Teuvo Moisa

OSAKKEIDEN DIGITALISOINTI LOHKOKETJUTEKNOLOGIAN AVULLA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Moisa, Teuvo Pauli
Osakkeiden digitalisointi lohkoketjuteknologian avulla
Jyväskylä: Jyväskylän yliopisto, 2022, 87 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Halttunen, Veikko

Suurinta osaa osakkeista ylläpidetään nykyään paperimuodossa tai sähköisesti yrityksen toimesta, minkä lisäksi lähinnä suurten ja vilkkaan kaupankäynnin kohteena olevien yritysten osakkeita ylläpidetään digitaalisesti arvo-osuusmuodossa arvo-osuusjärjestelmässä. Vuodesta 2012 lähtien osakkeiden digitalisointi on ollut teknisesti mahdollista myös lohkoketjuteknologialla. Tällä hetkellä suurin osa lohkoketjuteknologialla toteutetuista osakkeista perustuu security-token-viitekehykseen ja ERC20-tokenstandardiin. Tällöin osakkeet on toteutettu osakemuotoisina tokeneina. Osakkeet voidaan digitalisoida myös vahvistetun datan verkossa verifiable-claim-muodossa. Osakkeiden digitalisointi lohkoketjuteknologialla token-muodossa tarjoaa monia etuja verrattuna nykyisiin yksityisten osakeyhtiöiden käyttämiin manuaalisiin järjestelmiin, kuten parantunut likviditeetti ja osakekannan ylläpidon automatisointi, mutta myös arvo-osuusjärjestelmään verrattuna, kuten nopeampi end-to-end-prosessointinopeus ja kaupankäynnin helppous. Se voi myös tehdä välitys- ja säilytyspalvelut tarpeettomiksi. Lohkoketjuteknologian käyttöön liittyy kuitenkin myös paljon ongelmia erityisesti verkon suorituskyvyn ja lainsäädännön kannalta, jotka hidastavat sen käytön yleistymistä. Verifiable-claim-muotoisissa osakkeissa on paljon vähemmän ongelmia verrattuna token-muotoisiin, minkä vuoksi se saattaa tulevaisuudessa olla merkittävämpi tapa digitalisoida osakkeita. Tämä tutkimus koostuu kirjallisuuskatsauksesta, jossa käsitellään osakkeiden luonnetta, lohkoketjuteknologian luonnetta ja sen sopivuutta osakkeiden digitalisointiin sekä haastattelututkimuksesta, joka syventää kirjallisuuskatsauksen tuloksia.

Asiasanat: lohkoketjuteknologia, osake, digitalisointi, security token, arvo-osuusjärjestelmä, vahvistetun datan verkko

ABSTRACT

Moisa, Teuvo
Digitization of Corporate Shares using blockchain technology
Jyväskylä: University of Jyväskylä, 2022, 87 pp.
Information Systems, Master's Thesis
Supervisor: Halttunen, Veikko

Most of the company shares are now maintained in paper form or electronically by the company, in addition to which the shares of mainly large and heavily traded companies are maintained digitally in book-entry form in the book-entry system. Since 2012, the digitization of shares has also been technically possible with blockchain technology. Currently, most shares implemented with blockchain technology are based on the security token framework and the ERC20 token standard. In this case, the shares have been implemented as tokens in a form of shares. The shares can also be digitized in the verifiable-claim format on verifiable data network. The digitization of shares with blockchain technology in token form offers many advantages over current manual systems used by private limited companies, such as improved liquidity and automation of stock maintenance, but also over a book-entry system, such as faster end-to-end processing speed and ease of trading. It can also make brokerage and custody services unnecessary. However, the use of blockchain technology also poses many problems, especially in terms of network performance and legislation, which is slowing down its use to become common. Verifiable-claim-based stocks have far fewer problems compared to token-based stocks, which may make it a more significant way to digitize stocks in the future. This study consists of a literature review that discusses the nature of the shares, the nature of the blockchain technology and its suitability for digitizing the shares, and an interview study that deepens the results of the literature review.

Keywords: blockchain technology, corporate shares, digitization, security token, book-entry system, verifiable-data-network

KUVIOT

KUVIO 1 Yksinkertainen kaaviokuva lohkoketjusta 19
KUVIO 2 Yksinkertaistettu esitys hajautetun sovelluksen pohja-arkkitehtuurista A, jossa transaktiot tuotetaan itse. 24
KUVIO 3 Yksinkertaistettu esitys hajautetun sovelluksen pohja-arkkitehtuurista B jossa transaktiot vahvistetaan itse. 25
KUVIO 4 Yksinkertaistettu esitys hajautetun sovelluksen pohja-arkkitehtuurista C, jossa transaktiot on delegoitu. 26
KUVIO 5 Päätöksentekopuu määriteltäessä lohkoketjuteknologian soveltuvuutta. 31
KUVIO 6 Yksinkertaistettu esitys osakekauppaverkosta. 55

TAULUKOT

TAULUKKO 1 Lohkoketjujen luokittelu, kuvaus ja tapausesimerkki. 20
TAULUKKO 2 Lohkoketjutokenien vaikutus yrittäjyyteen, sijoittamiseen ja innovointiin. 38
TAULUKKO 3 Haastattelunumerot ja organisaatio..... 50
TAULUKKO 4 Yhtiömuotojen erot digitalisoinnin kannalta. 61

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

TAULUKOT 4

SISÄLLYS 5

KÄSITEHAKEMISTO 7

1 JOHDANTO 9
1.1 Keskeiset käsitteet 10
1.2 Tutkielman sisältö 11

2 OSAKKEET VARALLISUUTENA 13
2.1 Osakkeet rahoitusvälineinä 13
2.2 Arvo-osuusjärjestelmään kuuluvat osakkeet 14
2.3 Arvo-osuusjärjestelmään kuulumattomat osakkeet 16

3 LOHKOKETJUTEKNOLOGIA 18
3.1 Lohkoketjuteknologian perusteet 18
3.2 Konsensusmekanismit 20
3.3 Tokenit 21
3.4 Älykkäät sopimukset 22
3.4.1 Hajautetut sovellukset 22
3.4.2 Ethereum-virtuaalikone 26
3.5 Standardit 27
3.6 Lohkoketjuteknologiaan liittyvät riskit 28
3.7 Teknologioiden valinta 31

4 HAJAUTETTU FINANSSIMAAILMA 33
4.1 Lohkoketjuteknologian vaikutus transaktioihin, vaihdantaan ja rahoitusmarkkinoihin 33
4.2 Kryptovarallisuus ja sijoitusmuotoiset tokenit 35
4.2.1 Sijoitusmuotoisten tokenien edut 37
4.2.2 Sijoitusmuotoisten tokenien ongelmat sääntelyn, markkinoiden ja teknologian kehityksen suhteen 38
4.3 ICO-buumi 39
4.4 Rahoitusmarkkinainfrastruktuurit (FMI:t) ja hajautetut rahoitusmarkkinaninfrastruktuurit (dFMI:t) 40
4.5 ERC20-tokenit 42

4.6 Kaupankäynti kryptovarallisuudella 43
4.6.1 Hajautetut kauppapaikat 44
4.6.2 Kryptopörsseihin liittyvät lainsäädännölliset ongelmat 45
4.6.3 Kaupankäynti kryptopörsseissä 46
4.6.4 Kaupankäyntialustat ja protokollat 47
4.6.5 Hakkerointi ja manipulointi 47
4.7 Lohkoketjuteknologian käyttöönotto rahoitusmarkkinoilla 48

5 EMPIIRISEN TUTKIMUKSEN LÄHTÖKOHDAT JA MENETELMÄT 49
5.1 Aineiston keruu 49
5.2 Haastateltavien asiantuntemus 50
5.3 Aineiston analysointi 51

6 TUTKIMUKSEN TULOKSET 52
6.1 Osakkeiden digitalisoitiin käytetyt teknologiat 52
6.1.1 Lohkoketjuteknologiaan pohjautuva osakkeiden digitalisointi 53
6.1.2 Osakekauppaverkon toteutus Corda-verkossa eli Jupiter-malli 53
6.2 Osakkeiden digitalisoinnin kehityskulku 56
6.3 Lainsäädännön ongelmat 56
6.3.1 Identiteetinhallinta 57
6.3.2 Määrämuotoisuus 58
6.3.3 Eri maiden poikkeava lainsäädäntö ja lakien tulkinta 59
6.4 Yhtiömuodon vaikutus yrityksen digitalisointiin lohkoketjuteknologialla 59
6.5 Lohkoketjuteknologian ongelmat 62
6.6 Lohkoketjuteknologian edut 63
6.7 Arvo-osuusjärjestelmän ongelmat 64
6.8 Digitaalisten osakkeiden tulevaisuus 65
6.8.1 Trust-over-ip-protokollaan pohjautuva identiteettiverkko ja erilliset transaktioidenhallintapalvelut haastavat lohkoketjuihin nojaavan hajautetun finanssimaailman 65
6.8.2 Lohkoketjuteknologia on arvo-osuusjärjestelmän kilpailija ja voi korvata sen 67

7 TULOSTEN TULKINTA JA POHDINTA 68
7.1 Lohkoketjuteknologian kehitys osakkeiden digitalisoinnin kannalta 69
7.2 Lohkoketjuteknologian tuomat mahdollisuudet 70
7.3 Lohkoketjuteknologiaan liittyvät ongelmat 71

8 YHTEENVETO 74

LÄHTEET 76

LIITE 1 ENSIMMÄINEN LIITE 87

KÄSITEHAKEMISTO

Arvopapereiden toimitusjärjestelmä (SSS)
Arvopapereiden toimitusjärjestelmä (Securities Settlement system) on kokonaisuus, joka mahdollistaa arvopapereiden siirron ja säilyttämisen arvo-osuusjärjestelmässä ennalta määrättyjen monenvälisten sääntöjen mukaisesti.
Arvopaperikeskus (CSD)
Arvopaperikeskus (Central Securities Depository) on osakeyhtiö, jolle on myönnetty toimilupa pitää yllä arvo-osuusjärjestelmää ja tarjota siinä arvopapereiden liikkeellelaskua, säilytystä ja toimitusta. Suomessa on yksi arvopaperikeskus Euroclear Finland Oy.
Bysanttilainen vika
Bysanttilainen vika on sellainen vika, joka ilmenee järjestelmässä erilaisina oireina eri havaitsijoille ja tuottaa ristiriitaista dataa
Double-spending-hyökkäys
Double-spending-hyökkäys tapahtuu silloin, kun hyökkääjä onnistuu käyttämään samoja tokeneita tai coineja useita kertoja.
Keskusvastapuoli (CCP)
Keskusvastapuoli (central counterparty) on arvopaperikaupan arvoketjussa toimiva yhteisö, joka on arvopaperikeskuksen ja kaupankäyntipaikan välissä. Se asettuu myyjäksi ostajalle ja ostajalle myyjäksi.
Gas (Ethereum)
Ethereum-virtuaalikoneessa Gas on kulutettujen resurssien mittayksikkö, jonka käyttöä hinnoitellaan Ether-kryptovaluutassa. Jokainen transaktio Ethereum-lohkoketjussa maksaa tietyn määrän Gas-yksikköjä perustuen laskentatehon kulutukseen. Gas-yksikköjen avulla ehkäistään liiallista verkkoresurssien käyttöä ja palvelunestohyökkäyksiä.
Luovutus maksua vastaan (DVP)
Luovutus maksua vastaan (Delevery Versus Payment) tarkoittaa sitä, että käteinen ja arvopaperit vaihdetaan samanaikaisesti ja vasta sen jälkeen, kun ne on talletettu arvopaperikeskukseen.
Security token
Security token tai suomeksi sijoitusmuotoinen token on sellainen token, joka edustaa jotain kohde-etuutta, kuten kassavirtoja, osinkoja tai korkoja.
Systeemisesti tärkeä rahoituslaitos (SIFI)
Systeemisesti tärkeä rahoituslaitos (Systemically Important Financial Institution) on pankki, vakuutusyhtiö tai muu rahoituslaitos, jonka kaatuminen olisi vakava riski taloudelle.
Token
Lohkoketjuteknologiassa tokennilla tarkoitetaan yhteenvetoa/tilannekuvaa omistusoikeuksista, jotka on tallennettu lohkoketjuun.
Verifiable claim

Verifiable claim on digitaalinen fakta, joka on kryptografisesti varmennettua dataa jostakin kohteesta, joka on peräisin kohteen tunnistavalta entiteetiltä eli kolmannelta osapuolelta. Vefifiable claim koostuu kohteen tunnisteesta, verifioidusta väittämästä (claim) seka väittämän tai väittämien metadatasta.

1 JOHDANTO

Vaikka teknologinen kehitys on ollut nopeaa viimeisen 30 vuoden aikana, osakkeiden digitalisoinnissa vastaavaa kehitystä ei ole tapahtunut. Käytössä on edelleen monimutkainen, välittäjiin perustuva ja keskitetty rahoitusmarkkinainfrastruktuuri, jossa osakeannit ja osakkeiden jälkimarkkinaprosessit ovat hitaita ja kalliita toteuttaa, koska kauppojen täsmäyttämiseen, maksamiseen ja säilytykseen tarvitaan kaikkiin omat keskitetyt tietokannat ja niitä ylläpitävät systeemisesti tärkeät rahoituslaitokset keskustietokoneineen. Euroopassa jokaisessa maassa osakkeiden digitalisointi perustuu lähinnä arvo-osuusjärjestelmään, jota hallinnoi kussakin maassa lähes määräävässä markkina-asemassa oleva arvopaperikeskus. Useimmissa osakeyhtiöissä arvo-osuusjärjestelmäkään ei ole käytössä, vaan osakasluetteloita ylläpidetään sähköisesti esimerkiksi Ecxel-taulukossa tai paperimuodossa, ja osakasluettelon hallinnoinnissa käytetään paperisia asiakirjoja.

Lohkoketjuteknologia on lupaava teknologia, joka voi merkittävästi helpottaa osakkeiden hallinnointia ja kaupankäyntiä osakkeilla. Sen avulla voidaan luoda huomattavasti nykyistä rahoitusmarkkinainfrastruktuuria kustannustehokkaampi järjestelmä, jossa ei tarvita pörssejä eikä arvopaperikeskuksia ja jossa osakeannit ja kaupankäynti osakkeilla voidaan toteuttaa paperittomasti ja ilman manuaalisia prosesseja.

Teknisesti lohkoketjuteknologiaa on voitu käyttää osakkeiden digitalisoinnissa vuodesta 2012, kun kehitettiin Colored Coins -konsepti ja oivallettiin, että tokenit voivat edustaa jotain kohde-etuutta, mikä voi olla myös osake. (Rosenfeld, 2012) Sen jälkeen on kehitetty myös älysopimusalustoja, joiden avulla tokeneihin on voinut lisätä erilaisia toimintoja. Näistä tunnetuin on Ethereum ja yleisin käytössä oleva tokenstandardi kohde-etuuksien digitalisoinnissa on ERC20-token. (Howell, Niessner & Yermack, 2020)

Tällä hetkellä Ethereum-alusta on merkittävin kohde-etuuksien digitalisointiin käytetty lohkoketjualusta, mutta sen käyttöön liittyy ongelmia verkon suorituskyvyn skaalautuvuuden ja lainsäädännön kannalta. (Howell ym., 2020) Tässä tutkimuksessa potentiaaliseksi vaihtoehdoksi Ethereum-alustalle löytyi Suomalaisen Findynet-osuuskunnan kehittämä varmennetun datan verkko, joka

perustuu Trust Over Ip -protokollaan pohjautuvaan Hyper Ledger Indy -identiteettiverkkoon, johon on yhdistetty Corda-transaktioverkko.

Useat yritykset Suomessa ja maailmalla ovat kehittäneet lohkoketjuteknologiaan pohjautuvia alustoja, joiden avulla osakeannit ja kaupankäynti osakkeilla voitaisiin digitalisoida, mutta tällä hetkellä ne eivät ole laajassa käytössä, koska useimmissa maissa arvopaperilainsäädäntö ja osakeyhtiölaki asettavat tiukkoja rajoitteita niiden käytölle.

Tämän tutkimuksen tavoitteena on selvittää niitä edellytyksiä, joiden perusteella osakkeiden digitalisointi lohkoketjuteknologialla olisi mielekästä ja tässä tutkimuksessa asiaa pohditaan sekä teknologian tarjoamien mahdollisuuksien että lainsäädännön asettamien rajoitusten suhteen. Tutkimuksen tavoitteiden saavuttamiseksi määriteltiin seuraavat tutkimuskysymykset:

1. Miten lohkoketjuteknologiaa käytetään osakkeiden digitalisoinnissa?
2. Mitkä ovat lohkoketjuteknologian positiiviset ja negatiiviset vaikutukset osakkeita digitalisoitaessa?

Erityisesti on tarkoitus selvittää mitä mahdollisuuksia lohkoketjuteknologia tarjoaa, kun osakkeita digitalisoidaan ja millaisia sovelluksia ja kehitystyötä se edellyttää. Lohkoketjuteknologian soveltamista pyritään tarkastelemaan lohkoketjuteknologiaan pohjautuvien osakkeiden digitalisointialustojen kehittäjien näkökulmasta.

Tiedonkeruu on toteutettu tekemällä ensin kirjallisuuskatsaus ja täydentämällä kirjallisuuskatsauksen tietoja teemahaastattelujen avulla. Kirjallisuuskatsauksessa tutkitaan lohkoketjuteknologian toimintaperiaatetta ja sen tarjoamia mahdollisuuksia käytettäessä osakkeita yritysrahoituksessa. Tutkimuksen tarkoitus on tarjota perustiedot, miten lohkoketjuteknologia voi auttaa osakeannin toteuttamisessa ja osakkeiden jälkimarkkinoilla, sekä palvella osakkeiden digitalisointia tarjoavia yrityksiä, heidän asiakkaitaan sekä muita sidosryhmiä, kuten poliittiset päättäjät, virkamiehet ja yritysten osakkeiden omistajat.

1.1 Keskeiset käsitteet

Tutkimuksen keskeiset käsitteet ovat lohkoketjuteknologia, token, ERC20-token, älykäs sopimus, älysopimusalusta, osake, arvo-osuusjärjestelmä, rahoituslaitos, ja rahoitusmarkkinainfrastruktuuri. Tässä alaluvussa kuvaillaan lyhyesti keskeiset käsitteet.

Lohkoketjuteknologialla viitataan tässä tutkimuksessa paitsi teknologioihin, joissa transaktioita talletetaan hajautettuun verkkoon peräkkäisissä aikaleimatuissa lohkoissa eli lohkoketjuissa sekä myös teknologioihin, joissa sovelletaan hajautettua luottamusta ja hajautettua tietokoneverkkoa transaktioiden tallentamisen yhteydessä.

Tokeneilla tarkoitetaan tässä tutkimuksessa lohkoketjuihin talletettuja representaatioita erilaisista kohde-etuuksista, jotka voivat olla esimerkiksi kryptovaluuttaa, hyödykkeitä tai arvopapereita.

ERC20-token on Ethereum-token, joka toteuttaa standardi muodossa tietyt toiminnot, kuten transaktioiden vahvistamisen, pääsyn hallinnan ja tokenien kokonaistarjonnan. Se on merkittävin käytössä oleva tokenstandardi, jolla on toteutettu suurin osa erilaisista tokeneista.

Älykkäillä sopimuksilla viitataan tietokoneohjelmiin, jotka toteuttavat itsensä tiettyjen sopimusehtojen täyttyessä. (Lauslahti, Mattila & Seppälä, 2016) Ne on tyypillisesti tallennettu lohkoketjuihin, mutta älykkäitä sopimuksia voi toteuttaa myös esimerkiksi Corda-verkossa, jossa ei ole lohkoja.

Osakkeet ovat rahoitusinstrumentteja, joilla kerätään pääomaa yritysten rahoittamiseen ja ne oikeuttavat omistajansa osinkoon ja päätösvaltaan yhtiökokouksessa. (Begg, Fischer & Dornbusch, 1997; Niskanen & Niskanen, 2013)

Arvo-osuusjärjestelmä on tietojärjestelmäkokonaisuus, joka muodostuu arvo-osuustileistä ja niihin liittyvistä luetteloista. (Niemi, 2017) Arvo-osuudella tarkoitetaan osaketta, osuutta, muuta oikeutta, rahoitusvälinettä tai siihen rinnastettavaa oikeutta, joka on liitetty sähköiseen arvo-osuusjärjestelmään. Arvo-osuudet ja niihin kohdistuvat oikeudet kirjataan arvo-osuustileille, joita pidetään arvo-osuusrekisterissä. (Niemi, 2017.) Arvo-osuuksista ei anneta osakekirjaa, velkakirjaa tai muuta paperille merkittävää oikeuden olemassa-oloa tai sisältöä koskevaa asiakirjaa ja ne ovat numeroimattomia. (Niemi, 2017)

Rahoitusmarkkinainfrastruktuurit ovat tärkeä osa rahoitusjärjestelmää, koska ne tarjoavat palveluita, joiden varassa järjestelmä toimii. Arvopapereiden, hyödykkeiden ja johdannaisten jälkimarkkinaprosessit edellyttävät kauppaehtojen varmistamista sekä kauppojen toimitusta ja selvitystä. Näitä tehtäviä hoitavat usein erilaiset välittäjät, kuten arvopapereiden toimitusjärjestelmät, arvopaperikeskukset ja keskusvastapuolet, jotka ovat erikoistuneet tiettyihin maksu-, toimitus- ja selvitystoimintoihin. (Mills ym., 2016)

Tässä tutkimuksessa digitalisoinnilla tarkoitetaan analogisten prosessien muuttamista digitaaliseen muotoon ja konteksti on lähinnä osakkeiden muuttaminen digitaalisiksi sen sijaan, että omistajuuden hallinta hoidettaisiin manuaalisesti paperilla, kuten käyttämällä paperisia osakekirjoja.

1.2 Tutkielman sisältö

Luvussa 2 tarkastellaan osakkeiden juridista rakennetta, niiden käyttötarkoitusta sekä käydään läpi paperisten osakkeiden ja arvo-osuusjärjestelmässä säilytettävien osakkeiden keskeisiä ominaisuuksia.

Luvun 3 alaluvussa 3.1 selitetään pääpiirteissään lohkoketjuteknologian toimintaperiaate ja arkkitehtuuri. Alaluvussa 3.2 kerrotaan perusasiat konsensusmekanismeista. Alaluvussa 3.3 käsitellään tokeneita ja niiden erilaisia käyttötarkoituksia. Alaluvussa 3.4 käsitellään älykkäitä sopimuksia ja niiden soveltamista hajautetuissa sovelluksissa. Lisäksi tarkastellaan Ethereum-virtuaalikoneen merkitystä älykkäiden sopimusten toteuttamisessa. Alaluvussa 3.5 tarkastellaan standardien merkitystä lohkoketjuteknologian kehityksessä. Alaluvussa 3.6 tarkastellaan lohkoketjuteknologian käyttöä rajoittavia ongelmia ja sen

käytön turvallisuutta. Alaluvussa 3.7 tarkastellaan sitä, kuinka nämä ongelmat ja riskit tulee huomioida, kun käytetään lohkoketjuteknologiaa.

Luvussa 4 tarkastellaan lohkoketjuteknologian vaikutusta talousjärjestelmään. Alaluvussa 4.1 käsitellään lohkoketjuteknologian vaikutusta rahoitusmarkkinoihin ja yleisesti transaktioihin ja vaihdantaan. Alaluvussa 4.2 tarkastellaan sijoitusmuotoisia tokeneita ja niiden tarjoamia mahdollisuuksia yritysten rahoituksessa. Alaluvussa 4.3 käsitellään kryptopörssien toiminnan edellytyksiä ja niihin liittyviä lainsäädännöllisiä ongelmia. Alaluvussa 4.4 tarkastellaan ICO-buumia lähihistorian ilmiönä. Alaluvussa 4.5 kerrotaan, mitä ovat ERC20-tokenit ja mitä niillä tehdään. Alaluvussa 4.6 käsitellään kryptovarallisuudella käytävän kaupankäynnin erityispiirteitä, mahdollisuuksia ja ongelmia. Alaluvussa 4.7 käsitellään nykyisten rahoitusmarkkinainfrastruktuurien toimintaa ja ongelmia ja millaisia ratkaisuja lohkoketjuteknologia niihin tarjoaa. Alaluvussa 4.8 kuvaillaan erilaisia skenaarioita siitä, kuinka lohkoketjuteknologia voisi tulla käyttöön osakkeissa rahoitusmarkkinoilla.

Luvussa 5 kuvaillaan tutkimusmenetelmä siten, että alaluvussa 5.1 kerrotaan, miten aineisto kerättiin, alaluvussa 5.2 kerrotaan haastateltavien asiantuntemuksesta ja alaluvussa 5.3 kerrotaan, miten haastatteluaineisto analysoitiin. Sen jälkeen luvussa 6 kuvaillaan haastatteluaineisto luvussa 5 esitetyn menetelmän mukaisesti. Alaluvussa 6.1 kuvaillaan, millaisia osakkeiden digitalisointiin käytettäviä teknologioita aineistossa tuli esiin. Alaluvussa 6.2 kuvaillaan haastateltavien käsitystä osakkeiden digitalisoinnin kehityskulusta. Alaluvussa 6.3 kuvaillaan millaisia lainsäädännöllisiä ongelmia haastateltavat näkevät lohkoketjuteknologian käytössä osakkeiden digitalisoinnissa. Alaluvussa 6.4 käsitellään erilaisten yhtiömuotojen vaikutusta osakkeiden digitalisointiin, minkä lisäksi tarkastellaan yritysten omistuksenhallinnan digitalisointia eri yhtiömuodoissa. Alaluvussa 6.5 kuvaillaan haastateltavien näkemyksiä lohkoketjuteknologiaan liittyvistä ongelmista. Alaluvussa 6.6 kuvaillaan haastateltavien näkemyksiä lohkoketjuteknologian eduista osakkeiden digitalisoinnissa. Alaluvussa 6.7 kuvaillaan haastateltavien näkemyksiä siitä, millä tavalla lohkoketjuteknologia ja arvo-osuusjärjestelmä kilpailevat keskenään markkinoista. Alaluvussa 6.8 kuvaillaan, millaisia tulevaisuudenkuvia haastateltavilla on osakkeiden digitalisoinnin kehityksestä seuraavan kymmenen vuoden aikana. Alaluvussa 6.9 kuvaillaan haastateltavien näkemyksiä arvo-osuusjärjestelmästä ja sen ongelmista.

Luvussa 7 tutkimuksen tuloksia verrataan kirjallisuuskatsauksen tuloksiin ja muuhun kirjallisuuteen, joiden avulla muodostetaan johtopäätöksiä siitä, mikä on tulosten merkitys tutkimuskysymysten kannalta. Luku 8 on tutkimuksen yhteenveto, jossa käydään läpi keskeisimpiä saavutettuja tuloksia, niiden merkitystä ja keskeisiä rajoitteita tutkimusmenetelmän ja tulosten suhteen. Lisäksi tuodaan esiin se, miten tämän tutkimuksen tulokset poikkeavat kirjallisuuskatsauksessa käsitellyistä aiemmista tutkimuksista ja toisaalta ne tulokset, joiden osalta tämä tutkimus tukee aiempia tutkimustuloksia.

2 OSAKKEET VARALLISUUTENA

Tässä luvussa tarkastellaan osakkeita juridisena rakenteena, niiden käyttötarkoitusta sekä käydään läpi paperisten osakkeiden ja arvo-osuusjärjestelmässä säilytettävien osakkeiden keskeisiä ominaisuuksia.

2.1 Osakkeet rahoitusvälineinä

Osakkeet ovat rahoitusinstrumentteja, joiden avulla yrityksiin kerätään pääomaa, jota voidaan käyttää investointeihin ja yrityksen toimintaan. (Begg ym., 1997) Osakkeita voivat laskea liikkeelle osakeyhtiöt ja osuuskunnat. (Niskanen & Niskanen, 2013) Joskus osakkeisiin on kytketty jokin hyödyke, palvelu tai näiden yhdistelmä ja tällaisia tarjoavat yleensä osuustoiminnalliset osakeyhtiöt. Osuustoiminnallisten yritysten ainut osakkeenomistajille tarjoama taloudellinen hyöty on yleensä sen itse tuottamat palvelut tai alihankkijoilta hankkimat tavarat, joita se tarjoaa vastiketta tai käyttökorvausta vastaan. (Kyläkallio, Iirola & Kyläkallio, 2017.)

Tyypillisesti osakkeet ovat samanarvoisia osia yrityksestä, joihin liittyy äänioikeus yhtiökokouksessa. Osakesarjoja voi olla yrityksessä myös useita, jolloin äänivallan määrä yhtiökokouksessa riippuu siitä, mihin osakesarjaan osake kuuluu. Osakkeiden äänivallan määrä on kirjattu yhtiöjärjestykseen kunkin osakesarjan osalta. (Niskanen & Niskanen, 2013.) Äänivallan lisäksi osakesarjoissa voi olla eroja osinko-oikeuksien, yhtiötä purettaessa jaettavien varojen sekä lunastusoikeuksien ja -velvollisuuksien suhteen. (Leppiniemi, 2008, s. 30)

Maksullisessa osakeannissa lasketaan liikkeelle uusia osakkeita, jotka myydään entisille tai uusille osakkeenomistajille, jolloin yhtiö saa lisää pääomaa. Maksuttomassa osakeannissa yhtiö voi saada uusia osakkeita itselleen tai sitten uusia osakkeita annetaan yrityksen omistajille. Omistajille suunnatussa maksuttomassa osakeannissa kunkin osakkaan omistamien osakkeiden määrä tyypillisesti kaksin- tai kolminkertaistuu, mitä sanotaan osakkeiden jakamiseksi tai splitiksi. (Kyläkallio ym., 2017)

Yritykset voivat jakaa voitostaan osinkoja omistajilleen, joiden määrä jakaantuu osakeomistusten suhteen perusteella. (Niskanen & Niskanen, 2013) Osakkeiden omistajilla on rajoitettu vastuu yritysten velkojen suhteen ja he voivat menettää enintään sen verran kuin ovat sijoittaneet omistamiinsa osakkeisiin. (Begg ym. 1997)

Osakeyhtiöitä on julkisia ja yksityisiä ja julkisten yritysten osakkeilla voi käydä kauppaa säännellyllä markkinalla, kuten pörssissä. (Kyläkallio ym, 2017; Niskanen & Niskanen, 2013; Begg ym., 1997) Julkisen yhtiön osakepääoman on oltava vähintään 80 000 €. Pörssiyritykset ovat aina julkisia osakeyhtiöitä mutta kaikki julkiset osakeyhtiöt eivät ole pörssissä. (Kyläkallio ym., 2017) Yksityisten osakeyhtiöiden osakkeet eivät voi olla myynnissä säännellyllä markkinalla tai sellaista muistuttavassa kaupankäyntimenettelyssä. Niillä voi kuitenkin käydä kauppaa tarjoamalla niitä myytäviksi esimerkiksi internetissä tai sanomalehdissä. (Kyläkallio ym., 2017.) Niillä käytävään kauppaan sovelletaan irtaimen esineen kauppaa koskevaa kauppalakia. Samaa lakia sovelletaan myös julkisiin osakeyhtiöihin, jos niillä käydään kauppaa säännellyn markkinan tai vastaavan monenkeskisen kaupankäyntimenettelyn ulkopuolella. Joissakin tapauksissa sekä julkisten että yksityisten osakeyhtiöiden kauppaan sovelletaan myös kuluttajansuojalakia. (Kyläkallio ym., 2017.) Asunto-osakkeiden ja asuinhuoneistojen hallintaan oikeuttavien yhteisöosuuksien kauppaan sovelletaan asuntokauppalakia. (Kyläkallio ym., 2017)

Pörssiyhtiöiden osakkeilla käydään kauppaa sähköisesti arvo-osuuksilla, jotka ovat kirjattuna arvo-osuusrekistereissä pidetyillä arvo-osuustileillä. Suomessa arvo-osuusjärjestelmää (englanniksi book-entry system) pitää yllä Euroclear Finland Oy. (Niskanen & Niskanen, 2013) Arvo-osuustilin voi perustaa pankkien ylläpitämiin arvo-osuusrekistereihin tai arvopaperikeskukseen. (Niskanen & Niskanen, 2013)

2.2 Arvo-osuusjärjestelmään kuuluvat osakkeet

Jos yhtiössä on paljon osakkeita, omistajuuden hallinnan hoitaminen kannattaa toteuttaa arvo-osuusjärjestelmän avulla, koska osakekirjojen painatus ja jakelu aiheuttavat paljon työtä, vievät tilaa ja aiheuttavat paljon virheitä ja selvitystyötä. (Kyläkallio ym., 2017) Arvo-osuusjärjestelmä on tietojärjestelmäkokonaisuus, joka muodostuu arvo-osuustileistä ja niihin liittyvistä luetteloista. (Niemi, 2017) Arvo-osuudella tarkoitetaan osaketta, osuutta, muuta oikeutta, rahoitusvälinettä tai siihen rinnastettavaa oikeutta, joka on liitetty sähköiseen arvo-osuusjärjestelmään. Arvo-osuudet ja niihin kohdistuvat oikeudet kirjataan arvo-osuustileille, joita pidetään arvo-osuusrekisterissä. (Niemi, 2017.) Arvo-osuuksista ei anneta osakekirjaa, velkakirjaa tai muuta paperille merkittävää oikeuden olemassa-oloa tai sisältöä koskevaa asiakirjaa ja ne ovat numeroimattomia. (Niemi, 2017) Arvo-osuustileihin tekevät kirjauksia tilinhoitajat, joille arvo-osuusrekisterin pitäjä on antanut tilinhoitajan oikeudet. Tilinhoitajia ovat muun muassa pankit ja myös arvopaperikeskukset voivat itse toimia tilinhoitajina. (Kyläkallio ym., 2017)

Jos yhtiön osakkeet kuuluvat arvo-osuusjärjestelmään, siitä määrätään yhtiöjärjestyksessä. Yhtiö voidaan liittää arvo-osuusjärjestelmään jo yritystä perustettaessa (PRH, n.d..) Arvo-osuusjärjestelmään kuuluminen on mainittava tällöin kaupparekisterin perustamisilmoituksessa. Jos osakkeet liitetään arvo-osuusjärjestelmään myöhemmin, yhtiöjärjestystä pitää muuttaa ja asiasta tehdään muutosilmoitus kaupparekisteriin. (PRH, n.d..) Päätöksen liittymisestä tekee yhtiökokous ja sen tulee määrätä aika, jonka kuluessa siirtyminen arvo-osuusjärjestelmään tapahtuu tai valtuuttaa hallitus päättämään siitä. (PRH, n.d.) Kun osakkeet liitetään arvo-osuusjärjestelmään, osakkeenomistajien tehtävä on huolehtia siitä, että osakkeet kirjataan arvo-osuusjärjestelmään. (Kyläkallio ym., 2017) Jos osakkeet poistetaan arvo-osuusjärjestelmästä, siitä päättää myös yhtiökokous ja sen tulee määrätä päivä, jolloin poistaminen tapahtuu tai valtuuttaa hallitus päättämään siitä. (PRH, n.d..)

Suomen arvo-osuusjärjestelmää säätelee laki arvo-osuusjärjestelmästä ja selvitysjärjestelmää ja arvo-osuustilejä säätelee laki arvo-osuustileistä. (Niemi, 2017) Suomessa paperille merkittyjä osakkeita ja arvopapereita on korvattu sähköisillä arvo-osuuksilla vuodesta 1991 lähtien. (Niemi, 2017) Julkiseen kaupankäyntiin tarkoitetut yhtiöiden osakkeet täytyy Suomessa liittää arvo-osuusjärjestelmään. Liittäminen tapahtuu perustamalla liikkeeseenlaskutili, jolta osakkeet siirretään ostajien asiakastileille. (Niemi, 2017.)

Yhtiön hallituksen on pidettävä arvo-osuusjärjestelmään liitetyistä osakkeista ja niiden omistajista arvo-osuustilikirjauksiin perustuvaa osakasluetteloa, johon merkitään osakkeenomistajan tai hallintarekisteröinnin hoitajan nimi ja osoite, osakasluetteloon merkittävien osakkeiden lukumäärä osakelajeittain sekä henkilötunnus tai muu arvopaperikeskuksen määräysten mukainen yksilöintitunnus. (OYL, 624/2006) Laki arvo-osuusjärjestelmästä ja selvitystoiminnasta (348/2017) määrää, että osakasluetteloa on pidettävä arvopaperikeskuksessa liikkeeseenlaskijoiden lukuun. Osakasluetteloa pitää siis yllä käytännössä arvopaperikeskus.

Arvopaperikeskuksilla on kolme keskeistä roolia arvopapereiden selvityksessä. 1) Ne vahvistavat kaupat ja varmistavat niiden kirjanpidon. Ne esimerkiksi varmistavat, ettei kukaan tee kauppaa arvopapereilla, jotka eivät oikeasti ole olemassa. Kauppojen varmistaminen on tärkeää järjestelmän luotettavuuden ja rahoitusvakauden kannalta. (Benos, Garratt & Gurrola-Perez, 2017.) 2) Ne hoitavat laillisten omistusten siirron myyjiltä ostajille, mikä yleensä tapahtuu luovutuksella maksua vastaan. (Benos, Garratt & Gurrola-Perez, 2017.) 3) Ne pitävät yllä arvo-osuustilejä, joiden omistajuustietoja päivitetään jokaisen transaktion jälkeen. Arvo-osuustilien ansiosta arvopapereita voi pitää tavalla, joka mahdollistaa niiden helpon siirtämisen arvo-osuusjärjestelmässä sen sijaan, että käytettäisiin paperisia asiakirjoja. Ne voivat myös tarjota holveja fyysisten arvopapereiden säilytykseen. (Benos, Garratt & Gurrola-Perez, 2017.)

Arvopaperikeskukset ovat erittäin tärkeitä rahoitusmarkkinoiden toiminnan kannalta, minkä vuoksi niiden toimintaan liittyy paljon sääntelyä. Niitä koskee kansalliset arvopapereiden liikkeellelaskua, selvitystoimintaa ja säilytystä

säätelevät lait ja niitä valvoo erilaiset viranomaistahot mukaan lukien keskuspankit. (Benos ym., 2017)

2.3 Arvo-osuusjärjestelmään kuulumattomat osakkeet

Kun yhtiö ei kuulu arvo-osuusjärjestelmään, Osakeyhtiölaki (624/2006) määrää yhtiön hallituksen pitämään yhtiön osakkeista ja niiden omistajista osakasluetteloa. Lain mukaan osakasluetteloon tulee merkitä seuraavat tiedot:

- Kunkin osakkeenomistajan nimi ja osoite;
- Yksilöityjen osakkeiden tai osakekirjojen lukumäärä osakelajeittain;
- Osakkeiden antamispäivä;
- Erot osakkeiden tuottamissa oikeuksissa ja velvollisuuksissa;
- Osaketta rasittava panttioikeus tai muu vastaava oikeus;
- Osakkeen saajan yhtiölle ilmoittama saanto.

Laki myös edellyttää, että osakasluettelo on laadittava viivytyksettä yhtiön perustamisen jälkeen ja että sitä on pidettävä luotettavalla tavalla. Osakkeiden omistajat voivat käyttää heille yhtiössä kuuluvia oikeuksia, kun heidät on merkitty osakasluetteloon tai jos he ilmoittavat saantonsa esittäen siitä luotettavan selvityksen. Osakasluetteloa tulee pitää jokaisen nähtävänä yrityksen pääkonttorissa ja kenellä tahansa on oikeus saada siitä kopio kuluja vastaan. (OYL, 624/2006.) Osakasluettelon tulee olla nähtävillä myös yhtiökokouksessa. (OYL, 624/2006)

Jos yhtiö ei kuulu arvo-osuusjärjestelmään, se voi antaa osakkailleen osakekirjan, joka on osakkuuden todistava asiakirja. (Kyläkallio ym., 2017) Osakekirjojen antamista koskevat säännökset löytyvät osakeyhtiölain 3. luvusta 9–11 artikloista. Osakekirja voidaan antaa vain osakasluetteloon merkitylle osakkeenomistajalle. Se kuitenkin edellyttää, että yhtiö ja osake on sitä ennen rekisteröity. Hallituksen on pyydettäessä annettava osakekirja osakkeenomistajalle. (OYL, 624/2006.) Hallituksen pitää suorittaa osakekirjan jakaminen, osakekirjojen yhdistäminen tai muu vaihtaminen osakkeenomistajalle kuluja vastaan, jos osakkeenomistaja pyytää. (OYL, 624/2006)

Osakekirjan sisältöä koskevat säädökset löytyvät osakeyhtiölain (OYL. 624/2006) 3. luvun 10. artiklasta. Sen mukaan osake voidaan asettaa vain nimetylle henkilölle. Osakekirjassa pitää mainita:

1. Yhtiön nimi sekä yritys- ja yhteisötunnus;
2. Osakkeiden järjestysnumerot tai osakkeiden lukumäärä ja osakekirjan järjestysnumero;
3. Osakkeiden laji, jos yhtiössä voi osakekirjaa antaessa olla erilajisia osakkeita;
4. Osakekirjassa on myös mainittava velvollisuus maksaa erityisiä maksuja yhtiölle, osakeyhtiölain mukaiset muunto, lunastus- ja

suostumuslausekkeet sekä osakeyhtiölain mukaiset hankkimis- tai lunastusehdot, jos niistä on määrätty yhtiöjärjestyksessä. (OYL, 624/2006.)

Osakekirja on päivättävä ja siihen tarvitaan hallituksen tai hallituksen valtuuttaman henkilön allekirjoitus. Allekirjoituksen voi painaa tai tehdä muulla siihen verrattavalla tavalla. (OYL. 624/2006.) Osakekirjaan pitää merkitä osakkeiden mitätöinti, varojen tai osakkeiden jakaminen osakekirjaa vastaan. Osakekirjaan pitää merkitä myös se, kun sitä vastaan annetaan optio- tai osinkotodistus tai muu vastaavanlaista oikeutta osoittava todistus. (OYL, 624/2006.) Jos osakekirja annetaan kuoletettavan osakekirjan tilalle, siitä täytyy myös mainita. (OYL, 624/2006)

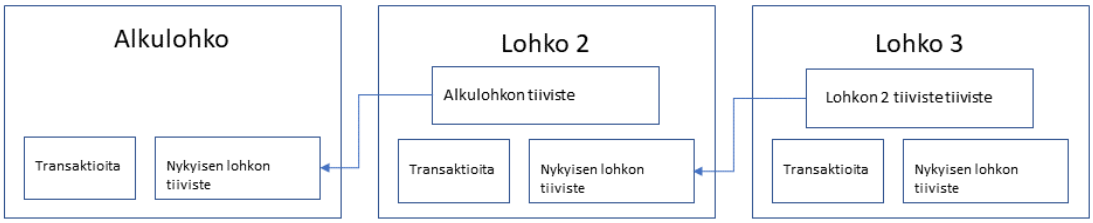
Osakasluettelon ulkoista muotoa ei ole säännelty, joten se voidaan laatia kirjamaisena sidottuna luettelona, irtolehti- tai korttijärjestelmänä, automaattisen tietojenkäsittelyn avulla tai se voidaan toteuttaa myös käsin. (Kyläkallio ym., 2017) Osakasluetteloon on merkittävä osakeyhtiölaissa vaaditut tiedot ja ne on pidettävä ajan tasalla. Kukaan ulkopuolinen ei saa päästä tekemään sen sisältöön tai muotoon muutoksia. Osakasluettelon merkittävät muutokset pitää päivätä. (Kyläkallio ym. 2017)

3 LOHKOKETJUTEKNOLOGIA

Tässä luvussa alaluvussa 3.1 selitetään pääpiirteissään lohkoketjuteknologian toimintaperiaate ja arkkitehtuuri. Alaluvussa 3.2 kerrotaan perusasiat konsensusmekanismeista. Alaluvussa 3.3 käsitellään tokeneita ja niiden erilaisia käyttötarkoituksia. Alaluvussa 3.4 käsitellään älykkäitä sopimuksia ja niiden soveltamista hajautetuissa sovelluksissa. Lisäksi tarkastellaan Ethereum-virtuaalikoneen merkitystä älykkäiden sopimusten toteuttamisessa. Alaluvussa 3.5 käsitellään standardien merkitystä lohkoketjuteknologian yleistymisen kannalta. Alaluvussa 3.6 tarkastellaan lohkoketjuteknologian käyttöä rajoittavia ongelmia ja sen käytön turvallisuutta ja alaluvussa 3.7 tarkastellaan sitä, kuinka nämä ongelmat ja riskit tulee huomioida, kun otetaan käyttöön lohkoketjuteknologiaa.

3.1 Lohkoketjuteknologian perusteet

Bitcoinin ja monien muiden kryptovaluuttojen perustana on lohkoketju, jota ylläpidetään hajautetun tietokoneverkon avulla (Nguyen, 2016). Lohkoketju voidaan ajatella listaksi transaktioista, jossa transaktiot on sisällytetty tiettyihin aikaleimattuihin lohkoihin. Jokaisella lohkolla on oma tiiviste, joka on salattu kryptaamalla. Jokaisen lohkon tiiviste viittaa sitä edeltävään lohkoon. Tiivisteiden avulla lohkot muodostavat ketjun. (Antonopoulos, 2014.) Kuviossa 1 on kuvattuna lohkoketjun perusrakenne. Lohkoketju koostuu aikaleimatuista lohkoista, joista ensimmäinen on alkulohko (englanniksi genesis block). Jokainen lohko lukuun ottamatta alkulohkoa sisältää edellisen lohkon tiivisteen. (Rouhani & Deters, 2019)



KUVIO 1 Yksinkertainen kaaviokuva lohkoketjusta (Rouhani & Deters, 2019, s. 2).

Tyypillisessä keskitetyssä transaktiojärjestelmässä transaktiot tarkistaa luotettava kolmas osapuoli, kuten pankki, mikä muodostaa pullonkaulan, kun transaktioita suoritetaan. Lohkoketjuteknologia mahdollistaa suorat peer-to-peer-transaktiot, joita minkään keskustahon ei tarvitse vahvistaa. (Zheng, Xie, Dai, Chen & Wang, 2018.) Muita lohkoketjuteknologian vahvuuksia ovat esimerkiksi sen mahdollistamat hajautetut tietokannat, pseudonyymisyys, datan suojaaminen peukaloinnilta ja varmennettavuus. (Zheng ym., 2018) Lohkoketjujen avulla toisilleen tuntemattomat tahot voivat tehdä yhteistyötä luotettavasti ilman kolmansia luottamuksen takaavia osapuolia. (Christidis & Devetsikiotis, 2016) Esimerkiksi pankkien välisten maksujen selvityksessä lohkoketjuteknologia tarjoaa huomattavia etuja nopeuttamalla selvityksiä ja eliminoimalla tarpeen käyttää muita rahoitusalan yrityksiä kolmansina osapuolina (Guo & Liang, 2016).

Lohkoketjujen hallinnoinnissa käytetään tyypillisesti yksityiseen ja julkiseen avaimeen perustuvaa rakennetta, jossa julkinen avain edustaa tiliä, joka vastaanottaa transaktioita. Transaktioiden asettamiseen tarvitaan yksityinen avain, joka voi olla salasana. Lohkoketjujen hallinnoinnissa tokeneiden omistajien pseudonyymisyys perustuu siihen, että julkiset avaimet ovat numeroista ja kirjaimista koostuvia merkkijonoja, joista ei selviä suoraan niiden omistajan identiteetti. Julkisen avaimen perusteella voidaan jäljittää kaikki transaktiot, jotka sillä on tehty. (Ante & Fiedler, 2019.)

Lohkoketjut voidaan jaotella avoimiin (englanniksi permissionless), jotka ovat vapaasti kaikkien saatavilla, eli kuka tahansa voi liittää koneensa lohkoketjuverkkoon ja suljettuihin (englanniksi permissioned), joiden verkkoon liittyminen on rajoitettua. (Xu, ym., 2017). Tämän lisäksi käytetään myös käsitettä hybridilohkoketju kuvaamaan sellaisia lohkoketjuja, joissa tietyillä johtajasolmuilla on paljon valtuuksia lohkoketjun ylläpidossa (Wu, Meng, Xu, Li, Ding & Suo, 2017). Taulukko 1 kuvailee lohkoketjujen luokittelua.

Lohkoketjut voidaan myös jakaa yksityisiin ja julkisiin. Yksityisissä lohkoketjuissa lohkoketjujen sisältämä tieto on vain tiettyjen vahvistettujen käyttäjien saatavissa, kun taas julkisissa lohkoketjuissa ne ovat kaikkien saatavilla. (Benos ym., 2017.) Käsitteitä avoin ja julkinen samoin kuin yksityinen ja suljettu käytetään monissa lohkoketjuteknologiaa käsittelevissä artikkeleissa samassa merkityksessä ilman tarkempaa erottelua.

TAULUKKO 1 Lohkoketjujen luokittelu, kuvaus ja tapausesimerkki (Kinnunen, Leviäkangas, Kostiainen, Nykänen & Rouhiainen, 2017).

Tilikirjan ylläpito	Kuvaus	Käyttötapausesimerkki
Rajattu (permissioned)	Tietokoneiden liittäminen lohkoketjuverkkojen solmuksi on rajoitettua ja lohkoketjuverkko toimii intranetin tavoin. (Kinnunen ym., 2017)	STAX: IHS Markit Ltd:n yksityinen lohkoketju, johon talletetaan tilisiirtoja (Marsh & Dewey, 2019).
Hybridi	Tietyt solmut muodostavat johtajasolmujen joukon, jonka solmuilla on paljon valtuuksia ja joihin luotetaan erityisesti. Johtajasolmut toteuttavat valtavan määrän liiketoimintaprosesseja ja suorittavat keskinäistä valvontaa. (Wu ym., 2017)	Energy Internet: LO3 nimisen yrityksen kehittämä lohkoketjuteknologiaa käyttävä sähköverkko (Wu ym., 2017).
Avoin (Permissionless)	Lohkoketju on vapaasti saatavilla internetissä. Kuka vain voi liittää tietokoneensa lohkoketjuverkkoon solmuksi (Casey, Crane, Gensler, Jonsson & Narula, 2018; Kinnunen ym., 2017; Swan, 2015)	Bitcoin: hajautettu kryptovaluutta.

3.2 Konsensusmekanismit

Konsensusprotokollat ovat mekanismi, jonka avulla lohkoketjujen käyttäjät vahvistavat datan oikeellisuuden. 4 keskeisintä konsensusprotokollaa ovat Proof of Work (PoW), Proof of Stake (PoS), Ripple Protocol ja Proof of Elapsed Time (PoET). (ENISA, 2016.) Konsensusmekanismi mahdollistaa verkossa suoritettavat transaktiot ilman kolmansia luottamuksen takaavia osapuolia tai välittäjiä (Swan, 2015).

Useimmissa kryptovaluutoissa käytetään proof-of-work -konsensusta, jonka Nakamoto esitteli 2009 artikkelissaan *Bitcoin: A peer-to-peer electronic cash system*. Protokollan avulla kryptovaluutat voidaan toteuttaa hajautetusti, jolloin uudet lohkot tuotetaan louhimalla. Louhijat vahvistavat ja hyväksyvät transaktioita samalla kun luovat uusia lohkoja, eli louhivat. Louhijat palkitaan uusilla coineilla esimerkiksi Bitcoineilla Bitcoin-lohkoketjussa uusista lohkoista. (Luu, Teutsch, Kulkarni & Saxena, 2015.) Proof of Work -protokollan yksi keskeinen ongelma on sen suuri energian kulutus. (Zheng ym., 2018)

Proof-of-stake-protokolla vaatii käyttäjiä todistamaan, että he omistavat tietyn määrän kryptovaluuttaa. Ratkaisua perustellaan sillä, että paljon kryptovaluuttaa omistavien henkilöiden uskotaan olevan vähemmän motivoituneita hyökkäämään verkkoon. PoS ratkaisee korkeaan energian kulutukseen liittyvän ongelman mutta sen ongelmana on epäoikeudenmukaiseksi koettu paljon kryptovaluuttaa omistavien suosiminen. (Zheng ym., 2018.)

Ripple-konsensusalgoritmi (RPCA) perustuu käyttäjien arvioihin toistensa luotettavuudesta, joiden perusteella se muodostaa kullekin solmulle uniikin listan konsensuksen muodostavista solmuista. Koska konsensuksen muodostamiseen ei tarvita kaikkia verkon solmuja, se onnistuu huomattavasti nopeammin kuin esimerkiksi PoW-mekanismissa. Tämän ansiosta RPCA:ta käyttävät lohkoketjut ovat skaalautuvia. (Schwarz, Youngs & Britto, 2014.)

PoET korvaa PoW:n luotettavalla laitteistolla, kuten Intel SGX. Vaikka protokolla ratkaiseekin PoW:n energiatehokkuuteen liittyvän ongelman, se tulee samalla luoneeksi vastaavan ongelman, jossa laskentatehon sijaan hankitaankin suuria määriä luotettavia laitteita. Toisin sanoen suuri energian kulutus korvautuu tolkuttomalla määrällä laitteita. (Eyal, 2017.)

3.3 Tokenit

Kryptotokenit ovat digitaalista varallisuutta, jota säilytetään kryptovaluutassa tai lohkoketjutokenissa eli erillisenä tokenina lohkoketjussa ja jota hallitaan älykkäällä sopimuksella, jotta sitä voi käyttää hajautetussa sovelluksessa tai projektissa. Kryptotokenit ovat samanlaisia kuin kryptovaluutat, mutta niillä ei ole omaa lohkoketjua, vaan sen sijaan ne on toteutettu jo ennestään olemassa olevaan lohkoketjuun. (Di Angelo & Salzer, 2020.)

Tokeneita voidaan käyttää maksuvälineenä ja ne voivat olla jonkin hajautetun sovelluksen oma maksuväline. Niitä voi käyttää myös moneen muuhun tarkoitukseen, koska ne ovat ohjelmoitavissa. Niitä voidaan esimerkiksi käyttää erilaisten toimintojen käynnistämiseen älykkäissä sopimuksissa tai niitä voi linkittää lohkoketjun ulkopuoliseen omaisuuteen. Ne toimivat varainhankinnassa ja sijoitusvälineenä mutta ne voivat myös olla rakennuspalikoita ekosysteemissä tai yhteisössä. (Di Angelo & Salzer, 2020)

Hyödyketokenit sisältävät yleensä jonkin määriteltävissä olevan etuisuuden, jonka tarjoaa jokin projekti, sovellus tai hajautettu sovellus. Etu voi olla esimerkiksi oikeus käyttää jotain palvelua. Hyödyketokenit on tarkoitettu tarjoamaan sovellusten ja palveluiden käyttöoikeuksia digitaalisesti, jolloin ne palvelevat digitaalisena lohkoketjuun pohjautuvana infrastruktuurina. Niihin voi sisältyä esimerkiksi äänioikeuksia tai palkkioita. (Di Angelo & Salzer, 2020.)

Älykkäät sopimukset ovat keskeisessä roolissa tokenien liikkeellelaskuissa. Älykkäissä sopimuksissa määritellyt säännöt voivat määrittää esimerkiksi tokenien hintaa ja myyntiaikoja. Useimmat tokeneiden liikkeellelaskut on toteutettu Ethereumin lohkoketjuprotokollassa. Liikkeellelaskijat käyttävät älykkäitä sopimuksia, joissa on tarpeen mukaan muunneltuja ominaisuuksia. Kun liikkeellelasku on toteutettu, älykäs sopimus aktivoituu ja se pystyy ottamaan vastaan sijoittajien varoja. Tyypillisesti tokenien liikkeellelaskuissa vaihtaa omistajaa erilaiset kryptovarallisuuden lajit. Kun älykkäät sopimukset ottavat vastaan varoja, ne siirtävät vastaavan määrän varoja sijoittajan lompakkoon. Nämä transaktiot ovat louhijoiden varmentamia ja talletettu lohkoketjuun. Liikkeellelaskun

jälkeen tokenit voi listata kryptopörsseihin ja niillä voi käydä kauppaa. (Kranz, Nagel & Yoo,2019.)

3.4 Älykkäät sopimukset

Lohkoketjuissa voidaan käyttää älykkäitä sopimuksia, jotka ovat ohjelmakoodilla toteutettuja tietokoneohjelmia ja toteuttavat itsensä tiettyjen ennalta määrättyjen sopimusehtojen toteuduttua. (Lauslahti ym., 2016) Älykkäisiin sopimuksiin viitataan myös tarkemmalla käsitteellä suoritettavat hajautetut ohjelmoidut sopimukset eli Executable Distributed Code Contracts (EDCC), mikä on tarkempi termi älykkäille sopimuksille. (Wessling & Gruhn, 2018) Moniin älykkäisiin sopimuksiin pohjautuviin projekteihin viitataan usein termillä hajautettu rahoitusmaailma eli englanniksi decentralized finance (DeFi). (Livshits, 2020)

Älykkäillä sopimuksilla voi automatisoida sopimusten toimeenpanon ja sellaista voisi käyttää esimerkiksi siirtämään auton omistajuus automaattisesti rahoitusyhtiöltä yksityishenkilölle, kun lainan viimeinen maksuerä on suoritettu. (Swan, 2015) Älykkäissä sopimuksissa voi olla mukana kaksi tai useampia osapuolia. (Yli-Huumo, Ko, Choi, Park & Smolander, 2016) Vaikka älykkäät sopimukset on keksitty kauan sitten, lohkoketjuteknologia on merkittävästi lisännyt niiden käyttöä ja kasvun taustalla on erityisesti Ethereum-virtuaalikone ja muut vastaavat järjestelmät. (Livshits, 2020) Ethereum on monimutkainen ekosysteemi, joka mahdollistaa hajautetun rahoitusmaailman (DeFi), stablecoinit ja paljon muuta. (Zheng, Zheng, Wu & Dai, 2020)

Rouhanin ja Detersin (2019) mukaan älykkäisiin sopimuksiin pohjautuvat sovellukset voidaan jaotella IoT-, terveydenhuolto-, toimitusketju-, yritysprosessien hallinta-, kirjanpito-, äänestys, ja digitaalisen identiteetin hallintasovelluksiin. Älykkäiden sopimusten avulla voidaan toteuttaa hajautettuja sovelluksia (distributed applications), joilla voi korvata kolmansia osapuolia ja käyttää sen sijaan osapuolten keskinäisiä transaktioita (peer-to-peer transaction). Älykkäillä sopimuksilla voidaan säästää kustannuksia raskaasti säännellyissä ympäristöissä ja niiden avulla voidaan toteuttaa kaupallisia transaktioita varten alustoja, joissa on vähemmän välivaiheita kuin perinteisissä vaihtoehdoissa. (Norta, Fernandez & Hickmott, 2018) Jotkut älykkäisiin sopimuksiin soveltuvat lohkoketjualustat tukevat älykkäiden sopimusten ohjelmoinnissa yleisesti tunnettuja ohjelmointikieliä, kuten Java, C++, NodeJS, Python ja Go. Näiden lisäksi älykkäiden sopimusten ohjelmoinnissa voi käyttää erityisesti älykkäiden sopimusten ohjelmointiin kehitettyjä kieliä, joista tunnetuin on Solidity. (Rouhani & Deters, 2019.)

3.4.1 Hajautetut sovellukset

Lohkoketju ja älykäs sopimus tarjoavat kätevän välineen hajautettujen sovellusten toteuttamiseen. Tunnetuimpia esimerkkejä hajautetuista sovelluksista ovat hajautetut kryptopörssit. (Hsieh, Hsueh & Wu, 2018) Hajautetut sovellukset ja

älykkäät sopimukset mahdollistavat uudenlaiset organisatoriset järjestelyt yksilöiden ja entiteettien välillä ennalta ohjelmoitujen transaktioiden avulla, joiden ansiosta tarvitaan vähemmän hallintoa ja edunvalvontaa. (Casey ym., 2018) Niillä voidaan mahdollistaa luottamuksettomat peer-to-peer-transaktiot ja vähentää tarvetta kolmansille osapuolille lohkoketjun toimiessa pysyvänä tapahtumien kirjaamisalustana. (Norta ym., 2018)

Frankenfield (2018) määrittelee hajautetut sovellukset digitaalisiksi sovelluksiksi tai ohjelmiksi, jotka on toteutettu ja joita käytetään lohkoketjussa tai vertaisverkossa yksittäisen tietokoneen sijasta ja yksittäisten toimijoiden toimivallan ja kontrollin ulottumattomissa. Wesslingin ja Gruhnin (2018) mukaan Hajautettu sovellus voidaan kuvata avoimen lähdekoodin ohjelmistoksi, johon liittyvä data ja käyttömerkinnät tallennetaan hajautettuun kirjanpitokirjaan, ja jonka yhdenmukaisuus käyttäjien kesken varmistetaan käyttäen konsensusalgoritmia ja soveltaen tokenmekanismia. Heidän mukaansa hajautetut sovellukset koostuvat liiketoimintalogiikasta ja käyttöliittymästä, jonka avulla hajautetun sovelluksen kanssa ollaan vuorovaikutuksessa. He esittävät, että liiketoimintalogiikkaa edustaa yksi tai useampi älykäs sopimus, joka on sijoitettu lohkoketjuverkostoon. Hajautettujen sovellusten front end on yleensä selain- tai sovelluskäyttöliittymä ja back end on osittain tai kokonaan toteutettu lohkoketjussa tai kryptovaluutassa. (Di Angelo & Salzer, 2020) Joidenkin hajautetun sovelluksen määritelmien mukaan myös Bitcoinia voidaan pitää hajautettuna sovelluksena. (Johnston ym. 2014)

Nykyisten hajautettujen sovellusten käyttöliittymät on toteutettu keskitetysti, koska niiden hallintaan käytettävä verkkosivu tyypillisesti toimii jollakin tietyllä palvelimella. Tulevaisuudessa myös käyttöliittymät voidaan luultavasti toteuttaa hajautetusti käyttämällä esimerkiksi tiedostojen hajautukseen tarkoitettua lohkoketjuteknologiaa hyödyntävää IPFS-protokollaa (interplanetary file system), jolloin sovelluksista tulee täysin hajautettuja. (Metcalfe, 2020)

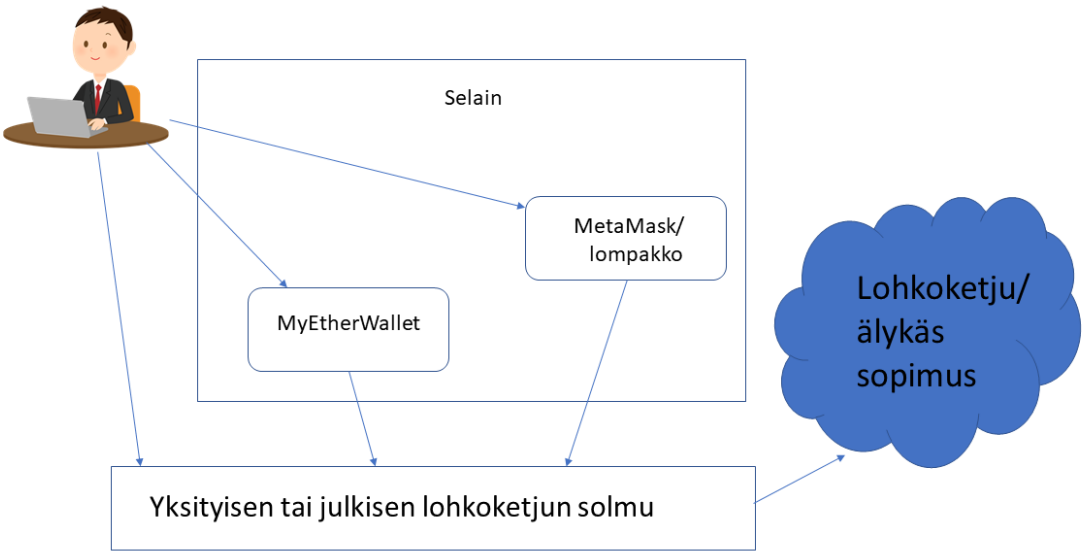
Hajautettuja sovelluksia kuvaillaan usein luottamuksettomiksi tai peer-to-peer-pohjaisiksi ja ero keskitettyihin sovelluksiin on se, ettei niillä ole yksittäistä palvelinta tai entiteettiä, joka kontrolloisi niitä, kuten asiakasohjelmamallissa tyypillisesti tapahtuu. (Metcalfe, 2020) Hajautetuissa sovelluksissa lohkoketjua käytetään datan varastointiin ja prosessointiin ja prosessointi toteutetaan älykkäiden sopimusten avulla. Hajautettujen sovellusten käyttöliittymät ovat tyypillisesti perinteisiä verkkosivuja, joten yksinkertaistettuna hajautettua sovellusta voisi kuvailla verkkosivun ja yhden tai useamman älykkään sopimuksen yhdistelmäksi. (Metcalfe, 2020)

Hajautettujen sovellusten käytöstä seuraa kolme etua: 1) Käyttäjä voi nähdä, mitä tulee tapahtumaan ennen kuin antaa sovellukselle mitään dataa, 2) kun käyttäjä on suorittanut toiminnon, sitä ei voi jälkikäteen vaihtaa, peukaloida tai poistaa, 3) hallinto voidaan hajauttaa, jolloin hajautetun sovelluksen käyttäjät voivat osallistua siihen suoraan. (Metcalfe, 2020)

Hajautettujen sovellusten avulla voidaan parantaa käyttäjien kontrollia datan suhteen, jolloin sen sijaan, että käyttäjien data päätyy suurille yrityksille, se on käyttäjien hallussa. (Metcalfe, 2020) Hajautetut sovellukset eivät ole mobiilisovelluksia. Niiden käyttäminen edellyttää yhteyttä lohkoketjuun ja käyttämiseen

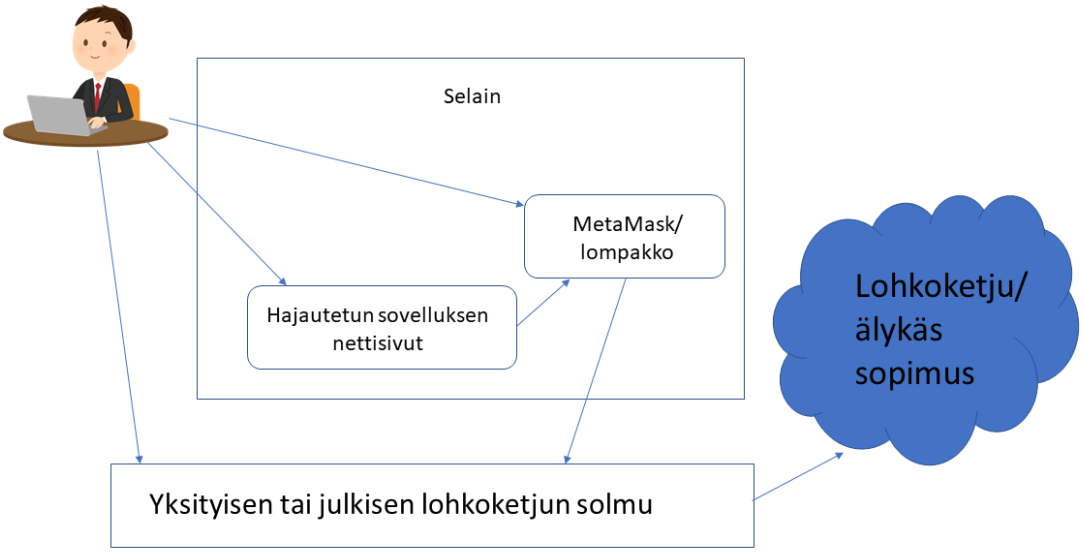
tarvitaan erityinen selain, kuten Mist, selaimen lisäosa, kuten Metamask tai mobiilikäyttöön tarkoitettu Trust-selain. (Quiniou, 2019) Erityyppisistä hajautetuista sovelluksista voi saada käsityksen tutustumalla sivustoon State of Dapps, johon on koottu tietoja monista hajautetuista sovelluksista. (Quiniou, 2019) Sivusto luokittelee hajautetut sovellukset kahdeksaantoista eri kategoriaan: 1) pelit, 2) kryptopörssit, 3) vedonlyönti, 4) rahoitus, 5) sosiaalinen media, 6) kehittäminen, 7) tallettaminen, 8) korkeariskiset, 9) media, 10) lompakot, 11) kauppapaikat, 12) hallinto, 13) turvallisuus, 14) kiinteistöt, 15) identiteetin hallinta, 16) energia, 17) terveys ja 18) vakuutus. (State of DApps, 25.10.2020) Yksi keskeisimmistä kategorioista hajautetuissa sovelluksissa on hajautettu finanssimaailma, mihin kuuluu esimerkiksi varainhankinta, rahoituspalvelut ja omaisuuden arvopaperistaminen. Muita tärkeitä kategorioita ovat uhkapelit, markkinapaikat, tunnistetietojen tarjonta, toimitusketjujen hallinta ja pelit. (Di Angelo & Salzer, 2020.; Metcalfe, 2020.)

Hajautettujen sovellusten etuosa eli front end, joka mahdollistaa vuorovaikutuksen liiketoimintalogiikan kanssa, voidaan toteuttaa monella tavalla. (Welllng & Gruhn, 2018) Wesslingin ja Gruhnin mukaan hajautetuissa sovelluksissa on 3 vaihtoehtoista pohja-arkkitehtuuria (A, B ja C). Kuviossa 2 on yksinkertaistettuna hajautettujen sovellusten pohja-arkkitehtuuri A, jossa käyttäjä on suoraan vuorovaikutuksessa älykkään sopimuksen kanssa tuottamalla ja lähettämällä transaktioita itsenäisesti. (Wessling & Gruhn, 2018) Vuorovaikutus älykkään sopimuksen kanssa voidaan tässä tapauksessa toteuttaa kolmella tavalla: 1) käyttäjä lähettää transaktiot suoraan lohkoketjuun, 2) käyttäjä käyttää front endinä MyEtherWallet -asiakasohjelmaa eli clientiä, 3) käyttäjä käyttää selaimen sisään rakennettua MetaMask-lompakkoa tai esimerkiksi Status- tai Cipher-selainta, joka toimii myös lompakkona. (Wessling & Gruhn, 2018)



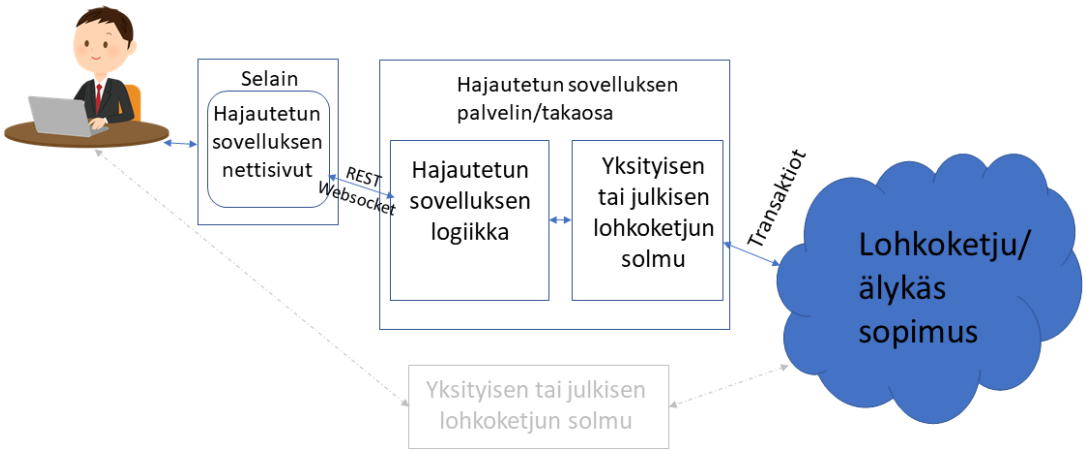
KUVIO 2 Yksinkertaistettu esitys hajautetun sovelluksen pohja-arkkitehtuurista A, jossa transaktiot tuotetaan itse. (Wessling & Gruhn, 2018, s. 45)

Jotta älykkään sopimuksen kanssa voi olla suoraan vuorovaikutuksessa, on tärkeää, että älykäs sopimus on julkisesti käytettävissä. (Wessling & Gruhn, 2018) Jotta kunkin älykkään sopimuksen toimeenpanema toiminta voidaan ymmärtää, lähdekoodin tulisi myös olla saatavilla. (Wessling & Gruhn, 2018) Kun hajautettu sopimus on suoraan vuorovaikutuksessa älykkään sopimuksen kanssa, käyttäjän ei tarvitse luovuttaa yksityisiä avaimiaan kolmansille osapuolille, vaan ne voidaan säilyttää omalla laitteella, jolloin he voivat tuottaa, allekirjoittaa ja lähettää transaktioita itsenäisesti. (Wessling & Gruhn, 2018) Tällaisen rakenteen ansiosta allekirjoitettuja transaktioita ei voi manipuloida eikä niiden toteuttaminen edellytä kolmansien osapuolten apua, joten rakenne mahdollistaa hajautetun sopimuksen käytön lähes luottamuksettomasti. Suora vuorovaikutus älykkään sopimuksen kanssa vaatii kuitenkin teknistä osaamista ja se on myös altis virheille. (Wessling & Gruhn, 2018.) Tällainen arkkitehtuuri löytyy esimerkiksi hajautetuista kryptopörsseistä, kuten EtherDelta tai IDEX ja uhkapelisovelluksista, kuten Ethorse. (Wessling & Gruhn, 2018)



KUVIO 3 Yksinkertaistettu esitys hajautetun sovelluksen pohja-arkkitehtuurista B jossa transaktiot vahvistetaan itse. (Wessling & Gruhn, 2018, s. 46)

Kuviossa 3 on esitetty hajautetun sovelluksen pohja-arkkitehtuuri B, joka on käyttäjän kannalta miellyttävämpi kuin arkkitehtuuri A, koska siinä ollaan vuorovaikutuksessa hajautetun sovelluksen kanssa kryptoselaimen tai selaimen lisäosan, MetaMaskin, avulla. Tässä tapauksessa käyttäjä tuottaa transaktiot, mutta hajautetun sovelluksen internetsivusto käynnistää ne ja toimittaa ne käyttäjälle varmistettavaksi, minkä jälkeen ne lähetetään lohkoketjuun manuaalisesti. (Wessling & Gruhn, 2018) Luotettavuuden kannalta tämä malli ei ole yhtä hyvä kuin malli A. Transaktioiden tuottaminen manuaalisesti voi olla vaikeaa tai epätarkoituksenmukaista erityisesti silloin, kun on tärkeää selvittää sen hetkinen lohkoketjun tila tai kerätä lisää dataa. Arkkitehtuurissa B sovelluksen tarjoajalta edellytetään A:ta enemmän luotettavuutta, koska transaktioiden suorittaminen ei ole täysin läpinäkyvää. (Wessling & Gruhn, 2018)



KUVIO 4 Yksinkertaistettu esitys hajautetun sovelluksen pohja-arkkitehtuurista C, jossa transaktiot on delegoitu. (Wessling & Gruhn, 2018, s. 46)

Kuviossa 4 on kuvattuna hajautetun sopimuksen pohja-arkkitehtuuri C, joka on käyttäjän kannalta vielä mukavampi kuin pohja-arkkitehtuuri B. Tässä arkkitehtuurissa hajautetun sovelluksen palvelut tarjotaan internetsivuston kautta, eikä palvelun käyttö edellytä MetaMask-lisäosan tai kryptoselaimen käyttöä. Internetsivusto kommunikoi hajautetun sovelluksen takaosan eli backendin kanssa REST-kutsuilla ja kapseloi lohkoketjukohtaiset toiminnot. (Wessling & Gruhn, 2018) Takaosan tehtävä on olla vuorovaikutuksessa lohkoketjun kanssa ja lähettää transaktiot käyttäjän puolesta, joka ei voi vahvistaa niitä. Tämä pohja-arkkitehtuuri edellyttää siksi täydellistä luottamusta palveluntarjoajaan, joka käsittelee käyttäjän kirjautumiset ja jolla on hallussaan käyttäjän yksityinen avain. Siinä tapauksessa, että palveluntarjoajan käyttämät älykkäät sopimukset tiedetään, käyttäjä voi tarkistaa takaosan käynnistämien transaktioiden suoritukset. Käyttäjä voi tarkkailla älykkään sopimuksen tilaa ja saada palautetta websocket-rajapinnan avulla palveluntarjoajan kautta. Esimerkkejä tällaisesta hajautetusta sovelluksesta ovat kryptopörssit kuten Kraken tai Binance, koska ne kommunikoivat lohkoketjun kanssa käyttäjän puolesta. (Wessling & Gruhn, 2018)

3.4.2 Ethereum-virtuaalikone

Ethereum-lohkoketjun ensimmäinen lohko eli alkulohko louhittiin 30 heinäkuuta 2015. (Paavolainen, Elo & Nikander, 2018) Ethereum mahdollistaa virtuaalisen ympäristön tietokoneohjelmien käyttämiseen autonomisesti siirtämällä ne lohkoketjuun ja minkä tahansa niukan hyödykkeen muuttamisen token muotoon, minkä ansiosta Ethereum-alustalle on rakennettu hyvin monenlaisia palveluita ja sovelluksia sekä niihin liittyen erilaisia tokeneita, joita käytetään vuorovaikutuksessa hajautettujen sovellusten kanssa. (Hsieh ym., 2018; Patsonakis Roussopoulos; Chen, 2018) Hajautetut sovellukset voivat ottaa vastaan ja siirtää Ethereum-alustan sisään rakennettua ETH-kryptovaluuttaa tai ne saattavat laskea liikkeelle niiden omia erityisiin tarpeisiin suunniteltuja tokeneita. (Rahimian, Eskandari & Clark, 2019) Räätälöidyt tokenit ovat kiinteä osa Ethereum- ja muille

alustoille sijoitettuja hajautettuja sovelluksia. Ethereum-alustalla ERC20-standardia käytetään laajasti tokenien käyttöliittymänä ja se on yhteensopiva monien hajautettujen sovellusten, käyttöliittymäalustojen ja suosittujen internetsovellusten kanssa. (Rahimian ym., 2019)

Ethereum-alustan sisältämät hajautetut sovellukset tarjoavat esimerkiksi nimipalvelua, moniallekirjoitusta hyödyntäviä lompakoita, paljon kaupankäyntikelpoisia tokeneita ja kryptattuja keräilykohteita. Se sopii luonnostaan datan varastointiin, kyselyihin ja oikeellisuuden tarkistamiseen, minkä vuoksi sen päälle on helppo rakentaa hajautettuja sovelluksia. (Patsonakis & Roussopoulos, 2019)

Ethereum-alustan avulla voi toteuttaa älykkäitä sopimuksia hyödyntäviä joukkorahoituskampanjoita, joita kutsutaan yleensä ICO:iksi ja niissä myydään tiettyjen hajautettujen sovellusten tokeneita Ether-kryptovaluuttaa vastaan. Hajautettujen sovellusten tokenit voivat toimia kansallisvaluutan tavoin tai niihin on voitu identifioida jonkinlainen osakkeenomistaja. (Chen, Zhang, Chen, Zhang & Lu, 2020)

3.5 Standardit

Lohkoketjuteknologian yleistymisen ja käyttöönoton kannalta on tärkeää kehittää standardeja, joiden avulla erilaiset lohkoketjuteknologiaan pohjautuvat järjestelyt ja ennestään olemassa olevat järjestelyt saadaan toimimaan yhteen. Avointen standardien avulla voidaan pienentää käyttöönotto- ja integraatiokustannuksia ja varmistaa, että odotukset lohkoketjuteknologiaan pohjautuvissa järjestelyissä ovat johdonmukaisia sen suhteen, kuinka informaatio on järjestetty ja kuinka siihen päästään käsiksi. (Mills ym., 2016.) Koska lohkoketjuteknologiassa on kyse pitkälti tietojen säilyttämisestä, sen soveltamiseen liittyvää vaatimusmäärittelyä voidaan arvioida myös tietojen säilyttämistä koskevien standardien, kuten ISO 15 489, ARMA:n yleisesti hyväksytyt kirjanpitoperiaatteet, ISO 14 721 ja ISO 16 363 kautta. (Lemieoux, 2016)

Jos uusia lohkoketjuteknologiaan pohjautuvia sovelluksia otetaan käyttöön ilman koordinointia, on vaarana lukemattomien eri standardeihin pohjautuvien siiloutuneiden sovellusten tulo markkinoille. (DTCC, 2016) Ethereumin ensimmäisinä vuosina sen alustalle tehtiin parissa vuodessa lukuisia hajautettuja sovelluksia älykkäisiin sopimuksiin pohjautuvaa kaupankäyntiä varten. Nopea iterointi ja puute parhaista käytännöistä johti siihen, että loppukäyttäjille oli tarjolla lukuisia erilaisia patentoituja tai tiettyyn sovellukseen liittyviä sovelluskohtaisia toteutuksia, jotka kuitenkin liittyivät samaan käyttötapaukseen eli kaupankäyntiin. (Warren & Bandeali, 2017.) Tätä ongelmaa ratkaisemaan on kehitetty esimerkiksi 0x, joka on avoimeen lähdekoodiin pohjautuva kaupankäyntiprotokolla. Se on tarkoitettu peruselementiksi, joka mahdollistaa uudet entistä paremmat protokollat. Taustalla on pyrkimys myös siihen, että avoimet protokollat syrjäyttäisivät pitkällä aikavälillä suljetut, kun lohkoketjuihin lisätään uutta token muotoista omaisuutta. (Warren & Bandeali, 2017.)

3.6 Lohkoketjuteknologiaan liittyvät riskit

Yleisimmät lohkoketjuteknologian käyttöön liittyvät riskit voidaan jakaa yhdeksään kategoriaan: 1) 51 %:n hyökkäykset, 2) yksityisen avaimen turvallisuus, 3) rikollinen toiminta, 4) double-spending-hyökkäys, 5) transaktioiden yksityisyyden vuotaminen, 6) rikolliset älykkäät sopimukset, 7) älykkäiden sopimusten haavoittuvuudet, 8) alioptimoidut älykkäät sopimukset ja 9) alihinnoitellut toiminnot. (Li, Jiang, Chen, Luo & Wen, 2020) Tässä alaluvussa näitä riskejä kuvaillaan lyhyesti.

51 %:n hyökkäykset perustuvat konsensusmekanismien hyväksikäyttöön, jossa hyökkääjä saa kontrolliinsa koko lohkoketjun. PoW-konsensusmekanismia käyttävässä lohkoketjussa se tarkoittaa sitä, että yksi louhija saa haltuunsa yli 50 % laskentatehosta ja PoS-konsensusmekanismissa se tarkoittaa sitä, että yksi louhija pitää hallussaan yli 50 %:n osuutta kaikista louhituista kryptovaluutoista. (Li ym., 2020.) Haavoittuvuuden takia hyökkääjä voi toteuttaa neljä erilaista hyökkäystä. peruuttaa tehtyjä transaktioita, muuttaa transaktiodataa, mikä voi aiheuttaa double-spending-hyökkäyksen, estää transaktioiden verifioinnin ja pysäyttää louhinnan. (Zheng ym., 2018; Lin & Liao, 2017)

Double-spending-hyökkäyksissä samoja krypto-omaisuuseriä käytetään moneen kertaan transaktioihin. (Li ym., 2020) Vaikka konsensusjärjestelmät varmistavat transaktioiden oikeellisuuden, double-spending-hyökkäyksiä ei voida kokonaan välttää. Esimerkiksi tilanteissa, joissa transaktion on tarkoitus tapahtua välittömästi, kuten maksettaessa ostoksia kivijalkakaupassa Bitcoinilla, double-spending-hyökkäys on mahdollinen, koska transaktioiden käsittelyyn menee keskimäärin 10 minuuttia ja hyökkääjä voi käyttää tätä viivettä hyväkseen. (Karame ym., 2015.)

Lohkoketjuihin on olemassa monenlaisia menetelmiä digitaalisia allekirjoituksia varten. (Fang ym, 2020) Niillä todennetaan transaktioiden kelvollisuus käyttämällä kryptografista algoritmia. Ne muodostuvat kolmesta ydinkomponentista, avaintenkehittämisalgoritmi, kirjautumisalgoritmi ja varmennusalgoritmi. Avaintenkehittämisalgoritmi tuottaa yksityisestä ja julkisesta avaimesta koostuvat kirjautumistiedot. Kirjautumisalgoritmi tuottaa allekirjoituksen syötteeseen, joka on allekirjoitettu yksityisellä avaimella. Varmennusalgoritmi ottaa vastaan allekirjoitussyötteen ja tarkistaa sen oikeellisuuden käyttäen syötteenä julkista avainta, minkä jälkeen se palauttaa boolean-arvon. (Zhang, Xue & Liu, 2019.) Lohkoketjuja käytettäessä käyttäjillä on hallussaan yksityinen avain, jonka avulla suoritetaan digitaalinen allekirjoitus transaktioiden oikeellisuuden varmistamiseksi. (Srivastav, Agrawal & Shivastava, 2020) Käyttäjien tietoja ei yleensä rekisteröidä millekään keskitetylle viranomaistaholle. (Zhang, Xue & Liu, 2019) Jos yksityinen avain menetetään, sitä ei voi korvata tai palauttaa mitenkään. Jos se joutuu varkaiden haltuun, käyttäjän lohkoketjutili on vaarassa tulla peukaloiduksi. Rikollisten liikkeitä on myös vaikea seurata ja muunneltuja tietoja lohkoketjussa on vaikea palauttaa ennalleen. (Li ym., 2020)

Bitcoinin lohkoketjussa ja myös monessa muussa lohkoketjussa käytetään elliptisen käyrän digitaalisen allekirjoituksen algoritmia (ECDSA) digitaalisen identiteetin hallintaan. Se ei tuota riittävästi satunnaisuutta allekirjoitusprosessin aikana, minkä vuoksi hyökkääjä voi mahdollisesti varastaa yksityisen avaimen. (Hussein & Kashmar, 2020)

Bitcoin- ja Ethereum-lompakoiden pseudonyymisyys mahdollistaa sen, että käyttäjillä voi olla useita lompakoita, eikä heidän todellinen identiteettinsä ole viranomaisten tiedossa. Tämän vuoksi erityisesti Bitcoinia käytetään paljon rikollisiin tarkoituksiin. (Liu ym, 2020; Li ym., 2020.) Monilla kolmansien osapuolten ylläpitämillä kaupankäyntialustoilla voi käyttää maksuvälineenä Bitcoinia, ja niillä voi ostaa mitä tahansa. Koska kaupankäyntiprosessi on anonyymi, sen avulla on vaikea seurata käyttäjien käyttäytymistä myös silloin, kun se on rikollista. (Li ym., 2020) Edellä mainituista syistä Bitcoinin avulla käytetään kiristysohjelmia, käydään laitonta kauppaa ja pestään rahaa. (Li ym., 2020).

Koska käyttäjien transaktiot lohkoketjuissa ovat jäljitettävissä, on lohkoketjujärjestelmissä tehty toimenpiteitä transaktioiden yksityisyyden suojaamiseksi. Bitcoin- ja Zcash-lohkoketjuissa käytetään tähän tarkoitukseen kertakäyttöisiä tilejä vastaanotetun kryptovaluutan säilyttämiseen. (Li ym., 2020) Lisäksi se, että kussakin transaktioissa käytetään erilaista yksityistä avainta, vaikeuttaa hyökkääjien pyrkimystä selvittää transaktioiden vastaanottajan identiteetti. Yksityisyyden lisäämiseen käytetään Monero-lohkoketjussa myös erityisiä hämäysrahakkeita, joiden tarkoitus on estää hyökkääjää selvittämästä todellisen transaktion suuruutta. (Li y., 2020.) Nämä menetelmät yksityisyyden lisäämiseksi eivät kuitenkaan ole kovin luotettavia, minkä vuoksi transaktioiden yksityisyyttä ei voida täysin varmistaa. (Li ym., 2020)

Monet lohkoketjuteknologian haavoittuvuudet liittyvät erityisesti älykkäisiin sopimuksiin. Älykkäitä sopimuksia voidaan käyttää monenlaisiin rikollisiin tarkoituksiin. (li ym., 2020) Rikolliset älykkäät sopimukset voivat helpottaa luottamuksellisen tiedon vuotamista, salausavainten varkauksia ja monenlaisia reaalimaailman rikoksia, kuten murhat, tuhopoltot ja terrorismi. (Juels, Kosba & Shi, 2016)

Älykkäissä sopimuksissa voi olla haavoittuvuuksia, jotka perustuvat puutteelliseen ohjelmointiin. (Li ym., 2020) Solidity-ohjelmointikielen semantiikka on ohjelmoijien kannalta epäjohdonmukainen ja epäintuitiivinen, mistä seuraa virheherkkyyttä. (Atzei, Bartoletti & Cimoli, 2017) Haavoittuvuudet ovat aiheuttaneet vakavia seuraamuksia. Tunnetuin esimerkki on DAO-hyökkäys, jossa hyökkääjät varastivat kryptovaluuttaa 60 miljoonan dollarin arvosta käyttämällä hyväkseen Parity Wallet -kirjastossa olevaa ohjelmointivirhettä. (Mavridou, Laszka, Stachtiari & Dubey, 2019) Luu ym. (2016) tutkivat kehittämällään Oyente-työkalulla 19 366 Ethereum-sopimusta joista 8 833 sisälsi haavoittuvuuden. Atzei ym. (2017) jakoivat systemaattisessa tutkimuksessaan Ethereum-sopimusten haavoittuvuudet 12 erilaiseen tyyppiin, joita esiintyy kolmella eri tasolla: Solidity, EVM-tavukoodi ja lohkoketju.

Kun käytetään älykkäitä sopimuksia Ethereum-lohkoketjussa, syntyy tietty määrä gas-kustannuksia, jotka hinnoitellaan Ether-kryptovaluutassa. Niillä

katetaan louhinnan kustannuksia louhijoille. Kaikki älykkäät sopimukset eivät ole gas-kustannusten kannalta optimaalisia. Chen, Li, Luo ja Zhang (2017.) luokittelevat epäoptimaaliset sopimukset seitsemään erilaiseen tyyppiin, jotka jaetaan kahteen kategoriaan, joista toinen liittyy käyttökelvottomaan koodiin ja toinen silmukoihin.

Käyttökelvottomaan koodiin liittyviä tyyppejä on kaksi:

- *Kuollut koodi:* koodi, jota ei suoriteta.
- *Näkyvä predikaattifunktio*: (opaque predicate) predikaattifunktio, jonka totuusarvo tiedetään ilman suorittamista.

Silmukoihin liittyviä tyyppejä on viisi:

- *Kalliit toiminnot:* toiminnot, jotka voidaan toteuttaa toisella vähemmän gas-yksikköjä käyttävällä tavalla.
- *Silmukan lopputuloksena on vakio:* silmukan suorittaminen johtaa aina samaan lopputulokseen.
- *Ylimääräiset silmukat:* silmukat, joiden toiminnot voitaisiin yhdistää toiseen silmukkaan, mikä säästää gas-yksikköjä.
- *Toistetut laskennat:* tilanteet, joissa silmukka suoritetaan useita kertoja sen sijaan, että se ajettaisiin kerran ja silmukan palauttama lopputulos käytettäisiin uudelleen.
- *Vertailu yksipuoliseen lopputulokseen:* vertailu suoritetaan jokaisessa silmukan iteraatiossa, vaikka vertailun lopputulos on aina sama. (Chen ym., 2017.)

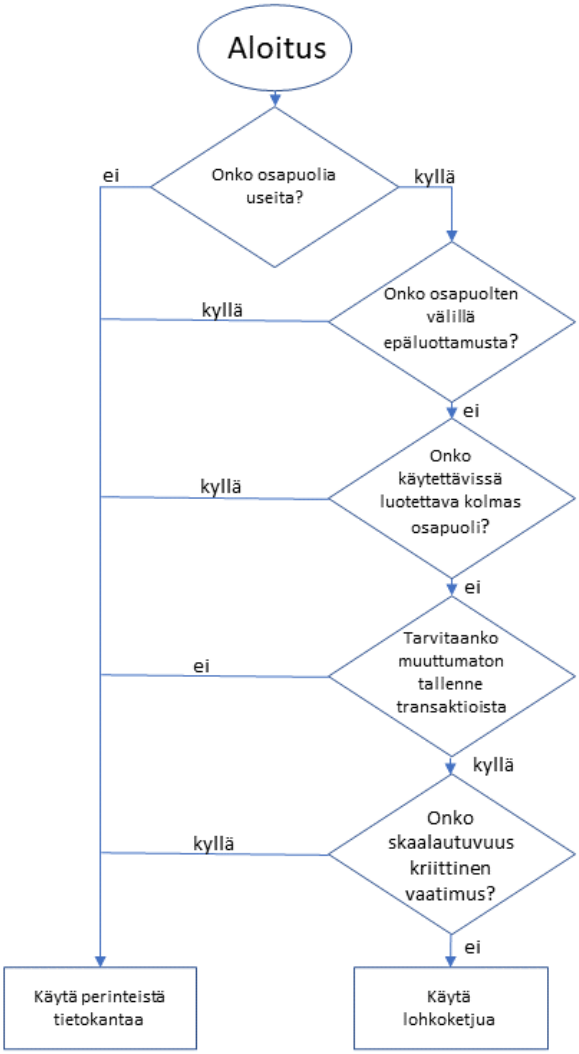
Alihinnoitellut toiminnot ovat sellaisia toimintoja lohkoketjuissa, joita hyökkääjät voivat käyttää palvelunestohyökkäykseen niiden alhaisen hinnan takia. Ethereum-lohkoketjussa hyökkääjät ovat käyttäneet palvelunestohyökkäyksissä EXTCODESIZE- ja SUICIDE-toimintoja. (Li ym., 2020.)

Se, että lohkoketjuteknologiasta puhutaan luottamuksettomana, voi aiheuttaa valheellisen turvallisuudentunteen. Lohkoketjuteknologiaan liittyy monia luottamustekijöitä. Kun organisaatiot ottavat käyttöönsä lohkoketjuteknologiaa, niiden tulisi ottaa huomioon samalla vaikeasti havaittavat luottamussuhteet, jotka lohkoketjut tuovat tullessaan ja ymmärtää niihin liittyvät turvallisuusriskit. (Puzt & Pernul, 2019)

Yksi lohkoketjuteknologian yleistymisen esteistä on se, että alan osaajista on pulaa ja harvat ohjelmoijat ymmärtävät, mistä lohkoketjuteknologiassa on kyse. (Honkanen, 2017.) Sovelluskehittämisen kannalta on tärkeää, että kyetään ideoimaan ja toteuttamaan toimivia sovelluksia. Lisäksi tarvitaan sovelluksille asiakaskunta, joka ymmärtää mihin lohkoketjuteknologia soveltuu ja mihin se ei sovellu. (Honkanen, 2017)

3.7 Teknologioiden valinta

Lohkoketjuteknologiaa käytettäessä on tärkeää, että sitä käytetään tarkoituksenmukaisiin kohteisiin. Usein valinta tehdään lohkoketjuteknologian ja perinteisen tietokannan välillä. (Chowdhury, Colman, Kabir & Han, 2018) Molemmilla teknologioilla on omat vahvuusalueensa ja heikot kohtansa. Lohkoketjun vahvuuksia ovat erityisesti hajautettu tietojen varastointi ja immutabiliteetti. Perinteisten tietokantojen vahvuutena on skaalautuvuus ja välittömät suoritukset. (Chowdhury ym., 2018.) Lohkoketjuteknologiaa ei ole kehitetty yleiseen datan prosessointiin ja perinteisiä tietokantoja kehitettäessä ei ole ollut intresseissä suojata datan eheyttä Bysanttilaisilta vioilta. (Dinh ym., 2018) Kun tehdään päätös lohkoketjuteknologian ja perinteisen tietokantateknologian välillä, voidaan käyttää apuna kuvion 5 mukaista päätöksentekopuuta.



KUVIO 5 Päätöksentekopuu määriteltäessä lohkoketjuteknologian soveltuvuutta. (Chowdhury ym., 2018, s. 6)

Sen lisäksi, että tehdään valinta perinteisen tietokannan ja lohkoketjun välillä, on hyvin tärkeää valita soveltuva lohkoketjuteknologia, koska sitä on vaikea vaihtaa jälkikäteen. Mikään lohkoketjualusta ei ole ideaalinen valinta kaikkiin käyttötapauksiin. (Kannengießer, Lins, Dehling & Sunyaev, 2020.) Suunniteltaessa lohkoketjusovelluksia täytyy siksi tehdä kompromisseja erilaisten ominaisuuksien suhteen. Jos esimerkiksi tarkastettavuus on tärkeää, voidaan joutua tinkimään anonymiteetistä ja jos älykkäiden sopimusten käyttö on tärkeää, voidaan tarvita suurempi kaistanleveys, enemmän aikaa transaktioiden tarkastamiseen ja lisäksi sovellusten haavoittuvuus erilaisille hyökkäyksille lisääntyy. (Kannengießer, Lins, Dehling & Sunyaev, 2019.)

4 HAJAUTETTU FINANSSIMAAILMA

Tässä luvussa tarkastellaan lohkoketjuteknologian vaikutusta talousjärjestelmään. Alaluvussa 4.1 käsitellään lohkoketjuteknologian vaikutusta rahoitusmarkkinoihin ja yleisesti transaktioihin ja vaihdantaan. Alaluvussa 4.2 tarkastellaan sijoitusmuotoisia tokeneita ja niiden tarjoamia mahdollisuuksia yritysten rahoituksessa. Alaluvussa 4.3 käsitellään kryptopörssien toiminnan edellytyksiä ja niihin liittyviä lainsäädännöllisiä ongelmia. Alaluvussa 4.3 tarkastellaan ICO-buumia lähihistorian ilmiönä. Alaluvussa 4.5 kerrotaan, mitä ovat ERC20-tokenit ja mitä niillä tehdään. Alaluvussa 4.6 käsitellään kryptovarallisuudella käytävän kaupankäynnin erityispiirteitä, mahdollisuuksia ja ongelmia. Alaluvussa 4.7 käsitellään nykyisten rahoitusmarkkinainfrastruktuurien toimintaa ja ongelmia ja millaisia ratkaisuja lohkoketjuteknologia niihin tarjoaa. Alaluvussa 4.8 kuvaillaan erilaisia skenaarioita siitä, kuinka lohkoketjuteknologia voisi tulla käyttöön rahoitusmarkkinoilla.

4.1 Lohkoketjuteknologian vaikutus transaktioihin, vaihdantaan ja rahoitusmarkkinoihin

Hajautettuun finanssimaailmaan sisältyy hajautetut versiot sekä velka- että pääomarahoituksesta. (Chanson, Martens & Wortmann, 2020) Lohkoketjuteknologia mahdollistaa monia liiketoimintamalleja, jotka eivät aiemmin olisi olleet mahdollisia korkeiden transaktiokustannusten ja kustannusintensiivisiin prosesseihin liittyvien järjestelyjen vaatiman luottamuksen takia. Esimerkiksi mikrotransaktiot ja IoT-laitteiden välillä tapahtuva automaattinen kaupankäynti onnistuvat lohkoketjuteknologian avulla. (Casey ym., 2018.) Se voi myös yksinkertaistaa liiketoimintaprosesseja pankki- ja rahoitusmarkkinoilla tuottamalla luotettavia tallenteita sopimuksista ja transaktioista. (Treleaven, Brown & Yang, 2017) Aivan kuten internet on muuttanut käytäntöjä, jotka liittyvät tiedonhakuun ja kommunikointiin,

lohkoketjuteknologia tulee suorasti ja epäsuorasti muuttamaan käytäntöjä, jotka liittyvät transaktioihin ja vaihdantaan. (Casey ym., 2018)

Hajautetun finanssimaailman keskeinen ominaisuus on sen kyky tuottaa hajautettuja protokollia, jotka ovat hyödyllisiä hajautetussa finanssimaailmassa toimiville käyttäjille. Monet hajautetun finanssimaailman protokollat mahdollistavat esimerkiksi hajautetut kryptopörssit. (Kaal, 2020) Hajautettujen tilikirjojen avulla voi nopeuttaa tiettyjen rahoituksellisten transaktioiden määritystä (clearing) ja selvittämistä (settlement) vähentämällä välikäsien määrää ja tekemällä yhteensovittamisesta tehokkaampaa. Se auttaa myös maiden rajat ylittävissä transaktioissa, missä se vähentää tarvetta käyttää välittäjiä. (ESMA, 2016.) Arvopaperikeskukset, kuten DTCC ja Euroclear ovat käynnistäneet lohkoketjuprojekteja, joiden tarkoituksena on parantaa arvopapereiden selvitystä. (Tsai ym., 2020)

Yrityksillä on monia syitä käyttää lohkoketjuteknologiaa. Sen avulla on mahdollista vähentää kompleksisuutta erityisesti monenkeskisissä ja rajat ylittävissä transaktioissa. Se mahdollistaa kehittyneen end-to-end-prosessointinopeuden sekä rahoituksen ja omaisuuden saatavuuden. (Mills ym., 2016.) Se vähentää tarvetta yhteensovittaa useita erilaisia kirjanpitoteknologioita. Se lisää läpinäkyvyyttä ja immutabiliteettia transaktioiden kirjanpidossa. Se parantaa verkon kestävyyttä hajautetun hallinnon avulla. Siihen liittyy myös vähemmän liiketoiminnallisia ja rahoituksellisia riskejä. (Mills ym., 2016.)

Arvo-osuusjärjestelmässä säilytettävien ja token muotoisten arvopapereiden transaktioiden valtuuttaminen tapahtuu eri tavalla. Arvo-osuuksiin pohjautuvissa arvopapereissa transaktioiden valtuuttaminen riippuu arvopaperikeskuksesta, joka varmentaa arvo-osuustilin omistajan identiteetin. Tokenmuotoisissa arvopapereissa transaktioiden valtuuttaminen perustuu tokenien validointiin, missä tokenin omistus osoitetaan yksityisellä tiedolla salausavaimen muodossa. Sitä voi verrata fyysisiin arvopapereihin kuten haltijavelkakirjoihin, joihin liitetyt kupongit osoittavat oikeuden korkoihin ja jotka itsessään osoittavat oikeuden pääomaan. (Bech, Hancock, Rice & Wadsworth, 2020.)

Rahoitusmarkkinoiden kannalta monet lohkoketjuteknologiaan liittyvät ominaisuudet, kuten Bitcoinin lohkoketjussa esiintyvät pseudonyymisyys, immuniteetti viranomaisvalvonnan suhteen, maailman laajuiset kaikille avoimet kopiot kirjanpidosta ja laittomien transaktioiden peruuttamattomuus, eivät ole kiinnostavia. Sen sijaan markkinoilla on kysyntää järjestelmille, jotka noudattavat vaadittuja standardeja, kuten know-your-customers (KYC) -sääntöjä, ovat läpinäkyviä ja tilivelvollisia sääntelyn suhteen, kunnioittavat lakeja kaupankäyntistrategioissa ja joiden ylläpito on edullista. (Pinna, Ruttenberg, 2016)

Rahoitusmarkkinoiden häiriöttömän toimivuuden kannalta selvitysten lopullisuus on tärkeää. Lopullisuus voidaan toteuttaa monella eri tavalla, jotka vaihtelevat sen suhteen, mikä hajautettua tilikirjaa käyttävä teknologia on kyseessä. (Pinna & Ruttenberg, 2016)

4.2 Kryptovarallisuus ja sijoitusmuotoiset tokenit

Euroopan arvopaperimarkkinaviranomaisen (ESMA) käyttämän luokituksen mukaan lohkoketjuihin tallennettavia kryptovarallisuusluokkia (englanniksi crypto asset) on kolme: kryptovaluutat eli maksuvälinemuotoiset tokenit, hyödyketokenit (englanniksi utility token) ja sijoitusmuotoiset tokenit (englanniksi tokenised tai digitized securities, security tokens, securities tokens, asset tokens, investment tokens tai crypto securities). (Advice, E. S. M. A., 2019; Howell ym., 2020; Ante & Fiedler, 2019; Baris, 2019) Tämän lisäksi on olemassa hybriditokeneita, joissa on ominaisuuksia kahdesta tai kolmesta kryptovarallisuusluokasta. (Advice, E. S. M. A., 2019; Kauppi, 2019) Tokeneihin voi myös lisätä uusia ominaisuuksia, jolloin ne voivat siirtyä kryptovarallisuusluokista toiseen. (Ante & Fiedler, 2019)

ESMAn käyttämän tokenien luokittelun lisäksi on muitakin tapoja luokitella niitä. Esimerkiksi sijoitusmuotoisten tokeneiden tilalla voi luokituksessa olla arvopaperitokenit ja pääomatokenit, jolloin arvopaperitokenit vastaavat jotain kohde-etuutta ja sen tuottokehitystä, kun taas pääomatokenit ovat arvopaperitokenien alaluokka ja sisältävät äänivaltaa ja omistusoikeutta yrityksiin. (Momtaz, Rennertseder & Schröder, 2019) Tällainen luokittelu ei kuitenkaan poikkea kovin radikaalisti ESMA:n käyttämästä.

Jokaisella kyptovarallisuuslajilla on oma käyttötarkoituksensa. Kryptovaluuttoja käytetään ainoastaan maksamiseen, eikä niihin liity mitään yhteyttä mihinkään tiettyyn projektiin. (Ante & Fiedler, 2019) Hyödyketokenit tarjoavat pääsyn johonkin palveluun tai sovellukseen, joita voivat olla esimerkiksi ohjelmistolisenssit tai pääsyliput. (Ante & Fiedler, 2019) Sijoitusmuotoisiin tokeneihin on ohjelmoitu niiden omistajien oikeudet pääomiin, kassavirtoihin, osinkoon tai korkoon ja niiden toiminnot vastaavat perinteisiä arvopapereita. (Ante & Fiedler, 2019; Cooke, Cohen & Denisenko, 2019; Kauppi, 2019) Ne antavat sijoittajille suhteellisen osuuden tulevista tuotoista, kuten osingoista tai voitoista. Niihin voi liittyä myös äänioikeuksia tai muuta päätösvaltaa. (Kranz ym., 2019)

Kryptovarallisuudella käytävässä kaupankäynnissä suurin osa kaupoista tapahtuu hyödyketokeneilla. (Momtaz ym., 2019) Vaikka myös hyödyketokeneita voidaan pitää sijoituskohteina, eroavat sijoitusmuotoiset tokenit niistä siten, että ne tarjoavat aina jonkin palvelun ulkopuolisen oikeuden. (Kauppi, 2019) Sijoitusmuotoisten tokeneiden rakenteelle ei ole olemassa yhtä yleistä standardia, vaan standardeja ja konfiguraatioita on useita erilaisia, ja ne riippuvat käyttötarkoituksesta ja lainsäädännöstä. Yhteistä niille kuitenkin on ERC-20-standardin käyttö, joka määrittää omaisuuden siirrot. (Rudolf, Kuhs, Baer & Zintl, 2018.)

Sijoitusmuotoiset tokenit tarjoavat pienille ja keskisuurille yrityksille pääsyn laajemmille rahoitusmarkkinoille (Ante & Fiedler). Pienten startup-yritysten ongelmana on usein rahoituksen puute. Tähän ongelmaan ratkaisuksi on kehitetty lohkoketjuteknologiaan perustuva ICO, jossa yritykset myyvät erilaisia

lohkoketjuihin talletettuja tokeneita ja saavat vastineeksi FIAT-valuuttaa tai kryptovaluuttaa. (Momtaz ym., 2019)

Initial Coin Offering (ICO) tarkoittaa uusien tokenien liikkeellelaskua, jossa tarkoituksena on kerätä rahaa johonkin projektiin. (Fenu, Marchesi, Marchesi & Tonelli, 2018) ICO:issa voidaan laskea liikkeelle viidenlaisia tokeneita: (1) osakemuotoisia tokeneita, jotka edustavat tavallisen yrityksen pääomaa ja joihin liittyy oikeudet äänivaltaan ja osinkoihin, (2) tokenmuotoisia pääomalainoja, jotka vastaavat muuten tavallista osaketta, mutta niihin ei liity äänivaltaa, (3) tokenmuotoisia velkakirjoja (4) tokenmuotoisia rahastoja ja (5) hyödyketokeneja. (Cooke, Cohen & Denisenko, 2019) ICO:issa liikkeelle laskettuihin tokeneihin on ohjelmoitu paljon ominaisuuksia lisäämään niiden myyntikelpoisuutta ja mahdollista arvostusta. Niihin on tyypillisesti ohjelmoitu rajoituksia liittyen tokenien tarjontaan tulevaisuudessa ja ne ovat keskenään samanlaisia, minkä ansiosta ne ovat korvattavissa vastaavilla tokeneilla. (Casey ym., 2018.; Kranz ym., 2019)

ICO:ihin liittyy juridisia ongelmia, koska tyypillisesti niissä myytävät tokenit eivät vastaa perinteisiä osakkeita. Tähän ongelmaan on kehitetty Security token offering (STO), jossa myytävät tokenit ovat perinteisiä arvopapereita tokenmuodossa. (Ante & Fiedler, 2019) Security token offering (STO) on listautumisantiin ja joukkorahoitukseen rinnastettava tapa kerätä riskipääomaa. (Ante & Fiedler, 2019) STO:ssa yritykset myyvät osakemuotoisia tokeneita, mikä vastaa juridisesti perinteisten arvopapreiden myymistä. Mikä tahansa yritys voi periaatteessa myydä niitä, mikäli ne vastaavat voimassa olevaa lainsäädäntöä. (Ante & Fiedler, 2019.) STO on älykkääseen sopimukseen pohjautuva ICO, jossa älykäs sopimus varmistaa kaikkien sopimuksen piirissä olevien arvopapereiden sopimusprosessien toiminnan. Sitä voidaan myös päivittää erilaisten liiketapahtumien perusteella. (McCullagh & Flood, 2019; Koverko & Houser, 2017.) ICO:t mielletään yleensä hyödyketokenien liikkeellelaskuun liittyviksi, kun taas STO:t kuvastavat kypsempää ja säännellympää tokenien liikkeellelaskua, joissa kyse on sijoitusmuotoisista tokeneista. (Kranz ym., 2019)

Sijoitusmuotoisten tokeneiden liikkeelle laskeminen tapahtuu siten, että liikkeellelaskija syöttää arvopapereiden myyntiä koskevat tiedot, kuten osoitteen, aloitusajan ja lopetusajan älykkääseen sopimukseen ja suorittaa sen. Liikkeellelaskijalla on oikeus tarkistaa sopimus. Kun sopimus vastaa liikkeellelaskijan odotuksia, hän voi siirtää sopimukseen arvopapereita, jotka ovat tämän jälkeen myytävänä aloitusajan jälkeen. (Koverko & Houser, 2017.)

Sijoitusmuotoisia tokeneita myydään usein samoilla kauppapaikoilla kuin kryptovaluuttoja, ja kryptovaluuttoja myyvät kauppapaikat pyrkivät saamaan myös sijoitusmuotoisilla tokeneilla käytävään kaupankäyntiin tarvittavat toimiluvat ja tekevät yhteistyötä arvopaperipörssien kanssa. Säänneltyjä markkinapaikkoja sijoitusmuotoisille tokeneille ei kuitenkaan ole juurikaan vielä olemassa. Jotkin startup-yritykset tarjoavat niiden kaupankäyntiin uusia ratkaisuja (esim. tZERO ja Templum), jotka mahdollistavat jälkimarkkinat. (Klayman, 2019; Ante & Fiedler, 2019.) Perinteiset arvopaperimarkkinoiden toimijat ovat sen sijaan keskittyneet tarjoamaan lohkoketjuteknologiaan perustuvia selvitys- ja maksupalveluita. (Ante & Fiedler, 2019.)

4.2.1 Sijoitusmuotoisten tokenien edut

Sijoitusmuotoisten tokeneiden liikkeellelasku ei periaatteessa eroa perinteisten arvopapereiden liikkeellelaskusta muuten kuin siinä, että liikkeellelaskussa hyödynnetään lohkoketjuteknologiaa. Lohkoketjuteknologian merkittävinä etuina verrattuna perinteisiin menetelmiin nähdään muun muassa läpinäkyvyys, pseudonyymisyys, lopullisuus ja turvallisuus. (Ante & Fiedler, 2019.) Lohkoketjussa kaikki transaktiot ovat näkyvissä, minkä ansiosta tokeneiden omistajuus on selkeää ja kaiken aikaa tiedossa. (Ante & Fiedler, 2019) Lohkoketjuteknologia on myös yksi teknologioista, joka mahdollistaa reaaliaikaisen transaktioiden selvityksen. (Embrasing Disruption, 2016)

Merkittävin sijoitusmuotoisiin tokeneihin liittyvä etu verrattuna perinteisiin arvopapereihin on lohkoketjuteknologian mahdollistama likviditeetti. Sen toteutuminen kuitenkin edellyttää laadukkaita arvopapereita, eli esimerkiksi hyvin tuottavia osakkeita, samoin kuin riittävän kehittyneet markkinat, joilla niillä voi käydä kauppaa. Myös infrastruktuurin pitää olla valmis, ennen kuin toimivat markkinat saadaan toteutettua. (Ante & Fiedler, 2019.)

Perinteisiin arvopapereihin verrattuna sijoitusmuotoisten tokeneiden etuna on (1) niiden siirrettävyys, mikä tarkoittaa mahdollisuutta myydä niitä milloin tahansa jälkimarkkinoilla riippumatta kellonajasta tai viikonpäivästä, (2) nopeat vain minuutteja kestävät selvitykset ja liikkeellelaskut, (3) mahdollisuus säilyttää osakkeita itse ilman kolmansien osapuolten tarjoamia välitys ja säilytyspalveluita ja (4) lohkoketjujen turvaama kaikkia transaktioita koskeva läpinäkyvyys. (Ante & Fiedler, 2019)

Lohkoketjuteknologialla on lukuisia ominaisuuksia, joista on hyötyä pankki- ja rahoituspalveluissa, kuten kestävyys ja hajautetut verkostot, jotka eivät tarvitse keskuspalvelinta, eikä niissä ole yksittäistä pistettä (single point of failure), jonka toimintahäiriö estäisi palvelun toiminnan. Hajautetut avoimeen lähdekoodiin pohjautuvat protokollat mahdollistavat eheyden ja luottamuksettomuuden, minkä vuoksi ei tarvita kolmansia osapuolia. (Treleaven ym., 2017.) Taulukossa 2 on tarkasteltu lohkoketjutokenien mahdollisia vaikutuksia yritysrahoitukseen, sijoittamiseen ja innovointiin. (Chen, 2018)

TAULUKKO 2 Lohkoketjutokenien vaikutus yrittäjyyteen, sijoittamiseen ja innovointiin. (Chen, 2018, s. 569)

	Ilman tokeneita	Tokeneiden kanssa
Varainkeruu	• Yrittäjät voivat saada rahoitusta enkelisijoittajilta ja pääomasijoittajilta. • Yrittäjät voivat saada rahoitusta joukkorahoituskampanjoilla.	• Yrittäjät voivat saada käyttöpääomaa suoraan sijoittajilta myymällä uusia tokeneita (ICO tai STO).
Investoinnit	• Keskivertosijoittajilla on vähän mahdollisuuksia sijoittaa siemenvaiheen yrityksiin. • Sijoitukset yksityisiin yrityksiin eivät ole likvidejä.	• Keskivertosijoittajien mahdollisuudet sijoittaa siemenvaiheen yrityksiin ovat lähes vastaavat kuin pääoma- ja enkelisijoittajilla. • Sijoitusmuotoiset tokenit ovat likvidejä.
Yhteisön rakentaminen	• Alustat alkavat saavuttaa käyttäjien suosiota, kun verkostovaikutus on vahva. • Alustat alkavat houkutella kehittäjiä, kun verkostovaikutus on vahva.	• Alustat voivat palkita varhaisia käyttäjiä tokeneilla ja kompensoida näin puutteellista verkostovaikutusta. • Alustat voivat palkita varhaisen vaiheen kehittäjiä tokeneilla ja kompensoida näin puutteellista verkostovaikutusta.
Avoin lähdekoodi	• Avoimen lähdekoodin projektit voivat rahoittaa toimintaansa lahjoituksilla. • Avoimen lähdekoodin projektit eivät yleensä jaa menestystä kehittäjiensä kanssa.	• Avoimen lähdekoodin projektit voivat rahoittaa toimintansa jatkamista myymällä tokeneita. • Avoimen lähdekoodin projektit voivat jakaa menestymistään kehittäjien kanssa jakamalla heille tokeneita.

4.2.2 Sijoitusmuotoisten tokenien ongelmat sääntelyn, markkinoiden ja teknologian kehityksen suhteen

Sijoitusmuotoisiin tokeneihin liittyy monia ongelmia liittyen lainsäädännön, markkinoiden ja teknologian kehitykseen. Perinteinen arvopapereiden sääntely ei ole täysin käyttökelpoista sijoitusmuotoisten tokeneiden suhteen, mikä voi avata uusia mahdollisuuksia mutta myös aiheuttaa ongelmia pääomasijoittajille. (Goforth, 2019, 21) Sijoitusmuotoiset tokenit ovat varsin uutta teknologiaa, minkä vuoksi niihin liittyvät kriittiset ongelmat eivät ole vielä selvillä. Tämän vuoksi sijoittajat saattavat olla liian varomattomia analysoidessaan projekteja. Sijoitusmuotoiset tokenit ovat säänneltyjä rahoitusinstrumentteja, joten sääntelystä vastaavien tahojen tulisi seurata niiden kehitystä ja pitää sääntely ajan tasalla, jotta niihin tehdyt investoinnit ovat turvallisia. (Ante & Fiedler, 2019.)

Sijoitusmuotoisiin tokeneihin liittyvät tekniset protokollat, jälkimarkkinat ja lainsäädäntö kehittyvät koko ajan, mutta kehitys on vielä hyvin varhaisella

asteella, joten jälkimarkkinoiden tuottojen ja hintojen arviointiin ei ole tarjolla erityisemmin tutkittua tietoa. (Ante & Fiedler, 2019.) Myös sijoitusmuotoisten tokeneiden markkinat ovat vielä niin kehittymättömät, ettei niihin liittyviä kriittisiä ongelmia ole vielä tunnistettu. (Ante & Fiedler, 2019)

Osakeyhtiöiltä tyypillisesti vaaditaan osakasluettelon ylläpitämistä ja niiden tulee pyydettäessä pitää tämä kaikkien osakkaiden saatavilla. Sijoitusmuotoiset tokenit saattavat tarvita sopimusjärjestelyjä, jotka ottavat tämän huomioon. (Goforth, 2019, 49)

Koska tokenit voivat edustaa mitä tahansa omaisuutta, voi myös sijoitusmuotoisiin tokeneihin lisätä ominaisuuksia, joiden ansiosta niitä voisi käyttää esimerkiksi hyödyketokenien tapaan tai maksuvälineenä kryptovaluuttojen tapaan. (Ante & Fiedler, 2019.) Sääntelyn näkökulmasta tällainen muunneltavuus on kuitenkin haasteellista, koska aiemmin lain mukainen token ei enää välttämättä noudatakaan samaa lainsäädäntöä. (Klayman, 2019, s. 77).

Sijoitusmuotoisilla tokeneilla käytävän kaupan oikeusvarmuus vaihtelee maittain ja USA on tässä suhteessa johtava maa. Veroparatiiseissa oikeuskäytännöt (legal framework) ovat olemassa, mutta niissä rahoituksen saanti on ongelmallista. (Ante & Fiedler, 2019)

Koska sijoitusmuotoisilla tokeneilla käytävään kaupankäyntiin liittyy paljon enemmän sääntelyä kuin muilla kryptovarallisuuslajeilla käytävään kauppaan, moni kryptopörssi ei käy niillä kauppaa lainkaan. Sijoitusmuotoisiin tokeneihin on myös ohjelmoitu erityisiä ehtoja sille, ketkä voivat käydä niillä kauppaa. (Koverko & Housser, 2017.)

4.3 ICO-buumi

ICO:t olivat erittäin suosittu tapa yritysten käyttöpääoman hankkimisessa vuosina 2017 ja 2018, mutta buumin jälkeen niiden suosio on romahtanut rajusti. (Gächter & Gächter, 2021) Suosion hiipumisen taustalla saattaa olla sääntelyyn liittyvä epävarmuus, koska ICO:iden kanssa operoivilla ihmisillä on usein puutteellinen tietämys sovellettavasta lainsäädännöstä ja tämän lisäksi ICO-buumin aikana esiintyi paljon huijauksia, minkä seurauksena tuli uutta sääntelyä ja joissakin maissa ICO:t on kielletty lailla. (Massey, Dalal & Dakshinamoorthy, 2017; Klayman, 2019; Chen 2018) ICO:ista ja niissä käytettävien tokeneiden myynnistä tuli väliaikaisesti tehokas tapa kerätä käyttöpääomaa, joka sivuutti perinteisiä toimijoita kuten rahoitusyhtiöitä, institutionaalisia sijoittajia ja säänneltyjä rahoitusmarkkinoita. Niiden näennäinen helppokäyttöisyys on kuitenkin johtanut siihen, että moni hyvääkin tarkoittava toimija on tullut rikkoneeksi arvopaperimarkkinoita koskevaa sääntelyä. (Cooke, Cohen & Denisenko, 2019; Massey ym., 2017)

ICO:iden määrän räjähdysmäinen kasvu perustui osittain kryptopörssien kehitykseen, jotka mahdollistavat kaupankäynnin tokeneilla ja niiden vaihtamisen fiat-valuuttoihin. (Casey ym, 2018) Monilla ICO:issa liikkeelle lasketuilla tokeneilla käydään kauppaa sekä kryptopörsseissä että niiden ulkopuolella. (Casey

ym., 2018) Noin puolet toteutetuista ICO:sta on listattu kryptopörsseihin. Listaaminen parantaa tokenien likviditeettiä, myyntikelpoisuutta ja siirrettävyyttä ja indikoi liikkeellelaskijan hyvää mainetta ja taloudellista aktiivisuutta. (Howell ym., 2020; Kranz ym., 2019)

4.4 Rahoitusmarkkinainfrastruktuurit (FMI:t) ja hajautetut rahoitusmarkkinaninfrastruktuurit (dFMI:t)

Arvopapereiden, hyödykkeiden ja johdannaisten jälkimarkkinaprosessit edellyttävät kauppaehtojen varmistamista sekä kauppojen toimitusta ja selvitystä. Näitä tehtäviä hoitavat usein erilaiset välittäjät, kuten arvopapereiden toimitusjärjestelmät (SSS:t), arvopaperikeskukset (CSD:t) ja keskusvastapuolet, jotka ovat erikoistuneet tiettyihin maksu-, toimitus- ja selvitystoimintoihin. (Mils ym., 2016)

Nykyiset rahoitusmarkkinoiden infrastruktuurit (FMI:t) nojaavat vahvasti välittäjiin, koska niitä kehitettäessä teknologia ei ole mahdollistanut talletetun tiedon jakamista ilman luotettavaa keskustahoa, eli organisaatiot eivät ole voineet jakaa talletettuja tietoja käyttämättä hyväkseen yksittäistä keskustahoa, joka hallinnoi tallenteita. Tämä on johtanut informaatiosiiloihin ja samalla sääntelyyn ja liiketoimintamalleihin, jotka edistävät välittäjien käyttöä. (Feenan ym., 2020.) Tämän takia rahoitusmarkkinoilla on järjestelmällisesti tärkeitä rahoituslaitoksia (SIFI) ja järjestelmällisesti tärkeitä rahoitusmarkkinainfrastruktuureja, joiden toimintaa ohjaavat kannustimet ovat vinoutuneita. Rahoitusmarkkinoiden infrastruktuureihin liittyy myös systeemistä riskiä, koska ne ovat niin vahvasti keskittyneet. (Feenan ym., 2020.)

Nykyiset infrastruktuurit ja keskeisten instituutioiden liiketoimintamallit erityisesti arvopapereiden selvityksissä nojaavat kohtuuttoman paljon välittäjiin erityisesti selvitystoiminnoissa, kuten arvopaperikeskuksissa ja keskusvastapuolissa, jotka on suunniteltu keskustietokoneiden ympärille. Keskeinen syy välittäjien käytölle on se, että nykyiset liiketoimintamallit ja markkinarakenteet sisältävät ratkaisuja, jotka on suunniteltu 70-luvulla käytettyjä tietojen tallennus- ja laskentamalleja varten. (Feenan ym., 2020.)

Viimeisen kymmenen vuoden aikana teknologinen edistyminen, kuten julkiseen avaimeen pohjautuva salaus, hajautusalgoritmit, virtualisointi, hajautettu konsensus, monen osapuolen laskenta ja vertaisverkot ovat johtaneet tilanteisiin, joissa entiset kilpailijat ovat kokeilleet tallenteiden jakamista. (Feenan ym., 2020) Viime vuosina sääntelyä on viety suuntaan, joka mahdollistaa eri toimijoiden toteuttaa yhteisiä infrastruktuureja aiempien keskitettyjen sijasta, mikä saattaa mahdollistaa hajautettujen rahoitusmarkkinainfrastruktuurien tulon markkinoille korvaamaan entisiä keskitettyjä infrastruktuureja. (Feenan ym., 2020)

Hajautetut rahoitusmarkkinainfrastruktuurit ovat konsortioita, joissa jäsenet käyttävät lohkoketjussa globaalisti päivittyvää tilikirjaa ylläpitäviä hajautetun verkon solmuja. Tilikirjassa hallinnoituja varoja voidaan hallita älykkäällä sopimuksella, jota voidaan muokata moniallekirjoituksella, jolla varmistetaan

määräenemmistön määräysvalta resursseista. Hajautetut rahoitusmarkkinainfrastruktuurit perustuvat keskinäisyyteen, jolloin markkinaosapuolet yhdistävät resurssinsa suojaten näin itsensä tilanteelta, jossa yksi osapuoli menee konkurssiin. Tämän ansiosta millään markkinaosapuolella ei ole keskeistä roolia ja systeemiriski poistuu. Tällöin ei siis tarvita valtioita pääomittamaan rahoituslaitoksia, jotka ovat liian suuria kaatumaan. (Feenan ym., 2019.) Rahoitusjärjestelmän toiminta perustuu vielä suurelta osin vanhoihin järjestelmiin, joiden korvaaminen hajautetuilla rahoitusmarkkinainfrastruktuureilla toisi rahoitusjärjestelmään dynaamisuutta ja turvallisuutta. (Feenan ym., 2020)

Hajautetut liiketoimintamallit vähentävät riskiä monella tavalla verrattuna keskitettyihin selvityksiin ja keskeisiin välittäjiin:

1. Talousnäkökulma: keskusvastapuolten vinoutuneet kannustimet korvataan hajautetun järjestelmän jäsenten kannustimilla, jotka ovat linjassa liiketoimintaroolin kanssa.
2. Rahoitusnäkökulma: toiminnallinen ja luottoriski eivät enää ole keskitettynä yhdelle keskustaholle, vaan se on hajautettu jäsenille.
3. Teknologinen näkökulma: Yksi epäonnistumispiste (single point of failure) on korvattu hajautetulla verkostolla. Toimintavarmuus perustuu redundanssiin, eli tiedonsiirtoa ja prosesseja ei tarvita jäsenten välillä. (Feenan ym, 2020.)

Hajautetut rahoitusmarkkinainfrastruktuurit toimivat digitaalista valuuttaa käyttävällä selvitysalustalla, joiden selvitys toteutuu konsensusalgoritmin suorituksen jälkeen. Tämän ansiosta selvitys voidaan toteuttaa tunneissa, kun se perinteisesti toteutettuna kestää päiviä. Kaupanteon ja selvityksen välisen viiveen dramaattinen pienentyminen yhdistettynä luovutus maksua vastaan -järjestelyihin voi pienentää merkittävästi kaupanteon riskejä. (Feenan ym., 2020.) Myös luovutus maksua vastaan voidaan toteuttaa välittäjien sijaan älykkäällä sopimuksella tai jollain muulla gryptografisella teknologialla, joka siirtää maksun myyjälle vasta luovutuksen tapahtuessa. (Feenan ym., 2020)

Hajautettua tilikirjaa käyttävät teknologiat voivat vaikuttaa monella tavalla arvopapereiden jälkimarkkinaprosesseihin. Benosin, Garrattin ja Gurrola-Perezin (2017) mukaan niillä on paljon myönteisiä vaikutuksia. Niiden avulla voidaan pienentää datan yhteensovittamis- ja hallinnointikustannuksia, koska hajautettu ja synkronoitu omistajuustietojen hallinta, joka on relevanttien osapuolten käytössä, voi yksinkertaistaa ja automatisoida monia prosesseja nykyisestä jälkimarkkinaprosessista vähentämällä tarvetta yhteensovittaa järjestelmiä, tarjoamalla yhteisen standardin ja poistamalla tarpeen pitää yllä varajärjestelmää. Hajautettu tilikirja voisi vähentää transaktioihin kuluvaa aikaa jälkimarkkinaprosesseissa, poistaa tarpeen käyttää erillistä selvitysosapuolta, poistaa tarpeen säilytyspalveluille, lisää jäljitettävyyttä ja parantaa turvallisuutta ja kestävyyttä. (Benos ym., 2017.)

Benos ym. (2017) mainitsevat myös useita mahdollisia ongelmia. Arvopaperikeskuksia tai muita luotettavia kolmansia osapuolia tarvittaisiin mahdollisesti edelleen varmistamaan, että arvopaperit ovat kelvollisia. Siirtyminen

hajautetun tilikirjan käyttöön edellyttää perinteisillä tavoilla säilytettyjen omistusten integrointia hajautettuun tilikirjaan, mihin voi liittyä teknisiä ja juridisia haasteita. Joissakin tilanteissa transaktioiden näkyminen ulkopuolisille voi muodostua ongelmalliseksi, mikä heikentää luottamuksellisuutta. (Benos ym., 2017.) Arvopapereiden selvitykset vaativat kapasiteettia käsitellä suuria määriä transaktioita, mikä on skaalautuvuuden kannalta ongelmallista. Omistajuuden siirtyessä sen tulisi olla virallista ja lakiin pohjautuvaa. Hajautetuissa tilikirjoissa identiteetin ja pääsyn hallintaa tulisi pystyä kontrolloimaan tehokkaasti. Hajautetun tilikirjan tulisi mahdollistaa luovutus maksua vastaan eli kyetä välittömään vuorovaikutukseen käteistilien kanssa ja tarjota riittävät toiminnot kauppojen täsmäytykseen. (Benos ym., 2017.) Konsensusmekanismi ei välttämättä pysty takaamaan riittävää varmuutta kaupanteon lopullisuudesta. (Benos ym., 2017)

4.5 ERC20-tokenit

Ethereum-lohkoketjuun talletetut älykkäät sopimukset ovat jo niin yleisiä, että niitä varten tarvitaan erityisiä standardeja, joiden avulla parannetaan käytettävyyttä. Näitä ovat kasvava määrä kehitys ehdotuksia, Ethereum Improvement proposal eli EIP, joiden yksi osajoukko ovat Ethereum Request for Comments eli lyhennettynä ERC. Tunnetuin ERC on ERC20, jonka tarjoamat standardoidut funktiot pitää toteuttaa kaikissa Ethereum-tokeneissa. (Norvill, Fiz, State & Cullen, 2019.)

ERC20-tokenit on kehitetty edustamaan laajaa kirjoa erilaisia kryptovarallisuuslajeja, minkä takia ne ovat tärkeässä asemassa Ethereumin ekosysteemissä. Näiden tokenien arvo riippuu niiden kohde-etuuden arvosta. (Chen, 2018) ERC20-teknologia on helpottanut ICO:iden kehittämistä ja samalla ollut merkittävä tekijä niiden yleistymisessä. (Zhang & Balogun, 2018) ERC20-sopimukset dominoivat älykkäiden sopimusten markkinoilla ja niillä on toteutettu paljon ICO:ita. Yli puolet älykkäistä sopimuksista perustuu ERC20-standardiin. (Howell ym., 2020; Hildenbrandt ym. 2018.) Yksi tunnetuimmista ERC20-tokeneista on Filecoin, joka käynnisti ICO:n vuonna 2017 elokuussa ja keräsi 250 miljoonaa dollaria noin puolessa tunnissa. (Hacker & Thomale, 2018) ERC20-standardi on yksi tärkeimmistä standardeista Ethreum-lohkoketjuun talletetuissa älykkäissä sopimuksissa. Se tarjoaa perustoiminnot, joiden avulla tokeneita voi siirtää ja siirrot hyväksyä ja määrittelee tokeneiden liikkeellelaskua, jakelua ja hallintaa. (Hildenbrandt ym. 2018.; Howell ym., 2020) ERC20-standardin noudattaminen on tärkeää, jos älykkään sopimuksen on tarkoitus toimia yhteen ulkoisten järjestelmien, kuten lompakkojen ja kauppapaikkojen kanssa. (Hildenbrandt ym. 2018)

ERC20 tokenstandardi kuvailee funktiot ja tapahtumat, jotka helpottavat kryptovarallisuudella käytävää kauppaa. (Patsonakis & Roussopoulos, 2019) ERC20-tokeneiden perustoiminnot määrittää sopimustyyppi *Basic* tai *BasicToken* (näissä on yksi toiminnallinen ero), joka mahdollistaa tokenien siirtelyn omistajien välillä. Tokeneille voi määrittää hyvin paljon muitakin erilaisia toimintoja mutta niitä ei ole välttämättä standardoitu. (Reibel. Yousaf & Meiklejohn, 2019.)

ERC20 määrittelee 6 metodia ja 2 tapahtumaa, joita tulee käyttää. (Rahimian ym., 2019) Jokaisen tokenin omistajan tili viittaa Ethereumin *address*-tietotyyppiin ja jokaisen tilin saldo on ilmaistu *uint*-tietotyypillä (unsigned integer). Jokainen ERC20-käyttöliittymä koostuu seuraavista kuudesta funktiosta:

1) *totalSupply()*, joka kertoo tokenien kokonaismäärän kaikilla tileillä.
2) *balanceOf(address owner)*, joka kertoo tilin omistajan tokensaldon.
3) *approve(address spender, uint tokens)*, jolla asetetaan transaktio, missä maksava osapuoli valtuuttaa tilinsä siirtämään tietyn määrän tokeneita.
4) *allowance(address owner, address spender)*, joka lähettää tokenien määrän, jonka maksajan omistamalta tililtä on hyväksytty maksettavaksi.
5) *transfer(address to, uint tokens)*, joka siirtää määrätyn määrän tokeneita *to*-tilille, jos jokin tili toteuttaa funktion.
6) *transferFrom(address from, address to, uint tokens)*, joka siirtää määrätyn määrän tokeneita *from*-tililtä *to*-tilille. (Patsonakis & Roussopoulos, 2019.; Hildenbrandt ym. 2018)

Vaikka lukuisia uusia tokenstandardeja on kehitetty, on ERC20 kuitenkin säilyttänyt merkittävän aseman. Erilaisia ERC20-tokeneita on satoja tuhansia ja monet kehitystyökalut, kaupankäyntisovellukset, kirjastot ja internetsovellukset on tehty näiden tokenien kaupankäyntiä varten. (Rahimian ym., 2019.)

4.6 Kaupankäynti kryptovarallisuudella

Lohkoketjuteknologian synnyttämä kryptoekosysteemi tarjoaa uusia innovatiivisia tapoja riskipääoman keräämiseen ja jälkimarkkinoihin kryptopörsseissä. (Casey ym., 2018) Lohkoketjuteknologia mahdollistaa myös tulevaisuudessa miljardien IoT-laitteiden keskinäiset mikrotransaktiot ja kaupankäynnin kryptovarallisuudella. Tämä edellyttää sulavia hajautettuja järjestelmiä, jotka ottavat huomioon epäluottamuksen ja mahdollistavat laitteiden väliset kauppapaikat. (Casey ym., 2018.) Lohkoketjuteknologia mahdollistaa käyttäjien keskinäisen toiminnan luotettavasti, koska transaktiot ovat pysyviä, eikä niitä voi jälkikäteen peukaloida ja lohkoketjuteknologia pystyy varmistamaan, että kaikilla osapuolilla on samanlainen tallenne transaktioista. (Treleaven ym., 2017)

Kun käytetään älykkäisiin sopimuksiin perustuvia järjestelmiä, joissa talletteita hallinnoidaan julkisesti saatavilla olevalla ohjelmointikoodilla, kuka tahansa ohjelmointitaitoinen henkilö voi luoda järjestelmän, jossa käsitellään valtavaa määrää omaisuutta. (Metcalfe, 2020) Älykkäiden sopimusten ymmärtäminen ei kuitenkaan ole helppoa ja triviaalia, vaikka niiden kehittäjät painottavat läpinäkyvyyttä ja liiketoimintasääntöjä. (Oliva, Hassan & Jiang, 2020)

Yksi tokeneilla käytävää kauppaa rajoittava seikka on se, ettei niillä voi välttämättä käydä kauppaa suoraan omistajien välillä, vaan siihen tarvitaan välittäjiä. Ongelma ilmenee sekä lohkoketjujen sisällä että niiden välillä. Atominen vaihdanta sen sijaan tapahtuu suoraan ilman välittäjiä ja siinä käytetään älykkäitä sopimuksia. (Miraz & Donald, 2019) Yleensä atominen vaihdanta ei ole mahdollista vaihdannan toteuttamisessa lohkoketjujen välillä, koska lohkoketjut eivät

toimi yhteen keskenään, vaan sen sijaan lohkoketjujen välillä tapahtuvaan vaihdantaan tarvitaan vanhanaikaista kryptopörssiä ja toisinaan niitäkin useampia kuin yksi, koska listattujen tokeneiden määrä pörsseissä on rajallinen eikä haluttua tokenia ole välttämättä listattuna samassa pörssissä kuin vaihtoon tarkoitettu tokeni. Lisäksi tarvitaan useita erilaisia tokeneita välittäjiksi, koska kaiken tyyppiset tokenit eivät ole keskenään vaihdettavissa. Useista vaihdoista seuraa transaktiokustannuksia, heikkoa likviditeettiä, haavoittuvuuksia ja sääntelyyn liittyviä ongelmia. (Miraz & Donald, 2019)

4.6.1 Hajautetut kauppapaikat

Hajautetut kauppapaikat ovat peer-to-peer-kaupankäyntijärjestelmiä, joissa jokainen tehty kauppa tapahtuu siirtämällä varat suoraan ostajan ja myyjän lompakkojen välillä. (Heilman, Lipmann & Goldberg, 2020.) Ne harjoittavat kauppaa ilman keskitettyä alustaa ja/tai keskitettyä toimeksiantojen sovittamisjärjestelmää. Ne eivät säilytä asiakkaidensa varoja mutta tarjoavat avoimeen lähdekoodiin pohjautuvia algoritmeja peer-to-peer-kaupankäyntiin. (Casey ym., 2018) Hajautetut kaupankäyntialustat eivät yleensä sovellu fiatrahan vaihtamiseen kryptovarallisuuteen, minkä vuoksi keskitetyt kaupankäyntialustat toimivat ensimmäisenä askeleena kryptovarallisuudella käytävässä kaupassa, vaikka alkuperäinen tarkoitus olisi ollut käyttää hajautettuja kaupankäyntialustoja. (Advice, E. S. M. A., 2019) Hajautetuissa kaupankäyntialustoissa kaupankäynnin likviditeetti voi jäädä heikoksi, koska kaupankäynti onnistuu vain silloin, kun sen osapuolet käyttävät samaa kaupankäyntialustaa ja niillä ei välttämättä ole kovin laajaa käyttäjäkuntaa. (Heilman ym., 2020) Toisaalta niiden pienet transaktiomaksut voivat houkutella asiakkaita, jolloin likviditeetti voi olla jopa parempi kuin keskitetyissä kaupankäyntialustoissa. (Wang, Tsai, He, Lie & Deng, 2018)

Hajautettu kryptopörssi (decenralized exchange) on terminologisesti hankala käsite, koska sitä käytetään sekä lohkoketjuun perustuvista vaihtoprotokollista että protokollia hyödyntävistä sovelluksista. Hajautettu vaihtoprotokolla kuvaa yleensä ohjelmistoa, jonka tietokantaa isännöidään yhdessä tai useammassa lohkoketjussa tai joka on integroitu yhteen tai useampaan lohkoketjuun (esim. Ethereumiin). Lohkoketju mahdollistaa vertaisoperaatiot, jotka suoritetaan automaattisesti. Käyttäjät pitävät yksityiset avaimet koko transaktioprosessin ajan. (Lin, 2019)

Hajautettuihin kauppapaikkoihin liittyy 3 ongelmaa, jotka heikentävät niiden käytettävyyttä: (1) pitkät suoritusajat, (2) alttius edelläkävijähyökkäyksille ja (3) lohkoketjun resurssien tuhlaaminen. (Hsieh ym., 2018) Koska hajautetuissa kauppapaikoissa suoritukset tapahtuvat lohkoketjussa, kaupankäynnin nopeus riippuu siitä, miten nopeasti lohkoketjujen uudet lohkot vahvistetaan, minkä vuoksi ne eivät sovellu reaaliaikaiseen kaupankäyntiin. Esimerkiksi EtherDelta, 0x ja TierNolan ovat kaupankäyntiprotokollia, jossa suoritukset tapahtuvat lohkoketjussa. (Heilman ym., 2020.)

Edelläkävijähyökkäyksissä joku tekee transaktion ennen muita odottavia transaktioita, mikä aiheuttaa odottavien transaktioiden epäonnistumisia ja niiden varojen menetyksiä. Edelläkävijähyökkäykset vaikeuttavat hajautettujen sovellusten suorittamaa transaktioiden prosessoinnin varmentamista, heikentäen käyttökokemusta ja älykkäiden sopimusten suorituksen tehokkuutta. (Hsieh ym., 2018.)

Hajautetuissa kryptopörsseissä jokainen yhteensovitettu transaktio sisältää vain yhden vastaanottajan ja yhden toimeksiannon tekijän. Jos merkittävä pörssikauppias haluaa suorittaa useita tehtyjä toimeksiantoja kerralla, hänen on lähetettävä sovitetut transaktiot kustakin toimeksiannosta ja hänen täytyy odottaa jokaisesta erillistä vahvistusta. Tämä tuhlaa laskenta- ja talletuskapasiteettia erityisesti päällekkäisten tehtyjen toimeksiantojen tapauksessa. Resurssiongelman lisäksi saman lähettäjän transaktiot täytyy suorittaa peräkkäin, mikä tarkoittaa, että vahvistuksen odotusaika pitenee. (Hsieh ym., 2018.)

Uusia hajautettuja kauppapaikkoja tulee markkinoille jatkuvasti. (Casey ym., 2018) Täysin hajautetun kryptopörssin toteuttaminen on kuitenkin teknisesti hyvin vaikeaa, minkä vuoksi useimmissa hajautetuissa kauppapaikoissa on keskitettyjä toimintoja eli ne ovat osittain hajautettuja. (Hsieh ym., 2018)

Yksi tapa toteuttaa kryptopörssi on dark pool, jossa kryptopörssillä on sisäinen tietokanta transaktioista, jotka ajoittain synkronoidaan lohkoketjuun yhteenvetona. (Swan, 2015) Rahoituksessa dark pool tarkoittaa yksityistä kauppapaikkaa rahoitusinstrumenteille, joiden kaupankäynti ei ole julkista. Dark pool ehkäisee edelläkävijähyökkäyksiä, koska kaupanteko ei ole ulkopuolisten tiedossa ja se sopii siksi tilanteisiin, joissa myydään suuria omaisuuseriä. (França, 2019.)

4.6.2 Kryptopörsseihin liittyvät lainsäädännölliset ongelmat

Koska kryptovarallisuudella ei juurikaan käydä kauppaa tavanomaisissa pörsseissä, liittyy niillä käytävään kauppaan ongelmia kauppapaikkoja koskevan sääntelyn kannalta. (Perlman, 2019) Kryptopörsseihin on liittynyt merkittäviä ongelmia niiden alusta asti, jotka liittyvät niitä koskevaan poliittiseen päätöksentekoon, laittomuuksiin ja taloudelliseen vakauteen. (Casey ym., 2018) Monet kryptopörssit ovatkin epäonnistuneet ja lopettaneet toimintansa. (Casey ym., 2018)

Sääntelijät haluavat varmistaa, että kryptopörssit eivät aiheuta taloudellista epävakautta tai laitonta toimintaa, kuten rahanpesua tai terrorismin rahoittamista. (Casey ym., 2018) Niin kauan kuin kryptopörssit ovat sääntelyn ulkopuolella ja niiden toiminnan läpinäkyvyys on puutteellista, keskuspankeilla ja muilla vastuullisilla tahoilla ei ole mahdollisuutta saada niiden toiminnasta selvää kuvaa. (Casey ym., 2018)

Jotkin kryptopörssit, joihin lukeutuu esimerkiksi Gemini, ovat muodostaneet itsesääntelyorganisaation, joka jäljittelee perinteisten kauppapaikkojen vastaavia organisaatioita. Ne eivät kuitenkaan kata kaikkia sääntelyn tehtäviä, jotka liittyvät rekisteröintiin ja valvontaan. (Casey ym., 2018.)

Hajautettujen kauppapaikkojen rekisteröinti ja sääntely voi osoittautua vaikeaksi. (Casey ym., 2018) Jos kauppapaikka on avoimeen lähdekoodiin pohjautuva kaupankäyntiprotokolla, voi olla hankala määritellä mihin se tulisi rekisteröidä ja kenen vastuulla se olisi. (Casey ym., 2018)

Poliitikkojen tulisi mahdollistaa innovaatiot, jotka tekevät vakiintunet liiketoimintamallit vanhentuneiksi. (Casey ym., 2018) Koska nykyinen lainsäädäntö on säädetty enimmäkseen ennen lohkoketjuteknologiaa, sitä pitäisi muuttaa sellaiseksi, että se huomioi uuden teknologian tuomat olosuhteet. (Casey ym., 2018) Lainsäädännöllisesti tavoitteiden pitäisi olla yhdensuuntaiset riippumatta siitä, koskevatko ne perinteistä varallisuutta vai kryptovarallisuutta. Toisaalta kryptopörssien ja niiden yhteistyökumppaneiden tulisi myös tehdä oma osuutensa, eivätkä ne saisi antaa asiakkaidensa varojen hävitä. (Casey ym., 2018.)

4.6.3 Kaupankäynti kryptopörsseissä

Toisin kuin nykyiset arvopaperipörssit, kryptopörssit tarjoavat asiakkailleen mahdollisuuden käydä kauppaa keskenään ilman välittäjiä. (Casey ym., 2018) Kauppojen välittämisen ja toimeksiantojen kirjaamisen lisäksi kryptopörssit tarjoavat monia muitakin palveluita, kuten markkinatakauksia, neuvontaa ja säilytyspalveluita. (Casey ym., 2018) Myös perinteiset pörssikaupan toimijat, kuten CME Group, CBOE Global Markets ja Nasdaq, ovat kiinnostuneita kryptovarallisuudella käytävästä kaupasta ja ne ovat ottaneet kaupankäynnin kohteeksi kryptovaluuttafutuureja. (Casey ym., 2018) Toisaalta kryptopörssit perivät korkeita maksuja listautumisesta, mikä voi muodostua esteeksi listaamiselle. (Howell ym., 2020) Kryptovarallisuudella käytävää kauppaa voi seurata CoinMarketCap-verkkopalvelusta, joka tarjoaa kootusti markkinatietoja erityyppisistä tokeneista. (Howell ym., 2020)

Suosituimmat kryptopörssit ovat keskitettyjä. Niissä kaupankäynti on säilyttävää, mikä viittaa siihen, että niillä on hallussaan asiakkaidensa yksityisiä avaimia eli ne käytännössä pitävät hallussaan asiakkaidensa varoja niin sanotuissa kuumissa lompakoissa, jotka ovat yhdistettynä internettiin. Tämä mahdollistaa reaaliaikaisen kaupankäynnin, mutta aiheuttaa samalla vastapuoliriskin, mikä tarkoittaa sitä, että kryptopörssi ei kykene palauttamaan asiakkaidensa varoja, jos ne ovat tietomurtojen tai väärinkäytösten takia joutuneet vääriin käsiin. (Heilman ym., 2020.; Bentov, Zhang, Breidenbach, Daian & Juels, 2019; Krimminger, Lloyd & Rocks, 2019.)

Ideaalinen kryptopörssi olisi sellainen, jossa kaupankäynti on reaaliaikaista kuten keskitetyissä kryptopörsseissä, jolloin hintojen vaihtelu voidaan ottaa paremmin huomioon mahdollistaen myös automaattisen kaupankäynnin. Kauppapaikan tulisi myös estää lohkoketjujen viivettä hyödyntävät edelläkävijähyökkäykset ja olla luottamukseton, jolloin se ehkäisisi varkaudet. (Bentov ym., 2019)

4.6.4 Kaupankäyntialustat ja protokollat

Hajautetut kaupankäyntialustat ovat hajautettuja sovelluksia, jotka on tarkoitettu kaupankäyntiin Etherillä ja Ethereum-pohjaisilla tokeneilla. Kryptopörssit, kuten EtherDelta, pyrkivät toimimaan hajautettuna pörssinä, mutta niiden toimeksiannot tallennetaan keskuspalvelimelle, jota ne hallitsevat ja joka näyttää käyttäjilleen verkkosivuston käyttöliittymän. Sekä hajautettuja että keskitettyjä kaupankäyntialustoja on useita. (Howell ym., 2020) Keskitettyjä ovat esimerkiksi Binance ja Poloniex ja hajautettuja ShapeShift, 0x, SparkSwap ja EtherDelta. (Howell ym.,2020; Heilman ym., 2020)

Useimmat hajautetut kaupankäyntiprotokollat suorittavat toimintonsa tietyn tyyppisellä teknisellä toteutuksella toimivilla tokeneilla ja yhdellä tietyllä lohkoketjualustalla. Esimerkiksi AirSwap, EtherDelta ja 0x ovat protokollia, jotka operoivat ERC20-tokeneilla Ethereum-lohkoketjussa. Vastaavasti Stellarin hajautetussa kryptopörssissä käydään kauppaa Stellar-verkostoon kuuluvilla tokeneilla ja BitSharesin hajautettu kryptopörssi OpenLedger operoi tokeneilla, jotka ovat BitShares-lohkoketjualustalla. (Lin, 2019) EtherDelta on yksi käytetyimmistä kaupankäyntialustoista. Sen käyttäminen edellyttää, että käyttäjä luo lompakon tai käyttää jo olemassa olevaa lompakkoa, joka on yhteensopiva älykkäiden sopimusten kanssa. (Pinna, Ibba, Baralla, Tonelli & Marchesi, 2019.; Hsieh ym., 2018.) Se tarjoaa yksinkertaisen käyttöliittymän ja peruskaupankäyntitoiminnot. (Hsieh ym., 2018)

4.6.5 Hakkerointi ja manipulointi

Kryptopörssit eivät ole onnistuneet kovin hyvin asiakkaidensa varojen suojaamisessa. (Casey ym., 2018) Vaikka lohkoketjuteknologia itsessään kestää hyvin hakkerointia, sen ekosysteemissä on muita haavoittuvuuksia, jotka liittyvät erityisesti kauppapaikkoihin. (Casey ym., 2018, 35) Monia kryptopörssejä on hakkeroitu, minkä seurauksena niiden asiakkaat ovat menettäneet huomattavan määrän varojaan. (Marinoff, 2018) Tavallisista pörsseistä poiketen, niillä on merkittäviä määriä kryptovarallisuutta talletettuna digitaalisiin lompakoihin. (Casey ym, 2018) Keskitetyissä kryptopörsseissä yleisesti käytetyt kuumat lompakot mahdollistavat nopeammat suoritukset kaupankäynnissä mutta varjopuolena on se, että ne ovat alttiita hakkeroinnille. Joissakin kryptopörsseissä tarjotaan asiakkaille myös kylmää lompakkoa pitkäaikaiseen säilytykseen ja kuumaa lompakkoa välittömiin transaktioihin. Kylmät lompakot eivät ole kytkettynä internettiin, minkä vuoksi ne ovat huomattavasti turvallisempia. (Krimminger, Lloyd & Rocks, 2019.) Kryptopörssit etsivät myös uusia ratkaisuja säilytyspalveluiden turvaamiseen, kuten moniallekirjoitusta käyttävät lompakot. (Casey ym., 2018)

Hakkerointi ei ole pelkästään keskitettyjen kryptopörssien ongelma, vaan myös hajautettuihin kryptopörsseihin liittyy ongelmia. Esimerkiksi EtherDelta joutui mies-välissä-hyökkäyksen uhriksi vuonna 2017, jolloin hakkerit onnistuivat varastamaan Ethereum-kryptovaluuttaa. (Sampson, 2018)

Hakkerointien lisäksi kryptopörsseissä on myös hintojen manipulointia. Bitcoinin hintaa on usein manipuloitu ja esimerkiksi vuoden 2013 hintapiikki johtui manipuloinnista. (Gandal, Hamrick, Moore & Oberman, 2018) Tammikuussa 2018 tutkittiin, oliko Bitcoinin kurssia mahdollisesti manipuloitu Bitfinex-kryptopörssissä. (Popper, 2018) Kryptopörssien tarjoamaa markkinadataa ei ole yleensä tarkastettu, eikä sitä säännellä. Niissä käydään näennäistä kauppaa, jonka tarkoitus on vain luoda vaikutelma suuresta markkinaosuudesta. Esimerkiksi OKex voi liioitella vaihtoa 95 % ja Huobi 82 %. (Ribes, 2018) Sijoittajille olisi edullista, jos token-markkinoilla olisi parempi suoja huijauksia ja manipulointia vastaan, mutta useimmat tokenit ja kryptopörssit operoivat kuitenkin sijoittajansuojaa valvovan järjestelmän ulkopuolella ja tokenien markkinoilla on paljon huijauksia ja manipulointia. (Casey ym., 2018)

4.7 Lohkoketjuteknologian käyttöönotto rahoitusmarkkinoilla

Pinnan ja Ruttenbergin (2016) mukaan lohkoketjuteknologian käyttöönoton suhteen voidaan hahmotella vähintään kolme erilaista skenaariota: (1) Vakiintuneet instituutiot ottavat uuden teknologian käyttöön parantaakseen yritysklusterin tai yksittäisen yrityksen tehokkuutta mutta käytänteet jäävät ennalleen. (2) Keskeiset toimijat, kuten arvopaperikeskukset omaksuvat koko markkinoille ulottuvat hajautetut tilikirjat ja samalla vähintään jotkin pienemmät toimijat tulevat tarpeettomiksi. (3) Liikkeellelaskijayritykset, hallitukset ja fintech-yritykset ottavat johtoaseman arvopaperitransaktioita varten tehtyjen järjestelmien käyttöönotossa ja johdattavat arvopapereiden jälkimarkkinat uuteen aikakauteen.

Verkostovaikutus on hajautettujen fintech-sovellusten yleistymisen kannalta tärkeää. Fintech-yritykset tulevat tarvitsemaan riittävän määrän käyttäjiä hajautetuille sovelluksilleen, jotta niiden käyttäminen onnistuu riittävän hyvin, koska jokainen uusi käyttäjä lisää sovelluksen tarjoamaa hyötyä muille käyttäjille. Varhaisille omaksujille sovellukset eivät välttämättä tarjoa erityistä hyötyä, mikä saattaa estää verkostovaikutuksen edellyttämän kriittisen massan saavuttamisen. (Mills ym., 2016)

Peer-to-peer-transaktio-operaatiot edellyttävät likviditeettiä, jonka saavuttaminen edellyttää markkinoiden riittävää laajuutta dynaamisten markkinoiden takaamiseksi, kun ostajat ja myyjät tai lainan antajat ja ottajat kohtaavat. (Feenan ym., 2020) Kriittisen massan saavuttaminen edellyttää kannustimien yhteensovittamista verkostoon osallistuvien tahojen kesken ja mahdollisesti likviditeetin lisäämistä ostamalla verkoston jäseniltä myytäviä kohteita varastoon. Likviditeetin takaamiseksi saatetaan tarvita myös korkean tason sopimuksia institutionaalisella tasolla ja huomattavan aikaa vievien teknisten päivitysten tekemistä. (Feenan ym., 2020.)

5 EMPIIRISEN TUTKIMUKSEN LÄHTÖKOHDAT JA MENETELMÄT

Tässä luvussa kuvaillaan tutkimuksessa käytetty empiirinen tutkimusmenetelmä eli kerrotaan, miten aineisto kerättiin ja miten se analysoitiin. Tämän tutkimuksen empiirinen aineisto kerättiin teemahaastatteluilla, minkä jälkeen sille tehtiin sisällön analyysi. Aineiston keräämisestä kerrotaan alaluvussa 5.1. Alalussa 5.2 analysoidaan haastateltavien asiantuntemusta ja aineiston analyysistä kerrotaan alaluvussa 5.3. Teemahaastatteluissa käytetyn haastattelurungon kysymykset perustuivat tutkimuskysymyksiin, minkä lisäksi niillä pyrittiin täydentämään kirjallisuuskatsauksessa saatuja tietoja.

5.1 Aineiston keruu

Aineisto kerättiin puolistrukturoidulla teemahaastattelulla. Haastattelu valittiin tiedonkeruu tavaksi, koska kyseessä on aihe, jota on tutkittu verrattain vähän. (Hirsijärvi, Hurme, 2000) Kaikkia haastateltavia haastateltiin saman haastattelurungon pohjalta, mutta osalle haastateltavia esitettiin myös lisäkysymyksiä. Haastattelurunko löytyy liitteestä 1.

Haastateltavat valittiin sen perusteella, että heillä oletettiin olevan asiantuntemusta käsiteltävästä aiheesta. Haastateltavia etsittiin Facebookista ryhmästä Bitcoin ja kryptovaluutat sekä lähettämällä sähköpostia ja soittamalla puheluita sellaisiin organisaatioihin, joissa voisi olla asiantuntemusta lohkoketjuteknologiasta ja osakkeiden digitalisoinnista. Yhteydenottolistalla olivat esimerkiksi sellaiset tunnetut Suomessa toimivat yritykset kuin Nasdaq, Euroclear, TietoEvry, Solteq, Osuuspankki, Privanet Capital ja Coinmotion mutta sen lisäksi myös pieniä yrityksia, kuten Stoxchange ja Capitalgram.

Haastateltavia oli viisi. Tähän määrään päädyttiin sitä kautta, että viiden haastattelun pohjalta kertyi riittävästi aineistoa tutkimuksen suunnitellun laajuuden kannalta. Määrä ei kuitenkaan riitä kovin merkittävään saturaatioon, joten tekemällä useampia haastatteluja, olisi saavutettu laajempi aineisto, jonka

perusteella olisi voinut arvioida paremmin aineiston reliabiliteettia vertaamalla eri haastateltavien antamia tietoja keskenään. Lisäksi haastateltavien pieni määrä vaikuttaa siihen, miten validia aineisto on, mikä käytännössä tarkoittaa sitä, ettei pieni aineisto anna niin paljon tutkimuskysymysten kannalta relevantteja vastauksia kuin suurempi aineisto. Potentiaalisten haastateltavien määrää rajoitti myös se, että haastattelut tehtiin suomeksi. Tästä syystä esimerkiksi Nasdaqilta ja Euroclearilta ei löytynyt sopivia haastateltavia. Haastattelut tehtiin Google Meet- ja Teams-sovelluksilla ja talletettiin OBS Studio -ohjelmalla. Korona-pandemian ja etäisyyksien vuoksi yhtään haastattelua ei tehty kasvokkain.

5.2 Haastateltavien asiantuntemus

Tässä alaluvussa analysoidaan haastateltavien asiantuntemusta lohkoketjuteknologiasta ja osakkeiden digitalisoinnista pohjautuen haastatteluaineistoon. Taulukossa 3 on listattu haastatteluiden numerot ja haastateltavan edustama organisaatio. Cryptosuvi Osuuskunta on pieni teknologiayritys, jossa on yksi työntekijä. Stoxchange on suomalainen start-up-yritys, joka kehittää STO-alustaa osakeantien digitalisointiin. Coinmotion on suomalainen kryptovaluuttakaupankäynnin palveluita tarjoava yritys. OP Financial Group on osuuskunta, joka koostuu 137:stä osuuspankista ja jolla on yli 2 miljoonaa omistaja-asiakasta. Sen liiketoimintaan kuuluu vähittäispankki-, yrityspankki- ja vakuutustoimintaa.

TAULUKKO 3 Haastattelunumerot ja organisaatio.

Haastattelunumero	Organisaatio
1	Cryptosuvi Osuuskunta
2	Stoxchange
3	Coinmotion
4	OP Financial Group
5	OP Financial Group

Haastateltava 1 on tutustunut lohkoketjuteknologiaan ja yritysten digitalisointiin liittyvään lainsäädäntöön omatoimisesti eri tavoin tehden esimerkiksi erilaisia yritysten digitalisointikokeiluja Suomessa, Delawaressa ja Virossa. Vuosina 2013-2014 hän tutustui kryptovaluuttoihin. 2015 hän tutustui Colored Coins -konseptiin, jonka pohjalle hän digitalisoi oman yrityksensä osakkeet 2016 ja myöhemmin samana vuonna hän digitalisoi yrityksen Ethereum-tokenien pohjalle. Hän on ollut myös töissä Token Market nimisessä yrityksessä, joka toteutti ICO:ita STO:ita. Lisäksi hän on tehnyt työkseen älysopimuskehitystä ja älysopimusauditointeja. (Haastattelu 1)

Haastateltava 2 on perehtynyt lohkoketjuteknologiaan vuodesta 2012 alkaen ja on kirjoittanut Bitcoin-sijoittamisesta kirjan minkä lisäksi hän on ollut perustamassa Start-up-yritystä, joka kehittää omaa STO-alustaa. Hän on myös osallistunut joihinkin lohkoketjuteknologiaan liittyviin konferensseihin.

Haastateltava 3 on ollut rahoitusalalla ennen siirtymistään työskentelemään virtuaalivaluuttoihin liittyvien liiketoimintojen ja palveluiden pariin, joista

hänellä on kokemusta 3 vuotta. Hän on myös ollut mukana muutamissa projekteissa, joissa on sovellettu yksityistä lohkoketjua.

Haastateltava 4 on työskennellyt 25 vuotta hajautetun tietojenkäsittelyn parissa. 90-luvulla hän on ollut töissä yrityksessä, jossa hänen tehtävänsä oli kehittää tietokannan hajautusarkkitehtuuria. Lohkoketjuteknologiaan hän on perehtynyt aluksi oman työnsä ohessa. Hän on ollut käynnistämässä ja toteuttamassa projektia, jonka lopputuotteena oli Corda-teknologiaan pohjautuvaa DIAS-asunto-osakekauppaverkko, joka on nykyisin laajassa käytössä. Sen lisäksi hän on ollut merkittävässä roolissa projektissa, joka toteuttaa vahvistetun datan verkkoa käyttävää Findynet-alustaa, jonka avulla voi muun muassa perustaa yrityksiä ja käydä omistuksilla kauppaa. (Haastattelu 4)

Haastateltava 5 on toiminut asiantuntijatehtävissä sekä päätyössään että sivutoimisesti projekteissa, joissa on toteutettu lohkoketjuteknologiaan pohjautuvia Findynet- ja Stoxchange-alustoja. Hänellä on yritysjuridiikkaan ja liiketoimintaprosesseihin liittyvää asiantuntemusta.

5.3 Aineiston analysointi

Haastatteluaineistoja analysoitaessa tässä tutkimuksessa menetelmänä on laadullinen aineistolähtöinen sisällön analyysi, jonka avulla tutkittavasta ilmiöstä pyritään antamaan tiivistetty kuvaus ja löytämään siitä merkityksiä. (Tuomi & Sarajärvi, 2004, s. 105–106) Tuomen ja Sarajärven (2004) mukaan laadullisen tutkimuksen analyysissä on neljä vaihetta:

1. Päätä, mikä aineistossa kiinnostaa.
2. Käy läpi aineisto, merkitse kiinnostavat asiat ja kerää merkityt asiat erilleen muusta aineistosta
3. Seuraavaksi aineisto luokitellaan teemoihin
4. Lopuksi kirjoitetaan yhteenveto.

Haastatteluista kertyi kaikkiaan viisi äänitallennetta, joiden pituus vaihteli puolesta tunnista tuntiin. Haastattelut litteroitiin, minkä jälkeen litterointi teemoiteltiin haastattelurungon kysymyksiin perustuen tiettyihin aihepiireihin merkitsemällä ne Word-dokumenttiin kommenteilla. Haastatteluissa vastaukset kysymyksiin rönsyilivät jonkin verran, minkä vuoksi yhden kysymyksen vastaus saattoi sisältää asioita, jotka liittyivät useisiin kysymysrungon kysymyksiin. Tästä syystä teemoittelu ei mennyt yksi yhteen sen kanssa, mihin kysymykseen haastateltavat vastasivat. Ne osat haastatteluaineistosta, jotka eivät vastanneet valittua teemoittelua, jätettiin analyysin ulkopuolelle. Luvussa 6 on tehty yhteenveto haastatteluista.

6 TUTKIMUKSEN TULOKSET

Tässä luvussa kuvaillaan haastatteluaineisto ja asioista pyritään antamaan sellainen kuva, mikä niistä on haastateltavilla. Tässä luvussa tuloksia tarkastellaan lähinnä haastatteluiden pohjalta, mutta joitakin faktoja on tarkastettu muista lähteistä. Tarkempi analyysi tulosten merkityksestä tehdään luvussa 7.

Alaluvussa 6.1 kuvaillaan, millaisia osakkeiden digitalisointiin käytettäviä teknologioita aineistossa tuli esiin. Alaluvussa 6.2 kuvaillaan haastateltavien käsitystä osakkeiden digitalisoinnin kehityskulusta. Alaluvussa 6.3 kuvaillaan millaisia lainsäädännöllisiä ongelmia haastateltavat näkevät lohkoketjuteknologian käytössä osakkeiden digitalisoinnissa. Alaluvussa 6.4 käsitellään erilaisten yhtiömuotojen vaikutusta osakkeiden digitalisointiin ja myös yritysten omistuksenhallinnan digitalisointiin eri yhtiömuodoissa. Alaluvussa 6.5 kuvaillaan haastateltavien näkemyksiä lohkoketjuteknologiaan liittyvistä ongelmista. Alaluvussa 6.6 kuvaillaan haastateltavien näkemyksiä lohkoketjuteknologian eduista osakkeiden digitalisoinnissa. Alaluvussa 6.7 kuvaillaan haastateltavien näkemyksiä siitä, millä tavalla lohkoketjuteknologia ja arvo-osuusjärjestelmä kilpailevat keskenään markkinoista. Alaluvussa 6.8 kuvaillaan, millaisia tulevaisuudenkuvia haastateltavilla on osakkeiden digitalisoinnin kehityksestä seuraavan kymmenen vuoden aikana. Alaluvussa 6.9 kuvaillaan haastateltavien näkemyksiä arvo-osuusjärjestelmästä ja sen ongelmista.

6.1 Osakkeiden digitalisoitiin käytetyt teknologiat

Nykyisen digitaalisten osakkeiden infrastruktuurin muodostavat pääpiirteissään arvo-osuusjärjestelmät, joihin osakkeet kirjataan ja pörssit, joihin ne listataan. Arvo-osuusjärjestelmät ja pörssit on perinteisesti eriytetty toisistaan riskienhallinnan vuoksi. (Haastattelu 3)

6.1.1 Lohkoketjuteknologiaan pohjautuva osakkeiden digitalisointi

Lohkoketjuteknologiaan perustuva osakkeiden digitalisointi on ollut mahdollista vuoden 2012 joulukuusta alkaen, jolloin markkinoille tuli yksi ensimmäisistä lohkoketjuteknologiaan pohjautuvista digitaaliset osakkeet mahdollistavista teknologioista eli Colored coins -konsepti, jonka avulla toteutettiin tokeneihin pohjautuvia digitaalisia osakkeita. (Rosenfeld, 2012; Haastattelu 1) Niissä ei kuitenkaan pystytty toteuttamaan esimerkiksi voitonjakoa, koska niissä ei ollut käytössä riittävän kehittyneitä älykkäitä sopimuksia. Konsepti mahdollisti vielä 2015 todella yksinkertaiset älysopimukset ja sitä kautta myös digitaaliset osakkeet, jotka toteutettiin COLU-sovelluksella. COLU-projekti on kuitenkin päättynyt, eikä COLU-työkaluja ole enää saatavilla internetissä, mutta konseptin avulla aikoinaan toteutettuja osakkeita voi edelleen löytää Bitcoinin lohkoketjusta. (Haastattelu 1.)

Digitalisointiin on kehitetty myös yksityiseen lohkoketjuun pohjautuvia alustoja. Tällaista on kehittänyt esimerkiksi Otonomos-yhtiö. (Haastattelu 1) Dan Larimerin johtama projekti nimeltä Bitshares mahdollisti käyttäjille omien tokenien tekemisen, mutta tarjosi kuitenkin heikot mahdollisuudet tehdä älykkäitä sopimuksia. Ethereumin julkistamisen jälkeen osakkeiden digitalisoinnissa on alettu hyödyntämään Ethereum-älysopimuksia. Ethereumin jälkeen on tullut useita muitakin älysopimusalustoja, kuten esimerkiksi EOS ja ADA. (Haastattelu 1.)

Lohkoketjuteknologialla toteutetut osakkeet ovat yleensä security-tokeneita, eli ne ovat tokeneilla toteutettuja arvopapereita. Myös muita arvopapereita voidaan toteuttaa samalla tavalla tokeneilla. (Haastattelu 3) Osakkeiden digitalisoinnissa voidaan käyttää julkista lohkoketjua, kuten Ethereum tai yksityistä lohkoketjua, kuten R3:n ylläpitämä Corda, jossa on mukana paljon rahoitusalan organisaatioita, jotka käyttävät sitä eri tavoin esimerkiksi palvelimissaan. (Haastattelu 3, Haastattelu 5) R3 on useiden suurten pankkien omistama konsortio. (Haastattelu 5) Yritysten välisissä hankkeissa käytetään yleensä yksityisiä lohkoketjuja, koska julkisia lohkoketjuja on mahdotonta kontrolloida. (Haastattelu 3) Yksi haastateltavista korosti, että Corda on pankkien välinen transaktioidenhallintaverkko, joka ei ole varsinaisesti lohkoketjuverkko, vaikka se lasketaan lohkoketjuteknologiaksi, vaan transaktioketjuverkko. (Haastattelu 4)

6.1.2 Osakekauppaverkon toteutus Corda-verkossa eli Jupiter-malli

Tässä alaluvussa kerrotaan, kuinka Findynet-osuuskunnan toteuttama ns. Jupiter-mallinen osakekauppaverkko toimii. Jupiter-malliseen verkkoon viitataan jäljempänä sanalla osakekauppaverkko. Nimitys Jupiter viittaa pilottiprojektiin, jossa toteutettiin osakekauppaverkon prototyyppi. Ennen Jupiteria oli myös projekti koodinimellä project-Mercury, jossa luotiin kahden verkon, eli Hyperledger Indy -identiteettiverkon ja Corda-transaktioverkon, yhdistelmä, jonka avulla pystyi luomaan osakeyhtiön.

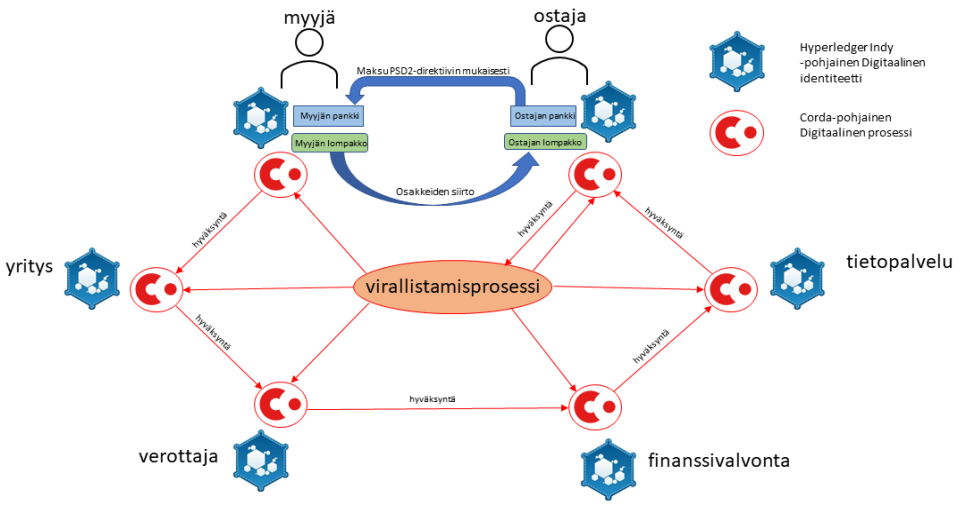
Osakkeiden digitalisoinnissa voidaan käyttää osakekauppaverkkoa, joka on hajautettuun luottamukseen pohjautuva identiteettiverkon, kuten Hyperledger Indy, ja Corda-teknologialla toteutetun transaktionhallintaverkon yhdistävä järjestelmä, jossa ei käytetä lohkoketjuja eikä tokeneita. Suomessa tällaista hajautettuun sopimiseen pohjautuvaa teknologiaa kehittää Findynet-Osuuskunta. Hajautettu sopiminen sopii myös kaikkeen muuhunkin kaupankäyntiin.

" …suunta on selvä, että tämä digitaalinen identiteetinhallinta menee siihen suuntaan kuin mitä me tässä Jupiter-harjoituksessakin prototttiin ja kun se menee siihen suuntaan, niin sitten tosiaan pystytään tämän kuvan mukaan tekemään sitä hajautettua digitaalista sopimista, mikä on yhtä kuin kaupankäyntitransaktiot, jotka ovat kaikki tätä kategoriaa ja pystytään tekemään huomattavasti parempia verkkoja kaiken näköiseen kaupankäyntiin, ei ainoastaan osakekaupankäyntiin." (Haastattelu 4)

Suomessa on jo käytössä Corda-teknologialla toteutettu Dias.fi niminen asuntokaupankäynnin alusta. Sen toteuttaminen osoitti, että Corda-teknologian päälle voidaan rakentaa melko monimutkaisiakin kauppaprosesseja ja sen avulla voi käydä myös kauppaa osakkeilla. Aiemmin vastaavia alustoja on ollut hyvin vaikea toteuttaa siten, että prosessi pysyy hallinnassa. (Haastattelu 4)

Kuviossa 6 on esitettynä yksinkertaistettuna kaupankäynnin kulku osakekauppaverkossa. Loogisesti kaupankäynti osakkeilla on yksinkertainen tapahtuma, jossa ostaja ja myyjä sopivat millä hinnalla myyjä on valmis luopumaan osakkeista ja vastaavasti ostaja ostamaan osakkeet. Käytännössä kaupankäynti on kuitenkin monenkeskinen sopimus, joten osakekauppaverkossa ovat mukana ostajan ja myyjän lisäksi muun muassa yritys, jonka osakkeilla käydään kauppaa, verottaja, valvova viranomaistaho eli Suomessa finanssivalvonta ja luottotietopalveluiden toimittaja, joiden lisäksi Corda-verkossa on kaupan vahvistava notaari, joka virallistaa kaupan. Kauppaprosessissa älykäs sopimus käy läpi kaikki sopimusosapuolet ja jos kaikki osapuolet hyväksyvät kaupan, Corda-verkossa oleva notaari vahvistaa sen, minkä jälkeen kauppa on virallisesti toteutunut. Virallistamisprosessiin kuuluu, että notaari toimittaa kaupantekoon osallistuneille identiteeteille tiedon kaupan virallistamisesta eli myyjälle, ostajalle, yritykselle, verottajalle ja luottotietopalveluiden toimittajalle. Rahojen liikkuminen voidaan toteuttaa PSD2-direktiivin mukaisesti siten, että ostaja valtuuttaa myyjän valtakirjalla nostamaan maksun pankkitililtään, jonne rahat on katevarauksella varattu. (Haastattelu 4)

Corda-verkossa osakkeet säilytetään ns. lompakoissa verifiable claim -muodossa, jolloin ne ovat faktoja, jotka kolmas osapuoli voi vahvistaa. Kaupankäynnin jälkeen ostajalla on lompakossaan verifiable claim, joka kertoo ostajan omistavan ostamansa osakkeet. Toinen saman identiteettiverkon jäsen, jolle fakta esitetään, voi tarkistaa transaktioverkosta onko väitetyn mukainen transaktio validi eli onko ostaja edelleen osakkeiden omistaja vai onko osakkeet myyty jo eteenpäin. (Haastattelu 4)



KUVIO 6 Yksinkertaistettu esitys osakekauppaverkosta. (Haastattelu 4)

Perinteinen digitaalisten osakkeiden kaupankäyntiprosessi on hyvin erilainen. Osakekauppaverkko on toteutettu kokonaan uudella teknologialla eikä siinä ole pörssiä, selvitys- ja määrityspalveluita eikä säilytyspalveluita, joiden olemassaoloon nykyinen järjestelmä perustuu. Osakekauppaverkossa osakkeilla voi käydä kauppaa yritysten omilla internetsivuilla ja niitä voidaan liikutella suoraan lompakosta toiseen. Osakekauppaverkossa palataan tavallaan aikakauteen, kun kaikki kaupanteko tapahtui paperilla mutta paperi on korvattu digitaalisella alustalla. Myös Ethereum-verkossa toteutettava kaupankäyntiprosessi poikkeaa merkittävästi osakekauppaverkosta, koska osakekauppaverkossa ei käytetä tokeneita eikä kryptovaluuttaa ja osakekauppaverkossa käytettävät älysopimukset ovat erilaisia kuin Ethereum-verkossa. Ethereum-verkossa ei ole myöskään osakekauppaverkosta poiketen digitaalisia identiteettejä, vaan sen sijaan siellä käytetään julkisenavaimen salaukseen pohjautuvaa identiteetinhallintaa. Yksityiseen Corda-verkkoon pohjautuva osakekauppaverkko takaa sen, että verkon kaatuessa on aina olemassa vastuullinen osapuoli, toisin kuin julkisessa lohkoketjussa, kuten Ethereumissa, jossa verkon kaatuessa kukaan ei ole vastuussa. (Haastattelu 4)

Osakekauppaverkossa on yksi lain tulkintaan liittyvä ongelma, joka liittyy siihen, että lain mukaan jokainen yksityisen osakeyhtiön osake pitää numeroida. Osakekauppaverkossa ei käytetä kuitenkaan paperisia osakekirjoja, eikä tällaista numerointia voi siksi tehdä. (Haastattelu 4)

Dias.fi-palvelusta poiketen osakekauppaverkko ei ole päässyt pilottivaihetta pidemmälle, vaikka teknologia on todettu toimivaksi. Yksi syy voi olla siinä, että solmun luominen Corda-verkkoon maksaa liikaa, jolloin tavallisilla startup-yrityksillä ei ole siihen varaa ja toisaalta osakekauppaverkko saattaa olla lainsäädännöllisesti harmaalla alueella. (Haastattelu 5)

Ethereum verkossa toimiviin kaupankäyntiverkkoihin verrattuna Jupiter-mallinen osakekauppaverkko tarjoaa kaksi tärkeää etua: (1) osakekauppaverkko on skaalautuva ja (2) siinä kaikilla osapuolilla on Know Your Customer -sääntöihin pohjautuva identiteetti. Ethereum-maailmassa vastapuolia ei tunneta, minkä

vuoksi transaktiot ovat käytännössä lainsuojattomia, koska lain näkökulmasta sopimukset tulisi tehdä tunnettujen osapuolten kesken. Lisäksi osakekauppaverkossa on pohjalla standardiprotokollat. Siinä identiteettiverkko toimii trust-over-ip-protokollalla, jonka standardoitumiskehitys on voimakasta. Identiteettiverkko käyttää esimerkiksi sellaisia standardeja kuin verifiable claim, distributed id ja kommunikointiprotokollana Dicomia. Ethereum sen sijaan ei ole standardiprotokolla. (Haastattelu 4)

6.2 Osakkeiden digitalisoinnin kehityskulku

Osakkeiden digitalisointi lohkoketjuteknologialla alkoi Bitcoinin ja Ethereumin kehittymisen myötä. Vuosien 2017 ja 2018 aikana alkaneen ICO-buumin aikana alettiin käytännössä tokenmuotoistamaan kaikkea, mikä liittyy omistamiseen. Silloin alettiin pohtia, että jos token edustaa jotain omistusta projektista tai yrityksestä, niin se on osakkeen tyyppinen instrumentti. Tällaisessa on samoja elementtejä kuin osakkeen digitalisoinnissa, minkä vuoksi herättiin siihen, että lohkoketjuteknologian päälle voisi alkaa tekemään perinteisiä osakkeita ja muita omaisuusluokkia, mikäli teknologiaa kehitetään eteenpäin. (Haastattelu 3) Suomessa ensimmäiset lohkoketjuteknologiaan pohjautuvat pilottiprojektit on jo tehty. Sveitsissä lohkoketjuteknologian käyttö on jo melko pitkällä ja Saksassakin yritys nimeltä Neufund on jo toiminnassa. (Haastattelu 5)

Lohkoketjut ovat hyvin merkittävä keksintö, koska niiden ansiosta oivallettiin, että internetin sisään voidaan rakentaa luottamus. Bitcoin oli ensimmäinen demonstraatio tästä ja Ethereum on jalostanut ajatusta eteenpäin muun muassa mahdollistamalla erilaiset tokenit. Vaikka lohkoketjuteknologialla on tehty monenlaisia demonstraatioita, niin niiden ongelmana on suorituskyvyn puute ja älysopimusten heikko yhteensopivuus lainsäädännön kanssa.

"Ethereumissa sitten tulivat nämä tokenit ja muut mukaan ja tuota niillä pystyy rakentamaan kaikkia kivoja demoja, mutta kun ei siellä ole sitä suorituskykyä ja siellä ei ole tukea tällaiselle vanhan liiton sopimiselle saatikka, että ne olisivat millään tavalla lain kanssa yhteensopivia ne nykyiset defi-ratkaisut, niin se on vähän niin kuin hakoteillä, eli hienoja demoja on saatu aikaiseksi siellä maailmassa, missä oikeasti pelataan lohkoketjuilla, mutta minä väitän, että siellä tulee vielä iso krapula, ennen kuin sinne on saatu siihen softapinkkaan kaikki se mitä vaaditaan, että se on skaalautuva ja täysin laillinen systeemi." (Haastattelu 4)

6.3 Lainsäädännön ongelmat

Suurin ongelma lohkoketjuteknologian käyttöönoton kannalta on saada se sopivaksi vanhan lainsäädännön kanssa ja toisaalta lainsäädännön muuttaminen sellaiseksi, että sitä voidaan käyttää. Jotta tämä toteutuu, kaikilla osapuolilla pitäisi olla siihen kannustimet. (Haastattelu 3) Suomessa lainsäädäntö ei ole vielä

osakkeiden digitalisoinnin suhteen valmis, mikä estää lohkoketjuteknologian hyödyntämisen osakkeiden digitalisoinnissa. (Haastattelu 3) Tosin Suomessa yhtiöt saavat itse digitalisoida osakkeensa, mutta siinä tapauksessa, että osakkeiden digitalisointia hoitaa jokin ulkopuolinen yritys, kuten esimerkiksi Stoxchange, Privanet Capital tai Nasdaq, tarvitsee tämä ulkopuolinen yritys toimiluvan, jotta se saa tarjota osakkeidendigitalisointipalveluita. (Haastattelu 2)

Ei-arvopaperimuotoisen omaisuuden digitalisointi onnistuu jo nykyisen lainsäädännön puitteissa. (Haastattelu 3) Arvopapereiden tokenmuotoistaminen sen sijaan on hyvin hidasta verrattuna muihin omaisuusluokkiin, koska se on tiukimmin säänneltyä. (Haastattelu 3) Voi mennä vielä vuosikymmen, että kaikki tarvittava osakkeiden digitalisointia koskeva lainsäädäntö saadaan voimaan ja adaptoidutaan uuteen teknologiaan. (Haastattelu 3)

Lainsäädäntö kehittyy mutta on yleensä jäljessä lohkoketjuteknologian kehityksestä, koska teknologian kehityskulkuja on vaikea ennustaa. Sääntely on kuitenkin yhteiskunnan kannalta tärkeä asia ja se luo perustan yritysten yhteistyölle. (Haastattelu 1) Lainsäädäntö ei ole lohkoketjuteknologian suhteen saavuttanut lopullista muotoaan, eikä sellaista ole välttämättä odotettavissakaan, koska uusia alustoja kehitellään, lohkoketjuteknologialle löytyy uusia käyttökohteita ja teknologian kehitys on nopeaa. (Haastattelu 1)

Yhteiskunta ei ole vielä valmis hyväksymään lohkoketjuteknologiaa lainsäädännön ja valvonnan taholta (Haastattelu 2) Jotta lainsäädäntö saadaan lohkoketjuteknologian kannalta suotuisaksi, tarvitaan kansallisen tason lobbausta sellaisen tahtotilan luomiseksi lainsäätäjille, joka on teknologian kannalta suotuisa. (Haastattelu 3) Esteeksi saattaa muodostua lohkoketjuteknologian huono maine, pelko markkinoille syntyvistä kuplista ja toisaalta se, että jotkut intressitahot haluavat pitää rahoituksen hakemisen tietyillä tahoilla. (Haastattelu 5)

Lainsäädännön kannalta yksi vaikea asia on se, jos kukaan ei omista verkkoa, jossa osakkeita säilytetään, jolloin verkon kaatuessa kukaan ei vastaa siitä. (Haastattelu 4) Tämä ongelma koskee erityisesti julkisia lohkoketjuja, mutta yksityisissä lohkoketjuissa asia on paremmin hallittavissa. (Haastattelu 3) Jupitermallissa on käytössä yksityinen Corda-verkko, jossa tätä ongelmaa ei ole. (Haastattelu 4)

6.3.1 Identiteetinhallinta

Lohkoketjualustojen Identiteetinhallinnassa on sääntelyn kannalta ongelmallista se, että tunnistustiedoista ei suoraan selviä tokenmuotoisen omaisuuden omistaja. Esimerkiksi Ethereumin identiteetinhallinta on pseudonyymistä, minkä vuoksi erilaisissa rekistereissä linkittäminen henkilöön täytyy tehdä erikseen. (Haastattelu 1) Identiteetinhallintaa koskevat ongelmat tulivat esiin kahden haastateltavan kohdalla, joista toinen näki ongelman lainsäädännöllisenä edellyttäen lakien muuttamista vastaamaan lohkoketjuteknologian ominaisuuksia ja toinen piti sitä Ethereum-verkon identiteetinhallinnan ongelmana korostaen sitä, että teknologian tulisi olla lain mukaista.

EU:n rahanpesudirektiivi vaikeuttaa digitaalisten yhtiösopimusten tekoa, koska se vaatii esimerkiksi sitä, että omistajien pitää olla tunnistettavissa ja monissa maissa myös joissakin tietyissä yrityksen toiminnoissa, kuten rahoituksessa tai johtajien nimeämisessä, vaaditaan tunnistautumista. (Haastattelu 1) Lain mukaan listaamattoman yrityksen tulee myös tietää kuka sen osakkeet omistaa, minkä vuoksi yritystä tulee aina informoida tehdyistä osakekaupoista. (Haastattelu 4) Tällaiset vaatimukset vaikeuttavat lohkoketjuteknologian käyttöä osakkeiden digitalisoinnissa. (Haastattelu 1) Know Your Customer -sääntöihin pohjautuvan identiteetinhallinnan puuttuminen tarkoittaa sitä, että vastapuolia ei tunneta, jolloin transaktiot ovat epävirallisia lainsäädännön kannalta. (Haastattelu 4)

6.3.2 Määrämuotoisuus

Suomessa lainsäädäntö on kankea ja vaatii liikaa Startup-yrityksiltä. (Haastattelu 5) Monien sopimusten suhteen laissa edellytetään määrämuotoisuutta, vaikka näin ei tarvitsisi olla. Joillakin maantieteellisillä alueilla erillinen laki sallii myös älysopimuksen käytön niissä tilanteissa, joissa paperinen sopimus on vaadittu. Suomessa tällaista mahdollisuutta ei ole, vaan sen sijaan sovelletaan suoraan esimerkiksi arvopaperimarkkinalakia. (Haastattelu 5; Haastattelu 1) Toinen tapa, jolla lohkoketjuteknologian käyttöönottoa voi helpottaa, on finanssivalvonnan myöntämä ns. hiekkalaatikkolupa, joka mahdollistaa lain muotoseikoista joustamisen lohkoketjuteknologiaa kehittäville yrityksille. Tällaisen sopimuksen voi tehdä esimerkiksi Britanniassa. Kaikissa sopimustilanteissa laki ei kuitenkaan edellytä Suomessakaan määrämuotoa, jolloin älysopimuksia voi käyttää. (Haastattelu 1) Teknologiaa kehittäessä pitää lain muodon lisäksi ottaa huomioon se, mitä lainsäätäjä on tarkoittanut, sillä vaikka lain muoto täyttyisi, niin lain henki ei välttämättä täyty.

" …mää olin törmännyt tähän aikaisemmin osakeyhtiölakia selatessani ja lipukkeessa, joka voi olla osinko- tai äänestyslipuke ja se vois olla tapa saada tokenisoitua helposti, mutta tässä on sellainen mahdollisuus, että juridisesti merkitsee myös lain esityöt, eli ei ainoastaan se mitä laissa lukee, vaan se mitä sillä on tarkoitettu, mitä lainsäätäjä on tarkoittanut. "

Useimmissa maissa lainsäädäntö edellyttää, että osakkeet ovat joltakin osin paperisia, mutta joissakin valtioissa, kuten USA:n Delawaressa lainsäädäntö ei edellytä paperisia sopimuksia kaikilta yhtiömuodoilta. (Haastattelu 1) Myös Jupiter-mallisen osakekauppaverkon ongelmana on se, että laki vaatii osakekirjojen numerointia, koska digitaalisissa osakkeissa ei ole paperisia osakekirjoja. (Haastattelu 4) Jupiter-mallisessa osakekauppaverkossa toimintalogiikka on kuitenkin vastaava kuin paperisilla osakkeilla, minkä vuoksi se on lainsäädännön kannalta huomattavasti helpompi toteuttaa kuin token-pohjainen digitalisointi. (Haastattelu 4)

6.3.3 Eri maiden poikkeava lainsäädäntö ja lakien tulkinta

Lohkoketjuteknologiaa käytettäessä täytyy huomioida eri maiden erilaiset lainsäädännöt ja valita ja sovittaa teknologia sen mukaan. (Haastattelu 2) Sveitsi on yksi ensimmäisistä maissa, joissa lainsäädäntö mahdollistaa osakkeiden digitalisoinnin lohkoketjuteknologialla, minkä vuoksi Sveitsi on eräänlainen testilaboratorio tällä alalla. (Haastattelu 3) Eri maissa on toteutettu Security token -hankkeita ja samalla on yritetty lobata lainsäädäntöä tällaisille suotuisaksi, jotta esimerkiksi osakkeita voisi toteuttaa tokenmuodossa. (Haastattelu 3) Joissakin maissa, kuten USA:ssa ja Singaporessa on lainsäädäntöhankkeita tällaisen suhteen ja myös EU-tasolla on tätä koskeva sääntelykehikko, joka tulee voimaan vuonna 2024. Sitä ennen lainsäädäntö hankaloittaa merkittävästi osakkeiden digitalisointia EU:ssa. EU-maissakin on kuitenkin eroja, mistä esimerkkinä Saksa, jossa digitaalisten osakkeiden toteuttaminen ns. e-security muodossa on mahdollista kansallisen lainsäädännön ansiosta. (Haastattelu 3)

Iso osa finanssisääntelystä tulee EU:sta, jossa eri maiden sääntelyä on yhtenäistetty. Kansallisella tasolla voidaan kuitenkin tehdä poikkeavaakin lainsäädäntöä, kuten Saksassa on tehty. (Haastattelu 3) Saksassa lohkoketjuja koskeva lainsäädäntö on kevyempi kuin Suomessa ja Sveitsissä se on vielä kevyempi. (Haastattelu 5) Suomen lainsäädäntö tulee käytännössä EU:n kautta ja sitä tulkitaan Suomessa kireämmin kuin olisi tarpeen. Eri maissa tulkinnat ja viranomaisten käyttäytyminen ovat erilaisia, vaikka lainsäädäntö olisi sama. Suomalaiset viranomaiset voisivat suhtautua myötämielisemmin lohkoketjuteknologiaan, mutta tätä jarruttaa se, että lohkoketjuteknologia on kryptovaluuttojen takia huonossa maineessa. (Haastattelu 5) Kun Suomessa viimeksi oli innostusta osakkeiden digitalisointiin, se tyrehtyi finanssivalvontaan ja valvojiin, jotka Suomessa ovat verrattain varovaisia. (Haastattelu 5)

ICO-buumin aikana monet suomalaiset päätyivät tekemään ICO:n Virossa, koska Suomen lainsäädäntöön liittyi epävarmuutta. Yksi menestyneimmistä tällaisista projekteista on Aave, joka on kansainvälisestikin merkittävä hajautettu alusta. Myöhemmin EU:n kryptovaluuttoja koskeva lainsäädäntö johti siihen, että ICO:t edellyttävät Finanssivalvonnan luvan myös Suomessa. (Haastattelu 3)

6.4 Yhtiömuodon vaikutus yrityksen digitalisointiin lohkoketjuteknologialla

Tyypillisesti digitalisoitavat yritykset ovat osakeyhtiöitä, mutta muitakin yhtiömuotoja voi digitalisoida. Muita yhtiömuotoja koskevat erot tulee ottaa huomioon tokenin sääntelyä tehtäessä tai teknologiaa määriteltäessä, koska yhtiömuoto voi vaikuttaa omistussuhteiden kautta muun muassa tokenien siirrettävyyteen ja siihen, miten tuottoja jaetaan. Yhtiömuoto siis vaikuttaa tokenien toimintalogiikkaan, joten sillä on merkitystä alustan tai tokenin

ohjelmoinnissa ja eri yhtiömuotojen tokenmuotoistamisessa on erilaiset rajoitteet tokenmuotoisuuden suhteen. (Haastattelu 3)

Erilaisten osakeyhtiöiden välillä, kuten yksityisten ja julkisten ja toisaalta sellaisten osakeyhtiöiden, joissa osakkeen omistus oikeuttaa johonkin palveluun, ei ole merkittäviä eroja tokenmuotoistamisen kannalta. Kaikkien osakeyhtiöiden juridinen omistusrakenne on samanlainen, minkä vuoksi tokenien toimintalogiikassa ei ole eroja. Esimerkiksi lomaosakkeiden tapauksessa token edustaisi lomaosakkeen omistusta, jolloin sitä voitaisiin hyödyntää lomaosakkeiden kaupankäynnissä tai palvelujen tarjoamisessa. Token auttaisi verifioimaan, kenellä lomaosake milloinkin on omistuksessaan ja mahdollistaisi osakasluettelon ylläpidon automatisoinnin. Nykyisin osakasluetteloiden ylläpito on manuaalista ja se voidaan hoitaa esimerkiksi taulukkolaskentaohjelmalla. Ylläpidon automatisointi helpottaisi työtä ja tekisi osakasluettelon hallinnasta myös skaalautuvampaa. (Haastattelu 3)

Se, hyväksyykö verottaja yrityksen omistamisen älykkääseen sopimukseen pohjautuen, riippuu yhtiömuodosta. (Haastattelu 1) Yhden haastateltavan mukaan yhtiömuodoissa voidaan nähdä tietynlainen jatkumo (Taulukko 4), jossa alkupäässä yhtiömiehet ovat täysin vastuullisia ja yhteenliittymät eivät ole virallisesti yrityksiä ja loppupäässä yritykset ovat oikeushenkilöitä ja yhtiömiehet eivät ole vastuullisia muusta kuin sijoittamastaan pääomasta. Alkupäähän kuuluu elinkeinoyhtymä, joka on puhdas sopimus ilman muotovaatimuksia, minkä vuoksi sellainen voi olla lohkoketjussa älykkään sopimuksen muodossa. Elinkeinoyhtymä ei ole lain mukaan oikeushenkilö, jolloin se ei itse omista mitään eikä se voi olla osapuolena oikeustoimissa. Sitä ei myöskään listata kaupparekisteriin vaan verottajan perustietoihin. Elinkeinoyhtymät näkyvät kuitenkin Yritys- ja yhteisötietojärjestelmässä. Elinkeinoyhtymän yhtiömiehinä toimivat luonnolliset henkilöt tai yritykset ja näihin liittyvät muutokset täytyy ilmoittaa verottajalle.

Jatkumon seuraavassa vaiheessa tulevat henkilöyhtiöt, kuten esimerkiksi avoin yhtiö, joka muistuttaa paljon elinkeinoyhtymää. Henkilöyhtiöissä yhtiömiehillä on rajaton vastuu, mutta elinkeinoyhtymästä poiketen se on oikeushenkilö, jolloin se voi omistaa, olla mukana sopimuksissa ja osapuolena oikeustoimissa. Henkilöyhtiöissä laki edellyttää jo määrämuotoisia sopimuksia, minkä vuoksi sen digitalisointi lohkoketjuun on vaikeampaa. Tällaisia asioita ovat esimerkiksi ilmoitukset yhtiömiehen muutoksista, jotka täytyy tehdä kaupparekisteriin.

Jatkumossa seuraavana tulee kommandiittiyhtiö, joka on oikeushenkilö ja jossa on 2 erilaista yhtiömiestyyppiä. Siinä vähintään yhdellä yhtiömiehellä on rajaton vastuu. Kommandiittiyhtiössä yhtiösopimus on määrämuotoinen, joten yhtiömiehet täytyy ilmoittaa tietyllä tavalla. Seuraavaksi jatkumossa tulevat osakaskunnat, kuten yhteismetsät ja kalastusosakaskunnat, jotka ovat oikeushenkilöitä. Niissä yksittäisillä osakkailla ei ole vastuuta osakaskunnan velvoitteista. Yhteismetsillä ei ole määrämuotoisia sopimuksia.

Jatkumossa seuraavana on osakeyhtiö, joka on oikeushenkilö ja osakkaiden vastuu rajoittuu siinä sijoittamaansa pääomaan. Osakeyhtiössä osakasluettelolle ei ole määrämuotoa. Jatkumon viimeisenä tulee osuuskunta. Siinä rekistereille ei

ole määrämuotoa. Toisaalta osuuskuntalaki sisältää kaikki osakeyhtiölain säädökset, mikä mahdollistaa sen, että osuuskunta voi osakeyhtiön tavoin laskea liikkeelle osakkeita, joita voivat omistaa muutkin kuin osuuksien haltijat. Osuuskuntien monipuolisuus on tokenmuotoistamisen kannalta hyvä asia.

"*Ja osuuskunnassa on se kiva, että siinäkään ei ole rekistereille mitään määrämuotoa. Ja sitten niin kuin sanoin äsken, niin osuuskunnassa on myös pervoa se, että siihen on upotettu kaikki osakeyhtiölain säädökset, eli sulla voi olla myös osakkaita, osakkeellisia osakkaita, joiden ei tarvi välttämättä olla osuuksien haltijoita ja sulla voi olla sitten niille annettu erikseen osinkoja ja osakkeita, kaikkea tällaista. Eli sen takia mää pitäydyn siinä muutaman vuoden takaisessa kannassani, että Suomessa osuuskunnassa voisi olla suurimmat mahdollisuudet tokenisointiin, että se on niin kuin tokenisoinnin kannalta mielenkiintoisin, sen takia että siinä on aika paljon askarreltavuutta.*" *(Haastattelu 1)*

Taulukko 4 Yhtiömuotojen erot digitalisoinnin kannalta. (Haastattelu 1)

Yhtiömuoto	***Omistajien ja oikeussubjektien velvoitteet ja oikeudet***	***Lain määräämä määrämuotoisuus sopimuksissa***
Elinkeinoyhtymä	*Ei ole oikeushenkilö, eikä voi omistaa tai olla osapuolena oikeustoimissa. Sopimusosapuolina ovat luonnolliset henkilöt tai oikeushenkilöt.*	*Sopimus ilman määrämuotoisuutta*
Henkilöyhtiöt	*Yhtiömiehillä on rajaton vastuu. On oikeushenkilö*	*Laki edellyttää määrämuotoisia sopimuksia*
Kommandiittiyhtiö	*On oikeushenkilö. Vähintään yhdellä yhtiömiehellä on rajaton vastuu. Äänettömillä yhtiömiehillä vastuut rajoittuvat sijoitettuun pääomaan*	*Yhtiösopimus on määrämuotoinen*
Osakaskunnat, kuten yhteismetsät ja kalastusosakaskunnat	*On oikeushenkilö. Omistajat ovat vastuussa vain sijoittamastaan pääomasta*	*Ei määrämuotoisia sopimuksia*
Osakeyhtiöt	*On oikeushenkilö. Omistajat ovat vastuussa sijoittamastaan pääomasta.*	*Osakasluettelo ei ole määrämuotoinen.*
Osuuskunnat	*On oikeushenkilö. Omistajat ovat vastuussa sijoittamastaan pääomasta.*	*Osakasluettelo ja jäsenluettelo eivät ole määrämuotoisia*

Jos osakkeiden digitalisointi toteutetaan Jupiter-mallin mukaisesti, niin liiketoimintalogiikka on sama kuin paperipohjaisessa omistuksenhallinnassa eli kauppaprosessit ja sopimusten sisällöt ovat samanlaisia. Trust-over-IP-protokolla ja sen päälle rakennettu vahvistetun datan verkko mahdollistavat sen, että kaikki mitä voi tehdä paperilla, voidaan tehdä kitkattomasti digitaalisesti. Toisin

sanoen myös muut yhtiömuodot voidaan digitalisoida, mutta lait, jotka pitää ohjelmoida hajautettuihin sopimuksiin ovat hieman erilaisia. (Haastattelu 4)

" Jos puhutaan tällaisesta mallista, joka meidän mielestä on hyvä, eli tällainen Jupiter-malli, jätetään ne Ethereumit sun muut pois, niin tässä maailmassa, tässähän oikeasti liiketoimintalogiikan näkökulmasta palataan takaisin aikaan ennen tietokoneita, eli ne kauppaprosessit ja sopimusten sisällöt, mitä tässä tehdään, ne ovat ihan samanlaisia, kuin ennen vanhaan oli paperipohjaisissa jutuissa. Nyt kun täällä on tämä trust over ip protokolla ja sen päällä tämä verifiable data -verkko, niin se mitä se aiheuttaa on se, että se mitä ennen tehtiin paperilla, niin täsmälleen sama asia pystytään nykyisin tekemään ilman paperia kitkattomasti." (Haastattelu 4)

Se, että Jupiter mallissa voi luoda uuden yrityksen viidessä minuutissa ja alkaa käymään sen osakkeilla välittömästi kauppaa, saattaa poistaa yrityksiltä tarpeen muuttua julkisiksi, koska ne ovat julkisia tavallaan jo syntyhetkellään. Myöskään pörssiin listautumista ei tarvita, koska Jupiter-mallissa mitään pörssiä ei ole, vaan osakkeilla käydään kauppaa osakekauppaverkossa, johon on pääsy yrityksen omilta internetsivuilta. Tämän myötä yrityksiltä poistuisi tiedotusynnä muita velvoitteita, jotka julkisilla osakeyhtiöillä nykyään on. (Haastattelu 4)

6.5 Lohkoketjuteknologian ongelmat

Aineistosta löytyi useita lohkoketjuteknologian ongelma-alueita, joista osa liittyy ihmisten tietämykseen, asenteisiin ja intentioihin mutta useimmat itse teknologiaan. Tässä luvussa tarkastellaan aluksi ensimmäistä kategoriaa ja lopuksi teknologiaan liittyviä ongelmia.

Haastattelu aineistosta löytyi muutamia tietämykseen, asenteisiin ja intentioihin liittyvää ongelma-aluetta, jotka vaikeuttavat kaikkien tarvittavien osapuolten saamista lohkoketjuteknologian käyttöönoton kannalle. (Haastattelu 3) Yrityksissä ja ihmisillä on tiedon puutetta lohkoketjuteknologiasta, johon liittyy ongelmallisia asenteita ja väärin ymmärtämistä. (Haastattelu 1; Haastattelu 2) Lohkoketjuteknologia on myös heikosti yhteensopiva lainsäädännön kanssa. (Haastattelu 4) Lainsäädännön ongelmia käsitellään tarkemmin luvussa 6.3. Ongelma, mikä yleensäkin liittyy uuden teknologian käyttöönottoon, on muutosvastarinta. (Haastattelu 3) Joillekin tahoille uusi teknologia on kilpailija, jolloin heillä ei ole motivaatiota edistää sitä, vaikka se olisi parempi teknologia kuin käytössä oleva. (Haastattelu 5)

Lohkoketjuteknologiaan itseensäkin liittyy paljon ongelmia. Sen kehitys ei ole vielä kovin pitkällä, ja siihen liittyy epävarmuutta ja riskejä. (Haastattelu 2; Haastattelu 4) Yrityksille voi olla vaikea perustella julkisen lohkoketjun käyttöä, koska sitä ei voi kontrolloida. (Haastattelu 3) Voi tulla tilanteita, joissa julkinen lohkoketjuverkko kaatuu, eikä kukaan vastaa siitä, koska kukaan ei omista sitä. Tällaista ongelmaa ei kuitenkaan tule yksityisessä Corda-verkossa. (Haastattelu 4)

Lohkoketjuteknologiaan pohjautuva rahoitusmaailma poikkeaa perinteisestä arvo-osuuksiin pohjautuvasta rahoitusmaailmasta niin paljon, ettei

entisestä voida säilyttää mitään, vaan teknologiat vaihtuvat täysin, samoin kuin liiketoimintamallit, ansaintamallit ja kannustinjärjestelmät. (Haastattelu 4) Toisaalta maailmassa on niin valtava määrä erilaisia arvo-osuuksia, että niiden vieminen uuden teknologian päälle on valtavan suuri hanke. Sen vuoksi se ei voi tapahtua nopeasti. (Haastattelu 3)

Tunnettuja ongelmia, jotka nousivat esiin myös kirjallisuuskatsauksessa ovat transaktioiden peruuttamattomuus, joka tekee virheellisten transaktioiden korjaamisen mahdottomaksi (Haastattelu 1), standardien puute ja skaalautuvuusongelma, joka koskee ainakin julkisia lohkoketjuja. Yksi haastateltavista oli sitä mieltä, että tietojen tallentaminen peräkkäisiin lohkoihin, jotka viittaavat toisiinsa ei ole hyvä tapa tallentaa tietoa ja hän piti myös konsensusalgoritmeja huonoina algoritmeina. (Haastattelu 4)

6.6 Lohkoketjuteknologian edut

Aineistosta löytyi useita lohkoketjuteknologian vahvuusalueita, joita tässä luvussa käydään läpi. Osa vahvuusalueista liittyi selkeästi juuri osakkeiden digitalisointiin ja muut lohkoketjuteknologian käyttöön yleisemmin.

Lohkoketjuteknologia voisi mullistaa osakemarkkinoiden rakenteen, koska pörssit säilytyspalvelut sekä selvitys- ja määrityspalvelut muuttuisivat ennen pitkää tarpeettomiksi, kun lohkoketjuteknologia tai Jupiter-mallinen osakekauppaverkko otetaan käyttöön. (Haastattelu 4) Lohkoketju tarjoaa osakasluettelon ylläpitoon yhden korruptoimattoman lähteen, josta pseudonyymisesti selviää, mitä osakkeita missäkin lompakossa on. (Haastattelu 1) Mikään yksittäinen taho ei hallitse lohkoketjuja ja älysopimuksia, jolloin mikään yritys ei voi mielivaltaisesti ottaa osakkeita yksiltä ja antaa toisille. (Haastattelu 1)

Lohkoketjuteknologia parantaisi osakkeiden siirreltävyyttä maasta toiseen, koska se ei ole samalla tavalla siiloutunut kuin eri maiden arvo-osuusjärjestelmät, vaan kaikilla olisi sama teknologia käytössä. Kaikilla olisi sama lähes reaaliaikainen ja ajantasainen informaatio osakkeista. Infrastruktuurin rakentaminen lohkoketjun päälle olisi helppoa, jos lainsäädäntö eri maissa saataisiin suunnilleen yhteneväiseksi. (Haastattelu 5)

Osakkeiden säilytyksen siirtäminen arvo-osuusjärjestelmästä lohkoketjuun voisi luoda kustannustehokkaamman mallin osakeomistusten siirtelyyn, kaupankäyntiin ja muuhun tähän liittyvään. Lohkoketjuteknologiaan perustuvassa omistuksen hallinnassa on rajapinnat valmiina ja lohkoketju tarjoaa koko ajan ajantasaisen tiedon omistuksista. (Haastattelu 3) Lohkoketjuteknologiaan pohjautuvilla osakkeiden digitalisointialustoilla voitaisiin helpottaa pienten ja keskisuurten yritysten rahoitusta kuten esimerkiksi kansainvälisiä osakeanteja, jotka nykyisellään ovat vaikeita toteuttaa. (Haastattelu 2; Haastattelu 5)

" ...jos ne (keskisuuret yritykset) tekee kansainvälisiä osakeanteja, niin siihen liittyy todella paljon hankaluutta jo ihan siihen rahojen siirtelyyn ja näin päin pois ja sitä lähdettiin siinä niin kuin parantamaan siinä stoxi-firmassa (Stoxchange)." (Haastattelu 2)

Lohkoketjuteknologia on yleiskäyttöinen teknologia, mikä tuli esiin jossain määrin myös haastatteluaineistossa. Se mahdollistaa globaalin yhteistyön, kaupankäynnin ja yrittämisen yhteisillä pysyvillä ehdoilla, jotka on ohjelmoitu älykkääseen sopimukseen. (Haastattelu 1) Ethereum-verkossa voidaan rakentaa hyvin monenlaista liiketoimintalogiikkaa, siirtämään arvoa, käyttämään kryptovaluuttaa maksamiseen ja tekemään kauppaprosesseja ja älykkäitä sopimuksia tuntemattomien ja toisistaan tietämättömien osapuolten välillä. (Haastattelu 4)

Lohkoketjuteknologian etu on siinä, että sen avulla voidaan tehdä monen keskistä digitaalista sopimista hyvin helposti verrattuna vanhoihin teknologioihin. Kaikki kauppatapahtumat, myös yksinkertaiset, ovat monenkeskistä sopimista. Jos ostaa vaikkapa maitopurkin kaupasta, siinä on kolme osapuolta: ostaja, myyjä ja verottaja, koska verottaja ottaa siitä arvonlisäveron. (Haastattelu 4) Lohkoketjuteknologia ratkaisee omistajuuden ongelman, koska lohkoketjuissa on sisäänrakennettu omistajuuden käsite, mikä perustuu siihen, että se taho joka tokenia hallinnoi myös omistaa sen, eikä omistuksen todentamiseen tarvita keskitettyä tietokantaa. (Haastattelu 2)

6.7 Arvo-osuusjärjestelmän ongelmat

Haastateltavien vastauksissa arvopaperikeskuksista löytyi 4 ongelma-aluetta, jotka kuitenkaan eivät olleet vastauksissa selkeästi rajattavissa, koska ne liittyvät toisiinsa: (1) Vanhentunut teknologia, (2) Jokainen arvopaperikeskus muodostaa oman siilon, (3) määräävä markkina-asema, (4) monimutkaisuus ja hallinnollinen raskaus.

Nykyiset arvo-osuusjärjestelmät ovat tilkkutäkki erilaisia vanhalla teknologialla toteutettuja järjestelmiä, minkä vuoksi nykyinen järjestelmä ei ole nopea, eikä tehokas. (Haastattelu 3) Arvo-paperikauppojen selvitys on hidasta ja osakkeiden osalta se on T+2 eli kaupanteon jälkeen menee 2 päivää kaupan selvittämiseen, koska kauppojen selvitykset, täsmäyttäminen ja maksuliikenne suoritetaan eri järjestelmissä. Arvo-osuusjärjestelmissä hidas infrastruktuuri aiheuttaa paljon kustannuksia. (Haastattelu 3) Nykyinen infrastruktuuri on pitkän kehityksen tulos ja uuden teknologian omaksuminen ja vanhan poisoppiminen ottaa aikansa. (Haastattelu 3)

Jokainen arvopaperikeskus on teknisesti erilainen, mikä johtuu maiden erilaisista lainsäädännöistä, ja ne muodostavat siilon. Euroopassa jokaisessa maassa on oma arvopaperikeskus, mutta Yhdysvalloissa on vain yksi. Suomessa on täysin erilainen järjestelmä kuin missään muussa Euroopan maassa, vaikka monissa maissa arvopaperikeskukset omistaa sama yritys, Euroclear. (Haastattelu 5) Eri maiden arvo-osuusjärjestelmien yhteen toimiminen on hyvin ongelmallista ja erittäin vaikea tekninen ongelma, jota kukaan ei halua ratkaista. (Haastattelu 2)

Arvo-osuusjärjestelmät ovat lähes määräävässä markkina-asemassa omilla alueillaan. (Haastattelu 5) Arvo-paperikeskustoiminta, mikä tarkoittaa arvo-osuustilien tarjoamista, on vahvasti säänneltyä Euroopassa ja arvopaperikeskusten tarjoamat arvo-osuudet ovat käytännössä ainut tapa, jolla osakkeita voi tällä

hetkellä digitalisoida lainsäädännön puitteissa, mikä on merkittävin jarruttava tekijä lohkoketjuteknologian käyttöönotolle. Näin siitä huolimatta, että lohkoketjuteknologia sopisi digitalisointiin paremmin, koska sen päälle rakennettuna osakkeiden säilytys voitaisiin toteuttaa tehokkaammin ja hajautetusti, jolloin olisi useampia osapuolia, jotka ylläpitäisivät omistajarekisteriä. (Haastattelu 3)

Nykyinen arvopaperimarkkinainfrastruktuuri on erittäin monimutkainen ja hallinnollisesti raskas, eikä sitä voi enää kehittää edelleen, koska jos siihen yrittää tehdä uusia ominaisuuksia, niin se tulee hyvin kalliiksi hyötyihin suhteutettuna. Arvo-osuusjärjestelmä on vain yksi osa arvopaperimarkkinainfrastruktuuria, joka vastaa arvopapereiden säilytyksestä. Nykyiseen infrastruktuuriin ei voi tehdä järjestelmää, jossa osakeyhtiön perustaminen onnistuisi 5 minuutissa, minkä jälkeen osakkeilla voisi käydä välittömästi kauppaa. Osakkeiden digitalisointi onnistuu nykyisessäkin infrastruktuurissa, mutta yhtiön osakkeiden siirtäminen arvo-osuusjärjestelmään kestää viikkoja tai kuukausia ja on kallista. (Haastattelu 4)

6.8 Digitaalisten osakkeiden tulevaisuus

Haastatteluissa nousi esiin, että digitaalisten osakkeiden tulevaisuus riippuu lainsäädännön ja teknologian kehittymisestä. Lohkoketjuteknologian päälle voidaan tehdä osakkeita ja muitakin omaisuusluokkia, kunhan teknologia saadaan valmiiksi. Myös lohkoketjuteknologiaa koskeva lainsäädäntö on menossa eteenpäin. Tällä hetkellä eletään jonkinlaista käymisvaihetta, mutta seuraavan vuosikymmenen aikana digitalisointi tulee kuitenkin tapahtumaan jollakin tavalla, ja tämä tapahtuu jossakin vaiheessa myös globaalisti, ei pelkästään Euroopassa. (Haastattelu 3.)

Heti, kun sääntely saadaan selkeäksi EU:n alueella muutenkin kuin stablecoinien osalta, niin osakkeiden digitalisointi kiihtyy ja siirtyy valtavirtaan, koska digitalisoinnista on huomattavia etuja. Todennäköisesti se ei kuitenkaan tule tapahtumaan avoimissa lohkoketjuissa, vaikka sama sääntely saataisiin koskemaan koko EU:ta. (Haastattelu 5)

6.8.1 Trust-over-ip-protokollaan pohjautuva identiteettiverkko ja erilliset transaktioidenhallintapalvelut haastavat lohkoketjuihin nojaavan hajautetun finanssimaailman

Osakkeiden digitalisointi ei välttämättä perustu tulevaisuudessa perinteiseen lohkoketjuteknologiaan, jossa käytetään lohkoketjuja ja tokeneita, kuten Ethereumiin. 2 haastateltavista toi esiin Corda-teknologian potentiaalisempana vaihtoehtona. (Haastattelu 4; Haastattelu 5) Toinen heistä näki Corda-teknologian kanssa yhteensopivalla trust-over-ip-protokollaan pohjautuvalla identiteettiverkolla tulevaisuudessa merkittävän roolin. Identiteettien digitalisointi edistyy erityisesti Euroopassa. EU on ilmoittanut, että EU:n alueelle pitää tulla kansalliset

identiteettiverkot seuraavan kolmen vuoden aikana, mutta siihen saattaa mennä pidempäänkin. Digitaalinen identiteetinhallinta on siis menossa samaan suuntaan, kuin Jupiter-mallisessa osakekauppaverkossa. Tämä tulee mahdollistamaan hajautetun digitaalisen sopimisen ja sitä kautta paremmat verkot kaikenlaiseen kaupankäyntiin, ei pelkästään osakkeilla käytävään kauppaan. Esimerkiksi se voisi mahdollistaa sen, että jos yritys pystyy laskemaan liikkeelle osakkeita, joilla voisi käydä kauppaa viiden minuutin kuluttua, se voisi samalla laskea liikkeelle myös joukkovelkakirjoja, joilla käytäisiin kauppaa hieman erilaisessa verkossa hieman erilaisella logiikalla. (Haastattelu 4)

Kaikenlaisten kaupankäyntiverkostojen kehitys seuraavan viiden vuoden aikana tulee olemaan merkittävää. Nykyiset lohkoketjupohjaiset kaupankäyntiverkostot saattavat kuitenkin olla historiaa jo viiden vuoden päästä, koska niissä osapuolet eivät tunne toisiaan, mikä vaikeuttaa hajautettua sopimista.

" Ja sitten nämä lohkoketjupohjaiset, eli nämä decentralized finance, niin minä en usko, että niitä on enää viiden vuoden päästä, koska siellä ei se hajautettu sopiminen, käytännössä, kun se vaatii sen, että ne osapuolet tuntevat toisensa, muuten se sopimus ei ole laillinen, laillisesti pitävä, niin se hajautettu sopiminen siinä maailmassa, sitä ei vain saada toimimaan." (Haastattelu 4)

Monimutkaisten monenkeskisten sopimusten, joita liittyy esimerkiksi osakkeisiin, velkakirjakauppaan ja vakuutustransaktioihin, toteuttaminen tulee sujumaan helposti, kunhan perusinfrastruktuuri saadaan kuntoon, jossa trust-over-ip-protokollaan pohjautuva digitaalinen luottamus voidaan toteuttaa. Sen päälle voidaan sitten rakentaa identiteettiverkko, jossa kulkee luotettavaa dataa ja identiteettiverkon päälle sitten voidaan rakentaa liiketoimintaverkkoja, joiden varaan taas voidaan rakentaa kaikenlaisia kaupankäynti- rahoitus- ynnä muita palveluita. (Haastattelu 4)

" Eli kun saadaan tämä digitaalisen luottamuksen pohja kuntoon, elikkä sen pohjalla on tällainen yhteinen protokolla trust over ip. Tämän päälle voidaan sitten rakentaa identiteettiverkko, jossa sitten kulkee tällaista luotettavaa dataa. Sen päälle pystytään tekemään businessverkkoja ja businessverkkoihin näitä kaikenlaisia kaupankäynti ja rahoitus- ym. palveluita ja erityisesti kaupankäynnin rahoituspalveluita eli tämä on tämä juttu, jonka tämä ns. lohkoketjuteknologia ratkaisee, tosin siinä vaiheessa, kun se on ratkaistu, siellä ei todennäköisesti ole sitä lohkoketjua mutta vähän fiksumpi ratkaisu."

Vaikka kehitys Ethereum-alustan ympärillä on nopeaa, niin suunta on väärä, koska se ei tarjoa tunnettuja osapuolia eikä niiden välittämiä luotettavia faktoja. Voi olla ylitsepääsemätön haaste saada Ethereum-alustaan kaikki tarvittavat ominaisuudet, jotta se olisi skaalautuva ja lainsäädännön kanssa yhteensopiva. (Haastattelu 4) Lohkoketjuvaihe on prototyyppivaihe, jonka aikana kehitetään erilaisia liiketoimintalogiikoita, mutta sen jälkeen hajautettuun maailmaan rakennetaan identiteettiverkot ja erilliset transaktioidenhallintapalvelut, joiden avulla liiketoimintalogiikat saadaan toimimaan skaalautuvasti ja lainmukaisesti, mikä tarkoittaa sitä, että ne täytyy toteuttaa tämän uuden alustan päälle, jotta niistä tulee toimivia.

"*Lohkoketjuteknologia sai ihmiset ajattelemaan, että tällaisten juttujen tekeminen on mahdollista ja nyt sitten kun päästään siitä eroon ja rakennetaan identiteettiverkot ja tällaiset transaktionhallintapalvelut sinne hajautettuun maailmaan uudestaan tällä*

tavalla niin kuin erillisinä toisiinsa yhteen liittyvinä ratkaisuina, niin täällä sitten päästään tekemään niitä asioita oikeasti. Eli näin ehkä sanoisin, että yhdellä teknologialla tehtiin paljon prototyyppejä ja toisella tehdään rewriting, jolloin näistä prototyypeistä saadaan kunnolliset implementaatiot. " (Haastattelu 4)

6.8.2 Lohkoketjuteknologia on arvo-osuusjärjestelmän kilpailija ja voi korvata sen

Lohkoketjuteknologia on pitkällä aikavälillä arvo-osuusjärjestelmän kilpailija ja noin 10 vuodessa se syrjäyttää arvo-osuusjärjestelmän kokonaan. (Haastattelu 3; Haastattelu 4) Arvo-osuusjärjestelmä ja lohkoketjuteknologia tulevat elämään jonkin aikaa rinnakkain osakkeiden digitalisoinnissa. (Haastattelu 3) Lohkoketjuteknologia, mukaan lukien Jupiter-mallinen osakekauppaverkko, ei tarvitse arvo-osuusjärjestelmää mutta voi korvata sen. (Haastattelu 4; Haastattelu 5) Lisäksi ne voivat tehdä pörssit ja selvityspalvelut tarpeettomiksi. (Haastattelu 4)

" Niin kuin kerroin niin, tämä minun suosikkitapa kuvata tällaista hajautettua osakekaupankäyntiverkkoa on että, siinä ei ole pörssiä, siinä ei ole kauppapaikkaa, siinä ei ole säilytyspalvelua, eikä siinä ole clearingpalvelua ja säilytyspalveluhan on sama kuin arvo-osuusjärjestelmä. Eli totta kai se silloin sen kilpailija on, jos sen koko homman voi tehdä ilman sitä."

Arvo-osuusjärjestelmän korvaajaksi otetaan luultavasti suurten toimijoiden, kuten esimerkiksi R3, kehittämä suljettu lohkoketjuverkko, joka syrjäyttää eri maiden siiloutuneet arvo-osuusjärjestelmät. Tällä hetkellä pankit käyttävät jonkin verran lohkoketjuteknologiaa back-office-toiminnoissaan, mutta se ei ole valtavirtaa. Kaikki suuret toimijat tulevat todennäköisesti käyttämään yhtä suljettua lohkoketjua, mihin siirtyy kaikki nykyisissä arvo-osuusjärjestelmissä olevat omistukset, joko maailmanlaajuisesti tai sitten esimerkiksi EU:n ja USA:n kaltaisilla maantieteellisillä alueilla. (Haastattelu 5)

7 TULOSTEN TULKINTA JA POHDINTA

Tässä luvussa tutkimuksen tuloksia verrataan kirjallisuuskatsauksen tuloksiin ja muuhun kirjallisuuteen, joiden avulla muodostetaan johtopäätöksiä siitä, mikä on tulosten merkitys tutkimuskysymysten kannalta. Alaluvussa 7.1 vastataan tutkimuskysymykseen 1: Miten lohkoketjuteknologiaa käytetään osakkeiden digitalisoinnissa? Alaluvuissa 7.2 ja 7.3 vastataan tutkimuskysymykseen 2: Mitkä ovat lohkoketjuteknologian positiiviset ja negatiiviset vaikutukset osakkeita digitalisoitaessa? Luku 7.2 keskittyy positiivisiin vaikutuksiin ja luku 7.3 negatiivisiin vaikutuksiin.

Kirjallisuuskatsauksessa osakkeiden digitalisointi tarkoitti lähinnä osakkeiden toteuttamista osakemuotoisina tokeneina tai arvo-osuusjärjestelmän käyttöä, mutta haastatteluaineistossa näille löytyi vaihtoehdoksi osakkeen toteuttaminen verifiable-claim-muodossa vahvistetun datan verkossa. Vahvistetun datan verkko on Suomessa kehitettyä teknologiaa, jota ei ole tutkittu tähän mennessä juuri lainkaan, joten tämä tutkimus on yksi harvoista, jossa aihetta käsitellään. Aihe kuitenkin kaipaa runsaasti lisätutkimusta, jos todella pitää paikkansa, että vahvistetun datan-verkko haastaa lohkoketjuihin pohjautuvan hajautetun rahoitusmaailman, jossa keskiössä ovat erilaiset lohkoketjuihin talletettavat tokenit.

Tutkimuksia, joissa käsiteltäisiin erilaisia vaihtoehtoisia teknologioita osakkeiden digitalisointiin, on tehty hyvin vähän, eikä tätä aihetta siksi käsitellä tämän tutkimuksen kirjallisuuskatsauksessa muuten kuin arvo-osuusjärjestelmien ja lohkoketjuteknologian osalta. Empiirisessä osuudessa arvo-osuusjärjestelmää käsitellään lähinnä kriittisestä näkökulmasta. Arvo-osuusjärjestelmän vahvuuksia verrattuna lohkoketjuteknologiaan ei juurikaan käsitellä, eikä niitä haastatteluissa edes kysytty.

Tässä tutkimuksessa käsitellään tarkemmin vain kahta lohkoketjuteknologiaan pohjautuvaa älysopimusalustaa, mikä johtuu siitä, että kirjallisuudessa korostuu Ethereum-älysopimukset ja toisaalta haastatteluaineistossa esiin tulleista alustoista lähinnä vahvistetun datan verkko otettiin tarkempaan analyysiin. Tutkimustulokset ovat lähinnä alustavia, joten aihetta tulisi tutkia enemmän, jotta saavutettaisiin parempi reliabiliteetti, validiteetti ja käsitys aiheen tieteellisestä merkittävyydestä.

Lohkoketjuteknologiaa on tutkittu verrattain vähän ja tutkimusala on uusi. Harvoista lohkoketjuteknologiaan liittyvistä aihepiireistä on tehty useita tutkimuksia, mikä vaikeuttaa lähteiden luotettavuuden arviointia ja teoreettista tutkimusta sekä vähentää lähteiden vuoropuhelua. Myös lohkoketjuteknologian käsitteelliset viitekehykset ovat puutteellisia ja tutkimuksissa käytetään paljon vertaisarvioimattomia lähteitä, kuten yritysten nettisivuilta löytyviä dokumentteja ja alan ammattilaisten kirjoittamia artikkeleita. Käsitteiden epäselvyys vaikeuttaa kokonaisuuksien hahmottamista ja tietojen löytämistä.

Haastattelututkimuksessa haastateltavien asiantuntemuksen etukäteisarviointi oli vaikeaa, minkä vuoksi haastateltavia ei ennakolta karsittu, vaan asiantuntemusta arvioitiin haastatteluissa annettujen vastausten perusteella. Haastatteluissa monet kysymyksistä käsittelivät lainsäädäntöä, mutta kukaan haastateltavista ei ollut oikeustieteilijä. Tämä näkyy muun muassa epämääräisenä käsitteistönä joidenkin haastateltavien vastauksissa. Haastateltavien käsityksissä oli myös ristiriitaisuutta. Kukaan haastateltavista ei myöskään ole saanut lohkoketjuteknologiaan liittyvää koulutusta, vaan asiantuntemus on hankittu työn kautta tai omatoimisesti. Tutkimuksen otos oli verrattain pieni, 5 haastateltavaa, minkä vuoksi kovin merkittävää saturaatiota ei syntynyt. Sen vuoksi tutkimuksen tulokset eivät ole kovin yleistettäviä.

7.1 Lohkoketjuteknologian kehitys osakkeiden digitalisoinnin kannalta

Osakkeiden digitalisointi on mahdollista monilla eri lohkoketjualustoilla, mutta Ethereumin julkistamisen jälkeen osakkeiden digitalisoinnissa on alettu hyödyntämään erityisesti Ethereum-älysopimuksia ja ERC20-tokenstandardia. (Haastattelu 1; Howell ym., 2020) Lohkoketjuteknologialla toteutetut osakkeet ovat yleensä security-tokeneita, eli ne ovat tokeneilla toteutettuja arvopapereita. Myös muita arvopapereita voidaan toteuttaa samalla tavalla. (Haastattelu 3) Osakkeiden digitalisoinnissa voidaan käyttää julkista lohkoketjua, kuten Ethereum tai yksityistä lohkoketjua. (Haastattelu 3, Haastattelu 5) Yritysten välisissä hankkeissa käytetään yleensä yksityisiä lohkoketjuja, koska julkisia lohkoketjuja on mahdotonta kontrolloida. (Haastattelu 3)

Osakkeita voi digitalisoida myös verifiable-claim-muodossa Corda-verkossa, jolloin ei siis käytetä tokeneita. Corda on erityisesti rahoitusmarkkinoille suunniteltu teknologia. (Marsh & Dewey, 2019) Tällaisessa tavassa digitalisoida on pohjalla trust-over-ip-protokolla, jonka päälle on rakennettu vahvistetun datan verkko. Tällaista teknologiaa kehittää suomalainen Findynet Osuuskunta. (Haastattelu 4)

Tutkimustulokset toivat uutta tietoa siitä, miten lohkoketjuteknologia on kehittynyt osakkeiden digitalisoinnin kannalta. Tällaisesta tiedosta voi olla hyötyä, kun arvioidaan uusien teknologioiden soveltuvuutta osakkeiden digitalisointiin pidemmällä aikavälillä. Esimerkiksi se, että Colored Coins -konsepti jäi

lyhytaikaiseksi suurista odotuksista huolimatta, muistuttaa siitä, että uudet tekniset konseptit eivät välttämättä vastaa niille asetettuja odotuksia ja jokin uusi kehittyneempi teknologinen konsepti voi korvata ne hyvinkin nopeasti.

Lohkoketjuteknologian kehitys on hyvin nopeaa, minkä vuoksi sitä koskeva tutkimustieto ja teknologiat saattavat vanhentua nopeasti. Esimerkiksi Colored Coins konsepti on jo käytännössä unohdettu, vaikka siitä kirjoitettiin lohkoketjuteknologiaa käsittelevässä kirjallisuudessa vielä 2018 melko paljon. Sen ovat korvanneet muut kehittyneemmät älysopimus- ja tokenalustat. Tämä tutkimus antaa viitteitä siitä, että uudempienkin alustojen kohtalo voi muistuttaa ennen pitkää Colored Coins -konseptin kohtaloa, kun esimerkiksi vahvistetun datan verkko tai jokin muu teknologia korvaa ne. Tulevaisuuden ennustaminen on kuitenkin vaikeaa.

7.2 Lohkoketjuteknologian tuomat mahdollisuudet

Lohkoketjuteknologia tarjoaa monia teknisiä etuja aiempiin teknologioihin verrattuna. Tässä alaluvussa käsitellään näitä ominaisuuksia.

Lohkoketjuteknologian avulla olisi mahdollista vähentää kompleksisuutta erityisesti monenkeskisissä ja rajat ylittävissä transaktioissa. (Mills ym., 2016) Jos osakkeiden säilytys saataisiin siirrettyä yhteen lohkoketjuun useiden arvopaperikeskusten sijasta, päästäisiin eroon arvopaperikeskusten muodostamista siiloista, koska kaikilla olisi sama teknologia käytössä. (Haastattelu 5) Infrastruktuurin rakentaminen lohkoketjun päälle olisi helppoa ja osaketransaktiot maasta toiseen olisivat huomattavasti nykyistä helpompia. Kaikilla olisi sama lähes reaaliaikainen ja ajantasainen informaatio osakkeista. (Haastattelu 5) Pienten ja keskisuurten yritysten rahoituksen saatavuus parantuisi samalla, koska kansainväliset osakeannit olisi helpompi toteuttaa. (Haastattelu 2; Haastattelu 5; Mills ym. 2016)

Lohkoketjuteknologialla voitaisiin huomattavasti parantaa osaketransaktioiden end-to-end-prosessointinopeutta. Nykyisissä arvo-osuuksilla toteutettavissa osaketransaktioissa selvityssykli on T+2 eli osakekaupan jälkeen menee 2 pankkipäivää ennen kuin transaktio kirjataan arvo-osuustilille. (Nordnet, 2021; Kaal & Evans, 2019) Lohkoketjuteknologialla selvitys voitaisiin hoitaa sekunneissa sen sijaan, että siihen kuluu useita vuorokausia. (Haastattelu 3: Haastattelu 5; Kaal & Evans, 2019)

Lohkoketjuteknologia mahdollistaa globaalin yhteistyön, kaupankäynnin ja yrittämisen yhteisillä pysyvillä ehdoilla, jotka on ohjelmoitu älykkääseen sopimukseen. (Haastattelu 1) Sen avulla voidaan tehdä monen keskistä digitaalista sopimista hyvin helposti verrattuna vanhoihin teknologioihin. Kaikki kauppatapahtumat, myös yksinkertaiset, ovat monenkeskistä sopimista. Jos ostaa vaikkapa maitopurkin kaupasta, siinä on kolme osapuolta: ostaja, myyjä ja verottaja, koska verottaja ottaa siitä arvonlisäveron. (Haastattelu 4) Ethereum-verkossa voidaan rakentaa hyvin monenlaista liiketoimintalogiikkaa, siirtämään arvoa, käyttämään kryptovaluuttaa maksamiseen ja tekemään kauppaprosesseja ja

älykkäitä sopimuksia tuntemattomien ja toisistaan tietämättömien osapuolten välillä. (Haastattelu 4)

Lohkoketjuteknologia mahdollistaa digitaalisen omistamisen ja hajautetun digitaalisen sopimisen ilman keskitettyä tietokantaa perustuen siihen, että se taho, joka hallinnoi tokenia myös omistaa sen. (Haastattelu 2; Haastattelu 4) Hajautettu digitaalinen omistajuus ja sopiminen onnistuu myös ilman tokeneita vahvistetun datan verkossa. Hajautetun omistajuuden ja sopimisen ansiosta keskitettyihin tietokantoihin pohjautuvat palvelut, kuten pörssit, säilytyspalvelut sekä selvitys- ja määrityspalvelut, muuttuvat tarpeettomiksi, kun lohkoketjuteknologia tai Jupiter-mallinen osakekauppaverkko otetaan käyttöön. (Haastattelu 4) Kirjallisuuskatsauksessa esitettiin, että arvopaperikeskuksille voisi edelleen jäädä rooli kauppojen virallistajina lohkoketjuteknologian käyttöönoton jälkeen, mutta Jupiter-mallisessa osakekauppaverkossa näin ei ole, vaan virallistamisprosessi on Corda-transaktioverkon ominaisuus. (Benos ym., 2017) Osakekauppaverkossa onnistuu myös käteistilien käyttö ja osakkeiden luovutus maksua vastaan, minkä toteuttamista Benos ym. (2017) pitivät poissuljettuna hajautetussa finanssimaailmassa. (Haastattelu 4.) Toisaalta Feenanin ym. (2020) mukaan luovutus maksua vastaan voidaan toteuttaa myös älykkäällä sopimuksella tai jollain muulla gryptografisella teknologialla, joka siirtää maksun myyjälle vasta luovutuksen tapahtuessa.

Tutkimustuloksista voi löytää hyviä perusteluja lohkoketjuteknologian käytölle osakkeiden digitalisoinnissa. Tällaista tietoa tarvitaan, kun valitaan digitaalisissa sovelluksissa käytettäviä teknologioita. Jatkotutkimuksissa voisi esimerkiksi pohtia erilaisten lohkoketjualustojen soveltuvuutta osakkeiden digitalisointiin. Lisäksi voisi tutkia sitä, mitkä ovat merkittävimpiä tekijöitä lohkoketjualustojen verkostovaikutusten kannalta ja alustaprojektien kriittisiä menestystekijöitä. Mahdollisuus käyttää vahvistetun datan verkkoa digitalisessa sopimisessa saattaa olla tämän tutkimuksen merkittävin tulos, ja tätä aihetta olisi hyvä tutkia enemmänkin. Myöhemmässä tutkimuksessa voisi tutkia spesifimmin myös lohkoketjuteknologian käyttöä kansainvälisissä osakeanneissa.

7.3 Lohkoketjuteknologiaan liittyvät ongelmat

Lohkoketjuteknologiaan pohjautuva rahoitusmaailma poikkeaa perinteisestä arvo-osuuksiin pohjautuvasta rahoitusmaailmasta niin paljon, ettei entisestä voida säilyttää mitään, vaan teknologiat vaihtuvat täysin samoin kuin liiketoimintamallit, ansaintamallit ja kannustinjärjestelmät. (Haastattelu 4) Tämä ei kuitenkaan tapahdu ongelmitta.

Lohkoketjuteknologian haasteena rahoitusmarkkinoiden kannalta on tuoda markkinoille järjestelmiä, jotka noudattavat vaadittuja standardeja, kuten know-your-customers (KYC) -sääntöjä, ovat läpinäkyviä ja tilivelvollisia sääntelyn suhteen, kunnioittavat lakeja kaupankäyntistrategioissa ja joiden ylläpito on edullista. Monet lohkoketjuteknologiaan liittyvät ominaisuudet voivat olla

ongelmallisia, vaikka ne miellettäisiin hyödyllisiksi. (Pinna & Ruttenberg, 2016; Haastattelu 4)

Maailmassa on niin valtava määrä erilaisia arvo-osuuksia, että niiden vieminen uuden teknologian päälle on valtavan suuri hanke. Sen vuoksi se ei voi tapahtua nopeasti. (Haastattelu 3.) Myös kaikkien tarvittavien osapuolten saaminen lohkoketjuteknologian käyttöönoton kannalle on suuri haaste. (Haastattelu 3)

Hajautetun finanssimaailman sovelluksia vaivaa heikko yhteensopivuus lainsäädännön kanssa. (Haastattelu 4) Vaikka teknologinen kehitys on nopeaa, lainsäädännön kehitys on erittäin tärkeä edellytys tekniselle edistykselle, joten nämä eivät ole täysin toisistaan erillisiä kysymyksiä. Aiempi lainsäädäntö on laadittu pitkälti arvo-osuusjärjestelmän ehdoilla, minkä vuoksi se on pitänyt yllä arvo-osuusjärjestelmän määräävää markkina-asemaa osakkeiden digitalisoinnissa. Kun uutta lainsäädäntöä kehitetään, sitä ei välttämättä kannata tehdä vastaamaan tiukasti jonkin tietyn teknologian asettamia muotovaatimuksia, vaan se kannattaisi muotoilla mahdollisimman pelkistetysti toteuttamaan niitä vaatimuksia, joita varten se on olemassa. Tällöin uudet ja paremmat teknologiat voidaan ottaa käyttöön välittömästi odottamatta lakimuutoksia.

Ihmisillä on tiedon puutetta lohkoketjuteknologiasta, johon liittyy ongelmallisia asenteita ja väärin ymmärtämistä. (Haastattelu 1; Haastattelu 2) Ongelma, mikä yleensäkin liittyy uuden teknologian käyttöönottoon, on muutosvastarinta. (Haastattelu 3) Tällöin motiivit voivat olla taloudellisia, koska joillekin tahoille uusi teknologia on kilpailija, jolloin heillä ei ole motivaatiota edistää sitä, vaikka se olisi parempi teknologia kuin käytössä oleva. (Haastattelu 5)

Lohkoketjuteknologian kehitys ei ole vielä kovin pitkällä, ja siihen liittyy epävarmuutta ja riskejä. (Haastattelu 2; Haastattelu 4) Julkisten lohkoketjujen maailman laajuiset kaikille avoimet kopiot kirjanpidosta eivät ole täysin ongelmattomia, koska niissä transaktioiden yksityisyys voi vuotaa. (Pinna & Rutenberg, 2016; Li, Jiang, Chen, Luo & Wen, 2020) Identiteetinhallinnan pseudonyymisyys, mikä koskee myös Ethereum-verkkoa, on ongelmallista, koska identiteetinhallinnassa tulisi noudattaa know-your-customers (KYC) -sääntöjä, mikä tarkoittaa sitä, että älykkäissä sopimuksissa osapuolien tulisi olla tunnistettavia. (Pinna & Ruttenberg, 2016; Haastattelu 1; Haastattelu 4) Ethereum-verkossa toimiviin rahoitusalan hajautettuihin sovelluksiin tämän kaltaiset ominaisuudet, joissa omistukset linkitetään henkilöön, pitää erikseen lisätä. (Haastattelu 1) Osakeyhtiöiltä tyypillisesti vaaditaan osakasluettelon ylläpitämistä ja niiden tulee pyydettäessä pitää tämä kaikkien osakkaiden saatavilla. Sijoitusmuotoiset tokenit saattavat tarvita sopimusjärjestelyjä, jotka ottavat tämän huomioon. (Goforth, 2019, 49; Haastattelu 1) Jupiter-mallisessa osakekauppaverkossa, jossa osakkeet talletetaan verifiable-claim-muodossa, tätä ongelmaa ei ole. (Haastattelu 4)

Hajautetun rahoitusmaailman sovellukset eivät noudata rahoitusalan standardeja. (Haastattelu 4) Lohkoketjuteknologian yleistymisen ja käyttöönoton kannalta on tärkeää kehittää standardeja, joiden avulla erilaiset lohkoketjuteknologiaan pohjautuvat järjestelyt ja ennestään olemassa olevat järjestelyt saadaan toimimaan yhteen. (Mills ym. 2016) Kaupankäyntiverkoissa olisi siksi hyvä

käyttää standardiprotokollia, kuten Trust over IP. Jupiter-mallinen osakekauppaverkko on toteutettu tällä tavalla. (Haastattelu 4.)

Yrityksille voi olla vaikea perustella julkisen lohkoketjun käyttöä, koska sitä ei voi kontrolloida. (Haastattelu 3) Voi tulla tilanteita, joissa julkinen lohkoketjuverkko kaatuu, eikä kukaan vastaa siitä, koska kukaan ei omista sitä. Tällaista ongelmaa ei kuitenkaan tule yksityisessä Corda-verkossa. (Haastattelu 4)

Muita tunnettuja teknisluonteisia ongelmia lohkoketjuissa ovat transaktioiden peruuttamattomuus, joka tekee virheellisten ja laittomien transaktioiden korjaamisen mahdottomaksi (Haastattelu 1) ja skaalautuvuusongelma, joka liittyy erityisesti julkisten lohkoketjujen konsensusalgoritmien kykyyn käsitellä transaktioita. (Haastattelu 4, Mills ym., 2016)

8 YHTEENVETO

Tässä luvussa käydään läpi keskeisimpiä saavutettuja tuloksia, niiden merkitystä ja keskeisiä rajoitteita tutkimusmenetelmän ja tulosten suhteen. Lisäksi tuodaan esiin se, miten tämän tutkimuksen tulokset poikkeavat aiemmista tutkimuksista ja toisaalta ne tulokset, joiden osalta tämä tutkimus tukee aiempia tutkimustuloksia. Tämän tutkimuksen tavoitteena on ollut selvittää lohkoketjuteknologian soveltuvuutta osakkeiden digitalisointiin, joten tutkimuksessa on käyty läpi tutkimuskirjallisuutta, joka liittyy lohkoketjuteknologiaan ja erityisesti pyrkimys on ollut käyttää sellaista kirjallisuutta, joka sisältää oleellista tietoa osakkeiden digitalisoinnin kannalta.

Kirjallisuuskatsauksessa selvisi, että hajautettu digitaalinen omistaminen voi perustua lohkoketjuihin talletettaviin tokeneihin, mutta empiirisestä aineistosta löytyi vaihtoehtoiseksi teknologiaksi vahvistetun datan verkko, jolloin tokeneiden sijasta omistus on verifiable-claim-muodossa. Molemmat teknologiat lasketaan yleensä lohkoketjuteknologioiksi, vaikka vahvistetun datan verkossa ei käytetäkään varsinaisesti lohkoketjua vaan Corda-teknologiaa, jossa käytetään transaktioketjua. Hajautetun digitaalisen omistamisen lisäksi molemmat teknologiat mahdollistavat älykkäät sopimukset. Erilaisia älysopimusalustoja on useita mutta tunnetuin niistä on Ethereum.

Lohkoketjuteknologiaan pohjautuva rahoitusmaailma poikkeaa perinteisestä arvo-osuuksiin pohjautuvasta rahoitusmaailmasta niin paljon, ettei entisestä voida säilyttää mitään, vaan teknologiat vaihtuvat täysin samoin kuin liiketoimintamallit, ansaintamallit ja kannustinjärjestelmät. Jos osakkeiden säilytys saataisiin siirrettyä yhteen hajautettuun tilikirjaan useiden arvopaperikeskusten sijasta, päästäisiin eroon arvopaperikeskusten muodostamista siiloista, koska kaikilla olisi sama teknologia käytössä. Periaatteessa arvo-osuusjärjestelmät, pörssit ja selvityspalvelut saattaisivat muuttua tarpeettomiksi. Lisäksi osakeomistusten siirtely maasta toiseen olisi huomattavasti nykyistä helpompaa ja osaketransaktioiden end-to-end-prosessointinopeus olisi huomattavasti parempi kuin nykyisissä arvo-osuusjärjestelmissä. (Mills ym., 2016)

Suuressa mittakaavassa lohkoketjuteknologian käyttö osakkeiden digitalisoinnissa voi vaatia nykyisen lainsäädännön muuttamista, koska

lohkoketjuteknologian adaptoituminen nykyisiin vaatimuksiin voi muuten olla liian vaikeaa. ERC-20 tokeneihin pohjautuvan hajautetun finanssimaailman sovelluksia vaivaa heikko yhteensopivuus lainsäädännön kanssa. Ethereum-älysopimuksista puuttuu muun muassa KYC-sääntöjen mukainen identiteetinhallinta, mistä seuraa se, että transaktiot eivät ole virallisia ja lakiin pohjautuvia. Lisäksi laki edellyttää tietyissä sopimustilanteissa määrämuotoisuutta, mikä voi estää älykkäiden sopimusten käyttämisen. Eri maissa on poikkeavia säädöksiä ja laintulkinnallisia käytäntöjä, minkä vuoksi maitten välillä on eroja sen suhteen, mitä teknologioita voi käyttää osakkeiden digitalisoinnissa.

Vahvistetun datan verkkoon liittyy paljon vähemmän tiettyjä ongelmia kuin perinteisempään lohkoketjuverkkoon. Siihen liittyy myös merkittäviä etuja, kuten huomattavasti parempi verkon suorituskyky, mahdollisuus kommunikointiin käteistilien kanssa, luovutus maksua vastaan ja Corda-verkon virallistamisprosessi, jonka ansiosta transaktioista tulee lain mukaisia. Vahvistetun datan verkossa toimiva osakekauppaverkko mahdollistaa periaatteessa osakeyhtiön perustamisen viidessä minuutissa, minkä jälkeen sen osakkeilla voisi välittömästi käydä myös kauppaa. Se on kuitenkin uutta teknologiaa, jonka tarjoamat edut ja johon liittyvät ongelmat eivät ole vielä kovin hyvin tiedossa. Tämä tutkimus on yksi harvoista, jossa aihetta käsitellään, joten aihe kaipaisi lisää tutkimusta.

Julkisessa Ethereum-verkossa on useita heikkouksia osakkeiden digitalisoinnin kannalta. Yrityksille voi olla vaikea perustella julkisen lohkoketjun käyttöä, koska sitä ei voi kontrolloida. Voi tulla tilanteita, joissa julkinen lohkoketjuverkko kaatuu, eikä kukaan vastaa siitä, koska kukaan ei omista sitä. Ethereum-verkkoon rakennetun hajautetun rahoitusmaailman sovellukset eivät myöskään noudata W3C-standardeja. Lohkoketjuteknologian yleistymisen ja käyttöönoton kannalta on tärkeää kehittää standardeja, joiden avulla erilaiset lohkoketjuteknologiaan pohjautuvat järjestelyt ja ennestään olemassa olevat järjestelyt saadaan toimimaan yhteen. (Mills ym. 2016)

Tätä tutkimusta varten haastateltiin viittä asiantuntijaa, mikä on verrattain vähän. Tämän takia aineistosta ei löytynyt saturaatiota. Suppea aineisto on myös validiteetin ja reliabiliteetin kannalta ongelmallista, mikä vähentää tutkimuksen merkittävyyttä ja yleistettävyyttä.

Vaikka tämän tutkimuksen empiirinen osuus käsitteli enimmäkseen eri aiheita kuin kirjallisuuskatsaus, niin joidenkin asioiden suhteen empiirinen tutkimus vahvisti kirjallisuuskatsauksessa käytettyä aiempaa tutkimusta. Lohkoketjuteknologian käyttö parantaa pienten ja keskisuurten yritysten mahdollisuuksia saada rahoitusta ja vähentää tarvetta välittäjille, kuten pörssit ja arvopaperikeskukset, joihin nykyinen rahoitusjärjestelmä pitkälti perustuu. Perinteisten arvopapereiden sääntely ei ole täysin käyttökelpoista osakemuotoisten tokeneiden suhteen. Osakasluettelon ylläpito osakemuotoisten tokeneiden tapauksessa voi vaatia erityisiä sopimusjärjestelyjä, koska tokeneiden omistus on yleensä pseudonyymista. Empiirinen aineisto tuki myös näkemystä, että konsensusmekanismi ei välttämättä pysty takaamaan kaupanteon lopullisuutta, jos asiaa tarkastellaan transaktioiden lainmukaisuuden kannalta.

LÄHTEET

Advice, E. S. M. A. (2019) Initial Coin Offerings and Crypto-Assets (ESMA50-157-1391). Haettu osoitteesta https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

Ante, L. & Fiedler, I. (2019). *Cheap Signals in Security Token Offerings.* Hamburg: Blockchain Research Lab. Haettu osoitteesta: https://www.researchgate.net/profile/Ingo_Fiedler/publication/331287045_Cheap_Signals_in_Security_Token_Offerings/links/5c8e4cf792851c1df946e7c9/Cheap-Signals-in-Security-Token-Offerings.pdf

Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital Cryptocurrencies.* Sebastopol: O'Reilly Media

Atzei, Bartoletti & Cimoli (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). Teoksessa M. Maffei & M. Ryan (toim.), *Principles of Security and Trust*, LNCS 10204 (164-188). Upsala: Springer. Haettu osoitteesta: https://link.springer.com/chapter/10.1007/978-3-662-54455-6_8

Bech, M. L., Hancock, J., Rice, T., & Wadsworth, A. (2020). On the future of securities settlement. BIS Quarterly Review, 4(1). Haettu osoitteesta: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561195

Benos, E., Garratt, R., & Gurrola-Perez, P. (2017). *The economics of distributed ledger technology for securities settlement* (Valmisteluasiakirja 670.) Lontoo: Bank of England.

Begg, D., Fischer, S. & Dornbusch, R. (1997). *Economics.* (5. uud. painos). Berkshire: McGrawhill Book Company Europe.

Bentov, I., Ji, Y., Zhang, F., Breidenbach, L., Daian, P., & Juels, A. (2019, November). Tesseract: Real-time cryptocurrency exchange using trusted hardware. Teoksessa *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (1521-1538).* Lontoo: Association for Computing Machinery

Casey, M., Crane, J., Gensler, G, Johnson, S. & Narula, N. (2018). *The Impact of Blockchain Technology on Finance: A Catalyst for Change.* (Julkaisusarjan osa 21.). Lontoo: International Center for Monetary and Banking Studies. Haettu 21.6.2019 osoitteesta: https://www.cimb.ch/uploads/1/1/5/4/115414161/geneva21.pdf

Chanson, M., Martens, N., & Wortmann, F. (2020). The Role of User-generated Content in Blockchain-based Decentralized Finance. *ECIS 2020 Research-in-Progress Papers*. 91. AISeL Haettu osoitteesta: https://aisel.aisnet.org/ecis2020_rip/91

Chen, T., Li, X., Luo, X., & Zhang, X. (2017). Under-optimized smart contracts devour your money. Teoksessa *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER) (442-446)*. IEEE. Haettu osoitteesta: https://ieeexplore.ieee.org/abstract/document/7884650

Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business Horizons, 61(4)*, 567-575.

Chen, W., Zhang, T., Chen, Z., Zheng, Z., & Lu, Y. (2020). Traveling the token world: A graph analysis of Ethereum ERC20 token ecosystem. Teoksessa *Proceedings of The Web Conference 2020 (1411-1421)*. New York: Association for Computing Machinery.

Christidis, K. & Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Things. *IEEE Access 4. 2291-2303.* Haettu osoitteesta https://ieeexplore.ieee.org/document/7467408

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018, August). Blockchain versus database: A critical analysis. Teoksessa *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1348-1353. IEEE.

Cooke, J., Cohen, R. & Denisenko, J. (2019) Initial Coin Off erings: A comparative overview of securities regulator environments in the US, UK and Asia Pacific. . Teoksessa J. Dewey (toim.), *Blockchain & Cryptocurrency Regulation 2019* (34-46). Lontoo: Global Legal Group. Haettu osoitteesta: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

Di Angelo, M., & Salzer, G. (2020). Tokens, Types, and Standards: Identification and Utilization in Ethereum. Teoksessa *Intl. Conf. Decentralized Applications and Infrastructures (DAPPS), (1-11)*. IEEE

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering, 30(7)*, 1366-1385. IEEE Haettu osoitteesta: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8246573

DTCC (2016). *Tapping the Potential of Distributed Ledgers to Improve the Post Trade Landscape* [white paper]. DTCC. Haettu osoitteesta: https://www.finyear.com/attachment/642038/

ENISA, (2016). *Distributed Ledger Technology & Cybersecurity: Improving information security in the financial sector.* European Union Agency For Network And Information Security. Haettu osoitteesta: https://www.enisa.europa.eu/publications/blockchain-security

ESMA. (2.6.2016). *The Distributed Ledger Technology Applied to Securities Markets* [Discussion paper]. ESMA/2016/773. Pariisi: European Securities and Markets Authority. Haettu osoitteesta: https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

Eyal, I. (2017). Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. *Computer, 50(9),* 38-49. Haettu osoitteesta: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8048646&tag=1

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1), 1-15

Feenan, S., Heller, D., Lipton, A., Morini, M., Ram, R., Sams, R., ... & Zalles, D. B. (2020). Decentralized Financial Market Infrastructures. *The Journal of FinTech, 1(02)*, Haettu oistteesta: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3530996

Fenu, G., Marchesi, L., Marchesi, M., & Tonelli, R. (2018, March). The ICO phenomenon and its relationships with ethereum smart contract environment. Teoksessa *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (s. 26-32). Campobasso: IEEE.

França, B. (2019). *Deep Ocean: A blockchain-agnostic dark pool protocol*. Zug: Trinkler Software. arXiv preprint arXiv:1910.02359.

Frankenfield, J. (2018). Decentralized Applications – dApps. *Investopedia.* New York: IAC / Dotdash Meredith. Haettu osoitteesta: https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp

Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, *95*, 86-96.

Goforth, C. R. (2019). How Blockchain Could Increase the Need for and Availability of Contractual Ordering for Companies and Their Investors. *North Dakota Law Review, 94(1),* 1-63

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation 2(1),* 1-12.

Gächter, I., & Gächter, M. (2021). Success factors in ICOs: Individual firm characteristics or lucky timing?. *Finance Research Letters, 40,* 101715. Haettu osoitteesta: https://www.sciencedirect.com/science/article/pii/S1544612320300866

Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *European Company and Financial Law Review, 15(4)*, 645-696.

Heilman, E., Lipmann, S., & Goldberg, S. (2020, February). The arwen trading protocols. Teoksessa *International Conference on Financial Cryptography and Data Security (s. 156-173).* Cham: Springer.

Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., ... & Rosu, G. (2018). Kevm: A complete formal semantics of the ethereum virtual machine. Teoksessa *2018 IEEE 31st Computer Security Foundations Symposium (CSF) (s. 204-217),* Oxford, UK, July 9-12., 2018. IEEE.

Honkanen, P. (2017). *Lohkoketjuteknologian lupaus.* (Arcada Working Papers). Helsinki: Yrkeshögskolan Arcada. Haettu osoitteesta: https://core.ac.uk/download/pdf/161422148.pdf

Howell, S. T., Niessner, M., & Yermack, D. (2020). Initial coin offerings: Financing growth with cryptocurrency token sales. *The Review of Financial Studies, 33(9),* 3925-3974.

Hsieh, Y. C., Hsueh, C. W., & Wu, J. L. (2018). The exchange center: A case study of hybrid decentralized and centralized applications in blockchain. Teoksessa *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (s. 232-233).* IEEE.

Hussein, N. T., & Kashmar, A. H. (2020, November*). An Improvement of ECDSA Weak Randomness in Blockchain*. IOP Conference Series: Materials Science and Engineering, 928(3), 032022. *2nd International Scientific Conference of Al-Ayen University (ISCAU-2020) 15-16 July 2020, Thi-Qar, Iraq*. IOP Publishing. Haettu osoitteesta: https://iopscience.iop.org/article/10.1088/1757-899X/928/3/032022/pdf

Johnston, D., Yilmaz, S. O., Kandah, J., Bentenitis, N., Hashemi, F., Gross, R., & Mason, S. (2014). The General Theory of Decentralized Applications.

Haettu osoitteesta: http://cryptochainuni.com/wp-content/uploads/The-General-Theory-of-Decentralized-Applications-DApps.pdf

Juels, A., Kosba, A., & Shi, E. (2016). The ring of gyges: Investigating the future of criminal smart contracts. Teoksessa *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (s. 283-295)*. New York: Association for Computing Machinery. Haettu osoitteesta: https://dl.acm.org/doi/pdf/10.1145/2976749.2978362

Kaal, W. A. (2020). Digital Asset Market Evolution. *Journal of Corporation Law, 46,* 909-963.

Kaal, W. A., & Evans, S. (2019). Blockchain-based securities offerings. *UC Davis Business Law Journal, 20*, 89-109.

Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2019). What does not fit can be made to fit! Trade-offs in distributed ledger technology designs. Teoksessa *Teoksessa Proceedings of the 52nd Hawaii international conference on system sciences,* Grand Wailea, Hawaii, January 8-11, 2019. Haettu osoitteesta: https://scholarspace.manoa.hawaii.edu/bitstream/10125/60143/1/0703.pdf

Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2020). Trade-offs between distributed ledger technology characteristics. *ACM Computing Surveys (CSUR)*, 53(2), 1-37. Haettu osoitteesta: https://dl.acm.org/doi/pdf/10.1145/3379463

Karame, G. O., Androulaki, E., Roeschlin, M., Gervais, A., & Čapkun, S. (2015). Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security* (TISSEC), 18(1), 1-32. Haettu osoitteesta: https://dl.acm.org/doi/abs/10.1145/2732196

Kauppi, N. (2019). ICO rahoituskeinona. *Helsinki Law Review*, *13*(2), 32-63.

Kinnunen, T. K., Leviäkangas, P., Kostiainen, J., Nykänen, L. & Rouhiainen, K. (2017). *Lohkoketjuteknologian soveltaminen ja vaikutukset liikenteessö ja viestinnässä* (Liikenne- ja viestintäministeriön julkaisuja 12). Helsinki: Liikenne- ja viestintäministeriö.

Klayman, J. A. (2019). Mutually assured disruption: The rise of the security token. Teoksessa J. Dewey (toim.), *Blockchain & Cryptocurrency Regulation 2019* (s. 60-88). Lontoo: Global Legal Group. Haettu osoitteesta: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

Koverko, T., Housser, C. (2017). *Polymath: The Securities Token Platform.* [White paper]. Haettu osoitteesta: https://uploads-ssl.webflow.com/5a46fad33472ef00014b540a/5a7f30c8d2e04c0001f46390_Polymath%20Whitepaper.pdf

Kranz, J., Nagel, E., & Yoo, Y. (2019). Blockchain token sale. *Business & Information Systems Engineering, 61(6)*, 745-753.

Kyläkallio, J., Iirola O. & Kyläkallio, K. (2017). *Osakeyhtiö I.* (7. uud. painos). Keuruu: Edita.

Laki arvo-osuusjärjestelmästä ja selvitystoiminnasta (348/2017). Haettu osoitteesta: https://www.finlex.fi/fi/laki/alkup/2017/20170348

Lauslahti, K., Mattila, J. & Seppälä, T. (2016) *Älykäs sopimus – Miten blockchain muuttaa sopimuskäytäntöjä* (ETLA Report No. 57). Helsinki: ETLA. Haettu osoitteesta https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-57.pdf

Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal,* 26(2). Haettu osoitteesta: https://www.emeraldinsight.com/doi/pdfplus/10.1108/RMJ-12-2015-0042

Leppiniemi, J. (2008). *Osakeyhtiö : varteenotettava vaihtoehto.* Helsinki: Tietosykli

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841-853. Haettu osoitteesta: https://www.sciencedirect.com/science/article/pii/S0167739X17318332?casa_token=oloS0nEoP1EAAAAA:p-yQ6yilXG0zBZKcBk4KLEBEhqA9X6rIKXa2oeyYv8I-HwIr4V8pkPX8DVIHgzEsoaQUTW_e8n4

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *IJ Network Security,* 19(5), 653-659. Haettu osoitteesta: http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf

Lin, L. X. (2019). Deconstructing decentralized exchanges. *Stanford Journal of Blockchain Law & Policy*, 58-77.

Liu, S., Fang, Z., Gao, F., Koussainov, B., Zhang, Z., Liu, J., & Zhu, L. (2020, October). Whispers on Ethereum: Blockchain-based Covert Data Embedding Schemes. Teoksessa *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure* (171-179). New York: Association for Computing Machinery

Livshits, B. (2020). Analyzing smart contracts with MadMax: technical perspective. *Communications of the ACM*, 63(10), 86-86.

Luu, L., Teutsch, J., Kulkarni, R. & Saxena, P. (2015). *Demystifying Incentives in the Consensus Computer.* New York: Association for Computing Machinery. Haettu 22.6.2019, ACM DL.

Marinoff, N. (2018, 11. kesäkuuta). South Korean Exchange Coinrail Hacked, $40 Million In Crypto Reported Stolen. Haettu 21.11.2020 osoitteesta: https://bitcoinmagazine.com/articles/south-korean-exchange-coinrail-hacked-40-million-crypto-reported-stolen

Marsh, B & Dewey, J.(2019). The loan market, blockchain, and smart contracts: The potential for transformative change. Teoksessa J. Dewey (toim.), *Blockchain & Cryptocurrency Regulation 2019 (s. 47-59)*. Lontoo: Global Legal Group. Haettu osoitteesta: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

Massey, R., Dalal, D., & Dakshinamoorthy, A. (2017). Initial coin offering: A new paradigm. Haettu 20.11.2020 osoitteesta: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-new-paradigm.pdf

Mavridou, A., Laszka, A., Stachtiari, E. & Dubey, A. (2019). VeriSolid: Correct-by-Design Smart Contracts for Ethereum. Teoksessa I. Goldberg & T. Moore (toim.), *Financial Cryptography and Data Security*, LNCS 11598 (446-465). Frigate Bay, St. Kitts ja Nevis. Cham: Springer. Haettu osoitteesta: https://link.springer.com/content/pdf/10.1007/978-3-030-32101-7.pdf

McCullagh, A., & Flood, J. (2019). ICOs and Cryptotokens: A New Fundraising Asset Class—An Australian Perspective. Haettu osoitteesta: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3356210

Metcalfe, W. (2020). Ethereum, Smart Contracts, DApps. Teoksessa M. Yano, C. Dai, K. Masuda & Y. Kishimoto (toim.), *Blockchain and Crypt Currency: Building a High Quality Marketplace for Crypt Data* (77-93). Singapore: Springer.

Mills, D. C., Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A. I., ... & Baird, M. (2016). *Distributed ledger technology in payments, clearing, and settlement* (Finance and Economics Discussion Series 2016-095). Washington, D.C.: Federal Reserve. Haettu ositteesta: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf

Miraz, M. H., & Donald, D. C. (2019). Atomic cross-chain swaps: development, trajectory and potential of non-monetary digital token swap facilities. *Annals of Emerging Technologies in Computing (AETiC) 3(1),* 42-50.

Momtaz, P. P., Rennertseder, K., & Schröder, H. (2019). Token Offerings: A Revolution in Corporate Finance?. Haettu osoitteesta: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3346964

Nguyen, Q. K. (2016). Blockchain – A Financial Technology for Future Sustainable Development. Teoksessa *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD),* Kaohsiung, Taiwan, November 24-25. IEEE Haettu osoitteesta: https://ieeexplore.ieee.org/document/7796617

Niemi, M. I, (2017). arvo-osuus. Teoksessa *Tieteen termipankki*. Haettu 28.11.2020 osoitteesta: https://tieteentermipankki.fi/wiki/Oikeustiede:arvo-osuus

Niskanen, J. & Niskanen, M. (2013). *Yritysrahoitus.* (7. uud. Painos) Porvoo: Edita Publishing.

Nordnet. (20.11.2021) *Mitä T+2 tarkoittaa?*. Haettu osoitteesta: https://www.nordnet.fi/faq/841-mitae-t-2-tarkoittaa

Norta, A., Fernandez, C. & Hickmott, S. (2018). Tokenizing Commercial Property With Smart Contracts. Teoksessa *2018 International Joint Conference on Neural Networks (IJCNN)*, Rio, Brazil, July 8-13, 2018. Haettu osoitteesta: https://icorating.com/upload/yellowpaper/bRm1XfR2AyNAunJ24hW3WX9VirMeL49cZtVIp1ck.pdf

Norvill, R., Fiz, B., State, R., & Cullen, A. (2019). Standardising smart contracts: Automatically inferring ERC standards. Teoksessa *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (192-195), Seoul, Korea (South), May 14-17. IEEE.

Oliva, G. A., Hassan, A. E., & Jiang, Z. M. J. (2020). An exploratory study of smart contracts in the Ethereum blockchain platform. *Empirical Software Engineering, 25(3)*, 1864-1904.

Osakeyhtiölaki (624/2006). Haettu osoitteesta: https://www.finlex.fi/fi/laki/ajantasa/2006/20060624

Paavolainen, S., Elo, T., & Nikander, P. (2018, November). Risks from spam attacks on blockchains for Intemet-of-Things devices. Teoksessa *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (314-320). IEEE.

Patsonakis, C., & Roussopoulos, M. (2019, April). An Alternative Paradigm for Developing and Pricing Storage on Smart Contract Platforms. Teoksessa *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)* (170-175). IEEE.

Perlman, L. (2019). A Model Crypto-Asset Regulatory Framework. Haettu osoitteesta: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=3370679

Pinna, A., Ibba, S., Baralla, G., Tonelli, R., & Marchesi, M. (2019). A massive analysis of ethereum smart contracts empirical study and code metrics. *IEEE Access, 7*, 78194-78213.

Pinna, A., & Ruttenberg, W. (2016). *Distributed ledger technologies in securities post-trading revolution or evolution?* (ECB Occasional Paper 172). Frankfurt: European Central Bank (ECB). Haettu osoitteesta: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770340

Popper, N. (2018, 30. tammikuuta). Worries Grow That the Price of Bitcoin Is Being Propped Up. *New York Times*. Haettu 21.11.2020 osoitteesta: https://www.nytimes.com/2018/01/31/technology/bitfinex-bitcoin-price.html?dlbk

PRH, (n.d.). *Osakkeiden kuuluminen arvo-osuusjärjestelmään*. Patentti- ja rekisterihallitus. Haettu 29.11.2020 osoitteesta: https://www.prh.fi/fi/kaupparekisteri/osakeyhtio/muutosilmoitus/osakkeet/arvoosuus.html

Puzt, B. & Pernul, G. (2019). Trust Factors and Insider Threats in Permissioned Distributed Ledgers: An Analytical Study and Evaluation of Popular DLT Frameworks. Teoksessa A. Hameurlain & R. Wagner. (toim.), *Transactions on Large-Scale Data- and Knowledge- Centered Systems XLII. LNCS 11860 (25-50).* Berlin: Springer. Haettu osoitteesta: https://link.springer.com/chapter/10.1007/978-3-662-60531-8_2

Quiniou, M. (2019). *Blockchain: the advent of disintermediation*. Hoboken: John Wiley & Sons.

Rahimian, R., Eskandari, S., & Clark, J. (2019, June). Resolving the Multiple Withdrawal Attack on ERC20 Tokens. Teoksessa *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (320-329).* IEEE.

Reibel, P., Yousaf, H., & Meiklejohn, S. (2019, February). Short Paper: An Exploration of Code Diversity in the Cryptocurrency Landscape. Teoksessa *International Conference on Financial Cryptography and Data Security (73-83).* Cham: Springer.

Ribes, S. (2018, 10. maaliskuuta). Chasing fake volume: a crypto-plague. Haettu 21.10.2020 osoitteesta: https://sylvain-ribes.medium.com/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e

Rosenfeld, M. (2012). *Overview of colored coins* [White paper]. Haettu osoitteesta: https://bitcoil.co.il/BitcoinX.pdf

Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access*, 7, 50759-50779.

Rudolf, B., Kuhs, M., Baer, M. & Zintl, S. (2018). *Proof of Existence for Supply Chain Finance* [White paper]. AZHOS.

Sampson, J. (2018). Secret digital coin mining and trading is a threat to your business. *Computer Fraud & Security*, *2018(4),* 8-10.

Schwartz, D., Youngs, N. & Britto, A. (2014). *The Ripple Protocol Consensus Algorithm* [White paper]. Ripple Labs. Haettu ositteesta: https://ripple.com/files/ripple_consensus_whitepaper.pdf

Srivastav, R. K., Agrawal, D., & Shrivastava, A. (2020). A Survey on Vulnerabilities and Performance Evaluation Criteria in Blockchain Technology. *Advances in Distributed Computing and Artificial Intelligence Journal, 9(2),* 91-105. Haettu osoitteesta: https://gredos.usal.es/bitstream/handle/10366/146094/A_Survey_on_Vulnerabilities_and_Performa.pdf?sequence=1

State of DApps. (25.10.2020). Category. Haettu osoitteesta: https://www.stateofthedapps.com/dapps/

Swan, M. (2015). *Blockchain, Blueprint for a New Economy*. Sebastopol: O'Reilly Media

Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer, 50(9),* 14-17.

Tsai, W. T., Luo, Y., Deng, E., Zhao, J., Ding, X., Li, J., & Yuan, B. (2020). Blockchain systems for trade clearing. *The Journal of Risk Finance*. Haettu osoitteesta: https://www.emerald.com/insight/content/doi/10.1108/JRF-02-2017-0022/full/pdf

Tuomi, J. & Sarajärvi, A. (2004) *Laadullinen tutkimus ja sisällönanalyysi* (1. –3. painos). Helsinki: Tammi

Wang, R., Tsai, W. T., He, J., Liu, C., & Deng, E. (2018). A Distributed Digital Asset-Trading Platform Based on Permissioned Blockchains. Teoksessa *International Conference on Smart Blockchain* (55-65). Cham: Springer.

Warren, W., & Bandeali, A. (2017). 0x: An open protocol for decentralized exchange on the Ethereum blockchain [White paper]. Haettu osoitteesta: https://www.exodus.com/assets/docs/zrx-whitepaper.pdf

Wessling, F., & Gruhn, V. (2018, April). Engineering software architectures of blockchain-oriented applications. Teoksessa *2018 IEEE International Conference on Software Architecture Companion (ICSA-C) (45-46)*. IEEE.

Woodside, J. M., Augustine Jr, F. K., & Giberson, W. (2017). Blockchain technology adoption status and strategies. *Journal of International Technology and Information Management, 26(2),* 65-93.

Wu, L., Meng, K., Xu, S., Li, S., Ding, M., & Suo, Y. (2017). Democratic centralism: a hybrid blockchain architecture and its applications in energy internet. Teoksessa *2017 IEEE International Conference on Energy Internet (ICEI) (176-181)*. IEEE.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C. & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Desing. 2017. *Teoksessa 2017 IEEE international conference on software architecture (ICSA) (243-252)*. IEEE.

Yli-Huumo, J., Ko, D., Choi, S., Park, S. & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? - A Systematic Review. *PLoS ONE, 11(10), 1-27*

Zhang, B., & Balogun, H. (2018, November). On the sustainability of blockchain funding. Teoksessa *2018 IEEE International Conference on Data Mining Workshops (ICDMW) (89-96)*. IEEE.

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR), 52(3), 1-34.* Haettu ositteesta: https://dl.acm.org/doi/abs/10.1145/3316481

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14(4),* 352-375.

Zheng, P., Zheng, Z., Wu, J., & Dai, H. N. (2020). XBlock-ETH: Extracting and exploring blockchain data from ethereum. *IEEE Open Journal of the Computer Society, 1*, 95-106.

LIITE 1 ENSIMMÄINEN LIITE

Haastattelurunko

Tausta kysymykset:

1. Mitä asiantuntemusta sinulla on lohkoketjuteknologiasta?
2. Mitä asiantuntemusta sinulla on osakkeiden digitalisoinnista?

Osakkeiden digitalisointi

3. Millaisia teknologioita osakkeiden digitalisoinnissa käytetään?
4. Millaisena näet osakkeiden digitalisoinnin kehityskulun tähän päivään?

Digitalisoinnin haasteet

5. Millaisia ongelmia arvo-osuusjärjestelmän käyttöön liittyy?
6. Mitä ongelmia lohkoketjuteknologia ratkaisee digitaalisten osakkeiden suhteen?
7. Mitä ongelmia lohkoketjuteknologian käyttöön liittyy osakkeita digitalisoitaessa?

Lohkoketjuteknologian käyttö osakkeiden digitalisoinnissa

8. Miten yhtiömuoto vaikuttaa osakkeiden digitalisointiin, kun käytetään lohkoketjuteknologiaa?
9. Miten hyvin lohkoketjuteknologia sopii osakkeiden digitalisointiin lainsäädännön kannalta?
10. Onko lohkoketjuteknologia arvo-osuusjärjestelmän kilpailija vai täydentävä teknologia?

Digitaalisten osakkeiden tulevaisuus

11. Miltä näyttää tulevaisuus digitaalisten osakkeiden kannalta?