Atte Komppa

Esineiden internetin turvallisuuden parantaminen lohkoketjulla

Tietotekniikan kandidaatintutkielma

28. huhtikuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Atte Komppa

Yhteystiedot: atte.v.komppa@student.jyu.fi

Ohjaaja: Tuomo Rossi

Työn nimi: Esineiden internetin turvallisuuden parantaminen lohkoketjulla

Title in English: Strengthening the security of IoT using a blockchain

Työ: Kandidaatintutkielma

Sivumäärä: 23+0

Tiivistelmä: Tässä tutkielmassa tarkastellaan, mitkä tekijät johtavat esineiden internet-laitteiden turvattomuuteen ja miksi ongelmaan ei ole yksinkertaista ratkaisua. Tähän ongelmaan selvitetään, voidaanko lohkoketjua soveltaa esineiden internet-laitteiden ja niiden tietojen turvaamiseksi. Tutkielmassa paneudutaan esineiden internetin tietoturvan nykytilanteeseen sekä lohkoketjun mahdollistamiin muutoksiin. Aihetta käydään läpi teknologioiden avaamisilla sekä antamalla konkreettisia esimerkkejä aiheista.

Avainsanat: Esineiden internet, tietoturvallisuus, kyberturvallisuus, lohkoketju

Abstract: This survey clarifies what are the factors that lead to the insecurity of IoT and why there is not a straight solution for these security problems. To solve the problem, blockchain is being studied, can it be used with IoT to secure devices and their informations. This survey focuses on information security of IoT at this moment and the changes that blockchain can offer for IoT. The topic is covered by introducing the technologies and by giving concrete examples.

Keywords: Internet of Things, information security, cyber security, blockchain

Kuviot

Sisällys

1 Johdanto

Tietotekniset laitteet ovat yleistyneet ja lisääntyneet maailmanlaajuisesti jatkuvasti. Internetiin yhdistettyjen laitteiden määrä kasvoi ihmisten väkilukua suuremmaksi jo vuosien 2008 ja 2009 välillä, minkä katsotaan olevan myös esineiden internetin, tunnetummin IoT-laitteiden (engl. Internet of Things) syntymisajankohta (Evans 2011). Tällä hetkellä internetiin kytkettyjä laitteita on kymmeniä miljardeja. Laitteiden kehitys jatkuu koko ajan uusiin tarkoituksiin ja erilaisiin ominaisuuksiin, mikä johtaa usein uudenlaisiin turvallisuusongelmiin.

Yksi laitteiden kehityksestä syntynyt osa-alue on aiemmin mainittu IoT. Näiden laitteiden turvallisuudesta on noussut suuri huolenaihe, minkä takia aihetta on alettu tutkia viimeisten vuosien aikana toden teolla (Alaba ym. 2017; Khan ja Salah 2018). Tarve oikeanlaisen turvallisuusratkaisun löytämiseksi kyseisille laitteille kasvaa koko ajan ja erilaisia menetelmiä testaillaan jatkuvasti. Tässä kandidaatin tutkielmassa selvitetään IoT-laitteiden turvallisuusriskejä ja niiden turvallisuuden tilanne tällä hetkellä. Turvallisuusongelmaan liittyen selvitetään onko mahdollista parantaa laitteiden turvallisuutta lohkoketjulla ja pystytäänkö sitä ylipäänsä käyttämään IoT-laitteille.

Tässä tutkielmassa selitetään lohkoketjun rakenne ja toimintaperiaate sekä lisäksi lohkoketjuun sisältyvä älysopimus luvussa 2. Luvussa 3 keskitytään esineiden internetiin, sen turvallisuuteen sekä ominaisuuksiin, mistä seuraa sen uusien turvallisuusratkaisujen tarve. Näiden lukujen perusteella jatketaan lukuun 4, jossa käydään läpi esineiden internetin ja lohkoketjun yhdistämiseen liittyviä hyötyjä sekä haasteita. Tässä luvussa esitellään myös esimerkki yritysmaailmasta, miten tekniikoita voidaan konkreettisesti yhdistää ja käyttää. Esimerkki sisältää osan jo toimivasta yritysmaailman palvelusta, mutta siihen ei paneuduta yksityiskohtaisesti. Tarkoituksena on antaa yleiskuva toiminnasta mitä on jo olemassa ja mitä voisi olla tulossa, mikäli tekniikkaa saadaan laajemmin käyttöön. Viimeiseksi luvussa 5 tehdään yhteenveto kaikista edellä käydyistä luvuista ja todetaan tutkielman edetessä saadut päätelmät käytettyjen lähteiden perusteella.

2 Lohkoketju

Lohkoketju on ajankohtainen ja lähivuosina paljon tutkittu ilmiö tietotekniikan alalla. Tämä selviää muun muassa vuoden 2016 tutkimuksien rahoituksista, jolloin ensimmäisten 9 kuukauden aikana lohkoketjun tutkimuksiin sijoitettiin yli 1.4 miljardia dollaria (Reyna ym. 2018). Tekniikka nousi pinnalle kryptovaluutta bitcoinin esittelyn kautta vuonna 2008, minkä yhteydessä Satoshi Nakamoto esitteli myös lohkoketjun ensimmäisen kerran (Nakamoto 2008; Reyna ym. 2018). Bitcoin oli myös ensimmäinen kryptovaluutta ja ylipäänsä asia, jossa lohkoketju otettiin käyttöön (Dorri, Kanhere ja Jurdak 2017). Tämän jälkeen lohkoketjua on alettu soveltamaan moniin muihinkin käyttötarkoituksiin, kuten terveydenhuollon datajärjestelmiin ja hajautettuihin varastointijärjestelmiin. Tässä tutkielmassa ei paneuduta bitcoiniin tai sen historiaan enempää, vaan pääpaino on lohkoketjun tekniikassa, rakenteessa ja soveltamisessa IoT-laitteille.

2.1 Lohkoketju yleisesti

Lohkoketju on tietokanta, jonka toiminta perustuu hajautettuun tietorakenteeseen, joka jaetaan kaikille verkossa mukana oleville osapuolille kopiona (Christidis ja Devetsikiotis 2016). Tämä tarkoittaa myös sitä, kun ketjuun tulee muutoksia, niin uusi kopio ketjusta lähetetään kaikille verkon osapuolille ja kaikkien tieto pysyy näin ajantasaisena ketjun rakenteesta ja sen tapahtumista. Ketju alkaa alkulohkosta, josta ei ole viittausta taaksepäin. Kun ketjuun luodaan uusi lohko alkulohkon lisäksi, niin ketjun edellisen lohkon hajautuskoodi syötetään uuden lohkon tietoihin tämän oman hajautuskoodin lisäksi (Samaniego, Jamsrandorj ja Deters 2016). Jokaisella lohkolla on siis oma hajautuskoodinsa, sekä muilla paitsi alkulohkolla edellisen lohkon hajautuskoodi, jonka avulla tunnistetaan ja ketjutetaan lohkot (ks. kuvio 1). Lohkoihin sisällytetään myös muita tarvittavia tietoja, joita voivat olla kontekstista riippuen esimerkiksi aikatiedot ja siirretty data. Lohkon hajautuskoodi ei suoranaisesti tarkoita käyttäjän tai laitteen tunnusta, jolla voidaan tunnistaa laite tai sen käyttäjä. Lohkoketjulla on ominaisuus, jolla voidaan pitää laitteen ja käyttäjän yksityisyys suojattuna vaihtuvalla julkisella avaimella (Wang ym. 2019), joka estää lohkon tiedoista jäljittämisen laitteeseen ja sitä kautta henkilöön. Wang ym. (2019) lisäävät myös, että ketjun osapuolilla on jokaisella oma

salattu yksityinen avain. Tämän avaimen avulla todistetaan tapahtumien yhteydessä, että on oikea henkilö vastassa, eikä jokin väärä osapuoli.

Kuvio 1. Lohkoketjun rakenne yksinkertaistettuna.

Ennen lohkon lisäämistä ketjuun suoritetaan salaustekniikka nimeltä proof of work (POW), jota kutsutaan myös louhimiseksi (Dorri, Kanhere ja Jurdak 2017; Reyna ym. 2018). Proof of work on laskennallisesti haastava toiminto, jonka avulla luodaan yhteisymmärrys luottamattomassa verkossa (Reyna ym. 2018), eli se tuo osaltaan luotettavuutta toimintaan. Toiminnossa otetaan mukaan osapuolien julkiset avaimet varmistamaan tapahtumien oikeellisuutta ja aitoutta (Wang ym. 2019). Kun POW on saatu suoritettua onnistuneesti, lohko siirtyy hyväksyttäväksi muille verkon osapuolille, eli verkossa oleville solmuille (Reyna ym. 2018). Reyna ym. (2018) lisäävät, että osapuolien tulee vielä hyväksyä lohko oikeelliseksi, minkä jälkeen lohko vasta lisätään ketjuun. Näin pystytään muodostamaan hajautettu vertaisverkko, jossa toisilleen tuntemattomat tahot voivat olla vuorovaikutuksessa toistensa kanssa ilman luotettavaa välittäjää välikätenä, johtuen salauksien runsaasta käytöstä (Christidis ja Devetsikiotis 2016).

Lohkoketju kasvaa tapahtumien myötä koko ajan pidemmäksi ja riippuen käyttötarkoituksesta uusia lohkoja voi syntyä hyvinkin nopealla tahdilla. Ketjuun voi yrittää tulla myös uusia laitteita, joiden omistajien tarkoitusperät eivät aina ole hyviä tai tarkoituksenmukaisia. Lohkoketju antaa kuitenkin suojaa tunkeilijoilta laajan verkkonsa ansiosta, sillä muokatakseen jo rakennettua ketjua tulisi muokata kaikkia aiempia lohkoja nopeammin kuin POW kerkeää suorittamaan muutoksen (Reyna ym. 2018). Mikäli jotakin ketjussa olevaa lohkoa on käyty

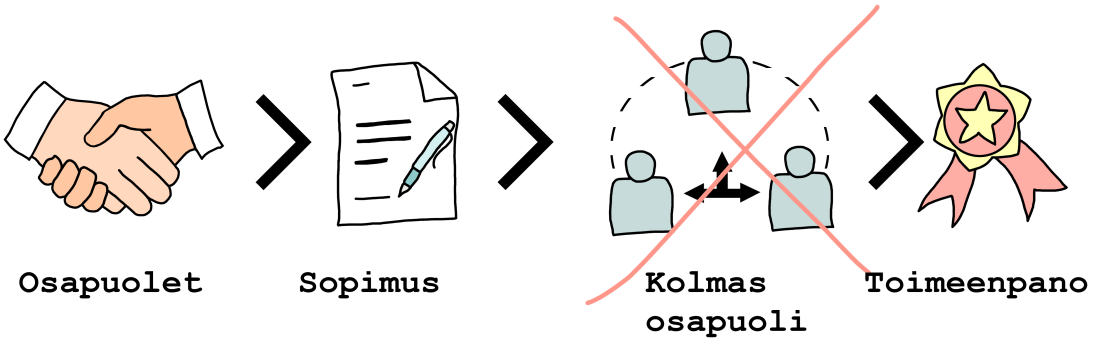
muokkaamassa jälkikäteen, kyseisen lohkon hajautuskoodi muuttuu ja ketjun seuraava lohko, joka sisältää tietona aiemman hajautuskoodin huomaa muutoksen. Muutos tulee myös näkymään jokaiselle verkossa olevalle osapuolelle niiden lohkoketjun kopiossa (Samaniego, Jamsrandorj ja Deters 2016). Käytännössä tämä tarkoittaa sitä, että muutoksen tekijällä tulisi olla enemmistö verkon käyttämien solmujen, eli osapuolien laitteiden suorittimien laskentakapasiteetista itsellään käytössä, jotta muutos saadaan hyväksyttyä (Reyna ym. 2018; Nakamoto 2008). Muuten enemmistö huomaa muutoksen, joka ei ole tarkoituksenmukainen ja hylkää tämän lisäyksen. Muutoksiin sisältyy myös lohkon poistaminen ketjusta, mikä ei onnistu lohkon lisäyksen jälkeen, vaikka lohko olisikin vahingossa tehty väärillä tiedoilla tai arvoilla. Näin ketju pysyy muuttumattomana ja rakenteeltaan samanlaisena kuin aiemmin.

2.2 Älysopimus lohkoketjulla

Älysopimukset (engl. Smart contract) ovat osa lohkoketjua, joita voidaan hyödyntää monissa tilanteissa. Nick Szabo esitteli älysopimus käsitteen ensimmäisen kerran jo vuonna 1994, jolloin hän itse kuvaili tätä ”Tietokoneistetuksi tapahtumaprotokollaksi, joka toteuttaa sopimuksen ehdot” (Tekijän käännös) (Christidis ja Devetsikiotis 2016). Toiminnaltaan ja rakenteeltaan älysopimukset ovat Christidis ja Devetsikiotis (2016) mukaan lohkoketjuun sijoitettuja komentosarjoja, jotka suorittavat itse itsensä ja täten mahdollistavat asianmukaiseen, hajautettuun ja automatisoituun työnkulkuun, mahdollistaen myös monivaiheisien prosessien automatisoinnin. Reyna ym. (2018) mukaan älysopimuksien yksi pääominaisuuksista on panna täytäntöön tai toteuttaa itse sopimuslausekkeita, mikä ei ole ollut mahdollista ennen lohkoketju-teknologian kehitystä ja syntymistä. Älysopimuksista on siis ollut käsitys jo vuosikymmeniä, mutta vasta lohkoketjun kautta sille on saatu toteutustapa.

Sengupta, Ruj ja Das Bit (2020) määrittelevät älysopimuksen itsevalvovaksi tietokoneohjelmaksi, jota voidaan käyttää yksinkertaisiin kahden osapuolen välisiin sopimuksiin aivan kuten normaaleja sopimuksia tehtäessä. Älysopimus sisältää säännöt ja rangaistukset sopimuksen noudattamattomuudelle, mutta eroten normaalista sopimuksesta, älysopimus voi laittaa kaiken saman tien käytäntöön (Sengupta, Ruj ja Das Bit 2020). Käytäntöönotolla viitataan siihen, ettei tarvitse allekirjoittaa papereita ja lähettää papereita eteenpäin käsiteltäväksi, jossa menisi aikaa ennen kuin ne hyväksytään ja niiden sisältävät pykälät astuvat voimaan.

Näin älysopimuksilla voidaan pudottaa pois kolmannet osapuolet sopimuksista ja siirroista, joka johtaa niistä johtuvien kustannuksien vähenemiseen (ks. kuvio 2). Muita hyötyjä ovat automaattisuus, skaalautuvuuden parantuminen sekä tiedon väärinkäytön estäminen, minkä avulla henkilö haluaisi hyötyä itselleen (Sengupta, Ruj ja Das Bit 2020).



Kuvio 2. Älysopimuksen vaiheet kuvitettuna. (Kuva: Samuel Lehikoinen 2021)

Palataan vielä takaisin älysopimuksen rakenteeseen lohkoketjussa. Lohkoketjun rakenteesta ja muodostumisesta johtuen myös älysopimukset ovat osa lohkoketjuun tallennettuja lohkoja, joihin on tallennettu erilaisia komentosarjoja tai dataa. Näin ollen myös älysopimuslohkoilla on omat uniikit osoitteet ja tunnisteet. Jokainen verkossa mukana oleva osapuoli voi siis tarkastella älysopimuksen sisältöä, eli koodia, miten se on toteutettu (Christidis ja Devetsikiotis 2016). Tästä samaisesta lohkoketjun toimintaperiaatteesta johtuen, lohkoketjussa älysopimuksia hallitaan samalla tavalla vertaisverkon kautta kuin mitä tahansa muutakin toimintaa, eli sopimuksen tekemät muutokset tulevat lisätyksi vain, jos enemmistö verkon osapuolista hyväksyy ne (Sengupta, Ruj ja Das Bit 2020).

Älysopimukset eivät kuitenkaan aivan kirjaimellisesti suorita itse itseään milloin ja millä tiedoilla tahansa haluavat. Jotta älysopimus saadaan aktivoitua, täytyy sen lohkoketjun osoitteelle osoittaa tapahtuma tehtäväksi (Christidis ja Devetsikiotis 2016). Tämän jälkeen sopimus vasta hoitaa loput automaattisesti sille ohjelmoidulla tavalla, jokaiseen verkossa olevaan solmuun tapahtuman antamilla tiedoilla. Christidis ja Devetsikiotis (2016) lisäävät, että sopimukseen tarvittavat tiedot on oltava älysopimuksen saatavilla, jotta toiminto voidaan suorittaa ilman ongelmia onnistuneesti. Vaikka älysopimus hoitaa sopimuksen automaattisesti,

niin silti se toimii aina täysin ennustettavalla tavalla (Christidis ja Devetsikiotis 2016). Älysopimuksilla on myös ominaisuus pitää hallussaan lohkoketjun käyttäjien yksityisiä avaimia ja vahvistaa näiden avulla ketjuun lisäyksiä tekevät osapuolet, ovatko lähettäjät sallittuja käyttäjiä verkossa (Singh, Singh ja Kim 2018).

Kuten kaikki verkossa tapahtuva toiminta, myös älysopimukset sisältävät riskejä. Reyna ym. (2018) mukaan ne ovat muunmuassa alttiita useille hyökkäyksille, jotka tuovat uusia haasteita mukanaan turvaamiselle. Yksi ongelma heidän mukaan syntyy sopimuksen siirrosta tietokoneille ja sen täytäntöönpanosta sen kautta, koska koneet ovat haavoittuvia hakkeroinnille, ohjelmistovirheille, viruksille sekä yhteyskatkoksiin. Toinen ongelma on sopimuksien koodaaminen, joka on erityisen haastavaa, koska niistä pitää saada ongelmattomia ja toimivia kerralla, johtuen lohkoketjun muuttumattomuudesta ja muokkaamattomuudesta (Reyna ym. 2018). Kun lohkoketjuun on lisätty sopimus lohkona, sitä lohkoa ei siis enää voi muokata. Tämän vuoksi on erityisen tärkeää taata sopimuksen toimivuus ja saada varmistuksia asiasta ennen laajaa käyttöönottoa (Reyna ym. 2018).

Älysopimuksetkaan eivät siis ole täysin luotettavia tapauksia, mutta hyvällä ohjelmoinnilla ja testauksella voidaan saavuttaa melko turvallinen ratkaisu. On kuitenkin sanomattakin selvää, että älysopimukset tuovat huiman edun ja uudistuksen sopimuksien tekoon. Lyhyesti summattuna "älysopimus on kokoelma koodeja tai toimintoja ja tietoja tai tiloja, jotka sijaitsevat jossain kohtaa lohkoketjua, jossakin tietyssä lohkoketjun osoitteessa"(Tekijän käännös) (Reyna ym. 2018).

3 Esineiden internet

Kuten aiemmin johdannossa mainittiin, uusia laitteita syntyy ja kehitetään jatkuvasti. Internetin ja fyysisten laitteiden kehittyessä syntyi myös näiden yhdistävä tekijä, IoT-laitteet. Gubbi ym. (2013) mukaan käsite kehitettiin vuonna 1999 alun perin toimitusketjun hallintaan, mutta nykyisin se kattaa laajemmin useiden alojen sovelluksia ja laitteita. ”Esine” sana tarkoittaa tässä yhteydessä enemmän laitteen ominaisuutta toteuttaa tietokoneena toimintoja ilman ihmistä välikätenä (Gubbi ym. 2013). IoT on internetin laajennus fyysiseen maailmaan, jossa laitteet ovat tietoisia ympäristöstään niihin asennettujen sensorien ja ohjelmistojen avulla (Abomhara ja Køien 2015). Lisäksi sensorien avulla laitteet keräävät tietynlaisia tietoja, kuten lämpötilaa, liikettä tai sijaintia. Abomhara ja Køien (2015) lisäävät vielä, että laitteet kommunikoivat toisien IoT-laitteiden kanssa internetin tai muun mahdollistavan teknologian välityksellä. Esineiden internet alkaa näkyä monien ihmisten arjessa, sillä se on levinnyt laajaan käyttöön sekä kodeissa että yrityksissä. On täysin mahdotonta antaa tarkkaa summaa verkkoon yhdistetyistä IoT-laitteista, mutta annettujen arvioiden mukaan luku on tällä hetkellä useita miljardeja ja määrä jatkaa koko ajan kasvamistaan.

3.1 Tietoturva tällä hetkellä

IoT-laitteet ovat yleistyneet parin vuosikymmenen aikana merkittävästi, eikä yleistyminen näytä laantuvan, suorastaan päinvastoin. Laitteiden kehitys on ollut räjähdysmäistä, mutta niiden turvallisuus ei ole kehittynyt yhtä nopeasti. Tällä hetkellä useimmat IoT-laitteet ovat kykenemättömiä puolustamaan itseään niihin kohdistuvilta hyökkäyksiltä, johtuen niiden rajallisesta laskennallisesta, muistillisesta, virrallisesta ja verkollisesta kapasiteetista (Khan ja Salah 2018; Abomhara ja Køien 2015). Kaiken lisäksi tästä vähäisestä kapasiteetista suurin osa kuluu laitteen suunniteltujen toimintojen ja ominaisuuksien käyttöön (Dorri ym. 2017). Tämän takia IoT-laitteiden rinnalle tarvitaan jokin elementti, joka toteuttaa tietojen ja laitteen toiminnan turvaamisen. Tähän on kokeiltu ratkaisuna erilaisia pilvitallennuksia laitteen tiedoille, mutta se ei ole antanut haluttua tulosta. Pelkkien pilvipalvelujen käyttäminen saattaa sisältää internetin mukana tuomia ongelmia, kuten mahdollisuudet erilaisiin kyberhyökkäyksiin, SQL-injektioihin tai tietojen peukalointiin (Wang ym. 2019). Tämän vuoksi Wang

ym. (2019) mukaan pilvitallennus ei takaa tietojen eheyttä ja saatavuutta, joten se ei ole soveltuva ratkaisu IoT-laitteille. Turvallisuuden heikkouksien syiksi Khan ja Salah (2018) lisäävät vielä standardien kehittymättömyyden yhtä nopealla tahdilla laitteiden kanssa sekä laitteisto- ja ohjelmistosuunnittelun turvallisuuden puutteet niitä kehittäessä ja käyttöönotossa.

Laitteiden sensorien avulla kerätty data jää laitteen muistiin tai jatkaa eteenpäin internetin välityksellä. Koska laitteilla on rajalliset kapasiteetit, ovat myös turvatoimet rajallisia. Tämä on suuri ongelma, sillä laitteista siirtyy valtava määrä sensorien avulla kerättyä dataa henkilökohtaisista tiloista ja tiedoista, kuten kodista tai yrityksestä, eteenpäin toisille laitteille ja verkkoon, mistä syntyy turvallisuusriskejä (Dorri, Kanhere ja Jurdak 2017). Tämän jälkeen osaava henkilö voi helposti kaivaa haluamansa tiedot laitteiden muistista tai tietoliikenteen seasta, millä voi olla merkittäviä seurauksia.

3.2 Tietoturvariskejä

Ongelmat eivät suinkaan jää laitteiden tietoturvan puutteeseen. IoT-laitteita kehitetään jatkuvasti uusiin tarkoituksiin ja uusilla ominaisuuksilla. Nämä laitteet pyritään yleisesti ottaen valmistamaan mahdollisimman halvalla, pienikokoisiksi sekä helppokäyttöisiksi, mikä aiheuttaa turvallisuusratkaisujen toteutuksille haasteita ja pahimmassa tapauksessa laitteiden turvaaminen jää taka-alalle (Singh, Singh ja Kim 2018).

Kotitalouksissa internetiin kytkettyjen laitteiden määrä voi nousta kymmeniin, ellei jopa satoihin laitteisiin. Harva kuitenkaan tulee ajatelleeksi suuria yrityksiä, joissa laitteita voi olla yhdistettynä samaan verkkoon tuhansia, jopa miljoonia. Sama pätee IoT-laitteilla, jotka ovat yhdistettynä verkkoon. Tässä piilee tietoturvariski, kun laitteita on niin paljon yhdessä verkossa. Silti olisi tärkeää pystyä tunnistamaan omat lailliset laitteet sekä poistamaan muiden toimesta lisättyjä ylimääräisiä, laittomia laitteita verkosta, joilla voidaan yrittää kalastaa tietoja (Singh, Singh ja Kim 2018).

Kaikkien ohjelmien ja laitteiden suunnittelun takana on ihminen. Jokainen tekee joskus virheitä tai jokaisella jää joskus jotakin oleellista huomaamatta, minkä takia IoT-laitteillekin jää mahdollisuus virheille ja puutteille. Jotta IoT-laitteista saataisiin täysin turvallisia, pitäi-

si niistä löytää ja korjata kaikki virheet, joiden kautta hakkerit voivat päästä niihin käsiksi (Singh, Singh ja Kim 2018). Laitteiden välillä liikkuu valtava määrä turvallisuuden ja henkilöllisyyden kannalta kriittisiä tietoja, jotka tekevät laitteista erityisen houkuttelevia kohteita erilaisille kyberhyökkäyksille (Dorri ym. 2017). Hakkereilla on aina omat motiivinsa hakkeroitua laitteisiin. He voivat hakea esimerkiksi taloudellista hyötyä tai kerätä tietoja omiin tarkoituksiin (Abomhara ja Køien 2015). Jokaisessa tapauksessa tulee silti esiin henkilökohtaiset tiedot ja paikat, jotka hakkeri voi saada selville. Esimerkiksi hakkeri voi päästä tarkkailemaan kodin turvakameroita ja aiheuttaa harmia turvajärjestelmiin.

4 Lohkoketjun soveltaminen esineiden internetin kanssa

Lohkoketjussa on monia hyötyjä, joiden avulla saataisiin tällä hetkellä tietoturvattomista IoT-laitteista turvallisempia. Tämä ei vain ole niin suoraviivaista, mitä voisi kuvitella. Tässä luvussa käydään läpi hyötyjä ja haasteita toteutuksen kannalta näiden yhdistämiseen.

4.1 Hyödyt ja tietoturvan muutos

Vaikka lohkoketjun soveltaminen IoT-laitteille on haaste, hyötyjä tekniikoiden yhdistämiselle on tutkittu ja analysoitu. Lohkoketjun hajautettu vertaisverkko auttaa torjumaan ongelmaa, jossa yhden laitteen vikatila voi aiheuttaa koko verkon liikenteen estymisen. Näin hajauttaminen tekee laitteille paremman saatavuuden, jonka seurauksena verkosta tulee vakaampi ja sen vikasietoisuus kasvaa (Sengupta, Ruj ja Das Bit 2020; Reyna ym. 2018) . Samaniego, Jamsrandorj ja Deters (2016) lisäävät hajautetun vertaisverkon lisäksi peukaloimattomuuden ketjun dataan sitä luodessa, varastoidessa ja siirtäessä, mikä on suuri lisäys IoT-systeemeille. Ketjun muuttumattomuus puolestaan estää hakkereiden hyökkäämisen yhdeltä keskitetyltä laitteelta, minkä johdosta hyökkäyksistä johtuvia kustannuksia voidaan vähentää tai parhaassa tapauksessa niiltä voidaan välttyä kokonaan (Sengupta, Ruj ja Das Bit 2020). Lohkoketjun hyödyllisyys ei siis jäisi ainoastaan turvallisuuden parantamiseen, vaan siitä voisi saada myös taloudellista hyötyä yritykselle, jossa käytetään paljon resursseja hakkerointien estämiseen ja torjumiseen.

Lohkoketjusta hyötyisi erityisesti yritykset, joilla on paljon IoT-laitteita ja he jakavat samoja verkkoja, laitteita ja tietoja yhteistyössä muiden yritysten kanssa. Lohkoketjun monet ominaisuudet lisäävät uudenlaista luotettavuutta ja turvallisuutta, mitä ei ole ennen voitu toteuttaa. Osapuolet voivat varmistua siitä, että tieto on luotettavaa, sen alkuperä voidaan selvittää ja tunnistaa kenen tai minkä laitteen tekemä lisäys on sekä tehdyt lisäykset pysyvät muuttumattomina ketjussa (Reyna ym. 2018). Laitteen tunnistus perustuu jokaisen laitteen omaan ”allekirjoitukseen”, joka lisätään lohkoketjuun uuden lohkon sisälle sen lisäyksen yhteydessä (Sengupta, Ruj ja Das Bit 2020). Näin IoT-laitteiden tiedot pysyvät turvallisesti tallessa, vaikka tieto on jaettuna kaikille yhteistyössä mukana oleville yrityksillä. Tämä ei suinkaan

tarkoita, että lohkoketjun hyöty koskisi vain yritystoimintaa, sillä samat turvallisuusaspektit pätevät pienempiin kotiverkkoihin, missä laitteita on huomattavasti vähemmän, mutta tietoihin ei haluta päästää ketään ylimääräisiä osapuolia.

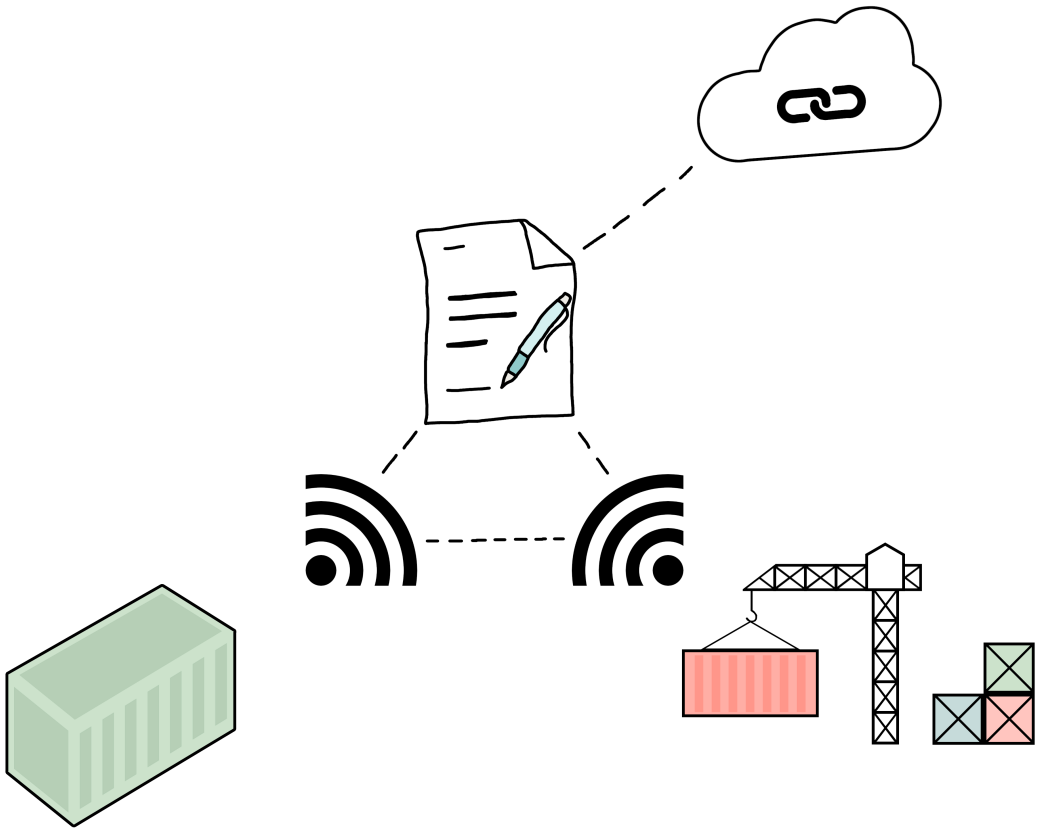
4.1.1 Yritysmaailman esimerkkejä

Hyvänä käytännön esimerkkinä IoT:n ja lohkoketjun yhdistämiseen toimii toimitusketjut sekä ruokakuljetukset. Toimitusketjussa toimii välikäsinä monia eri yrityksiä ja kuljetukset menevät monien pisteiden kautta. Jokaisella välikädellä on yleensä oma tietokanta, johon tehdään merkinnät tavaran saapumisesta, uudelleenlähetyksistä sekä merkitään muiden antamien tietojen perusteella, missä tavara kulkee milläkin ajanhetkellä (Christidis ja Devetsikiotis 2016). Lohkoketjun toimintaperiaatteen avulla voidaan siirtyä jokaisen omasta tietokannasta yhteiseen jaettuun tietokantaan, missä jokaisen tekemät lisäykset ja muutokset pysyvät muuttumattomina, kuten aiemmin mainittiin kappaleessa 2.1 Lohkoketju yleisesti. Jokainen osapuoli merkitsee tähän tietokantaan toimituksen saapuneeksi tai lähetetyksi omalla sähköisellä kuittauksella, jonka jälkeen tieto päivittyy ketjuun ja ketju päivittyy kaikille osapuolille ja näin tieto on aina tarkasteltavissa (Christidis ja Devetsikiotis 2016).

Hyöty ei jää ainoastaan yhteiseen tietokantaan, vaan lisäksi saadaan kerättyä täysin uudenlaista tietoa kuljetuksista. Ruokakuljetuksissa on tärkeä pitää tiettyjä ehtoja yllä, esimerkiksi tiettyä lämpötilaa. Lohkoketjun ja lämpömittarilla varustetun kuljetuskontin avulla voidaan pitää huoli siitä, että lämpötila on pysynyt koko kuljetusketjun ajan oikeana, tai jos ei ole, niin tieto pysyy lohkoketjussa, eikä sitä voi muokata pois (Reyna ym. 2018). Näin voidaan välttyä ikäviltä tapahtumilta ja taudeilta. Tämä on vasta yksi esimerkki, minkä lisäksi Reyna ym. (2018) luettelevat esimerkeiksi älykaupungit ja älyautot, joille tämän kaltainen toiminto soveltuu. Tämä siksi, että datan luottamuksellisuus on välttämätöntä, jotta voidaan parantaa palvelujen toimivuutta ja niiden käyttöönottoa laajennettua entistä enemmän.

Toimitusketjua voidaan ehostaa vielä entisestään lisäämällä toimintaan mukaan älysopimus, josta tarkempi esittely kappaleessa 2.2 Älysopimus lohkoketjulla. Älysopimuksen avulla saadaan välistä pois suurin osa ihmisten tekemistä merkinnöistä tietokantaan, kun tekniikka hoitaa sen automaattisesti. Toiminta perustuu Christidis ja Devetsikiotis (2016) esittämäs-

sä esimerkissä kuljetuskontteihin, joissa on radiotaajuuslähetin sekä -vastaanotin muiden tarvittavien anturien sekä IoT-ominaisuuksien lisäksi, edellyttäen, että myös jokaisella yhteistyökumppanilla on omat radiotaajuuslaitteet sekä lohkoketju asennettuna (ks. kuvio 3). Radiotaajuudet toimivat vain lyhyen matkan päähän, joten esimerkissä niitä käytetään tunnistamaan mikä tavara on missäkin sekä tunnistamaan kontin vastaanotto. Tämän jälkeen asiakkailta kirjautuu automaattisesti kirjaus lohkoketjuun tavaran vastaanottamisesta heidän omilla sähköisillä kuittauksilla, ilman että he antavat itse minkäänlaisia syöttötietoja (Christidis ja Devetsikiotis 2016).



Kuvio 3. Radiotaajuuksin varustetun kuljetuskontin ja sataman välinen älysopimus kuvitettuna. (Kuva: Samuel Lehikoinen 2021)

Yritysmaailmassa on jo tämän kaltaista toimintaa olemassa, sillä IBM tarjoaa lohkoketjupalveluja IoT-laitteille omille asiakkailleen. IBM toimii lohkoketjun palveluntarjoajana ja heillä on useita vaihtoehtoja erilaisille toimialoille. Esimerkkeinä IBM:n tarjoamista lohkoketjupalveluista ovat toimitusketju, ruokatoimitukset sekä maailmanlaajuiset maksut (“IBM Iot

blockchain” 2021).

4.2 Toteutuksen haasteet

IoT-laitteiden turvallisuudessa on huomattu puutteita jo pidemmän aikaa. Tästä juontuu juuret monien alojen kiinnostukseen hyödyntää lohkoketjua IoT-laitteille, mutta nykyisellä lohkoketjujärjestelmällä se ei vielä ole laajasti mahdollista (Wang ym. 2019). Lohkoketju kehitettiin alun perin toimimaan tehokkaiden tietokoneiden kanssa, joista IoT-laitteet ovat kaukana (Reyna ym. 2018). IoT-laitteiden resurssien vajeesta syntyy suuri ongelma tähän soveltamiseen, minkä takia ne ovat kykenemättömiä toimimaan raskaan lohkoketjun isäntänä tai solmuna (Samaniego, Jamsrandorj ja Deters 2016). Esimerkkinä bitcoinin lohkoketju on tällä hetkellä 330 gigatavua suuri kokonaisuus (“Bitcoin blockchain size” 2021), joka pitäisi pystyä lataamaan laitteelle. IoT-laitteista harvoilla on tämänlaisia muistikapasiteetteja. Resurssien vajeesta tulee ongelma myös lohkoketjun sisältämään proof of workiin, jolla on suuret resurssivaatimukset esimerkiksi suorittimen laskemisteholle (Dorri, Kanhere ja Jurdak 2017). Lisäksi lohkoketju käyttää liian suurta kaistanleveyttä ja sen sisältämä viive on liian suuri suoraan käytettäväksi useimmille IoT-laitteille (Dorri, Kanhere ja Jurdak 2017).

IoT-laitteet kommunikoivat toistensa kanssa paljon ja mitä enemmän laitteita on samassa verkossa, sitä enemmän dataa syntyy. Datan määrä määrittää vaadittavan tallennustilan lohkoketjun tiedostolle, johon kaikki tapahtumat kirjataan. Tiedoston kasvaessa suureksi alkaa aiheutua skaalautuvuusongelmia, jonka jälkeen lohkoketjun ylläpidosta alkaa tulla suuria siirto- ja varastointikustannuksia (Sengupta, Ruj ja Das Bit 2020). Skaalautuvuusongelmaa lisää IoT-laitteiden skaalautuvuusrajoitteet, jotka tekevät ongelmasta vielä suuremman. Lisäksi IoT-laitteet tuottavat gigatavujen verran dataa jatkuvasti, mutta lohkoketju pystyy toteuttamaan nykyisillä ratkaisuilla vain muutaman toiminnon sekunnissa, joten tästä koituu taas hitautta datan siirtymiselle (Reyna ym. 2018). Pidemmän päälle uusien lohkojen lisäykseen syntyy pitkä jono, joka kasvaa vain koko ajan kun dataa syntyy nopeammin, kuin lohkoja tietojen varastoimiseksi.

4.3 Mahdolliset toteutustavat

Ongelmien ratkomiseksi on mietitty monenlaisia ratkaisuja, jotta lohkoketju saataisiin käytäntöön laajemmin IoT-laitteille. Yhtenä ratkaisuna Samaniego, Jamsrandorj ja Deters (2016) esittävät pilvi- tai sumupalvelujen käyttämisen lohkoketjun rinnalla. Toisena Dorri ym. (2017) sisällyttävät pilvipalvelun käytön sekä keventävät bitcoinin lohkoketjua poistamalla proof of work:n sekä kryptovaluuttoihin liittyviä ominaisuuksia, joita ei IoT-laitteiden kanssa tarvita. Samaniego, Jamsrandorj ja Deters (2016) esimerkki muodostaisi lohkoketjun palveluna (engl. Blockchain as a service), jota isännöidään pilven tai sumun kautta, kun taas Dorri ym. (2017) esimerkissä pilvipalvelu varastoi ja jakaa tietoja. Samaniego, Jamsrandorj ja Deters (2016) tutkimuksessa testattiin yksityisen verkon ja pilvipalvelupohjaisen lohkoketjun toimintaa IoT-laitteen rinnalla. Samalla selvitettiin, miten kirjoitusoperaatioihin lisätty viive vaikuttaa toimintaan ja kirjoitusoperaatioiden ruuhkautumiseen. Tutkimuksesta selviää, että yksityisessä verkossa ei synny pullonkaulaefektiä ja laitteet saa toimimaan pienen viiveen avulla ilman suurempia piikkejä kirjoitusoperaatioissa. Pilvipohjaisessa lohkoketjussa taas huomataan piikkejä koko ajan, vaikka viivettä lisätäänkin. Tämän Samaniego, Jamsrandorj ja Deters (2016) tulkitsivat johtuvan verkon viiveestä johtuen pilvipalvelusta, joka lisää vasteaikaa.

Dorri ym. (2017) tutkimuksessa kohteena on älykoti, mutta tätä menetelmää voidaan soveltaa myös muihin IoT-ratkaisuihin. Lyhyesti avattuna jokaisessa älykodissa on oma louhija, joka tekee lisäykset lohkoketjuun sekä omat tallennustilat, joihin tallennetaan kaikkien laitteiden tiedot. Tallennustila sisältää sekä pilven että paikallisen kovalevyn. Tällä ratkaisulla lohkoketjua saadaan sovellettua IoT-laitteille ja niille saadaan lohkoketjun tuomia turvallisuusparannuksia, muun muassa palvelunestohyökkäyksille (engl. Distributed Denial of Service, DDoS) sekä linkitetyille hyökkäyksille (engl. Linking Attack) (Dorri ym. 2017).

Lopputulkinta liittyy Samaniego, Jamsrandorj ja Deters (2016) tutkimuksessa olennaisesti pilven ja sumun keskinäisiin eroihin: Pilvipalvelut tarjoavat paremman skaalaavuuden ja antavat mahdollisuuden resurssirajoitetuille IoT-laitteille, mutta sisältävät suuret viiveongelmat. Sumupalveluilla pystytään puolestaan toimimaan päinvastoin, eli resurssit ovat rajallisemmat, mutta viive pysyy pienempänä (Samaniego, Jamsrandorj ja Deters 2016). Tutkimuksessa selvisi, että verkon viive lisää vasteaikaa, joten sitä ei haluta lisätä entistä enemmän

pilvipalvelun avulla. Tässä paras ratkaisu olisi siis hyödyntää sumupalveluja, jolla saadaan viive pienemmäksi, mutta lohkoketjun muut hyödyt käyttöön (Samaniego, Jamsrandorj ja Deters 2016). Tämän lisäksi Dorri ym. (2017) tutkimuksesta selviää, että turvallisuutta saa parannettua huomattavasti, mutta se tuo mukanaan hieman korkeamman energiankulutuksen sekä viiveen laitteille. Ero ei ole kuitenkaan niin suuri, etteikö turvallisuuden paraneminen menisi etusijalle tässä taistelussa (Dorri ym. 2017). Näiden kahden tutkimuksen pohjalta olisi siis paras ratkaisu luoda lohkoketjun ja IoT-laitteiden yhdistäminen käyttämällä kevennettyä lohkoketjurakennetta, sekä tallentamalla tiedot sumupalveluihin.

5 Yhteenveto

Tämän tutkielman tavoitteena oli tarkastella IoT-laitteiden nykytilannetta turvallisuutta koskevissa asioissa. Lisäksi tarkasteltiin lohkoketjua sekä sen mahdollista soveltamista turvaamaan IoT-laitteita. Ensimmäisessä luvussa käytiin läpi lohkoketjun muuttumaton rakenne ja hajautetun vertaisverkon toimintaperiaate. Näiden avulla verkkoon tuodaan haluttu turvallisuus tuntemattomien osapuolien välille. Lisäksi luvussa käsiteltiin älysopimukset lohkoketjun rinnalla, joiden avulla sopimuksien tekemisestä saataisiin sujuvampia nykyhetkeen verrattuna.

Toisessa luvussa esiteltiin IoT-laitteet sekä niiden tämänhetkinen turvallisuustilanne. Suurimpana ongelmana IoT-laitteiden turvaamiseen on niiden rajalliset kapasiteetit, joka estää monien tämänhetkisten turvallisuusratkaisujen käytön. Ongelma on tiedostettu ja asiaa on tutkittu paljon, mutta mullistavaa suojausratkaisua ei ole vielä löydetty.

Kolmannessa luvussa otettiin kuvioon mukaan lohkoketjun ja IoT-laitteiden yhdistäminen. Päällimmäisenä selvitettiin hyötyjä teknologioiden yhdistämisestä ja pohdittiin laitteiden turvallisuuden muutosta. Lohkoketjua on jo sovellettu osittaiseen käyttöön IoT-laitteiden kanssa, joten sen toiminnasta esiteltiin esimerkki. Ilman haasteita näitäkään ei saada yhdistettyä, koska lohkoketjun ominaisuudet eivät vastaa suoraan IoT-laitteiden erityistarpeisiin. Tämä johtaa suurempaan tarkasteluun, jotta löydettäisiin sopiva ratkaisu IoT-laitteiden lohkoketjun hyödyntämiseen.

Lohkoketjun käyttäminen parantaisi IoT-laitteiden turvallisuutta, kunhan löydettäisiin sopiva ratkaisu yhdistämiseen. Tutkielmasta paljastuu pari jo tutkittua ratkaisua, joita voitaisiin hyödyntää tässä yhdistämisessä. Silti jatkotutkimuksena olisi hyvä paneutua vielä enemmän soveltamismahdollisuuksiin, miten lohkoketjusta saadaan vieläkin sopivampi ja toimivampi IoT-laitteille. Tulevaisuudessa IoT-laitteiden määrä tulee vain kasvamaan, joten olisi tärkeää saada laitteet turvattua, ennen kuin tapahtuu jotakin peruuttamatonta.

Lähteet

Abomhara, Mohamed, ja Geir M. Køien. 2015. “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks”. 4. https://doi.org/https://doi.org/10.13052/jcsm2245-1439.414. https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4.

Alaba, Fadele Ayotunde, Mazliza Othman, Ibrahim Abaker Targio Hashem ja Faiz Alotaibi. 2017. “Internet of Things security: A survey”. *Journal of Network and Computer Applications* 88:10–28. ISSN: 1084-8045. https://doi.org/https://doi.org/10.1016/j.jnca.2017.04.002. https://www.sciencedirect.com/science/article/pii/S1084804517301455.

“Bitcoin blockchain size”. 2021. Viitattu 4. maaliskuuta 2021. https://www.blockchain.com/charts/blocks-size.

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

Dorri, A., S. S. Kanhere ja R. Jurdak. 2017. “Towards an Optimized BlockChain for IoT”. Teoksessa *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI),* 173–178.

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

Evans, Dave. 2011. “How the Next Evolution of the Internet Is Changing Everything”, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic ja Marimuthu Palaniswami. 2013. “Internet of Things (IoT): A vision, architectural elements, and future directions”. Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services Cloud Computing and Scientific Applications — Big Data, Scalable Analytics, and Beyond, *Future Generation Computer Systems* 29 (7): 1645–1660. ISSN: 0167-739X. https://doi.org/https://doi.org/10.1016/j.future.2013.01.010. https://www.sciencedirect.com/science/article/pii/S0167739X13000241.

“IBM Iot blockchain”. 2021. Viitattu 8. maaliskuuta 2021. https://www.ibm.com/blockchain/iot.

Khan, Minhaj Ahmad, ja Khaled Salah. 2018. “IoT security: Review, blockchain solutions, and open challenges”. *Future Generation Computer Systems* 82:395–411. ISSN: 0167-739X. https://doi.org/https://doi.org/10.1016/j.future.2017.11.022. https://www.sciencedirect.com/science/article/pii/S0167739X17315765.

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf.

Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler ja Manuel Díaz. 2018. “On blockchain and its integration with IoT. Challenges and opportunities”. *Future Generation Computer Systems* 88:173–190. ISSN: 0167-739X. https://doi.org/https://doi.org/10.1016/j.future.2018.05.046. https://www.sciencedirect.com/science/article/pii/S0167739X17329205.

Samaniego, M., U. Jamsrandorj ja R. Deters. 2016. “Blockchain as a Service for IoT”. Teoksessa *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),* 433–436. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102.

Sengupta, Jayasree, Sushmita Ruj ja Sipra Das Bit. 2020. “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT”. *Journal of Network and Computer Applications* 149:102481. ISSN: 1084-8045. https://doi.org/https://doi.org/10.1016/j.jnca.2019.102481. https://www.sciencedirect.com/science/article/pii/S1084804519303418.

Singh, M., A. Singh ja S. Kim. 2018. “Blockchain: A game changer for securing IoT data”. Teoksessa *2018 IEEE 4th World Forum on Internet of Things (WF-IoT),* 51–55. https://doi.org/10.1109/WF-IoT.2018.8355182.

Wang, Xu, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu ja Kangfeng Zheng. 2019. “Survey on blockchain for Internet of Things”. *Computer Communications* 136:10–29. ISSN: 0140-3664. https://doi.org/https://doi.org/10.1016/j.comcom.2019.01.006. https://www.sciencedirect.com/science/article/pii/S0140366418306881.