Alvar Mahlberg

LOHKOKETJUTEKNOLOGIA JA SEN HYÖDYNTÄMINEN YRITYSTEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Mahlberg, Alvar
Lohkoketjuteknologia ja sen hyödyntäminen yritysten näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2018, 32 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Halttunen, Veikko

Lohkoketjut ja laajemmin lohkoketjuteknologia ovat uusia ja ajankohtaisia innovaatiota. Ne rakentuvat lukuisista muista tekniikoista, mahdollistaen sellaisia tiedon tallennukseen ja transaktioihin liittyviä toimintoja, jotka eivät ennen ole olleet mahdollisia. Lohkoketjuteknologia on laaja kokonaisuus, jonka ymmärtäminen voi olla hankalaa. Tämän tutkimuksen tarkoituksena on perehdyttää lukija lohkoketjuteknologiaan, sekä tutkia sitä, miten yritykset voisivat hyödyntää lohkoketjuteknologiaa, mitä mahdollisuuksia ja haasteita siihen liittyy, sekä miten nämä tulisi ottaa huomioon. Nämä seikat toimivat myös motivaationa toteuttaa tämä tutkielma. Tutkielmassa tarkastellaan lohkoketjuteknologiaa uutena teknologisena innovaationa ja tutkitaan lohkoketjuteknologian toimintaperiaatteita. Tutkielmassa vertaillaan erilaisia lohkoketjuja ja niiden toimintaa, sekä käyttötarkoituksia. Tutkimus käsittelee lohkoketjuteknologiaa ja sen hyödyntämistä yritysten näkökulmasta tieteellisen aineiston, teknisten valkopaperien sekä kirjallisuuden avulla. Tutkimus on toteutettu kirjallisuuskatsauksena. Tutkimuksen perusteella lohkoketjuteknologia on sekoitus olemassa olevia teknologisia ratkaisuja. Lohkoketjut taas nähdään eräänlaisina tietokantoina tai hajautettuina tilikirjoina. Tutkimuksesta käy ilmi, että lohkoketjuteknologiaa on otettu käyttöön monilla eri toimialoilla viime vuosina ja sen onnistunut hyödyntäminen mahdollistaisi yrityksille uusien palveluiden kehittämistä. Toisaalta useimpien nykyisten toimintojen korvaaminen lohkoketjuteknologialla tuskin on kannattavaa.

Asiasanat: lohkoketju, hajautettu tilikirja, data, kryptografia, konsensus, liiketoiminta, luottamus

ABSTRACT

Mahlberg, Alvar
Utilization of blockchain technology from the perspective of enterprises
Jyväskylä: University of Jyväskylä, 2018, 32 pp.
Information Systems, Bachelor´s thesis
Supervisor: Halttunen, Veikko

Blockchains and the blockchain technology are new and topical innovations. They are built from a number of other technologies, enabling such things as data storage and transaction-related functions that were not previously possible. Blockchain technology is a large entity that can be difficult to understand. The purpose and of this thesis is to familiarize the reader with the blockchain technology, as well as to explore how companies can take advantage of the blockchain technology, the opportunities and challenges involved, and how these should be taken into account. These things were also the motivation to implement this thesis. The thesis examines the blockchain technology as a new technological innovation and explores the principles of the blockchain technology. The thesis compares different blockchains and their activities and uses. The thesis deals with the blockchain technology and its exploitation from the point of view of business through scientific material, technical white papers and literature. The thesis was implemented as a systematic literature review. Based on the research, blockchain technology is a blend of existing technological solutions. Blockchains, on the other hand, are seen as types of databases or decentralized ledgers. The study shows that blockchain technology has been introduced in many different industries over the past few years and its successful exploitation would enable companies to develop new services. On the other hand, replacing most current activities with blockchain technology is unlikely to be profitable.

Keywords: blockchain, distributed ledger, data, cryptography, consensus, business, trust

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Lohkoketju on vaihtoehtoinen tapa siirtää ja säilöä arvoa. Lohkoketjua voidaan kuvata julkisena tilikirjana, joka säilyttää datan ja sen siirtojen eheyden (Swan, 2015). Lohkoketjut ovat osa hajautetun tilikirjan teknologiaa (Distributed ledger technology). Ne ovat hajautettuja tietokantoja, jotka on suojattu kryptografialla ja joita hallinnoidaan erilaisin konsensusmenetelmin. Käytännössä lohkoketju on siis digitaalisten tapahtumien rekisteri. (Beck ym., 2017). Yritysten näkökulmasta lohkoketju mahdollistaa niille uusia liiketoimintamalleja, sekä mahdollistaa nykyisten liiketoimintaprosessien kehittämistä nopeuttamalla toimintoja ja vähentämällä kustannuksia (Nowinski & Kozma, 2017). Markets ja Marketsin (2015) julkaiseman tutkimuksen mukaan lohkoketjumarkkinan koon arvioidaan kasvavan vuoden 2016 210 miljoonasta dollarista 2.3 miljardiin dollariin vuoteen 2021 mennessä.

Lohkoketjuteknologiaa on käsitelty tieteellisissä aineistoissa viime vuosina jonkin verran, mutta pääasiassa tutkimukset käsittelevät lohkoketjujen ja siihen liittyvien teknisten ja matemaattisten ratkaisujen toteuttamista. Yritysten näkökulmasta lohkoketjuteknologiaa ei ole tutkittu juuri ollenkaan. Suuri osa aiheeseen liittyvistä tutkimuksista käsittelee Bitcoin-järjestelmää. Tässä tutkielmassa ei ole haluttu keskittyä erityisesti juuri siihen, vaan lohkoketjuteknologiaan, joka mahdollistaa Bitcoin-järjestelmän toiminnan.

Tämän tutkielman tarkoituksena on selventää, mitä lohkoketjuteknologia tarkoittaa. Tutkimuksessa selvitetään miten tämä uusi teknologia tulisi huomioida yritysten näkökulmasta. Tavoitteena on rakentaa ymmärrettävä ja tiivis kuvaus siitä, mitä lohkoketjuteknologiasta tiedetään tänä päivänä ja miten yritykset voivat mahdollisesti hyötyä siitä. Tutkielmassa pyritään vastaamaan kahteen tutkimuskysymykseen, jotka ovat:

1. Mitä lohkoketjuteknologia on?
2. Miten lohkoketjuteknologia tulisi huomioida yritysten näkökulmasta?

Tutkielma on toteutettu kirjallisuuskatsauksena. Aineisto on kerätty IEEE Xplore Digital Library-, Springer Link- sekä Google Scholar -tietokantojen avul-

la. Aihealueen ja tutkimuksen uutuusarvosta johtuen on lähteinä käytetty myös muita julkaisuja. Näitäkin lähteitä on kuitenkin tarkasteltu kriittisesti ja niitä on pyritty valitsemaan sen perusteella, että vastaavat tutkimukset ovat myös niihin viitanneet. Tiedonkeruussa käytin avainsanoja: blockchain (lohkoketju), blockchain technology (lohkoketjuteknologia), distributed ledger (hajautettu tilikirja), cryptography (kryptografia) ja cryptocurrencies (kryptovaluutat). Pyrin rajaamaan hakuani mahdollisimman uusiin artikkeleihin.

Luvussa 2 tarkastellaan lohkoketjuteknologiaa. Tarkastelemme lohkoketjuteknologian kehitystä ja lohkoketjuteknologian määrittelyä. Näiden lisäksi vertailemme erilaisia lohkoketjuja. Luku 3 keskittyy itse lohkoketjuun. Tarkastelemme lohkoketjun toimintaperiaatetta, yksittäisen lohkon toimintaa, sekä erilaisia konsensus menetelmiä. Luvussa 4 käsitellään lohkoketjun hyödyntämistä. Tarkastelemme lohkoketjuteknologiaa yritysten näkökulmasta, eli miten yritykset voivat siitä hyöytä, mitä tulisi ottaa huomioon, jos aiotaan käyttää lohkoketjuteknologiaa ja mitä yrityksille suunnattuja ratkaisuja on jo olemassa. Lopuksi tarkastelemme vielä lohkoketjuteknologian nykytilaa. Luku 5 on yhteenveto, jossa käydään läpi vastauksia tutkimuskysymyksiin ja mahdollisia jatkotutkimuksen aiheita.

2 LOHKOKETJUTEKNOLOGIA

Lohkoketjuteknologia on sekoitus olemassa olevia teknologisia ratkaisuja. Se on uusi tapa yhdistellä julkisen avaimen salausta, kryptografiaa ja vertaisverkkoja (Nakamoto, 2008). Yksinkertaisesti lohkoketjuteknologian avulla toisilleen tuntemattomat tahot voivat tuottaa ja ylläpitää lähestulkoon mitä tahansa tietokantoja täysin hajautetusti keskenään. Tietokantaan tehdyt muutokset käsitellään ja hyväksytään ennalta määriteltyjen sääntöjen pohjalta. Nämä muutokset kootaan tietyin väliajoin paketeiksi, joita kutsutaan lohkoiksi. (Mattila & Seppälä, 2015). Lohkoketju rakentuu näistä yksittäisistä lohkoista, jotka on ketjutettu toisiinsa muodostaen kronologisessa järjestyksessä olevan lohkojen ketjun, eli lohkoketjun (Nair & Sebastian, 2017). Tässä luvussa tutkimme lohkoketjuteknologian historiaa ja kehitystä. Luvussa pyritään selvittämään lohkoketjujen, sekä lohkoketjuteknologian määritelmiä. Näiden lisäksi pyritään tarkastelemaan erilaisia lohkoketjuja ja tekemään eroja niiden välille.

2.1 Lohkoketjuteknologian historia

Vuonna 1982 David Chaum julkaisi tutkimuksensa Blind signatures for untraceable payments, jossa hän käsitteellisti ajatuksensa anonyymistä ja digitaalisesta vaihdannan välineestä. Chaum (1982) esitteli tutkimuksessa kryptografiaan perustuvia keinoja, joiden avulla digitaalisen valuutan kehittymistä hidastanut kaksinkertaisen käytön ongelma kyettäisiin ratkaisemaan ja näin ollen anonyymi ja digitaalinen vaihdannan väline olisi mahdollista toteuttaa. Kaksinkertaisen käytön ongelmalla tarkoitetaan digitaalisessa maailmassa ilmenevää ongelmaa, jossa digitaalista rahaa voidaan helposti kopioida ja käyttää useaan kertaan, jos turvallisuudesta on karsittu ja ongelmaa ei ole huomioitu (Chohan, 2017). Chaumin (1982) tutkimus oli aikansa edelläkävijä ja myöhemmin laajalle levinnyttä anonyymiä ja digitaalista vaihdannan välinettä saatiin odotella vielä toista kymmentä vuotta. Vuonna 2008 pseudonyymi Satoshi Nakamoto (2008) julkaisi tutkimuksensa ”Bitcoin; A Peer-to-Peer Electronic Cash System”, jossa hän esitteli kaksinkertaisen käytön ongelman ratkaisemiseksi

käyttäjien ylläpitämää hajautettua vertaisverkkoa, poistaen tarpeen luotetusta keskuspalvelimesta. Nakamoton oikeaa henkilöllisyyttä ei ole kyetty varmistamaan (Drainville, 2012). The Economist (2015) kuvailee Nakamoton ajatusta järjestelmästä, jossa turvallisuus ja väärinkäytösten välttäminen saavutettaisiin ilman tarvetta turvautua luotettuihin kolmansiin osapuoliin. Nakamoton ajatuksessa tämä luotettu keskuspalvelin korvattaisiin konsensusmenetelmällä nimeltä proof-of-work. Juuri vaatimus luotetusta keskuspalvelimesta oli hidastanut digitaalisen rahan kehitystä ja yleistymistä. (Back ym., 2014.) Bitcoin sai alkunsa tammikuussa 2009, kun ensimmäinen Bitcoin-lohko louhittiin (Barber, Boyen, Shi & Uzun, 2012). Bitcoin on toiminnaltaan hajautettu teknologinen alusta, joka on sekä valuutta että digitaalisen rahan sekä muiden digitaalisten asioiden siirtämisen perustana oleva infrastruktuuri. Sen ominaispiirteenä on kyky toimia ilman luotettua kolmatta osapuolta. (Huberman, Leshno & Moallemi, 2017.) Bitcoin oli ensimmäinen sovellus, jossa kaksi tai useampi toisiaan tuntematon tai toisiinsa luottamaton taho kykeni ylläpitämään luottamusta ilman tarvetta kolmannelle osapuolelle tai keskitetylle järjestelmälle (Olnes, 2015). Bitcoinin toiminnan mahdollisti joukko teknologisia ratkaisuja ja tekniikoita, joiden yhdistelmänä syntyi lohkoketjuteknologia. Lohkoketjuteknologia ei kuitenkaan rajoitu pelkästään Bitcoin-järjestelmään, vaan sen avulla voidaan tehdä ja toteuttaa paljon muutakin, mihin tässä tutkielmassa tutustutaan paremmin.

2.2 Lohkoketjuteknologian määrittely

Lohkoketjuteknologia voidaan nähdä osana hajautetun tilikirjan (Distributed ledger technology) ratkaisuja. Hajautettu tilikirja on erityisesti omaisuustietokanta, joka voidaan jakaa verkossa eri toimijoiden kesken hajautetusti. Näin ollen jokaisella toimijalla on samanlainen kopio tilikirjasta. Näitä kahta ei kuitenkaan pidä täysin sekoittaa toisiinsa, sillä hajautetun tilikirjan ratkaisuja voidaan toteuttaa myös ilman varsinaista lohkoketjua. (UK Government, 2016.) Voimme siis tarkastella lohkoketjuja uudenlaisina hajautettuina tietokantoina. Verrattuna perinteisiin hajautetun tietokannan hallintajärjestelmiin kuten SQL-pohjaiseen Oracleen ja NoSQL-pohjaiseen Apache Cassandraan, voidaan esiin nostaa selviä eroja. Ensinnäkin lohkoketjut ovat hajautetusti hallinnoituja. Edellä mainitut perinteiset hajautetun tietokannan hallintajärjestelmät taas ovat logiikaltaan keskitetysti hallinnoituja. Toiseksi kirjausketjun muuttumattomuudessa on eroja, sillä perinteiset hajautetun tietokannan hallintajärjestelmät tukevat komentoja luo, lue, päivitä ja poista. Lohkoketjuissa on ainoastaan luo ja lue komennot, tarkoittaen että lohkoketjuihin tallennettua dataa on erittäin vaikea muuttaa. Kolmanneksi tiedon alkuperää ja varojen omistajuutta ei voi lohkoketjussa muuttaa kuin ennalta määritellyin säännöin. Vastaavasti perinteisissä hajautetun tietokannan hallintajärjestelmissä järjestelmän ylläpitäjä voi muokata tiedon alkuperää, tai varojen omistajuutta. (Kuo, Kim & Ohno-Machado, 2017.)

Lohkoketjuteknologian ja lohkoketjujen määrittely on vaikeaa. Swan (2015) mukaan lohkoketju voidaan nähdä uutena sovelluskerroksena, joka toimii osana muita Internet-protokollia. Vitalik Buterin (2015) taas kuvailee lohkoketjua taikatietokoneeksi, johon kuka tahansa voi ladata ohjelmia ja jättää ohjelmat ”itsestään suoritettaviksi”. Buterinin (2015) mukaan kaikkien ohjelmien nykyiset ja aikaisemmat versiot ovat julkisesti nähtävissä, ne ovat vahvasti suojatut ja niillä on takuu, että ohjelmat suorittavat täsmälleen niin kuin lohkoketjun protokollassa on määritelty. Pilkington (2015) kritisoi Buterinin (2015) termiä ”taikatietokone”, mutta toteaa samalla Buterinin (2015) kuvaileman määrittelyn hyödylliseksi, sillä se alleviivaa lohkoketjun perusolemusta informatiivisena ja prosessuaalisena, joka ei siis suoraan liity rahapolitiikkaan, johon se Bitcoinin toimesta helposti sekoitetaan. Davidson, De Filippi ja Potts (2016) taas lähestyvät lohkoketjuteknologiaa näkökulmasta, jonka mukaan lohkoketju avoimena alustana tulisi nähdä hajautettavuuden teknologiana. Heidän mukaansa lohkoketjuteknologian päätarkoitus on tarjota hajautettavuutta, joka taloudellisesta näkökulmasta yhdistää lohkoketjuteknologian organisaatioihin ja markkinoihin. Mattila (2016) mukaan sanalla lohkoketjuteknologia saatetaan tarkoittaa hajautetun konsensus arkkitehtuurin koko pinoa, tai sen yksittäistä kerrosta. Kuten edellä mainitusta käy ilmi, emme vielä täysin ymmärrä mitä termit lohkoketju ja lohkoketjuteknologia tarkoittavat, sillä riippuen kontekstista, niillä saatetaan tarkoittaa eri asioita. Krujiff ja Weigand (2017) mukaan lohkoketjuteknologian ollessa vielä niin uusi innovaatio, puuttuu siltä selkeä terminologia.

Lohkoketjuilla on kuitenkin olemassa tiettyjä ominaispiirteitä, eli sellaisia elementtejä joihin lohkoketjujen toiminnat nojaavat. Ymmärtääksemme paremmin, mistä lohkoketjuissa on kysymys, on meidän hyvä tarkastella näitä elementtejä. Lin ja Liao (2017) ovat esitelleet lohkoketjuteknologian kuusi keskeisestä elementtiä. Ensimmäinen elementti on **hajautettavuus**. Hajautettavuudella tarkoitetaan vastakohtaa keskittämiselle, jossa hallinto ja valta on luovutettu tietylle yksittäiselle toimijalle eli luotetulle keskuspalvelimelle. Lohkoketjua voidaan ylläpitää vertaisverkossa, jossa käyttäjät osallistuvat sen ylläpitämiseen ja transaktioiden varmentamiseen. Lohkoketju voi tällä tavoin vähentää palvelinkustannuksia, sekä käyttökustannuksia. (Zheng ym, 2017; Lin & Liao 2017.)

Toisena elementtinä on **läpinäkyvyys**. Läpinäkyvyydellä tarkoitetaan datan tallentamista lohkoketjuun, joka on läpinäkyvää jokaiselle käyttäjälle. Kaikki lohkoketjussa tehdyt transaktiot on tallennettu ja niitä voi tarkastella jälkeenpäin. (Lin & Liao, 2017; Zheng ym, 2017.)

Kolmantena elementtinä on **avoin lähdekoodi**. Suurin osa lohkoketjuista on ainakin vielä tänä päivänä julkisia, eli avoimia kaikille. Avoimen lähdekoodin avulla järjestelmää voidaan kehittää käyttäjien yhteistyöllä. Avoin lähdekoodi kasvattaa luottamusta, parantaa joustavuutta ja vähentää kustannuksia. (Lin & Liao, 2017; Pilkington, 2016.) Käytännössä julkisten lohkoketjujen kehittäminen perustuu avoimeen lähdekoodiin ja aktiiviseen yhteisöön sen taustalla.

Neljäntenä elementtinä on **autonomia**. Autonomialla eli itsehallinnolla viitataan lohkoketjujen konsensukseen. Lohkoketjun toiminta nojaa kryptografiaan ja taloudellisiin kannustimiin. Järjestelmä on määritelty toimivaksi tietyllä

tavoin ja se kannustaa käyttäjiä toimimaan, kuten protokollassa on määritelty. Yksittäisen toimijan on hyvin vaikea muuttaa järjestelmän toimintaa. (Lin & Liao, 2017).

Viidentenä elementtinä on **muuttumattomuu**s. Lähtökohtaisesti lohkoketjuun tallennettua tietoa ei jälkikäteen voi muuttaa, tai ainakin se on erittäin vaikeaa. Lohkoketjuteknologian avulla voidaan luoda muuttumattomia rekisterejä eri tyyppisille asioille (Lin & Liao, 2017; Mattila, 2016).

Kuudentena elementtinä on **anonymiteetti**. Anonymiteetillä viitataan digitaaliseen allekirjoitukseen ja muihin kryptografisiin menetelmiin, joiden avulla dataa voidaan siirtää lohkoketjussa käyttäjien välillä ilman tarvetta tietää heidän oikeaa identiteettiä. (Lin & Liao, 2017.)

Lin ja Liao (2017) esittelemät lohkoketjuteknologian elementit antavat hyvää perspektiiviä ominaisuuksista ja toiminnasta. Meidän tulee kuitenkin huomioida, että on olemassa erilaisia lohkoketjuja ja näissä lohkoketjuissa on eroja. Edellä mainittuja elementtejä ei siis voida pitää täysinä totuuksina liittyen kaikkiin lohkoketjuihin. Seuraavassa kappaleessa tutkitaan tarkemmin näiden erityyppisten lohkoketjujen eroja ja ominaisuuksia.

2.3 Erityyppiset lohkoketjut

Lohkoketjuja on olemassa erityyppisiä. Lin ja Liao (2017) mukaan erityyppisillä lohkoketjuilla on omat vahvuutensa ja ne soveltuvat parhaiten eri tyyppisiin käyttötarkoituksiin, riippuen siitä minkä tyyppisessä ympäristössä tiettyä lohkoketjua halutaan hyödyntää. Zheng ym. (2017) havainnollistavat tutkimuksessaan kolmen erilaisen lohkoketjun eroja (taulukko 1). Kolme erilaista lohkoketjua ovat:

1. **Julkinen lohkoketju**: on avoin kaikille, tarjoaa läpinäkyvyyttä ja pyrkii estämään vallan keskittymistä tietylle yksittäiselle taholle. Kaikki toimijat voivat osallistua järjestelmän ylläpitoon, käyttämiseen ja transaktioiden hyväksymiseen. Julkisessa lohkoketjussa toimijoiden ei tarvitse luottaa toisiinsa.
2. **Yksityinen lohkoketju**: Yksityiset lohkoketjut toimivat suljetummissa ympäristöissä ja käyttäjillä on useasti tiettyjä rajattuja oikeuksia. Jokaisella halukkaalla ei ole lupaa osallistua lohkoketjun käyttöön. Yksityinen lohkoketju soveltuu paremmin tietyille toimialoille, joissa halutaan toimia ainoastaan luotettujen kumppaneiden kanssa.
3. **Hybridi lohkoketju**: jota kutsutaan myös nimellä konsortio-lohkoketju (Buterin 2015). Hybridi-lohkoketju sijoittuu ominaisuuksiltaan julkisen ja yksityisen lohkoketjun väliin. Hybridi-lohkoketjut ovat soveltuvia järjestelmiin, joissa toimijoiden välillä tulee olla jonkinlaista luottamusta. Hybrid-lohkoketjut soveltuvat yritysten väliseen yhteistyöhön. (Zheng ym., 2017.)

Taulukko 1. Lohkoketjujen eroja, suomennettu. (Zheng ym, 2017, 7)

Ominaisuus	**Julkinen lohkoketju**	**Hybridi lohkoketju**	**Yksityinen lohkoketju**
Konsensus määrittely	Louhijat	Valitut noodit	Yksi organisaatio
Käyttöoikeudet	Julkiset	Julkiset tai rajoitetut	Julkiset tai rajoitetut
Muuttumattomuus	Lähes mahdoton peukaloida	Mahdollista peukaloida	Mahdollista peukaloida
Tehokkuus	Matala	Korkea	Korkea
Keskitetty	Ei	Osittain	Kyllä
Konsensus prosessi	Ei vaadi lupaa	Vaatii luvan	Vaatii luvan

Erityyppiset lohkoketjut voidaan jakaa myös karkeammin kahteen ryhmään. Wust ja Gervais (2017) mukaan ensimmäinen ryhmä on **avoimet lohkoketjut**, jotka ovat hajautettuja ja avoimia kaikille. Avoimet lohkoketjut ovat sama asia kuin julkiset lohkoketjut. Toinen ryhmä on **luvan vaativat lohkoketjut.** Näissä lohkoketjuissa on jonkinlainen keskusyksikkö, joka päättää ja antaa oikeuksia yksittäiselle toimijalle osallistua lohkoketjun toimintaan. Se päättää myös eri käyttäjien oikeuksista luku- tai kirjoitustoimintoihin. Näiden kahden ryhmän eroavaisuuksia on hahmoteltu taulukossa 2. Taulukosta voidaan todeta, että lupaa vaatimattomissa lohkoketjuissa osallistuminen on vapaata, kun taas luvan vaativassa tarvitaan jonkinlainen lupa keskushallinnolta. Avoimissa lohkoketjuissa on vapaat kirjoitus- ja lukuoikeudet, kun taas luvan vaativissa ne on rajoitettu. Identiteetti on avoimissa salattu, kun taas luvan vaativissa se on useimmiten tunnistettava.

Vertailtaessa näitä kahta ryhmää, voidaan todeta, että julkisten lohkoketjujen suurin merkitys uskotaan olevan kehittyville talouksille, sillä julkinen

lohkoketju poistaa tarpeen luottamukselle. Kehittyvien talouksien lisäksi julkisista lohkoketjuista uskotaan olevan hyötyä laitteiden yhdistämiseen ja asioiden internetin kehittymiselle (Zheng ym 2017; Mattila 2016). Krujiff ja Weigand (2017) mukaan avoimet lohkoketjut tarjoavat läpinäkyvyyttä ja niiden päätarkoitus on estää vallan keskittymistä. Toisaalta on mahdollista, että valta keskittyy myös avoimissa lohkoketjuissa. Jos yksittäinen toimija omistaa puolet verkon laskentatehosta on valta silloin keskittynyt hänelle.

Luvan vaativat lohkoketjut taas kykenevät tarjoamaan kannattavia ratkaisuja esimerkiksi tilintarkastuksen käyttötarkoituksiin (Glaser, 2017). Esimerkiksi mahdollisuus lukea ja tarkastella lohkoketjuun tallennettua dataa saattaa olla arvokasta yritykselle tai organisaatiolle (Krujiff ja Weigand, 2017). Luvan vaativissa lohkoketjuissa jokin keskusyksikkö käyttää suurempaa määräysvaltaa kuin muut jäsenet. Tällöin voidaan kritisoida sitä, kuinka hajautetusta järjestelmästä on enää kysymys.

Taulukko 2. Avoimien ja luvan vaativien lohkoketjujen eroja, suomennettu. (Clresearch, 2018)

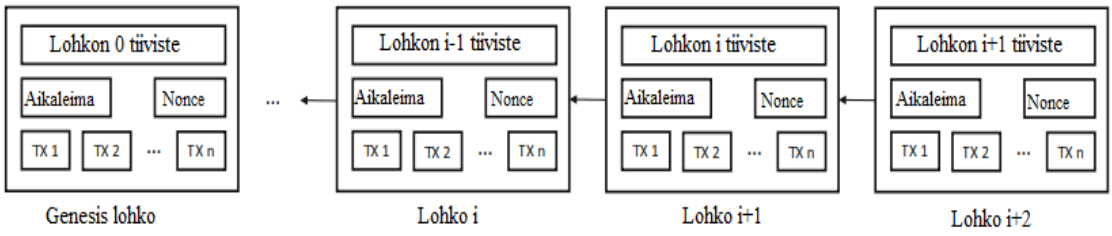
	Avoimet lohkoketjut	**Luvan vaativat lohkoketjut**
Osallistuminen	Kuka tahansa voi osallistua	Kutsu, tarkastus tai kriteeri
Oikeudet	Kuka tahansa voi lukea ja kirjoittaa	Luku- ja kirjoitusoikeudet saattavat olla rajoitettuja
Identiteetti	Pseudonyymi	Osallistujat mahdollisesti tunnistettava

3 LOHKOKETJU

Tässä luvussa käymme läpi lohkoketjuteknologiaa ja erityisesti lohkoketjun toimintaperiaatetta. Luvussa tarkastellaan tarkemmin niitä tärkeitä elementtejä, joista lohkoketjut rakentuvat. Nämä elementit ovat kryptografiset menetelmät, sekä konsensusmenetelmät. Käymme läpi sellaisia kryptografisia menetelmiä, joita lohkoketjut hyödyntävät toiminnassaan. Konsensusmenetelmistä pureudumme kahteen yleisesti tunnetuimpaan, eli proof-of-work, sekä proof-of-stake menetelmään.

3.1 Lohkoketjun toimintaperiaate

Lohkoketju koostuu datakokonaisuuksista, jossa useat datapaketit on koottu ketjuksi. Näitä datapaketteja kutsutaan lohkoiksi. Yksittäinen lohko sisältää useita tapahtumia. Lohkoketju laajentuu aina uudella lohkolla ja sen seurauksena lohkoketju edustaa kokonaista tilikirjaa kaikista tapahtumista. (Nofer ym., 2017.) Kunkin lohkon kaikesta tietosisällöstä lasketaan yksilöllinen tiiviste. Tähän tietosisältöön lisätään myös edellisen lohkon tiiviste, jolloin uusin lohko saadaan linkitettyä edeltäjäänsä. (Storås, 2016.) Tämä tarkoittaa sitä, että jos yksikin merkki jossain lohkossa muuttuu, vaikuttaa se kaikkiin sen jälkeisiin tiivisteisiin. Näin ollen lohkoketjun tapahtumahistoriaa on erittäin vaikea muuttaa jälkikäteen. Tässä esimerkki lohkoketjusta (kuvio 1):



Kuvio 1 Esimerkki lohkoketjusta, suomennettu (Zheng ym, 2017, 4).

Lohkoketjusta muodostuu lohkojen sarja, joka on samalla tietokanta käyttäjien toteuttamista tapahtumista ja heidän omistuksistaan. Yhteen lohkoon on sijoitettu useita eri tapahtumia, mutta lohkon koko on ennalta määritelty, joten sen kokoa ei voi ylittää. Yhden lohkon tapahtumat katsotaan tapahtuneen samanaikaisesti. Lohkoketjun ensimmäistä lohkoa kutsutaan genesis-lohkoksi. Kun alkuperäiseen tietokantaan liitetään uusia lohkoja, muodostuu niistä ajantasainen tietokanta, eli lohkoketju. Kun yksittäinen lohko on liitetty lohkoketjuun, sen sisältämät transaktiot ovat tämän jälkeen pysyvä osa lohkoketjua, eikä niitä voi enää lähtökohtaisesti jälkeenpäin muokata. (Mattila & Seppälä, 2015; Zheng ym., 2017; Arias & Yongseok 2013.)

Lohkoketjujen toimintaperiaatteita voidaan tarkastella myös työskentelyprossien kautta. Lohkoketjun työskentelyprosessit voidaan karkeasti jakaa neljään vaiheeseen. **Ensimmäisessä vaiheessa** solmu eli toimija tallentaa uutta dataa ja julkaisee sen viestinä verkkoon. **Toisessa vaiheessa** vastaanottava solmu tarkastaa viestin, ja jos se pitää paikkansa, säilötään se lohkoon. **Kolmannessa vaiheessa** hyödynnetään konsensusmenetelmiä, jotta varmistetaan lohkon tietojen pitävän paikkansa ja näin ollen se voidaan luotettavasti lisätä osaksi lohkoketjua. **Neljännessä vaiheessa** verkon solmut ovat hyväksyneet lohkon osaksi ketjua ja se on liitetty sen osaksi. Seuraava lohko jatkaa lohkoketjua viimeisimmäksi liitetystä lohkosta. (Lin & Liao 2017.)

3.2 Kryptografiset menetelmät

Kuten aiemmin totesimme, lohkoketjuteknologia hyödyntää älykkäästi jo olemassa olevia tekniikoita ja teknologisia ratkaisuja. Yhtenä näistä tekniikoista ovat kryptografiset menetelmät. Näiden menetelmien avulla jopa arkaluontoista tietoa voi lähettää julkisessa verkossa ilman, että kolmannet osapuolet kykenevät sitä manipuloimaan (Bellare & Rogaway, 2005). Modernissa kryptografiassa käytetään laajalti algoritmisia sekä matemaattisia menetelmiä turvaamaan digitaalista informaatiota ja järjestelmiä. Kryptografiaa on perinteisesti pidetty armeijan ja tiedusteluorganisaatioiden toteuttamana tapana lähettää ja purkaa salattuja viestejä. Ennen 2000-lukua sen käyttö on ollut rajoittunutta ja se on perustunut koodien tekemiseen ja purkamiseen sitä taitavien henkilöiden luovuuden ja henkilökohtaisten taitojen pohjalta. Kryptografian tieteellinen tutkimus on alkanut vasta 2000-luvulla, mutta nykypäivänä se on huomattavasti perinteistä laajempaa - kattaen salaisen viestinnän lisäksi digitaalisia allekirjoituksia, salaisten avaimien protokollia, todennusprotokollia ja digitaalisen rahan tutkimusta. Nykypäivänä kryptografiaa on lähes kaikkialla ja hyödynnämme kryptografiaa päivittäin, vaikka emme sitä välttämättä itse huomaa. (Katz & Lindell, 2015.)

Kryptografisista menetelmistä on valtavasti hyötyä lohkoketjuteknologiassa. Lohkoketjuteknologiassa kryptografiaa hyödynnetään tiivisteiden, digitaalisten allekirjoitusten ja julkisen avaimen salausmenetelmän parissa (Bonneau ym., 2016). Lohkoketjuissa käytetään julkisen avaimen salausta, jolla suo-

jellaan käyttäjiä ja heidän lähettämiä tietoja niin, ettei luvattomat henkilöt pysty niitä kaappaamaan. Yksityisen ja julkisen avaimen parilla ihmisillä on mahdollisuus salata tietoa jota he lähettävät toisilleen. (Peters & Panay, 2015.) Lohkoketjuja käytettäessä jokaisella käyttäjällä on yksityisen ja julkisen avaimen pari. Näitä avaimia tarvitaan, jotta tapahtumia ja transaktioita voidaan toteuttaa, sekä jotta käyttäjillä on pääsy heidän omistuksiinsa. Yksityistä avainta käytetään siirtojen allekirjoittamiseen ja sitä voisi verrata salasanaan, jota tulee säilyttää salassa ja jota ilman ei ole pääsyä omistuksiin. Julkista avainta hyödynnetään verkossa tapahtuviin siirtoihin. Ne ovat kryptografisesti toteutettuja osoitteita, jotka on tallennettu lohkoketjuun. Näiden osoitteiden avulla erilaisia digitaalisten hyödykkeiden siirtoja on mahdollista toteuttaa. Julkiset avaimet ovat nähtävillä kaikille verkossa oleville ja niiden avulla kaikkia entisiä siirtoja voidaan tarkastella myöhemmin. (Zheng ym., 2017.) Julkiset avaimet eivät ole kuitenkaan varsinaisesti sidottu käyttäjän oikeaan identiteettiin, joten toimiminen on anonyymiä (Pilkington, 2015). Toisaalta, kuten aiemmin mainitsimme, on lohkoketjuja erilaisia. Näin ollen esimerkiksi anonymiteettiä ei voida pitää täysin oletusarvoisena, jos puhumme laajasti kaikista lohkoketjuista.

3.3 Konsensusmenetelmät

Lohkoketju on tietorakenteena hajautettu arkkitehtuuri ja jotta uutta tietoa voidaan lisätä tietokantaan turvallisesti, tarvitaan osapuolten välille riittävä konsensus. Keskitetyssä arkkitehtuurissa yksittäinen toimija ylläpitää ja muokkaa tietokantaa. Lohkoketjuteknologiassa taas jokaisella osallistujalla on oma sananvalta siitä, miten he ajattelevat tapahtumien todellisen kulun. Kyseessä on eräänlainen demokratia, jossa kannustetaan toimimaan yhtenäisen konsensuksen puolesta. (Mattila, 2016.) Riittävän konsensuksen aikaansaamiseksi käytetään erilaisia konsensusalgoritmeja, eli erilaisia menetelmiä, joiden avulla ratkaistaan konsensusongelma (Zheng ym., 2017). Yleisesti tunnettu ongelma on niin kutsuttu bysanttilaisten kenraalien ongelma, jossa hajautetun järjestelmän kaikkiin solmuihin ei voida luottaa, vaan osan ajatellaan toimivan vihamielisesti ja häiritsevän järjestelmän toimintaa. Ideaalisessa tilanteessa tiettyä algoritmia suoritettaisiin ympäristössä, jossa ei tapahdu ongelmia ja sen toimivuus on taattu. Reaalimaailmassa tämän ideaalitilanteen saavuttaminen on kuitenkin hyvin harvinaista. (Virkkala, 2007.) Lohkoketjussa järjestelmän toimijoiden, eli solmujen ei tarvitse luottaa toisiinsa. Konsensus ongelmaksi muodostuu tilanne, jossa solmujen joukossa on toimijoita, joiden tarkoitusperät ovat epärehellisiä tai vilpillisiä. Nämä toimijat saattavat levittää tietoa, joka on valheellista ja tämä tiedon kulkeutuessa eteenpäin se vahingoittaa tai sekoittaa lohkoketjun toimintaa. Bysanttilaisten kenraalien ongelmaa pyritään ratkaisemaan konsensusmenetelmien avulla. Ylipäätänsä konsensusmenetelmien avulla pyritään pitämään järjestelmä käynnissä ja ajan tasalla.

Konsensusmenetelmät on pyritty suunnittelemaan niin, että ne kannustavat käyttäjiä toimimaan oikein ja takaamaan järjestelmän turvallisuus, sekä oikean ja paikkansa pitävän tiedon lisäämisen lohkoketjuun (Li ym., 2017). Toimi-

joiden voida olettaa toimivan täysin vilpittömästi ja yhteisen hyvän puolesta, siksi tarvitaan konsensusmenetelmiä. Samoin on hyvä huomioida, että lohkoketjut ovat ihmisten suunnittelemia järjestelmiä, joten epärehellistä toimintaa voi tapahtua jo järjestelmän suunnittelu- ja rakennusvaiheessa. Esimerkiksi konsensusmenetelmä on mahdollista suunnitella toimimaan eri tavalla kuin on annettu ymmärtää. Lohkoketjujen luotettavuutta ei siis voida pitää universaalina totuutena. Konsensusmenetelmien pohjimmaisena tarkoituksena voidaan pitää yritystä luoda sellaiset kannustinmallit, että toimijoiden kannattaa toimia vilpittömästi ja yhteisen hyvän puolesta. Tämän takia useimmiten tiedon lisäämisestä ja konsensusprosessiin osallistumisesta maksetaan arvokas palkkio, joka toimii ikään kuin kannustimena tehdä toimia oikein (Li ym., 2017).

Kannustimella, eli hyödyllä viitataan vahvasti peliteoriaan. Catalini ja Gans (2017) mukaan lohkoketjuissa yhdistyy älykkäästi kryptografia ja peliteoria.

> *"Kiteytettynä peliteoria on oppi strategisesta vuorovaikutuksesta sellaisten omaa etuaan ajavien agenttien välillä, jotka pyrkivät toimintansa avulla tuottamaan sellaisia lopputuloksia, joista seuraa heille itselleen suurin mahdollinen hyöty."* (Honkanen, 2015, 11)

Honkanen (2015) mukaan ulkomaailman ilmiöitä tutkiessamme agenteilla tarkoitetaan oikeita ihmisiä ja höydyllä taas mitä tahansa rahan ja onnellisuuden väliltä. Lohkoketjuista puhuttaessa höydyllä tarkoitetaan kryptovaluuttoja, joita voidaan kutsua myös tokeneiksi tai rahakkeiksi. Joissakin tapauksissa, kuten tietyissä luvan vaativissa lohkoketjuissa hyöty voi olla pelkästään mahdollisuus käyttää lohkoketjua.

Konsensus menetelmissä päätöksentekovalta on luovutettu toimijoille, jotka omistavat kryptovaluuttaa järjestelmässä. Rationaalinen ajatus tämän takana on, että nämä toimijat ovat näin ollen soveltuvia järjestelmän turvallisuuden säilyttämiseen. Järjestelmän ongelmat ja turvallisuuden heikentyminen vaikuttaisi tokeneiden arvoon, jolloin toimijat kokisivat taloudellisia tappioita (Bentov ym., 2016). Tilannetta voidaan verrata peliteoriasta tuttuun tilanteeseen, jossa omaa etuaan ajavat agentit pyrkivät toimintansa avulla tuottamaan sellaisia lopputuloksia, joista seuraa heille itselleen suurin mahdollinen hyöty. Tässä tutkielmassa esitellään kaksi yleisesti tunnetuinta ja käytetyintä konsensus menetelmää.

3.3.1 Proof-of-Work

Yleisin konsensus menetelmä on proof-of-work (PoW), jossa hyödynnetään koneiden laskentatehoa uuden tiedon lisäämiseen ja yhteisen konsensuksen ylläpitämiseen lohkoketjussa. O'Dwyer ja Malone (2014) kuvailevat louhintaa toiminnaksi, jonka avulla lohkot ketjutetaan toisiinsa, sekä taataan käyttäjien tiedonsiirto turvallisesti. Useassa tapauksessa louhinnan tuloksena syntyy lisää

kyseisen järjestelmän rahakkeita. Yksittäinen käyttäjä voi harjoittaa louhintaa esimerkiksi näytönohjaimilla tai prosessoreilla.

Louhinnassa yksittäiset solmut käyttävät laitteidensa laskentatehoa ja pyrkivät löytämään ratkaisun eräänlaiseen matemaattiseen tehtävään. Sillä solmulla, jolla on eniten laskentatehoa, on myös paras mahdollisuus ratkaista tehtävä. Ensimmäiseksi oikean vastauksen löytänyt solmu lähettää sen tarkistettavaksi koko muulle verkolle ja jos vastaus on oikein, palkitaan tämä solmu ennalta määrätyllä palkkiolla. Tämä palkkio yhdistettynä transaktiomaksuihin, joita on mahdollisesti sisällytetty siirtoihin toimivat louhijoiden kannustimina. Louhintaan osallistuvilla solmuilla on siis kannustimena palkkio ja louhinta voidaan nähdä kannattavana niin pitkään, kun louhinnasta saatava palkkio ylittää siihen käytettävät kustannukset, kuten esimerkiksi sähkönkulutuksen. Lohkoketjut, jotka käyttävät PoW -menetelmää ovat juuri niin turvallisia kuin se laskentatehon määrä, joka louhintaan kyseisessä lohkoketjussa käytetään. (Catalini & Gans, 2017.)

Proof-of-work -konsensus menetelmää voidaan ajatella myös datana, jota on kallista tai aikaa vievää tuottaa, mutta jota muiden on helppo todentaa. Prosessina siihen tarvitaan keskimäärin paljon kokeiluja ja virheitä, ennen kuin sitä voidaan pitää täysin validina (Lin & Liao, 2017). Vaatiessaan paljon laskentatehoa, voidaan menetelmää kritisoida sen sähkönkulutuksesta ja kustannuksista. Dinh ym. (2017) toteavat, että PoW on ei-determinisminen ja laskennallisesti kallis, joten se ei sovellu esimerkiksi pankki- ja finanssialan sovelluksille, joiden on hoidettava paljon tapahtumia, eikä niissä ole tilaa satunnaisuudelle. Myös skaalautuvuus on nostettu erittäin kiireelliseksi huolenaiheeksi lohkoketjuissa, jotka käytävät proof-of-work -menetelmää (Croman ym, 2016).

3.3.2 Proof-of-stake

Proof-of-stake (PoS) konsensusmenetelmässä ei käytetä laskentatehoa. Louhinta toteutetaan käyttämällä järjestelmän omaa kryptovaluuttaa. Proof-of-stake menetelmässä louhija asettaa tietyn määrän rahakkeita ikään kuin panokseksi, todentaakseen mikä tilikirjan kopioista on oikea. Päätäntävalta lohkoketjun ylläpidosta on tässäkin menetelmässä siirretty niille henkilöille, jotka omistavat kyseisen järjestelmän rahakkeita. Proof-of-stake menetelmä ratkaisee Proof-of-work menetelmästä syntyneet ongelmat sähkönkulutuksesta ja kustannuksista. Kyseinen menetelmä ei kuitenkaan ole täysin aukoton. Yksittäisen tekijän tai ryhmän omistaessa yli 50% prosenttia tokeneista, on mahdollista syntyä tilanne, jossa voi tapahtua väärinkäytöksiä. Lähtökohtaisesti tämän tyyppistä tilannetta voitaisiin pitää erittäin kalliina toteuttaa. Rahakkeen jakelun aikana voi kuitenkin tapahtua suhteettomia voimasuhteita, joissa yksittäiset toimijat omistavat valtavan osuuden tokeneista ja näin ollen päätäntävallasta. (Bentov, 2016.)

4 LOHKOKETJUTEKNOLOGIAN HYÖDYNTÄMINEN

Tässä luvussa tarkastellaan lohkoketjuteknologiaa ja sen hyödyntämistä yritysten näkökulmasta. Luvussa tutkitaan, minkälaisia mahdollisuuksia lohkoketjuteknologian onnistunut hyöydyntäminen mahdollistaisi yrityksille ja organisaatioille, sekä minkälaisia hyötyjä lohkoketjuissa on verrattuna perinteisiin tietokantaratkaisuihin. Luvussa kartoitetaan lohkoketjuteknologian mahdollisuuksia eri toimialoillle, sekä haasteita, jotka liittyvät lohkoketjueknologiaan yritysten näkökulmasta. Luvussa perehdytään myös lohkoketjuteknologian nykytilaan.

4.1 Lohkoketjuteknologia yritysten näkökulmasta

Lohkoketjuteknologia ja sen onnistunut hyödyntäminen mahdollistaisi yrityksille uusien palveluiden kehittämisen. Lohkoketjuteknologia voi tukea nykyistä liiketoimintaa, tai vastaavasti olla haasteena nykyisille liiketoimintamalleille. (Kavakand, Kost De Sevres & Hilton, 2017). Zheng ym. (2017) mukaan lohkoketjuteknologia on jo tähän päivään mennessä osoittanut potentiaalinsa muokata perinteistä teollisuutta, sillä sen avulla voidaan parantaa tehokkuutta ja turvallisuutta, jonka ansioista siitä on mahdollista hyötyä monella eri toimialla. Toisaalta Lindman ym. (2017) kritisoivat, ettei liiketoiminnallisten näkökulmien mahdollisuuksia vielä ymmärretä tarpeeksi hyvin. Glazer ja Bezzenger (2015) mukaan hajautetun konsensuksen järjestelmät voivat muuttaa sitä tapaa millä yritykset, yksilöt ja organisaatiot rakentuvat ja toimivat toistensa kanssa. Myös Kavand ym. (2017) toteavat lohkoketjuteknologian olevan mullistamassa tapaa, jolla ihmiset kommunikoivat digitaalisessa maailmassa.

Tarkasteltaessa lohkoketjujen hyötyjä yritysten näkökulmasta, tulee meidän ensin verrata lohkoketjuteknologiaa muihin perinteisiin tietokantaratkaisuihin. Hyvärinen ym. (2017) mukaan perinteisiin tietokantajärjestelmiin verrattuna lohkoketju tarjoaa kattavan ratkaisun eli infrastruktuurin, sovellus- ja esitystasot, joihin muut sidosryhmät, kuten veroviranomaiset, rahoituslaitokset ja

yksittäiset käyttäjät voivat mukautua suhteellisen helposti. Toisin kuin keskitetyissä järjestelmissä, lohkoketjuissa verkkotoiminnot jatkuvat, vaikka yksittäinen solmu hajoaisi. Toisin sanoen tällä tarkoitetaan robustisuutta, joka on yksi lohkoketjujen ominaisuuksista. Lohkoketjuja parissa käyttäjien ei tarvitse luottaa välittäjään tai verkon muihin käyttäjiin. Tämä taas lisää luottamusta. Riittää, että käyttäjät luottavat itse järjestelmään kokonaisuutena. (Nofer ym, 2017). Lohkoketjuja voidaan siis lähtökohtaisesti pitää luotettavina. On kuitenkin huomioitava, että käyttäjien tulee luottaa itse järjestelmään. Järjestelmän tulee siis itsessään saavuttaa jotenkin käyttäjien luottamus. Miten voimme olla varmoja, että järjestelmät suunnitellut taho on luotettava ja hänen tarkoitusperänsä ovat rehelliset?

Tiedon tallennukseen ja siihen suoritettavien tietokantasiirtojen kannalta lohkoketju ei tarjoa mitään uutta, mutta jos järjestelmän keskeiset haasteet liittyvät luottamukseen ja robustisuuteen, tarjoaa lohkoketju uusia mahdollisuuksia. Näiden lisäksi yhtenä ominaisuuksista on lohkoketjujen takaama peruuttamattomuus. (Hyvärinen ym., 2017). Tämä tarkoittaa, että lähtökohtaisesti tiedon ollessa hyväksytty ja tallennettuna lohkoketjuun, on tietoa hyvin vaikea manipuloida tai muuttaa. Käytännössä tiedon manipulointi vaatisi, että yksittäinen toimija omistaisi yli 50% verkon laskentatehosta ja pystyisi sen avulla muuttamaan tai poistamaan lohkoketjuun tallennettua tietoa (Hoffman ym., 2017). Vastaavasti keskitetyissä järjestelmissä ei voida puhua peruuttamattomuudesta, sillä luotettu osapuoli voi halutessaan manipuloida, muuttaa, tai poistaa tietoja. Todettakoon, että peruuttamattomuus voidaan nähdä hyvänä ominaisuutena niin kauan, kun mikään ei mene vikaan. Virheellisen tiedon tallentuessa lohkoketjuun, tulee siitä helposti ongelma. Erityisesti yritysten näkökulmasta sellaisten virheiden, kuten esimerkiksi varojen siirtämisen väärälle tilille voisi muodostua ongelmaksi. Myös tietosuoja asettaa omat haasteensa, sillä lohkoketjuun tallennettua väärää, tai arkaluontoista tietoa ei välttämättä saada sieltä enää pois. Hyvärinen ym. (2016) mukaan muissa järjestelmissä kyseiset virheet on helppo korjata käsin, mutta lohkoketjuissa tämä ei lähtökohtaisesti ole mahdollista. Edellä mainittujen ominaisuuksien lisäksi läpinäkyvyys eli lohkoketjuun tallennettujen tietojen avoimuus on olennainen osa lohkoketjuja. Tiedon läpinäkyvyyden määrä ja katseluoikeudet ovat kuitenkin määriteltävissä riippuen lohkoketjusta. (Wust ym, 2017.)

Lohkoketjut eroavat nykyisistä keskitetyistä palvelinratkaisuista ja pilviarkkitehtuureista. Mattila ja Seppälä (2015) mukaan nykyiset keskitetyt palvelinratkaisut sekä hajautetut pilviarkkitehtuurit ovat monissa tapauksissa hyviä ratkaisuja, mutta ongelmaksi muodostuvat älykkäät tuotteet ja palvelut, joiden hinnat ovat huokeita ja elinkaari pitkä. Nykyiset palveluratkaisut ovat usein liian raskaita ja kalliita näihin käyttötarkoituksiin. Wust ym. (2017) taas toteavat, että avoimen tai luvan vaativan lohkoketjun käyttäminen on järkevää ainoastaan silloin, kun toisiinsa luottamattomat toimijat haluavat olla vuorovaikutuksessa ja pitää yllä järjestelmää, mutta eivät ole valmiita luottamaan verkossa toimivaan kolmanteen osapuoleen. Keskitetyissä järjestelmissä suorituskyky, eli viive ja läpimenoaika ovat yleensä paljon nopeampia verrattuina lohkoketjuihin, sillä konsensusmenetelmät aiheuttavat ylimääräistä monimutkaisuutta. Toisaalta on mahdollista, että lohkoketjuteknologian ratkaisut ovat yrityksille kustan-

nustehokkaampia verrattuna keskitettyihin ratkaisuihin. (Davidson, De Filippi & Potts, 2016.)

Lohkoketjuteknologia nousee usein esiin puhuttaessa uudenlaisesta rahansiirrosta. Korpela ym. (2017) mukaan lohkoketjuteknologia näyttää pystyvän tarjoamaan turvallisuutta ja joustavuutta halvemmalla verrattuna perinteisiin rahansiirtomenetelmiin. Pilkingtonin (2015) mukaan nykyisessä pankkijärjestelmässä kansainvälisillämaksuilla voi kestää useita päiviä ja niiden toteuttaminen voi olla kallista pankeille. Lohkoketjuteknologian avulla samat maksut voidaan suorittaa hetkessä ja minimoiduilla kustannuksilla. Maksujen toteuttaminen lohkoketjuteknologian avulla olisi siis nopeampaa, sekä kustannustehokkaampaa verrattuna nykyisiin järjestelmiin. Myös Nowinski ja Kozma (2017) toteavat, että transaktioiden nopeampi toteutus parantaa toiminnan tehokkuutta, sekä laskee operatiivisia kustannuksia. Peters ja Panay (2016) mukaan pankkialalla on lukuisia sellaisia toimintoja, joihin lohkoketjuteknologiasta voi olla hyötyä, kuten esimerkiksi kirjanpidossa, transaktioprosesseissa ja kaupankäynnissä. Mahdollisuudet eivät kuitenkaan rajoitu pelkästään edellä mainittuihin. Suikkanen (2017) mukaan lohkoketjuteknologia hyödyttää vähentämällä tuotantokustannuksia, muokkaamalla organisaation rakennetta ja poistamalla sellaisia tasoja joita ei tarvita. Tätä kautta myös organisaation tehokkuus paranee.

Ymmärtääksemme paremmin lohkoketjuteknologian vaikutuksia yritysten näkökulmasta, tulee meidän tarkastella teknologian vaikutuksia laajemmin, kuin vain vertaillen lohkoketjuja perinteisiin tietokantamalleihin. Suikkanen (2017) mukaan lohkoketjuteknologialla on kyky synnyttää kokonaan uusia markkinoita. Tämä tarkoittaa sitä, että lohkoketjuteknologian avustuksella sellaisten tuotteiden ja palveluiden vaihto, joka ei ennen ollut kannattavaa tai merkityksellistä helpottuu. Yrityksille tämä taas tarkoittaa kasvavia voittoja. Toisaalta uusien tuotteiden ja palveluiden tullessa markkinoille, tietyt yritykset joutuvat uudelleen muuttamaan liiketoimintaansa, sillä lohkoketjuteknologia heikentää heidän tarjoamiaan palveluita (Nowinski & Kozma 2017).

Lohkoketjuteknologialla on vaikutuksia olemassa oleviin liiketoimintamalleihin, sillä sen avulla kyetään todentamaan kauppatavaroita entistä paremmin. Kauppatavaroiksi lasketaan kaikki aineelliset ja aineettomat tuotteet ja palvelut. Kauppatavaroiden aitoutta voi olla vaikea todentaa ja se muodostuu ongelmaksi, jos kauppatavaroiden brändiarvo on korkea tai todentamisen tarve vahva. (Nowinski & Kozma, 2017.) Todentaminen liittyy vahvasti myös logistiikka- ja tuotantoketjuihin. Todentamiseen liittyviä lohkoketjupohjaisia ratkaisuja toteuttavat muun muassa ShipChain, Provenance ja Everledger. Nämä yritykset hyödyntävät lohkoketjuteknologiaa jäljentämään ja tallentamaan tuotteiden logistiikka- tai tuotantoketjuja.

Logistiikka- ja tuotantoketjujen lisäksi lohkoketjuteknologia helpottaa välillistä toimintaa. Tällä tarkoitetaan välikäsiä ja ylimääräistä paperityötä, joka tuo mukanaan tehottomuutta. Lohkoketjuteknologialla voidaan poistaa välikäsiä ja niiden aiheuttamia kustannuksia. Parhaimmillaan tämä saattaa aiheuttaa jopa uutta liiketoimintaa, joka ei olisi mahdollista välikäsien läsnä ollessa. (Nowinski & Kozma, 2017.) Juuri välikäsien aiheuttamien kustannuksien ja paperityön karsimisesta pankit ovat kiinnostuneita. Kuten IBM (2016) toteuttamassa tutkimuksessa todettiin, juuri pankki- ja finanssiala ottaneet lohkoketjuteknolo-

giaa käyttöön huomattavasti oletettua nopeammin. Esimerkiksi Osuuspankki ja Nordea ovat osa kansainvälistä R3-konsortiota, joka tutkii ja kehittää lohkoketjuteknologian ratkaisuja finanssisektorille. R3-konsortion kehittämä Corda on avoimen lähdekoodin alusta, joka on suunniteltu yritysten käyttöön erityisesti rahoitusalalla (Corda, 2017). Osuuspankki ja Nordea ovat myös yhteistyössä suomalaisen Tomorrow Labsin kanssa kehittämässä järjestelmää, jossa asunto-osakekirjat voidaan säilyttää lohkoketjussa (Helsingin Sanomat, 2017).

Lohkoketjuteknologialle on hahmoteltu monia käyttötapauksia sosiaali- ja terveydenhuollossa. Nämä käyttötapaukset liittyvät tietojen käsittelyyn ja turvaamiseen, maksuliikenteeseen ja sähköisiin sosiaali- ja terveyspalveluihin (Salonen ym., 2018). Esimerkki käytännön toteutuksista on Mediledger, joka on lääketeollisuudelle suunnattu yksityinen lohkoketjualusta. Alustan tarkoituksena on valvoa lääkkeiden toimitusketjua ja sitä kautta taata, että lääkkeiden hinnat ovat aina säädeltyjä (Mediledger, 2018). Toinen esimerkki on Dentacoin, joka on hammasalalle suunnattu sovellus, jossa käyttäjiä palkitaan heidän tuottamastaan tiedosta liittyen palvelun laatuun ja arviointiin (Dentacoin, 2018).

Isot monikansalliset yritykset kuten IBM, Amazon ja Microsoft ovat myös huomanneet lohkoketjuteknologian mahdollisen potentiaalin. Nämä yritykset tarjoavat lohkoketjupalveluna ratkaisuja (Blockchain as a Service, BaaS), eli pilvipohjaisia kehitysympäristöjä lohkoketjujen kehittäjille. Näitä kaupallisia lohkoketjuteknologioita ovat esimerkiksi Hyperledger ja Microsoft Azure BaaS.

4.2 Lohkoketjuteknologian nykytila

Vuonna 2015 The Economist kuvaili lohkoketjuteknologian ja hajautetun kirjanpidon avaavan monia kokonaan uusia mahdollisuuksia. Gartnerin ”The Hype Cycle for Emerging Technologies 2017” –tutkimuksen mukaan lohkoketjuteknologia on yksi nousevista teknologioista ja sen oletetaan adaptoituvan valtavirran omaksumaksi seuraavan 5-10 vuoden aikana. Lansiti ja Lakhani (2017) mukaan vuonna 2017 lohkoketjuteknologian adaptoituminen on jo vahvassa käynnissä finanssialalla ja tulee hyvin suurella todennäköisyydellä vaikuttamaan liiketoimintaan myös monilla muilla eri toimialoilla.

Thomond ja Lettice (2002) mukaan termiä murroksellinen (disruptive) innovaatio käytetään kuvaamaan innovaatiota, jolla on vallankumouksellinen luonne. Murrokselliselle teknologialle on ominaista suoriutua alkuun vakiintuneita tuotteita heikommin, mutta samalla herättäen kiinnostusta kokonaan uusissa asiakkaissa, joilla ei välttämättä ole ollut aikaisemmin mahdollisuutta käyttää kyseistä tuotetta. Murroksellisen innovaation tuotteille ominaisia piirteitä ovat: edullisuus, yksinkertaisuus ja kätevämpi käyttö. Vaikka murrokselliset innovaatiot alisuoriutuvat alkuun, kehittyvät ne lopulta valtamarkkinoille täysin kilpailukykyisiksi. (Christensen 1997.) Pilkington (2015) kuvaa lohkoketjuteknologiaa murroksellisena teknologiana. Murroksellisen teknologian lisäksi se on myös perustavanlaatuinen teknologia, jolla on mahdollisuus mullistaa rajapintaa taloudellisten toimijoiden välillä (Pilkington, 2015.) Lansiti ja Lakha-

ni (2017) mukaan lohkoketju ei ole murroksellinen teknologia vaan se voidaan nähdä ennemmin perustavana (foundational) teknologiana. Murroksellinen teknologia synnyttää lyhyessä ajassa uusia markkinoita, jotka muuttavat täysin jo olemassa olevia. Perustava teknologia synnyttää yhtä lailla uusia markkinoita ja liiketoimintamalleja, mutta niiden adaptoituminen ja kehitys taloudellisen ja sosiaalisen infrastruktuurin järjestelmiin vie vuosia, ellei jopa vuosikymmeniä. Lansiti ja Lakhani (2017) uskovat teknologian omaksumisen olevan tasaista ja maltillista, mutta sen vaikutuksien olevan valtavia; koskettaen sosiaalisia, taloudellisia ja poliittisia järjestelmiä.

IBM (2016) julkaiseman tutkimuksen mukaan pankit ja finanssiala ovat ottaneet lohkoketjuteknologiaa käyttöön huomattavasti nopeammin kuin alun perin on ajateltu. Tutkimuksessa kartoitettiin 200 pankkia 16 eri valtiosta. IBM (2016) mukaan vuoden 2017 aikana 15% prosentilla pankeista oletetaan olevan lohkoketju kaupallisessa tuotannossa. Esimerkiksi SWIFT ja Visa ovat kehittämässä karkeaa prototyyppiä hyödyntäen lohkoketjuteknologiaa kansainvälisiin maksuihin (SWIFT, 2017.). Vaikka käyttöönotto on ollut odotettua nopeampaa, voidaan todeta, että suurin osa pankeista ovat vielä testausvaiheessa ja pyrkivät miettimään, miten he voivat hyödyntää lohkoketjuteknologiaa tuotteissaan ja palveluissaan.

Wörner ym. (2016) kritisoivat nykyisten lohkoketjuteknologiaan pohjautuvien toteutuksien olevan vain kopioita toisistaan pienillä parametrisillä eroilla. Myös Mattila (2016) toteaa, että tällä hetkellä vain pieni osa lohkoketjuteknologian parissa työskentelevistä yrityksistä keskittyvät varsinaisen lohkoketjuteknologian kehittämiseen. Toisaalta Wörner ym. (2016) toteavat, että tällä hetkellä on myös kehitystä, jolla on potentiaalia viedä teknologiaa ja sovelluksia huomattavasti eteenpäin.

Lohkoketjuteknologian tutkimuksessa on omat haasteensa ja rajoituksensa, joihin on törmätty myös tätä tutkimusta tehdessä. Lohkoketjuteknologian tutkimus on tähän asti keskittynyt pääasiassa Bitcoiniin. Yli-Huumo, Ko, Choi, Park ja Smolanderin (2016) julkaisemassa tutkimuksessa on käyty läpi 41 tutkimusartikkelia jotka tarkastelevat lohkoketjuteknologiaa sen teknologisen toteutuksen perspektiivistä. Tutkimuksen mukaan 80% prosenttia papereista liittyvät Bitcoiniin ja loput 20% muihin lohkoketjupohjaisiin sovelluksiin. Myös Zheng ym. (2017) toteavat lohkoketjuteknologian tutkimukset liittyvän pääasiassa Bitcoiniin. Lindman, Rossi ja Tuunainen (2017) peräänkuuluttavat kiireellistä tarvetta teorian ja käytännön tutkimukselle lohkoketjuteknologiasta.

Jotta lohkoketjuteknologian haasteita ja rajoituksia voitaisiin tunnistaa ja ratkaista, tulisi lohkoketjuteknologian ratkaisuja tutkia laajemmalti. Teknisestä näkökulmasta nykyiset tutkimukset keskittyvät pääasiassa haasteisiin ja rajoituksiin; kuten skaalautuvuuteen, turvallisuuteen, yksityisyyteen ja suorituskykyyn. Suurin osa tutkimuksista keskittyy lohkoketjuteknologiaan yksityisyyden ja turvallisuuden näkökulmasta. Joitakin teknisiä haasteita ja rajoituksia on jätetty kokonaan tutkimatta. (Yli-Huumo ym., 2016.).

Myös lohkoketjuteknologian terminologian todetaan olevan puutteellista. Virallinen ja standardisoitu terminologia puuttuu, sillä lohkoketjuteknologiaa käytetään monella eri alustalla. Tämän lisäksi akateeminen kirjallisuus on tähän mennessä kirjoitettu joko puhtaasti teknisestä näkökulmasta tai taloudellisesta

näkökulmasta. (Krujiff & Weigand, 2017). Krujiff ja Weigand (2017) toteavat terminologian kehityksen vaativan tavallisten internet käyttäjien ja yritysjohtajien perustavanlaatuista ymmärrystä lohkoketjuteknologian toiminnasta ja vaikutuksista. Tämän perusteella voidaan olettaa, että tarkempi tutkimus ja terminologia tulee kehittymään lohkoketjuteknologian adaptoituessa yleisempään käyttöön.

Gartner (2017) arvio lohkoketjuteknologian olevan siirtymässä vaiheesta, jossa se on noussut hypen huipulle (Peak of Inflated Expectations) kohti vaihetta, jossa kiinnostus laskee, kun teknologian kokeilut epäonnistuvat (Through of Disillusioment). Tämän arvion pohjalta lohkoketjuteknologiaan kohdistuneen innostuksen huippu olisi juuri nähty ja olisimme matkalla kohti vaihetta, jossa investoinnit teknologiaan jatkuvat vain, jos tekniikkaa onnistutaan parantamaan. Käytännössä tämä tarkoittaisi siis edellä mainittujen haasteiden ratkaisemista, sekä laajempaa kehitys- ja tutkimustyötä.

5 YHTEENVETO

Tässä tutkielmassa selvitettiin, mitä on lohkoketjuteknologia, miten se on kehittynyt ja miten sitä pyritään määrittelemään. Tutkielmassa selvitettiin lohkoketjujen toimintaperiaatteita ja niiden rakennetta. Erityisesti tutkimuksessa selvitettiin lohkoketjuteknologiaa yritysten näkökulmasta. Tutkielmassa esitettiin kaksi tutkimuskysymystä, jotka olivat: ”Mitä on lohkoketjuteknologia?” sekä ”Miten lohkoketjuteknologia tulisi huomioida yritysten näkökulmasta?”. Tutkielma toteutettiin kirjallisuuskatsauksena ja sen lähteinä toimivat useat tieteelliset artikkelit ja julkaisut, sekä erilaiset lehtiartikkelit ja valkopaperit, joissa käsiteltiin lohkoketjuteknologiaa tai niitä osia ja ilmiöitä, mistä lohkoketjuteknologia muodostuu.

Tutkielman toisessa luvussa vastattiin kysymykseen mitä on lohkoketjuteknologia. Luvussa esiteltiin lohkoketjuteknologian historiaa ja kehitystä, sekä pyrittiin selvittämään sitä, miten lohkoketjuteknologiaa määritellään. Luvussa esiteltiin myös erilaisia lohkoketjuja. Kolmannessa luvussa esiteltiin tarkemmin lohkoketjun toimintaperiaatetta ja rakennetta. Luvussa tarkasteltiin yksittäistä lohkoa ja selvitettiin avoimiin lohkoketjuihin liittyviä konsensus menetelmiä. Neljännessä luvussa vastattiin kysymykseen ”miten lohkoketjuteknologia tulisi huomioida yritysten näkökulmasta?”. Luvussa esiteltiin lohkoketjuteknologian nykytilaa, selvitettiin olemassa olevia toteutuksia, sekä haasteita ja mahdollisuuksia yritysten näkökulmasta.

Tutkielman tuloksina kysymykseen mitä on lohkoketjuteknologia, voidaan todeta, että kyseessä on sekoitus olemassa olevia teknologisia ratkaisuja, joita yhdistelemällä saadaan luotua lohkoketjuja. Lohkoketjut voidaan nähdä tietokantoina, tai tarkemmin osana hajautetun tilikirjan ratkaisuja. Lohkoketjuissa tehdyt muutokset käsitellään ja hyväksytään ennalta määritellyin säännöin, jonka jälkeen niistä kootaan paketteja, joita kutsutaan lohkoiksi (Mattila & Seppälä, 2015). Nämä lohkot kiinnitetään toisiinsa, jonka avulla yksittäisistä lohkoista muodostuu lohkoketju. Ominaista lohkoketjuille on, että ne ovat hajautetusti hallinoituja, sekä muuttumattomia tietokantoja. Olennaista kuitenkin on, että lohkoketjuja on hyvin erilaisia ja ne eroavat ominaisuuksiltaan toisistaan, joten niiden ominaisuudet vaihtelevat, eikä yhtä tiettyä ja tarkkaa määrittelyä voi tehdä isolle joukolle erilaisia lohkoketjuja. Karkeasti lohkoketjut voi-

daan jakaa kahteen ryhmään: avoimiin ja luvan vaativiin lohkoketjuihin, joiden ominaisuudet ja toimintaperiaatteet poikkeavat ainakin osittain toisistaan (Wust & Gervais, 2017). Näin ollen, erilaiset lohkoketjut soveltuvat erilaisiin käyttötarkoituksiin. Lohkoketjuteknologiaa voidaan pitää käsitteenä, joka pitää sisällään erilaiset lohkoketjut, sekä ne teknologiat ja toimintaperiaatteet, joita lohkoketjut tarvitsevat toimiakseen.

Tutkielmassa esiteltiin muutamia lohkoketjuille olennaisia tekniikoita ja teknologiaratkaisuja. Yhtenä olennaisista tekniikoista ovat kryptografiset menetelmät. Kryptografisia menetelmiä voidaan pitää lohkoketjuille olennaisena tekniikkana, sillä lohkoketjuteknologia hyödyntää kryptografiaa tiivisteiden, digitaalisten allekirjoitusten ja julkisen avaimen salausmenetelmän parissa (Bonneau ym., 2015). Käytännössä nämä menetelmät edesauttavat tiedon lähettämistä salatusti, ilman että kolmannet osapuolet pystyvät sitä manipuloimaan tai kaappaamaan. Kryptografiset menetelmät ovat olennainen osa lohkoketjujen toimintaa ja osa niitä olemassa olevia teknologisia ratkaisuja, joita yhdistelemällä saadaan luotua lohkoketjuja. Toinen olennainen tekniikka on konsensusmenetelmät. Konsensus menetelmien avulla pyritään ratkaisemaan ongelma, jossa kaikkiin järjestelmän toimijoihin ei voida luottaa, vaan heidän joukossaan voi olla toimijoita, jotka toimivat epärehellisesti ja levittävät väärää tietoa. Tätä ongelmaa nimitetään myös bysanttilaisten kenraalien ongelmaksi ja sitä ilmenee erityisesti hajautetuissa järjestelmissä, joissa uutta tietoa tulee lisätä tietokantaan turvallisesti. Käytännössä tätä ongelmaa pyritään ratkaisemaan luovuttamalla päätöksentekovalta toimijoille, jotka omistavat kyseisen järjestelmän kryptovaluuttaa, eli rahakkeita. Nämä rahakkeet toimivat eräänlaisena kannustimena toimia oikein, sillä ongelmat ja turvallisuuden heikentyminen vaikuttaisi negatiivisesti rahakkeen arvoon, jolloin toimijat kokisivat taloudellisia tappiota (Bentov ym., 2016). Konsensus menetelmiä on olemassa erilaisia, mutta kaksi yleisesti eniten käytettyä ovat Proof-of-work ja Proof-of-stake. Kiteytettynä Proof-of-work hyödyntää laskentatehoa konsensuksen ylläpitämiseen, kun taas Proof-of-stake menetelmässä ei käytetä laskentatehoa, vaan lohkoketjun omaa kryptovaluuttaa, ikään kuin panoksena.

Tutkielman tuloksena kysymykseen miten lohkoketjuteknologia tulisi huomioida yritysten näkökulmasta, voidaan todeta, että lohkoketjuteknologian onnistunut hyödyntäminen mahdollistaisi yrityksille uusien palveluiden kehittämistä, mutta nykyisten toimintojen korvaamien lohkoketjuteknologialla useimmiten tuskin on kannattavaa. Suikkanen (2017) nosti esiin lohkoketjuteknologian kyvyn synnyttää kokonaan uusia markkinoita, joka mahdollistaisi uusien tuotteiden ja palveluiden kehittämistä. Toisaalta tämä olisi hyvä huomioida myös haasteena, sillä uudet markkinat saattaisi vaikuttaa nykyisten yritysten liiketoimintaan myös negatiivisesti. Liiketoiminnallisten näkökulmien vaikutuksista ei vielä voida olla täysin varmoja. Lindman (2017) kritisoikin, ettei niitä ymmärretä vielä tarpeeksi hyvin. Eri toimialoilla on kuitenkin otettu lohkoketjuteknologiaa käyttöön viime vuosina. Näitä toimialoja ovat pankki- ja finanssiala, logistiikka, sosiaali- ja terveysala, sekä teknologia-ala, jossa erityisesti isot monikansalliset toimijat ovat rakentaneet omia lohkoketjuteknologiaan liittyviä palveluja. Perinteisiin tietokantajärjestelmiin verrattuna lohkoketjut tarjoavat kattavan ratkaisun, joka edesauttaa useiden eri toimijoiden mukautu-

misen siihen. Tämä edesauttaa uusien alustojen ja konsortioiden luomista, sekä uusien palveluiden kehittämistä. Erityisesti älykkäät tuotteet ja palvelut ovat keskiössä, sillä nykyiset keskitetyt palvelinratkaisut ja hajautetut pilviarkkitehtuurit eivät aina sovellu niihin tarpeeksi hyvin.

Tehokkuus ja turvallisuus olivat sellaisia ominaisuuksia ja höytyjä, jotka nousivat tutkimuksessa esille, kun tarkasteltiin lohkoketjuteknologiasta saatavia hyötyjä yritysten näkökulmasta. Tehokkuus liittyy pääasiassa välikäsien poistamiseen ja turvallisuus taas kryptografian hyödyntämiseen. Tiedon tallennuksen ja tietokantasiirtojen näkökulmasta lohkoketjut eivät tarjoa yrityksille valtavasti uusia mahdollisuuksia. Erityisesti avoimet lohkoketjut vaativat paljon resursseja, jotta ne toimisivat ja pysyisivät turvallisina. Keskitetyt tietokannat ovat tehokkaampia ja virheiden sattuessa ne ovat helpommin korjattavissa. Lohkoketjujen muuttumattomuus voidaan laskea monessa tapauksessa haasteeksi, sillä lisättyä tietoa ei välttämättä saada enää pois lohkoketjusta. On kuitenkin hyvä huomioida, että lohkoketjuja on erilaisia ja niiden ominaisuuksien puitteissa tietyt lohkoketjut toimivat tiettyyn tarkoitukseen ja toiset eivät. Yleisesti tunnistettuja teknisiä haasteita ovat skaalautuvuus, turvallisuus, yksityisyys ja suorituskyky. Lohkoketjuteknologian parissa toimivien toimijoiden on kyettävä ratkaisemaan nämä ongelmat. Tämän lisäksi lohkoketjuteknologiaa tulee tutkia vielä tarkemmin ja yleinen ymmärrys teknologiaa kohtaan on kasvettava, jotta lohkoketjuteknologia adaptoituisi ihmisten ja yritysten yleisempään käyttöön.

Edellä mainitut haasteet antavat hyvää suuntaa jatkotutkimukselle: tekniset haasteet, kuten skaalautuvuus ja suorituskyky ovat hyvin oleellisia asioita liittyen lohkoketjuteknologian kehitykseen ja adaptoitumiseen. Näitä teknisiä haasteita ja kehittyviä, sekä olemassa olevia ratkaisuja olisi oleellista tutkia tarkemmin. Muita ajankohtaisia jatkotutkimusaiheita voisi olla luvussa 3.3 tutkittujen konsensus menetelmien kehitys, sekä eri konsensus menetelmien soveltuvuus luvanvaraisiin lohkoketjuihin.

LÄHTEET

Arias, M. & Yongseok, S. (2013). There are two sides to every coin—even to the bitcoin, a virtual currency. The Regional Economist, October. Haettu osoitteesta https://www.stlouisfed.org/publications/re/articles/?id=2427

Back, A., Corallo, M., Dashjr, L., Friedenback, M., Maxwell, G., Miller, A., Poelstra, A., Timon, J., &.Wuille, P. (2014). Enabling Blockchain Innovations with Pegged Sidechains. Haeuttu osoitteesta https://blockstream.com/sidechains.pdf

Barber, S., Boyen, X., Shi, E & Uzun, E. (2012). Bitter to Better – How to Make Bitcoin a Better Currency. Teoksessa Financial Cryptography, volume 7397 of Lecture Notes in Computer Science, (399-414). Springer, 2012.

Beck, R., Czepluch, J., Lollike, N. & Malone, S. (2016) Blockchain - The Gateway to trust-free cryptographic transactions. Teoksessa ESICS 2016 Proceedings, Research Papers. 153.

Bellare, M & Rogaway, P. (2005) Intoroduction to modern cryptography. UCSD CSE 207 Course Notes. Haettu osoitteesta http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf

Bentov, I., Gabizon, A. & Mizrahi. (2016) Cryptocurrencies without proof of work. Teoksessa *International Conference of Financial Cryptography and Data security*, 142-157. Springer, 2016.

Bonneau, J., Naraynan, A., Felte, E., Miller, A. & Goldefeder, S. (2016) *Bitcoin and Cryptocurrency Technologies.* New Jersey: Princeton University Press

Buterin, V. *Visions, Part 1: The Value of Blockchain Technology*. Ethereum Blog. Haettu osoitteesta https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

Capgemini Consult. (2016*) Smart Contracts in Financial Services: Getting from Hype to Reality*. Digital Transformation Institute.

Catalini, C & Gans, J. (2016*) Some simple economics of the blockchain*. Technical report, National Bureau of Economic Research.

Chaum, D. (1982). *Blind Signatures for Untraceable Payments*. Haettu osoitteesta https://taler.net/papers/chaum-blind-signatures.pdf

Chohan, U. (2017) *The Double Spending Problem and Cryptocurrencies.* Discussion Paper Series: Notes on the 21st Century

Christensen, C. (1997) *The Innovator`s Dilemma: When New Technologies Cause Great Firms to Fail*. Boston: Harward Business School Press.

Clresearch. (2018). *Blockchain, Identity and CSR in 2018*. Haettu osoitteesta www.clresearch.com/research

Croman, K. Ym. (2016). *On Scaling Decentralized Blockchains. Financial Cryptography and Data Security*. Lecture Notes is Computer Science, vol 960, 106-125.

Davidson, S., De Filippi, P. & Potts, J. (2016) *Economics of blockchain*.

Dentacoin: *The Blockchain Solution for the Globan Dental Industry*. (2018). Whitepaper v.2.0. Haettu osoitteesta https://dentacoin.com/web/white-paper/Whitepaper-en1.pdf

Dinh, T. Ym (2017) *Blockbench: A Framework for Analyzing Private Blockchains*. National University of Singapore, Singapore.

Drainville, D. (2012). *An Analysis of the Bitcoin Electronic Cash System*. University of Waterloo. 10. 2012.

Gartner. (2017) *Gartner Identifies Three Megatrends that will drive digital business into the nect decade*. Haettu osoitteesta https://www.gartner.com/newsroom/id/3784363

Glaser, F & Bezzenger, L. (2015) Beyond Cryptocurrencies – A taxonomy of decentralized consensus systems. Teoksessa *23rd European Conference on Information Systems (ECIS)*, Münster, Germany.

Hoffman, F, Wurster, S., Ron, E., & Böhmecke-Schwafert. (2017). The immutability concept of blockchains and benefits of early standardization. Teoksessa *ITU Kaleidoscope: Challenges for a Data-Driven Society (ITUK)*. 2017.

Honkanen, V. (2015) *Kokeellinen peliteoria ja rahalliset palkkiot* (Pro gradu – tutkielma) Tampereen yliopisto.

Helsingin Sanomat. (2017, 2. marraskuuta). Kohta asunto-osakkeesi on bittivirtaa eikä panttikirjoja tarvitse kiikutella pankista toiseen. Haettu 2.12.2017 osoitteesta https://www.hs.fi/talous/art-2000005433023.html

Huberman, G, Leshno, J., & Moallemi, C. (2017). *Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System*. Bank of Finland Research Discussion Paper No. 27/2017.

Hyvärinen, H, Risius, M., & Friis, G. (2017). *A Blockchain-Based Approach Towards Overcoming Financial Fraud In Public Sector Services*. Business & Information Systems Engineering 59 (6), 441-456.

IBM, (2016). Leading the pack in blockchain banking: Trailblazers set the pace. Haettu 10.12.2017 osoitteesta https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBP03467USEN

Katz, J. & Lindell, Y, (2015). *Introduction to modern cryptography*. Chapman & Hall.

Kavakand, H., Kost De Sevres, N & Hilton, B. (2017) *The Blockchain Revolution: An analysis of regulation and technology related to distributed technologies*. DLA Piper.

Korpela, K, Hallikas, J, & Dahlberg, T. (2017). Digital Supply Chain Transformation toward Blockchain Integration. Teoksessa *Proceedings of the 50th Hawaii International Conference on System Sciences.* 2017.

Kruijff, J & Weigand, H. (2017) Understanding the Blockchain using Enterprise ontology. *Teoksessa Advanced Information Systems Engineering. Lecture Notes in Computer Science, vol 10253*. 2017.

Kuo, T., Kim, H & Ohno-Machado, L. (2017) Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 23 (6). 1211-1220.

Lansiti, M & Lakhani, K. (2017) The truth about blockchain. Harward Business Review. Haettu 10.11.2017 osoitteesta https://hbr.org/2017/01/the-truth-about-blockchain

Lindman, J., Rossi, M & Tuunainen, V. (2017) Opportunities and risks of Blockchain Technologies in payments – a research agenda. Teoksessa *Proceedings of the 50th Hawaii International Conference on System Science HICSS/IEEE Computer Society*. 1533-1542.

Li, X., Jiang, P., Cheng, X., Luo, Q & Wen, A. (2017) *A Survey on the security of blockchain systems*. Future Generation, Computer systems.

Lin, I & Liao, T (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, 19(5), 653-659.

Mattila, J. (2016) *The Blockchain phenomenon – The disruptive potential of distributed consesus architectures*. ETLA working papers numero 38.

Mattila, J & Seppälä, T. (2015). *"Laitteet pilveen – vai pilvi laitteisiin? Keskustelunavauksia teollisuuden ja yhteiskunnan digialustojen uusista kehitystrendeistä"* (Julkaisusarjan osa 44). Helsinki. Elinkeinoelämän tutkimuslaitos.

Mediledger. (2018, 24. huhtikuuta). The Mediledger Project. Haettu 24.4.2018 osoitteesta https://www.mediledger.com/

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Nair, G & Sebastian, S. (2017) BlockChain Technology Centralised Ledger to Distributed Ledger. *International Research Journal of Engineering and Technology*, 04(03), 2823-2827.

Nofer, M., Gomber, P., Hinz, O & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*. 59(3), 183-187.

Nowinski, W & Kozma, M (2017. How Can Blockchain Technology Disrupt the Existing Business Models? *Entrepreneurial Business and Economics review* 5(3). 173-188.

O`Dwyer, K & Malone, D. (2014). Bitcoin Mining and its Energy Footprint. Communication technologies. Teoksessa *25th IET Irish Signals & Systems Conference 2014. IET* (280-285). Limerick, Ireland.

Olnes, S. (2015). Beyond Bitcoin – Public Sector Innovation Using the Bitcoin Blockchain Technology. Teoksessa *NOKOBIT 2015*, 23. Ålesund.

Pilkington, M (2015*). Blockchain Technology: Principles and Applications*. Research Handbook on Digital Transformations.

Peters, G & Panay, E. (2015). Understanding Modern Banking Ledgers through Blockchain technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. *Banking beyond banks and money* (239-278). Springer.

Salonen ym. (2017*). Lohkoketjuteknologian mahdollisuudet ja hyöydyt sosiaali- ja terveydenhuollossa* (Julkaisusarjan osa 80). Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2017.

Storås, N. (2016, 5. huhtikuuta) Lohkoketjuteknologia pähkinäkuoressa – tämä kannattaa tietää. Haettu 12.12.2017 osoitteesta https://www.tivi.fi/Kaikki_uutiset/lohkoketjuteknologia-pahkinakuoressa-tama-kannattaa-tietaa-6537904

Suikkanen, H. (2017). *Economic and Institutional Implications of Blockchain* (Pro-gradu –tutkielma). Aalto yliopisto.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O`Reilly Media, Inc.

The Economist. (2017, 12. joulukuuta). The great chain of being sure about things. Haettu 20.12.2017 osoitteesta https://www.economist.com/news/briefing/21677228-technology-

behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

Thomond, P & Lettice, F. (2002). *Understanding and enabling disruptive innovation*. In proceedings of the British Academy of Management Science 35(3): 321-339.

UK Government. (2016). *Distributed Ledger Technology: beyond block chain*. Government office for science.

Wust, K & Gervais, A. (2017). *Do you need a blockchain?* IACR Cryptology. 375.

Wörner, D., Von Bomhard, T., Schreier, Y & Bilgeri, D. (2016) The Bitcoin Ecosystem: Disruption Beyond Financial Services? *Twenty-Fourth European Conference of Financial Sysytems (ECIS)*. Istanbul, 2016.

Zheng, Z., Xie, S., Dai, H & Wang, H. (2017). *Blockchain Challenges and Opportunites Survey*. International Journal of Electric and Hybrid Vehicles, 1-23.