Joonas Lähde

LOHKOKETJUTEKNOLOGIA OSANA IOT-EKOSYSTEEMEJÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Lähde, Joonas
Lohkoketjuteknologian osana IoT-ekosysteemejä
Jyväskylä: Jyväskylän yliopisto, 2019, 27s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja(t): Riekkinen, Janne

Viimeisen vuosikymmenen aikana IoT, eli esineiden internet, on juurtunut pysyväksi osaksi eri yhteiskuntamme osa-alueita. Esineiden internettiä hyödynnetään niin kotitalouksissa kuin teollisuudessakin erilaisten tehtävien hoitamiseen ja liiketoiminnan tehostamiseen. Yleistymisen myötä on kuitenkin herännyt paljon kysymyksiä IoT laitteiden turvallisuuteen ja skaalautumiseen liittyen nykyisen arkkitehtuurimallin puitteissa. Ennen kuin IoT voidaan ottaa laajemmin käyttöön, on siihen liittyvät heikkoudet pyrittävä ratkaisemaan mahdollisimman tehokkaasti. Yksi keino näiden heikkouksien ratkaisuun on lohkoketjuteknologian käyttö osana IoT-ekosysteemeitä. Tutkielman tavoitteena on tutkia kuinka IoT:n ja lohkoketjuteknologian yhdistäminen tapahtuu erilaisten mallien avulla ja millaisia positiivisia vaikutuksia sillä on. Lisäksi tutkielmassa otetaan kantaan tiedossa oleviin mahdollisiin ongelmiin. Tutkielma toteutettiin kirjallisuuskatsauksena ja sen lopputuloksena saatiin selville erilaisia malleja, joilla yhdistäminen voidaan toteuttaa. Tutkimuksessa saatiin myös selville, minkälaisia positiivisia vaikutuksia lohkoketjujen käytöllä on IoT laitteiden toimintaan erilaissa ympäristöissä. Tämän lisäksi selville saatiin mahdolliset ongelmat, joita voi ilmetä teknologioiden yhdistämisen seurauksena. Tutkielmassa todettiin, että lohkoketjujen ja IoT laitteiden onnistuneella migraatiolla saadaan huomattavaa etua, verrattuna vanhaan keskitettyyn arkkitehtuuriin. Keskeisiä etuja on hajautetun arkkitehtuurin tuoma vakaus ja tiedon säilyvyys. Erityisesti lohkoketjujen ja IoT-ekosysteemeiden rooli osana teollisuuden kehitystä on tutkielmassa suuressa osassa. Tutkielmassa selviää myös paljon mahdollisia ongelmakohtia niin teknisessä toteutuksessa kuin vallitsevassa ympäristössä, jotka voivat hidastaa ratkaisujen käyttöönottoa tulevaisuudessa. Ongelmia aiheuttaa muun muassa lainsäädännöt ja laitteiden nykyinen suoritusteho.

Asiasanat: IoT, esineiden internet, blockchain, hajautettu arkkitehtuuri

ABSTRACT

Lähde, Joonas
Blockchain as a part of IoT ecosystems
Jyväskylä: University of Jyväskylä, 2018, 27pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Riekkinen, Janne

Over the last decade Internet of Things (IoT) has become a permanent part of all aspects of our society. The Internet of Things is used in both households and industry to perform various tasks and increase business efficiency. However, with widespread use, many questions have been raised about the security and scalability of IoT devices within the current architectural model. Before IoT can be more widely deployed in everyday life and in critical infrastructure, its weaknesses must be addressed as effectively as possible. One way to address these weaknesses is to use blockchain technology as part of IoT ecosystems. The aim of this thesis is to investigate how the migration of IoT and blockchain technology takes place using different models and what positive effects it has. In addition, the thesis takes a position on known problems. This thesis was carried out as a literature review. The study also found out what positive effects the use of blockchains has on the operation of IoT devices in different environments. In addition, potential problems that may arise as a result of the combination of technologies were identified. The study found that successful migration of blockchains and IoT-devices provides a significant advantage over the old centralized architecture. Key benefits include the stability and data retention provided by a decentralized architecture. In particular, the role of blockchains and IoT ecosystems as part of industrial development is largely covered in the dissertation. However, the dissertation also reveals many possible problem areas both in the technical implementation and in the prevailing environment. Problems are caused by for example legislation and the current performance of IoT devices.

Keywords: IoT, blockchain, Internet of Things, Decentralization

KUVIOT

KUVIO 1 IoT Reference Model (Cisco, 2014.) 10
KUVIO 2 Lohkoketjun ydinvaiheet (Rosic, 2019; Niranjanamurthy, Nithya & Jagannatha, 2019.) 12
KUVIO 3 Hajautetut arkkitehtuurit (Baran, 1964) 13
KUVIO 4 HASH-salauksen vaiheet (Paranello ym., 2018) 14
KUVIO 5 IoT -IoT -ratkaisu (Reyna ym., 2018) 16
KUVIO 6 IoT- Blockchain -ratkaisu (Reyna ym., 2018) 16
KUVIO 7 Hybrid – IoT -ratkaisu (Reyna ym., 2018) 17

TAULUKOT

TAULUKKO 1 Lohkoketjuteknologian käytön positiivisia vaikutuksia 18
TAULUKKO 2 Lohkoketjuteknologian käytön negatiivisia vaikutuksia 20

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT
TAULUKOT

1 JOHDANTO 6

2 ESINEIDEN INTERNET 8
2.1 Tulevaisuuden näkymät 9
2.2 IoT-laitteiden sovellusarkkitehtuuri 10

3 LOHKOKETJUT 11
3.1 Yleistä lohkoketjuista 11
3.2 Hajautettu arkkitehtuuri 12
3.3 Yksityiset ja julkiset lohkoketjut 13
3.4 Kryptografia 13
3.4.1 Avainsalaus 14
3.4.2 HASH-salaus 14

4 ESINEIDEN INTERNETIN JA LOHKOKETJUTEKNOLOGIAN YHDISTÄMINEN 15
4.1 Lohkoketjuarkkitehtuuri ongelman ratkaisuna 15
4.1.1 IoT – IoT -ratkaisu 16
4.1.2 IoT – Blockchain -ratkaisu 16
4.1.3 Hybrid-IoT -ratkaisu 17
4.2 Ratkaisujen erilaiset käyttöympäristöt 17
4.3 Positiiviset vaikutukset 18
4.4 Mahdolliset ongelmat 20

5 YHTEENVETO 22

1 JOHDANTO

IoT (Internet of Things) -laitteiden käytön suosio on kasvanut edellisten vuosien aikana kovaa tahtia niin kuluttajamarkkinoilla kuin teollisuudessakin, ja sen kasvun on ennustettu vain kiihtyvän tulevaisuudessa. Ennusteiden luvut vaihtelevat paljon lähteiden mukaan, mutta kaikilla on sama suuntaviiva, joka ennustaa IoT-laitteiden määrän vakaata ja nopeaa kasvua seuraavien vuosien aikana. Esimerkiksi Ericsson (2019) on ennustanut raportissaan kasvun olevan noin 22 % vuosittain ja McKinsey (2013) on raportissaan povannut IoT:lle keskeistä asemaa seuraavan vuosikymmenen mullistavimpana teknologiana.

Räjähdysmäisen kasvun ohella on herännyt kysymyksiä IoT-laitteiden turvallisuudesta ja keskeisten ongelmien korjaamisesta ennen kuin IoT-ekosysteemien kokonaisvaltainen käyttöönotto voidaan suorittaa (Khan, Salah, 2018). Khanin ja Salahin (2018) mukaan lohkoketjuteknologian (engl. blockchain) käyttö osana IoT-ekosysteemejä voisi olla ratkaisu suurimpien haasteiden ja kriittisten ongelmien ratkaisemiseen.

IoT:n ja lohkoketjujen yhdistämistä on alettu viimeisen viiden vuoden aikana tutkimaan enemmän ja uusia tutkimuksia on julkaistu kiihtyvällä tahdilla. Esimerkiksi IEEE Xplore -tietokannasta löytyy hakusanoilla ”IoT Blockchain” vain yksi tulos vuodelle 2015. Yhteensä julkaisuja on julkaistu kuitenkin 851 vuoden 2020 maaliskuuhun mennessä, mikä kertoo aiheen kasvaneesta suosiosta. IEE Xploressa ”IoT” ja ”Internet of Things” ovat vuoden 2020 alussa olleet kuudenneksi suosituin käsite hakutermeissä ja saatavilla olevissa dokumenteissa. Termi ”Blockchain” on samalla listalla sijalla 12.

Tämä tutkielma toteutetaan kirjallisuuskatsauksena, jonka tarkoituksena on koota yhteen tieto tämän hetkisestä tutkimuksen tilasta ja esitellä aihepiirin keskeisimmät käsitteet (Webster & Watson, 2002). Lähdeaineisto kerätään erilaisista tieteellisten artikkeleiden julkaisukanavista, kuten IEEE Xplore ja Scopus. Edellä mainittujen sivustojen lisäksi lähdekirjallisuutta on etsitty googlen Scholar -hakukoneen avulla. Lähteiden painottamisessa käytetään viittausten määrää ja julkaisujen tuoreutta. Lähteiden arvioinnissa käytetään Julkaisufoorumi.fi tarjoamaa julkaisukanahakua, joka arvostelee tieteellisiä lehtiä, sarjoja, konferensseja ja kirjakustantajia asteikolla 0-3 niiden tason perusteella.

Arvostelluista julkaisijoista tutkielmaan valitaan 2-3 tason julkaisuja, joka tarkoittaa alan johtavaa ja korkeinta tasoa.

Tutkielmassa on tarkoitus vastata näihin tutkimuskysymyksiin käyttäen hyväksi aiheeseen liittyvää tutkimustietoa ja tieteellisiä julkaisuja:

1. Millä tavalla IoT:n ja lohkoketjujen yhdistäminen voidaan toteuttaa?

2. Minkälaisia positiivisia ja negatiivisia vaikutuksia IoT:n ja lohkoketjujen yhdistämisellä on IoT-ekosysteemeihin liiketoiminnan ja teknisten ratkaisuiden kannalta?

Tutkielma on jaettu viiteen lukuun. Johdannon jälkeen ensimmäisessä sisältöluvussa on esineiden internetin eli IoT:n määrittelyn lisäksi tarkasteltu tulevaisuuden näkymiä kasvun ennusteita ja mainittu keskeisimpiä ongelmia. Tämän lisäksi luvussa on perehdytty IoT-laitteiden sovellusarkkitehtuuriin. Luvun tarkoituksena on pohjustaa aihetta ja antaa lukijalle tarvittava ymmärrys IoT-laitteista.

Toisessa sisältöluvussa kerrotaan taustaa lohkoketjuteknologian synnystä ja taustausta, jonka jälkeen lohkoketjuteknologian käsite määritellään. Määrittelyn jälkeen kerrotaan lohkoketjujen nykyisistä käyttötarkoituksista eri liikeelämän sektoreilla. Luvussa esitellään lohkoketjuteknologian ja lohkojen luomisen toimintaperiaate prosessikuvauksena. Tämän lisäksi luvussa kerrotaan myös lohkoketjujen mahdollistamasta hajautetusta arkkitehtuurista ja sen eri muodoista. Viimeisenä luvussa kerrotaan lohkoketjujen salauksesta ja siinä käytettävästä kryptografiasta. Luvussa on käytetty hyväksi Bashirin kirjaa "Mastering blockchain" (2017), jossa kerrotaan kattavasti lohkoketjuteknologiasta ja sen takana olevasta tekniikasta.

Neljännessä luvussa käsitellään IoT:n ja lohkoketjuteknologian yhdistämistä ja erilaisia malleja, joilla yhdistämine voidaan toteuttaa. Luvun tarkoituksena on kartoittaa millä tavoin lohkoketjuteknologian yhdistäminen IoT-ekosysteemeihin voidaan toteuttaa ja miten lähestymistavat sopivat erilaisiin ympäristöihin. Luvussa neljä esitellään myös edellä mainittujen teknologioiden yhdistämisen positiivisia vaikutuksia. Luvun tarkoituksena on kartoittaa IoT:n ja lohkoketjujen yhdistämisestä seuraavia positiivisia vaikutuksia liiketoiminalle sekä sitä, kuinka lohkoketjuteknologian avulla voidaan vähentää IoT-laitteiden heikkoja kohtia. Neljännen luvun viimeisessä alaluvussa kerrotaan lohkoketjujen ja IoT:n yhdistämisestä aiheutuvia mahdollisia ongelmia ja heikkoja kohtia. Tämän luvun tarkoituksena on kartoittaa, minkälaisia heikkouksia ja negatiivisia vaikutuksia IoT:n ja lohkoketjujen yhdistämisellä voi olla IoT-ekosysteemeille ja liiketoiminnalle. Neljännestä luvusta siirrytään viimeiseen, viidenteen lukuun, joka on yhteenveto. Yhteenvedossa tiivistetään tutkimuksen tulokset, esitellään jatkotutkimusaiheita sekä pohditaan mahdollisia rajoitteita tutkielmassa.

2 ESINEIDEN INTERNET

Nykyinen Internet on saanut syntynsä Massachusettsin teknillisessä yliopistossa 60-luvun lopussa. Ensimmäiset toisiinsa yhdistetyt tietokoneet sijaitsivat Massachusettsin (MIT) ja Kalifornian (UCLA) yliopistoissa. Tällöin Internet kulki vielä nimellä ARPANET eli Advanced Research Projects Agency Network. ARPANET oli pakettikytkentäinen tietokoneverkko, josta Internet myöhemmin kehittyi. (Leiner, ym., 2009.) Alkuaikoina Internetin pääasiallinen tarkoitus oli yhdistää tietokoneita toisiinsa pitkien välimatkojen takaa. Siirryttäessä kohti vuosituhannen loppua, Internetin tarkoitukseksi oli muodostunut koneiden lisäksi ihmisten yhdistäminen ympäri maailmaa. Tämän jälkeen suunta on ollut kaikkien laitteiden yhdistäminen Internettiin. (Taivalsaari & Mikkonen, 2017.) Ensimmäisen kerran esineiden Internet käsitteen on maininnut Kevin Ashton vuonna 1999. Alun perin sillä tarkoitettiin RFID (Radio Frequency IDentification) teknologiaa käyttäviä laitteita. IoT:n käyttötarkoitukset ja laitteiden käyttämät teknologiat ovat kuitenkin kehittyneet paljon edellisten vuosien aikana. (Wang, Valerdi, Zhou & Li, 2015.) Merkittävä langattomien viestintäteknologioiden kehitys on osaltaan kiihdyttänyt IoT:n kasvua ja ratkaisujen teknistä kehitystä. Erityisesti WiFi:n, 4G, 5G, RIFD ja Bluetoothin kehitys ovat olleet tärkeitä IoT:n kehitykselle. (Lund, Turner, MacGillivary & Morales 2014.)

Määritelmiä esineiden Internetille on monia, johtuen käsitteen laajuudesta. Useimmiten esineiden internetillä tarkoitetaan kuitenkin toisiinsa yhteydessä olevien laitteiden ja infrastruktuurin yhdistelmää, joka mahdollistaa näiden laitteiden ohjaamisen, tiedon louhinnan ja dataan käsiksi pääsemisen. IoT-laitteet käyttävät sensoreita ja aktuaattoreita erilaisten toimintojen suorittamiseen ja datan keräämiseen. Infrastruktuurin tehtävänä on mahdollistaa datan siirto, säilytys, prosessointi ja saatavuus käyttäjälle tai toisille järjestelmille. (Dorsemaine, Gaulier, Wary, Kheir, Urien, 2015.)

Esineiden internet voidaan jakaa karkeasti kahteen kategoriaan. Arkikielessä IoT-laitteilla viitataan yleensä kuluttaja markkinoille suunnattuihin ratkaisuihin. Kuluttajamarkkinoiden lisäksi IoT on otettu laajasti käyttöön erityisesti teollisuudessa. Ne on otettu käyttöön kaikilla yleisimmillä teollisuuden sektoreilla. IoT-laitteita tehokkaasti käyttämällä yritykset voivat kerätä suuria määriä dataa prosesseistaan ja käyttää sitä apuna liiketoiminnan kehittämisessä ja pää-

töksenteon tukena. Teollisuudessa käytettävistä IoT-laitteista käytetään käsitettä Industrial Internet of Things (IIoT). (Banafa, 2015.)

Yrityksille IoT-laitteet luovat arvoa muun muassa niiden tuottaman datan avulla. IoT-laitteiden tuottaman datan, ja sen analysoinnin avulla voidaan helpottaa yritysjohdon päätöksentekoa. Dataa voidaan tuottaa esimerkiksi erilaisista teollisuuden prosesseista IoT-laitteiden avulla. Laitteita voi olla esimerkiksi tuotantoa seuraavat sensorit ja kamerat. (Lee & Lee, 2015.)

2.1 Tulevaisuuden näkymät

IoT-laitteiden määrän on ennustettu nousevan 43 miljardiin vuoteen 2023 mennessä. Se tarkoittaa IoT-laitteiden määrän kasvua noin kolminkertaiseksi vuoteen 2018 verrattuna (Dahlqvist, Patel, Rajko, & Shulman, 2019). McKinseyn (2013) raportin mukaan IoT tulee olemaan yksi seuraavan vuosikymmenen mullistavimmista teknologioista, joka tulee muuttamaan yritysten, yhteisöjen ja talouksien toimintaa. Syynä kasvulle on uuden nanoteknologian syntyminen, valmistuskustannusten pienentyminen, laskutehon lisääntyminen sekä nopeammat ja luotettavammat langattoman yhteydet (Dahlqvist, 2019). Ericssonin (2019) raportin mukaan erilaisten IoT-laitteiden kasvun oletetaan olevan noin 20-30% vuosina 2016-2022. Kasvu on nopeaa verrattuna esimerkiksi älypuhelinten 3% ennustettuun kasvuun samalla ajanjaksolla.

Taivalsaaren ja Mikkosen (2017) mukaan olemme nyt siirtymässä esineiden internetin aikakaudelle ja vuoteen 2025 mennessä saavutamme universaalin IoT-aikakauden. Universaalin IoT-aikakauden alussa laskentatehoa pyritään siirtämään pilvestä yksittäisille IoT-laitteille. Siirtyminen laitevalmistajien ja toimialojen spesifeistä rajapinnoista universaalien rajapintojen käyttöön on seuraava harppaus kehityksessä. (Taivalsaari & Mikkonen, 2017.)

IoT-laitteiden suosion kasvun myötä myös niiden heikkouksia on alettu tarkastelemaan kriittisemmin. IoT-laitteissa ja niiden muodostamissa verkostoissa on paljon havaittuja ongelmakohtia, joiden ratkaisemiseksi olisi löydettävä keinoja ennen kuin laitteiden määrä kasvaa hallitsemattomaksi. Yksi suurimmista ongelmia aiheuttavista asioista on IoT-laitteiden ja niiden toteutuksessa käytettyjen ratkaisujen vähäinen standardointi, jonka takia esiintyy paljon yhteensopivuusongelmia. Muita ongelmia ovat muun muassa tietoturva, syntyvän datan määrä ja asiantuntijuuden vähäisyys. (Al-Qaseemi, Almulhim, H., Almulhim, M. & Chaudhry.) World Economic Forumin julkaisemassa Global Risks Report for 2018 raportissa on painotettu IoT-laitteiden merkitystä kasvavana riskinä tulevaisuudessa, joka kuvastaa hyvin havaittujen ongelmien merkitystä.

2.2 IoT-laitteiden sovellusarkkitehtuuri

IoT-laitteiden sovellusarkkitehtuuri koostuu seitsemästä eri kerroksesta, jotka Cisco (2014) on määritellyt IoT Reference Model:issa. Ensimmäisessä kerroksessa sijaitsevat kaikki fyysiset laitteet. Kuviossa 1 on kuvattu IoT reference modelin kerrokset. Fyysisen (engl. physical devices and controllers) kerroksen laitteita ovat kaikki, sensorit, laitteet ja koneet. Tämä on mallin uloin kerros eli niin sanottu edge level. Siirtoyhteyskerroksen (engl. connectivity level) tarkoituksena on toimia viestien välittäjänä yksittäisten laitteiden ja verkojen välillä. Kerros pyrkii mahdollistamaan luotettavan ja turvallisen kommunikoinnin. Tällä kerroksella myös hoidetaan erilaisten protokollien implementointi ja eri protokollien väliset muutokset. Reunalaskentakerroksella (engl. edge computing level) tapahtuu datan analysointi ja muuttaminen jalostettuun muotoon, jota voidaan myöhemmin käyttää varastointiin ja tarkempaan analysointiin. Fyysisen kerroksen laitteet tuottavat jatkuvasti dataa, jonka hyödyntämiseksi sitä täytyy jalostaa, jotta sitä voidaan tehokkaasti hyödyntää. Varastointikerroksen (engl. data accumulation level) tehtävänä on muuttaa liikkuva data paikallaan olevaksi dataksi. Tarkoituksena on muuttaa analysoitu data verkkopaketeista tietokantoihin, joista ohjelmat sitä lukevat. Tällä tasolla relevantti data pyritään erottamaan turhasta ja siten vähentää tallennettavan datan määrää. Tiedon erottelukerroksella (engl. data accumulation level) tallennetusta datasta erotellaan oikea informaatio sovellusten käyttöön. Sovelluskerroksella (engl. application level) sijaitsevat ohjelmistot, jotka muuttavat kerätyn informaation luettavaan muotoon. Tähän kerrokseen kuuluvat erilaiset ERP-järjestelmät, BI-raportointiohjelmat, mobiiliapplikaatiot ja analytiikkaohjelmat. Yhteistyö- ja prosessikerroksen (engl. collaboration and processes level) tarkoituksena on yhdistää kuudennen tason ohjelmistot, organisaatioiden prosessit ja työntekijät. (Cisco, 2014).

KUVIO 1 IoT Reference Model (Cisco, 2014.)

3 LOHKOKETJUT

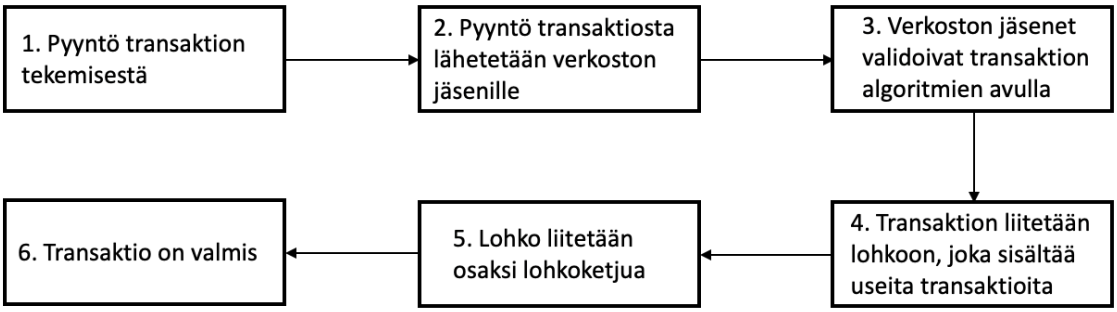
Lohkoketjuteknologia (engl. blockchain) tuli maailmalle tutuksi vuonna 2009 kun henkilö tai ryhmä nimeltä Satoshi Nakamoto julkaisi Bitcoinin. Bitcoinin ansiosta lohkoketjut ovat nousseet yleiseen tietoisuuteen 2010-luvulla. Marc Andreessen, ensimmäisen selaimen tekijä ja sijoittaja, on kuvaillut lohkoketjuteknologiaa yhdeksi 2000-luvun suurimmaksi tietotekniikan läpimurroksi. Vähitellen lohkoketjujen käyttö on saanut huomiota myös finanssialan ulkopuolella, jossa sitä on alettu hyödyntää muun muassa teollisuudessa. Bitcoinin rinnalle on syntynyt suuri määrä muita lohkoketjuja, mutta perusperiaate on niissä kaikissa sama. (Sidhu & Fred-Ojala, 2018.)

3.1 Yleistä lohkoketjuista

Lohkoketju on tietorakenne, joka mahdollistaa transaktioiden tekemisen, taltioinnin ja jakamisen turvallisesti ja läpinäkyvästi hajautetun verkon jäsenten kesken. Läpinäkyvyyden ja hajautetun rakenteen ansiosta kaikki verkon jäsenet pystyvät osallistumaan transaktioiden tekemiseen ilman kolmannen osapuolen valvontaa. (Norton, 2016.) Yksinkertaistettuna lohkoketju on hajautettu, julkinen tietokanta, joka on jaettu siihen osallistuvien osapuolten kesken. Lohkoketjun tarkoituksena on luoda pysyvä jälki kaikista tapahtuneista transaktioista. Ketjua ei pysty poistamaan tai sen osia jälkikäteen muuttamaan. (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2016.) Lohkoketjun toiminta koostuu viidestä ydinvaiheesta. Kuviossa 2 on esitetty viisi ydinvaihetta käyttäen esimerkkinä kryptovaluuttojen transaktioprosessia.

- Verkon jäsen haluaa tehdä transaktion.
- Halututtu transaktio lähetetään kaikille verkon jäsenille validoitavaksi.
- Verkon jäsenet validoivat transaktion sisällön, sekä lähettäjän statuksen algoritmien avulla.
- Validoinnin jälkeen haluttu tieto, kuten kryptovaluutta, älysopimus tai muu data, pakataan muiden transaktioiden kanssa yhteen lohkoon. Lohko voi siis sisältää useampia transaktioita.

- Lohko yhdistetään pysyväksi osaksi lohkoketjua. Ketjuun liittämisen jälkeen lohkon sisältämää dataa ei voi enää muuttaa. (Niranjanamurthy, Nithya & Jagannatha, 2019.)



KUVIO 2 Lohkoketjun ydinvaiheet (Rosic, 2019; Niranjanamurthy, Nithya & Jagannatha, 2019.)

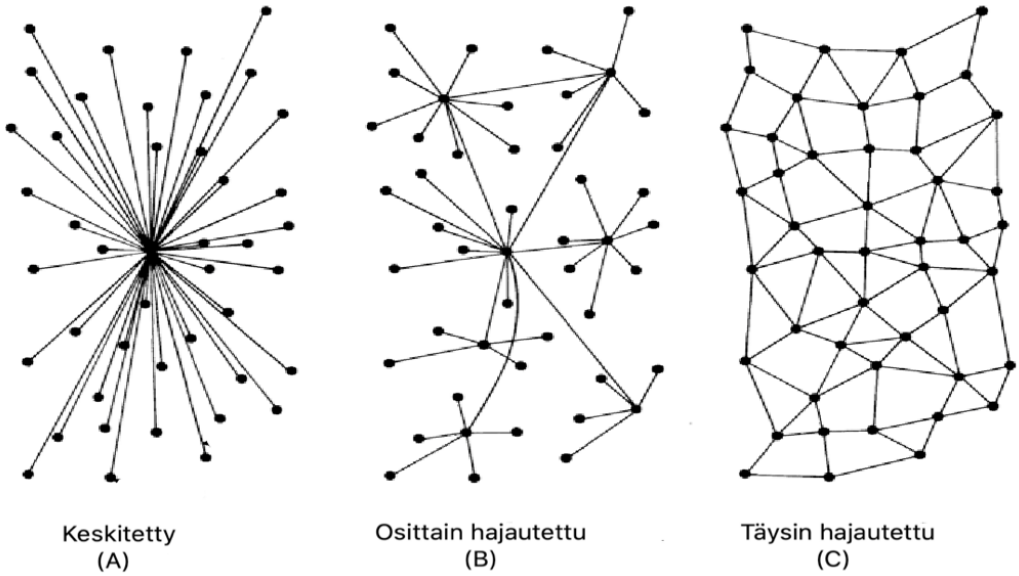
Näkyvin lohkoketjujen käyttötarkoitus tällä hetkellä on kryptovaluutat. Niiden käyttö on yleistynyt ja bitcoinin rinnalle on syntynyt tuhansia erilaisia kryptovaluuttoja. Rahoitusala hyödyntää lohkoketjuja, koska se mahdollistaa paremman tietoturvan, muuttumattomuuden, läpinäkyvyyden ja poistaa tarpeen kolmannelle osapuolelle (Underwood, 2016.). Myös muut alat ovat alkaneet käyttämään lohkoketjuja liiketoiminnan tehostamisessa. (Marr, 2019.)

Esimerkiksi IBM on kehittänyt logistiikka ja tuotantojärjestelmiä, jotka käyttävät lohkoketjuja hyväkseen. Lohkoketjujen avulla mahdollistetaan mm. läpinäkyvä tuotteiden paikantaminen ja omistajuustietojen jakaminen. (IBM, 2020.) Toisena hyvänä esimerkkinä lohkoketjujen laajoista käyttömahdollisuuksista on viihde ja musiikkiteollisuudessa Spotify, joka on alkanut hyödyntämään lohkoketjuja hajautetun musiikkitietokannan luomisessa (Perez, 2017).

3.2 Hajautettu arkkitehtuuri

Lohkoketjujen ansiosta on pystytty luopumaan keskitetystä mallista ja siirtymään hajautettuun arkkitehtuuriin. Hajautettu (engl. distributed) malli poistaa auktoriteetin tarpeen, kuten pankin, transaktion osapuolten toimintaa valvovana osapuolena. (Bashir, 2017.) Hajautettu malli tekee verkosta huomattavasti vakaamman kuin keskitetty malli, koska taakka on jaettu verkon jäsenille yhden keskitetyn palvelimen sijaan. Hajautettu malli mahdollistaa myös verkoston orgaanisen kasvun siihen osallistuvien osapuolten määrän kasvaessa. Verkon laskentakyky kasvaa, kun siihen lisätään jäseniä. Laskentatehon määrä ja sen edullisuus on myös yksi hajautetun verkon suurimpia etuja. (Drescher, 2017.) Keskitetyssä (engl. centralized) mallissa pankki toimii transaktion vahvistajana ja validoi rahan liikkumisen. Lohkoketjuja hyödyntävät kryptovaluutat mahdollistavat turvallisen transaktion kahden yksilön välillä ilman välikäsiä. (Neittaanmäki & Ogbechie, 2016.) Täysin hajautetun mallin lisäksi on olemassa

vain osin hajautettuja (engl. decentralized/semi-decentralized) verkostoja, joissa esimerkiksi verkkoon kuuluvat koneet tai pilvipalvelu ylläpitää osaa datasta. Kuvio 3. on havainnollistava kuva kaikista kolmesta mallista. (Bashir, 2017.)



KUVIO 3 Hajautetut arkkitehtuurit (Baran, 1964)

3.3 Yksityiset ja julkiset lohkoketjut

Lohkoketjut on jaettu yleisesti yksityisiin ja julkisiin, sen mukaan miten ne ovat saatavilla, ja kuka niiden osaksi voi liittyä. Julkisella lohkoketjulla tarkoitetaan ketjua, johon liittyminen on vapaata ja sillä ei ole omistajaa. Julkisia lohkoketjuja ovat esimerkiksi kryptovaluutat Bitcoin ja Ethereum. Julkisten lohkoketjujen rinnalle on syntynyt yksityisiä ja osittain yksityisiä muotoja lohkoketjuista. Yksityisissä lohkoketjuissa verkkoon liittymiseen ja transaktioiden tekemiseen tarvitaan lohkoketjun omistajan lupa. Yksityisiä lohkoketjuja ovat esimerkiksi valtioiden ja yritysten sisäiset järjestelmät ja niiden lohkoketjut. Osittain yksityisellä tarkoitetaan sitä, että yksityinen taso kontrolloi osaa lohkoketjusta, mutta muuten siihen liittyminen on vapaata. (Bashir, 2017.; Zheng, Xie, Dai, Chen & Wang, 2017.)

3.4 Kryptografia

Lohkoketjujen hajautetun arkkitehtuurin ja pysyvyyden ansiosta sen sisältämä tieto on luotettavaa ja helposti saatavilla, mutta tietoturvaa se ei luonnostaan tarjoa. Tietoturvan takaamiseksi lohkoketjut käyttävät useita eri suojauksen keinoja, mutta niistä keskeisimpinä ovat avainsalaus ja HASH-salaus. (Kosba, Miller, Shi, Wen & Papamanthou, 2016.)

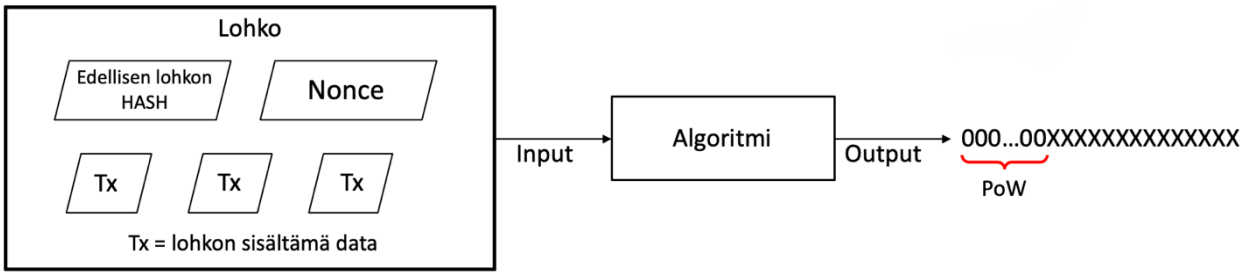
3.4.1 Avainsalaus

Lohkoketjun salauksen lisäksi myös transaktiot on suojattu. Suojaamisessa käytetään salausavaimia. Jokaisella verkon jäsenellä on julkinen ja salainen avain, joiden avulla transaktion osapuolten identiteetit varmistetaan oikeiksi. Transaktion lähettäjä käyttää salaista avainta transaktion lähettämiseen, jota transaktion vastaanottaja vertaa julkisesti saatavilla olevaan julkiseen lähettäjän avaimeen. Transaktio toteutuu, jos julkinen ja salainen avain sopivat toisiinsa. (Bashir, 2017.)

3.4.2 HASH-salaus

Lohkoketjun salauksessa käytetään Cascaded Encryption menetelmää. Cascaded Encryption tarkoittaa sitä, että jokaisen uuden lohkon salauksessa käytetään edellisen lohkon HASH-salauksen tulosta. Tämän ansiosta lohkojen sisältöä ei voi muuttaa jälkikäteen, koska tällöin lohkojen HASH-salauksien summa ei täsmää. Yleisimmin käytetty HASH-salaus on SHA-256, joka on käytössä myös bitcoinissa. SHA-256 luo aina 256 merkkisen jonon kirjaimia ja numeroita annetusta datasta. Kaikki HASH salaukset toimivat pohjimmiltaan samalla periaatteella. Annetusta tiedosta muodostetaan standardimittainen jono lukuja ja kirjaimia. HASH salaus toimii vain yhteen suuntaan, eli salattua tietoa on käytännössä mahdoton enää selvittää. (Bashir, 2017.)

Lohko validoidaan PoW-konsensusmenettelyn (Proof-of-Work) avulla, jossa jokaisen lohkon HASH-luvun alun tulee vastata lohkoketjulle annettua standardia. Jos esimerkiksi lohkoketjun PoW on numerot 000 jokaisen lohkon HASH:in ensimmäisinä numeroina. Tällöin lohkojen louhijat laskevat niin kauan uusia HASH-lukuja lohkolle, kunnes saavat sen validoitua PoW:n mukaisesti. Nonce on satunnainen luku, jota käytetään HASH:n luomisessa. Myös lohkon sisältämää dataa käytetään osana HASH-luvun luomista. (Paranello, Tapas, Merlino, Longo, & Puliafito, 2018.) Kuvio 4 on havainnollistava kuvaus HASH-luvun luomisesta.



KUVIO 4 HASH-salauksen vaiheet (Paranello ym., 2018)

4 ESINEIDEN INTERNETIN JA LOHKOKETJUTEKNOLOGIAN YHDISTÄMINEN

IoT-laitteiden määrän kasvaessa ja niiden tuottaman datan määrän räjähdysmäinen kasvu vaativat paljon varastointi- ja laskentaresursseja. Pilvipalvelut ovat mahdollistaneet reaaliaikaisen datan analysoinnin ja informaation prosessoinnin, joka on vienyt IoT-laitteiden käytettävyyttä eteenpäin viimevuosien aikana. Pilvipalveluiden käyttämä keskitetty infrastruktuuri kuitenkin altistaa datan monille erilaisille tietoturvauhkille. Tietoturvauhkien lisäksi keskitetty infrastruktuuri ei mahdollista datan läpinäkyvyyttä eikä tietoa siitä mihin dataa on siirretty ja minkälaiseen käyttötarkoitukseen. Sen takia uusien ratkaisujen löytäminen on tärkeää ja lohkoketjujen tarjoama hajautettu infrastruktuuri voi olla ratkaisu nykyisten keskitettyjen arkkitehtuurien sisältämiin ongelmiin. (Mahmoud, Yousuf, Aloul, & Zualkernan, 2015.)

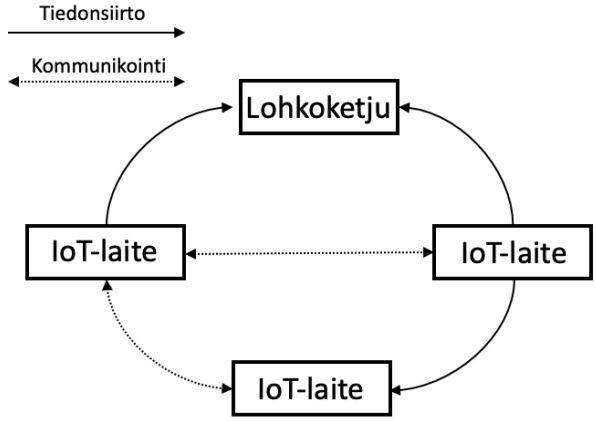
4.1 Lohkoketjuarkkitehtuuri ongelman ratkaisuna

Nykyisten IoT-järjestelmien käyttämät keskitetyt serverit muodostavat pullonkauloja, joihin kyberhyökkäykset on helppo kohdistaa ja siten vaikuttaa koko verkon toimintaan ja datan luotettavuuteen. Ongelman ratkaisemiseksi on ehdotettu lohkoketjuteknologian käyttöä. Lohkoketjulla mahdollistetaan datan tallennus hajautettuun, jaettuun ja luotettavaan tietokantaan, jolla pystytään varmistamaan tallennetun datan luotettavuus. Hajautetun arkkitehtuurin ansiosta pullonkaulojen määrä on minimoitu ja siten heikkojen kohtien määrä on saatu minimoitua. Lohkoketjujen avulla voidaan myös ratkaista ongelmat, jotka liittyvät IoT-laitteiden ja taustalla olevien servereiden väliseen luottamukseen ja transaktioiden taltioimiseen. Lohkoketjujen käyttämisellä osana IoT-ekosysteemeitä voidaan siis tehostaa IoT-laitteiden tuomia hyötyjä samalla ratkaisten niihin liittyviä ongelmia. Lohkoketjujen avulla voidaan tehostaa IoT-ekosysteemeiden toimintaa ja siten tehostaa liiketoimintaprosesseja. (Liang, Zhao, Shetty, Li, 2017.) Seuraavissa alaluvuissa on esitetty kolme eri tapaa, joilla

IoT-laitteiden ja niiden luomien ekosysteemeiden yhdistäminen lohkoketjuteknologiaan voidaan toteuttaa.

4.1.1 IoT – IoT -ratkaisu

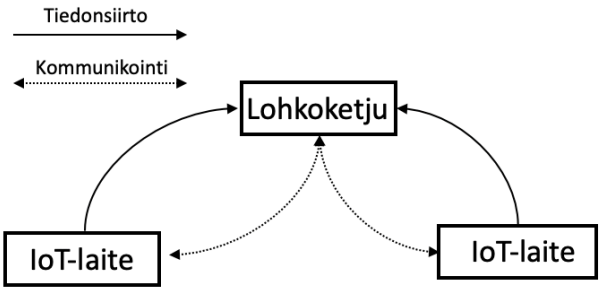
IoT – IoT ratkaisussa lohkoketjuun on taltioitu osa syntyneestä datasta. Muuten laitteiden välinen kommunikointi tapahtuu normaalien verkkolaiteiden välityksellä. Tällä lähestymistavalla viive on saatu minimoitua laitteiden välisessä kommunikoinnissa ja tiedonsiirrossa. IoT – IoT ratkaisu on paras tilanteisiin, joissa datan kulun on oltava nopeaa ja luotettavaa. Tietoturvallisuus IoT – IoT ratkaisussa on erittäin hyvä, koska laitteiden ei tarvitse olla yhteydessä Internettiin, vaan ne voivat kommunikoida keskenään suljetussa verkossa. (Reyna, Martin, Chen, Soler, & Diaz, 2018.) Kuvio 5 havainnollistaa IoT – IoT -ratkaisun toimintaa.



KUVIO 5 IoT -IoT -ratkaisu (Reyna ym., 2018)

4.1.2 IoT – Blockchain -ratkaisu

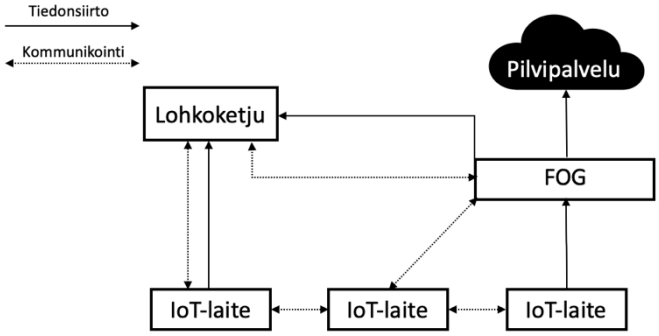
IoT – Blockchain lähestymistavassa kaikki liikenne menee lohkoketjun läpi, luoden historian kaikista tapahtuvista transaktioista. Lohkoketjuun siis tallennetaan kaikki syntyvä data ja tiedot laitteiden välisestä kommunikoinnista. Lohkoketjun ansiosta jokainen transaktio ja niiden sisältö on mahdollista jäljittää. Tämä ratkaisu myös lisää IoT-laitteiden itsenäisyyttä. Ongelmana on lisääntyvä tiedonsiirron määrä ja tarve suuremmalle kaistanleveydelle, joka kasvattaa toimivan kokonaisuuden vaatimia järjestelmävaatimuksia. (Reyna ym., 2018.) Kuvio 6 havainnollistaa IoT – Blockchain -ratkaisun toimintaa.



KUVIO 6 IoT- Blockchain -ratkaisu (Reyna ym., 2018)

4.1.3 Hybrid-IoT -ratkaisu

Hybridi lähestymistavassa on pyritty yhdistämään IoT – IoT ja IoT – Blockchain ratkaisujen parhaimmat puolet mahdollisimman monipuolisen mallin luomiseksi. Osa laitteiden välisestä kommunikoinnista ja tuotetusta datasta tallennetaan lohkoketjuun. Loput kommunikoinnista ja tiedon tallennuksesta tapahtuu laitteiden välillä. Molempien teknologioiden hyödyntäminen mahdollistaa lohkoketjun positiiviset ominaisuudet ja IoT-laitteiden nopean kahdenkeskisen kommunikoinnin. Hybrid-IoT käyttää usein myös hyväkseen pilvi- ja FOG-palveluita, jotka mahdollistavat suuremman laskentatehon käytön. (Reyna ym., 2018.) FOG-laskennalla tarkoitetaan mallia, jossa osa datasta ja prosessoinnista suoritetaan verkon reunalla olevissa laitteissa. FOG-laskennan avulla saadaan vähennettyä pilvipalveluiden tarvetta ja samalla hyödynnettyä kasvavien IoT-verkostojen laskentatehoa. (Bonomi ym., 2012.) Kuvio 7 havainnollistaa Hybridi-IoT -ratkaisun toimintaa.



KUVIO 7 Hybrid – IoT -ratkaisu (Reyna ym., 2018)

4.2 Ratkaisujen erilaiset käyttöympäristöt

Edellä mainitulla ratkaisuilla on omat vahvuutensa erilaisissa toimintaympäristöissä. On tärkeää, että valittu ratkaisutapa vastaa toimintaympäristön asettamia vaatimuksia. Sen avulla voidaan varmistaa tehokkain ja taloudellisin lopputulos. IoT-IoT -ratkaisu on paras vaihtoehto, kun halutaan mahdollisimman kevyt ja kustannustehokas malli. Ratkaisu on paras ympäristöön, jossa laskentatehon tarve on pientä, tieto ei ole sensitiivistä ja viiveajat halutaan minimoida. IoT-Blockchain -ratkaisu toimii parhaiten ympäristössä, jossa liikutellaan paljon arkaluonteista tietoa, jonka salaus ja luotettava tallennus on keskeisessä asemassa. Hybrid-IoT -ratkaisua saadaan hyödynnettyä tehokkaimmin, kun se yhdistetään osaksi IoT-ekosysteemiä, jossa käsitellään arkaluontoista dataa, mutta osa toiminnoista on suoritettava mahdollisimman pienellä viiveellä. Hybrid-IoT -ratkaisu mahdollistaa myös suuremman laskentatehon käytön muuan muassa reunalaskennan avulla. Hybrid-IoT sopii parhaiten tilanteisiin, joissa tarvitaan kokonaisvaltainen ratkaisu IoT-ekosysteemin rinnalle. (Reyna ym., 2018; Bonomi ym., 2012.)

4.3 Positiiviset vaikutukset

Kaikki ratkaisut, jotka yhdistävät useita eri käyttäjiä tai laitteita voivat hyötyä lohkoketjujen käyttämisestä osana niiden verkostoja. IoT-laitteiden muodostamat ekosysteemit sisältävät paljon laitteita ja niiden välillä tapahtuu jatkuvasti transaktioita, joissa lohkoketjuteknologiaa voidaan käyttää muun muassa luotettavuuden ja turvallisuuden parantamiseen. (Ramachandran & Krishnamachari, 2018.) Taulukossa 1. ja sitä seuraavassa kappaleessa on esitetty positiivisia vaikutuksia, joita on havaittu seuraavan lohkoketjujen yhdistämisestä osaksi IoT-ekosysteemejä.

TAULUKKO 1 Lohkoketjuteknologian käytön positiivisia vaikutuksia

Positiiviset vaikutukset
Hajautettu infrastruktuuri
Yksilöity identiteetti
Autonomia
Tiedon luotettavuus ja pysyvyys
Turvallisuus
Palvelumarkkinat
Koodin sisäänajo ja päivitykset
Saatavilla olevat resurssit
Kustannusten laskeminen

Yksi suurimmista lohkoketjun eduista on siirtyminen keksitetystä infrastruktuurista hajautettuun Peer-to-Peer (P2P) malliin. Hajautetun infrastruktuurin avulla voidaan välttää järjestelmään syntyvät pullonkaulat ja heikot kohdat. Hajautetun infrastruktuurin ansiosta suurten organisaatioiden ei ole mahdollista hallita verkkoa ja siten suurta määrää ihmisten ja laitteiden tuottamasta datasta. Pullonkaulojen poistumisen ja sen mahdollistaman nopeamman tiedonsiirron ansiosta IoT-ratkaisujen parempi skaalautuminen on mahdollista. (Reyna, Martin, Chen, Soler & Diaz, 2017.) Koska valtaosan verkon jäsenistä on validoitava jokainen transaktio, on verkon sisäinen luottamus korkea (Samaniego & Deters, 2016). Lisäksi hajautettu arkkitehtuuri vähentää keskittynyttä dataliikennettä ja siten parantaa IoT-ekosysteemien vakautta (Atlam, Alenezi, Alassafi & Wills, 2018).

Lohkoketjun ansiosta yksittäisten IoT-laitteiden tunnistaminen ja transaktioiden seuraaminen olisi mahdollista. Jokainen laitteiden välinen transaktio siirtyy osaksi lohkoketjua ja on siten aina jäljitettävissä. Yksilöidyn identiteetin avulla voidaan myös varmistaa, että vastaanotettu data on tullut varmasti oikealta laitteelta. Yksilöidyn identiteetin luomiseksi käytetään hyväksi julkisia ja yksityisiä avaimia, sekä laitteiden omia UID (Unique Indetifier) koodeja. Yksilöidyn identiteetin ansiosta transaktioiden turvallisuus ja läpinäkyvyys paran-

tuu huomattavasti. (Reyna ym., 2017.) Vaikka jokainen käyttäjä on tunnistettavissa niin käyttäjän oikean identiteetti on silti anonyymi (Atlam, Alenezi, Alassafi & Wills, 2018). Tämä mahdollistaa sen, että yksittäisiä laitteita ja niiden transaktioita ei voi yhdistää yksittäiseen laitteiseen ja organisaatioon. Sen ansiosta laitteet voivat lähettää verkon sisällä kriittistä tietoa sisältäviä transaktioita ilman että kukaan osaa kohdistaa hyökkäystä kyseisen laitteeseen. (Ramachandran & Krishnamachari, 2018.)

Lohkoketjujen avulla mahdollistetaan IoT-laitteiden siirtyminen autonomisempaan toimintaympäristöön. Siirtyminen hajautettuun infrastruktuurin tarkoittaa myös sitä, että laitteet eivät tarvitse keskitettyjä servereitä transaktioiden suorittamiseen ja kommunikointiin. Autonomia mahdollistaa universaalien laitteiden ja ohjelmistojen kehittämisen, koska niiden ei tarvitse olla yhteensopivia palvelimien ja niiden ohjelmistojen kanssa, jotka usein eroavat laitevalmistajien välillä. (Reyna ym., 2017.)

IoT-laitteiden tuottaman datan säilöminen lohkoketjussa mahdollistaa luotettavuuden ja pysyvyyden takaamisen. Lohkoketjujen muokkaaminen jälkikäteen ei ole mahdollista, joten dataan voidaan aina palata ja luottaa sen oikeellisuuteen. Tämä mahdollistaa erityisesti sensorien tuottaman datan jäljittämisen ja siihen luottamisen. Tiedon luotettavuus onkin yksi suurimmista lohkoketjujen tarjoamista hyödyistä. (Reyna ym., 2017.) Kaikki keskitetyt tietokannat ovat alttiita hyökkäyksille, ja vastuu tietokantojen luotettavuudesta on yleensä kolmannen osapuolen vastuulla. Lohkoketjut poistavat tämän ongelman, koska tietokanta on jaettuna kaikille verkkoon kuuluville jäsenille. Hyökkääjällä tulisi olla pääsy valtaosaan verkon laitteista, jotta se pystyisi muokkaamaan lohkojen sisältöä. (Atlam, Alenezi, Alassafi & Wills, 2018.)

Lohkoketjut tarjoavat IoT-laitteiden väliselle kommunikoinnille ja niiden tuottamalle datalle mahdollisuuden parantaa tietoturvaa erilaisten enkryptaus menetelmien avulla. Itse lohkot on suojattu cascaded HASH kryptauksella, jonka murtaminen on lähes mahdotonta nykyisellä laskentateholla. Tämän lisäksi laitteiden kommunikointi toteutetaan älysopimusten avulla, joissa käytetään julkisia ja yksityisiä avaimia osapuolten identiteetin varmistukseen. Tämän lisäksi laitevalmistajien omat tietoturvaohjelmistot on helppo sulauttaa toimimaan yhdessä lohkoketjun kanssa. (Reyna ym., 2017.) Lohkoketjut tarjoavat mahdollisuuden toimia turvallisesti verkossa, joka sisältää suuren määrän heterogeenisiä laitteita. Tämä mahdollistaa sen, että yritykset voivat hyödyntää julkisia lohkoketjuja omassa toiminnassaan, huolehtimatta tietoturvan vaarantumisesta. (Dorri, Kanhere, Jurdak, 2016.)

Lohkoketjujen avulla voidaan mahdollistaa markkinapaikka, jossa datan ja palveluiden myynti ja ostaminen tapahtuu verkoston jäsenten kesken. Lohkoketjut mahdollistavat myös mikromaksut, joiden ansiosta transaktiot nopeutuvat ja halpenevat. (Reyna, 2017.) Erityisesti suurten IoT-ekosysteemien kuten älykaupunkien toiminnassa datan ja laskentakyvyn kauppaaminen verkon jäsenten kesken mahdollistaa sen tehokkaan toiminnan. Mikromaksujen avulla verkon jäsenet saavat rahallisen korvauksen datan tai resurssien käytöstä ja siten palkitsee verkon jäseniä ekosysteemin tehokkaasta ylläpidosta. (Ramachandran & Krishnamachari, 2018.) Tämän kaltaiset palvelumarkkinat voivat mah-

dollistaa yrityksille ylimääräisten resurssien ja kertyneen datan muuttamisen liiketoiminnaksi.

IoT-laitteisiin ajettavat päivitykset ovat lohkoketjujen ansiosta helppo varmentaa ja päivityshistorian seuraaminen on helppoa. Päivitysten turvallinen ajaminen laitteisiin lisää tietoturvaa huomattavasti IoT-laitteissa. (Reyna ym., 2017.) Mitä enemmän verkossa on laitteita, sitä enemmän resursseja sillä on käytössä. Tuhansien laitteiden verkostoilla on käytössään huomattavasti enemmän laskentatehoa kuin keskitetyillä servereillä. (Atlam ym., 2018) Keskitettyjen servereiden skaalaaminen ja ylläpito on kallista, joten hajautetun verkon käyttö voi laskea kustannuksia tehokkaasti. (Atlam ym., 2018) McKineseyn raportin (2018) mukaan lyhyellä aikavälillä lohkoketjujen käyttö mahdollistaa kustannusten laskemisen. Pidemmällä aikavälillä lohkoketjujen käyttö voi myös luoda kassavirtaa. Vaikka

4.4 Mahdolliset ongelmat

Tässä luvussa perehdytään ongelmiin, joita lohkoketjujen käyttö IoT-laitteissa voi aiheuttaa. Yksi keskeisimmistä ongelmista on se, että lohkoketjuteknologia on suunniteltu käytettäväksi tehokkailla tietokoneilla, kun taas puolestaan IoT-laitteet ovat useimmiten kevyitä ja omaavat vähän suorituskykyä. Lohkoketjuteknologiaa on myös kritisoitu sen huonosta skaalautumisesta ja tallenustilaan liittyvistä ongelmista. Osa havaituista ongelmista tulee vielä näkyvämmin esille, kun lohkoketjut yhdistetään IoT-laitteisiin ja niiden luomiin verkostoihin. (Reyna ym. 2018.) Taulukossa 2. ja sitä seuraavassa kappaleessa on esitetty mahdollisia ongelmia, joita on havaittu seuraavan lohkoketjujen yhdistämisestä osaksi IoT-ekosysteemejä.

TAULUKKO 2 Lohkoketjuteknologian käytön negatiivisia vaikutuksia

Mahdolliset ongelmat
Kyberhyökkäykset
Prosessointiteho ja aika
Skaalautuvuus
Tallennustila
Asiantuntijuuden puute
Lailliset ongelmat
Nimeäminen ja laitteiden löytäminen

Vaikka lohkoketjujen turvaamisessa käytetään useita erilaisia salauksia ja protokollia on se silti haavoittuvainen useille tunnetuille hyökkäyksille. Hyökkäyksien tarkoituksena on lohkoketjun sisältämän datan muokkaus ja uuden virheellisen datan lisääminen osaksi ketjua. Hyökkäykset voidaan jakaa karkeasti viiteen kategoriaan, jotka ovat identiteettiin perustuvat hyökkäykset (engl. identity based attacs), manipulaatioon perustuvat hyökkäykset (engl. manipu-

lation-based attacks), kryptoanalyyttiset hyökkäykset (engl. crypto-analytic atta s), luotettavuuteen perustuvat hyökkäykset (engl. reputation-based attacks), viimeisenä kategoriana on palvelimiin kohdistuvat hyökkäykset (engl. denial of Service attacs). (Ferrag, Derdour, Mukherjee, Derhab, Mag- laras & Janicke, 2018.) Kyberhyökkäykset voivat vaikuttaa negatiivisesti järjestelmien saatavuuteen ja luotettavuuteen, erityisesti kun tarkastellaan laajoja IoT-ekosysteemejä.

Skaalautuvuuteen liittyvät ongelmat voivat johtaa siihen, että joudutaan siirtymään takaisin kohti keskitettyä arkkitehtuuria. Lohkoketjut skaalautuvat huonosti solmukohtien määrän kasvaessa. Heikko skaalautuvuus saattaa tulevaisuudessa koitua suureksi ongelmaksi, koska IoT-ekosysteemit sisältävät paljon solmukohtia. (Samaniego & Deters, 2016.)

Yksi lohkoketjujen hyvistä puolista on keskitetyn rakenteen tarpeettomuus. Koska keskitettyjä servereitä ei tarvita enää datan varastointiin, tallennus tapahtuu lohkoketjuverkon solmukohtiin. Ongelmia alkaa kuitenkin syntymään, kun datan määrä ketjussa alkaa kasvamaan eikä IoT-laitteiden laskentateho ja tallennustila riitä sen ylläpitämiseen. IoT-laitteet harvoin omaavat paljon tallennustilaa tai laskentaresursseja. (Atlam, 2018.)

Lohkoketjuteknologia on syntynyt vasta viimeisen vuosikymmenen aikana, joten alan osaajista on paljon pulaa. Tällä hetkellä osaajia löytyy eniten finanssialalta, jossa lohkoketjut ovat olleet pisimpään käytössä. Muilla aloilla osaajista on paljon pulaa ja siten hidastaa lohkoketjujen käyttöönottoa. (Atlam, 2018.)

Lohkoketjujen tai IoT-laitteiden käytölle ei ole laillisia rajoituksia tai protokollaa. Tämä vaikeuttaa palveluntarjoajien ja valmistajien toimintaa, koska toiminnalle ei ole selkeitä suuntaviivoja. Suurimmat ongelmat liittyvät siihen, että julkisilla lohkoketjuilla ei ole omistajaa. Koska lohkoketjulla ei ole omistajaa, niin tietovuodon sattuessa vastuun määrittely on vaikeaa. Tämän lisäksi maanosilla on erilaisia lakeja ja säädäntöjä, joiden noudattaminen ja tulkitseminen on vaikeaa. Tästä hyvänä esimerkkinä Euroopassa uusi GDPR-säädäntö, joka on muokannut todella paljon järjestelmien vaatimuksia. (Fabiano, 2017.) Ratkaisuna tähän voisi olla, että yritysten ja organisaatioiden käyttöön luotaisiin standardisoitu viitekehys, jota sovellettaisiin maiden omien lakien kanssa. Viitekehyksellä voitaisiin saavuttaa yhtenäisempi pohja, joiden päälle IoT-ekosysteemit pystytetään.

Lohkoketjuteknologia on syntynyt vasta viimeisen vuosikymmenen aikana, joten alan osaajista on paljon pulaa. Tällä hetkellä osaajia löytyy eniten finanssialalta, jossa lohkoketjut ovat olleet pisimpään käytössä. Muilla aloilla osaajista on paljon pulaa ja siten hidastaa lohkoketjujen käyttöönottoa. Osaajien puutteen vuoksi uusien ratkaisujen toteuttaminen on hankalaa ja ennestään hidastaa teknologian yleistymistä. (Banafa, 2017.)

Lohkoketju on suunniteltu niin, että verkon jäsenillä ei ole tietoa toisten jäsenten sijainnista, vaan ne näkevät vain viereiset laitteet verkossa. IoT-laitteiden on kuitenkin pystyttävä kommunikoimaan toisten laitteiden kanssa ja siksi myös tiedettävän niiden sijainti verkon sisällä. (Dorri, Kanhere, Jurdak & Guaravaram, 2017.)

5 YHTEENVETO

Tässä kirjallisuuskatsauksena toteutetussa kandidaatintutkielmassa tutkittiin, kuinka lohkoketjuteknologiaa voidaan hyödyntää IoT-laitteiden luomissa verkostoissa. Aiheen tutkimus on tärkeää ja ajankohtaista, koska IoT:n ja lohkoketjujen käyttö osana liiketoimintaa tulee ennusteiden mukaan kasvamaan paljon lähitulevaisuudessa. Erityisesti edellä mainittujen teknologioiden yhdistämisen mahdollisuuksista on käyty paljon keskustelua viimeisten vuosien. Aiheeseen liittyvä tutkimus on yleistynyt paljon vuoden 2015 jälkeen. Tutkielmassa pyrittiin vastaamaan kahteen asetettuun tutkimuskysymykseen, jotka olivat *Millä tavalla IoT:n ja lohkoketjujen yhdistäminen voidaan toteuttaa? Minkälaisia positiivisia ja negatiivisia vaikutuksia IoT:n ja lohkoketjujen yhdistämisellä on IoT-ekosysteemeihin liiketoiminnan ja teknisten ratkaisuiden kannalta?*

Tutkielma aloitettiin IoT:n ja lohkoketjujen määrittelyllä. Molempien käsitteiden yhteydessä kerrottiin niihin liittyvät keskeiset teknologiat ja tulevaisuuden kehityssuuntia. Molempien käsitteiden kohdalla kasvun on todettu olevan nousussa ja tulevaisuudessa niiden merkitys liiketoiminnalle tulee ennestään kasvamaan. Käsitteiden määrittelyn jälkeen tutkielmassa siirryttiin käsittelemään teoreettisia malleja, joiden mukaan lohkoketjujen ja IoT-ekosysteemeiden yhdistäminen voidaan toteuttaa. Tutkimuksessa saatiin selville kolme erilaista mallia; IoT-IoT -malli, IoT-Blockchain -malli ja Hybrid-IoT -malli. Jokainen tutkielmassa esitetty malli sopii tietyt kriteerit täyttävään ympäristöön. IoT-IoT -mallin käyttö sopii parhaiten kevyeen ympäristöön, jossa laskentatehoa tai tallennustilaa ei tarvita paljon. IoT-Blockchain -malli sopii hyvin esimerkiksi älykotien ratkaisuksi, koska viiveajoilla ei ole suurta merkitystä ja laskentatehon tarve on vähäistä. Hybrid-IoT -malli soveltuu parhaiten esimerkiksi teollisuuden ja muiden suurien IoT-ekosysteemien yhteyteen. Hybrid-IoT mahdollistaa parhaimman ratkaisun, kun tarvitaan paljon laskentatehoa ja tuotetun datan määrä on suuri. Tutkielmassa esitetyt mallit vastaavat tämän hetkisen tutkimuksen tuloksia, mutta jatkotutkimuksen avulla uusia malleja voi tulevaisuudessa syntyä.

Teoreettisten mallien lisäksi tutkielmassa selvitettiin IoT-laitteiden muodostamien ekosysteemien ja lohkoketjujen yhdistämisen mahdollisuuksia ja mahdollisia ongelmia. Havaittuja mahdollisuuksia oli paljon, niistä keskeisim-

pinä hajautetun infrastruktuurin tuomat vahvuudet ja parantunut tietoturvallisuus. Muita mahdollisuuksia olivat muun muassa, tiedon pysyvyys ja kustannusten aleneminen. Heikkouksia ilmeni tutkimuksessa myös paljon. Tutkielmassa suurimmiksi heikkouksiksi tunnistettiin lohkoketjuja ja IoT-laitteita vastaan ilmenevät kyberhyökkäykset ja heikko skaalautuminen, joka johtuu IoT-laitteiden rajallisesta laskenta tehosta ja tallennustilasta. Tämän lisäksi ongelmia syntyy myös asiantuntijuuden puutteesta ja kansainvälisellä tasolla eriävistä lainsäädännöistä. Tämän hetkisen tutkimuksen perusteella voidaan todeta, että vaikka teknologioiden yhdistämisen hyödyt ovat suuria, niin havaitut vaikeuttavat sen laajempaa käyttöönottoa. Vaikka toteuttamiseen tarvittavat teknologiat ovat saatavilla, niin ennen tutkimuksessa esitettyjen suurimpien ongelmakohtien ratkaisemista ei laajoja käyttöönottoja voida toteuttaa turvallisesti ja tehokkaasti.

Aiheen tuoreus ja tutkimuksen keskeneräisyys monilta osin aiheutti ongelmia luotettavan ja relevantin tutkimuksen löytämiseen aiheesta. Esineiden internetistä ja lohkoketjuista löytyy paljon tutkimuksia, mutta niiden yhdistämistä tehdyssä tutkimuksessa on paljon aukkoja. Yhtenä jatkotutkimusaiheena ehdotan lisätutkimuksen kohdentamista IoT:n ja lohkoketjuteknologian yhdistämisen teoreettisiin malleihin, koska tällä hetkellä aiheesta löytyy vain muutama tutkimus. Lohkoketjujen ja IoT laitteiden käyttöä osana liiketoiminnan prosesseja on vasta alettu käyttämään hyväksi eri toimialoilla. Koska käytännön implementoinnit ovat vasta tulossa yleisemmin osaksi eri alojen liiketoimintaa, niin myös yhdistämisestä seuraavien mahdollisten hyötyjen ja negatiivisten vaikutusten tutkimus perustuu pitkälti teorioihin.

Yleisesti voidaan sanoa, että IoT:ta ja lohkoketjuja on tutkittu tekniikan ja organisaatioiden näkökulmasta paljon, kun otetaan huomioon teknologioiden uutuus. IoT:n ja lohkoketjujen yhdistämisen tutkimus on kuitenkin vielä varhaisessa vaiheessa. Tämän hetkinen tutkimus pystyy kuitenkin tarjoamaan malleja ja pohjaa tulevaisuuden tutkimusta ja toteutuksia varten. Toimivien ratkaisujen toteuttamiseksi ja tutkimuksen edistämiseksi on tärkeää, että aiheesta tehdään korkeatasoista tutkimusta.

LÄHTEET

Atlam, H. F., Alenezi, A., Alassafi, M. O., & Wills, G. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), 40-48.

Atlam, H., Alenezi, A., Alasssafi, M. & Wills, G. (2018). Blockchain with Internet of Things: Benefits, Challenges, and Future Directions

Banafa, A. (2015). The Industrial Internet of Things (IIoT): Challenges, Requirements and Benefits

Banafa, A. (2017). IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things.

Baran, P. (1964) On Distributed Communications: 1. Introduction To Distributed Communications Networks

Bashir, I. (2017). Mastering blockchain 56-63, 69-98

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing (pp. 13-16).

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). Blockchain beyond the hype: What is the strategic business value. McKinsey & Company, 1-13.

Cisco. (2014). The Internet of Things Reference Model

Conway, J. (2016). The Industrial Internet of Things: an evolution to a smart manufacturing enterprise.

Crosby M., Nachiappan, Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin

Dahlqvist, F., Patel, M., Rajko, A. & Shulman J. (2019). McKinsey: Growing opportunities in the Internet of Things

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home

Dorri, A., Kanhere, S., Jurdak, R & Gauravam, P. (2017). Blockchain for IoT Security and Privacy: The Case Study of a Smart Home

Dorsmaine, B., Gaulier J-P., Wary J-P. & Kheir N. (2015). Internet of Things: A definition & Taxonomy

Drescher, D. (2017). Blockchain basics (Vol. 276). 12-13

Ericsson Mobility Report: June 2019

Fabiano, N. (2017). The Internet of Things ecosystem: the blockchain and privacy issues. The challenge for a global privacy standard

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories.

Ferrag, M., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L. & Janicke, H. (2018). Blockchain Technologies for the Internet of Things: Research Issues and Challenges

Helmiö, P. (2017). Open source in Industrial Internet of Things: a systematic literature review.

IBM nettisivut. (2020). Luettu: 31.1.2020. https://www.ibm.com/blockchain/industries/supply-chain

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP) (pp. 839-858). IEEE.

Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. Business & information systems engineering, 6(4), 239-242.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Liang, X., Zhao, J., Shetty, S & Danyi, L. (2017). Towards Data Assurance and Resilience in IoT Using Blockchain

Lund, D., Turner, V., MacGillivary, C., Morales, M. 2014.Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand

Mahmoud, R., Yousuf, T., Aloul, F. & Zualkernan I. (2015). Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures

Maier, J. (2017). Fig. 16. P51. Made Smarter Review.

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P. & Marrs, A. (2013). McKinsey Global Institute: Disruptive technologies: Advances that will transform life, business, and the global economy

Marr, B. (2018). Julkaistu: Forbes. 30+ Real Examples Of Blockchain Technology In Practice

Neittaanmäki, P. & Ogbechie, A. (2016). Blockchain – The Ultimate Disruption in the Financial System

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: pros, cons and SWOT.

Norton, S. (2016). Julkaistu: The Wall Street Journal. CIO Explainer: What is Blockchain

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. Sensors, 18(8), 2575.

Perez, S. (2017). Julkaistu: Techcrunch.com. Spotify acquires blockchain startup Mediachain to solve music's attribution problem

Postel, J., Roberts, L.G. & Wolff, S. (2009). A brief history of the Internet. 3-4.
Ramachandran, G.S. & Krishnamachari, K. (2018). Blockchain for the IoT: Opportunities and Challenges

Reyna, A., Martin, C., Chen, J., Soler, E & Diaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities

Rosic, A. (2019). What is Blockchain Technology? A Step-by-Step Guide For Beginners NETTISIVU?

Samaniego, M., & Deters, R. (2016, December). Blockchain as a Service for IoT. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 433-436). IEEE.

Sidhu, I. & Fred-Ojala, A. (2018). Future of Blockchain – A Berkley Perspective

Taivalsaari, A. & Mikkonen, T. (2017). Software challenges in the IoT era

Underwood, S. (2016). Blockchain beyond bitcoin

Wang, P., Valerdi, R., Zhou, S. & Li, L. (2015). Inroduction: Advances in IoT research and applications

Webster, J. & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), Xiii-xxiii.

World Economic Forum (WEF). (2018). Global Risks Report for 2018

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M. F., & Chaudhry, S. R. (2016, December). IoT architecture challenges and issues: Lack of standardization. In 2016 Future Technologies Conference (FTC) (pp. 731-738). IEEE.