Jussi Häkkänen

LOHKOKETJUN ROOLI JA POTENTIAALI INNOVAATIONA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Häkkänen, Jussi
Lohkoketjun rooli ja potentiaali innovaationa
Jyväskylä: Jyväskylän yliopisto, 2018, 29 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Clements, Kati

Tutkielma selvittää lohkoketjun roolia innovaationa ja sen potentiaalisia käänteentekeviä vaikutuksia yhteiskuntaan ja talouteen. Tutkielma toteutettiin kirjallisuuskatsauksena. Lohkoketjuun viitataan usein disruptiivisena innovaationa, mutta myös muita määritelmiä, kuten perustava innovaatio ja radikaali innovaatio, esiintyy. Eri innovaatiotyyppien väliset määritelmät eivät ole täysin vakiintuneita, mutta tutkielman perusteella voidaan sanoa, että melko vähän käytetty perustavan innovaation määritelmä sopii hyvin lohkoketjuun. Internetin leviämisen nykyiseen laajuuteensa mahdollistanut internet-protokolla TCP/IP on esimerkki perustavasta innovaatiosta, joka loi pohjan jatkoinnovaatioille, jotka myöhemmin mullistivat tapoja tehdä monia asioita. Tutkielmassa päädyttiin tulokseen, että lohkoketjussa on potentiaalia muuttaa monia asioita tulevaisuudessa, mutta suuriin muutoksiin kuluu todennäköisesti vielä useita vuosia aikaa, koska teknologian kehitys ja laajempi hyödyntäminen ovat vielä hyvin varhaisessa vaiheessa. Lohkoketjun leviäminen jaetaan tutkielmassa neljään eri vaiheeseen; yksittäinen käyttökohde, paikallinen käyttökohde, korvaava teknologia ja muutokseen johtava teknologia. Yksittäisellä käyttökohteella tarkoitetaan teknologian hyödyntämistä yksittäisessä käyttötarkoituksessa, paikallisessa käyttökohteessa teknologiaa hyödynnetään paikallisesti, korvaavalla teknologialla tarkoitetaan tilannetta, jossa teknologia tarjoaa uuden korvaavan tavan tehdä jokin vanha asia ja muutokseen johtavalla teknologialla tarkoitetaan tilannetta, jossa teknologia mahdollistaa täysin uusien asioiden tekemisen. Lohkoketjuteknologiassa on potentiaalia käydä kaikki nämä vaiheet läpi, mutta tällä hetkellä teknologiaa hyödynnetään lähinnä yksittäisissä käyttökohteissa ja paikallisesti.

Asiasanat: lohkoketju, älysopimus, teknologinen innovaatio, disruptiivinen innovaatio, perustava innovaatio

ABSTRACT

Häkkänen, Jussi
The role and the potential of blockchain as an innovation
Jyväskylä: University of Jyväskylä, 2018, 29 p.
Information Systems, bachelor's thesis
Supervisor(s): Clements, Kati

This thesis aims to clarify type and potential of blockchain as an innovation and potential social and economic impacts it may have. The thesis was conducted as a literature review. Blockchain is often referred to as a disruptive innovation, however, other types of definitions such as foundational innovation and radical innovation have been used as well. Typology around technological innovations in literature is not consistent. This thesis came to conclusion that blockchain is close to a definition of foundational innovation, such as, TCP/IP-protocol that enabled internet to grow to its current form. Blockchain has potential to change many things in future, yet, it is still likely many years away. The development and broader usage of the technology are still in early phase. Diffusion of the technology is divided in four parts; single use, localization, substitution and transformation. Single use refers to a situation where technology is being used in single use case. Localization refers to a situation where technology is being used in local environment. Substitution refers to a situation where technology replaces traditional ways to do things and transformation refers to a situation where technology fundamentally changes large-scale operations and enables completely new things to do. Blockchain technology has potential to go through all these phases, though, currently it is used mainly in single use cases and locally.

Keywords: blockchain, smart contract, technological innovation, disruptive innovation, foundational innovation

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kryptovaluutat ja lohkoketjuteknologia ovat saaneet runsaasti medianäkyvyyttä viimeisen kahden vuoden aikana. Satoshi Nakamoto nimimerkillä toimiva tuntematon henkilö/ryhmä julkaisi vuonna 2008 tutkimusraportin, jossa uusi kryptovaluutta Bitcoin esiteltiin. Bitcoin perustuu lohkoketjuteknologiaan, joka esiteltiin raportissa ensimmäisen kerran. Teknologia ei herättänyt alussa vielä valtavaa kiinnostusta, mutta nyt lähes kymmenen vuotta myöhemmin innostus sitä kohtaan on levinnyt laajalle.

Lohkoketjuteknologiaan liittyy runsaasti lupauksia, kuten lupaukset siitä, että se vähentää tulevaisuudessa radikaalisti välikäsien tarvetta informaation käsittelyssä. Mattila (2016a) selventää asiaa seuraavasti: verkottuneessa yhteiskunnassa dataa on totuttu siirtämään kopioimalla datakappale paikasta A paikkaan B. Mutta ongelmana on, miten voidaan varmistua siirretyn datan oikeellisuudesta? Ongelma ei ole sinänsä vaikea ratkaista, mutta yleensä se on vaatinut luottamusta johonkin toiseen, ulkoiseen osapuoleen. Mattila näkee tässä lohkoketjun suurimman potentiaalin, koska lohkoketjuteknologia mahdollistaa datan oikeellisuuden varmistamisen osapuolien välillä ilman tarvetta luotetuille välikäsille (engl. intermediaries). Lohkoketjuteknologiaa käyttäessä kuka tahansa voi vahvistaa datan oikeellisuuden itsenäisesti, riippumatta siitä, mistä tai keneltä verkostosta data on lähtöisin.

Tämä tutkielma pyrkii selvittämään lohkoketjuteknologian todellista potentiaalia käytänteitä muuttavaksi teknologiaksi. Tarkoituksena on siis selvittää minkä tyyppinen teknologinen innovaatio lohkoketju on, ja millaisia vaikutuksia sillä mahdollisesti on. Lohkoketjuun viitataan usein, esimerkiksi (Mattila, 2016a; Swan, 2015) käänteentekevänä innovaationa (engl. disruptive), joka syrjäyttää tulevaisuudessa perinteisiä toimintatapoja monilta eri toimialoilta. Tutkielmassa pyritään selvittämään väitteen oikeellisuutta.

Disruptiiviselle innovaatiolle ei ole olemassa yksiselitteistä määrittelyä, mutta Christensenin tutkimus aihepiiriin liittyen (Christensen, 1997; Christensen, Raynor & McDonald, 2015) on saanut arvostusta. Disruptiiviset innovaatiot ovat innovaatioita, jotka herättävät alkuun vain pienen joukon mielenkiinnon, mutta leviävät sieltä vähitellen suuren joukon tietoisuuteen ja muuttavat käsi-

tyksiä toimintatavoista. Niille on yhteistä, että ne esittelevät usein kokonaan uuden tavan toimia, mikä on toisinaan johtanut aiemmin toimialallaan menestyneiden yritysten romahduksiin, koska uusi tapa toimia tarjoaa merkittävän kilpailuedun, johon vanhat toimijat eivät pysty enää vastaamaan perinteisillä menetelmillään. (Baiyere, 2016.)

Lohkoketjuihin liittyvää tutkimusta on julkaistu toistaiseksi melko vähän, mutta myös akateemisen maailman kiinnostus teknologiaa kohtaan on heränyt, ja tällä hetkellä lohkoketjuista tehdään paljon tutkimusta. Yli-Huumo, Ko, Choi, Park ja Smolander (2016) toteavat kirjallisuuskatsauksessaan, jossa selvitettiin lohkoketjututkimuksen nykytilaa, että valtaosa julkaistuista tutkimuksesta on toistaiseksi liittynyt Bitcoiniin. Lohkoketjuissa nähdään kuitenkin runsaasti mahdollisuuksia sovellettuna myös muihin käyttötarkoituksiin ja tutkielman tarkoituksena on kartoittaa näitä mahdollisuuksia.

Lohkoketjun uskotaan sopivan hyvin meneillään olevan alustatalouden ja jakamistalouden trendiin. Etenkin lohkoketjuteknologian liittämisessä esineiden internetiin nähdään suuria mahdollisuuksia. Lohkoketjuteknologian on sanottu olevan parhaimmillaan useiden keskenään luottamuksettomien osapuolten välisessä kommunikaatiossa, joten sovelluskohteita voi löytyä usealta eri toimialalta.

Myöhemmissä luvuissa lohkoketju ja siihen liittyvät laajennukset, kuten älysopimukset, määritellään tarkemmin. Toinen luku esittelee lohkoketjuteknologian perusperiaatteet ja sen laajennukset, kolmas luku käsittelee teknologisia innovaatioita ja esittelee disruptiivisen teknologisen innovaation ja perustavan teknologisen innovaation käsitteet. Neljännessä luvussa selvitetään lohkoketjun roolia innovaationa; sopiiko se usein käytetyn disruptiivisen innovaation määritelmään vai kuvaako innovaatiota paremmin perustavan innovaation (engl. foundational innovation) määritelmä. Lopussa tehdään vielä yhteenveto tutkielman tuloksista ja käydään läpi johtopäätökset, joihin tutkielmassa päädyttiin.

Tutkielma toteutetaan kirjallisuuskatsauksena. Lähdekirjallisuuden laatua arvioidaan viittausten lukumäärällä ja mahdollisuuksien mukaan hyödynnetään julkaisufoorumin laatuluokituksia. Aihepiirin tuoreudesta johtuen valtaosa käytetyistä lähteistä on julkaistu viimeisen kahden vuoden aikana ja ne painottuvat konferensseihin, joten lähteiden julkaisualustoilla on suuri painoarvo, sillä viittauksia ei ole välttämättä ehtinyt vielä kertyä paljoakaan.

2 LOHKOKETJU

Tässä luvussa esitellään lyhyesti lohkoketjuteknologian historiaa ja sen yleiset toimintaperiaatteet. Luvussa esitellään myös lyhyesti lohkoketjun potentiaalin kannalta olennaiset laajennukset, älysopimukset.

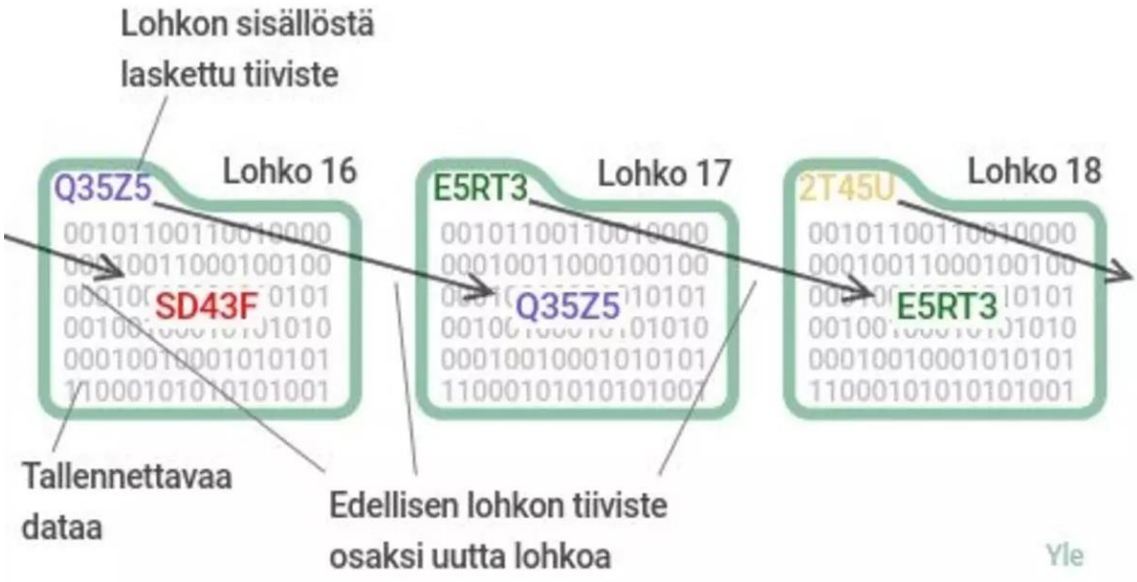
Lohkoketju nousi julkisuuteen Satoshi Nakamoto nimimerkillä (2008) julkaistun tutkimusraportin myötä, jossa esiteltiin lohkoketjuteknologiaan perustuva kryptovaluutta bitcoin. Nakamoto kuvaa teknologiaa vertaisverkon tavoin toimivana teknologiana, joka mahdollistaa bitcoin-rahakkeiden lähettämisen ja vastaanottamisen kahden osapuolen välillä luotettavasti ilman keskitettyä valvojaa. Luottamus varmistetaan kryptografian keinoin konsensusmenetelmällä, joka tässä tapauksessa käyttää hyväksi verkossa mukana olevien tietokoneiden laskentatehoa. (Nakamoto, 2008.)

Lohkoketjun taustalla olevista komponenteista suurin osa on ollut olemassa jo 80-90-luvulta lähtien, mutta tutkijan oivallus oli yhdistää nämä komponentit innovatiivisella tavalla, josta syntyi uusi kryptovaluutta Bitcoin (Mattila, 2016b). Huomionarvoista on, että Nakamoto ei itse käytä termiä lohkoketju (engl. blockchain) kuvaamaan lohkoketjuteknologiaa raportissaan, vaan termiä ”ketju lohkoja” (engl. chain of blocks). Termin lohkoketju alkuperä on epäselvä. (Lauslahti, Mattila & Seppälä, 2016.)

Lohkoketju on jaettu tietokanta, joka säilyttää jatkuvasti kasvavan listan tiedon palasista, jotka ovat vahvistettu ketjussa toimivien solmujen kautta (Beck, Czepluch, Lollike & Malone, 2016; Yli-Huumo, Ko, Choi, Park & Smolander, 2016). Data tallennetaan julkiseen tilikirjaan, joka sisältää tiedon kaikista transaktioista, jotka ovat suoritettu lohkoketjun olemassaolon aikana(Yli-Huumo ym., 2016). Beck ym., (2016) toteavat kuitenkin, että lohkoketjusta yleisesti käytetty vertaus tilikirjaan on rajoittava, koska teknologiaa voi hyödyntää myös huomattavasti monipuolisemmin.

Lohkoketju on siis nimensä mukainen järjestelmä: ketju, joka muodostuu toisiinsa linkitetyistä lohkoista. Jokainen lohko sisältää kaikki tietyn aikamääreen sisällä tapahtuneet transaktiot. Esimerkiksi Bitcoinissa uusi lohko syntyy noin 10 minuutin välein (Nakamoto, 2008). Jokainen lohko sisältää myös viittauksen edelliseen lohkoon. Sovellettava kryptografia riippuu käytettävästä

protokollasta, mutta käytännössä kaikki transaktiot ovat jäljitettävissä aina ensimmäiseen transaktioon saakka. (Beck ym., 2016.) Kuviossa 1 havainnollistetaan lohkoketjun rakennetta. Kuviosta näkee, kuinka edellisen lohkon tiiviste sisällytetään aina osaksi uutta lohkoa. Näin muodostuu lohkoketjun ketjutettu rakenne.



KUVIO 1 Lohkoketjun muodostuminen
Mäntylä J. (2017, 27. joulukuuta). Bitcoin on tuomittu kuplaksi, mutta samaa teknologiaa käytetään pian asuntokaupassa, kuljetuksissa, viennin rahoituksessa ja jopa sotessa. Haettu 10.2.2018 osoitteesta https://yle.fi/uutiset/3-9989602

Cachin (2016) mukaan lohkoketju on parhaiten ymmärrettävissä tila-automaatin jäljennöksenä (engl. state-machine replication), missä järjestelmä säilyttää tietyn tilan, ja asiakkaat suorittavat operaatioita, jotka muuttavat järjestelmän tilaa ja tuottavat tulosteita. Järjestelmää ylläpitävät hajautetusti internetin välityksellä eri toimijat, joita kutsutaan solmuiksi. Järjestelmä ylläpitää tai luo omaisuuserää, jossa kaikilla solmuilla on jokin osuus. Solmut jakavat yhteisen päämäärän järjestelmän ylläpitämiseksi, mutta eivät välttämättä luota toisiinsa sen enempää.

Lohkoketjuja on kahta eri tyyppiä: avoimia ja suljettuja lohkoketjuja. Myös hybridilohkoketjut, jotka yhdistävät näiden molempien ominaisuuksia ovat mahdollisia. Avoimessa lohkoketjussa, kuten bitcoin, kuka tahansa voi osallistua ketjun ylläpitämiseen tarjoamalla laskentatehoaan verkon käyttöön. Suljetussa lohkoketjussa verkon ylläpitäjillä on mahdollisuus valikoida, ketkä osallistuvat verkon transaktioiden vahvistamiseen ja protokollan suorittamiseen. Näissä verkoissa toimivilla solmuilla on yleensä vahvistettu identiteetti ja ne kuuluvat johonkin konsortioon. (Cachin, 2016.)

Lohkoketju hyödyntää julkisen avaimen hallintajärjestelmää (engl. public-key cryptography) tiedon salauksessa. Jokaiselle järjestelmän käyttäjälle

annetaan käyttöön julkinen avain ja yksityinen avain. Yksityistä avainta käytetään transaktioiden allekirjoittamiseen ja julkista avainta käytetään järjestelmässä käyttäjän osoitteena. Tämä mahdollistaa järjestelmän pseudonymiteetin, koska tarvetta reaalimaailman tunnistautumiselle ei ole. (Conoscenti, Vetro & De Martin, 2017.) Esimerkiksi Bitcoinista puhutaan silti usein virheellisesti anonymiteetin takaavana kryptovaluuttana, vaikka tosiasiassa teknologia mahdollistaa vain pseudonymiteetin (Swan, 2015).

Lohkoketjun hyvänä ominaisuutena pidetään sen sisältämän tiedon väärentämisen hankaluutta. Englanninkielisessä kirjallisuudessa tästä käytetään nimitystä ”tamper-proof”. Lohkoketju sisältää ainoastaan vahvistettua dataa, koska vertaisverkossa toimivat solmut varmistavat datan oikeellisuuden yhteistyössä. Sen vuoksi lohkoketju sopii myös moniin muihin käyttötarkoituksiin, kuin vain kryptovaluutaksi. (Beck ym., 2016; Conoscenti ym., 2017.)

Nakamoto (2008) esittelee lohkoketjun toimintaperiaatteen bitcoinin taustalla seuraavasti:

- Uudet transaktiot lähetetään kaikille solmuille
- Jokainen solmu kerää uudet transaktiot lohkoon
- Jokainen solmu työskentelee löytääkseen ratkaisun vaikeaan kryptografiaan perustuvaan laskutoimitukseen (engl. proof-of-work) lohkoonsa
- Kun solmu löytää ratkaisun, se lähettää lohkon kaikille muille solmuille
- Solmut hyväksyvät lohkon vain, jos kaikki siinä olevat transaktiot ovat valideja ja käyttämättömiä
- Solmut ilmaisevat lohkon hyväksymisen ketjuun siirtymällä luomaan uutta lohkoa ketjuun käyttämällä nyt luodun, hyväksytyn, lohkon tiivistettä viittauksena edellisen lohkon tiivisteeseen (engl. hash)

2.1 Hajautettu luonne

Lohkoketju ei toimi keskitetyllä palvelimella, vaan se on hajautettu ketjussa mukana olevien koneiden kesken. Kaikilla ketjun osapuolilla on kaikki ketjun data hallussaan ja he toimivat yhdessä laajentaakseen ketjua. Näitä toimijoita kutsutaan usein louhijoiksi. (Beck ym., 2016.) Järjestelmä ei vaadi keskitettyä toimijaa, ja järjestelmä on siten läpinäkyvämpi kuin keskitetyt ratkaisut, joissa on mukana ulkoinen toimija (Yli-Huumo ym., 2016).

Suikkanen (2017) toteaa, että keskitetyistä järjestelmistä tulee niiden kasvaessa tehottomia ja kalliita. Suuret ja monimutkaiset keskitetyt järjestelmät ovat vähemmän tehokkaita, turvallisia, joustavia ja ne sietävät vähemmän virheitä. Keskitettyjen järjestelmien rajakustannus kasvaa niiden koon ja monimutkaisuuden kasvaessa. Esimerkiksi taloudellinen järjestelmä vaatii luotta-

musta eri osapuolten kesken ja lohkoketju on suhteellisen tehokas vaihtoehto luottamuksen luontiin verrattuna keskitettyyn järjestelmään.
Beck ym., (2016) näkevät lohkoketjuteknologian suurimman edun verrattuna perinteisiin järjestelmiin siinä, että sen sijaan että henkilön täytyisi luottaa siihen, että toinen osapuoli hoitaa osuutensa sopimuksesta sovitulla tavalla, lohkoketjuteknologissa henkilö voi itse nähdä missä tilassa transaktio on ja voi seurata mitä tapahtumaketjussa on meneillään. Esimerkiksi bitcoin mahdollisti ensimmäistä kertaa historiassa sen, että arvoa voitiin luotettavasti siirtää kahden toisistaan kaukana sijaitsevan osapuolen välillä ilman tarvetta välikäsille (Catalini & Gans, 2016).

Lohkoketjun potentiaali liitetään usein esineiden internetiin ja näiden teknologioiden yhdistämisessä nähdään suuria mahdollisuuksia. Esineiden internet tuottaa tulevaisuudessa runsaasti dataa. Tämän datan turvallisuus ja omistajuus ovat tärkeitä kysymyksiä. Vaikka pilvipalvelut tarjoavat mahdollisuuden datan skaalautuvuuden hallitsemiseen, ne eivät välttämättä tarjoa ratkaisuja datan turvallisuuden takaamiseksi. Esineiden internetin laajuudessa luottamuksen varmistaminen on erittäin hankalaa ja kallista, ja ehkä jopa mahdotonta taata. (Huckle, Bhattacharya, White & Beloff, 2016.)

Li, Da Xu & Zhao (2015) listaavat viisi turvallisuus ja yksityisyysongelmaa esineiden internetiin liittyen.

1. Turvallisuus ja yksityisyys yhteiskunnallisesta, laillisesta ja kulttuurillisesta näkökulmasta
2. Luottamusmekanismit
3. Kommunikoinnin turvallisuus
4. Käyttäjän yksityisyys
5. Palveluiden ja sovellusten turvallisuus

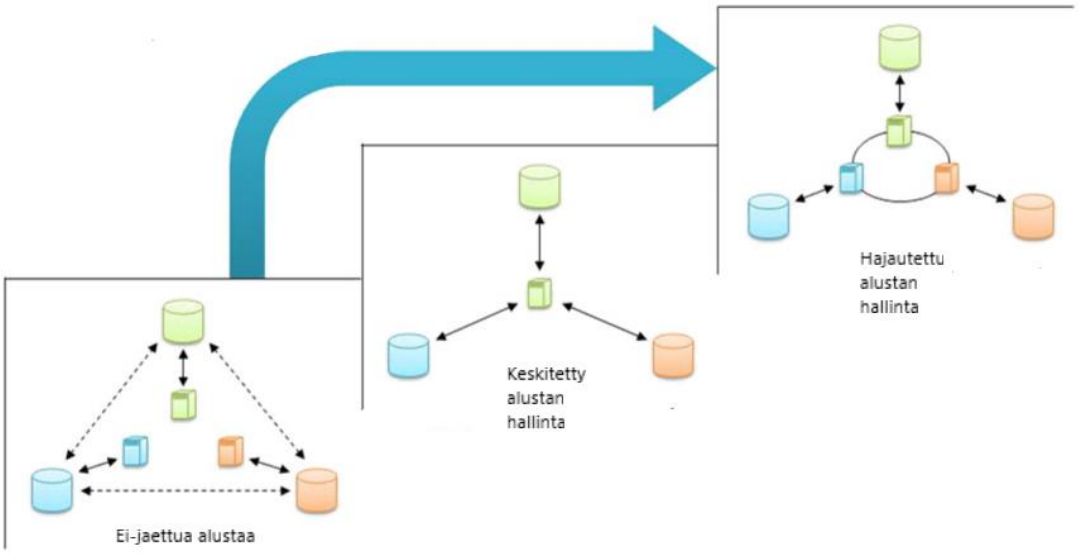
Huckle ym., (2016) uskovat, että lohkoketju on teknologia, jonka avulla näihin ongelmiin voidaan löytää ratkaisu, sillä lohkoketjua voidaan käyttää datan väärinkäytösten huomaamiseen ja käyttölupien määrittämiseen ilman tarvetta luovuttaa ihmisten dataa keskitetysti hallittavaksi (Conoscenti ym., 2017).

Suikkasen (2017) mukaan kaikista utopistisimmat näkemykset luottavat siihen, että lohkoketju poistaa lopulta välikäsien tarpeen kaikilla markkinoilla, mutta hän ei itse näe sitä kovin todennäköisenä skenaariona. Lohkoketju muuttaa todennäköisemmin vain välikäsien tarpeen astetta. Lohkoketju alentaa transaktiokustannuksia ja mahdollistaa uudenlaisten markkinapaikkojen synnyn (Catalini & Gans, 2016).

Lohkoketju mahdollistaa jaetun tietokannan toteuttamisen kokonaan hajautetusti. Sen sijaan, että järjestelmä olisi keskitetysti jonkin osapuolen hallinnassa, kaikki osapuolet pääsevät osallistumaan tietokannan ylläpitoon.

Kuviossa 2 esitetään lohkoketjun mahdollistama hajautettu tietokannan ylläpito. Kuvio esittelee kolme mahdollista skenaariota. Vasemmassa reunassa jokaisella yrityksellä on oma alustansa, keskellä yhteinen alusta on keskitetty ulkoisen osapuolen hallittavaksi ja oikeassa reunassa esitetään lohkoketjun

mahdollistama ratkaisu yhteisestä alustasta, jota hallitaan yhteisesti. Kuvion idea on peräisin (Mattila, Seppälä & Holmström, 2016) raportista.



KUVIO 2 Lohkoketjun mahdollistama hajautettu alusta
(Mattila, Seppälä & Holmström, 2016)

2.2 Konsensusmekanismi

Lohkoketjuissa käytettävästä vahvistusmenetelmästä käytetään termejä konsensusmekanismi ja konsensusprotokolla. Ne molemmat tarkoittavat samaa asiaa. Konsensusmekanismin avulla voidaan saavuttaa hajautettu konsensus, mikä tarkoittaa, että kaikki solmut (toimijat) vahvistavat saman version lohkoketjusta, ja että tämä lohkoketju sisältää vain vahvistettua dataa (Conoscenti ym., 2017).

Konsensusmekanismin tehtävänä lohkoketjuissa on varmistaa kaksi asiaa: 1) tarkastaa, että lohkot ovat oikein rakennettuja ja 2) tarkastaa transaktioiden oikeellisuus jokaisessa lohkossa. Useimmat kryptovaluutat käyttävät konsensusmekanismina julkista konsensusmekanismia, joka tunnetaan nimellä Nakamoto konsensus, nimettynä sen keksijän mukaan. Tämän protokollan ydin on lohkoketju, joka toimii julkisen tilikirjan tavoin; se säilyttää koko verkon täyden transaktiohistorian. (Luu, Teutsch, Kulkarni & Saxena, 2015).

Louhijat vahvistavat ja hyväksyvät transaktioita samalla kun ne luovat, tai louhivat, uusia lohkoja ketjuun. Konsensusmekanismia käytetään kahdessa vaiheessa lohkoketjun vakauden varmistamiseksi. 1) verkoston jäsenten täytyy hyväksyä samat säännöt, joilla transaktioita ja lohkoja vahvistetaan. 2) Datan lohkoketjussa tulee olla yhdenmukaista, jotta jokainen verkoston jäsen tietää kuka omistaa ja mitä (Luu ym., 2015). Nakamoto konsensus mahdollistaa sen, että kuka tahansa voi koska tahansa liittyä protokollan toteuttamiseen tai lähteä

siitä. Järjestelmässä ei ole siis keskitettyä auktoriteettia, joka myöntäisi lupia liittyä protokollan toteuttamiseen, vaan järjestelmä on täysin avoin. (Pass, Seeman & Shelat, 2017.)

Lohkoketjun turvallisuus perustuu kryptografian hyödyntämiseen. Louhijoiden tulee ratkaista vaikeita kryptografisia pulmia. Järjestelmä ei luota siihen, että valtaosa verkoston toimijoista (louhijoista) olisi rehellisiä, vaan järjestelmän vakaus ja turvallisuus perustuu siihen, että suurin osa *verkoston laskentatehosta* on rehellisten toimijoiden (louhijoiden) hallussa (Pass ym., 2017). Kryptovaluuttaympäristössä louhijoita palkitaan heidän tekemästään työstä, joten heillä on myös itsekkäitä motiiveja toimia oikein (Marc, 2016). Esimerkiksi Bitcoinissa louhijat kilpailevat keskenään siitä, kuka ratkaisee ensimmäisenä kryptografisen pulman. Kilpailun voittaja saa palkinnoksi oikeuden osaan uusista luoduista bitcoineista, kun luotu lohko liitetään osaksi lohkoketjua (Yuan & Wang, 2016).

Lohkoketjun ydinprotokolla, Nakamoto konsensus, on siis menetelmä, jonka avulla säilytetään *julkinen*, *muuttumaton* ja *järjestetty* rekisteri, tai tilikirja, tallenteista. Bitcoinin tapauksessa nämä tallenteet ovat transaktioita. Tallenteita voidaan liittää koska tahansa, mutta ainoastaan rekisterin loppuun. Lisäksi voidaan luottaa siihen, että aikaisemmin lisättyjä tallenteita ei voida muuttaa tai poistaa, ja että kaikilla rehellisillä jäsenillä on yhdenmukainen näkymä rekisteriin. (Pass ym., 2017.)

Tietokoneen laskentatehon hyödyntäminen ei ole nykyisin ainoa lohkoketjuissa hyödynnettävä konsensusteknologia, vaan muitakin ratkaisuja on kehitetty ja niistä käydään aktiivista keskustelua (Cachin, 2016). Tässä tutkielmassa niihin ei kuitenkaan paneuduta sen syvällisemmin, mutta on hyvä tiedostaa, että muitakin ratkaisuja kuin laskentatehon hyödyntäminen konsensusmenetelmänä on olemassa. Becker ym., (2013) esittävät arvion, että jos proof-of-work-menetelmää käytettäisiin kaikkien sähköisen maksuliikenteen tapahtumien vahvistamisessa, sen ekologinen jalanjälki olisi vastaavaa kokoluokkaa kuin globaalin lentoliikenteen hiilijalanjälki. Proof-of-work-menetelmälle on kuitenkin esitetty kirjallisuudessa halvempia vaihtoehtoja (Conoscenti ym., 2017).

2.3 Lohkoketjun laajennukset

Lohkoketjuun voidaan liittää teoriassa mitä tahansa dataa, joten sen päälle voidaan rakentaa hyvin erilaisia sovelluksia (Conoscenti ym., 2017). Eniten keskustelussa ovat esiintyneet niin kutsutut älysopimukset, jotka eivät nimestään huolimatta kuitenkaan vaadi toimiakseen tekoälyä (Lauslahti ym., 2016).

Älysopimus konseptina on jo lähes 20 vuotta vanha. Aiemmissa älysopimustoteutuksissa mukana on ollut luotettuja palvelimia turvallisuuden takaamiseksi. Alkuperäisenä visiona oli luoda luotettava virtuaalikone, joka suorittaisi rahaan ja dataan liittyviä ohjelmia. Nykyisin vallalla on ajatus Ethereumin kaltaisista kryptovaluutta-alustoista, jotka rakentuvat siihen ajatukseen, että lohkoketjun päällä voidaan ajaa käyttäjien luomia ohjelmia, mikä mahdol-

listaa hajautetun älysopimusalustan luomisen. (Kosba, Miller, Shi, Wen & Papamanthou, 2016.) Älysopimusten avulla lohkoketju on siis mahdollista ohjelmoida toteuttamaan transaktioita itsestään (Iansiti & Lakhani, 2017).

Szabo (1997) määrittelee älysopimuksen koneluettavana transaktioprotokollana, joka luo sopimuksen aiemmin määritellyin ehdoin. Uudemman määritelmän mukaan älysopimus on joukko digitaalisessa muodossa olevia lupauksia, jotka sisältävät myös protokollat joiden mukaan osapuolet toteuttavat näitä lupauksia. Yksinkertaistettuna älysopimus on koneluettava ohjelma, joka toteuttaa itse itsensä ennalta määriteltyjen ehtojen toteuduttua. Parhaiten älysopimusten synnyn kuvaamiseen sopii vertaus myyntiautomaattiin. Kuluttajan vastapuolena on siinä kone, jonka kanssa kuluttaja tekee hiljaisen sopimuksen ja sitoutuu ennalta määrättyihin ehtoihin. (Lauslahti ym., 2016.)

Älysopimusten yhdistämisessä lohkoketjuihin on myös ongelmia. Nykyisessä muodossaan lohkoketjun päälle rakennettuna älysopimukset eivät mahdollista transaktioiden yksityistä suorittamista. Kaikki älysopimuksissa suoritetut tapahtumat lähetetään kaikille verkon osapuolille ja ne tallentuvat lohkoketjuun ja ovat siten julkisesti nähtävissä. Pseudonymiteetti ei ole riittävä ratkaisu tähän ongelmaan, koska hyökkäykset sitä vastaan ovat todistetusti mahdollisia. (Kosba ym., 2016.) Nykyisessä muodossaan kaikkien transaktioiden arvot ja tilien saldot ovat siis julkisesti kaikkien osapuolien nähtävissä.

3 TEKNOLOGISET INNOVAATIOT

Tässä luvussa käsitellään ensin lyhyesti innovaatiota käsitteenä ja esitellään kirjallisuudessa esiintyviä teknologisten innovaatioiden luokitteluja. Alaluvuissa esitellään tarkemmin lohkoketjujen yhteydessä yleisimmin esiintyvät disruptiivisen ja perustavan innovaation määritelmät.

Garcia ja Calantone (2002) toteavat, että innovaatiota käsitteenä ei ole tarkoin määritelty ja eri innovaatiotyyppejä ei ole kategorisoitu riittävän johdonmukaisesti. Tämä on johtanut hämmennykseen termien käytön välillä. Eri tutkijat voivat käyttää samasta innovaatiosta eri määritelmiä, koska käsitteet eivät ole vakiintuneita. Toinen voi kutsua innovaatiota disruptiiviseksi innovaatioksi ja toinen voi käyttää samasta innovaatiosta termiä radikaali innovaatio tai poikkeava innovaatio (engl. discontinuous). Yhtenäisen typologian käyttö olisi heidän mukaansa tärkeää, jotta voimme luokitella ja ymmärtää eron eri innovaatiotyyppien välillä. He kuitenkin muistuttavat, että innovaatiotypologia on myös suhteellista. Se on suhteellista eri yritysten välillä. Innovaatio jonka toinen yritys määrittelee "todella uudeksi" voi olla toiselle yritykselle inkrementaalinen innovaatio.

Garcia ja Calantone (2002) määrittelevät innovaation käsitteenä seuraavasti: Innovaatio on iteratiivinen prosessi, joka saa alkunsa uudesta ajatuksesta, mikä johtaa uuden keksinnön kehittämiseen, tuotantoon ja markkinointiin ajatuksena keksinnön kaupallinen hyödyntäminen. Määritelmä erottaa kaksi erillistä ulottuvuutta: 1. Innovaatioprosessi sisältää keksinnön teknisen kehittämisen lisäksi keksinnön esittelemisen kuluttajamarkkinoille ja sitä kautta sen leviämisen loppukäyttäjille. 2. Innovaatio on luonteeltaan iteratiivinen prosessi, joka sisältää automaattisesti ensin uuden innovaation esittelyn, jota seuraa jatkumo, jossa innovaatiosta esitellään uusia paranneltuja versioita.

Garcia ja Calantone (2002) huomauttavat, että on tärkeä erottaa keksinnön ja "löydöksen" (engl. invention, discovery) käsitteet innovaation käsitteestä. Innovaatio termin käyttäminen sisältää myös keksinnön taloudellisen hyödyntämisen aspektin. Keksinnöstä ei tule innovaatiota ennen kuin se on edennyt tuotanto- ja markkinointiprosessien kautta markkinoille. Keksinnöstä ei tule innovaatiota, jos se kehitetään tutkimusympäristössä, mutta se ei kos-

kaan leviä sieltä muuhun käyttöön. Innovaation ja keksinnön ero on siis siinä, että innovaatiossa on taloudellista arvoa ja se leviää kehitysympäristön ulkopuolelle myös kolmansien osapuolien käyttöön.

Teknologiset innovaatiot voidaan Garcian ja Calantonen mukaan jakaa viiteen luokkaan. 1. radikaalit innovaatiot 2. inkrementaalit innovaatiot 3. todella uudet innovaatiot 4. poikkeavat innovaatiot ja 5. imitoivat innovaatiot.

Radikaalit innovaatiot eivät vastaa tunnettuun tarpeeseen, vaan luovat uuden tarpeen, joka ei ollut aikaisemmin kuluttajan tiedossa. He määrittelevät esimerkiksi internetin radikaalina innovaationa. Radikaalin innovaation juuret ovat Schumpeterin (1934) väitöksessä, että radikaali teknologinen muutos on voimakas mekanismi, joka voi haastaa monopolien voiman. Hänen pääargumenttinsa oli, että radikaali teknologinen muutos vie pohjan monopolien skaalaeduilta olemassa olevassa teknologiassa muuttamalla tapaa kilpailla. Olemassa oleva tapa tehdä asioita vanhentuu, kun keksitään uusi, parempi tapa tehdä sama asia. (Dahlin & Behrens, 2005.)

Dahlin ja Behrensin (2005) määritelmän mukaan radikaalilla innovaatiolla on seuraavat kolme piirrettä: 1. Innovaatio on uusi: innovaation täytyy erota aikaisemmista innovaatioista. 2. Innovaatio on uniikki: innovaation täytyy erota jo olemassa olevista innovaatioista. 3. Innovaatiolla on vaikutus tulevaan teknologiaan: innovaation täytyy vaikuttaa tulevien innovaatioiden sisältöön.

Inkrementaalit innovaatiot voidaan määrittää jo olemassa olevaan tuotteeseen, teknologiaan tai palveluun parannuksia tarjoavina innovaatioina olemassa olevilla markkinoilla. Ne voivat olla esimerkiksi uusia toiminnallisuuksia vanhaan tuotteeseen tai parannuksia olemassa olevaan teknologiaan. Inkrementaalit innovaatiot voivat olla myös parannuksia esimerkiksi toimitusketjussa ja tuotannossa. (Garcia & Calantone, 2002.)

Todella uudet innovaatiot ovat Garcian ja Calantonen mukaan innovaatioita, jotka sijoittuvat radikaalin ja inkrementaalin innovaation välimaastoon. Todella uudet innovaatiot voivat aiheuttaa poikkeamia markkinoilla tai teknologiassa, mutta eivät molemmissa.

Poikkeavat innovaatiot ovat innovaatioita, jotka voivat olla joko radikaaleja innovaatioita tai todella uusia innovaatioita. Imitoivilla innovaatioilla tarkoitetaan innovaatioita, jotka imitoivat jo aiemmin julkaistuja innovaatioita. Ne voivat olla uusia innovaatioita yritykselle itselleen, mutta eivät markkinoille. (Garcia & Calantone, 2002.)

Govindarajan, Kopalle & Danneels (2011) erottavat radikaalin innovaation ja disruptiivisen innovaation käsitteet seuraavalla tavalla: Radikaalit tuoteinnovaatiot perustuvat uuteen teknologiaan ja ne voidaan alun perin kohdistaa joko suoraan valtavirran ulottuville tai orastaville markkinasegmenteille. Sitä vastoin disruptiiviset innovaatiot kohdistuvat alun perin vain orastaville markkinasegmenteille ja ne eivät välttämättä sisällä uusinta teknologiaa. He myös toteavat, että markkinoiden "kannibalisointi" (engl. cannibalization) korreloi positiivisesti disruptiivisten innovaatioiden kanssa, mutta radikaalit innovaatiot eivät välttämättä vaadi olemassa olevien innovaatioiden "kannibalisointia". (Govindarajan, Kopalle & Danneels, 2011.)

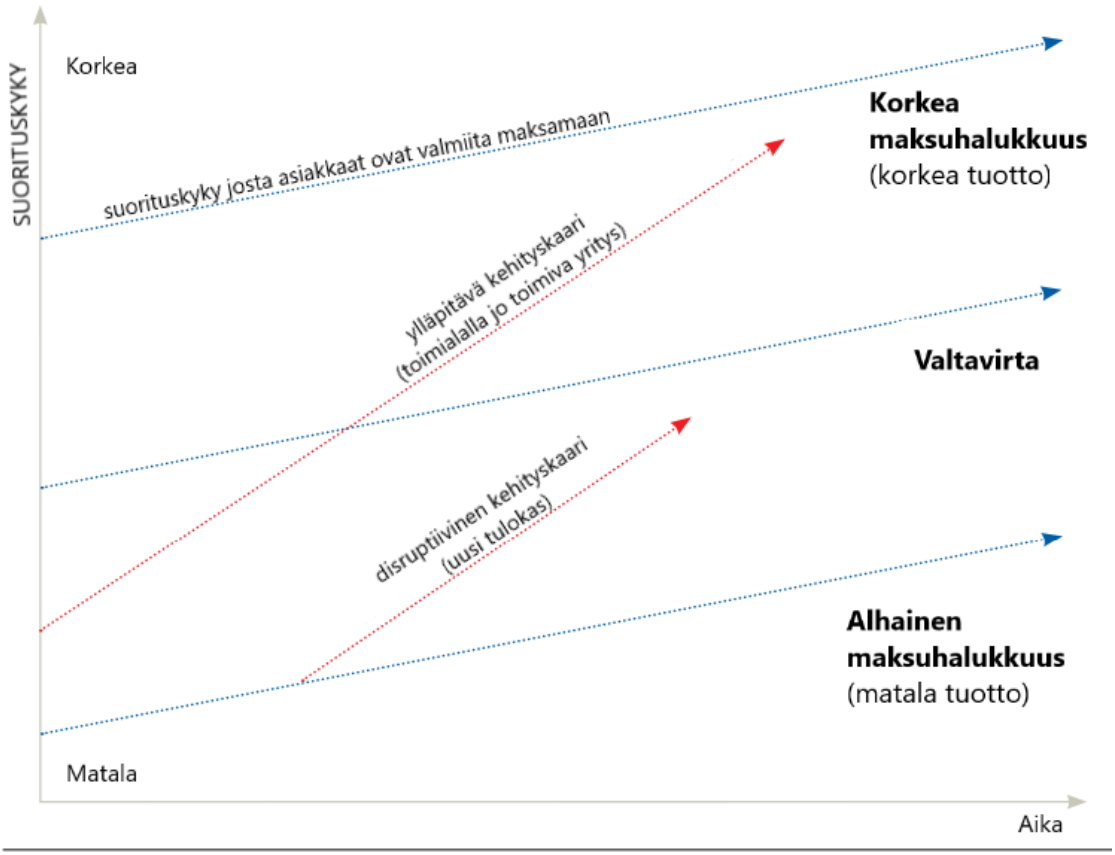
3.1 Disruptiivinen teknologinen innovaatio

Markides (2006) jakaa disruptiivisen innovaation käsitteen kolmeen eri osaan; disruptiivinen teknologinen innovaatio, disruptiivinen tuoteinnovaatio ja disruptiivinen liiketoimintamalli-innovaatio. Kaikille näille innovaatiotyypeille on yhteistä, että niillä on disruptiivisia vaikutuksia jo olemassa oleville markkinoille, mutta ne vaikuttavat niihin eri tavoin ja vaativat erilaisia toimenpiteitä johdolta. Disruptiivisille teknologisille innovaatioille on ominaista, että ne lopulta kasvavat hallitsevaan markkinaosuuteen. Christensen (1997) toteaa, että on tärkeä ymmärtää, että disruptio on prosessi, ei tapahtuma. Muutokset eivät välttämättä tapahdu hetkessä ja voi mennä aikaa ennen kuin disruptiiviset innovaatiot kasvavat hallitsevaan markkinaosuuteen, mutta loppujen lopuksi niin käy (Christensen, 1997).

Christensen ym., (2015) mukaan termiä disruptio (engl. disruption) käytetään nykyisin liian löyhästi. Monet käyttävät termiä disruptiivinen innovaatio kuvaamaan mitä tahansa tilannetta, jossa toimialalla ennen menestyneet yritykset ovat vaikeuksissa jonkin uuden tilanteen vuoksi, mutta se on heidän mukaansa termin liian karkeaa käyttöä. Kirjallisuudessa termiä disruptiivinen (teknologinen) innovaatio kuvataan usein seuraavasti: Uusi teknologia (disruptiivinen innovaatio) ei pärjää aluksi vanhalle tuotteelle, joka käyttää vanhempaa teknologiaa ja on kuluttajien suosiossa (se alisuorittaa). Tämän vuoksi toimialalla jo toimivat yritykset eivät ole huolissaan uudesta innovaatiosta, koska sen ei koeta täyttävän suurinta osaa asiakkaiden vaatimuksista. Uusi tuote voi kuitenkin pärjätä paremmin uudessa tavassa tehdä asioita, ja siten avata uuden markkina-alueen. Ajan myötä disruptiivinen innovaatio parantaa tuotekehityspanostusten kasvaessa ja teknologian kypsyessä, ja lopulta se on tasolla, jolla myös ne valtavirran kuluttajat jotka aiemmin hylkäsivät teknologian, siirtyvät sen käyttöön. Tämän myötä aiemmin hyvin pärjänneet yritykset, jotka käyttivät edeltävää teknologiaa ja panostivat sen kehitykseen, syrjäytetään markkinoilta uutta teknologiaa hyödyntävien yritysten vallatessa niiden markkina-aseman (Christensen ym., 2015; Danneels, 2004; Schmidt & Druehl, 2008).

Danneels (2004) toteaa, että vaikka Christensenin työ disruptiivisen innovaation suhteen on levinnyt hyvin laajalle, konseptia kohtaan on esitetty hyvin vähän rakentavaa kritiikkiä. Hänen määritelmänsä mukaan disruptiivinen teknologinen innovaatio on teknologia, joka muuttaa yritysten välisen kilpailun perusteita muuttamalla ominaisuuksien tyyppiä, joiden paremmuudesta yritykset kilpailevat. Disruptiivinen teknologinen innovaatio saa asiakkaan arvostamaan eri asioita tuotteessa/palvelussa kuin mihin aiemmin on totuttu. Näillä uusilla tuotteilla on aluksi huonompi suorituskyky valtavirran asiakkaiden arvostamissa ominaisuuksissa, mutta niillä on parempi suorituskyky asioissa, joita pieni, mutta nouseva markkinasegmentti arvostaa. Teknologian kypsyessä ja kehittyessä se täyttää lopulta myös valtavirran asiakkaiden vaatimukset ja valtaa sitä kautta markkinaosuuksia.

Christensen ym., (2015) esittävät mallin, jonka avulla teknologisen innovaation disruptiivisuutta voidaan arvioida. Malli muodostuu kahdesta kehityskaaresta; 1) eri markkinasegmenttien vaatima suorituskyky 2) vaihtoehtoisten teknologioiden suorituskyky. Disruptio ilmenee, kun disruptiivisen teknologian tarjoaman suorituskyvyn kehityskaari kohtaa valtavirran asiakkaiden vaatiman suorituskyvyn. Kuviossa 3 on havainnollistettu tätä mallia.



KUVIO 3 Disruptiivisen innovaation malli
Christensen (2015)

3.2 Perustava teknologinen innovaatio

Datta (2016) määrittelee perustavat innovaatiot innovaatioina, joilla on suuri vaikutus tulevaisuuden innovointiin. Ahuja & Lampert (2001) käyttävät samasta asiasta termiä läpimurtoinnovaatio (engl. Breakthrough innovation). Läpimurtoinnovaatiot siis luovat heidän mukaansa perustan, jonka päälle voidaan rakentaa uusia innovaatioita. Läpimurtoinnovaatiot ja perustavat innovaatiot tarkoittavat siis käsitteenä samaa asiaa.

Iansiti ja Lakhani (2017) käyttävät lohkoketjua vastaavan teknologisen ratkaisun leviämisestä esimerkkinä TCP/IP-protokollan (transmission control protocol/internet protocol) yleistymistä. TCP/IP-protokolla on internetin

kuljetuskerroksen protokolla, joka loi pohjan ja mahdollisti internetin leviämisen nykyiseen laajuuteensa. Teknologialla meni kuitenkin vuosikymmeniä ennen kuin se saavutti nykyisen käyttöasteensa. Tutkijat uskovat, että lohkoketjun kohdalla on edessä sama tilanne.

TCP/IP-protokollaa hyödynnettiin aluksi sähköpostin välityksessä ARPAnet:ssa, internetin edeltäjässä, tutkijoiden välillä. Ennen protokollan keksimistä yhteydet perustuivat piirikytkentään ja yhteydet kahden osapuolen välillä täytyi muodostaa aina etukäteen ja niitä täytyi pitää yllä yhteyden ajan. Tietoliikenneoperaattorit investoivat miljoonia linjojen rakentamiseen varmistaakseen, että mitkä tahansa kaksi solmukohtaa verkossa pystyivät kommunikoimaan. TCP/IP-protokolla teki täyskäännöksen tapaan tehdä asioita. Uusi protokolla digitalisoi informaation ja muutti sen pieniksi paketeiksi, jotka kaikki sisälsivät osoitetiedon. Verkkoon laskemisen jälkeen paketit saattoivat valita minkä tahansa reitin vastaanottajan luo. TCP/IP-protokolla loi avoimen, julkisen verkon, jonka hallinnasta ja parantamisesta ei vastannut yksin mikään keskitetty taho. (Iansiti & Lakhani, 2017.)

Protokollaan suhtauduttiin aluksi skeptisesti, koska sen skaalautuvuuteen ja turvallisuuteen ei luotettu. Muutamat yritykset lähtivät kuitenkin kehittämään protokollaa laajentaen sen käyttömahdollisuuksia sähköpostin ulkopuolelle. Yritykset hyödynsivät teknologiaa aluksi paikallisten verkkojen luomisessa organisaatioiden sisälle. TCP/IP-malli levisi laajaan julkiseen käyttöön internetin keksimisen myötä 1990-luvun puolivälissä. Perusinfrastruktuurin kehittyessä tarpeeksi pitkälle, uusia yrityksiä, jotka hyödynsivät internetin ominaisuuksia, ilmestyi markkinoille. Ne tarjosivat esimerkiksi korvaavan vaihtoehdon sanomalehdelle tarjoamalla uutisia luettavaksi internetissä. Seuraava muutosaalto liittyi internetin laajaan leviämiseen. Syntyi yrityksiä, jotka kehittivät muutokseen johtavia liiketoimintamalleja. Tällaisia olivat esimerkiksi musiikkipalveluja tarjoavat yritykset, jotka mahdollistivat täysin uuden tavan ostaa musiikkia digitaalisessa muodossa. TCP/IP-mallilla meni kuitenkin kaiken kaikkiaan yli 30 vuotta ennen kuin se ylitti kaikki viitekehyksessä esitetyt vaiheet (yksittäinen käyttökohde, paikallinen käyttökohde, korvaava teknologia, muutokseen johtava teknologia). (Iansiti & Lakhani, 2017.)

Yhteneväisyydet lohkoketjun ja TCP/IP-protokollan välillä ovat selkeästi havaittavissa. TCP/IP-protokolla mahdollisti kahdenkeskisen sähköpostin välityksen, kun taas bitcoin mahdollistaa kahdenkeskiset rahansiirrot. Molempien teknologioiden kehitys ja ylläpito on *hajautettua*, *avointa* ja *jaettua*. Myös teknologioiden leviämisessä pienen yhteisön joukosta suuren yhteisön tietoon on samankaltaisuuksia. TCP/IP-protokolla laski dramaattisesti yhteyksien muodostamisen hintaa. Lohkoketju voi vastaavasti laskea huomattavasti transaktioiden hintaa (Suikkanen, 2017), ja lohkoketjussa on potentiaalia tulla keskeiseksi järjestelmäksi kaikissa transaktioissa. (Iansiti & Lakhani, 2017.)

Tutkijat Iansiti ja Lakhani käyttävät esimerkkinä osakkeiden välitystä. Nykyisin osakekauppoja voidaan suorittaa mikrosekunneissa kokonaan ilman ihmisen osallistumista. Osakkeiden omistuksen siirto ei kuitenkaan tapahdu yhtä nopeasti, vaan voi viedä jopa viikon. Transaktion osapuolilla ei ole

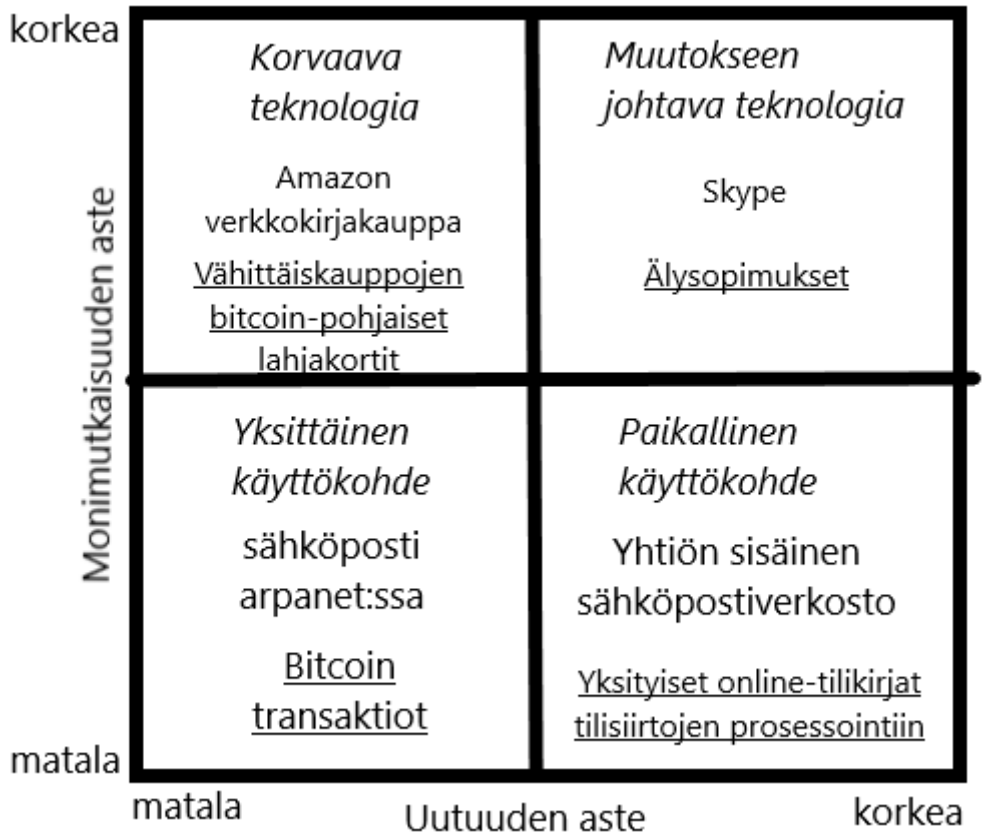
oikeutta päästä automaattisesti käsiksi toistensa tilikirjoihin ja sitä kautta varmistaa, että kaupan kohteena olevat omistukset ovat oikeasti olemassa ja myyjän hallussa sekä siirrettävissä. Tästä syystä kauppoja valvovat useat osakevälittäjät, jotka vahvistavat kaupat ja takaavat omistusten siirron. Lohkoketjujärjestelmässä näille välittäjille ei ole tarvetta, sillä omistusten siirrot päivittyvät automaattisesti kaikkien osapuolien tilikirjoihin ja ovat sieltä vahvistettavissa. Lohkoketjujärjestelmässä osakekauppa voidaan toteuttaa turvallisesti ja luotettavasti sekunneissa.

Iansiti ja Lakhani luovat viitekehyksen perustavan teknologian yleistymisen vaiheista. Muutos sisältää kaksi ulottuvuutta. Uutuus (engl. novelty) ja monimutkaisuus (engl. complexity). Uutuus tarkoittaa nimensä mukaisesti innovaation uutuuden astetta. Mitä korkeampi uutuuden aste innovaatiolla on, sitä enemmän käyttäjillä menee aikaa sen ymmärtämiseen, minkä ongelman innovaatio ylipäätään ratkaisee. Jos innovaatio on täysin uusi maailmalle, sen uutuuden aste on korkea. Garcia & Calantone (2002) käyttävät innovaation uutuuden asteesta termiä "tuotteen innovatiivisuus". Innovatiivisuus mittaa siis tuotteen, prosessin tai palvelun potentiaalia aiheuttaa "häiriötä jatkumossa" ja muuttaa käytänteitä (engl. potential discontinuity) siinä vaiheessa, kun innovaatio esitellään markkinoille. Makroperspektiivistä innovatiivisuus mittaa heidän mukaansa innovaation potentiaalia aiheuttaa ajattelutavan muutos tieteessä, teknologiassa ja/tai teollisuudenalan markkinarakenteessa. Mikroperspektiivistä innovatiivisuus mittaa innovaation potentiaalia vaikuttaa yrityksen jo olemassa oleviin resursseihin, kuten sen kyvykkyyteen, tietoon, taitoihin, strategiaan ja teknologisiin resursseihin.

Iansitin ja Lakhanin viitekehyksen toinen ulottuvuus on monimutkaisuus, joka liittyy ekosysteemin hallinnan tarpeeseen. Ekosysteemin jäsenet toimivat yhdessä luodakseen arvoa teknologian avulla. Järjestelmä on sitä monimutkaisempi, mitä enemmän ja mitä erilaisempia jäseniä verkostossa on mukana. Monimutkaisuus mittaa koordinoinnin tarpeen astetta näissä ekosysteemeissä. Lohkoketju on esimerkki innovaatiosta, jonka monimutkaisuuden aste on korkea, koska se on lähtökohtaisesti kehitetty useiden osapuolien välisiin transaktioihin ja yhteistyöhön heidän välillään. Toinen esimerkki korkean monimutkaisuuden asteen innovaatiosta on sosiaalinen media. Sosiaalinen media ilman useita jäseniä ei ole erityisen hyödyllinen, mutta useiden ihmisten liittyessä siihen mukaan, keksinnön vaikuttavuus, mutta myös sen monimutkaisuuden aste ja koordinoinnin tarve kasvaa.

Iansiti ja Lakhani (2017) toteavat, että lohkoketju ei ole disruptiivinen teknologinen innovaatio, vaan he liittävät siihen käsitteen *perustava teknologinen innovaatio (engl. foundational technology)*. He perustavat näkemyksensä siihen, että lohkoketjussa on potentiaalia uuden perustan luomiseen yhteiskunnalle ja taloudellisille järjestelmille, mutta se ei suoraan tarjoa halvempaa/parempaa ratkaisua johonkin tiettyyn ongelmaan, jolla se syrjäyttäisi toimijoita tietyiltä toimialoilta.

Viitekehys muodostuu neljästä eri lohkosta. Jokainen lohko (engl. quadrant) muodostaa teknologian kehittymisen asteen. Kartta auttaa hahmottamaan kunkin innovaation vaatimuksia ja sen aiheuttamia muutoksia.
Kuviossa 4 on esitetty muutama esimerkki kunkin tyypin sovellutuksista. Paljaan tekstin esimerkit ovat TCP/IP-teknologian sovellutuksia ja alleviivatut esimerkit pohjautuvat lohkoketjuun.



KUVIO 4 Perustavien teknologioiden leviäminen
Iansiti & Lakhani (2017)

4 LOHKOKETJUTEKNOLOGIAN POTENTIAALI INNOVAATIONA

Tämä luku käsittelee lohkoketjua innovaationa. Alussa käydään läpi kirjallisuudessa esitettyjä lohkoketjun käyttökohteita ja sen jälkeen selvitetään lohkoketjun potentiaalia käyttämällä apuna Iansitin ja Lakhanin (2017) luomaa viitekehystä perustavan teknologian leviämisestä. Luvun alaluvut ovat osia viitekehyksessä esitetyistä lohkoista. Conoscenti ym., (2017) toteuttivat systemaattisen kirjallisuuskatsauksen, jossa he selvittivät lohkoketjun käyttökohteita kryptovaluuttojen lisäksi. Seuraavassa taulukossa on listattu 18 heidän kirjallisuudesta löytämäänsä käyttökohdetta lohkoketjulle.

Kategoria	**Lohkoketjun käyttö**
Tietovarastonhallinta	Käyttöoikeuksien hallinta ja viittaukset käyttäjän dataan
	Tiedonvarastointisopimusten hallinnointi
	Asiakirjojen varastointisopimusten hallinnointi
	Väärennöksiltä suojattu tapahtumaloki ja datan käyttöoikeuksien hallinnointi
	Metadatan hallinnointi
	Automaattinen korvausjärjestelmä tallennuspalvelimen asiakkaalle datan kadotessa
	Hajautettujen järjestelmien lähettämien viestien pysyvä (engl. immutable) tallennus
Kaupankäynti datasta ja hyödykkeistä	Hyödykkeiden/sensoridatan osto laitteen/ihmisen toimesta
	IoT-laitteiden sensoridatan osto
Identiteetin hallinta	Identiteetin vahvistuksen hallinta/ PGP-sertifikaattien peruutus
	Julkisten avainten hallintajärjestelmä – avainten päivitys, rekisteröinti ja peruutus
Arvostelujärjestelmä	Äänestysjärjestelmä
	Palautejärjestelmä kuluttajille
Muut	Ohjelmistolisenssien hallinta
	Aikaleimajärjestelmä; todistus siitä, että sisältö on tuotettu ennen tiettyä päivämäärää
	Arvontajärjestelmän toteutus
	Pankkisovellukset, kuten automaattiset ja hajautetut tilikirjat
	”Sosiaalisen kryptovaluutan” toteutus sosiaalisen vaikutusvallan määrittämiseen

TAULUKKO 1 Lohkoketjun käyttökohteita

4.1 Yksittäinen käyttökohde

Ensimmäisen lohkon sisällä ovat yhden käyttökohteen sovellutukset (engl. single use). Se sisältää yksinkertaiset, yhteen käyttötarkoitukseen erikoistuneet innovaation sovellutukset. Ensimmäisen lohkon sovellutuksille on yhtenäistä, että sekä niiden uutuuden aste että monimutkaisuuden aste ovat matalia. Nämä sovellutukset tarjoavat kuitenkin tehokkaampia ja halvempia ratkaisuja johonkin tunnettuun ongelmaan. Bitcoin-transaktiot ovat esimerkki lohkoketjuteknologian sovellutuksista, jotka sopivat tähän lohkoon. Bitcoin-transaktiot tarjoavat yksinkertaisesti vaihtoehtoisen maksutavan, mutta sen edut tulevat esiin etenkin kansainvälisissä rahansiirroissa, joissa perinteisillä valuutoilla on rajoituksensa. Esimerkki TCP/IP-protokollan ensimmäisen lohkon sovellutuksesta on sähköposti. Sähköposti korvasi paljon puhelinliikennettä tarjoamalla helpomman, halvemman ja nopeamman tavan viestiä. (Iansiti & Lakhani, 2017.) Toimijat, kuten NASDAQ, ovat jo alkaneet hyödyntää lohkoketjua prosessien automatisoinnissa, jotka olivat ennen lakimiesten vastuulla (Beck ym., 2016).

4.2 Paikallinen käyttökohde

Toisen lohkon sisällä ovat paikallisen käyttökohteen sovellutukset (engl. localization). Lohkon sovellutuksilla uutuuden aste on korkea, mutta niiden monimutkaisuuden aste, eli tarve koordinoinnille, on suhteellisen matala. Näiden innovaatioiden käyttöönotto ei siis ole vielä kovin hankalaa, vaan niiden omaksuminen tapahtuu suhteellisen nopeasti. Tämän lohkon sisällä olevat innovaatiot ovat usein jatkoa yhden käyttökohteen innovaatioille. Yksityisen lohkoketjun avulla toteutettu yhteinen hajautettu alusta yritysten jaettavaksi on esimerkki tämän lohkon sovellutuksesta. (Iansiti & Lakhani, 2017.)

Mattila ym., (2016) uskovat vahvasti alustatalouden menestykseen. Alustataloudella viitataan yritysten muodostamiin yhteisalustoihin, joiden välityksellä yritykset voivat yhdessä luoda arvoa. Mattila (2016) näkee, että lohkoketjuteknologia voi muuttaa yhteiskuntaa kahdella tavalla. Ensimmäiseksi, lohkoketjuteknologia tarjoaa hajautetun, sensuurille ja väärennöksille immuunin digitaalisen alustan, jossa kaikki voivat vapaasti innovoida sekä suorittaa transaktioita. Toiseksi se tarjoaa kustannussäästöjä parantamalla tehokkuutta yritysten välisessä yhteistyössä poistamalla tarpeen aktiiviselle datan synkroinnille ja datan yhdenmukaisuuden varmistamiselle. Lohkoketjun hyödyntäminen parantaa huomattavasti näiden yhteisalustojen läpinäkyvyyttä. Yritykset voivat välittää tuotekeskeistä informaatiota (engl. product-centric information) huomattavasti tehokkaammin datan jäljitettävyyden ja luotettavuuden paranemisen ohella.

Myös monet suuret pankit ovat lähteneet etujoukoissa kehittämään lohkoketjuteknologiaa, koska ne näkevät siinä suuria mahdollisuuksia oman toimintansa kannalta. Lohkoketjua hyödynnetään nykyisin jo esimerkiksi timant-

tien toimitusketjujen seurannassa. (Iansiti & Lakhani, 2017.) Timanttien kulkua seurataan lohkoketjun avulla aina kaivoksista kuluttajille asti. Iansiti ja Lakhani odottavatkin tarkoin määrättyihin käyttötarkoituksiin kehitettyjen yksityisten lohkoketjujen määrän räjähdysmäistä kasvua eri teollisuudenhaaroilla.

4.3 Korvaava teknologia

Kolmas lohko sisältää korvaavat teknologian sovellutukset (engl. substitution). Tämän lohkon sisällä olevien innovaatioiden uutuuden aste on melko matala, koska ne rakentuvat yksittäisten ja paikallisten käyttökohteiden sovellutusten päälle, mutta niiden monimutkaisuuden ja koordinoinnin tarpeen aste on korkea, koska ne ovat suunnattu laajemmalle käyttäjäkunnalle. Nämä sovellutukset on lähtökohtaisesti kehitetty yhä julkisempaan käyttöön ja innovaatioiden tavoitteena on kokonaan korvata perinteisiä tapoja tehdä asioita. Tämän kaltaisten innovaatioiden omaksuminen vie aikaa ja ennakkoluulot niitä kohtaan ovat korkealla. Kryptovaluutat ja sähköinen äänestysjärjestelmä (Conoscenti ym., 2017) ovat esimerkki tämän lohkon sovellutuksesta. Kryptovaluuttojen käyttäminen edellyttää, että kaikki rahansiirroissa mukana olevat osapuolet omaksuvat teknologian ja hyväksyvät ne valuuttana ja maksuvälineenä. Kryptovaluutat haastavat valtiohallinnot ja pankit, jotka ovat olleet perinteisesti vastuussa näiden asioiden käsittelystä ja hallinnasta. Myös kuluttajien täytyy ymmärtää teknologian toiminnallisuus ja muuttaa käyttäytymistään. (Iansiti & Lakhani, 2017.)

Iansiti ja Lakhani kertovat esimerkin MIT-yliopistossa vuonna 2014 suoritetusta kokeesta, jossa kaikille yliopiston opiskelijoille, joilla ei ollut vielä tutkintoa, tarjottiin 100$ arvosta bitcoineja. 30% opiskelijoista ei ottanut bitcoineja lainkaan vastaan ja 20% vaihtoi ne käteiseen heti muutaman viikon sisällä. Ihmisillä oli vaikeuksia ymmärtää, miten ja mihin bitcoineja pystyi käyttämään, mikä vaikeutti teknologian omaksumista.

4.4 Muutokseen johtava teknologia

Neljäs lohko sisältää muutokseen johtavat sekä sitä edellyttävät teknologian sovellutukset (engl. transformation). Tämän lohkon innovaatioilla sekä niiden uutuuden, että monimutkaisuuden aste ovat erittäin korkealla. Ne tarjoavat täysin uusia tapoja tehdä uusia asioita ja niiden omaksuminen edellyttää suuria yhteiskunnallisia, laillisia ja poliittisia muutoksia. Parhaimmillaan ne voivat yleistyessään mullistaa kokonaan taloudellisia ja yhteiskunnallisia rakenteita, mutta vaativat useiden eri osapuolien välisen toiminnan koordinointia ja instituutioiden välisiä sopimuksia standardeista ja prosesseista. (Iansiti & Lakhani, 2017.) Älysopimukset ovat tällä hetkellä lohkoketjuteknologian sovellutuksista parhaiten tähän lohkoon sopivia. Ne voivat automatisoida maksuja ja omai-

suuden siirtoja, kun sovitut ehdot täyttyvät. Älysopimus voi esimerkiksi siirtää maksun automaattisesti toimittajalle, kun lähetys on saapunut. Transaktioita voivat toteuttaa myös esineiden internetin laitteet keskenään lohkoketjuteknologian ja älysopimusten avustuksella (Conoscenti ym., 2017; Huckle ym., 2016). Älysopimuksia on jo testattu esimerkiksi tekijänoikeuksien hallinnassa ja pankkiliiketoiminnassa. (Iansiti & Lakhani, 2017.)

Tosiasiassa älysopimusteknologia ei ole kuitenkaan vielä kovin pitkällä, mistä syystä reaalimaailman sovellutuksia on vielä hyvin rajallinen määrä. Älysopimuksiin liittyvä keskustelu on siis tällä hetkellä hyvin pitkälti teoreettista. Digitaalisten älysopimusalustojen evoluutio vaatii teknologian, talouden ja lain näkökulmien yhdistämistä. Älysopimusten yleistyminen vaatii sen, että instituutiot hyväksyvät ne, mikä edellyttää suuria panostuksia eikä myöskään teknologisia haasteita pidä unohtaa. (Lauslahti ym., 2016.)

5 YHTEENVETO

Tutkielman tarkoituksena oli selvittää lohkoketjun potentiaalia innovaationa ja liittää se teknologisten innovaatioiden teoriaan. Pyrkimyksenä oli yrittää tuoda selvyyttä lohkoketjujen ympärillä pyörivään keskusteluun, koska lohkoketjujen tyyppi innovaationa on määritelty eri tutkimuksissa hyvin eri tavoin ja julkisessa keskustelussa lohkoketjuihin viitataan hajanaisin tavoin. Tutkielma toteutettiin kirjallisuuskatsauksena. Ensimmäisessä sisältöluvussa johdannon jälkeen esiteltiin lohkoketju ja sen toimintaperiaate ja määriteltiin sen kannalta keskeisen laajennuksen älysopimuksen käsite. Kolmas luku käsitteli teknologisia innovaatioita ja niiden leviämistä. Neljännessä luvussa selvitettiin lohkoketjun potentiaalisia käyttökohteita, ja arvioitiin sen mahdollista leviämistä liittämällä lohkoketju perustavan teknologisen innovaation leviämisen viitekehykseen.

Lohkoketjuteknologialta odotetaan paljon ja usko teknologiaa kohtaan on kova. Lohkoketjuteknologia lunastaa monilta osin siihen kohdistuvat lupaukset ja teknologialle löytyy monia käyttökelpoisia sovelluskohteita, niin toimitusketjun hallinnan suhteen (Mattila, 2016) kuin esineiden internetin puolelta (Conoscenti ym., 2017; Huckle ym., 2016). Tosiasia kuitenkin on, että monet lohkoketjuun liitetyt uskomukset sen mullistavuudesta ovat vielä hyvin kaukana. Teknologiaan itsessään liittyy vielä ratkaisemattomia ongelmia, ja sen lisäksi sen vaikutukset ulottuvat parhaimmillaan niin suureen osaan yhteiskunnallisia rakenteita, että muutokset eivät tapahdu hetkessä. Yuan & Wang (2016) esittelevät esimerkiksi lohkoketjun mahdollisuuksia älykkään liikennejärjestelmän toteuttamisessa. Liikennejärjestelmän toteutus on vielä hyvin teoreettisella tasolla, mutta lohkoketju nähdään olennaisena osana järjestelmän kehitystä. Lisäksi älysopimusten kaltaisten teknologioiden yhdistäminen lohkoketjuun on hyvin mielenkiintoinen ajatus, mutta niiden yleistyminen vaatii suuria laillisia ja yhteiskunnallisia muutoksia teknologian kehittymisen lisäksi. Tutkimus siihen liittyen on vielä alkutekijöissään (Lauslahti ym., 2016.)

Lohkoketju tulee ensin yleistymään yksinkertaisissa, paikallisissa, sovelluskohteissa. Lohkoketju on saanut jo jalansijaa yksittäisissä käyttökohteissa ja panostukset sen paikalliseen hyödyntämiseen ovat suuria. Monet yritykset ovat lähteneet mukaan teknologian kehittämiseen, ja lohkoketjun edut

esimerkiksi yritysten toimitusketjujen hallinnassa ovat ilmeiset. Lohkoketju sopii hyvin meneillään olevaan alustatalouden trendiin, jossa yritykset hyödyntävät yhteisiä alustoja ja luovat sitä kautta yhteistä arvoa (Mattila, 2016).

Lohkoketjun kehityksessä on yhteneväisyyksiä disruptiivisen teknologisen innovaation kehityksen teoriaan, mutta lohkoketju ei itsessään ole disruptiivinen teknologinen innovaatio, vaan teknologia, joka *mahdollistaa* disruptiivisen liiketoimintamallin kehittämisen. Lohkoketjun pohjalle voidaan rakentaa liiketoimintamalleja, jotka voivat muuttaa radikaalisti totuttuja tapoja tehdä asioita, mutta lohkoketju itsessään ei syrjäytä mitään. Iansitin ja Lakhanin (2017) määritelmä lohkoketjusta perustavana innovaationa (engl. foundational innovation) sopii hyvin lohkoketjun kuvaukseen. Innovaatioihin liittyvä typologia ei ole kuitenkaan vakiintunutta ja eri innovaatiotyyppien määritelmät menevät osin ristiin. Lohkoketjussa on myös ominaisuuksia, jotka menisivät radikaalin tai poikkeavan innovaation määritelmään. Perustava innovaatio on toistaiseksi melko vähän käytetty termi verrattuna muihin määritelmiin, mutta määritelmän käytön yleistyminen ei olisi välttämättä huono asia.

Tutkielmassa käsiteltiin asioita melko yleisellä tasolla pureutumatta tarkemmin teknisiin yksityiskohtiin. Tavoitteena oli tarkastella lohkoketjua suhteessa teknologisten innovaatioiden teoriaan, joten tekniset yksityiskohdat eivät ole keskeisessä roolissa tutkielman tavoitteen kannalta. Aihepiirissä on kuitenkin vielä monia mahdollisuuksia auki jatkotutkimukselle. Moni lohkoketjuun liittyvä tutkimus liikkuu vielä melko korkealla tasolla; esimerkiksi lohkoketjuteknologian ja esineiden internetin yhdistämisestä löytyy tutkimuksia, mutta käytännön toteutukset ovat vielä harvassa. Älysopimusteknologioiden yhdistäminen lohkoketjuteknologiaan on myös vielä hyvin tuore aihe, ja valtaosa siihen liittyvästä tutkimuksesta on julkaistu vasta viimeisen kahden vuoden aikana. Myös erilaisten konsensusmekanismien kehittäminen julkisiin lohkoketjuihin on hyvin mielenkiintoinen aihe jatkotutkimukselle. Aiheita jatkotutkimukselle löytyy siis vielä hyvin laajalta skaalalta niin teknisestä, laillisesta, yhteiskunnallisesta kuin taloudellisesta näkökulmasta.

LÄHTEET

Ahuja, G., & Morris Lampert, C. (2001). Entrepreneurship in the large corporation: A longitudinal study of how established firms create breakthrough inventions. *Strategic management journal*, *22*(6-7), 521-543.

Baiyere, A. (2016). *Discovering the role of information technology in disruptive innovations : Enabler, sustainer or barrier?*. Turku: Turun yliopisto. Haettu osoitteesta http://urn.fi/URN:ISBN:978-951-29-6680-6

Beck, R., Czepluch, J. S., Lollike, N. & Malone, S. (2016). Blockchain -the gateway to trustfree cryptographic transactions.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P. & Böhme, R. (2013). Can we afford integrity by proof-of-work? scenarios inspired by the bitcoin currency. *The economics of information security and privacy* (s. 135-156) Springer.

Cachin, C. (2016). Architecture of the hyperledger blockchain fabric.

Catalini, C. & Gans, J. S. (2016). Some simple economics of the blockchain.

Christensen, C. M. (1997). *The innovator's dilemma : When new technologies cause great firms to fail*. Boston (MA): Harvard Business School. Haettu osoitteesta https://jyu.finna.fi/Record/jykdok.833212

Christensen, C. M., Raynor, M. E. & McDonald, R. (2015). What is disruptive innovation. *Harvard Business Review, 93*(12), 44-53.

Conoscenti, M., Vetro, A. & De Martin, J. C. (2017). Blockchain for the internet of things: A systematic literature review. doi:10.1109/AICCSA.2016.7945805

Dahlin, K. B. & Behrens, D. M. (2005). When is an invention really radical?: Defining and measuring technological radicalness. *Research Policy, 34*(5), 717-737. doi:10.1016/j.respol.2005.03.009

Danneels, E. (2004). Disruptive technology reconsidered: A critique and research agenda. *Journal of Product Innovation Management, 21*(4), 246-258.

Datta, A. (2016). Evaluating the antecedents of foundational innovations: A longitudinal look at patents from information technology industry. *International Journal of Innovation Management, 20*(1) doi:10.1142/S1363919616500134

Garcia, R. & Calantone, R. (2002). A critical look at technological innovation typology and innovativeness terminology: A literature review. *Journal of Product Innovation Management, 19*(2), 110-132.

Govindarajan, V., Kopalle, P. K. & Danneels, E. (2011). The effects of mainstream and emerging customer orientations on radical and disruptive innovations. *Journal of Product Innovation Management, 28*(s1), 121-132.

Huckle, S., Bhattacharya, R., White, M. & Beloff, N. (2016). *Internet of things, blockchain and shared economy applications* doi://doi.org/10.1016/j.procs.2016.09.074

Iansiti, M. & Lakhani, K. R. (2017). The truth about blockchain.

Kosba, A., Miller, A., Shi, E., Wen, Z. & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. (s. 839-858) IEEE. doi:10.1109/SP.2016.55

Lauslahti, K., Mattila, J. & Seppälä, T. (2016). Smart Contracts–How will blockchain technology affect contractual practices?

Li, S., Da Xu, L. & Zhao, S. (2015). The internet of things: A survey. *Information Systems Frontiers, 17*(2), 243-259.

Luu, L., Teutsch, J., Kulkarni, R. & Saxena, P. (2015). Demystifying incentives in the consensus computer. (s. 706-719) ACM.

Marc, P. (2016). Blockchain technology: Principles and applications. *Handbook of research on digital transformations' edited by F. xavier olleros, and majlinda zhegu* () Edward Elgar. Haettu osoitteesta https://halshs.archives-ouvertes.fr/halshs-01231205

Markides, C. (2006). Disruptive innovation: In need of better theory. *Journal of Product Innovation Management, 23*(1), 19-25.

Mattila, J., Seppälä, T., Holmström, J. (2016). Product-centric information management: A case study of a shared platform with blockchain technology. . Industry Studies Association Conference:

Mattila, J. (2016a). The blockchain Phenomenon–The disruptive potential of distributed consensus architectures.

Mattila, J. (2016b). *Product-centric information management a case study of a shared platform with blockchain technology : Conference paper : Industry studies association conference, 24.5 26.5.2016, minneapolis, MN, USA* Haettu osoitteesta https://jyu.finna.fi/PrimoRecord/pci.gbv862225590

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Pass, R., Seeman, L. & Shelat, A. (2017). Analysis of the blockchain protocol in asynchronous networks. (s. 643-673) Springer.

Schmidt, G. M. & Druehl, C. T. (2008). When is a disruptive innovation disruptive? *Journal of Product Innovation Management, 25*(4), 347-369.

Suikkanen, H. (2017). *Economic and institutional implications of blockchain.* Haettu osoitteesta http://urn.fi/URN:NBN:fi:aalto-201711137552 [urn]

Swan, M. (2015). *Blockchain: Blueprint for a new economy* " O'Reilly Media, Inc.".

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday, 2*(9)

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) doi:10.1371/journal.pone.0163477

Yuan, Y. & Wang, F. (2016). Towards blockchain-based intelligent transportation systems. (s. 2663-2668) IEEE.