Veikko Haakana

LOHKOKETJURATKAISUT ESINEIDEN INTERNETIN HAASTEISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Haakana, Veikko
Lohkoketjuratkaisut esineiden internetin haasteissa
Jyväskylä: Jyväskylän yliopisto, 2020, 26 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja(t): Clements, Kati

Esineiden internet kasvaa jatkuvasti ja on arvioitu, että tämän vuoden aikana esineiden internetissä tulee olemaan jopa 20 miljardia laitetta. Tämän teknologian kasvun myötä sen erilaiset haasteet, kuten tietoturva, yksityisyys, datan hallinnointi ja kulunvalvonta, ovat nousseet isoksi tutkimusaiheeksi. Tässä tutkielmassa otettiin kirjallisuuskatsauksen keinoin selvää, millaisia lohkoketjuratkaisuja on ehdotettu ratkaisuiksi esineidein internetin haasteisiin. Tutkielmassa huomattiin, että kaikissa haasteissa nousee esiin keskitetyn järjestelmän tuomat ongelmat. Lohkoketjujen avulla esineiden internetistä on mahdollista tehdä paremmin skaalautuva, tietoturvallisempi ja paremmin hallittavissa oleva järjestelmä.
Lohkoketjuteknologian ensimmäinen merkittävä toteutus on kryptovaluutta Bitcoin. Bitcoinin ja muiden kryptovaluuttojen myötä lohkoketjun suosio on noussut ja erilaisia lohkoketjun sovellutuksia on tehty paljon muillekin aloille.

Asiasanat: esineiden internet, lohkoketju, hajautettu järjestelmä

ABSTRACT

Haakana, Veikko
Blockchain solutions for Internet of Things' challenges
Jyväskylä: University of Jyväskylä, 2020, 26 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Clements, Kati

The Internet of Things is growing, and it is estimated that there will be up to 20 billion devices this year. With the growth of this technology, its various challenges, such as data security, privacy, data management and access control, have become a major research topic. In this thesis, the literature review explored what kind of blockchain solutions have been proposed for solving the challenges of the Internet. The study noted that all challenges highlight the problems of a centralized system. Blockchains make it possible to make the Internet of Things a more scalable, secure and more manageable system.
The first major implementation of blockchain technology is Bitcoin cryptocurrency. With the rise of Bitcoin and other cryptocurrencies, the blockchain has gained in popularity and many applications of the blockchain have been made in many other areas.

Keywords: blockchain, internet of things, decentralized system

KUVIOT

KUVIO 1 Lohkoketjun toimintaperiaate (Zheng ym., 2016) 14

TAULUKOT

TAULUKKO 1 Lohkoketjuratkaisut esineiden internetin haasteissa 17

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

KUVIOT 4

TAULUKOT 4

SISÄLLYS 5

1 JOHDANTO 6

2 ESINEIDEN INTERNET 7
2.1 Määritelmä 7
2.2 Esineiden internetin käyttötarkoituksia 8
2.3 Esineiden internetin avainteknologiat 9
2.4 Esineiden internetin haasteet 10
2.4.1 Tietoturva ja yksityisyys 10
2.4.2 Datan hallinnointi 11
2.4.3 Kulunvalvonta 11

3 LOHKOKETJUTEKNOLOGIA 13
3.1 Lohkoketjuteknologian määritelmä 13
3.2 Lohkoketjuteknologian sovellutuksia 15
3.2.1 Kryptovaluutat 15
3.2.2 Älysopimukset 15
3.2.3 Muita lohkoketjusovellutuksia 16

4 LOHKOKETJUTEKNOLOGIAN HYÖDYNTÄMINEN ESINEIDEN INTERNETIN HAASTEISSA 17
4.1 Tietoturva ja yksityisyys 18
4.2 Kulunvalvonta 19
4.3 Datan hallinnointi 20
4.4 CBM-järjestelmien tehottomuus 21
4.5 Datan yhtenäisyyden varmistaminen 21

5 YHTEENVETO 23

LÄHTEET 24

1 Johdanto

Tutkielmassa selvitetään, minkälaisia lohkoketjuratkaisuja on kehitetty vastaamaan esineiden internetin eri haasteisiin. Tutkielma on toteutettu kirjallisuuskatsauksena.

Esineiden internetin teknologia kehittyy jatkuvasti ja uusia laitteita otetaan käyttöön. On arvioitu, että vuoteen 2020 mennessä esineiden internetissä tulee olemaan yli 20 miljardia laitetta. (Lee & Fumagalli, 2019) Tällaiset laitteet hankkivat tietoa ympäristöstä, ja ne kommunikoivat keskenään ja ohjelmistojärjestelmien kanssa Internetin välityksellä. Monipuolisen vuorovaikutuksen seurauksena ne tuottavat myös paljon dataa. (Conoscenti, Vetrò, & De Martin, 2016) Datan suurta määrää ei pystytä käsitellä, sillä tällä hetkellä ei ole olemassa alustaa, joka mahdollistaisi helpon pääsyn laitteisiin ja laitteiden datan siirtoon edullisin kustannuksin. Tästä syystä paljon dataa menetetään. (Yu ym., 2018) Tämän tutkielman tarkoituksena on tarkastella aiempaa kirjallisuutta esineiden internetin haasteista.

Tutkielman tutkimuskysymys on: *Miten lohkoketjuteknologiaa voidaan hyödyntää esineiden internetin haasteissa*? Tutkielmassa käytettyä kirjallisuutta on haettu Google Scholarista. Tärkeimpiä hakusanoja ovat olleet ”blockchain”, ”internet of things” ja ”blockchain internet of things”. Luettujen artikkeleiden lähdeluetteloista löytyi myös lisää käyttökelpoista kirjallisuutta, jota on hyödynnetty tutkielmassa.

Tutkielman tarkoituksena on selvittää, millaisia lohkoketjuratkaisuja esineiden internetissä voisi hyödyntää. Tutkielmassa on kolme päälukua. Ensimmäisessä pääluvussa käsitellään esineiden internetiä, sen avainteknologioita ja käyttötarkoituksia. Toisessa pääluvussa käsitellään lohkoketjuteknologiaa ja sen sovellutuksia. Kolmannessa luvussa tarkastellaan esineiden internetiin liittyviä haasteita ja aiemman tutkimuksen avulla pohditaan, miten lohkoketjuteknologiaa voidaan hyödyntää haasteiden ratkaisemiseksi. Tässä luvussa esitellään tutkielman tulokset taulukon avulla. Taulukossa eritellään esineiden internetin haasteet ja esitellään niihin soveltuvia lohkoketjuratkaisuja. Tutkielman viimeinen luku on yhteenveto, jossa pohditaan tutkielman tuloksia sekä mahdollisia jatkotutkimusaiheita.

2 Esineiden internet

Tässä luvussa käsitellään esineiden internetiä. Ensin määritellään esineiden internet tätä tutkielmaa varten. Luvussa esitellään myös erilaisia esineiden internetin käyttötarkoituksia sekä esineiden internetin mahdollistavat avainteknologiat. Luvun lopussa käsitellään esineiden internetiin liittyviä haasteita. Koska tutkielma käsittelee erilaisia lohkoketjuratkaisuja esineiden internetiin, luvussa käsitellään tarkemmin haasteet, joihin on kehitetty lohkoketjuratkaisuja. Käsiteltäviksi haasteiksi valittiin tietoturva ja yksityisyys; datan hallinnointi ja kulunvalvonta.

2.1 Määritelmä

Alun perin Ashtonin esittämä termi esineiden internet (eng. *Internet of Things*, IoT) on muovautunut yläkäsitteeksi näkökulmille, jotka liittyvät internetin ja verkon laajennuksiin fyysiseen maailmaan. Esineiden internetiin liittyvää kirjallisuutta tarkasteltaessa haasteeksi voi muodostua, mitä esineiden internet todella tarkoittaa. Syy epämääräisyyteen perustuu itse termiin, joka voidaan syntaktisesti jakaa kahdeksi eri termiksi. Ensimmäinen termi käsittää enemmän IoT:n internet-orientoitunutta visiota, kun toisen termin pääkohtana on laitteiden kytkeminen verkkoon. (Atzori, Iera, & Morabito, 2010) Esineiden internetiä lähestytään tarkastelun tavoitteen mukaan aina joko internet- tai laiteorientoituneesta näkökulmasta. Näiden kahden näkökulman lisäksi on olemassa myös kolmas, semanttisesti orientoitunut näkökulma. Semanttisesti esineiden internet tarkoittaa maailmanlaajuista yhteen kytkettyjen, uniikisti tunnistettavissa olevien laitteiden verkkoa, joka perustuu standardeihin viestintäprotokolliin. (Atzori et al., 2010) Esineiden internet on laitteiden verkosto, joka kommunikoi keskenään IP-yhteyden avulla ilman ihmisen puuttumista. Esineiden internet koostuu esimerkiksi älykkäistä laitteista, älypuhelimista ja tableteista. Laitteiden väliseen kommunikointiin käytetään radiotaajuustunnistusta (RFID), QR-koodeja, sensoreita tai langatonta teknologiaa. (Singh & Singh, 2015)

Esineiden internetille ei ole olemassa yhtä standardisoitua määritelmää. Termiä käytetään usein jopa väärin, ja esineiden internetistä onkin tullut helposti väärinymmärrettävä asia. Termiä on käytetty päällekkäin esimerkiksi termien ”älylaitteet”, ”kyberfyysinen järjestelmä” tai ”älykäs toimintaympäristö” kanssa. Kirjallisuudessa esiintyvissä esineiden internetin määritelmissä toistuu kuitenkin samat pääpiirteet, jotka luetellaan seuraavaksi. (Atzori, Iera, & Morabito, 2016)

- Vaatii globaalin tietoliikenneinfrastruktuurin, joka sallii esineiden internetin elementtien yhteen toimivuuden, niiden saumattoman integroinnin ja ainutlaatuisen osoitusjärjestelmän. Tämän on oltava

globaali infrastruktuuri, joka mahdollistaa irrallisen ”Esineiden intranetin”.

- Päivittäistavarat ovat päärooliss esineiden internetissä. Näiden on oltava luettavissa, tunnistettavissa, paikannettavissa, osoitettavissa ja kontrolloitavissa. Tämän seurauksena on oltava ratkaisuja, joiden myötä fyysisten ja virtuaalisten asioiden yhdistäminen onnistuu.
- Esineiden tulee olla autonomisia, jotta kompleksia järjestelmää voidaan kontrolloida.
- Ihmisten ja esineiden välille ja esineiden välille täytyy rakentaa älykkäitä käyttöliittymiä.
- Teknologioiden heterogeenisuus.
- Palvelut yhdistyvät laitteisiin. Palvelut voivat olla yksinkertaisia tai monimutkaisia, mutta ne on rakennettu

Määritellään esineiden internet tässä tutkielmassa seuraavasti: ”Esineiden internetissä esineillä on identiteetit ja virtuaaliset persoonallisuudet, ja ne toimivat älykkäissä ympäristöissä käyttäen älykkäitä rajapintoja yhteydenpitoon ja kommunikointiin sosiaalisessa kontekstissa, ympäristökontekstissa ja käyttäjäkontekstissa”. (Lu Tan & Neng Wang, 2010) 1970-luvulla kehitetyssä internetissä edelleen suurin osa liikenteestä on ihmisten välistä liikennettä. Esineiden internetin myötä ihmisten ja laitteiden välinen sekä pelkkien laitteiden välinen kommunikointi kasvaa merkittävästi. Esineiden internetin visiona on, että sen yleistymisen myötä ihmisten välinen kommunikaatio vähenee ja tilanne muuttuu niin, että laitteet kommunikoivat keskenään ihmisten puolesta. (Lu Tan & Neng Wang, 2010)

2.2 Esineiden internetin käyttötarkoituksia

Esineiden internet mahdollistaa monia erilaisia käyttötarkoituksia yksityisille käyttäjille, tuottajille ja yrityksille. IoT-teknologiat tarjoavat laajoja sovellutuksia tuotantosektorilla, esimerkiksi ympäristön tarkkailussa, terveydenhuollossa sekä varaston- ja tuotannonhallinnassa. Lisäksi mahdollisia sovellutuksia ovat IoT-ratkaisut työpaikalla, älykodeissa sekä turvallisuuden ja valvonnan alalla. (Miorandi, Sicari, Pellegrini, & Chlamtac, 2012)

Teollisessa esineiden internetissä (IIoT) on kyse toisiinsa kytketyistä sensoreista, instrumenteista ja muista laitteista, jotka on verkotettu tietokoneiden teollisten sovellusten kanssa, mukaan lukien tuotanto ja energianhallinta. (Boyes, Hallaq, Cunningham, & Watson, 2018) Teollisessa esineiden internetissä on paljon erilaisia käyttötarkoituksia. IIoT:n avulla voidaan tuottaa historiallista, ennakoivaa tai ohjailevaa analyysiä, jonka avulla saadaan paremmin tietää mitä koneissa tai erilaisissa prosesseissa tapahtuu. Sensoreiden ja älykkäiden laitteiden

avulla teollisuudessa voidaan vähentää epätehokkaita prosesseja tai turhia ylläpitokustannuksia. Yleinen käyttötarkoitus teollisuuden esineiden internetillä on toimintojen ja varojen kauko-ohjattava hallinta sekä ennakoiva ylläpito. (Gilchrist, 2016)

Käytännön esimerkkinä IIoT:sta on sensoreilla varustetut rekkojen renkaat. Logistiikkayritys ei osta suoraan renkaita niiden valmistajalta, koska niiden kestävyydessä voi olla vaihtelevuutta. Tämän takia renkaiden ostomäärää on vaikea arvioida, ja siitä voi koitua tarpeettomia kuluja. Sen sijaan logistiikkayritys ostaa rengasvalmistajalta palvelun, joka kattaa renkaat logistiikkayrityksen rekkoihin. Renkaat sisältävät sensoreita, joiden datan perusteella tiedetään kuinka paljon renkailla on ajettu, ja laskutus tapahtuu sen mukaan. Rengasvalmistaja voi saada lisähyötyä sensoreiden tuottamasta datasta myymällä sitä logistiikkayritykselle. Tällä datalla logistiikkayritys voi esimerkiksi kouluttaa kuljettajiaan taloudellisempaan ajoon. (Gilchrist, 2016)

Terveydenhuollossa esineiden internetiä voidaan hyödyntää potilaan tarkkailussa. Iso-Britanniassa on käynnissä kokeilu, jossa potilas voi olla kotona, ja mitata päivittäin painon, sykkeen ja verenpaineen. Nämä tiedot välittyvät Bluetoothin avulla potilaan älypuhelimeen, josta tiedot menevät sairaalalle. Jos tähän lisätään vielä automaattisesti terveystietoja kerääviä sensoreita, terveystietoja voidaan välittää sairaalaan ilman erillisiä potilaan mittauksia. Muita käytännön sovelluksia IIoT:ssa on muun muassa älytoimistoissa, öljy- ja kaasuteollisuudessa sekä vähittäiskaupassa. (Gilchrist, 2016)

2.3 Esineiden internetin avainteknologiat

Esineiden internetin tärkeimpänä mahdollistavana teknologiana pidetään RFID:tä (Radio Frequency IDentification). Alhaiset kustannukset, teknologian kypsyys ja yhteisön kannatus on syynä RFID:n suosioon IoT:ssa. (Atzori et al., 2010) RFID:n historia ulottuu toisen maailmansodan ajalle, ja ajan saatossa se on kehittynyt päivittäiseksi teknologiaksi, jota käytetään esimerkiksi toimitusketjun seuraamisessa tai parkkeeraamisen kulunvalvonnassa. RFID on yleinen termi teknologioille, jotka käyttävät radioaaltoja tunnistaakseen ihmisiä tai objekteja. Yleisin tapa tunnistautumiseen on laittaa fyysinen RFID-tunniste objektiin. RFID-järjestelmä koostuu tyypillisesti RFID-tunnisteesta, antennilla varustetusta tunnisteen lukijasta ja isäntäjärjestelmästä. (Roberts, 2006) Antenni lähettää radioaaltoja, jotka kantavat kymmenien metrien päähän. Mikäli radioaallot kantavat tunnisteelle asti, tunniste aktivoituu ja siitä voidaan lukea dataa tai siihen voidaan kirjoittaa dataa. (Domdouzis, Kumar, & Anumba, 2007)

WSN (Wireless Sensor Network)

2.4 Esineiden internetin haasteet

Esineiden internetissä on paljon teknologiaan liittymättömiä haasteita. Näitä haasteita ovat esimerkiksi internetin ja energian esteetön saatavuus sekä energiankulutus. Esineiden internetin onnistumista varten internet-yhteyden pitäisi olla saatavilla kaikkialla. Haasteina nähdään myös esimerkiksi sensorijärjestelmien kehitys ja itse sensoreiden valmistaminen tarpeeksi pienin kustannuksin. (Mukhopadhyay & Suryadevara, 2014)

Tässä tutkielmassa keskitytään niihin esineiden internetin haasteisiin, joihin on esitetty lohkoketjuratkaisua. Näistä haasteista kaksi suurinta ovat tietoturva ja yksityisyys. Näiden myötä esineiden internetin kulunvalvonta on noussut erittäin tärkeäksi tutkimusaiheeksi. (Ouaddah, Mousannif, Elkalam, & Ouahman, 2017)

IoT:n käyttöoikeuksia hallinnoi yleensä keskitetty taho, joka osoittautuu ongelmalliseksi luottamuksen kannalta. Tätä ongelmaa varten on kehitetty hajautettuja malleja, joissa IoT-laite hoitaa käyttöoikeuksien validoinnin. IoT-laitteiden kyvykkyydet ovat vähäisiä, joten käyttöoikeuksiin voi päästä helposti käsiksi jokin vahingollinen taho. Keskitetty, mutta turvallinen kulunvalvonta voi olla mahdollista toteuttaa lohkoketjun ja älysopimusten avulla. (Zhang, Kasahara, Shen, Jiang, & Wan, 2019)

2.4.1 Tietoturva ja yksityisyys

Esineiden internetissä on huomattavia tietoturvaan ja yksityiseen liittyviä haasteita, koska sovellukset vaikuttavat virtuaalisen maailman sijaan oikeassa, fyysisessä maailmassa. IoT-laitteilla voi olla pääsy arkaluontoisiin tietoihin ja ne voivat olla helposti muokattavissa. Lisäksi laitteilla on rajoitetusti laskenta-, varastointi- ja energiakapasiteettia, mikä aiheuttaa haasteita tietoturvan ja yksityisyyden kannalta. (Fotiou, Kotsonis, Marias, & Polyzos, 2016)

IoT-laitteet keräävät valtavasti dataa käyttäjistään. Tulevaisuudessa älykkäät mittarit voivat esimerkiksi tietää, milloin käyttäjä käy suihkussa tai milloin käyttäjä ei mene töihin. Nämä ovat arkaluontoisia ja henkilökohtaisia tietoja, joiden ei toivottaisi päätyvän mahdollisten kyberhyökkääjien tietoisuuteen. (Ouaddah et al., 2017)

Käyttäjällä on tällä hetkellä rajoitettu mahdollisuus hallita omaa dataa ja miten sitä käytetään. IoT-laitteiden luoma data tallennetaan kolmannen osapuolen pilvipalvelimille, joten käyttäjän on pakko luottaa tämän kolmannen osapuolen olevan turvallinen ja saatavissa oleva. Esineidein internetin tietoturva keskittyy lähinnä point-to-point -yhteyden, eli kahdenvälisen yhteyden suojaamiseen. (Shafagh, Burkhalter, Hithnawi, & Duquennoy, 2017)

2.4.2 Datan hallinnointi

IoT-laitteet tuottavat valtavan määrän dataa. Vielä ei ole keksitty ratkaisua, jolla tätä datamäärää voitaisiin hallita ja hyödyntää riittävän hyvin. Globaali IoT-verkko on kooltaan valtava, eikä perinteiset tietokantojen hallintaratkaisut täytä tämän tarpeita. IoT-laitteiden oletetaan kommunikoivan keskenään laitteiden havaintojen perusteella luodun datan avulla. Datan hallinnan takaamiseksi laitteille pitäisi olla alusta, joka mahdollistaisi päätöksenteon luodun datan ja aiemmin tallennetun datan avulla. Esineiden internetissä datan hallinnointi tapahtuu esineiden ja laitteiden välillä, jotka luovat dataa. Erilaiset sovellukset pääsevät käsiksi tähän dataan ja muuntavat dataa käyttäjälle sopivaksi. (Abu-Elkheir, Hayajneh, & Ali, 2013)

Esineiden internet sisältää lukuisia kytkettyjä solmuja erilaisilla teknologia- ja viestintästandardeilla. Moni solmu tallentaa, välittää ja varastoi dataa, kun samanaikaisesti moni solmu muuntaa ja integroi dataa informaatioksi, jota nämä sovellukset voivat noutaa ja analysoida käyttäjää varten. Tämän sekä datan valtavan määrän takia perinteiset datan hallintaan liittyvät teknologiat eivät sovi esineiden internetin datan hallintaan. (Fan & Chen, 2010)

Myös datan varastointi keskitetyille pilvipalvelimille aiheuttaa ongelmia esineiden internetissä. Tämän hetkinen pilvipohjainen arkkitehtuuri on luonut paljon eristettyjä datasiiloja, jonka seurauksena esineidein internetin datalla ohjautuvaa analytiikkaa ei saada hyödynnettyä niin hyvin kuin mahdollista. (Shafagh et al., 2017)

2.4.3 Kulunvalvonta

Kulunvalvonta on tärkeä osa esineiden internetiä, sillä se estää luvattoman pääsyn informaatioon tai laitteen aktivointiin. Esineiden internetin kulunvalvonnassa haasteeksi muodostuu se, että kulunvalvontajärjestelmän pitää olla tarpeeksi yleinen kattamaan erilaisia IoT-laitteita, mutta sen pitää olla samalla mahdollisimman kevyt järjestelmä. (Fotiou et al., 2016) Esineidein internetin laitteilla voi olla paljon erilaisia valtuutustapoja, jotka vaativat kulunvalvontajärjestelmän. Laitteiden heterogeenisuuden takia järjestelmän täytyy olla rakenteeltaan kevyt, jotta se tukee erilaisia valtuutustapoja. (Burange & Misalkar, 2015)

Keskitetyt kulunvalvontajärjestelmät, eli asiakas/palvelin malli on alun perin suunniteltu ihmisen ja tietokoneen välisiin skenaarioihin. Jotkut IoT-skenaariot ovat kuitenkin paljon dynaamisempia kuin perinteiset tietokoneen ja ihmisen väliset skenaariot. Jotkin IoT-laitteet voivat olla liikuteltavia, tai ne voivat kuulua usealle eri hallinnoijalle elinkaarensa aikana. Toisaalta IoT-laitteita voidaan hallita usean eri entiteetin toimesta samanaikaisesti, ja laitteiden resurssit voivat olla tähän liian rajoitettuja. (Novo, 2018)

Ouaddah ym. (2017) arvioivat erilaisia kulunvalvontaratkaisuja esineiden internetille. Artikkelissaan he tunnistivat erilaisia kulunvalvontajärjestelmiä, joita esineiden internetissä käytetään tällä hetkellä. Tulokseksi saatiin, että

nykyisiä internetprotokollia ei pysty hyödyntämään kaikissa esineiden internetin skenaarioissa.

3 Lohkoketjuteknologia

Tässä luvussa käsitellään lohkoketjuteknologiaa, sen toimintaperiaatetta ja erilaisia sovellutuksia. Lohkoketjuteknologian ensimmäinen merkittävä sovellutus on vuonna 2008 julkaistu kryptovaluutta Bitcoin. Bitcoinin myötä myös monia muita kryptovaluuttoja on julkaistu. Kryptovaluutat eivät kuitenkaan ole lohkoketjuteknologian ainut sovellutus, vaan lohkoketjuratkaisuja on kehitetty moniin eri käyttötarkoituksiin.

3.1 Lohkoketjuteknologian määritelmä

Lohkoketju on hajautettu julkinen tilikirja, jossa tehtävät transaktiot tallennetaan lohkoihin. Lohkot ovat kronologisessa järjestyksessä, salattuja ja yhteydessä sekä edelliseen että seuraavaan lohkoon. Lohkoketjun ensimmäistä lohkoa kutsutaan genesis-lohkoksi. Kaikista lohkoketjun lohkoista on mahdollista jäljittää ensimmäinen lohko. (Yuan & Wang, 2018)

Kaikissa verkossa tapahtuvissa transaktioissa luotetaan johonkin tiettyyn osapuoleen. Esimerkiksi sähköpostin tullessa sähköpostiohjelma kertoo viestin sisällön ja keneltä se on. Samalla tavalla verkkopankista voi katsoa tilin saldon. Elämme siis digitaalisessa maailmassa luottaen tietoturvan ja yksityisyyden kolmansille osapuolille. Lohkoketjuteknologialla on mahdollista poistaa kolmas osapuoli erilaisista transaktioista. Lohkoketjuteknologian avulla myös mikä tahansa transaktio voidaan varmistaa lohkosta koska tahansa. (Crosby ym., 2016) Lohkoketjuteknologia perustuu tilikirjan rakenteeseen ja hajautettuun konsensukseen. Kukaan ei omista tai hallinnoi tätä tilikirjaa, ja se on kaikkien sen käyttäjien tarkasteltavissa. Kun käyttäjä haluaa lisätä transaktion tilikirjaan, sen data salataan ja tarkastetaan muiden käyttäjien toimesta algoritmien avulla. (Underwood, 2016)

Lohkoja luovia käyttäjiä kutsutaan louhijoiksi, jotka saavat lohkon luomisesta palkkion. Esimerkiksi Bitcoinin louhijoille annetaan lohkon luomisesta palkkioksi Bitcoineja. Uusi lohko lisätään lohkoketjuun, kun louhijat ovat konsensusmekanismin avulla todentaneet lohkon kelpaavaksi. Transaktiot eivät siis automaattisesti tallennu lohkoketjuun, vaan ne kirjataan ensin aktiiviseen lohkoon. Kun lohko on täynnä transaktioita, se tarkastetaan, ja vasta sitten lisätään itse lohkoketjun. Kun lohko on lisätty lohkoketjuun, siinä olevaa tietoa ei voi enää muokata. (Nofer ym., 2017)

Lohkoketjun toimintaperiaate on kuvattu kuviossa 1. Kuviossa havainnollistetaan, miten lohkot liittyvät aina edelliseen lohkoon. Lohkoketjun ensimmäisellä lohkolla, eli genesis-lohkolla ei ole edeltävää lohkoa, eikä myöskään viitettä toiseen lohkoon. Jokaisen lohkon otsikkona on edellisen lohkon tiiviste (eng.

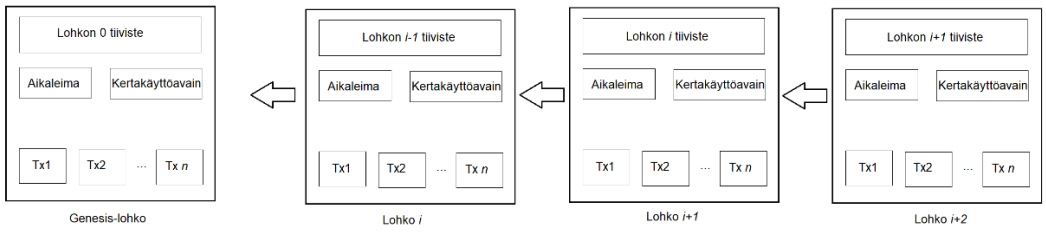
hash). Tiivistealgoritmi muuttaa suuren määrän dataa lyhyemmäksi tiivisteeksi. Esimerkiksi Bitcoinin lohkoketjussa käytetään SHA-256-tiivistealgoritmia, joka luo satunnaisen merkkijonon. (Bitcoin.it, 2020) Lohkoketjun louhijat yrittävät ratkaista tätä tiivistettä kertakäyttöavaimien (eng. *nonce*) avulla. Kun tiiviste on ratkaistu, lohko luodaan ja lisätään lohkoketjuun. Jokaisessa lohkossa on lisäksi aikaleima, joka kertoo sekunnin tarkkuudella, milloin lohko on lisätty lohkoketjuun. Transaktioiden määrä lohkossa riippuu lohkon ja transaktioiden koosta. (Zheng ym., 2018)

Lohkoketjun konsensusmekanismi on vastuussa lohkoketjussa olevan tiedon yhtenäisyydestä. Hajautetussa järjestelmässä ei ole luotettua keskitettyä tahoa, joka pitäisi huolta tiedon oikeellisuudesta. Lohkoketjun käyttäjät saavuttavat konsensusmekanismin avulla yhteisymmärryksen tiedon oikeellisuudesta, ilman että heidän tarvitsee luottaa toisiinsa. (Reyna ym., 2018)

Kaksi yleisintä lohkoketjuissa käytettyä konsensusmekanismia ovat Proof-of-Work (PoW) sekä Proof-of-Stake (PoS). PoW perustuu yksinkertaisesti laskentatehoon. Lohkoketjun louhijoiden pitää suorittaa laskentateholtaan haastava tehtävä, ennen kuin lohko lisätään lohkoketjuun. Suurin PoW:ta konsensusmekanisminaan käyttävä lohkoketju on Bitcoin. (Bentov, Lee, Mizrahi, & Rosenfeld, 2014) PoW:n huonona puolena on se, että lohkoketju on riippuvainen energiankulutuksesta. Lisäksi siinä on suuri viive, koska uusi lohko luodaan aina 10 minuutin välein. Lohkoketjun viive ja suuri energiankulutus tekevät PoW:sta sopimattoman konsensusmekanismin monille sovellutuksille. (Reyna ym., 2018)

PoS puolestaan perustuu louhijoiden järjestelmässä olevaan omaisuuteen. Esimerkiksi kryptovaluuttojen lohkoketjuissa lohkoja generoivat todennäköisemmin ne, jotka omistavat enemmän kyseistä kryptovaluuttaa. (Bentov et al., 2014) PoS luottaa siihen, että enemmän valuuttaa omistavat käyttäjät haluavat pitää järjestelmän turvallisena ja luotettavana, omien omistuksiensa takia. PoS:ssa lohkon generoiva käyttäjä valitaan satunnaisesti algoritmilla, joka kuitenkin perustuu käyttäjän valuutan määrään. (Reyna ym., 2018)

PoS:n tarkoituksena on siirtää lohkoketjun toiminnan kustannukset järjestelmän ulkopuolelta sen sisäpuolelle. PoS on paljon PoW:ta energiaystävällisempi. Kritiikiksi on kuitenkin sanottu, että tämä konsensusmekanismi tukee rikkaitten rikastumista, koska lohkon luomisesta saa palkinnoksi lisää kryptovaluuttaa. Älysopimuksia tarjoaja Ethereum käytti aiemmin konsensusmekanisminaan PoW:ta, mutta on myöhemmin siirtynyt käyttämään PoS:a. (Reyna ym., 2018)



KUVIO 1 Lohkoketjun toimintaperiaate (Zheng ym., 2016)

3.2 Lohkoketjuteknologian sovellutuksia

Tässä alaluvussa käsitellään erilaisia lohkoketjuteknologian sovellutuksia. Ensin käsitellään kryptovaluuttoja, joista Bitcoin on ensimmäinen suureen suosioon noussut lohkoketjun sovellutus. Seuraavaksi käsitellään älysopimuksia ja lopuksi käsitellään lohkoketjun muita sovellutuksia.

3.2.1 Kryptovaluutat

Lohkoketjuteknologian tunnetuin sovellutus on Bitcoin. (Crosby ym., 2016) Bitcoin on kryptovaluutta, joka on luotu vuonna 2008. Bitcoinin toiminnan kuvaavan valkopaperin on kirjoittanut nimimerkki Satoshi Nakamoto. Bitcoinin tarkoitus on poistaa välikäsi, eli pankit, verkossa tehtävistä transaktioista. Välikäden kautta tehtävät transaktioit perustuvat aina luottamukseen, ja maksut ovat peruttavissa. Bitcoin tekee maksuista peruuttamattomia ja poistaa myös tuplakulutuksen mahdollisuuden. Bitcoinin maksujärjestelmä ei perustu instituutioon luottamiseen, vaan proof-of-work menetelmään. (Nakamoto, 2008) Bitcoinin lohkoketju on turvallinen niin kauan, kun yksikään louhiva osapuoli ei hallitse yli 50% lohkoketjun laskentatehosta. (Yuan & Wang, 2018)

Bitcoinilla on selkeästi suurin osuus kryptovaluuttojen kokonaismarkkinasta noin 63 prosentilla. (Coinmarketcap.com, 2020) Bitcoinin lisäksi on kuitenkin olemassa muitakin krypovaluuttoja. Kaksi Bitcoinin lisäksi suurinta kryptovaluuttaa ovat älysopimuksiin erikoistunut Ethereum sekä Ripple.

3.2.2 Älysopimukset

Älysopimukset ovat lohkoketjussa toimivia ohjelmia tai sovelluksia. Ethereum-lohkoketju on suosituin alusta älysopimuksille. Ethereum on julkinen lohkoketju, johon voi tehdä omia älysopimuksia. Älysopimusten ylläpitäminen maksaa käyttäjälle Ethereumin omaa kryptovaluutta Etheriä. Älysopimuksen tarkoituksena on suorittaa automaattisesti sopimuksen kohtia, kun määritetyt ehdot täyttyvät. (Alharby & Moorsel, 2017) Älysopimus koostuu ohjelmakoodista, tallennustiedostosta ja käyttäjän saldosta. Käyttäjä voi tehdä älysopimuksen lähettämällä transaktion lohkoketjuun. Kun älysopimus on luotu, sen sisältöä ei voi enää muokata. Älysopimuksen sisältöä suoritetaan aina, kun käyttäjä tai toinen älysopimus lähettää sille viestin. Lohkoketjun louhijat varmistavat konsensusmekanismin avulla, että älysopimuksen suoritus on oikeellinen, ja päivittävät lohkoketjua. Älysopimuksen luominen ja jokainen sen suorituskerta maksaa käyttäjälle lohkoketjun valuuttaa, Ethereumin tapauksessa Etheriä. (Delmolino ym., 2016)

Älysopimuksien etuna on huomattavasti pienemmät transaktiokulut verrattuna perinteisiin kolmansiin osapuoliin. Esimerkiksi saksalainen slock.it -niminen yritys hyödyntää Ethereum-älysopimuksia liiketoiminnassaan. Slock.it:n avulla voi myydä tai vuokrata mitä tahansa ilman kolmannen osapuolen osallistumista. Esimerkiksi asunnon vuokraaminen on käyttäjälle halvempaa kuin

jonkun kolmannen osapuolen, kuten vuokravälittäjän kautta. (Alharby & Moorsel, 2017)

Ethereum on suosituin alusta älysopimuksille, koska se tukee kehittyneitä ja kustomoituja älysopimuksia ja useita eri ohjelmointikieliä. Toinen suosittu alusta älysopimuksille on NXT. Se on julkinen lohkoketjualusta, jossa on sisäänrakennettuja älysopimuksia. Se ei kuitenkaan tue kustomoitua älysopimuksia, vaan siinä on valmiita pohjia erilaisille sopimuksille. (Alharby & Moorsel, 2017)

3.2.3 Muita lohkoketjusovellutuksia

Kryptovaluutat ja älysopimukset ovat lohkoketjuteknologian käytetyimpiä sovellutuksia, mutta esimerkkejä muistakin käyttötarkoituksista on olemassa. Lohkoketjualustalle tehty äänestysjärjestelmä toisi läpinäkyvyyttä äänestykseen, kun jokainen ääni olisi tallennettuna lohkoketjussa. Lohkoketjun ominaisuuksien mukaisesti tällainen äänestysjärjestelmä olisi myös erittäin luotettava ja turvallinen. Lohkoketjuäänestysjärjestelmää on kokeiltu tanskalaisen poliittisen puolueen sisäisissä vaaleissa vuonna 2014. (Pilkington, 2016)

Toisena esimerkkinä muista sovellutuksista on toimitusketjujen seurantaan tarkoitetut lohkoketjut. Everledger on yritys, joka hyödyntää lohkoketjua timanttien aitouden todentamisessa. Everledger seuraa timanttien kulkua kaivokselta markkinoille asti. Täten asiakkaat saavat tietää, timantin alkuperän ja mitä kautta se on tullut markkinoille. Timantin aitous voidaan todentaa lohkoketjun avulla, koska kaikista välikäsistä ja timantin reitistä on tiedot lohkoketjussa. Everledgerin tarkoitus on myös laajentaa toimintaa muiden arvokkaiden esineiden, kuten taideteosten tai keräilyautojen seurantaan. (Underwood, 2016)

Keskitetyssä tietokannassa järjestelmän ylläpitäjällä on mahdollisuus muokata tallennettua tietoa. Lohkoketjussa tallennettu tieto ei ole muokattavissa. Ylläpijä voi myös muuttaa tiedon omistajaa, kun lohkoketjussa vain tiedon omistaja voi vaikuttaa sen omistajuuteen. Tämän takia lohkoketju on hyvä ratkaisu kriittisen informaation hallintaan. Tällaista kriittistä informaatiota on esimerkiksi potilastiedot. Muutama iso IT-alan yritys, kuten Accenture ja Deloitte, ovat mukana kehittämässä lohkoketjussa toimivaa potilastietojärjestelmää. (Kuo, Kim, & Ohno-Machado, 2017)

4 Lohkoketjuteknologian hyödyntäminen esineiden internetin haasteissa

Tässä luvussa käsitellään, miten lohkoketjuteknologiaa voidaan hyödyntää esineiden internetin haasteissa. Ensimmäisessä alaluvussa käsitellään yleisellä tasolla, miksi lohkoketjuteknologiasta voi olla hyötyä esineiden internetissä. Myöhemmissä alaluvuissa tutustutaan tieteellisissä artikkeleissa esitettyihin esineidein internetin lohkoketjuratkaisuihin, jotka on lajiteltu haasteittain luvun 2.4 mukaisesti.

Tutkimuksen pohjalta on luotu taulukko, johon on kerätty esineiden internetin haasteita ja niihin esitettyjä lohkoketjuratkaisuja. Näitä ratkaisuja käydään läpi seuraavissa alaluvuissa.

Tämän hetkinen esineiden internetin keskitetty malli on kallis ylläpitää IoT-laitteiden valmistajien näkökulmasta. Esineiden internetin käyttäjän näkökulmasta keskitetyssä järjestelmässä suurin haitta on yleinen luottamus laitteisiin. Läpinäkyvyyden kautta saavutettavaa turvallisuutta tarvitaan laitteille, jotka pääsevät käsiksi arkaluontoiseen tietoon sovellusten taustalla, käyttäjän huomaamatta. Nämä ongelmat voitaisiin ratkaista skaalautuvalla, vertaisverkkoon perustuvalla mallilla, joka toimii läpinäkyvästi ja hajauttaa datan turvallisesti. Yksi vaihtoehto tällaiseksi malliksi on lohkoketju. (Christidis & Devetsikiotis, 2016)

TAULUKKO 1 Lohkoketjuratkaisut esineiden internetin haasteissa

IoT:n haaste:	Ehdotettu lohkoketjuratkaisu:
Tietoturva ja yksityisyys (Weber 2010)	• Lohkoketjualusta IoT-laitteille (Dorri ym. 2017) • Lohkoketjustalusta IoT-laitteille (Li ym. 2017) • ”Permissioned Blockchain” -alusta IoT-laitteille (Cooper, Kravitz 2017) • Hajautettu lohkoketjupohjainen todentamisjärjestelmä IoT-laitteille (Hammi ym. 2018)
Kulunvalvonta	• Skaalautuva, lohkoketjussa toimiva IoT-laitteiden kulunvalvontajärjestelmä (Novo, 2018) • Lohkoketjuun pohjautuva arkkitehtuuri IoT-laitteiden kulunvalvonnalle (De Bona, Gregio, Pinno 2017)

	• Älysopimuksiin pohjautuva kulunvalvontajärjestelmä (Zhang ym. 2018)
Datan hallinnointi (Chu, Ma, Wang 2013)	• Lohkoketjupohjainen hajautettu datavarasto IoT-laitteiden datalle (Burkhalter ym. 2017) • Lohkoketjualusta IoT-laitteille (Guo ym. 2018)
CBM-järjestelmien tehottomuus	• Lohkoketjualusta IIoT-laitteille (Bahga, Madisetti 2016)
Datan yhtenäisyyden varmistaminen	• Lohkoketjuun pohjautuva viitekehys datan yhtenäisyyden varmistamiseksi (Liu ym. 2017) • Lohkoketjuun pohjautuva viitekehys reunalaskennan avulla (Casado-Vara ym. 2018)

4.1 Tietoturva ja yksityisyys

Yritysten toimitusketjuissa voisi hyödyntää esineiden internetin lohkoketjuratkaisua, esimerkiksi merikonttien hallinnassa. Tyypillisessä toimitusketjussa merikontti siirtyy valmistajan, sataman ja muiden välikäsien kautta vastaanottajalle. Kaikki merikontin kanssa tekemisissä olevat sidosryhmät kirjaavat kontin saapumisen ja lähtemisen omiin tietokantoihinsa. Toimitusketjun seuranta voitaisiin toteuttaa luomalla lohkoketju, johon sidosryhmät tekevät merkinnän, kun merikontti on saapunut. Täten kaikilla sidosryhmillä on pääsy seuraamaan merikontin toimitusta lohkoketjussa. Kaikki tieto tallentuu lohkoketjuun, joten siitä on helppo seurata toimitusta aikaleimoineen. Koko edellä mainittu prosessi saadaan automatisoitua, kun otetaan esineiden internet käyttöön. Jos merikontit sisältävät IoT-sensoreita, ja kaikilla sidosryhmillä on omat älyseurantalaitteensa, seuranta saadaan tallennettua lohkoketjuun automaattisesti sensoreiden ja älyseurantalaitteiden etäisyyden avulla. (Christidis & Devetsikiotis, 2016)

Dorri ym. (2017) toteuttivat tutkimuksessaan älykodin, jonka IoT-laitteet operoivat yksityisessä lohkoketjussa. Käyttäjällä on oma lohkoketjussa toimiva louhija, joka käsittelee älykodin tulevat ja lähtevät transaktiopyynnöt. Samalla se tarkistaa, autentikoi ja valvoo laitteiden tekemiä transaktiopyyntöjä. Laitteet pystyvät kommunikoimaan keskenään ja pyytämään toisiltaan dataa jaetun avaimen avulla. Louhija myöntää jaetun avaimen niille laitteille, jotka käyttäjä hyväksyy. Näin laitteet voivat kommunikoida keskenään niin kauan, kunnes käyttäjä haluaa lopettaa tiedonjakamisen, ja hylkää avaimen. Käyttäjällä on lista laitteista, jotka jakavat dataa, joka on turvattu jaetulla avaimella. Transaktiopyynnöt, jotka tulevat muiden laitteiden toimesta, menevät aina louhijan, eli myös käyttäjän

kautta. Täten virheelliset ja haitalliset transaktiopyynnöt voidaan hylätä, joka tekee kulunvalvonnasta tietoturvallista. DDoS-hyökkäys tähän järjestelmään on erittäin vaikea toteuttaa, koska ilman jaettua avainta transaktiot eivät etene. (Dorri ym., 2017)

Hammi ym. (2018) esittävät esineiden internetin tietoturvan parantamiseksi virtuaalialuetta nimeltään ”bubbles of trust”. Virtuaalialueen jäsenet voivat luottaa toisiinsa ja alueelle on mahdotonta päästä, jos ei ole jäsen. Järjestelmä toimii julkisessa lohkoketjussa ja hyödyntää älysopimuksia. Laitteiden välinen viestintä tapahtuu lohkoketjussa transaktioiden avulla. Objekteilla voi olla vain yksi identiteetti ja yksi avainpari kerrallaan, joka estää väärennetyllä identiteetillä hyökkäämisen. Mahdollinen hyökkääjä ei voi myöskään muuttaa laitteiden viestien sisältöä tai viedä laitteen identiteettiä, koska nämä toimenpiteet vaativat yksityisen avaimen.

Lohkoketjussa toimivaa järjestelmää vastaan tehtävät mahdolliset palvelunestohyökkäykset ovat myös tehottomia hajautetun rakenteen ansiosta. Palvelut on hajautettu ja monistettu useille eri solmuille. Vaikka hyökkääjä onnistuisi estämään yhden solmun, kaikkien muiden solmujen estäminen ei ole mahdollista. Lisäksi julkisessa lohkoketjussa transaktiot ovat maksullisia, joten hyökkääminen järjestelmää kohtaan tulisi kalliiksi. Lisäksi lohkoketjussa aikaleimatut transaktiot varmennetaan konsensusmekanismilla. Hyökkääjä ei siis voi vastata näihin transaktioihin, koska konsensusmekanismi hylkää ne. (Hammi ym., 2018)

Cooper & Kravitz (2017) esittävät esineiden internetin turvallisuuden parantamiseksi ratkaisua, joka hyödyntää yksityistä lohkoketjua. Yksityistä lohkoketjua pääsevät tarkastelemaan vain luvan saaneet tahot. Transaktiot saadaan turvattua paremmin yksityisen lohkoketjun avulla. (Kravitz & Cooper, 2017)

4.2 Kulunvalvonta

Novo (2018) esittää keskitetyn kulunvalvonnan tilalle hajautettua kulunvalvontajärjestelmää IoT-laitteiden hallinnointia varten. Tämä hajautettu kulunvalvontajärjestelmä on yhdistetty sensoriverkostoihin, jotka ovat maantieteellisesti hajautettuja. Esineiden internetissä yhdestäkin keskitetystä kulunvalvontapalvelimesta voi tulla pullonkaula, jos kulunvalvontakyselyitä ja päivityksiä esiintyy paljon.

Hajautetun kulunvalvontajärjestelmän kaikki osat kuuluvat lohkoketjuun, paitsi IoT-laitteet ja hallintakeskus (eng. *management hub*), joka pyytää kulunvalvontainformaation laitteiden puolesta. Kulunvalvontajärjestelmään kuuluu lisäksi yksi älysopimus, jossa kaikki kulunvalvontaan liittyvät operaatiot määritellään ja suoritetaan. Transaktioiden toteutuminen lohkoketjussa vie paljon aikaa, joka voisi aiheuttaa ongelmia esineiden internetin käytettävyydelle. Tässä mallissa hallintakeskus eivätkä IoT-laitteet sisälly lohkoketjuun, joten transaktioita ei tarvitse tehdä laitteiden tiedon saamiseksi.

Tämän hajautetun kulunvalvontajärjestelmän yksi eduista on se, että laitteiden hallinnan kontrolli (eng. *management control*) on helppo siirtää solmulta toiselle, koska kaikki operaatiot määritellään ja tapahtuvat samassa älysopimuksessa. Ainoastaan laitteiden hallinnasta vastaavat solmut voivat tehdä transaktioita lohkoketjussa, ja sitä kautta maksavat transaktiokuluja. Nämä solmut voivat olla yhteydessä IoT-laitteisiin ilman transaktioita, koska ne eivät kuulu itse lohkoketjuun.

De Bona ym. (2017) esittävät esineiden internetin kulunvalvontaan toisenlaista lohkoketjuratkaisua, ControlChainia. ControlChain koostuu neljästä erillisestä lohkoketjusta, jotka hallinnoivat entiteettien pääsytietoja ja suhteita, sensoreiden kontekstuaalista tietoa, tietoja käyttöoikeuksien myöntämisestä tai estämisestä sekä valtuuttamisen sääntöjä. Nykyisiin esineiden internetin kulunvalvontajärjestelmiin verrattuna ControlChain tarjoaa paremmin skaalautuvaa ja tietoturvallisempaa hajautettua ratkaisua, jossa ei tarvitse luottaa kolmanteen osapuoleen.

Zhang ym. (2019) toteuttivat älysopimuksiin pohjautuvan kulunvalvontaalustan IoT-laitteille kahdella tietokoneella ja kahdella Raspberry Pi:llä. Alustalla on kolme erilaista älysopimusta, ACC, JC ja RC. JC on tarkoitettu tunnistamaan ja tuomitsemaan laitteiden vääränlaista käytöstä. ACC on älysopimus laitteiden välistä kulunvalvontaa varten ja RC on älysopimus, jolla hallitaan kahta muuta älysopimusta. Kulunvalvontajärjestelmä pohjautuu Ethereumin älysopimuksiin.

Sekä De Bona ym. (2017), Zhang ym. (2019) että Novon (2018) esittämissä esineidein internetin kulunvalvonnan lohkoketjuratkaisuissa keskeistä on kolmannen osapuolen, eli keskitetyn järjestelmän poistaminen, jotta kulunvalvonnasta tulee luotettavampaa.

4.3 Datan hallinnointi

Shafagh ym. (2017) esittävät esineiden internetin datan hallinnointiongelman ratkaisuksi uudenlaista tarkastettavissa olevaa lohkoketjupohjaista datanhallintajärjestelmää. Pilvipalvelimet sijaitsevat yleensä suurissa datakeskuksissa, jotka ovat internetin runkoverkon reunoilla. Pilvipalvelinten etäisyys voi aiheuttaa vaihtelevuutta viiveessä etenkin mobiililaitteita käytettäessä. Tässä datanhallintajärjestelmässä käytetään datavarastoina pilvenhattaroita (eng. *cloudlet*), jotka sijaitsevat maantieteellisesti lähempänä käyttäjiä.

Shafagh ym. (2017) mallissa hallintataso sekä datataso on erotettu toisistaan. Kulunvalvontatasona käytetään julkista lohkoketjua, jonka avulla kulunvalvonta on hajautettua, joustavaa sekä tarkastettavissa olevaa. Lohkoketjussa säilytetään tietoja käyttöoikeuksista turvallisesti. Data on strukturoitu datavirtoihin, ja joihin käyttöoikeuksia jaetaan. Datan omistaja voi perua datavirran jakamisen palvelun koska tahansa. Jakaakseen datavirtansa jonkin palvelun kanssa käyttäjä luo uuden transaktion lohkoketjuun.

Datavirrat jaetaan isompiin datalohkareisiin, jotka ketjutetaan toisiinsa. Dataa ei kuitenkaan tallennetta lohkoketjuun, vaan siihen tallennetaan datalohkareen tunniste. Tunnisteen avulla datan omistaja sekä datan omistajan sallimat tahot pääsevät käsiksi dataan. (Shafagh ym., 2017)

Guo ym. (2018) esittävät esineidein internetin datan hallinnoinnin parantamiseksi lohkoketjualustaa. Lohkoketjualusta koostuu kolmesta kerroksesta, jotka ovat älykkäiden laitteiden kerros, lohkoketjukerros ja hajautettu sovelluskerros. Vertailtaessa tätä älykkäiden laitteiden lohkoketjua Ethereum-lohkoketjuun sekä Bitcoin-lohkoketjuun huomattiin, että viive on huomattavasti pienempi samalla kun suoritusteho on huomattavasti korkeampi.

Datan hallinnointiin liittyvissä ongelmissa suurimmaksi haasteeksi nousee keskitetyt pilvipalvelimet. Niiden tuoma mahdollinen viive sekä epävarmuus aiheuttavat haasteita. Lohkoketjun myötä hajautettu järjestelmä tuo luotettavuutta, koska silloin järjestelmässä ei tarvitse luottaa ainoastaan yhteen tahoon.

4.4 CBM-järjestelmien tehottomuus

CBM (eng. Cloud-Based Manufacturing), eli pilvipohjainen tuotanto mahdollistaa on-demand pääsyn resursseihin teollisuudessa. Bahga & Madisetti (2016) esittävät lohkoketjussa toimivaa BPIIoT-nimistä järjestelmää teolliseen esineiden internetiin. ¨Tämän järjestelmän toiminta perustuu hajautettuihin sovelluksiin, jotka toimivat älysopimuksien avulla. Lohkoketjun myötä BPIIoT tarjoaa hajautetun, turvallisen ja jaetun tilikirjan kaikista transaktioista. Lisäksi järjestelmä mahdollistaa käyttäjien ja koneiden väliset transaktiot ilman kolmatta osapuolta. Älysopimusten avulla myös koneiden huoltotoimenpiteet voidaan automatisoida. (Bahga & Madisetti, 2016)

4.5 Datan yhtenäisyyden varmistaminen

Liu ym. (2017) esittävät esineidein internetin datan yhtenäisyyden varmistamiseksi lohkoketjuun pohjautuvaa viitekehystä. Viitekehys korvaa keskitetyn tahon yhtenäisyydenhallinnan omalla lohkoketjuratkaisulla, joka lisää datan yhtenäisyyden luotettavuutta. Viitekehys soveltuu tietynlaisen datan tunnistamiseen sekä datan omistajille että datan käyttäjille. Viitekehyksen soveltamista varten datan yhtenäisyyden varmistamisen protokollia implementoitiin älysopimuksiin, jotka toimivat yksityisessä Ethereum-lohkoketjussa. Lohkoketjun avulla datan yhtenäisyyden varmistaminen nopeutui, koska varmistamisesta on vastuussa useampi taho.

Myös Casado-Vara ym. (2018) esittävät lohkoketjuun pohjautuvaa viitekehystä esineiden internetin datan haasteisiin. Viitekehyksen tarkoituksena on parantaa esineidein internetin datan laatua sekä parantaa virheellisen datan

tunnistamista. IoT-laitteiden tuottama data säilötään lohkoketjuun. Peliteoriaan pohjautuva algoritmi toimii arkkitehtuurin reunalaskentakerroksessa, ja tämän ansiosta lohkoketjuun säilötty data on luotettavaa, ja siitä saadaan poistettua mahdolliset virheellisyydet.

5 Yhteenveto

Tämä tutkielma käsitteli erilaisia lohkoketjuratkaisuja esineiden internetin haasteisiin. Tutkielman tarkoituksena oli selvittää, millaisia haasteita esineiden internetissä on ja millaisia lohkoketjuun pohjautuvia ratkaisuja näihin haasteisiin on esitetty. Tutkimus suoritettiin kirjallisuuskatsauksena ja sen tavoitteena oli vastata seuraavaan kysymykseen: ”Miten lohkoketjuteknologiaa voidaan hyödyntää esineiden internetin haasteissa?”

Neljännessä luvussa käsiteltiin erilaisia esineiden internetin lohkoketjuratkaisuja. Luvussa käsiteltiin ensin yleisellä tasolla, miten lohkoketjuratkaisut voivat parantaa esineiden internetiä.

Tutkielman tulokset on kuvailtu taulukossa, johon on eritelty esineiden internetin haaste ja siihen esitetty lohkoketjuratkaisu. Esineiden internetissä on paljon erilaisia haasteita, joista tässä tutkielmassa perehdyttiin kolmeen. Nämä haasteet olivat tietoturva ja yksityisyys, kulunvalvonta sekä datan hallinnointi.

Erilaisia lohkoketjuratkaisuja läpikäydessä huomattiin, että suurena haasteena on nykyinen esineiden internetin keskitetty malli. Palveluiden ja palvelimien keskittyminen tietyille kolmansille osapuolille luo haasteita sekä tietoturvan, kulunvalvonnan että IoT-laitteiden datan kannalta. Kaikissa tutkielmassa käsitellyissä ratkaisuissa nousi esiin se, että esineiden internetin pitäisi toimia hajautetusti.

Tulevassa tutkimuksessa olisi hyvä arvioida, miten erilaisten lohkoketjuratkaisujen käyttöönotto esineiden internetissä olisi mahdollista. Tämän hetken tutkimuksessa on esitetty ratkaisuja, joita on kokeiltu pienessä mittakaavassa. Lohkoketjut tuovat paljon mahdollisuuksia esineiden internetille, mutta lohkoketjussa on myös haavoittuvuuksia. Tässä tutkielmassa ei käsitelty lainkaan lohkoketjun huonoja puolia, vaan esiteltiin erilaisia ratkaisuja, jotka voisivat mahdollistaa esineiden internetin paremman toimivuuden.

LÄHTEET

Abu-Elkheir, M., Hayajneh, M., & Ali, N. A. (2013). Data Management for the Internet of Things: Design Primitives and Solution. *Sensors*, *13*(11), 15582–15612. https://doi.org/10.3390/s131115582

Alharby, M., & Moorsel, A. van. (2017). Blockchain Based Smart Contracts : A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT)*. https://doi.org/10.5121/csit.2017.71011

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/https://doi.org/10.1016/j.comnet.2010.05.010

Atzori, L., Iera, A., & Morabito, G. (2016). Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, *56*. https://doi.org/10.1016/j.adhoc.2016.12.004

Bahga, A., & Madisetti, V. (2016). Blockchain Platform for Industrial Internet of Things. *Journal of Software Engineering and Applications*, *25*, 533–546. https://doi.org/http://dx.doi.org/10.4236/jsea.2016.910036

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y. *SIGMETRICS Perform. Eval. Rev.*, *42*(3), 34–37. https://doi.org/10.1145/2695533.2695545

Bitcoin Wiki. (2020). Luettu 4.3.2020 osoitteessa https://en.bitcoin.it/wiki/Hash

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/https://doi.org/10.1016/j.compind.2018.04.015

Burange, A. W., & Misalkar, H. D. (2015). Review of Internet of Things in development of smart cities with data management privacy. *2015 International Conference on Advances in Computer Engineering and Applications*, 189–195. https://doi.org/10.1109/ICACEA.2015.7164693

Casado-Vara, R., de la Prieta, F., Prieto, J., & Corchado, J. M. (2018). Blockchain framework for IoT data quality via edge computing. *Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems*, 19–24.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Coinmarketcap.com. (2020). Cryptocurrencies Percentage of Total Market Capitalization. Luettu 22.2.2020 osoitteessa coinmarketcap.com

Conoscenti, M., Vetrò, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 1–6. https://doi.org/10.1109/AICCSA.2016.7945805

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review*, (2), 16.

Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). *Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a*

Cryptocurrency Lab BT - Financial Cryptography and Data Security (J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, & K. Rohloff, Eds.). Berlin, Heidelberg: Springer Berlin Heidelberg.

Domdouzis, K., Kumar, B., & Anumba, C. (2007). Radio-Frequency Identification (RFID) applications: A brief introduction. *Advanced Engineering Informatics*, *21*(4), 350–355. https://doi.org/https://doi.org/10.1016/j.aei.2006.09.001

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

Fan, T., & Chen, Y. (2010). A scheme of data management in the Internet of Things. *2010 2nd IEEE InternationalConference on Network Infrastructure and Digital Content*, 110–114. https://doi.org/10.1109/ICNIDC.2010.5657908

Fotiou, N., Kotsonis, T., Marias, G. F., & Polyzos, G. C. (2016). Access Control for the Internet of Things. *2016 International Workshop on Secure Internet of Things (SIoT)*, 29–38. https://doi.org/10.1109/SIoT.2016.010

Gilchrist, A. (2016). Industrial Internet Use-Cases. In *Industry 4.0: The Industrial Internet of Things* (pp. 13–31). https://doi.org/10.1007/978-1-4842-2047-4_2

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126–142. https://doi.org/https://doi.org/10.1016/j.cose.2018.06.004

Kravitz, D. W., & Cooper, J. (2017). Securing user identity and transactions symbiotically: IoT meets blockchain. *2017 Global Internet of Things Summit (GIoTS)*, 1–6. https://doi.org/10.1109/GIOTS.2017.8016280

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Lee, C., & Fumagalli, A. (2019). Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 24–28. https://doi.org/10.1109/WF-IoT.2019.8767227

Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain Based Data Integrity Service Framework for IoT Data. *2017 IEEE International Conference on Web Services (ICWS)*, 468–475. https://doi.org/10.1109/ICWS.2017.54

Lu Tan, & Neng Wang. (2010). Future internet: The Internet of Things. *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, *5*, V5-376-V5-380. https://doi.org/10.1109/ICACTE.2010.5579543

Miorandi, D., Sicari, S., Pellegrini, F. De, & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/https://doi.org/10.1016/j.adhoc.2012.02.016

Mukhopadhyay, S. C., & Suryadevara, N. K. (2014). *Internet of Things: Challenges and Opportunities BT - Internet of Things: Challenges and Opportunities* (S. C. Mukhopadhyay, Ed.). https://doi.org/10.1007/978-3-319-04223-7_1

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, *112*, 237–262. https://doi.org/https://doi.org/10.1016/j.comnet.2016.11.007

Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research Handbook on Digital Transformations* (pp. 225–253). https://doi.org/10.4337/9781784717766.00019

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/https://doi.org/10.1016/j.future.2018.05.046

Roberts, C. M. (2006). Radio frequency identification (RFID). *Computers & Security*, *25*(1), 18–26. https://doi.org/https://doi.org/10.1016/j.cose.2005.12.003

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards Blockchain-Based Auditable Storage and Sharing of IoT Data. *Proceedings of the 2017 on Cloud Computing Security Workshop*, 45–50. https://doi.org/10.1145/3140649.3140656

Singh, S., & Singh, N. (2015). Internet of Things (IoT): Security challenges, business opportunities reference architecture for E-commerce. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 1577–1581. https://doi.org/10.1109/ICGCIoT.2015.7380718

Underwood, S. (2016). Blockchain beyond Bitcoin. *Commun. ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581

Yu, S., Lv, K., Shao, Z., Guo, Y., Zou, J., & Zhang, B. (2018). A High Performance Blockchain Platform for Intelligent Devices. *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, 260–261. https://doi.org/10.1109/HOTICN.2018.8606017

Yuan, Y., & Wang, F. (2018). Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *48*(9), 1421–1428. https://doi.org/10.1109/TSMC.2018.2854904

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of Things Journal*, *6*(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705