Com. https://www.blockchain.com/charts/n-transactions?timespan=all&format=json

Bower, J. L., & Christensen, C. M. (1995). Disruptive Technologies: Catching the Wave. Harvard Business Review 73 (1), 43–53. https://doi.org/10.1016/0024-6301(95)91075-1

Bueno, T., Morais, E., Fernandes, L., Righi, R., & Alberti, A. (2020). Blockchain and Industry 4.0: Overview, Convergence, and Analysis. In Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment. 27–58. Springer. https://doi.org/10.1007/978-981-15-1137-0_2

Bullmann, D., Klemm, J., & Pinna, A. (2019). In Search for Stability in Crypto-Assets: Are Stablecoins the Solution? ECB Occasional Paper No. 230. SSRN Scholarly Paper ID 3444847. https://papers.ssrn.com/abstract=3444847

Burns, J., Steele, A., Cohen, E. E., & Ramamoorti, S. (2020). Blockchain and Internal Control — The COSO perspective. https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf

Cai, C. (2019). Triple-entry accounting with blockchain: How far have we come? Accounting & Finance, 61 (2), 71–93. https://doi.org/10.1111/acfi.12556

Casey, Michael. J., & Vigna, P. (2018). In blockchain we trust. MIT Technology Review. https://www.technologyreview.com/2018/04/09/3066/in-blockchain-we-trust/

Castillo, M. del. (2016). Ethereum Executes Blockchain Hard Fork to Return DAO Funds. https://www.coindesk.com/tech/2016/07/20/ethereum-executes-blockchain-hard-fork-to-return-dao-funds/

Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., & Secundo, G. (2021). Blockchain technology design in accounting: Game changer to tackle fraud or technological fairy tale? Accounting, Auditing & Accountability Journal. https://doi.org/10.1108/AAAJ-10-2020-4994

Christ, M. H., Eulerich, M., & Wood, D. A. (2019). Internal Auditors' Response to Disruptive Innovation. The Internal Audit Foundation. ISBN-13: 978-1-63454-062-9

Cimaglia, M. (2022). Web3 Is the Future of the Creator Economy. Entrepreneur. https://www.entrepreneur.com/article/403948

Coinbase. (2022). About—Coinbase. https://Www.Coinbase.Com/About. https://www.coinbase.com/about

COSO. (2013). Internal Control—Integrated Framework Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

COSO. (2017). Enterprise Risk Management Integrating with Strategy and Performance Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/documents/2017-coso-erm-integrating-with-strategy-and-performance-executive-summary.pdf

Coyne, J. G., & McMickle, P. L. (2017). Can Blockchains Serve an Accounting Purpose? Journal of Emerging Technologies in Accounting, 14(2), 101–111. https://doi.org/10.2308/jeta-51910

de Winter, J. C. F., Gosling, S. D., & Potter, J. (2016). Comparing the Pearson and Spearman correlation coefficients across distributions and sample sizes: A tutorial using simulations and empirical data. Psychological Methods, 21(3), 273–290. https://doi.org/10.1037/met0000079

Deloitte. (2018). Auditing the Risks of Disruptive Technologies. Internal Audit in the age of digitalization. https://www2.deloitte.com/us/en/pages/advisory/articles/internal-audit-anticipating-risk-of-new-technology.html

Deloitte. (2019). An internal auditor's guide to blockchain: Blurring the line between physical and digital. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-blockchain-for-internal-auditors.pdf

Deloitte. (2021). The Business Benefit of Using Cryptocurrency. https://www2.deloitte.com/us/en/pages/audit/articles/corporates-using-crypto.html

Drath, R., & Horch, A. (2014). Industrie 4.0: Hit or Hype? [Industry Forum]. IEEE Industrial Electronics Magazine, 8(2), 56–58. https://doi.org/10.1109/MIE.2014.2312079

Dutta, S. K. (2020). The Definitive Guide to Blockchain for Accounting and Business: Understanding the Revolutionary Technology. Emerald Publishing Limited. https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=6354162

Dyball, M. C., & Seethamraju, R. (2021). The impact of client use of blockchain technology on audit risk and audit approach—An exploratory study. International Journal of Auditing, 25(2), 602–615. https://doi.org/10.1111/ijau.12238

Ethereum Foundation. (2022). Non-fungible tokens (NFT). Ethereum.Org. https://ethereum.org

Euroopan keskuspankki. (2019). Crypto-assets – trends and implications. European Central Bank. https://www.ecb.europa.eu/paym/intro/mip-online/2019/html/1906_crypto_assets.fi.html

Faccia, A., & Petratos, P. (2021). Blockchain, Enterprise Resource Planning (ERP) and Accounting Information Systems (AIS): Research on e-Procurement and System Integration. Applied Sciences, 11(15), 6792. https://doi.org/10.3390/app11156792

Finanssivalvonta. (2019a). Finanssivalvonta myönsi viidelle virtuaalivaluutan tarjoajalle rekisteröinnin – valvonnan tavoitteena on rahanpesun estäminen. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2019/finanssivalvonta-myonsi-viidelle-virtuaalivaluutan-tarjoajalle-rekisteroinnin--valvonnan-tavoitteena-on-rahanpesun-estaminen2/

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

Flora, P., & Rai, S. (2015). Navigating Technology's Top 10 Risks—Internal Audit's Role. The Global Internal Audit Common Body of Knowledge. https://www.iia.nl/SiteFiles/Publicaties/Navigating%20Technology's%20Top%2010%20Risks%20_Small.pdf

Friedman, M. (1999). Mr. Market. Hoover Institution. https://www.hoover.org/research/mr-market

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. International Journal of Information Management, 51(102029). https://doi.org/10.1016/j.ijinfomgt.2019.10.014

Gartner. (2021). Gartner Says 20% of Large Enterprises Will Use Digital Currencies by 2024. https://www.gartner.com/en/newsroom/press-

releases/2021-12-16-gartner-says-20-percent-of-large-enterprises-will-use-digital-currencies-by-2024

Gomaa, A. A., Gomaa, M. I., & Stampone, A. (2019). A Transaction on the Blockchain: An AIS Perspective, Intro Case to Explain Transactions on the ERP and the Role of the Internal and External Auditor. Journal of Emerging Technologies in Accounting, 16(1), 47–64. https://doi.org/10.2308/jeta-52412

Grassi, L., Lanfranchi, D., Faes, A., & Renga, F. M. (2022). Do we still need financial intermediation? The case of decentralized finance – DeFi. Qualitative Research in Accounting & Management. https://doi.org/10.1108/QRAM-03-2021-0051

Grigg, I. (2005). Triple Entry Accounting. https://doi.org/10.13140/RG.2.2.12032.43524

Grym, A. (2018). Kryptovarat eivät ole rahaa. Euro ja talous. https://www.eurojatalous.fi/fi/blogit/2018/kryptovarat-eivat-ole-rahaa/

Harrast, S. A., Mcgilsky, D., & Sun, Y. (2021). Determining the Inherent Risks of Cryptocurrency: A Survey Analysis. Current Issues in Auditing. https://doi.org/10.2308/CIIA-2020-038

Hayek, F. A. von. (1990). Denationalisation of money: The argument refined ; an analysis of the theory and practice of concurrent currencies. 3. painos. The Institute of Economic Affairs.

Hayes, A. (2022). Blockchain Explained. Investopedia. https://www.investopedia.com/terms/b/blockchain.asp

Helsingin HAO. 6.7.2018. 18/0426/3. Ennakkoratkaisu: https://oikeus.fi/hallintooikeudet/helsinginhallinto-oikeus/fi/index/hallintooikeusratkaisut/1530879000488.html

HMRC. (2021). CRYPTO10100—Cryptoassets Manual. HM Revenue & Customs. https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100

Hon, H., Wang, K., Bolger, M., Wu, W., & Zhou, J. (2022). Crypto Market Sizing Global Crypto Owners Reaching 300M. Crypto.com. https://crypto.com/research/2021-crypto-market-sizing-report-2022-forecast/

Ibañez, J. I., Bayer, C. N., Tasca, P., & Xu, J. (2021). Triple-entry Accounting, Blockchain and Next of Kin: Towards a Standardization of Ledger Terminology. https://doi.org/10.2139/ssrn.3760220

IRFS-Committee. (2019). IFRS - Tentative Agenda Decision and comment letters—Holdings of Cryptocurrencies. https://www.ifrs.org/projects/completed-projects/2019/holdings-of-cryptocurrencies/tad-holdings-of-cryptocurrencies/

Ito, J., Narula, N., & Ali, R. (2017). The Blockchain Will Do to the Financial System What the Internet Did to Media. Harvard Business Review. https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

Javaid, M., Haleem, A., Pratap Singh, R., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. Blockchain: Research and Applications, 2(4), 100027. https://doi.org/10.1016/j.bcra.2021.100027

Jiang, L., Messier, W. F., & Wood, D. A. (2020). The Association between Internal Audit Operations-Related Services and Firm Operating Performance. Auditing: A Journal of Practice & Theory, 39(1), 101–124. https://doi.org/10.2308/ajpt-52565

Kaikkonen, H., & Wang, S. (2021). Mitä ovat NFT:t ja mikä on niiden merkitys tekijänoikeuden tai sopimusten kannalta? Alma Talent Pro. https://pro.almatalent.fi/article/mita-ovat-nftt-ja-mika-on-niiden-merkitys-tekijanoikeuden-tai-sopimusten-kannalta-2/18323

Kari, J. (2021). NFT - ihmiskunnan tuho vai tulevaisuus? Jussi Karin blogi. https://www.jussikari.fi/nft-ihmiskunnan-tuho-vai-tulevaisuus/

Kauko, K. (2020). Mitä on fiat-raha? Euro ja talous. https://www.eurojatalous.fi/fi/blogit/2020/mita-on-fiat-raha/

Kela. (2019). The Social Insurance Institution of Finland to test a new type of digital smart money—Press releases. https://www.kela.fi/in/web/en/press-releases-media/-/asset_publisher/iOlErAd3fOTY/content/the-social-insurance-institution-of-finland-to-test-a-new-type-of-digital-smart-money

Kloch, R., & Little, S. (2019). Blockchain and Internal Audit. Internal Audit Foundation, 1–20. ISBN-13: 978-1-63454-065-0

KHO 26.9.2006/2469. Korkeimman hallinto-oikeuden ratkaisuja: https://finlex.fi/fi/oikeus/kho/lyhyet/2006/200602469

Kotb, A., Elbardan, H., & Halabi, H. (2020). Mapping of internal audit research: A post-Enron structured literature review. Accounting, Auditing & Accountability Journal, 33(8), 1969–1996. https://doi.org/10.1108/AAAJ-07-2018-3581

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. WEIS 2013. http://www.infosecon.net/workshop/downloads/2013/pdf/The_Economics_of_Bitcoin_Mining,_or_Bitcoin_in_the_Presence_of_Adversaries.pdf

Lacalle, D. (2021). Eurozone inflation is high when it comes to the prices of daily purchases. https://www.dlacalle.com/en/eurozone-inflation-is-high-when-it-comes-to-the-prices-of-daily-purchases/#more-12084

Laki 18.7.2008/521 Vakuutusyhtiölaki. FINLEX ® - Ajantasainen lainsäädäntö: https://www.finlex.fi/fi/laki/ajantasa/2008/20080521

Laki 21.7.2006/624 Osakeyhtiölaki. FINLEX ® - Ajantasainen lainsäädäntö: https://www.finlex.fi/fi/laki/ajantasa/2006/20060624

Laki 24.6.1968/360 Laki elinkeinotulon verottamisesta. FINLEX ® - Ajantasainen lainsäädäntö: https://www.finlex.fi/fi/laki/ajFantasa/1968/19680360

Laki 30.12.1992/1535 Tuloverolaki. FINLEX ® - Ajantasainen lainsäädäntö: https://www.finlex.fi/fi/laki/ajantasa/1992/19921535#O4P110

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382–401. https://doi.org/10.1145/357172.357176

Lee, L., Fiedler, K., & Mautz, R. (2018). Internal Audit and the BLOCKCHAIN: There's more to blockchain than bitcoin, and auditors have much to learn about how it works. Internal Auditor, 75(4), 41–45. https://link.gale.com/apps/doc/A551669460/AONE?u=anon~b301dd84&sid=googleScholar&xid=62e60437

Leppänen, M. (2018). Pankit sulkivat suomalaisen bitcoin-välittäjän tilejä – ”Olemme melkein pankkisaarrossa”. Yle Uutiset. https://yle.fi/uutiset/3-10094597

Lightning.network. (2022). The Bitcoin Lightning Network. https://lightning.network/lightning-network-summary.pdf

Lineros, J. V. (2021). IT Governance Considerations for Permissioned Blockchains. Journal of Emerging Technologies in Accounting, 18(1), 45–59. https://doi.org/10.2308/JETA-19-12-01-49

Liu, R. (2020). A Preliminary Study of the Impact of Blockchain Technology on Internal Auditing. 2020 2nd International Conference on Applied Machine Learning (ICAML), 286–293. https://doi.org/10.1109/ICAML51583.2020.00066

Lähitapiola. (2021). Enemmän kuin joka kymmenes suomalainen harkitsee sijoittamista bitcoiniin – hyvät tuottonäkymät houkuttelevat. https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/uutiset-ja-tiedotteet/uutiset/uutinen/1509572274155

Maiti, M., Kotliarov, I., & Lipatnikov, V. (2021). A future triple entry accounting framework using blockchain technology. Blockchain: Research and Applications, 2(4), 1–8. https://doi.org/10.1016/j.bcra.2021.100037

Mallers, J. (2021). Announcing the Strike API. Medium. https://jimmymow.medium.com/announcing-the-strike-api-c18a4e9c54de

Mattila, J., Laikari, A., Markkanen, K., Koulu, R., & Jia, K. (2019). Lohkoketjuteknologian hyödyntämismahdollisuudet palkkatulojen verotuksessa. Prime Minister's Office Finland. http://urn.fi/URN:ISBN:978-952-287-733-8

Meho, L. I. (2006). E-mail interviewing in qualitative research: A methodological discussion. Journal of the American Society for Information Science and Technology, 57(10), 1284–1295. https://doi.org/10.1002/asi.20416

Metsämuuronen, J. (2011). Tutkimuksen tekemisen perusteet ihmistieteissä 2, opiskelijalaitos. International Methelp Oy.

Moore, B. (2020). Internal Controls in Blockchain and Digital Assets Transactions. International Federation of Accountants, 35–43. https://www.ifac.org/system/files/uploads/gateway/Crypto%20Assets%20Webinar%20Slide%20Deck%20v.6_FINAL.pdf

Morris, N. (2018). Will blockchain disrupt SAP? Ledger Insights - Enterprise Blockchain. https://www.ledgerinsights.com/blockchain-disrupt-sap/

Nascimento, S., Pólvora, A., & Lourenço, J. S. (2018). #Blockchain4EU: Blockchain for industrial transformations. Publications Office of the European Union. https://data.europa.eu/doi/10.2760/410134

Niemi, P. (2018). Sisäinen tarkastus käytännössä. 1. painos. Alma Talent Oy. nhttps://verkkokirjahylly.almatalent.fi/teos/BAXBBXATEBEED

Nokia. (2021). Nokia launches blockchain-powered Data Marketplace for secure data trading and AI models. Nokia. https://www.nokia.com/about-us/news/releases/2021/05/05/nokia-launches-blockchain-powered-data-marketplace-for-secure-data-trading-and-ai-models/

O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. Intelligent Systems in Accounting, Finance and Management, 24(4), 138–147. https://doi.org/10.1002/isaf.1417

Ozeran, A., Gura, N., Gura, N., & Taras Shevchenko National University of Kyiv. (2020). Audit and accounting considerations on cryptoassets and related transactions. Economic Annals-XXI, 184(7–8), 124–132. https://doi.org/10.21003/ea.V184-11

Pierre, E. (2019). ABC's Internal Control Working Group Releases Industry-First Blockchain Risk Assessment And Mitigation Tool. Accounting Blockchain Coalition. https://accountingblockchain.net/abcs-internal-control-working-group-releases-industry-first-blockchain-risk-assessment-and-mitigation-tool/

Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 1–59. https://lightning.network/lightning-network-paper.pdf

Popchev, I., Radeva, I., & Velichkova, V. (2021). The impact of blockchain on internal audit. 2021 Big Data, Knowledge and Control Systems Engineering, 1–8. https://doi.org/10.1109/BdKCSE53180.2021.9627276

Popescu, A.-D. (2021). Non-Fungible Tokens (NFT)—Innovation beyond the craze. Proceedings of Engineering & Technology Journal, 66, 26–30.

Pozsar, Z. (2022). Bretton Woods III. Credit Suisse Economics. https://plus2.credit-suisse.com/content/dam/credit-suisse-research/SearchPDF?DocumentID=1191091&DocumentType=NR%20Publication&documentClick=true&AuthRequired=true&tagFormat=PDF#toolbar=0&navpanes=0&pagemode=none&zoom=FitH

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate Accounting & Finance, 31(2), 21–28. https://doi.org/10.1002/jcaf.22415

Ratsula, N. (2017). Yrityksen sisäinen valvonta. Edita. ISBN: 978-951-37-7167-6

Research and Markets. (2021). Global Blockchain Market Report 2021. https://www.researchandmarkets.com/reports/5025113/blockchain-market-with-covid-19-impact-analysis

Robert, J., Kubler, S., & Ghatpande, S. (2020). Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems. Future Generation Computer Systems, 112, 283–296. https://doi.org/10.1016/j.future.2020.05.033

Rooney, H., Aiken, B., & Rooney, M. (2017). Q&A. Is Internal Audit Ready for Blockchain? Technology Innovation Management Review, 7, 41–44. https://doi.org/10.22215/timreview/1113

Roussy, M., & Perron, A. (2018). New Perspectives in Internal Audit Research: A Structured Literature Review. Accounting Perspectives, 17(3), 345–385. https://doi.org/10.1111/1911-3838.12180

Roussy, M., & Rodrigue, M. (2018). Internal Audit: Is the 'Third Line of Defense' Effective as a Form of Governance? An Exploratory Study of the Impression Management Techniques Chief Audit Executives Use in Their Annual Accountability to the Audit Committee. Journal of Business Ethics, 151(3), 853–869. https://doi.org/10.1007/s10551-016-3263-y

Sarwar, M. I., Iqbal, M. W., Alyas, T., Namoun, A., Alrehaili, A., Tufail, A., & Tabassum, N. (2021). Data Vaults for Blockchain-Empowered Accounting Information Systems. IEEE Access, 9, 117306–117324. https://doi.org/10.1109/ACCESS.2021.3107484

Savin, N. E., & White, K. J. (1977). The Durbin-Watson test for serial correlation with extreme sample sizes or many regressors. Econometrica, 45(8), 1989-1996. https://EconPapers.repec.org/RePEc:ecm:emetrp:v:45:y:1977:i:8:p:1989-96

Schwab, K. (2016). The Fourth Industrial Revolution: What it means and how to respond. World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Economic Research - Federal Reserve Bank of St. Louis, 103(2). https://doi.org/10.20955/r.103.153-74

Seago, J. (2015). Delivering on the Promise Measuring Internal Audit Value and Performance 1–24. The Global Internal Audit Common Body of Knowledge. https://www.iia.nl/SiteFiles/Publicaties/CBOK_Delivering_on_the_Promise.pdf

Selgin, G. (2015). Synthetic commodity money. Journal of Financial Stability, 17, 92–99. https://doi.org/10.1016/j.jfs.2014.07.002

Shrestha, N. (2020). Detecting multicollinearity in regression analysis. American Journal of Applied Mathematics and Statistics, 8(2), 39-42.

Singer, M. (2020). Crypto-Assets: Overview of Use Case Traction – Accounting, Assurance, Tax and Internal Control Implications. Accounting Blockchain Coalition, 5–23. https://www.ifac.org/system/files/uploads/gateway/Crypto%20Assets%20Webinar%20Slide%20Deck%20v.6_FINAL.pdf

Sintonen, E. (2017). Sisäisen tarkastuksen uudistuttava voimakkaasti. PwC:n Uutishuone. https://uutishuone.pwc.fi/sisaisen-tarkastuksen-uudistuttava-voimakkaasti

Sisäiset tarkastajat ry. (2022a). Ammatillinen ohjeistus. https://theiia.fi/sisainen-tarkastus/ammatillinen-ohjeistus/

Sisäiset tarkastajat ry. (2022b). Standardit. Sisäiset tarkastajat ry. https://theiia.fi/sisainen-tarkastus/ammatillinen-ohjeistus/standardit/

Sisäiset tarkastajat ry. (2022c). Sisäiset tarkastajat ry—Toiminta. Sisäiset tarkastajat ry. https://theiia.fi/yhdistys/

Smith, A. (2021). How Did the Field of Accounting Evolve? Investopedia. https://www.investopedia.com/articles/08/accounting-history.asp

S-ryhmä. (2018). Kuhatutka jäljittää kotimaisen kalan alkuperän. https://s-ryhma.fi/uutinen/-/news-4593888_384136

Swyftx Learn. (2022). What is The Blockchain Trilemma? | Swyftx Learn. Learn. https://learn.swyftx.com/blockchain/blockchain-trilemma/

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

Tanninen, T. (2021). Virtuaalivaluutan liikkeeseenlasku edellyttää lupaa Finanssivalvonnalta – keskiössä asiakkaansuoja ja rahanpesun estäminen. www.finanssivalvonta.fi. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2021/virtuaalivaluutan-liikkeeseenlasku-edellyttaa-lupaa-finanssivalvonnalta--keskiossa-asiakkaansuoja-ja-rahanpesun-estaminen/

The Institute of Internal Auditors. (2016). International Standards for the Professional Practice of Internal Auditing (Standards). The Institute of Internal Auditors. https://www.theiia.org/globalassets/documents/standards/standards-2017/ippf-standards-2017-english.pdf

Tieto. (2018). Listaamattomien osakkeiden kaupankäynti digitalisoidaan lohkoketjun avulla. https://www.tietoevry.com/fi/uutishuone/kaikki-uutiset-ja-tiedotteet/tiedotteet/2018/11/asiakastieto-nordea-op-ryhma-privanet-ja-tieto-digitalisoivat-listaamattomien-osakkeiden-kaupankaynnin-ja-osakashalli/

Tikhomirov, S., Moreno-Sanchez, P., & Maffei, M. (2020). A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network. 2020 IEEE European Symposium on Security and Privacy Workshops, 387–396. https://doi.org/10.1109/EuroSPW51379.2020.00059

Tähtinen, J., Laakkonen, E., & Broberg, M. (2020). Tilastollisen aineiston käsittelyn ja tulkinnan perusteita. 2. painos. Turun yliopiston kasvatustieteiden laitos. https://www.utupub.fi/handle/10024/149687

Vaivio, J. & Sirén, A. (2010). Insights into method triangulation and "paradigms" in interpretive management accounting research. Management Accounting Research, 21(2), 130-141. https://doi.org/10.1016/j.mar.2010.03.001

Verohallinto. (2020). Virtuaalivaluuttojen verotus—Vero.fi. https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen-verotus3/

Vilkka, H. (2007). Tutki ja mittaa: Määrällisen tutkimuksen perusteet. Tammi. ISBN 978-952-03-0099-9

Vincent, N. E., & Wilkins, A. M. (2019). Challenges when Auditing Cryptocurrencies. Current Issues in Auditing, 14(1), A46–A58. https://doi.org/10.2308/ciia-52675

VISA. (2022). Visa Study: Small Businesses Optimistic, Looking to Digital Payments for Growth in New Year. https://usa.visa.com/about-visa/newsroom/press-releases.html

Weingärtner, T. (2019). Tokenization of physical assets and the impact of IoT and. European Union Blockchain Observatory and Forum, 10, 1–16. https://www.eublockchainforum.eu/sites/default/files/research-paper/convergence_of_blockchain_ai_and_iot_academic_2.pdf

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. Journal of Financial Regulation, 6(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

LIITE 1. KRYPTOVAROJEN VEROTUS

Kryptovarat voivat näyttäytyä yritysten toiminnassa eri tavoin ja tällä on vaikutuksia verotukseen. Toiset yritykset voivat esimerkiksi vastaanottaa kryptovaroja maksuna hyödykkeistä, kun taas jonkun toisen yrityksen päätoimialaa voi olla kryptovarojen välittäminen ja kaupankäynti tai toimiminen kryptovaluuttojen louhijana. Tässä tutkielmassa kuitenkin keskitytään tarkastelemaan suomalaisia organisaatioita, joiden päätoimialaa eivät ole kryptovaluuttojen louhinta tai niiden välittäjänä toimiminen, joten näiden osalta verotusta käsitellään hyvin pintapuolisesti.

Verohallinnon (2020) ohjeessa annetaan kattava kuva virtuaalivaluuttojen, joihin kryptovaluutat kuuluvat, verotuskohtelusta erilaisissa yleisimmissä tilanteissa. Pääsääntö on että, virtuaalivaluuttojen arvonmuutos realisoituu aina virtuaalivaluuttojen vaihdantatilanteessa. Arvonmuutoksen realisoitumiseen ei vaikuta se, vaihdetaanko virtuaalivaluutta A:ta toiseksi virtuaalivaluutaksi vai viralliseen valuuttaan. Käytännössä arvonmuutosta verrataan kuitenkin aina suhteessa euromääräiseen hintaan, eli myös virtuaalivaluutta - virtuaalivaluutta vaihdantatilanteessa joudutaan määrittämään ja kirjaamaan ylös euromääräinen voitto tai tappio, joka vaihdannasta syntyy. (HAO 2018; Verohallinto 2020.) Arvonnousu on puolestaan yrityksille aina veronalaista tuloa ja tulon hankkimisesta sekä säilyttämisestä aiheutuneet kustannukset vähennyskelpoisia. Arvonalentumiset voivat puolestaan olla vähennyskelpoisia elinkeinotoiminnan tulolähteestä. Vähennyskelpoisuuteen vaikuttaa omaisuuslaji (rahoitus-, vaihto-, sijoitus- ja käyttöomaisuus), johon virtuaalivaluutta luokitellaan. (Verohallinto 2020.)

Sijoitustoimintaa, jossa virtuaalivaluuttaa myydään ja ostetaan aktiivisesti, tavoitteellisesti ja voittoa tavoitellen pidetään Verohallinnon ohjeen mukaisesti EVL 1 §:n 1 momentin mukaisena elinkeinotoimintana. Myös muun elinkeinotoiminnan ohessa suoritettava aktiivinen sijoitustoiminta voidaan luokitella elinkeinotoiminnaksi, eli virtuaalivaluutoilla tehtävä kaupankäynti ei tarvitse olla niin sanottu päätoimiala. Elinkeinotoiminnan tunnusmerkistön täyttyessä virtuaalivaluutat luokitellaan yrityksen vaihto-omaisuuteen. (Verohallinto 2020.) Vaihto-omaisuuden arvonlasku on vähennyskelpoista suoraan tulosta (EVL 8.1 §; EVL 28 §). Vaihto-omaisuuteen kuuluvien kryptovaluuttojen hankintamenon suuruuden määrittelyyn käytetään oletuksena FIFO-periaatetta (EVL 14.2 §) ellei verovelvollinen pysty osoittamaan todellista hankintamenoa. LIFO-periaatteen käyttö ei ole mahdollista virtuaalivaluuttojen hankintamenon määrityksessä (KHO 2006/2469; Verohallinto 2020).

Tilapäisesti varojen sijoittaminen virtuaalivaluuttaan on myös mahdollista ilman aktiivista kaupankäyntiä. Tällöin nämä varat kuuluvat verohallinnon ohjeen (2020) mukaan rahoitusomaisuuteen. Suoritemyynnistä, jossa maksuna vastaanotetaan virtuaalivaluuttaa, saatu tulo kuuluu myös pääsääntöisesti rahoitusomaisuuteen. Rahoitusomaisuuteen kuuluvan erän arvonlasku on vähennyskelpoista suoraan tulosta (EVL 8.1.1 §; EVL 17.1.2 §). Rahoitusomaisuuteen kuuluvien erien hankintamenon määrittämiseen ei ole erityisiä säännöksiä,

vaan hankintameno määritetään todellisen hankintamenon mukaisesti (Verohallinto 2020).

Mikäli virtuaalivaluutalla tehtävä kaupankäynti ei täytä elinkeinotoiminnan tunnusmerkkejä tapahtuu verotus TVL:n mukaan samoin kuin yksityishenkilöilläkin. Yksityishenkilöille kuuluvia etuoikeuksia, verovapaat pienet luovutusvoitot ja hankintameno-olettama, yritys ei voi kuitenkaan hyödyntää. (Verohallinto 2020). Eli TVL 110 § mukaisesti tulo on sen verovuoden tuloa ”jona se on nostettu, merkitty verovelvollisen tilille tai muutoin saatu vallintaan. Luovutusvoitto katsotaan sen verovuoden tuloksi, jona kauppa tai vaihto on tehty tai muu luovutus on tapahtunut.” (TVL 110 §). Omaisuuden luovutuksesta saatu voitto on veronalaista pääomatuloa ja puolestaan luovutuksesta syntynyt tappio tulee vähentää omaisuuden luovutuksesta saadusta voitosta kuluvan ja seuraavien viiden verovuoden aikana. Hankintameno määritetään todellisen hankintamenon mukaisesti. (TVL 45.1 §; TVL 50.1 §; Verohallinto 2020.)

LIITE 2. KYSELY

Kysely sisäisille tarkastajille

1. Vastaa seuraaviin väittämiin oman kokemuksesi mukaan

	Täysin eri mieltä	Jokseenkin eri mieltä	En samaa enkä eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä
Olen kiinnostunut uusista IT-teknologioista	○	○	○	○	○
Olen kiinnostunut lohkoketjuteknologiasta	○	○	○	○	○
Olen kiinnostunut kryptovaluutoista tai NFT:stä	○	○	○	○	○
Uskon lohkoketjuteknologian käyttämisen (esim. tietojärjestelmissä) voivan luoda lisäarvoa organisaatiolle	○	○	○	○	○
Uskon kryptovaluuttojen tai NFT:n käytön voivan luoda lisäarvoa organisaatiolle	○	○	○	○	○
Uskon lohkoketjuteknologian ratkaisevan nykyisten järjestelmien ongelmia	○	○	○	○	○
Lohkoketjuteknologia on merkityksellistä työni kannalta	○	○	○	○	○

2. Uusien teknologioiden tuntemus

Valitse vaihtoehto joka kuvaa tietämystäsi parhaiten

	En tunne aihetta	Tunnen aiheen huonosti	Tunnen aiheen keskinkertaisesti	Tunnen aiheen hyvin	Tunnen aiheen erinomaisesti
Kryptovaluutat	○	○	○	○	○
NFT (Non-Fungible Token)	○	○	○	○	○
Lohkoketju	○	○	○	○	○
IoT (Internet of Things, esineiden internet)	○	○	○	○	○
Koneoppiminen	○	○	○	○	○
Tekoäly	○	○	○	○	○
Ohjelmistorobotiikka	○	○	○	○	○
Pilvipalvelut	○	○	○	○	○

3. Kokemukset

Vastaa alla oleviin väittämiin kokemuksesi mukaisesti.

	Täysin eri mieltä	Jokseenkin eri mieltä	En samaa enkä eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä
Minulla on hyvät IT-taidot	○	○	○	○	○
Hallitsen lohkoketjuteknologian pääpiirteet	○	○	○	○	○
Lohkoketjuteknologian ymmärtäminen on minulle helppoa	○	○	○	○	○
Osaan/osaisin käsitellä hyvin lohkoketjuja sisäisen tarkastuksen tehtävissä	○	○	○	○	○
Olen tarvinnut lohkoketjuteknologiaan liittyvää osaamista työssäni	○	○	○	○	○
Olen tarvinnut kryptovaluuttoihin tai NFT:hen liittyvää osaamista työssäni	○	○	○	○	○
Tunnen kryptovaluuttoja koskevan keskeisen lainsäädännön	○	○	○	○	○
Tiedän kuinka lohkoketjun rakenne (julkinen, yksityinen, hajautettu, keskitetty) vaikuttaa lohkoketjujärjestelmän riskeihin	○	○	○	○	○
Osaan/osaisin varmentaa lohkoketjujärjestelmiä	○	○	○	○	○
Osaan/osaisin tunnistaa lohkoketjujärjestelmien riskikohteet	○	○	○	○	○
Osaan/osaisin antaa konsultaatiota lohkoketjujärjestelmien kontrollien luomisessa	○	○	○	○	○
Osaan/osaisin auttaa lohkoketjujärjestelmien sisäisen valvonnan järjestämisessä	○	○	○	○	○
Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönoton päätösprosessiin	○	○	○	○	○
Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa	○	○	○	○	○

4. Yleinen rooli

Vastaa alla oleviin väittämiin näkemyksesi perusteella

	Täysin eri mieltä	Jokseenkin eri mieltä	En samaa enkä eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä
Koen, että uusien teknologioiden tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia	○	○	○	○	○
Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä aktiivisesti uusiin teknologioihin	○	○	○	○	○
Lohkoketjujen varmentaminen kuuluu sisäisten tarkastajien työtehtäviin	○	○	○	○	○
Sisäisillä tarkastajilla voi olla rooli lohkoketjujärjestelmien käyttöönotossa	○	○	○	○	○
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa	○	○	○	○	○
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän riskikohteiden löytämisessä	○	○	○	○	○
Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän valvonnan rakentamisessa	○	○	○	○	○
Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia	○	○	○	○	○
Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan	○	○	○	○	○

5. Tulevaisuus

Vastaa alla oleviin kysymyksiin näkemyksesi perusteella

	Täysin eri mieltä	Jokseenkin eri mieltä	En samaa enkä eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana	○	○	○	○	○
Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana	○	○	○	○	○
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän IT-osaamista	○	○	○	○	○
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista lohkoketjuista	○	○	○	○	○
Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä	○	○	○	○	○
Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa	○	○	○	○	○
Uskon, että organisaatiomme on osaamisvalmiuksien puolesta valmis ottamaan käyttöön lohkoketjuteknologiaa	○	○	○	○	○
Lohkoketjupohjaisten järjestelmien parissa työskentely ei aiheuta/aiheuttaisi minulle stressiä	○	○	○	○	○
Lohkoketjuteknologia tulee helpottamaan sisäisten tarkastajien työtä	○	○	○	○	○
Lohkoketjuteknologia tulee vaikeuttamaan sisäisten tarkastajien työtä	○	○	○	○	○
Lohkoketjuteknologia tulee lisäämään sisäisten tarkastajien työmäärää	○	○	○	○	○
Lohkoketjuteknologia tulee vähentämään sisäisten tarkastajien työmäärää	○	○	○	○	○
Sisäisiä tarkastajia tarvitaan tulevaisuudessa enemmän	○	○	○	○	○

6. Organisaatio/-ssa jossa työskentelen

Valitse kaikki vaihtoehdot, jotka pitävät paikkansa

- [ ] on keskusteltu lohkoketjuteknologian käyttömahdollisuuksista
- [ ] on suunnitelmia lohkoketjuteknologian käyttöönotolle
- [ ] on pilotoinut lohkoketjupohjaisen järjestelmän käyttöä
- [ ] käyttää yhtä tai useampaa lohkoketjupohjaista järjestelmää
- [ ] on keskusteltu kryptovaluutojen tai NFT:n hyödyntämisestä liiketoiminnassa
- [ ] on ottamassa käyttöönsä kryptovaluuttoja tai NFT:tä liiketoiminnassa
- [ ] käyttää toiminnassaan kryptovaluuttoja tai NFT:tä
- [ ] Ei mitään edellisistä
- [ ] En osaa sanoa

7. Kuinka monta vuotta olet työskennellyt sisäisenä tarkastajana

- ◯ Alle 5 vuotta
- ◯ 6-10 vuotta
- ◯ 11-15 vuotta
- ◯ 16-20 vuotta
- ◯ Yli 20 vuotta

8. Toimiiko organisaatiosi yksityisellä vai julkisella sektorilla

- ◯ Yksityinen sektori
- ◯ Julkinen sektori
- ◯ Muu/molemmissa

9. Teetkö sisäistä tarkastusta organisaation sisäisenä toimijana vai ulkoisen palveluntarjoajan kautta

- ◯ Organisaation oma sisäinen tarkastaja
- ◯ Teen sisäistä tarkastusta toimeksiantoina

10. Ikä

- ◯ Alle 30
- ◯ 31-40
- ◯ 41-50
- ◯ Yli 50

11. Sukupuoli

- ◯ Nainen
- ◯ Mies
- ◯ Muu
- ◯ En halua vastata

12. Rooli organisaatiossa/tehtävänimike

Roolini/tehtävänimikkeeni on: _____

13. Organisaation toimiala

Organisaationi päätoimiala on (esim. teollisuus, rahoitus- ja vakuutustoiminta) _____

LIITE 3 KORRELAATIOMATRIISI

Correlations

			Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa	Osaamisen mittari	Olen tarvinnut lohkoketjutekn ologiaan liittyvää osaamista työssäni	Olen kiinnostunut lohkoketjutek nologiasta	Olen kiinnostunut kryptovaluutoi sta tai NFT: stä	Uskon lohkoketjutek nologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana	Uskon lohkoketjutek nologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana	Uusien teknolo-gioiden tuntemuksen mittari
Spearman's rho	Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa	Correlation Coefficient	1,000	,532**	,509**	,092	,188	,408**	,330**	,244*
		Sig. (2-tailed)	.	<,001	<,001	,456	,124	<,001	,006	,045
		N	68	68	68	68	68	68	68	68
	Osaamisen mittari	Correlation Coefficient	,532**	1,000	,621**	,462**	,594**	,470**	,547**	,668**
		Sig. (2-tailed)	<,001	.	<,001	<,001	<,001	<,001	<,001	<,001
		N	68	68	68	68	68	68	68	68
	Olen tarvinnut lohkoketjutekn ologiaan liittyvää osaamista työssäni	Correlation Coefficient	,509**	,621**	1,000	,463**	,504**	,541**	,512**	,493**
		Sig. (2-tailed)	<,001	<,001	.	<,001	<,001	<,001	<,001	<,001
		N	68	68	68	68	68	68	68	68
	Olen kiinnostunut lohkoketjutekn ologiasta	Correlation Coefficient	,092	,462**	,463**	1,000	,808**	,482**	,607**	,566**
		Sig. (2-tailed)	,456	<,001	<,001	.	<,001	<,001	<,001	<,001
		N	68	68	68	68	68	68	68	68
	Olen kiinnostunut kryptovaluutoista tai NFT: stä	Correlation Coefficient	,188	,594**	,504**	,808**	1,000	,435**	,554**	,594**
		Sig. (2-tailed)	,124	<,001	<,001	<,001	.	<,001	<,001	<,001
		N	68	68	68	68	68	68	68	68
	Uskon lohkoketjutekn ologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana	Correlation Coefficient	,408**	,470**	,541**	,482**	,435**	1,000	,749**	,455**
		Sig. (2-tailed)	<,001	<,001	<,001	<,001	<,001	.	<,001	<,001
		N	68	68	68	68	68	68	68	68
	Uskon lohkoketjutekn ologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana	Correlation Coefficient	,330**	,547**	,512**	,607**	,554**	,749**	1,000	,552**
		Sig. (2-tailed)	,006	<,001	<,001	<,001	<,001	<,001	.	<,001
		N	68	68	68	68	68	68	68	68
	Uusien teknologioiden tuntemuksen mittari	Correlation Coefficient	,244*	,668**	,493**	,566**	,594**	,455**	,552**	1,000
		Sig. (2-tailed)	,045	<,001	<,001	<,001	<,001	<,001	<,001	.
		N	68	68	68	68	68	68	68	68

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

LIITE 4 TULEVAISUUDEN (5V) NÄKYMIÄ SELITTÄVÄT MUUTTUJAT

Model Summary[a]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	,671[b]	,450	,441	,67711	,450	53,932	1	66	<,001
2	,723[c]	,523	,508	,63538	,073	9,954	1	65	,002
3	,755[d]	,570	,550	,60750	,048	7,103	1	64	,010
4	,773[e]	,598	,572	,59245	,027	4,292	1	63	,042

a. Dependent Variable: Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana

b. Predictors: (Constant), Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan

c. Predictors: (Constant), Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan, Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia

d. Predictors: (Constant), Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan, Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia, Uskon, että organisaatiomme on osaamisvalmiuksien puolesta valmis ottamaan käyttöön lohkoketjuteknologiaa

e. Predictors: (Constant), Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan, Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia, Uskon, että organisaatiomme on osaamisvalmiuksien puolesta valmis ottamaan käyttöön lohkoketjuteknologiaa, Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
4	(Constant)	,907	,282		3,222	,002	,345	1,470		
	Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan	,187	,096	,239	1,952	,050	-,004	,378	,424	2,358
	Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia	,424	,107	,497	3,978	<,001	,211	,638	,408	2,449
	Uskon, että organisaatiomme on osaamisvalmiuksien puolesta valmis ottamaan käyttöön lohkoketjuteknologiaa	,287	,085	,349	3,371	,001	,117	,456	,595	1,682
	Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa	-,200	,097	-,223	-2,072	,042	-,394	-,007	,550	1,817

a. Dependent Variable: Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan viiden vuoden aikana

LIITE 5 TULEVAISUUDEN (10V) NÄKYMIÄ SELITTÄVÄT MUUTTUJAT

Model Summary[a]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	,672[b]	,452	,443	,68664	,452	54,366	1	66	<,001
2	,736[c]	,542	,527	,63263	,090	12,750	1	65	<,001
3	,778[d]	,605	,587	,59171	,064	10,303	1	64	,002
4	,802[e]	,644	,621	,56660	,038	6,798	1	63	,011
5	,817[f]	,667	,640	,55222	,023	4,325	1	62	,042
6	,809[g]	,654	,632	,55840	-,013	2,418	1	62	,125

a. Dependent Variable: Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana

b. Predictors: (Constant), Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia

c. Predictors: (Constant), Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia, Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa

d. Predictors: (Constant), Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia, Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa, Ikä

e. Predictors: (Constant), Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia, Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa, Ikä, Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä

f. Predictors: (Constant), Koen, että lohkoketjuteknologian tuntemisen pitäisi kuulua osaksi sisäisten tarkastajien ammatillisia valmiuksia, Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa, Ikä, Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä, Lohkoketjuteknologia tulee lisäämään sisäisten tarkastajien työmäärää

g. Predictors: (Constant), Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa, Ikä, Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä, Lohkoketjuteknologia tulee lisäämään sisäisten tarkastajien työmäärää

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Tolerance	VIF
6	(Constant)	,873	,489		1,785	,079	-,105	1,850		
	Uskon lohkoketjuteknologian käytön yleistyvän tulevaisuudessa	,343	,099	,325	3,483	<,001	,146	,540	,630	1,587
	Ikä	-,340	,087	-,294	-3,892	<,001	-,514	-,165	,964	1,037
	Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista kryptovaluutoista tai NFT:stä	,435	,090	,443	4,806	<,001	,254	,615	,646	1,548
	Lohkoketjuteknologia tulee lisäämään sisäisten tarkastajien työmäärää	,229	,088	,192	2,588	,012	,052	,405	,994	1,006

a. Dependent Variable: Uskon lohkoketjuteknologian vaikuttavan paljon sisäisten tarkastajien työhön seuraavan kymmenen vuoden aikana

LIITE 6 OSAAMISTA SELITTÄVÄT MUUTTUJAT

Model Summary[f]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	,777[a]	,603	,597	,75636	,603	100,303	1	66	<,001
2	,865[b]	,747	,740	,60796	,144	37,152	1	65	<,001
3	,877[c]	,769	,759	,58544	,022	6,099	1	64	,016
4	,889[d]	,791	,778	,56206	,021	6,433	1	63	,014
5	,897[e]	,804	,788	,54809	,013	4,253	1	62	,043

a. Predictors: (Constant), Tiedän kuinka lohkoketjun rakenne (julkinen, yksityinen, hajautettu, keskitetty) vaikuttaa lohkoketjujärjestelmän riskeihin

b. Predictors: (Constant), Tiedän kuinka lohkoketjun rakenne (julkinen, yksityinen, hajautettu, keskitetty) vaikuttaa lohkoketjujärjestelmän riskeihin, Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa

c. Predictors: (Constant), Tiedän kuinka lohkoketjun rakenne (julkinen, yksityinen, hajautettu, keskitetty) vaikuttaa lohkoketjujärjestelmän riskeihin, Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa, Tunnen kryptovaluuttoja koskevan keskeisen lainsäädännön

d. Predictors: (Constant), Tiedän kuinka lohkoketjun rakenne (julkinen, yksityinen, hajautettu, keskitetty) vaikuttaa lohkoketjujärjestelmän riskeihin, Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa, Tunnen kryptovaluuttoja koskevan keskeisen lainsäädännön, Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän IT-osaamista

e. Predictors: (Constant), Tiedän kuinka lohkoketjun rakenne (julkinen, yksityinen, hajautettu, keskitetty) vaikuttaa lohkoketjujärjestelmän riskeihin, Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa, Tunnen kryptovaluuttoja koskevan keskeisen lainsäädännön, Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän IT-osaamista, Lohkoketjuteknologia on merkityksellistä työni kannalta

f. Dependent Variable: Osaamisenmittari

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
5	(Constant)	1,217	,549		2,216	,030	,119	2,315		
	Tiedän kuinka lohkoketjun rakenne (julkinen, yksityinen, hajautettu, keskitetty) vaikuttaa lohkoketjujärjestelmän riskeihin	,453	,083	,494	5,423	<,001	,286	,619	,381	2,626
	Organisaatiossani sisäiset tarkastajat osallistuvat uusien teknologioiden käyttöönottoon varhaisessa vaiheessa	,257	,054	,306	4,764	<,001	,149	,365	,765	1,307
	Tunnen kryptovaluuttoja koskevan keskeisen lainsäädännön	,231	,082	,225	2,827	,006	,068	,395	,498	2,008
	Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän IT-osaamista	-,361	,128	-,183	-2,821	,006	-,617	-,105	,754	1,326
	Lohkoketjuteknologia on merkityksellistä työni kannalta	,187	,091	,161	2,062	,043	,006	,369	,516	1,937

a. Dependent Variable: Osaamisenmittari

LIITE 7 KIINNOSTUSTA SELITTÄVÄT MUUTTUJAT

Model Summary[a]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	,811[b]	,657	,652	,59975	,657	126,442	1	66	<,001
2	,865[c]	,748	,740	,51851	,090	23,300	1	65	<,001
3	,888[d]	,789	,779	,47747	,042	12,655	1	64	<,001
4	,905[e]	,819	,807	,44597	,030	10,360	1	63	,002
5	,913[f]	,834	,821	,43044	,015	5,630	1	62	,021

a. Dependent Variable: Olen kiinnostunut lohkoketjuteknologiasta

b. Predictors: (Constant), Olen kiinnostunut kryptovaluutoista tai NFT:stä

c. Predictors: (Constant), Olen kiinnostunut kryptovaluutoista tai NFT:stä, Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan

d. Predictors: (Constant), Olen kiinnostunut kryptovaluutoista tai NFT:stä, Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan, Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa

e. Predictors: (Constant), Olen kiinnostunut kryptovaluutoista tai NFT:stä, Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan, Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa, Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista lohkoketjuista

f. Predictors: (Constant), Olen kiinnostunut kryptovaluutoista tai NFT:stä, Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan, Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa, Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista lohkoketjuista, Olen kiinnostunut uusista IT-teknologioista

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95,0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Tolerance	VIF
5	(Constant)	,466	,342		1,363	,178	-,218	1,150		
	Olen kiinnostunut kryptovaluutoista tai NFT:stä	,448	,061	,540	7,353	<,001	,326	,570	,497	2,013
	Työyhteisöni mielestä sisäisten tarkastajien pitäisi perehtyä lohkoketjuteknologiaan	,263	,059	,301	4,487	<,001	,146	,380	,597	1,676
	Sisäiset tarkastajat voivat auttaa lohkoketjujärjestelmän soveltuvuuden arvioinnissa	-,216	,060	-,214	-3,616	<,001	-,335	-,096	,764	1,309
	Sisäiset tarkastajat tarvitsevat tulevaisuudessa enemmän osaamista lohkoketjuista	,265	,090	,210	2,952	,004	,086	,444	,528	1,894
	Olen kiinnostunut uusista IT-teknologioista	,180	,076	,154	2,373	,021	,028	,333	,637	1,570

a. Dependent Variable: Olen kiinnostunut lohkoketjuteknologiasta