Kai-Markus Lehtimäki

HAJAUTETUT MIKROMAKSUT ESINEIDEN INTERNETISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Lehtimäki, Kai-Markus
Hajautetut mikromaksut esineiden internetissä
Jyväskylä: Jyväskylän yliopisto, 2017, 28 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Seppänen Ville, Hämäläinen Mervi

Tämä tutkimus käsittelee mikromaksuja esineiden internetin kontekstissa vertaisarvioidun tieteellisen aineiston, teknisten valkopapereiden sekä kirjallisuuden avulla. Tutkielmassa tarkastellaan perinteisten mikromaksujen problematiikkaa ja tutkitaan mitä etuja hajautetut tilikirjatekniikat tuovat perinteisiin keskitettyihin mikromaksumenetelmiin verrattuna. Lopuksi tarkastellaan, minkälaisia käyttötapauksia mikromaksuille on esineiden internetissä ja miten hajautetut maksuratkaisut voidaan sulauttaa osaksi esineiden internetin kokonaisarkkitehtuuria. Tutkielma esittelee myös mikromaksuja ja hajautettuja maksuverkkoja hyödyntävän älyparkkihalli-sovellutuksen.

Asiasanat: mikromaksu, esineiden internet, hajautettu tilikirja, hajautettu maksuverkko, lohkoketju, tangle, älykaupunki

ABSTRACT

Lehtimäki, Kai-Markus
Decentralized micropayments in the Internet of Things
Jyväskylä: University of Jyväskylä, 2017, 28 p.
Information Systems, bachelor's thesis
Supervisor(s): Seppänen Ville, Hämäläinen Mervi

This thesis studies micropayments in the Internet of Things context through peer reviewed papers, technical white-papers and literature. Research focuses on weaknesses of traditional centralized micropayment schemes and utilization of distributed ledger technologies in order to solve these challenges. Scope of the research also includes use cases of micropayments and placement of the distributed ledger in the logical architecture of the Internet of Things. This paper also presents smart parking concept utilizing micropayments and distributed payment networks.

Keywords: micropayment, internet of things, distributed ledger, distributed payment network, blockchain, tangle, smart city

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Esineiden internet ja sen kanssa yhdessä hyödynnetyt hajautetut mikromaksut mahdollistavat uusia universaaleja liiketoimintamalleja ja prosesseja, joissa älykkäät laitteet siirtävät valuuttaa keskenään tai ihmisten kanssa täysin autonomisesti ja koneellisesti, ilman tarvetta ulkopuoliselle vuorovaikutukselle. Esineiden internetin markkinasegmentit, jossa mikromaksuja voidaan tulevaisuudessa hyödyntää saattavat McKinsleyn (2013) arvioista johdettuna olla alle kymmenen vuoden päästä jopa 800 miljardia euroa.

Hajautettuja mikromaksuja on käsitelty tieteellisessä aineistossa viime vuosien aikana jonkin verran, mutta esineiden internetin kontekstissa hajautettuja mikromaksuja ei ole tutkittu käytännössä juuri ollenkaan. Tämä kandidaatintutkielma käsittelee mikromaksuja ja tapoja toteuttaa ne esineiden internetin ympäristössä. Aluksi tutkielmassa käsitellään perinteisten keskitettyjen mikromaksumenetelmien heikkouksia ja käytännön toteutuksen ongelmia vertaisarvioidun tieteellisen aineiston avulla. Kun perinteisten menetelmien heikkoudet ovat tiedossa, tutkitaan hajautettuja tilikirjatekniikoita ja sitä, miten mikromaksuja voidaan toteuttaa niiden avulla ja miksi ne ovat keskitettyjä ratkaisuja paremmin soveltuvia mikromaksuihin. Hajautettuja maksuverkkoja ja tilikirjatekniikoita tarkastellaan pääosin niiden teknisten valkopapereiden ja niihin liittyvän kirjallisuuden avulla koska tieteellistä aineistoa aiheesta ei ollut saatavilla. Seuraavaksi tutkitaan, minkälaisissa vertikaalisten markkinoiden sovellutuksissa mikromaksuja voitaisiin mahdollisesti hyödyntää ja kuinka isoja nämä markkinasegmentit tulevaisuudessa saattavat olla. Tutkielman lopuksi esitetään mikromaksuja ja hajautettua tilikirjaa hyödyntävän älyparkkihallin konsepti.

Tutkielmassa aihealuetta käsitellään kandidaatintutkielmalle ominaisella suhteellisen matalalla syvyydellä. Tämä tutkielma ei ole systemaattinen kirjallisuuskatsaus, vaan se sisältää myös paljon omaa pohdintaa ja synteesiä tieteellisen aineiston puutteellisuuden takia. Tarkoituksena on, että tutkielma antaa teknisesti kompetentille lukijalleen tarvittavan pohjaosaamisen aihealueeseen liittyvien ratkaisuiden suunnittelua ja toteuttamista varten.

Tutkielmassa pyritään hankkimaan vastauksia seuraaviin tutkimuskysymyksiin:

- Miten hajautettua tilikirjaa voidaan hyödyntää esineiden internetin mikromaksuliikenteessä?
- Voidaanko esineiden internetin mikromaksut toteuttaa hajautetun tilikirjan avulla ilman luotettua kolmatta osapuolta?
- Mitä hyötyjä hajautetut mikromaksut tuovat perinteisiin keskitettyihin mikromaksuihin verrattuna?
- Miten hajautettu tilikirja sulautetaan osaksi esineiden internetin kokonaisarkkitehtuuria?
- Mitä käyttötapauksia ja markkinoita mikromaksuille on esineiden internetissä?

2 ESINEIDEN INTERNET (IoT)

Tänä päivänä melkein neljä miljardia ihmistä ympäri maailman käyttää internetiä moneen eri käyttötarkoitukseen päivittäin. Internet käsitteenä on kuitenkin murrosvaiheessa. Internetistä on muodostumassa aikaisemman lisäksi myös maailmanlaajuinen alusta erilaisten älykkäiden laitteiden väliselle kommunikaatiolle. International Telecommunication Unionin mukaan esineiden internetillä (IoT) tarkoitetaan tätä verkkoa ja siihen kytkettyjä älykkäitä laitteita ja palvelimia. (ITU, 2016).

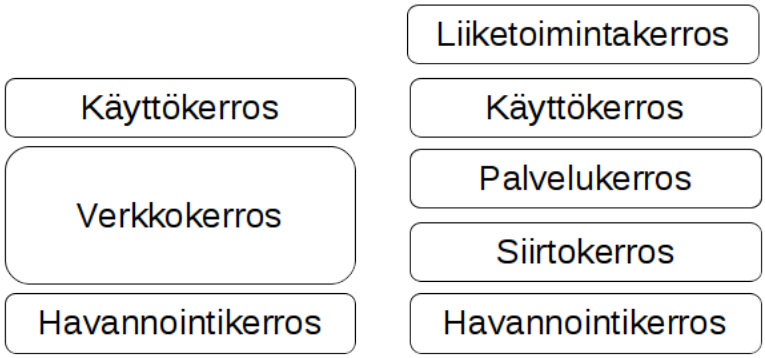
Esineiden internet ei ole itsessään kuitenkaan täysin yksiselitteinen käsite. Aihetta on tutkittu jo vuosien ajan, mutta silti täydellisen yksimielistä määritystä käsitteelle ei ole olemassa. Jotkin tutkijat jakavat esineiden internetin paradigman osiin erilaisten lähestymistapojen perusteella. (Aztori, Lera & Morabito, 2010). Esineiden internetiä voidaan määrittää myös teknisemmästä, arkkitehtuurillisesta näkökulmasta esimerkiksi loogisten rakennemallien avulla. (Wu, Lu, Ling, Sun & Du, 2010; Khan, Zaheer & Khan, 2012).

2.1 Esineiden internetin looginen rakenne

Esineiden internetiin kuuluvien verkkojen, laitteiden ja muun infrastruktuurin järjestelmällinen kuvaaminen on tekniikoiden sulautuneisuuden takia hankalaa. Kolmitasoinen arkkitehtuurikuvaus on aineistona käytetyssä tutkimuskirjallisuudessa yleisesti käytetty viitekehys esineiden internetin teknisen kokonaisarkkitehtuurin järjestelmälliselle tarkastelulle (Khan ym., 2012; Al-Fuqaha, Guizani, Mohammadi, Aledhari & Ayyash, 2015). Kolmitasoinen malli on kuitenkin liian yksinkertainen tapauksiin, joissa arkkitehtuuria täytyy mallintaa tarkemmin, esimerkiksi tietoa varastoivien ja käsittelevien palvelimien osalta. Tämän takia tutkijat, kuten Wu ym. (2010) sekä Zhong, Zhu ja Huang (2016) ovat ehdottaneet käytettäväksi myös muita kehittyneempiä malleja, kuten viisitasomallia, joka laajentaa alkuperäistä kolmitasomallia.

Esineiden internetin kolmi- ja viisitasomallit muistuttavat päällisin puolin TCP/IP- ja OSI- mallia, mutta niitä ei pidä kuitenkaan sekoittaa keskenään. Kolmi- ja viisitasomallista kummastakin löytyy yhteneväisyyksiä, mutta suurin

ero näissä kahdessa mallissa löytyy verkkokerrokselta: viisitasomallissa verkkokerros on jaettu edelleen kahteen osaan siirto- ja palvelukerrokseksi. Viisitasomallissa käyttökerroksen päälle on myös lisätty liiketoimintakerros. Tutkimuksessa käytetyssä lähdeaineistossa arkkitehtuurin kerroksia kuvataan tutkimuksesta riippumatta suhteellisen yhteneväisesti. Ainoastaan joidenkin kerrosten nimeämiset eroavat hieman tutkimuksesta riippuen.



Kuvio 1: Esineiden internetin kolmi- ja viisitasomalli

2.1.1 Kolmitasomalli

Kummankin arkkitehtuurimallin alin kerros, eli **havainnointikerros** toimii rajapintana fyysisen maailman ja esineiden internetin välillä (Zhong ym., 2016). Kerroksen tehtävänä on havainnoida fyysisen esineen ominaisuuksia, kuten lämpötilaa, liikettä, sijaintia tai painoa. Kun tieto on kerätty, havainnointikerros muuttaa sen digitaaliseen muotoon ja välittää sen eteenpäin ylemmille arkkitehtuurin kerroksille verkon yli siirtämistä varten. Havainnointikerrokseen liittyvät läheisesti älykkäät esineet ja erilaisia suureita mittaavat sensorit. (Khan ym., 2012.) Älykkäillä esineillä viitataan fyysisiin esineisiin, joihin on lisätty ”älyä” sulautetun tietotekniikan avulla. Tyypillisesti verkkoon kytketyt älykkäät laitteet keräävät tietoa ympäristöstään ja kommunikoivat muiden laitteiden tai palvelimien kanssa verkon ylitse autonomisesti, ilman ihmisen ja esineen välistä vuorovaikuttamista. (Kortuem, Kawsar, Sundramoorthy & Fitton, 2010). Kolmitasomallissa esiintyvän **verkkokerroksen** tehtävänä on siirtää ja prosessoida dataa, jota havainnointikerros tuottaa. Kolmitasomallin mukaiseen verkkokerrokseen sisältyvät mm. sensoriverkot, perinteiset verkot sekä datan prosessointi- ja tallennuskomponentit. (Wu ym., 2010) Suurin kolmi- ja viisitasomallin välinen ero löytyy tästä kerroksesta; viisitasomallissa verkkokerros on jaettu kahteen eri kerrokseen: siirtokerrokseen ja palvelukerrokseen. Kummassakin mallissa esiintyvän **käyttökerroksen** tehtävä on hakea tietoa alemmalta arkkitehtuurin kerrokselta ja tarjota tarvittavat palvelut loppukäyttäjälle. Käyttökerroksen palvelu voi esimerkiksi tarjota lämpötila- ja kosteusarvoja tietyltä laitteelta, kun loppukäyttäjä tätä tietoa pyytää. Käyttökerroksen toteuttamat palvelut riippuvat kontekstista, jossa esineiden internetiä hyödynnetään. Tämä arkkitehtuurin taso tarjoaa pääsyn dataan useille vertikaalisille markkinoille, kuten älykodille ja älykaupungille. (Al-Fuqaha ym., 2015)

2.1.2 Viisitasomalli

Viisitasomallissa esiintyvän **siirtokerroksen** tehtävänä on siirtää havainnointikerroksen laitteelta vastaanotettu digitalisoitu data langattomien tai langallisten verkkojen avulla ylöspäin palvelukerrokselle. Tähän kerrokseen liittyvät olennaisesti erilaiset pitkän ja lyhyen kantomatkan verkkotekniikat, kuten: 5G, Bluetooth, Zigbee ja LoRa. (Khan ym., 2012.) Viisitasomallin mukaisen **palvelukerroksen** tehtävänä on yhtenäistää, transformoida ja varastoida siirtokerrokselta vastaanotettua dataa. Dataa lähettävästä älykkäästä laitteesta riippuen laitteet toteuttavat erilaisia palveluita, eivätkä laitteet pysty kommunikoimaan keskenään, jolleivat kumpikin toteuta samaa palvelua. (Khan ym., 2012). Palvelukerros toimii rajapintana heterogeenisten älykkäiden esineiden sekä ylempien arkkitehtuurikerrosten keskinäisessä viestinnässä. Tämä mahdollistaa sen, että laitteet ja ohjelmistot pystyvät hyödyntämään muita verkon laitteita palvelukerroksen kautta homogeenisena joukkona, riippumatta arkkitehtuurin alemmilla kerroksilla käytetyistä tekniikoista. Viisitasomallin ylimmän kerroksen eli **liiketoimintakerroksen** tehtävänä on hallita esineiden internetin sovelluksia ja niihin liittyviä liiketoimintamalleja. Tämä kerros ja sen sisältämät liiketoimintamallit ovat tärkeässä osassa esineiden internetin menestyksellistä hyödyntämistä (Wu ym., 2010). Myös Khan ym. (2012) painottaa liiketoimintakerroksen ratkaisujen merkitystä. Liiketoimintakerrokseen liittyvät keskeisesti erilaiset kaaviot ja mallit, joiden avulla alempien kerrosten keräämästä big datasta saadaan analysoimalla jotain uutta, strategista liiketoimintapäätöstä tukevaa informaatiota (Al-Fuqaha ym., 2015).

2.2 Kohti ubiikkia esineiden internetiä

Esineiden internetiin kytkettyjen älykkäiden laitteiden määrä on kasvussa kiihtyvällä tahdilla (Gartner, 2015). Älykkäiden laitteiden määrän kasvaessa perinteinen käsitys internetistä loppukäyttäjän päätteen verkkoon yhdistävänä infrastruktuurina on muuttumassa. Tulevaisuuden internet tulee olemaan saumaton ja ubiikki kokonaisuus, joka koostuu perinteisistä verkoista ja palvelimista, uusista verkkoteknologioista ja verkkoon kytketyistä älykkäistä laitteista. Sisältö ja palvelut tulevat olemaan kaikkialla ympärillämme ja aina saatavilla. Muutoksen myötä aukeavat mahdollisuudet uusille palveluille ja sovellutuksille, jotka yhdistävät virtuaalisen ja fyysisen maailman toisiinsa sulautetun tietotekniikan ja verkkojen avulla (Miorandi, Sicari, De Pellegrini & Chlamtac, 2012.) Tulevaisuudessa myös ilman ihmisen vuorovaikutusta toimivat laitteiden väliset maksut alkavat yleistyä teknologioiden ja infrastruktuurien kehittyessä. Koneellisesti suoritettuna maksut voivat olla todella tarkkoja ja esimerkiksi auton parkkiaikaa voidaan maksaa sekunti kerrallaan käytön mukaan, täysin reaaliaikaisesti. Jotta edellä mainittu mikromaksuliikenne voitaisiin käytännössä toteuttaa, täytyy teknisen ratkaisun lisäksi kehittää menetelmiä myös pienten ja tiheään tapahtuvien maksujen toteuttamista ja käsittelyä varten.

3 PERINTEISET MIKROMAKSUT

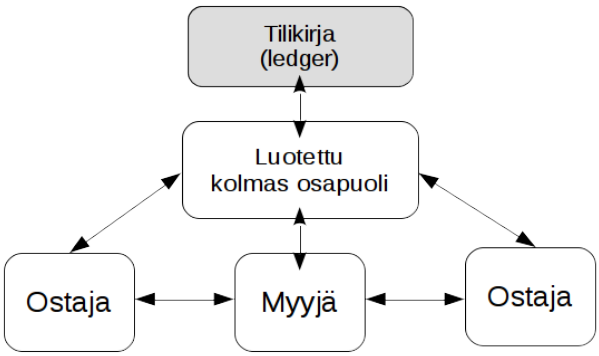
Mikromaksuista puhuttaessa tarkoitetaan yleensä vähäarvoista elektronista rahansiirtotapahtumaa. Vähäarvoisen maksun määritelmä on mikromaksualustasta ja käyttötapauksesta riippuvainen. Yleisen käsityksen mukaan mikromaksun summa on sentin kymmenyksestä muutamaan dollariin. (Kytöjoki, Kärpijoki, 2000.) Mikromaksuja ja niiden käytännön toteutuksia on tutkittu paljon jo viime vuosituhannelta lähtien. (Rivest & Shamir, 1996; Rivest, 1997; Jarecki & Odlyzko, 1997). Perinteiset keskitetyt mikromaksualustat ja ratkaisumenetelmät eivät ole vuosien saatossa kuitenkaan yleistyneet niiden sisältämien heikkouksien takia. (Chiesa, Green, Liu, Miao, Miers & Mishra, 2017). Merkittäviä keskitettyjen ratkaisumenetelmien heikkouksia ovat esimerkiksi siirtokuluongelma ja offline-siirtojen aiheuttama ylikulutusongelma. Kumpikin näistä ongelmista liittyy luotetun kolmannen osapuolen tarpeeseen siirtojen varmentamisessa. (Chiesa ym., 2017.)

Tässä luvussa käsitellään lähdeaineiston avulla mikromaksuja ja niihin liittyvää problematiikkaa. Aluksi perehdytään perinteisiin keskitettyihin mikromaksumenetelmiin, niiden geneerisiin ongelmiin ja toteutuksen osapuoliin sekä heidän rooleihinsa osana toteutuksen kokonaisuutta. Seuraavaksi läpikäydään jo olemassa olevia keskitettyjä menetelmiä ja pyritään selvittämään, mitä haasteita ja ongelmia ratkaisuiden keskitetty luonne aiheuttaa.

3.1 Keskitetyt mikromaksumenetelmät

Keskitetyillä mikromaksumenetelmillä tarkoitetaan tässä tutkielmassa menetelmiä, joissa mikromaksukokonaisuuden ylläpidosta vastaa tiedossa oleva luotettu entiteetti, eli luotettu kolmas osapuoli. Jokainen osapuolten välinen siirto täytyy tulla luotetun kolmannen osapuolen tietoon, koska luotetun kolmannen osapuolen tehtävänä on tilikirjan ylläpito ja ajan tasalla pitäminen. Käytännössä luotettu kolmas osapuoli toimii solmuna ostajien, myyjien ja tilikirjan välillä. Tämä tekee luotetun kolmannen osapuolen avulla toteutetuista menetelmistä keskitettyjä. (Chiesa, 2017.)

Käytännössä jokaisessa perinteisessä keskitetyssä mikromaksumenetelmässä ovat tavasta riippumatta osallisena samat osapuolet, joiden roolit ovat myös kutakuinkin samat (kuvio 2). Yleisesti ratkaisuissa esiintyviä rooleja ovat ostaja, joka lähettää maksun, myyjä, joka vastaanottaa maksun ja luotettu kolmas osapuoli. (Lipton & Ostrovsky, 1998.) Luotettu kolmas osapuoli pitää huolen esimerkiksi siitä, että myyjät saavat maksun kokonaisuudessaan ja että ostajalla on tarvittavat varat siirron suorittamiseen. Luotetun kolmannen osapuolen sisältävässä skenaariossa myyjän ja ostajan ei tarvitse luottaa toisiinsa, riittää että kumpikin luottaa luotettuun kolmanteen osapuoleen. Luotetun kolmannen osapuolen vastuulla on ratkaista mahdolliset konfliktitilanteet muiden osapuolien kesken. (Lipton & Ostrovsky, 1998.) Useassa perinteisissä toteutuksissa luotetun kolmannen osapuolen käytännön tehtävänä on kryptografian avulla digitaalisesti allekirjoittamalla varmistaa ostajan luotettavuus ja varallisuus. Luotettu kolmas osapuoli voi myös tarvittaessa laskea liikkeelle virtuaalivaluuttaa ja lunastaa sekä vaihtaa myyjän keräämät maksut takaisin fiat-valuutaksi. (Rivest & Shamir, 1996.)



Kuvio 2: Perinteisten menetelmien roolit ja vuorovaikutus

3.2 Käytännön toteutuksen ongelmat

Perinteinen mikromaksujen toteutuksessa vastaan tuleva ongelma on luotetun kolmannen osapuolen aiheuttama **siirtokuluongelma**. Maksuliikenteen prosessoija, eli luotettu kolmas osapuoli ottaa maksun siirtojen käsittelystä. Tämä on ongelmallista tilanteessa, jossa mikromaksun siirtokulut saattavat olla jopa suuremmat, kuin maksun summa itsessään. (Chiesa ym., 2017.) Elektronisten maksujen käsittelijälle maksujen prosessoinnista aiheutuu kustannuksia esimerkiksi käytetyn laskentatehon, virrankulutuksen ja verkkoresurssien käytön takia. Tämän takia luotetun kolmannen osapuolen ei ole kannattavaa hoitaa rooliansa ilman rahallista kompensaatiota. Luotetun kolmannen osapuolen rooli vaatii rahallisten kulujen lisäksi myös monimutkaisen liikesuhdeverkoston kaikkien alustaa käyttävien osapuolten välille (Chiesa ym., 2017). Tämä vaikeuttaa huomattavasti yleiskäyttöisten mikromaksualustoiden toteuttamista. Jotta yleiskäyttöisiä keskitettyjä mikromaksualustoja voitaisiin tehokkaasti toteuttaa, täy-

tyisi maksunkäsittelijöiden ja pankkien maailmanlaajuisesti muuttaa toimintatapojaan näille menetelmille yhteensopivimmiksi. (Pass & Shelat, 2015).

Ongelmia keskitettyjen mikromaksumenetelmien suunnittelussa ja toteuttamisessa aiheuttaa myös se, että useat menetelmät vaativat jatkuvaa yhteydenpitoa luotetun kolmannen osapuolen ja siirron muiden osapuolten välillä. Menetelmät, joissa luotettu kolmas osapuoli varmentaa kaikki siirrot kutsutaan online-menetelmiksi. Offline-menetelmät eroavat online-menetelmistä siten, että niissä luotetun kolmannen osapuolen ei tarvitse erikseen varmentaa jokaista siirtoa, vaan usein esimerkiksi koko päivän maksut varmennetaan yhdellä kertaa, päivän päätteeksi. Tämä saattaa kuitenkin aiheuttaa ns. **ylikulutusongelman**, joka tunnetaan myös nimellä double spending problem. (Chiesa, 2017.) Käytännössä tämä tarkoittaa sitä, että ostaja saattaa käyttää samoja varoja useaan kertaan ennen kuin tilikirja on päivitetty, koska tilikirjaa ei offline-siirroissa päivitetä jokaisen siirron yhteydessä. Tässä tapauksessa ostajan varallisuus menee negatiiviseksi ja mahdollinen ylikulutus selviää myyjälle vasta päivän päätteeksi, kun tilikirjaan päivitetään päivän siirrot. Perinteisissä mikromaksumenetelmissä ylikulutuksesta koituva taloudellinen tappio jää usein myyjän maksettavaksi. (Jareck & Odlyzko, 1997; Rivest & Shamir, 1996.)

Käytännössä jokainen seuraavassa osiossa läpi käyty keskitetty mikromaksumenetelmä pyrkii ratkaisemaan enemmän tai vähemmän edellä mainittuja perinteisiä mikromaksujen ongelmia. Vaikka ratkaisumenetelmissä esitetään toimivia tapoja ongelmien ratkaisemiseksi, perustuvat ne silti vahvasti siihen, että mikromaksukokonaisuutta hallinnoi yksi tai useampi luotettu kolmas osapuoli.

3.3 Keskitetyt menetelmät lähdekirjallisuudessa

Wheeler (1996) ja Rivest (1997) ehdottavat mikromaksujen toteuttamiseksi toistuvien maksujen todennäköisyyksiin ja odotusarvoihin perustuvaa menetelmää. Yksinkertaisuudessaan tämä toimii niin, että maksun vastaanottaja saa isomman summan tietyllä todennäköisyydellä, joka riippuu mikromaksun summasta. Tällä tavalla maksun saaja vastaanottaa odotusarvoisesti oikean määrän rahaa. Esimerkiksi yhtä senttiä maksaessa ostaja voi myöntää myyjälle arpalipukkeen, josta voittaa 1/1000 todennäköisyydellä kymmenen euron voiton. Tällä tavalla myyjä saa pitkässä juoksussa juuri oikean määrän rahaa. Tämä menetelmä tarvitsee luotetun kolmannen osapuolen varmistamaan, että ostajalla on oikeus myöntää arpalipuke (ostajan tilillä on rahaa). Tämän menetelmän heikkous piilee siinä, että ostaja saattaa omistaa enemmän myönnettyjä lipukkeita kuin tilillä on rahaa, jos ostajalla on käynyt ”huono tuuri” ja myönnetyistä arpalipukkeista voitokkaita on ollut odotusarvoa suurempi määrä. Tässä tapauksessa häviön joutuu kärsimään arpalipukkeen vastaanottanut myyjä. Mikromaksut ovat yleensä kuitenkin usein toistuvia ja summiltaan pieniä. Hetkellinen ylikulutus korjaantuu usein maksujen toistuessa odotusarvon mukaisesti, joten ylikulutuksella ei ole pitkässä juoksussa merkittävää taloudellista vaikutusta.

Myös Rivest ja Shamir (1996) ovat kehittäneet myös kaksi tapaa joiden avulla mikromaksut voidaan toteuttaa mahdollisimman pienellä määrällä paljon resursseja kuluttavia kryptografisia allekirjoituksia. Näissä menetelmissä suurin osa kryptografisista allekirjoituksista on korvattu tehokkaammilla hajautusalgoritmioperaatioilla. Tämä tekee maksujen käsittelystä kustannustehokkaampaa. Kumpikin menetelmä perustuu siihen, että luotettu kolmas osapuoli valtuuttaa ostajan tekemään mikromaksuja ja lunastaa myyjien vastaanottamat maksut. Kumpikin menetelmistä ratkaisee myös ylikulutusongelman. Ensimmäinen esitetty ”PayWord” (Rivest & Shamir, 1996) menetelmä perustuu maksusanaketjuun. Tämä menetelmä on suunniteltu tarpeisiin, joissa mikromaksuja tehdään tiheästi ja jatkuvasti kahden saman osapuolen välillä. Kuvitellaan esimerkin vuoksi, että yhden maksusanan arvo on yksi sentti. Aluksi luotettu kolmas osapuoli valtuuttaa ostajan luomaan maksusanaketjun. Kun ostaja tekee ensimmäisen maksun myyjälle, luodaan uuden ostajan ja myyjän välisen maksusanaketjun julkisten avainten ja hajautusalgoritmien avulla. Aina kun ostaja maksaa yhden sentin myyjälle, paljastaa se yhden sanan verran maksusanaketjusta. Tämän jälkeen myyjä varmistaa, että maksusana on validi lisäämällä sen maksusanaketjun loppuun ja ajamalla ketjun hajautusalgoritmin läpi. Tällä tavalla ostaja ja myyjä voi tehdä useita maksuja ilman luotetun kolmannen osapuolen vuorovaikuttamista joka maksun välissä. Riittää, että luotettu kolmas osapuoli päivän lopuksi vastaanottaa pisimmän ostajan ja myyjän välisen maksusanaketjun, velottaa ostajalta kokonaissumman ja tilittää sen myyjälle. Toinen Rivestin ja Shamirin (1996) esittämä ”MicroMint” menetelmä perustuu siihen, että mikromaksualustan ylläpitäjä louhii ja vaihtaa virtuaalisia kolikoita alustan käyttäjille. Alustan ostajat vaihtavat fiat-valuuttaa kolikoiksi alustan ylläpitäjän kanssa ja maksavat kolikoilla maksuja hyödykkeistä myyjille. Lopuksi myyjät vaihtavat kolikot fiat-valuutaksi alustan ylläpitäjän kanssa. Kolikoiden louhiminen tapahtuu hajautusalgoritmien avulla. Kolikot on suunniteltu siten, että niiden aitous on helposti laskettavissa, mutta niiden väärentäminen vie niin paljon laskentaresursseja, että pieniarvoisten kolikoiden väärentäminen ei ole taloudellisesti kannattavaa.

Probalistic polling - menetelmä (Jareck & Odlyzko, 1997) on todennäköisyyksiin perustuva ”hybridimenetelmä”. Tämä tarkoittaa sitä, että menetelmä toteuttaa offline- ja online-siirtoja. Menetelmä pyrkii hyödyntämään kummankin, online- ja offline-siirtojen hyötyjä ja samalla minimoimaan niiden haittoja. Käytännössä menetelmä toimii siten, että lähtökohtaisesti siirrot toimivat ilman luotetun kolmannen osapuolen varmistusta. Jokaista siirtoa suorittaessa on kuitenkin pieni todennäköisyys, että luotettu kolmas osapuoli otetaan mukaan varmentamaan maksua. Tällä tavalla luotetulla kolmannella osapuolella on arvio siitä, kuinka paljon maksaja on varojaan kuluttanut ja paljonko varoja on jäljellä. Todennäköisyys, jolla luotetun kolmannen osapuolen varmistus maksuun tarvitaan, riippuu siitä, kuinka iso varmistettavan maksun summa on ja kuinka ison ylikulutusriskin luotettu kolmas osapuoli haluaa ottaa. Tällä menetelmällä mikromaksut voidaan siis toteuttaa niin, että jokaista siirtoa ei tarvitse varmentaa luotetun kolmannen osapuolen avulla, mutta riskit taloudelliseen tappioon ylikulutuksen takia on minimoitu.

4 HAJAUTETTU TILIKIRJA

Kuten jo aikaisemmin tässä tutkielmassa todettiin: suurin osa aikaisempiin mikromaksuihin liittyvistä ongelmista liittyi jollain tavalla luotettuun kolmanteen osapuoleen, jonka tehtävänä on toimia solmuna maksuverkon käyttäjien ja tilikirjan välillä. Viimeaikaiset mikromaksuja käsittelevät tieteelliset julkaisut (Chiesa, 2017; Pass & Sheelat, 2016) ovat kuitenkin keskittyneet **hajautettuihin tilikirjatekniikoihin** jotka pyrkivät toteuttamaan luottovapaita siirtoja. Luottovapailla siirroilla tarkoitetaan tässä tutkielmassa siirtoja, jotka ovat kaikkien osapuolten varmennettavissa julkisesta tilikirjasta ilman tarvetta luotetun kolmannen osapuolen vuorovaikutukselle.

Hajautetut tilikirjatekniikat, kuten Lohkoketju (Nakamoto, 2008) ja Tangle (Popov, 2016) tarjoavat mikromaksujen toteutukseen täysin uudet puitteet. Hajautetut tilikirjatekniikat ratkaisevat useita keskitettyjen ratkaisujen suurimmista ongelmista poistamalla luotetun kolmannen osapuolen ja tekemällä siirroista luottovapaita. Maksuverkon käyttäjien ei siis enää tarvitse omistaa yhteistä luotettua entiteettiä vaan riittää, että käyttäjät luottavat maksuverkon protokollaan ja sääntöihin, jotka protokollassa on määritelty. Saavutettu hyöty on niin merkittävä, että se saattaa aiheuttaa jopa paradigmahypyn perinteisistä keskitetyistä menetelmistä uuteen, ilman kolmatta osapuolta toimivaan hajautettuun tapaan suunnitella ja toteuttaa mikromaksualustoja ja menetelmiä.

Yksi suurimpia ratkaistuja ongelmia hajautetun tilikirjan ratkaisuissa on se, miten kaikki verkon jäsenet pääsevät yhteisymmärrykseen eli konsensukseen julkisen tilikirjan sisältämien tilien saldoista. Lohkoketju ja Tangle kumpikin ratkaisevat ongelman proof of work menetelmän avulla. Perimmäinen ajatus kummassakin tekniikassa on sama, mutta tekninen toteutus Tanglen ja Lohkoketjun välillä eroaa hieman toisistaan. Erot menetelmän hyödyntämisessä vaikuttavat merkittävästi myös maksuverkkojen mikromaksuille olennaisiin ominaisuuksiin, kuten siirtokuluihin ja maksujen varmennusaikoihin.

4.1 Bitcoin ja perinteinen lohkoketju

Bitcoin esiteltiin ensimmäistä kertaa Satoshi Nakamoto pseudonyymiä käyttävän entiteetin julkaisemana valkopaperina. (Nakamoto, 2008) Julkaisusta eteenpäin Bitcoin on toiminut avoimen lähdekoodin projektina. (Bitcoin.org, 2017) Bitcoinin lohkoketjun ja elinkaaren aloittava genesis-block louhittiin vuonna 2009. Käytännössä Bitcoin on kokoelma käsitteitä ja tekniikoita, jotka yhdessä muodostavat ekosysteemin hajautetuille digitaalisille maksuille. Bitcoinit ovat valuuttaa, jota Bitcoin verkon käyttäjät voivat säilyttää ja siirtää toisilleen. Maksuverkon käyttäjät ovat toisiinsa yhteydessä internetin ylitse Bitcoin protokollan avulla. Bitcoineja voi ostaa, myydä ja vaihtaa muihin valuuttoihin esimerkiksi siihen tarkoitetuissa kryptovaluuttapörsseissä. (Antonopoulous, 2014, s.1.)

4.1.1 Bitcoinin korkean tason toiminta

Korkean tason toimintaa avaavassa esimerkissä asiakas maksaa kaupan kassalla ruokaostoksensa Bitcoinilla. Aluksi asiakkaan on saatava käsiinsä Bitcoineja (BTC); valuuttaa jolla hän voi maksaa ostoksensa. Asiakkaalla on muutama tapa hankkia Bitcoineja. Niitä voi ostaa niitä käteisellä kasvotusten tehtävässä kaupassa jonkun muun ihmisen kanssa. Asiakas voi ostaa Bitcoineja myös automaatista tai kryptovaluutan vaihtoon erikoistuneelta yritykseltä. Internetissä toimii myös pörssejä, joissa Bitcoineja vaihdetaan fiat –valuuttapareja vasten. Kun asiakas ostaa Bitcoineja, hän saa sen hetkisen vaihtokurssin mukaisen määrän Bitcoineja. Vastaanotettu valuutta siirtyy säilytettäväksi asiakkaan mobiililaitteessa sijaitsevaan virtuaaliseen lompakkoon. Supermarketketju on alkanut vastaanottaa maksuja eurojen lisäksi myös Bitcoinilla ja hankkinut point-of-sale järjestelmät, jotka tukevat Bitcoinia maksutapana. Kun asiakas menee asioimaan kauppaan ja siirtyy kassalle maksamaan ostoksensa, saa hän tietää ostoksensa kokonaishinnan paikallisella valuutalla. Ennen maksua asiakas saa valita maksaako hän ostoksensa paikallisella valuutalla vai Bitcoinilla. Kun asiakas valitsee käytettäväksi Bitcoinin, antaa kassalla oleva näyttö QR-koodin ja reaaliaikaisen vaihtokurssin paikallisen valuutan ja Bitcoinin välillä. Asiakas skannaa koodin älypuhelimensa kameralla ja vahvistaa maksun älypuhelimellaan sijaitsevasta lompakostaan. Muutaman sekunnin päästä maksusta point-of-sale järjestelmä havaitsee suoritetun maksun Bitcoin-verkossa. Lopuksi asiakas vastaanottaa kuitin ostoksistaan.

4.1.2 Lohkoketjun tekninen toiminta ja käsitteet

Viime kappaleen esimerkissä asiakas suoritti maksun omasta lompakostaan maksuksi ostoksistaan. Todellisuudessa Bitcoinit eivät kuitenkaan olleet konkreettisesti missään vaiheessa asiakkaan hallussa. Asiakkaan omistamat Bitcoinit sijaitsevat **julkisessa tilikirjassa** eli Bitcoinin tapauksessa lohkoketjussa. Valuutan omistaja on siis käytännössä se entiteetti, joka pystyy todistamaan omistus-

suhteen lohkoketjussa sijaitsevaan valuuttaan. Maksuverkon käyttäjät todistavat omistussuhteensa lohkoketjussa sijaitseviin Bitcoineihin omistamalla julkista avainta vastaavan **yksityisen avaimen** joka mahdollistaa siirtojen allekirjoituksen lohkoketjussa. Tätä kutsutaan julkisen avaimen salaukseksi. Käytännössä kuitenkin loppukäyttäjä ei aina itse pidä huolta omista avaimistaan. Edellisen kappaleen esimerkissä asiakkaan yksityistä avainta säilytti asiakkaan mobiililaitteessa sijaitseva **lompakkosovellus**. 256 -bittisestä yksityisestä avaimesta johdetaan elliptisen käyrän kryptografian avulla **julkinen avain**, josta johdetaan eteenpäin lompakon osoite. **Lompakon osoite** on käytännössä 256-bittinen luku, mutta se esitetään heksadesimaalimuodossa, jolloin sen pituus on 64 merkkiä pitkä. Lompakon osoite sisältää julkisen avaimen lisäksi myös esimerkiksi tarkistussumman näppäilyvirheen varalta. Maksuverkon käyttäjä vastaanottaa valuuttaa lohkoketjussa omasta yksityisestä avaimesta johdettuun lompakko-osoitteeseensa. (Antonopoulous, 2014, s. 61-105.)

Lohkoketjua käytetään Bitcoinin tapauksessa julkisena tilikirjana. Käytännössä lohkoketju siis sisältää tiedon kaikista **siirroista**, jotka ovat tapahtuneet Bitcoinin synnyn, eli **genesis-lohkon** jälkeen. Lohkoketjun sisältämät digitaalisesti allekirjoitetut siirrot kertovat verkolle, että valuutan nykyinen omistaja (lompakon osoite) on hyväksynyt valuutan siirron toiseen osoitteeseen. Aikaisemmassa esimerkissä supermarketin point-of-sale järjestelmä luo siirron ja antaa sen QR koodin muodossa asiakkaan puhelimen luettavaksi. Asiakkaan puhelin lukee koodista lompakon osoitteen ja maksun loppusumman sisältävän siirron puhelimen lompakkosovellukseen, allekirjoittaa sen lompakkosovelluksen ylläpitämillä avaimilla ja lähettää sen Bitcoin-verkkoon. Bitcoin-verkkoon yhdistetty point-of-sale järjestelmä havaitsee maksun pian sen lähettämisen jälkeen verkkoon julkaistujen **varmistamattomien siirtojen** joukosta ja viimeistelee maksutapahtuman. Jos myyjä vastaanottaa normaalia suuremman maksun, voidaan ennen maksutapahtuman hyväksymistä odottaa muutaman lohkon syntymisen ajan ja sen jälkeen varmistaa, että siirto on vieläkin varmennettavissa julkisesta tilikirjasta. Mitä useamman lohkon ajan myyjä odottaa ennen maksun hyväksymistä, sitä pienempi riski ylikulutukseen on. Kolmen uuden lohkon jälkeen ylikulutus on käytännössä mahdotonta. Kun Bitcoin-verkkoon julkaistu siirto on lisätty osaksi lohkoketjuun liitettyä lohkoa, siitä tulee **varmistettu siirto**. Lohkoketju on siis yksinkertaisuudessaan loogisesti ajateltuna linkitetty lista **lohkoja** jotka sisältävät siirtoja lompakko-osoitteesta toiseen (Antounoupoulos, 2014, 163). Käytännössä lohkot sisältävät kryptografisen tiivisteen lohkon otsikosta (block header). Lohkon otsikko sisältää aikaleiman, noncen, edellisen lohkon tiivisteen ja **Merkle-puun** juuren avulla luodun tiivisteen kaikista lohkoon liitetyistä siirroista. Valuutan omistaja voi siirtää vastaanottamaansa valuuttaa taas eteenpäin seuraavalle entiteetille muodostaen lohkoketjussa säilytetyn omistajuusketjun. Siirtoja lohkoketjusta tutkimalla voidaan siis päätellä, missä osoitteissa kyseinen virtuaalinen valuutta on minkäkin lohkon kohdalla sijainnut. Kun asiakas on aikaisemmin vastaanottanut lompakkoonsa pörssistä 2 BTC ja maksanut sillä 0.1 BTC maksavat ostokset, rekisteröidään lohkoketjuun käytännössä kolme tapahtumaa. Jokaisessa lohkossa siirrossa on **sisääntuloja** ja **ulostuloja**, jotka määrittävät miten valuuttaa siirtyy eri osoitteiden välillä. Esimerkkitapauksessa sisääntulona olisi siis 2 BTC jotka asiakas on

vastaanottanut pörssistä. Ulostuloina olisi kaksi siirtoa: toinen joka siirtää 0.1 BTC maksuksi supermarketille ja toinen, joka siirtää vaihtorahat eli 1.85 BTC takaisin asiakkaan lompakon osoitteeseen. Tässä vaiheessa on olennaista huomata, että kolmas eli ns. vaihtoraha-tapahtuma luo alkuperäisen maksajan yksityisellä avaimella hallinnoitavan vaihtorahan summan kokoisen ulostulon lohkoketjuun. Tätä ulostuloa voidaan siirron varmennuksen jälkeen käyttää uuden siirron sisääntulona. Edellä mainitussa skenaariossa sisääntulojen ja ulostulojen välinen erotus eli 0.05 BTC menee verkkoa turvaaville ja uusia lohkoja laskeville **louhijoille** siirtokuluna. Siirtokulujen kokoa säätämällä voidaan priorisoida tiettyjä maksuja: isommalla siirtokululla varustetut siirrot lisätään louhittuun lohkoon ennen matalan siirtokulun omaavia siirtoja. (Antonopoulos, 2014, s. 111-134.)

Lohkoketju esittää täysin uuden tavan päästä **konsensukseen**, eli yhteisymmärrykseen tilikirjan tilasta **proof-of-work menetelmän** avulla. Louhiminen on prosessi, jonka avulla uutta valuuttaa luodaan Bitcoinin ekosysteemiin kiertoon. Louhiminen myös turvaa verkkoa lisäämällä siirtoja lohkoihin ja varmentamalla aikaisempia siirtoja. Käytännössä louhijat tarjoavat laskentatehoaan vastineeksi **louhintapalkkioista**. Uusi siirroilla täytetty lohko louhitaan noin kymmenen minuutin välein. Tämä lisää lohkon sisältämät siirrot osaksi lohkoketjua. Louhintapalkkio kostuu lohkojen luomisesta ja siirtokuluista syntyvistä Bitcoineista. Jotta louhija ansaitsee palkkion, joutuu hän kilpailemaan muiden louhijoiden kanssa siitä, kuka löytää ensimmäiseksi vastauksen yksisuuntaisen kryptografisen funktion avulla muodostettuun ongelmaan. Tätä kutsutaan proof-of-work menetelmäksi. Ensimmäiseksi vastauksen ongelmaan löytänyt louhija lähettää lohkonsa Bitcoin-verkkoon, jossa muut käyttäjät varmentavat sen. Tämän jälkeen lohko lisätään osaksi lohkoketjua. Heti tämän jälkeen alkaa kisa siitä, kuka löytää seuraavan lohkon. Jokainen lohko sisältää viitteen edelliseen lohkoon, joten uuden lohkon laskeminen voidaan aloittaa vasta sitten, kun edellinen lohko on lisätty hyväksytysti osaksi lohkoketjua. Louhinnan vaikeus määräytyy **dynaamisen vaikeustason** mukaan siten, että lohkojen luomisen tavoiteaika on noin kymmenen sekuntia. Louhintaprosessi on ekosysteemin kannalta hyvin samankaltainen kuin arvometallien louhinta. Lohkon luomisesta saatava palkkio puolittuu noin neljän vuoden välein (210 000 lohkon keskimääräinen aika) ja loppujen lopuksi louhijoiden palkkio koostuu pelkästään siirtokuluista. Tutkielman kirjoitushetkellä noin 80% kaikista Bitcoineista on jo louhittu. (Antonopoulos, 2014, s. 177 – 214.) Bitcoinissa ja lohkoketjussa käytetyt algoritmit perustuvat monilta osin **yksisuuntaisiin kryptograafisiin funktioihin** ja **digitaalisiin allekirjoituksiin**. Avainten luomisessa käytetty julkisen avaimen salaus ja louhinnassa hyödynnetty proof-of-work algoritmi perustuvat kumpikin yksisuuntaisiin kryptograafisiin funktioihin. Yksisuuntaiset kryptografiset ovat helppoja varmentaa, mutta todella työläitä laskea. (Antonopoulos, 2014, s. 61-76.)

4.1.3 Yhteneväisyydet keskitettyihin menetelmiin

Aikaisemmin tutkielmassa esitelty MicroMint (Rivest & Shamir, 1996) menetelmä sisälsi etäisesti Bitcoinia muistuttavan virtuaalisen valuutan. Se kuitenkin poikkeaa Bitcoinista siten, että MicroMint menetelmässä kolikot ovat digitaalisesti omistajansa hallussa, kun taas Bitcoinissa valuutan omistaja omistaa pelkästään avaimen, joka todistaa omistussuhteen lohkoketjussa sijaitsevaan valuuttaan. Myös Payword (Rivest & Shamir, 1996) menelmässä on samoja piirteitä kuin Bitcoinin lohkoketjussa. Payword-menetelmässä käytetty maksusanaketju on lohkoketjun tavoin linkitetty lista. Lohkoketju on kuitenkin maksusanaketjusta poiketen kaikille julkinen ja yhteinen ketju siirtoja sisältäviä lohkoja. Maksusanaketju on lohkoketjusta poiketen aina kahden tietyn entiteetin välinen väliaikainen siirtoketju.

Yhteneväistä Bitcoinilla sekä Rivestin ja Shamirin (1996) esittämillä keskitetyillä mikromaksumenetelmillä on myös se, että ne perustuivat suurilta osin yksisuuntaisiin kryptograafisiin funktioihin. Yhtenevää lohkoketjussa ja MicroMint -menetelmässä on esimerkiksi se, että kummassakin digitaalista valuuttaa louhitaan ekosysteemiin yksisuuntaisten kryptograafisten funktioiden avulla. Tärkeää on kuitenkin huomioida, että lohkoketjun tapauksessa valuuttaa ei varsinaisesti louhita vaan louhijat louhivat siirtoja sisältäviä lohkoja, jonka oheistuotteena uutta valuutta syntyy. MicroMint -menetelmässä louhinta on täysin luotetun kolmannen osapuolen vastuulla ja se on tapa luoda helposti varmennettavaa virtuaalista valuuttaa.

4.1.4 Lohkoketjulla toteutetut mikromaksut

Bitcoinin yleistyminen viime vuosina on todistanut, että hajautetut tilikirjatekniikat tulevat olemaan olennaisessa osassa tulevaisuuden digitaalisten maksujen kehitystä. Bitcoin ja perinteinen lohkoketju eivät kuitenkaan sovellu itsessään geneeriseksi maksualustaksi, joka pystyisi toimimaan ratkaisuna kaikkien digitaalisten maksujen tarpeille. Vaikka lohkoketju ratkaisee tehokkaasti perinteisten mikromaksujen yhteydessä esiintyvän ylikulutusongelman se ei silti tarjoa ratkaisua esimerkiksi siirtokuluongelmaan protokollatasolla. Jotta mikromaksut voitaisiin käytännössä toteuttaa Bitcoinin avulla, täytyy maksuverkon päälle rakentaa korkeamman tason ratkaisuja, jotka laajentavat sen toiminnallisuutta mikromaksuille suotuisammiksi. Tulevaisuudessa hajautetut tilikirjatekniikat saattavatkin olla helposti toisistaan rajattavien tekniikoiden sijasta monikerroksisia ja sulautuneita protokollapinkkoja.

Pass ja Sheelat (2015) pyrkivät ratkaisemaan siirtokuluongelman toteuttamalla Wheelerin (1996) ja Rivestin (1997) aikaisemmin esittämän odotusarvoihin perustuvan mikromaksumenetelmän Bitcoin -maksuverkon päälle rakennettuna. Tutkimuksessa esitetty ilman luotettua kolmatta osapuolta toimiva menetelmä ei kuitenkaan sovellu nykyisen Bitcoin-protokollan päälle ilman siihen tehtäviä muutoksia. Esitetty menetelmä olisi kuitenkin mahdollista toteuttaa esimerkiksi älysopimusten ja Ethereum (2014) verkon avulla suoraan protokollatasolla ilman korkeamman tason ratkaisuja. Tutkimuksessa esitetään

myös kaksi muuta Bitcoin-verkon päälle toteutettavaa menetelmää, jotka kuitenkin tarvitsevat toimiakseen luotetun kolmannen osapuolen. (Pass & Sheelat, 2015.) Myös Chiesa ym. (2017) esittävät menetelmän joka hyödyntää Wheelerin (1996) ja Rivestin (1997) aikaisempaa työtä odotusarvollisista mikromaksuista. Tutkimuksessa esiteltävät menetelmät ovat *hajautettuja anonyymejä mikromaksumenetelmiä*. (Chiesa ym. 2017). Anonyymin mikromaksuista tekee zk-SNARK eli zero knowledge proof menetelmä. Käytännössä zk-SNARKeilla voidaan todistaa, että jokin tieto on todistajan hallussa ilman tiedon paljastamista tai todistajan ja varmentajan keskinäistä vuorovaikutusta. (Zerocash, 2014).

4.2 Uuden sukupolven hajautetut tilikirjatekniikat

Mikromaksujen toteuttaminen perinteisen lohkoketjun ja Bitcoinin avulla on hajautetusta luonteesta riippumatta hankalaa ja epäkäytännöllistä. Bitcoin ei mahdollista esimerkiksi komplekseja monivaiheisia siirtoja suoraan protokollatasolla ja se tekee erilaisten mikromaksumenetelmien toteuttamisesta käytännössä mahdotonta ilman korkeamman tason ratkaisuja. Viime vuosien aikana Bitcoinin kanssa kilpailemaan on noussut myös useita muita kehittyneempiä kryptovaluuttoja jotka pyrkivät ratkaisemaan perinteisen lohkoketjun heikkouksia tai laajentamaan sen toimintaa suoraan protokollatasolla. Tutkielmassa näitä tekniikoita kutsutaan **uuden sukupolven hajautetuiksi tilikirjatekniikoiksi**. Tässä tutkielmassa käsitellään kahta uuden sukupolven tekniikkaa: älysopimusalusta Ethereum (Buterin, 2014) ja Tangle (Popov, 2017).

Nämä uuden sukupolven hajautetut tilikirjatekniikat ovat kykeneväisiä suorittamaan mikromaksuja suoraan protokollatasolla. Ethereum-verkon avulla mikromaksut voidaan toteuttaa hajautetusti Ethereumin virtuaalikoneen ja siinä ajettavien älysopimusten avulla. (Pass & Sheelat, 2017). Käytännössä Ethereum laajentaa lohkoketjun toimintaa tarjoamalla alustan monimutkaisemman logiikan suorittamiseksi lohkoketjun päällä. Tanglen avulla mikromaksut voidaan suorittaa vaivattomasti suoraan protokollatasolla koska maksuverkko itsessään mahdollistaa täysin kuluttomien siirtojen tekemisen. (Popov, 2017).

4.2.1 Ethereum ja älysopimukset

Älysopimus on käsitteenä vanha ja ensimmäisiä kertoja se esiintyi tieteellisessä kirjallisuudessa jo viime vuosituhannella Szabo:n (1997) esittelemänä. Älysopimus sisältää ennalta määrättyjä sääntöjä, jotka voidaan vahvistaa luotettavasti ja digitaalisesti. Älysopimuksia ei olla kuitenkaan onnistuttu tehokkaasti toteuttamaan käytännössä ennen vuotta 2014. Buterin (2014) esittelemä Ethereum-verkko hyödyntää lohkoketjua, johon on sisäänrakennettuna Turing-täydellinen virtuaalikone. Ethereum –verkkoa kehittää Ethereum Foundation. (Ethereum Foundation, 2017). Aluksi Ethereumin virtuaalikonetta piti ohjelmoida matalan tason EVM-koodilla, mutta myöhempien päivitysten yhteydessä

Ethereumiin lisättiin mahdollisuus ohjelmoida älysopimuksia korkeamman tason kielellä Solidityllä.

Ethereum-verkko ja EVM toimivat alustana usealle eri verkon päällä ajettavalle sovellutukselle. Tänä päivänä yleisin käyttötapaus verkolle on uuden kryptovaluutan luominen. Älysopimukset ovat kyvykkäitä myös moneen muuhun käyttöön. Esimerkiksi monia liiketoimintaan ja siihen liittyvään vuorovaikuttamiseen liittyviä perinteisiä prosesseja voitaisiin automatisoida ja hajauttaa älysopimusten avulla. Älysopimukset ovat perinteisiä sopimuksia parempia, koska ne ovat luottovapaita ja kaikkien osapuolten auditoitavissa, milloin tahansa. Kun älysopimus otetaan käyttöön, jokainen sopimusta hyödyntävä osapuoli hyväksyy ne ehdot, jotka älysopimukseen on määritetty sen luomisen yhteydessä. Älysopimusta ajava virtuaalikone valvoo, että älysopimuksen ohjelmointikoodin mukaisia ehtoja noudatetaan. Ethereum-verkon ja älysopimusten yhteydessä *koodi on laki*. Tämä on ongelmallista tapauksissa, jos ohjelmoijan tekemä virhe koodissa saa älysopimuksen toimimaan oletetusta poikkeavasti. Koska älysopimusta ei voida muuttaa enää sen käynnistämisen jälkeen, täytyy ohjelmointikoodi auditoida erityisen hyvin sen kehitysvaiheessa ennen sen käyttöönottoa.

4.2.2 IOTA ja Tangle

Vuonna 2015 käynnistetty IOTA -verkko on esineiden internetin resurssiniukoille laitteille suunniteltu maksuverkko. Muista kryptovaluutoista poiketen IOTA -verkossa siirretyt maksut eivät sisällä ollenkaan siirtokuluja. Tämä tekee IOTA:sta kyvykkään mikromaksujen suorittamiseksi suoraan protokollatasolla ilman korkeamman tason ratkaisuja. IOTA verkkoa kehittää IOTA Foundation. IOTA:n kehittäjien tulevaisuuden tavoitteena on upottaa maksuverkon toiminnallisuus yksinkertaiseen mikropiiriin, joka voidaan sulauttaa osaksi havainnointitason älykkäitä esineitä. Tutkielman kirjoitusaikana Tangle on ollut toiminnassa noin kaksi vuotta ja sen toiminnallisuutta pystyy jo nyt sulauttamaan osaksi niitä älykkäitä esineitä, jotka ovat kyvykkäitä ajamaan tarjottua Javascript -kirjastoa. (IOTA Foundation, 2017.)

IOTA:n ja kuluttomat hajautetut siirrot mahdollistava uusi tekniikka on Tangle, joka lohkoketjun tavoin toimii julkisena tilikirjana. Tangle on DAG eli suunnattu syklitön verkko joka sisältää siirtoja jotka varmistavat aikaisempia siirtoja verkossa. Jokainen verkkoon lähetetty siirto tekee pienen määrän työtä proof of work -menetelmällä ja varmistaa kaksi aikaisempaa siirtoa. Tällä tavalla siirron lähettäjä käytännössä maksaa omat siirtokulut pienellä määrällä laskentaa ja samalla varmentaa muita verkkoon lähetettyjä maksuja. Tämä menetelmä turvaa verkon ilman louhijoita, poistaen ne kokonaan IOTA:n ekosysteemistä. Usein proof of work menetelmän vaatima laskenta kuitenkin suoritetaan resurssiniukan älykkään esineen sijasta erillisellä reitittimenä toimivana palvelimella, joka toimii solmuna IOTA verkon ja älykkäiden esineiden välillä. Tanglesta tulee nopeampi ja turvallisempi mitä enemmän maksuverkko käsittelee siirtoja. Toisin sanoen Tangle on skaalautuva ja se hyötyy esineiden internetin kasvavasta laitemäärästä. (Popov, 2017.)

5 HAJAUTETUT MIKROMAKSUT ESINEIDEN INTERNETISSÄ

Tulevaisuudessa ihmisen ja älykkäiden esineiden välinen vuorovaikutus ja maksuliikenne saattavat olla osa jokapäiväistä arkeamme. Esineiden internetin infrastruktuuri kuten LPWAN verkot ovat kasvaneet paikoittain jo kokonaisia kaupunkeja kattaviksi. Sitä mukaa kun esineiden internetin infrastruktuuri ja ekosysteemi kehittyvät helpottuvat myös ratkaisuiden suunnittelutyö ja käytännön toteutus. Erilaiset mikromaksuja ja esineiden internetiä hyödyntävät ratkaisut saattavat tuoda suuriakin kustannussäästöjä useilla eri liiketoimintasektoreilla esimerkiksi parantamalla aikaisempia liiketoimintamalleja ja niihin liittyviä prosesseja. Myös hajautetut maksuverkot yleistyvät ja niiden ekosysteemit kehittyvät siten, että niiden käyttämä maksuvaluutta on päivä päivältä helpommin saatavilla myös normaalille, teknisesti osaamattomalle maallikolle. Mitä enemmän hajautettuja maksuverkkoja hyödyntäviä sovellutuksia otetaan käyttöön, sitä enemmän niiden käyttämälle valuutalle on tarvetta. Käytännön sovellutusten yleistyminen siis luo tarpeen uusille, helpoille tavoille vaihtaa fiat-valuuttaa näiden sovellutusten käyttämään digitaaliseen valuuttaan.

Tutkielman viimeisessä yhteenvetoluvussa tarkastellaan mikromaksuja ja hajautettuja tilikirjatekniikoita esineiden internetin kontekstissa. Aluksi pyritään selvittämään, minkälaisia vertikaalisia markkinoita esineiden internetissä on ja kuinka arvokkaita ne tulevaisuudessa saattavat olla. Lopuksi tarkastellaan hajautetun tilikirjan sisältävän maksuverkon sulauttamista osaksi esineiden internetiä IOTA-maksuverkkoa hyödyntävän käytännön sovellutuksen kautta. Tässä vaiheessa hyödyksi käytetään aikaisemmin tutkielmassa käsiteltyä esineiden internetin arkkitehtuurin viisitasomallia. Esitellyssä käyttötapauksessa parannetaan perinteisen parkkitalon toimintaprosesseja ja maksuliikennettä esineiden internetin tekniikoiden, hajautettujen maksuverkkojen ja mikromaksujen avulla.

5.1 Mikromaksut tulevaisuuden vertikaalisilla markkinoilla

Esineiden internetin havainnointikerroksella sijaitsevat älykkäät laitteet suorittavat yleensä tehtäviä jollekin **vertikaaliselle markkinalle**. Vertikaalisella markkinalla tarkoitetaan jotain käyttötapauksesta riippuvaa sovellutusta kuten älykästä logistiikkaa, älykästä maanviljelyä tai älykästä terveydenhuoltoa. (Khan ym., 2012.) On arvioitu, että vertikaalisten markkinoiden yhteenlaskettu arvo vuonna 2025 on noin 2.6 – 6.2 triljoonaa Yhdysvaltojen dollaria. (McKinsley, 2013) Tulevaisuuden arvokkaimmat markkinat ovat arvion mukaan terveydenhuolto ja tuotantotekniikka (taulukko 1).

TAULUKKO 1: Esineiden internetin vertikaaliset markkinat 2025

Markkina	**Arvo (miljardia USD)**	**Prosentuaalinen osuus**
Terveydenhuolto	1100 – 2500	41%
Tuotantotekniikka	900 – 2300	33%
Sähkö	200 – 500	7 %
Älykaupunki	100 – 300	4 %
Turvallisuus	100 – 200	4 %
Luonnonvarojen jalostus	100 – 200	4 %
Maanviljely	noin 100	4 %
Vähittäiskauppa	20 – 100	1 %
Logistiikka	noin 5	2 %
YHTEENSÄ	**2625 - 6205**	100 %

Arvion mukaan tulevaisuuden esineiden internetin suurin markkinaosuus olisi sellaisissa vertikaalisissa markkinoissa, jotka eivät varsinaisesti hyödy mikromaksuista. Mikromaksuja voidaan kuitenkin hyödyntää esimerkiksi älykkään sähkön tai älykaupungin kontekstissa useassa eri käytössä. Nämä kaksi markkinaa ovat arvion mukaan tulevaisuudessa markkina-arvoltaan jopa 800 miljardia dollaria ja vievät yhdessä noin 11% kaikkien vertikaalisten markkinoiden kokonaisarvosta. Edistys aurinkopaneeli- ja akkuteknologiassa on mahdollistanut sen, että yksityishenkilö voi tuottaa esimerkiksi omakotitalonsa kattotiilten avulla sähköä omaan käyttöönsä. Tulevaisuudessa hajautettu tilikirja ja mikromaksut mahdollistavat myös ylimääräisen sähkön myymisen takaisin sähköverkkoon muiden käytettäväksi ilman monimutkaisia liiketoimintasuhteita. Älykaupungissa mikromaksuilla on useita eri käyttötapauksia. Esimerkiksi tietullit ja parkkimaksut voitaisiin suorittaa tehokkaasti hajautetun tilikirjan ja mikromaksujen avulla. Myös älykkäiden esineiden ja sensoreiden keräämällä datalla on itseisarvoa ja sitä voidaan myydä eteenpäin muiden hyödynnettäväksi. Hajautetut maksuverkot ja mikromaksut tekevät mahdolliseksi sen, että sensoridatasta kiinnostunut kolmas osapuoli voi helposti ostaa yhden tai useamman sensorin keräämää dataa sekä maksaa siitä käytön mukaan ja reaaliaikaisesti mikromaksujen avulla.

5.2 Hajautettu mikromaksuverkko esineiden internetissä

Hajautetun tilikirjan sisältävän maksuverkon sulauttamista osaksi esineiden internetiä tarkastellaan tässä luvussa teoreettisesti älykaupungin parkkihallisovellutuksen kautta. Tässä toteutuksessa ei oteta tarkasti kantaa varsinaiseen tekniseen toteutukseen esimerkkitekniikoiden ulkopuolella, vaan asiaa käsitellään korkeammalla tasolla konseptin ja kokonaisarkkitehtuurin näkökulmasta.

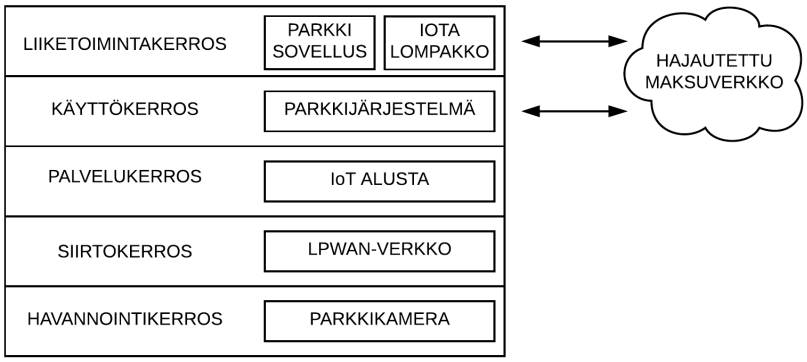
Esitetty älyparkkihallin konsepti on toteutettavissa tänä päivänä saatavilla olevien teknisten ratkaisuiden, kuten LPWAN verkon, konenäön ja hajautetun IOTA –maksuverkon avulla. Tässä luvussa esitetyt tekniikat mahdollistavat tarvittavan toiminnallisuuden, mutta niitä voidaan tarvittaessa muuttaa esimerkiksi silloin, kun LPWAN verkon kantavuutta ei ole saatavilla. Tässä tapauksessa siirtokerroksella käytetyksi tekniikaksi voitaisiin vaihtaa esimerkiksi jokin mobiiliverkko. Älyparkkihallin konseptiin tutustutaan aluksi korkealla tasolla asiakkaana toimivan loppukäyttäjän näkökulmasta. Seuraavaksi tarkastellaan, miten parkkihallisovellutuksen toteutuksen palaset sulautuvat yhteen esineiden internetin viisitasomallin mukaisen arkkitehtuurimallin kanssa.

5.2.1 Älykkään parkkihallin konsepti

Kun älykästä parkkihallia hyödyntävä asiakas haluaa parkkeerata autonsa, täytyy hänen ensin ladata parkkihallin mikromaksutoiminnan mahdollistava sovellus älypuhelimeensa. Tähän sovellukseen tehdään tili ja siihen liitetään parkkeerattavan auton rekisteritunnus. Sovellus sisältää myös lompakko-osoitteen, johon IOTA valuuttaa voidaan ladata parkkimaksuja varten. Kun käyttäjätiliin liitetty auto ajaa parkkihalliin sisään, tunnistetaan kameran ja konenäön avulla auton rekisterikilpi. Jos rekisteritunnukseen liitetyllä tilillä on valuuttaa parkkimaksusovelluksessa, päästetään auto sisään parkkihalliin. Kun auto tulee parkkihalliin sisälle, alkaa parkkijärjestelmä ottaa maksua asiakkaan parkkisovelluksen lompakosta esimerkiksi viiden sekunnin välein. Tätä jatketaan, kunnes konenäkö tunnistaa oikean rekisterikilven parkkihallista poistuvasta autosta. Jos tilillä ei ollut tarpeeksi rahaa ja se on mennyt miinukselle parkkihallista ulos pyrkiessä, ei puomi päästä autoa ulos parkkihallista. Puomi aukeaa vasta sitten kun parkkisovelluksen lompakkoon on ladattu lisää valuuttaa ja sen saldo on positiivinen.

5.2.2 Älykkään parkkihallin kokonaisarkkitehtuuri

Edellisessä luvussa esitelty konsepti koostuu käytännössä parannetusta perinteisen parkkihallin liiketoimintamallista ja sen mahdollistavista teknisistä komponenteista. Älykkään parkkihallin toiminnan mahdollistavat komponentit voidaan asettaa esineiden internetin viisitasomalliin eri kerroksille. Seuraavassa kuviossa (kuvio 3) esitetään älykkään parkkihallisovellutuksen korkean tason arkkitehtuuri peilattuna esineiden internetin viisitasomallia vasten.



Kuvio 3: Parkkisovellutuksen komponentit viisitasomallissa

Alimpana kokonaisarkkitehtuurissa on havainnointikerros, joka sisältää parkkihallissa sijaitsevan kameran, jonka tehtävänä on lukea autojen rekisterikilpiä konenäön avulla. Tieto tunnistetuista rekisterikilvistä voidaan siirtää esimerkiksi LPWAN –verkon avulla IoT-alustaan, joka sisältää tiedon prosessointiin ja varastoimiseen liittyvät komponentit. IoT alusta tarjoaa rekisterikilpitietoja helppokäyttöisen rajapinnan kautta parkkijärjestelmään, joka sisältää tarvittavan sovelluslogiikan. Parkkijärjestelmän tehtävänä on myös olla yhteydessä hajautettuun maksuverkkoon sekä avata ja hallinnoida asiakkaan ja parkkihallia ylläpitävän entiteetin välisiä mikromaksukanavia ja niissä tapahtuvia siirtoja. Järjestelmän loppukäyttäjälle rajapintana parkkijärjestelmään ja hajautetussa maksuverkossa sijaitsevaan parkkimaksutiliin toimii liiketoimintakerroksella sijaitseva helppokäyttöinen parkkisovellus. Asiakkaan älypuhelin saattaa myös sisältää IOTA lompakon, josta valuuttaa voidaan ladata parkkisovelluksen tarjoaman osoitteen kautta parkkimaksutilille. Myös parkkihallin ylläpitäjä pääsee parkkisovelluksen avulla käsiksi kerättyihin maksuihin sekä liiketoiminnan strategisia päätöksiä hyödyntävään analysoituun dataan esimerkiksi erilaisten raporttien avulla. Tällä tavalla toteutettuna kaikki maksuliikenne toimii parkkijärjestelmästä erotetusta hajautetussa ja universaalissa maksuverkossa, jota kuitenkin hyödynnetään olennaisena osana parkkijärjestelmän toiminnallisuutta.

5.3 Yhteenveto ja jatkotutkimusaiheet

Mikromaksulla tarkoitetaan summaltaan vähäarvoista digitaalista maksua. Mikromaksuja ollaan yritetty toteuttaa käytännössä jo pitkän aikaa keskitettyjen mikromaksumenetelmien avulla, mutta niiden keskitetystä luonteesta ja siitä aiheutuvista ongelmista johtuen niitä ei ole otettu laajamittaisesti käyttöön. Keskitetyissä mikromaksumenetelmissä ongelmia aiheuttaa luotetun kolmannen osapuolen rooli maksuverkon ja siirtojen hallinnassa. Keskitetyt mikromaksumenetelmät pyrkivät ratkaisemaan osittain näitä ongelmia, mutta usein yhden ongelman ratkaiseminen aiheuttaa uusien ongelmien ilmaantumisen.

Hajautetut tilikirjatekniikat ja niiden avulla toteutetut hajautetut maksuverkot mahdollistavat hajautettujen digitaalisten maksujen toteuttamisen ilman luotettua kolmatta osapuolta. Kaikki hajautetut maksuverkot eivät kuitenkaan

itsessään sovellu mikromaksujen toteuttamiseen. Bitcoinin ja perinteinen lohkoketjun avulla mikromaksuja ei voida toteuttaa ilman monimutkaisia korkean tason ratkaisuja. Ethereum-verkon ja älysopimusten avulla mikromaksut voidaan toteuttaa soveltamalla perinteisiä mikromaksumenetelmiä ja toteuttamalla ne hajautetusti lohkoketjun päällä. IOTA-verkko mahdollistaa siirtokuluttomien ja hajautettujen mikromaksujen toteuttamisen suoraan protokollatasolla. Erilaisia hajautettuja maksuverkkoja on tänä päivänä useita, ja tutkielmassa ei käsitellä tarkemmin muuta kuin kolme edellä mainittua maksuverkkoa. Jatkotutkimusta olisi hyvä tehdä myös sen suhteen, että mikä hajautettu tilikirjatekniikka on mikromaksuille suotuisin. Tällä hetkellä vaikuttaa siltä, että Tanglen tyyliset DAG –tietorakenteet ovat siirtokuluttomuuden takia mikromaksujen toteutukseen lohkoketjua suotuisampia tekniikoita.

Esineiden internetiä voidaan järjestelmällisesti mallintaa loogisten rakennemallien avulla. Yleisimmin käytettyjä malleja ovat esineiden internetin kokonaisarkkitehtuuria kuvaavat kolmi- ja viisitasomallit. Viisitasomalli on näistä kahdesta kehittyneempi. Viisitasomalli jakaa älykkäät laitteet, tiedonsiirtoverkot, dataa prosessoivat palvelut, sovelluslogiikan sekä liiketoimintamallit toisistaan erotettaville kerroksille. Mikromaksut mahdollistavat hajautetut maksuverkot asettuvat rinnakkain viisitasomallin kahden ylimmän kerroksen: käyttökerroksen ja liiketoimintakerroksen kanssa. Aiheesta olisi hedelmällistä suorittaa jatkotutkimusta: tämän tutkimuksen johtopäätökset perustuvat hajautettujen tilikirjatekniikoiden tämän hetkiseen toiminnallisuuteen ja toteutuksiin. Kun tulevaisuudessa nämä tekniikat kehittyvät, saattaa hajautetun maksuverkon toiminnallisuus siirtyä arkkitehtuurimallien alemmille kerroksille. Tulevaisuudessa hajautettujen maksuverkkojen toiminnallisuus saattaa olla esimerkiksi sulautettuna suoraan havainnointikerroksella sijaitseviin älykkäisiin esineisiin.

Tulevaisuudessa esineiden internetin vertikaaliset markkinat, joissa mikromaksuja voidaan hyödyntää, saattavat olla jopa 800 miljardin dollarin arvoiset. Hajautettuja mikromaksuja ei ole kuitenkaan vielä hyödynnetty laajamittaisesti esineiden internetissä. Hajautettujen maksuverkkojen ekosysteemit kehittyvät kovaa vauhtia ja se osaltaan helpottaa niiden avulla tehtyjen ratkaisujen toteutusta ja universaalia käyttöönottoa. Hajautetut maksuverkot ovat vielä suhteellisen tuore keksintö ja tässä vaiheessa onkin vaikea arvioida, mitkä tekniikat otetaan laajamittaisimmin käyttöön. Tämä aiheuttaa omat haasteensa näitä tekniikoita hyödyntäville sovelluskehittäjille. Kokonaisuudessaan hajautetut maksuverkot kuitenkin tarjoavat luottovapaan, universaalin ja helposti käyttöönotettavan tavan toteuttaa mikromaksuja hyödyntäviä ratkaisuja esineiden internetissä. Kaikki tarvittavat työkalut hajautettujen mikromaksujen toteuttamista varten ovat saatavilla jo tänä päivänä.

LÄHTEET

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015). *Internet of things: A survey on enabling technologies, protocols, and applications.* IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

Antonopoulos, A. M. (2015). *Mastering bitcoin: Unlocking digital cryptocurrencies* (1. ed.). O'Reilly.

Atzori, L., Lera, A., & Morabito, G. (2010). *The internet of things: A survey.* Computer networks, 54(15), 2787-2805.

Bitcoin.org. (2017). *Bitcoin: Innovative payment network and a new kind of money*. Haettu osoitteesta www.bitcoin.org

Buterin, V. (2014). *A next generation smart contract & decentralized application platform.*

Chiesa, A., Green, M., Liu, J., Miao, P., Miers, I., & Mishra, P. (2017). *Decentralized Anonymous Micropayments.* International Conference on the Theory and Applications of Cryptographic Techniques (pp. 609-642). Springer, Cham.

Ethereum foundation. (2017). *Ethereum Foundation.* Haettu osoitteesta https://www.ethereum.org/foundation

Kortuem, G., Kawsar, F., Sundramoorthy, V., & Fitton, D. (2010). *Smart objects as building blocks for the internet of things.* IEEE Internet Computing, 14(1), 44-51.

International Telecommunication Union (2015). *Measuring the information society report.* Haettu osoitteesta http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

IOTA foundation. (2017). *IOTA Foundation.* Haettu osoitteesta https://iotasupport.com/foundation.shtml

Jarecki, S., & Odlyzko, A. (1997). *An efficient micropayment system based on probabilistic polling.* In Financial Cryptography (pp. 173-191). Springer Berlin/Heidelberg.

Kytöjoki, J., & Kärpijoki, V. (2000). *Micropayments-Requirements and solutions.* In Helsinki University of Technology Seminar on Network Security 1999.

Lipton, R. J., & Ostrovsky, R. (1998). *Micro-payments via efficient coin-flipping.* In International Conference on Financial Cryptography (pp. 1-15). Springer, Berlin, Heidelberg.

McKinsey. (2013). *Disruptive technologies May 2013.*

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). *Internet of things: Vision, applications and research challenges.* Ad Hoc Networks, 10(7), 1497-1516.

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

Pass, R. (2015, October). *Micropayments for decentralized currencies.* In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 207-218). ACM.

Popov, S. (2016). *The tangle.*

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). *Future internet: the internet of things architecture, possible applications and key challenges*. In Frontiers of Information Technology (FIT), 2012 10th International Conference on (pp. 257-260). IEEE.

Rivest, R. L. (1997). *Electronic lottery tickets as micropayments.* In International Conference on Financial Cryptography (pp. 307-314). Springer, Berlin, Heidelberg.

Rivest, R. L., & Shamir, A. (1996). *PayWord and MicroMint: Two simple micropayment schemes.* In International Workshop on Security Protocols (pp. 69-87). Springer, Berlin, Heidelberg.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). *Zerocash: Decentralized anonymous payments from bitcoin*. In Security and Privacy (SP), 2014 IEEE Symposium on (pp. 459-474). IEEE.

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

Wheeler, D. (1996). *Transactions using bets*. In International Workshop on Security Protocols (pp. 89-92). Springer, Berlin, Heidelberg.

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). *Research on the architecture of Internet of things.* In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on (Vol. 5, pp. V5-484). IEEE.

Zhong, C. L., Zhu, Z., & Huang, R. G. (2015, August). Study on the IOT architecture and gateway technology. In Distributed Computing and Applications for Business Engineering and Science (DCABES), 2015 14th International Symposium on (pp. 196-199). IEEE.