Karri Hakala

LOHKOKETJUTEKNOLOGIA KOHDENNETUSSA VERKKOMAINONNASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Hakala, Karri
Lohkoketjuteknologia kohdennetussa verkkomainonnassa
Jyväskylä: Jyväskylän yliopisto, 2020, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Clements, Kati

Niin lohkoketjuteknologia kuin kohdennettu verkkomainonta ovat hyvin ajankohtaisia aiheita. Lähes kaikki verkossa oleva mainonta on kohdennettua mainosten ollessa elinehto monelle nykyiselle palvelulle; lohkoketjuteknologian kuitenkin ennustetaan muuttavan nykyiset liiketoimintamallit. Kirjallisuuskatsauksena toteutetun tutkielman tavoitteena on tunnistaa, miten lohkoketjuteknologiaa voitaisiin hyödyntää kohdennetussa verkkomainonnassa. Tutkimuskysymykseksi muodostettiin: ”Miten lohko-ketjuteknologian avulla voidaan ratkaista kohdennetun verkkomainonnan haasteita?” Kirjallisuuskatsauksen perusteella lohkoketjuteknologia voisi tarjota ratkaisuja useisiin kohdennetun verkkomainonnan haasteisiin. Lohkoketjuteknologian hyödyntäminen voisi korjata ongelmia käyttäjien tunnistautumisessa poistaen verkkomainonnalle ongelmallisen keinotekoisen liikenteen aiheuttamat kuluja. Lohkoketjuteknologia voisi poistaa kolmansia osapuolia tehden mainonnasta tehokkaampaa yrityksille vähentäen turhia osapuolia. Kolmansien osapuolten vähentyminen voisi palauttaa yksityisyyden tunnetta kuluttajille, mikä on oleellista mainonnan toimivuuden kannalta. Lisäksi lainsäädäntö olisi mahdollista ohjelmoida suoraan lohkoketjuun. Lohkoketjupohjaisia korvaajia nykyisille järjestelmille ei ole kuitenkaan vielä onnistuttu toteuttamaan. Suurimpia ongelmia aiheuttaa järjestelmien skaalautuvuus tarpeeksi suuriksi, sekä lisäksi lainsäädäntö lohkoketjuteknologian ympärillä on vielä sekavaa. Nykyiset lohkoketjuteknologiaan perustuvat järjestelmät ovat siis vielä riittämättömiä, mutta niissä uskotaan olevan potentiaalia.

Asiasanat: kohdennettu verkkomainonta, lohkoketjuteknologia, blockchain

ABSTRACT

Hakala, Karri
Blockchain technology in targeted online advertising
Jyväskylä: University of Jyväskylä, 2020, 27 p.
Information Systems Science, Bachelor's Thesis
Supervisor: Clements, Kati

Both blockchain technology and targeted online advertising are very topical issues. Almost all online advertising is targeted, with ads being the lifeblood of many existing services; however, blockchain technology is projected to change current business models. The aim of this literature review is to identify how blockchain technology could be used in targeted online advertising. The research question was: "How can blockchain technology solve the challenges of targeted online advertising?" Based on the literature review, blockchain technology could provide solutions to many of the challenges of targeted online advertising. Utilizing blockchain technology could solve problems in user identification and eliminate ad fraud saving money in online advertising budgets. Blockchain technology could eliminate third parties, making advertising more effective for businesses, reducing unnecessary parties. A reduction in third parties could restore the feeling of privacy to consumers, which is essential for the effectiveness of advertising. In addition, legislation could be programmed directly into the blockchain. However, large enough blockchain-based substitutes for existing systems have not yet been implemented. The biggest problems are caused by the scalability of the systems, and the legislation around blockchain technology is still confusing. Existing blockchain-based systems are thus still inadequate but are believed to have potential.

Keywords: targeted online advertising, blockchain technology, blockchain

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tämä tutkielma käsittelee lohkoketjuteknologian mahdollisuuksia kohdennetussa verkkomainonnassa, sen mahdollisia hyötyjä ja ongelmia. Niin lohkoketjuteknologia kuin kohdennettu verkkomainonta ovat aiheina hyvin ajankohtaisia ja herättävät paljon keskustelua niiden roolista nyt ja tulevaisuudessa. Lohkoketjuteknologian ennustetaan mullistavan ihmisten tavan toimia kaikilla aloilla ja olevan tärkein keksintö sitten internetin (Tapscott & Tapscott, 2016). Sen ennustetaan poistavan turhat kolmannet osapuolet ja takaavan datan turvallisuus, oikeellisuus ja yksityisyys (Swan, 2015). Kohdennetun mainonnan on tutkittu olevan huomattavasti tehokkaampaa kuin kohdentamattoman, mutta vain kun kuluttajalla on tunne yksityisyytensä säilymisestä (Tucker, 2014). Kun kuluttajat huomaavat, että heidän henkilökohtaista dataansa seurataan ja analysoidaan ilman heidän suostumustaan, aiheuttaa se selkeän laskun mainonnan tehokkuudessa (Aguirre, Mahr, Grewal, de Ruyter & Wetzels, 2015). Kohdennetun verkkomainonnan eettisyyttä ja ihmisten yksityisyyden loukkaamista kritisoidaankin runsaasti. Tutkielman tavoitteena on tunnistaa, miten lohkoketjuteknologiaa voitaisiin hyödyntää kohdennetussa verkkomainonnassa. Tämän pohjalta muodostettiin tutkimuskysymys:

- Miten lohkoketjuteknologian avulla voidaan ratkaista kohdennetun verkkomainonnan haasteita?

Tietojärjestelmätieteen opiskelijalle aihe on erittäin osuva tähänastisiin opiskeluihin nähden, jotka ovat sisältäneet kursseja niin markkinoinnista, uusista teknologioista kuin tietokannoistakin, eli juuri niistä aiheista, joita tämä tutkielma käsittelee. Tutkielman tarkoituksena on löytää jatkotutkimusta vaativia aiheita sekä auttaa organisaatioita tunnistamaan lohkoketjuteknologian mahdollisuuksia. Tutkielmasta tekee tärkeän se, kuinka siinä tutkitaan aihetta, joka vaikuttaa kaikkiin verkkoselaimia ja älylaitteita käyttäviin ihmisiin.

Tutkielma on toteutettu kirjallisuuskatsauksena. Lähdekirjallisuudeksi pyrittiin valitsemaan mahdollisimman ajankohtaisia lähteitä tietojärjestelmätieteen, kauppatieteiden ja tietotekniikan alalta. Lähdekirjallisuutta on haettu Google Scholar, JYKDOK ja Scopus -palveluista. Joitain lähteitä on haettu myös

Googlen normaalilla hakukoneella aiheiden uutuudesta johtuvan vähäisen tutkimuksen vuoksi tukemaan vertaisarvioutuja tieteellisiä lähteitä. Tärkeimpiä hakusanoja ovat olleet: ”digital advertising”, “online advertising”, ”targeted advertising” sekä ”blockchain”.

Tutkielma rakentuu viidestä luvusta. Johdantoluvun jälkeen toinen luku esittelee kohdennettua verkkomainontaa ja kolmas luku lohkoketjuteknologiaa. Neljännessä luvussa vastataan tutkimuskysymykseen ja esitellään lohkoketjuteknologian mahdollisuuksia kohdennetussa verkkomainonnassa. Viides luku on yhteenveto, jossa esitetään myös ideoita jatkotutkimukselle.

2 KOHDENNETTU VERKKOMAINONTA

Ensimmäiset kohdennetun verkkomainonnan toteutukset tapahtuivat 1990-luvun lopussa, mutta eivät menestyneet internetin käyttäjien vähäisyyden, laitteiden rajallisuuden ja heikkojen siirtonopeuksien vuoksi (Schlee, 2013 s. 61). Nämä ongelmat ovat kuitenkin väistyneet ja verkkomainonta on vuonna 2019 maailmanlaajuisesti yli kolmensadan miljardin dollarin bisnes ja verkkomainonnan osuus kattaa jo noin puolet kaikesta mainontaan käytettävästä rahasta (Enberg, 2019). Esimerkiksi Yhdysvalloissa verkossa tapahtuvaan mainontaan käytettävät summat ovat jatkaneet nousuaan koko 2010-luvun ajan vuosittain vähintään 15% (PwC, 2019). Verkkomainonnassa on kaksi suurta hallitsijaa; Google yli sadan miljardin dollarin osuudella ja Facebook lähes seitsemänkymmenen miljardin dollarin osuudella (Enberg, 2019). Tässä luvussa määritellään mitä kohdennettu verkkomainonta on sekä mitkä ovat sen vahvuudet ja haasteet.

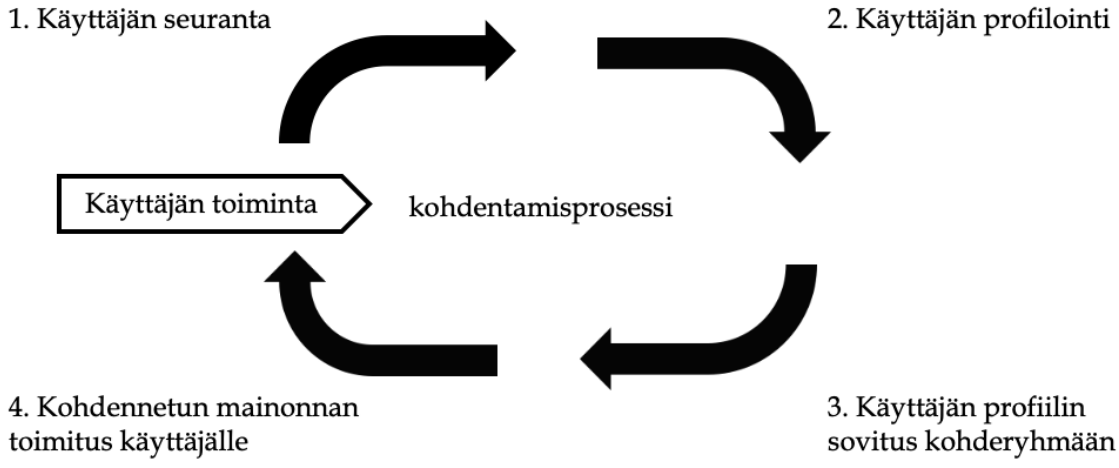
2.1 Kohdennetun verkkomainonnan määritelmä

Kohdennettu verkkomainonta on verkossa tapahtuvaa mainontaa, joka kohdennetaan käyttäjälle esimerkiksi sijainnin, iän, vuorokauden ajan, selaushistorian tai niiden yhdistelmien perusteella (Plummer, Rappaport, Hall & Barocci, 2007 s. 8-9, 17). Tämänkaltaista mainontaa kohtaa muun muassa nettisivuilla, sosiaalisen median palveluissa ja mobiilisovelluksissa olevissa mainoksissa. Kohdennetulla mainonnalla pyritään tunnistamaan käyttäjien ominaisuuksia sekä mielenkiinnon kohteita ja sitä kautta vastaamaan heidän tarpeisiin ja haluihin paremmin (Schlee, 2013 s. 9).

Mainonnan kohdentamiseen on alustoista ja yrityksistä riippuen erilaisia käytännön toteutuksia, mutta perusperiaatteet ovat samat. Murthi ja Sakar (2003) määrittelevät kohdentamisprosessiin kolme vaihetta: oppiminen, sovitus ja arviointi. Oppimisvaiheessa yritys kerää tietoa käyttäjästä selvittääkseen hänen tarpeitaan ja mielenkiinnon kohteita. Sovitusvaiheessa tätä tietoa sovitetaan kohdennettuun sisältöön, jotta se olisi mahdollisimman tehokasta ja osuvaa.

Lopuksi arvioidaan kohdennuksen tehokkuutta ja tämä voidaan tehdä esimerkiksi seuraamalla mainokseen kohdistuneiden klikkausten määrää. Myös Schlee (2013 s. 10-11) kuvaa mainostamisen kohdentamisprosessia vaiheittain mutta tarkemmin ja nimenomaan verkkoympäristössä (kuvio 1). Schleen (2013, s 10-11) mukaan käyttäjän toiminta johtaa neljävaiheiseen prosessiin mainoksen näyttämiseksi:

1. Käyttäjän seuranta eli datan kerääminen käyttäjästä. Tämä datan kerääminen tapahtuu käyttäjän tekemien toimintojen ja suoraan saatavien tietojen seuraamisen lisäksi yhdistämällä siihen käyttäjästä kolmansilta osapuolilta ostettuja tietoja.
2. Käyttäjän profilointi eli kerätyn datan prosessointi ja analysointi. Kerättyä dataa järjestellään ja arvioidaan hyödyntämällä erilaisia työkaluja ja algoritmeja, jotta saadaan selville mainonnan kannalta oleellisimmat asiat.
3. Käyttäjän profiilin sovitus tiettyihin kohderyhmiin, joita on luotu esimerkiksi erilaisten kiinnostusten kohteiden kuten harrastusten tai tietynlaisen käyttäytymisen perusteella. Edellisessä vaiheessa suoritetun kerätyn datan analysoinnin ja prosessoinnin perusteella käyttäjä sovitetaan kohderyhmiin.
4. Kohdennetun mainoksen toimitus sen mukaan mille kohderyhmille mainostaja on määrittänyt mainoksensa näkyvän. Esimerkiksi mainostaja voisi määrittää mainoksensa kohderyhmäksi 40-60 vuotiaat mobiililaitteella sivustolla vierailevat Suomessa sijaitsevat naiset. Kun sivustolla vierailee tämänkaltaiseen kohderyhmään tunnistettava käyttäjä, näytetään hänelle kyseinen mainos.



KUVIO 1 Kohdentamisprossein vaiheet (Schlee, 2013 s. 10).

Kohdennetun mainonnan jopa oleellisin mahdollistava asia ovat evästeet ja käyttäjän seuranta verkkoympäristössä tapahtuu ennen kaikkea evästeiden avulla. Evästeet ovat käyttäjän avaamien verkkosivustojen luomia tiedostoja,

jotka tallentavat selaustietoja (Google, 2020). Evästeitä käytetään moneen muuhunkin tarkoitukseen kuin vain mainontaan sillä evästeiden avulla sivustot voivat pitää käyttäjän sisäänkirjautuneena palveluihin, muistaa käyttäjän valitsemat asetukset ja antaa esimerkiksi paikallisia säätietoja tietoja sijainnin perusteella. Evästeitä on kahta tyyppiä: ensimmäisen osapuolen evästeet ovat peräisin avoinna olevalta sivustolta ja kolmannen osapuolen evästeet ovat peräisin muilta sivustoilta (Englehardt & Narayanan, 2016; Google, 2020). Evästeiden avulla tietoa keräävät ensimmäisen osapuolen lisäksi myös kolmannet osapuolet (Google, 2020). Facebook (2020) selvittää kuinka esimerkiksi käyttäjän vieraillessa verkkosivulla, jossa on Facebookin tykkää-painike, pystyy Facebook keräämään tiedot sivustolla vierailevasta käyttäjästä, vaikka hän ei henkilökohtaisesti käyttäisi mitään Facebookin palveluita. Evästeitä voi kytkeä pois päältä ja poistaa, mutta kaikki palvelut eivät tällöin toimi (Facebook, 2020). Evästeiden lisäksi sosiaalisen media käyttäjäprofiileissa olevaa tietoa voidaan myös hyödyntää (Facebook, 2020).

Esimerkiksi mainoksia voidaan näyttää perustuen toimintoihin, joita ihmiset tekevät Facebookissa ja jotka liittyvät esimerkiksi heidän käyttämiinsä laitteisiin ja heidän matkamieltymyksiinsä (Facebook, 2020). Google (2020) tarjoaa muun muassa kohdentamista käyttäjille, jotka ovat hakeneet tietyn yrityksen tarjoamia tuotteita tai palveluita, jolloin käyttäjät haluavat ehkä tehdä ostoksia tai ovat tehneet ostoksia aiemmin tältä yritykseltä ja voivat edelleen olla tarpeeksi kiinnostuneita reagoidakseen mainoksiin. Kuten voidaan huomata, pystytään mainonta kohdentamaan todella tarkasti tietyn laisille käyttäjille. Kohdennetun verkkomainonnan hinnoittelussa käytetään enimmäkseen kolmea eri tapaa: CPM (cost per mille) maksetaan tuhannesta näyttö-/latauskerrasta, CPC (cost per click) maksetaan kun mainosta klikataan ja CPA (cost per action) maksetaan toteutuneista tapahtumista kuten toteutuneista myyntitapahtumista (PwC, 2019; Daswani, ym., 2008).

2.2 Kohdennetun verkkomainonnan vahvuudet

Koska verkossa tapahtuva mainonta mahdollistaa hyvin tarkan kohdentamisen ovat perinteiset mainontakanavat kuten televisio, radio, sanomalehdet ja ulkomainonta menettäneet merkitystään (Schlee, 2013 s. 1). Tämä tarkan kohdentamisen mahdollisuus johtaa hyötyihin niin yritysten kuin käyttäjien näkökulmasta.

Mainostajat ovat huomanneet verkkomainonnan olevan tehokkaampaa ja palauttavan paremman tuoton perinteisiin keinoihin verrattuna. (Schlee, 2013 s. 1) Tamin ja Hon (2006) tutkimus osoittaa kuinka kohdentaminen voi tarjota etuja verkkoympäristössä, koska käyttäjät pitävät kohdennettua sisältöä hyödyllisempänä ja ovat halukkaampia tutustumaan kohdennettuun sisältöön verrattuna kohdentamattomaan. Kohdennuksella on potentiaalia vähentää ”informaatioähkyä” ja tarjota apua päätöksenteossa (Tam & Ho, 2006). Käyttäjät saavat osuvampia suosituksia tuotteista ja palveluista (Vesanen, 2007). Lisäksi kohden-

taminen vähentää kognitiivista ylikuormittumista ja lisää mukavuutta (Ansari & Mela, 2003).

Kohdentamisen ansiosta yritykset voivat palvella käyttäjiä paremmin, joka johtaa lisääntyneeseen asiakastyytyväisyyteen (Rust & Chung, 2006) ja uskollisuuteen yritystä kohtaan (Ansari & Mela, 2003) sekä auttaa hallitsemaan asiakkaiden käsitystä yrityksen nopeasta reagoinnista. Yritykset voivat onnistuneen kohdentamisen kautta saada kilpailuetua (Murthi & Sarkar, 2003), veloittaa korkeampia hintoja (Vesanen, 2007) ja parantaa tuottavuuttaan (Rossi, McCulloch & Allenby, 1996; Zhang & Wedel, 2009). Lisäksi erityisesti verkkomainonnan alalla yritykset hyötyvät paremmasta asiakkaiden palaamisesta sivuille, paremmin arvioidusta sisällöstä ja lisääntyneistä ostoista (Tam & Ho, 2006). Kohdennettu verkkomainonta onkin ainakin kaksi kertaa tehokkaampaa kuin vastaava kohdentamaton mainonta (Tucker, 2016).

2.3 Kohdennetun verkkomainonnan haasteet

Monista vahvuuksista huolimatta kohdennettu verkkomainonta sisältää myös monia ongelmallisia asioita. Kohdennetussa mainonnassa on erittäin tärkeää säilyttää käyttäjän luottamus. Mainonnan tehokkuus laskee heti, jos käyttäjä tuntee, että häntä vakoillaan tai että hänestä kerätään tietoja vastoin hänen tahtoaan (Aguirre, ym., 2015). Tarkasti kohdennettu mainonta on myös tehokkaampaa vain, jos sen toteuttaa yritys johon käyttäjä luottaa valmiiksi sillä käyttäjän huolet yksityisyydestä kasvavat, jos luottamus yritystä kohtaan ei ole suuri, vaikka yritysten tekemät toimet ja seuranta olisivatkin samanlaista (Bleier & Eisenbeiss, 2015). Esimerkiksi skandaali Yhdysvaltojen presidentinvaalien ympärillä on herättänyt kysymyksiä kerättävän datan käytöstä. Skandaali tapahtui, kun Facebook antoi Cambridge Analytica nimiselle yhtiölle yli 87 miljoonan käyttäjän tietoja ilman käyttäjien suostumusta, joiden perusteella luotiin kohderyhmiä, joiden avulla vaikutettiin Yhdysvaltojen 2016 presidentin vaalien äänestäjiin kohdistamalla heille suunniteltua mainontaa (Isaak & Hanna, 2018). Euroopassa Euroopan Unioni onkin säätänyt uuden henkilötietolain; GDPR:n, jolla pyritään muun muassa tuomaan kuluttajalle valta hänestä kerättävistä tiedoistaan (Euroopan unionin virallinen lehti, 2016). Osassa palveluita on kuitenkin vaikea estää datan kerääminen kokonaan ja joitain palveluita ei voi edes käyttää suostumatta tietojen keräämiseen, mikä estää osan esimerkiksi amerikkalaisten palveluiden käytön EU-maista (PwC, 2019). Onkin sanottu, että nykyään palveluista ei enää makseta rahalla vaan tiedoilla, joita sittemmin kaupataan muun muassa mainostajien käytettäväksi.

Käyttäjien selatessa ja vuorovaikuttaessa verkkosivulla, heitä tarkkaillaan ensimmäisten osapuolien, jotka ovat sivuja, joilla he vierailevat suoraan, mutta myös kolmansien osapuolien, jotka ovat yleensä piilotettuja seurantapalvelimia kuten mainontaverkkoja, joita on upotettuna useimpiin verkkosivuihin. Myös kolmannet osapuolet voivat saada käyttäjän selainhistorian yhdistelemällä evästeitä ja muita seurantateknologioita, jotka mahdollistavat heidän tunnistavan ja yksilöivän henkilöitä ja kertovan millä sivulla käyttäjä vierailee. Kol-

mannet osapuolet voivat saada haltuunsa myös muita tärkeitä tietoja kuten esimerkiksi käyttäjän sähköpostiosoitteen. (Englehardt & Narayanan, 2016).

Verkkomainonnan ala onkin täynnä kolmansia osapuolia ja välikäsiä, joiden liiketoimintamalli perustuu käyttäjien datan hyödyntämiseen. Mainostajat ovat huolissaan huijauksista ja mainosten väärinasettelusta, julkaisijat vähenevistä mainosbudjeteistaan ja käyttäjät taas yksityisyydestään. Kaikki mainostamisprosessin osapuolista ovat siis jotenkin huolissaan kolmansiin osapuoliin liittyen ja kuinka monissa tapauksissa nämä kolmannet osapuolet toimivat ainakin yhtä edellä mainituista avainpelaajaa vastaan. Tähän mennessä verkkomainonta-alan sääntöjen säätely ei ole onnistunut poistamaan vilpillisisiä aktiviteetteja. (Pärssinen, Kotila, Rumin, Phansalkar, & Manner, 2018.)

Lisäksi yritysten rahaa menee hukkaan keinotekoisen liikenteen ja muiden epäaitojen tapahtumien takia. Jos yritys maksaa siitä, että mainos avataan, voidaan esimerkiksi jonkinlainen bottiverkko laittaa avaamaan mainosta toistuvasti johtaen valheellisiin lukuihin. (Daswani, ym., 2008.) Myös käyttäjien mainosten esto-ohjelmat ovat suosittuja etenkin tietokoneiden selaimilla ja niitä käyttävät henkilöt ovat ryhmä, jota mainokset eivät tavoita aiheuttaen vaikeuksia mainostajille (Nithyanand, ym., 2016).

3 LOHKOKETJUTEKNOLOGIA

Lohkoketjuteknologian toimintaperiaatteet nähtiin ensimmäisen kerran 2008, kun kryptovaluutta Bitcoinin white paper julkaistiin toistaiseksi tuntemattoman Satoshi Nakamoton toimesta. Ensimmäinen käytännön toteutus tapahtui noin kaksi kuukautta myöhemmin 2009, kun Bitcoinin itse tekninen toteutus julkaistiin. Lohkoketjuteknologian toimintaperiaatteet pohjautuvat kuitenkin erityisesti Haberin ja Stornettan jo 1990-luvulla kirjoittamiin julkaisuihin (Nakamoto, 2008). Bitcoin on edelleen tunnetuin lohkoketjuteknologiaan perustuva käytännön sovellus herättäen paljon eriäviä mielipiteitä sen ominaisuuksista, mutta itse lohkoketjuteknologia nähdään lähes poikkeuksetta merkittävänä ja hyvänä keksintönä (Crosby, Pattanayak, Verma & Kalyanaraman, 2016). Lohkoketjuteknologia nousi erittäin suosituksi kryptovaluuttojen yhteydessä, mutta nyt niin kutsuttu ”kryptobuumi” on laskenut ja itse lohkoketjuteknologia kryptovaluuttojen takana on noussut esiin enemmän (Jeffries, 2019). Lohkoketjuteknologiaan perustuvia järjestelmiä nähdäänkin jo Facebookin ja IBM:n kaltaisilta isoilta yrityksiltä. Tässä luvussa määritellään mitä lohkoketjuteknologia on tässä tutkielmassa sekä mitkä ovat sen vahvuudet ja haasteet.

3.1 Lohkoketjuteknologian määritelmä

Mattilan ym. (2018) mukaan lohkoketjuteknologialle ei ole löydettävissä yksiselitteistä selkeää määritelmää tutkimuskirjallisuudesta vaan käsitykset teknologian luonnehdinnasta eroavat eri tahojen välillä, ja käsitettä käytetään myös useilla eri keskustelun tasoilla, eri laajuisiin ja tasoisiin asiakokonaisuuksiin viitaten. Lohkoketjuteknologia on määritelty muun muassa seuraavasti:

> Lohkoketju on tietokantatyyppi, joka ottaa useita tietueita ja sijoittaa ne lohkoon (hieman kuten kokoaisi ne yhdelle paperiarkille). Sitten jokainen lohko ”ketjutetaan” seuraavaan lohkoon käyttämällä kryptografiaa. Tämä sallii lohkoketjujen käytön kuten tilikirjan, jonka kuka tahansa voi jakaa ja vahvistaa, jolla on asianmukaiset oikeudet. (Walport, 2016.)

> Lohkoketju on pohjimmiltaan hajautettu tietokanta tietueista tai julkinen tilikirja kaikista transaktioista tai digitaalisista tapahtumista, jotka on toteutettu ja jaettu osallistuvien osapuolten kesken. Jokainen julkisen tilikirjan tapahtuma vahvistetaan järjestelmän osallistujien enemmistön konsensuksella. (Crosby, ym., 2016.)

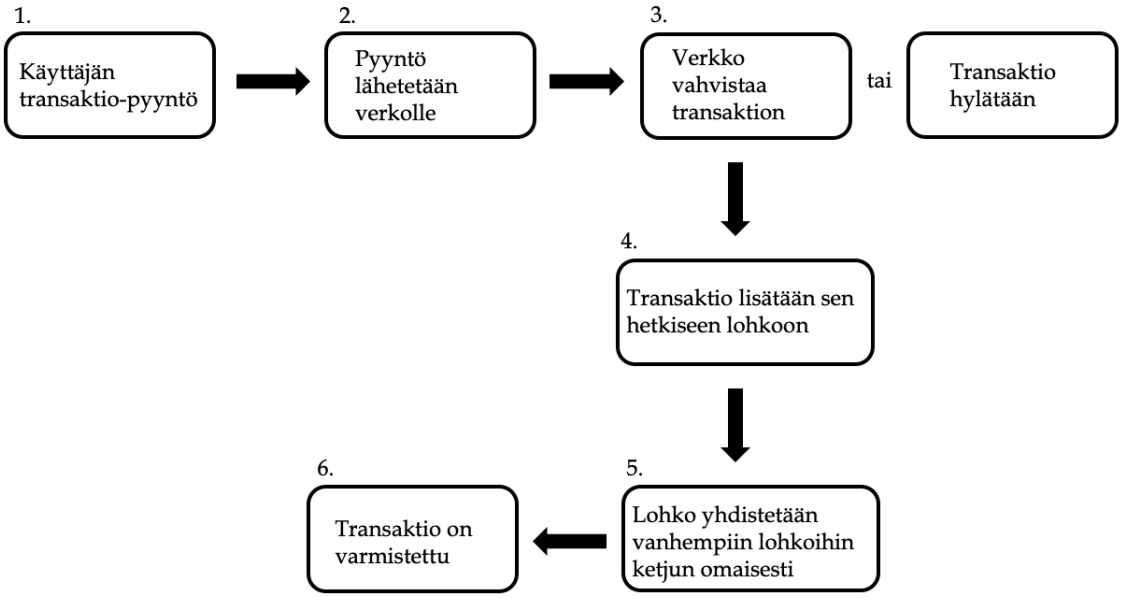
> 'Lohkoketjuteknologialla' tarkoitetaan lohkoketjutietorakenteeseen pohjautuvaa epähierarkista vertaismenetelmää hajautettujen ja replikoitujen digitaalisten tietokantojen luomiseksi (Mattila, ym., 2016).

Yhteistä määritelmille on, että lohkoketju on käyttäjien kesken hajautettu tietokanta, jossa tiedon oikeellisuus vahvistetaan käyttäjien toimesta. Tämän kaltaisessa toteutustavassa ei välttämättä tarvita kolmatta osapuolta ylläpitämään tietokantaa. Lohkoketju-nimen voidaan sanoa olevan erittäin kuvaava kyseisen teknologian kuvaamiseksi, sillä lohkoketjuissa tapahtumat lisätään lohkoihin, jotka linkittyvät edelliseen lohkoon ketjun omaisesti (Walport, 2016).

Termejä lohkoketju (blockchain) ja hajautettu tilikirja (distributerd ledger) käytetään välillä virheellisesti keskenään tarkoittaen samaa asiaa. Hajautetulla tilikirjalla kuitenkin viitataan teknologian yleiseen muotoon ja lohkoketjulla tiettyyn lisäominaisuuksia omaavaan muotoon. Molemmilla viitataan tilikirjaan eli tiedostoon, joka pitää kirjaa kuka omistaa ja mitä. Hajautetuilla tilikirjoilla on neljä keskeistä ominaisuutta: 1. transaktio-/tapahtumatietokanta, joka on jaettu verkon jäsenten kesken 2. päivitetään yksimielisesti 3. tapahtumat merkitään uniikeilla kryptografisilla allekirjoituksilla 4. turvallinen tarkasteltava historia kaikista tapahtumista. Tähän lohkoketju lisää ominaisuuden, joka on näiden tietokantojen yhdistämisen toisiinsa. Lohkoketjut voidaan jaotella karkeasti julkisiin ja yksityisiin. Julkiset ovat kaikille avoimia, tasavertaisia ja anonyymeja. Yksityisissä taas käyttäjiä voidaan tunnistaa ja erilaisia rooleja määritellä. (Swan, 2017)

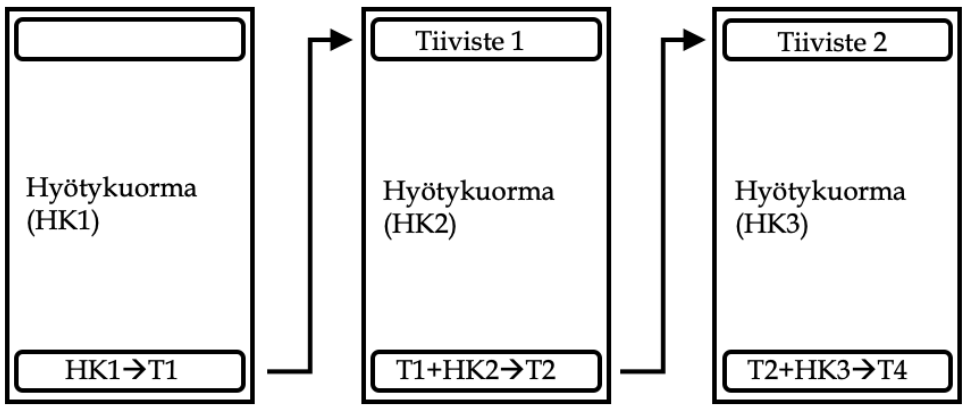
Jokaiselle erilaisella lohkoketjutoteutuksella on omanlaisensa algoritmit tapahtumien toteuttamiseksi. Onkin useita erilaisia malleja, joilla lohkoketjuissa päädytään konsensukseen eli yhteisymmärrykseen oikeasta tiedosta koska erilaiset lohkoketjut ovat tehty eri käyttötarkoituksiin. Jotkin lohkoketjut ovat arvon vaihtamiseen, osa datan säilömiseen ja osa sopimuksien tekemiseen. Laurence (2017) on kuvannut kuinka lohkoketjussa tapahtuvat tapahtumat yleisesti etenevät (kuvio 2) vaikka käytännössä toteutukset voivatkin hieman erota tästä yksityiskohdillaan. (Laurence, 2017 s. 12.) Malli on kuusivaiheinen:

1. Käyttäjä tekee toiminnon aiheuttaen transaktiopyynnön.
2. Tämä pyyntö lähetetään koko lohkoketjuverkolle.
3. Verkko joko vahvistaa tai hylkää transaktiopyynnön.
4. Mikäli transaktio hyväksytään, lisätään tieto siitä sen hetkiseen lohkoon.
5. Tämä transaktion tiedot sisältävä lohko yhdistetään vanhempiin lohkoihin ketjun omaisesti.
6. Transaktio on varmistettu ja tieto siitä säilyy lohkoketjussa.



KUVIO 2 Transaktio lohkoketjussa (Laurence, 2017 s. 12)

Lohkoketjutietorakenteessa (kuvio 3) kaikki muokkaukset lisätään tietokantaan kryptografisesti ketjutettuina lohkoina (Mattila, ym., 2016). Lohkon hajautustiiviste muodostetaan aina kyseisen lohkon hyötykuormasta (payload) ja edellisen lohkon hajautustiivisteestä (hash) (Mattila, ym., 2016). Juuri tämä dataa sisältävien lohkojen ketjuttaminen toisiinsa erottaa lohkoketjut mistä tahansa hajautetuista tilikirjoista (Swan, 2017).



KUVIO 3 Lohkoketjun tietorakenne (Mattila, ym., 2019)

Lohkoketjuteknologiasta puhuttaessa myös älysopimukset (smart contracts) ovat monesti esille nouseva asia. Moniin lohkoketjuihin on sisäänrakennettuna älysopimusten toteutus ja erityisesti Ethereum-niminen lohkoketjutoteutus on tästä tunnettu. Älysopimukset ovat tapa tehdä seurattavia, peruuttamattomia ja luotettavia transaktioita ilman sopimuksen varmentavia ulkopuolisia kolman-

sia osapuolia. Älysopimuksissa lohkoketjuverkko toteuttaa ja varmentaa sopimuksen, kun jokin tietty tapahtuma suoritetaan. Sopimus voi olla periaatteessa mikä tahansa tapahtumasarja lohkoketjutoteutuksesta riippuen. Esimerkiksi jos henkilö lähettää tietyn tiedon itsestään lohkoketjuverkko varmistaa, että hän saa siitä palkkion. (Luu, Chu, Olickel, Saxena & Hobor, 2016.)

Lohkoketjut voidaan jaotella karkeasti yksityisiin (permissioned) ja julkisiin (permissionless). Yksityisistä voidaan käyttää myös nimeä suljettu lohkoketju ja julkisista avoin lohkoketju. Näiden toteutustapojen välillä ominaisuudet eroavat toisistaan (Mattila, 2015). Kinnunen, ym. (2017) tiivistävät julkaisussaan lohkoketjuteknologian tapahtumarekisterityypit rajattuun yksityiseen, avoimeen yksityiseen, rajattuun julkiseen sekä avoimeen julkiseen (taulukko 1).

TAULUKKO 1 Erilaiset lohkoketjun toteutustavat (Kinnunen, ym., 2017)

Tapahtumarekisterin tyyppi	**Kuvaus**
Rajattu, yksityinen (Permissioned private ledger)	Intranetin kaltaisesti toimiva, yhden tai useamman tahon hallinnoima yksityinen tapahtumarekisteri. Käyttö edellyttää liittymistä ja hallinnoivan tahon hyväksymistä (Walport, 2016).
Avoin, yksityinen (Permissionless private ledger)	Intranetin kaltaisesti toimiva, yhden tai useamman tahon hallinnoima avoin tapahtumarekisteri. Käyttö ei edellytä liittymistä, mutta vaatii pääsyn yksityiseen verkkoon.
Rajattu, julkinen (Permissioned public ledger)	Internetissä toimiva, yhden tai useamman tahon hallinnoima julkinen tapahtumarekisteri. Käyttö edellyttää liittymistä ja hallinnoivan tahon hyväksymistä. (Walport, 2016).
Avoin, julkinen (Permissionless public ledger)	Lohkoketju on vapaasti saatavilla internetissä, ei kenenkään omistama tai hallitsema ja avoin kenelle tahansa (Walport, 2016).

3.2 Lohkoketjuteknologian vahvuudet

Lohkoketjuteknologia omaa yleisesti paljon vahvuuksia, jonka takia sen nähdäänkin olevan merkittävä teknologia. Lohkoketjussa tietokannan hajauttamisen ansiosta se tarjoaa korkeaa viansietokykyä, sillä vaikka osa siitä joutuisi esimerkiksi verkkohyökkäyksen kohteeksi jatkaa järjestelmä toimimistaan koska siitä on kopio usealla eri tahoilla. Hajauttamisen ja lohkoketjuteknologiaratkaisujen ansioista myös tietojen läpinäkyvyys ja yhteneväisyys toteutuvat. (Syed, ym, 2019.) Lohkoketjuteknologialla nähdään voitavan helpottaa käyttöoikeuksien hallintaa ja varmentamista ympäristössä, jossa useiden eri tahojen on kyettävä hallitsemaan sekä varmentamaan erilaisia käyttöoikeuksia (Mattila, ym., 2019).

Lohkoketjun salauksen takia yksityisyys voidaan säilyttää, kun tietoa siirretään jäsenten välillä ja jokainen jäsen voi päästä käsiksi vain tietoihin, joihin

heillä on oikeus oikeiden kryptografisten avaimien ansioista. Jokainen jäsen voi kuitenkin luottaa saamaansa tietoon, koska heillä on hallussaan rikkomaton ketju, joka on identtinen muiden ketjujen kanssa voiden tarkastaa sen yhtenäisyyden ja ehjyyden. (Engelhart, 2017.)

Lohkoketjujen vahvuudet vaihtelevat kuitenkin paljon toteutustavan mukaan. Kuten ylempänä on käyty läpi (taulukko 1) yksityisissä lohkoketjuissa verkon tapahtumien oikeellisuudesta vastaa vain luotetut jäsenet, kun taas julkisissa toiminnasta vastaa verkon kaikki jäsenet (Kinnunen, ym, 2017). Yksityisten lohkoketjujen vahvuutena voidaan pitää niiden skaalautuvuutta, energiatehokkuutta ja nopeutta (Mattila, 2016). Tämä johtuu erityisesti siitä, että yksityisissä lohkoketjuissa tapahtuman varmistamiin tahoihin luotetaan, joten koneellisesti vaativia laskutoimituksia (proof-of-work) ei tarvita luottamuksen savuttamiseksi (Luu, ym., 2016). Avoimien lohkoketjujen vahvuutena ovat erityisesti läpinäkyvyydestä johtuvat turvallisuus ja sensuroimattomuus (Mattila, 2016). Siispä lohkoketjuteknologian vahvuudet ja heikkoudet riippuvat paljolti toteutustavasta, joka määräytyy käyttökohteen mukaan.

3.3 Lohkoketjuteknologian haasteet

Mattila, ym. (2018) toteaa, että kokonaisuutena arvioiden lohkoketjujärjestelmät ovat monessa suhteessa varsin kankeita ja yleensä myöskin perinteisiä tietojärjestelmiä huomattavasti kalliimpia ylläpitää. Lohkoketjuteknologian ongelmat ovat yleisesti tunnettuja ja teknologiaa kehittävät tahot koittavat löytää näihin ratkaisuja (Swan, 2015, s. 81). Nykyiset systeemit vielä riittämättömiä ja kehitystä tarvitaan lisää kovia kilpailijoita vastaan. Monet järjestelmät ovatkin vielä ”puuhasteluvaiheessa”.

Erityisesti GDPR asettaa EU-maissa rajoitteita tai vähintäänkin kysymyksiä lohkoketjuteknologian ympärille (Euroopan unionin virallinen lehti, 2016). GDPR:n mukaan henkilötietojen takana on oltava vähintään yksi oikea henkilö, joka on vastuussa tiedoista, mutta lohkoketjuissa vastuu jaetaan kaikkien kesken. Dataa pitäisi voida muokata tai poistaa mutta lohkoketjuissa pyritään nimenomaan datan muuttamattomuuteen. Datan säilöntäsijaintia on myös vaikea hahmottaa järjestelmän ollessa hajautettu. GDPR pyrkii datan minimalisointiin, kun lohkoketju taas kopioi datan kaikille ja lisää dataa aina uuden päälle. (Fink, 2019).

Suljettujen ja avointen lohkoketjujen välillä erityisesti avoimien lohkoketjujen suuri haaste liittyy lohkoketjujen varmistusprosessiin, eli tapaan, jolla verkossa päästään lopputulokseen siitä, mitä seuraavaan lohkoon kirjataan. Kun luotettava välikäsi otetaan pois yhtälöstä, luottamus täytyy luoda koneellisesti, joka vaatii tietokoneilta paljon laskentatehoa ja energiaa. Esimerkiksi Bitcoin-transaktioiden varmistaminen vaatii monimutkaisten laskutoimitusten ratkaisemisen. Tätä louhijoiden suorittamaa prosessia kutsutaan työtodistukseksi (proof-of-work) ja se vie paljon sähköä. (Vranken, 2017.)

4 LOHKOKETJUTEKNOLOGIA KOHDENNETUSSA VERKKOMAINONNASSA

AdLedgerin (2018) yhteistyössä TV[R]EV:n kanssa tuottamassa tutkimuksessa, jossa haastateltiin sataa ylempää mainonnan johtajaa erilaisista yrityksistä ja heistä yli 70% piti lohkoketjuteknologiaa mainonnan tulevaisuutena ja yli 50% lohkoketjujen vähentävän turhia välikäsiä. Tämä tarkoittaa sitä, että mainonnan alalla päätöksiä tekevät ovat tietoisia lohkoketjuteknologiasta ja uskovat sen olevan oleellinen teknologia tulevaisuudessa. Tässä luvussa vastataan tutkimuskysymykseen ja tarkastellaan tutkielman tuloksia.

4.1 Lohkoketjuteknologian hyödyntäminen kohdennetussa verkkomainonnassa

Engelhartin (2017) mukaan lohkoketjuteknologia on hyödyllinen kun:

1. Useita sidosryhmiä on osallisena.
2. Tarvitaan enemmän luottamusta osapuolten välille kuin nykyisin.
3. On välikäsiä, joita voitaisiin jättää pois luottamuksen tai tehokkuuden lisäämiseksi.
4. On tarve luotettavalle aktiviteettien seurannalle.
5. Datan luotettavuudelle on tarve pitkällä aikavälillä.

Jokainen näistä kohdista soveltuu kohdennetun verkkomainonnan alaan. Kohdennetussa verkkomainonnassa osapuolia on useita, kuten kuluttaja, mainostajat, julkaisijat, kolmannet osapuolet (Englehardt & Narayanan, 2016). Kohdennetussa verkkomainonnassa halutaan enemmän luottamusta näiden osapuolten välille ja erityisesti käyttäjät haluavat lisää läpinäkyvyyttä ja luottamusta (Goldfarb & Tucker, 2011; Schlee, 2013, s. 268). Tämä luottamus on välttämätöntä mainonnan onnistumiseksi (Bleier & Eisenbeiss, 2015; Aguirre, ym., 2015) Verkkomainonnan ala myös on täynnä välikäsiä ja kolmansia osapuolia (Pärssinen, ym., 2018). Kohdennetussa verkkomainonnassa on tarve luotettavalle

aktiviteettien seurannalle, jotta mainonta saadaan kohdistettua onnistuneesti (Tam & Ho, 2016). Lisäksi tarvitaan luotettavaa dataa erityisesti käyttäjästä heti kohdentamisprosessin alussa kuten Schlee (2013, s. 10) kohdentamisprosessin mallissaan kuvaa. Engelhartin (2017) selvittämien lohkoketjuteknologian hyötyjen perusteella lohkoketjupohjaiset ratkaisut pystyisivät tarjoamaan siis ratkaisun useisiin verkkomainontaa piinaaviin ongelmiin.

Tutkielman alussa muodostettiin tutkimuskysymys: Miten lohkoketjuteknologian avulla voidaan ratkaista kohdennetun verkkomainonnan haasteita? Lohkoketjuteknologian hyödyntäminen voisi korjata ongelmia käyttäjien tunnistautumisessa varmistaen käyttäjän aitouden (Mattila, ym., 2019). Mikäli käyttäjät ovat tunnistettavissa aidoiksi, voisi tämä poistaa verkkomainonnalle ongelmallisen keinotekoisen liikenteen aiheuttamat kulut (Daswani, ym., 2008). Lohkoketjuteknologia voisi poistaa kolmansia osapuolia tehden mainonnasta tehokkaampaa yrityksille vähentäen turhia osapuolia (Nofer, Gomber, Hinz & Schiereck, 2017), sillä iso osa mainostamiseen menevästä rahasta voi mennä mainostajan sijasta mainosverkoille (Stone-Gross, ym., 2011). Kolmansien osapuolten vähentyminen voisi palauttaa yksityisyyden tunnetta kuluttajille, mikä on oleellista mainonnan toimivuuden kannalta (Tucker, 2014; Aguirre, ym., 2015). Lohkoketjuteknologialla voitaisiin tarjota tarkempaa seurantaa (Swan, 2015 s. 28), joka voisi parantaa mainosten osuvuutta. Lisäksi on arveltu, että lohkoketjupohjaiset ratkaisut voisivat lopettaa Googlen ja Facebookin monopoliaseman (Harvey, Moorman & Toledo, 2018). Mainosten maksamisessa voitaisiin käyttää lohkoketjuun liitettyjä kryptovaluuttoja, jotka yhdessä älysopimusten kanssa voisivat hoitaa mainoksista maksamisen automaattisesti lohkoketjussa ilman kolmansia osapuolia (Luu, ym., 2016). Lisäksi lainsäädäntö olisi mahdollista ohjelmoida suoraan toteutukseen (Syed, ym., 2019).

TAULUKKO 2 Miten lohkoketjuteknologian avulla voidaan ratkaista kohdennetun verkkomainonnan haasteita?

Kohdennetun verkkomainonnan haasteet	**Lohkoketjuteknologian hyödyntäminen**	**Lähteet**
Kolmansien osapuolten runsas määrä	Lohkoketjuteknologian on luvattu vähentävän kolmansia osapuolia. Kolmansia osapuolia voisi vähentää erityisesti nykyisten mainontaverkkojen toimijoista.	Englehardt & Narayanan, 2016; Nofer, ym., 2011; Pärssinen, ym., 2018; Swan, 2015;
Luottamuksen puute osapuolten välillä	Mikäli lohkoketjut palauttavat luottamuksen mainontaan, nostaisi se mainonnan tehokkuutta. Luottamusta voisi parantaa parempi hallinta omista tiedoista ja järjestelmän läpinäkyvyys.	Aguirre, ym., 2015; Goldfarb & Tucker, 2011; Pärssinen, ym., 2018 Schlee, 2013; Tucker, 2014
Mainoksiin liittyvät huijaukset	Lohkoketjuteknologia voisi tehdä käyttäjistä paremmin tunnistettavia ja tehdä keinotekoisesta liikenteestä helpommin huomattavaa.	Daswani, ym., 2008; Stone-Gross, ym., 2011; Mattila, ym., 2019;

	Lisäksi lohkoketjujen läpinäkyvyys ja tarkasteltava historia voisivat auttaa tässä asiassa.	
Lainsäädännön noudattaminen	Lohkoketjun toimintaan voidaan ohjelmoida suoraan lainsäädäntö, joka pakottaisi järjestelmän noudattamaan tiettyjä toimintatapoja.	Fink, 2019, Luu, ym., 2016; Mattila, ym., 2019; Syed, ym., 2019

4.2 Lohkoketjuteknologian haasteet kohdennetussa verkkomainonnassa

Ongelmia lohkoketjuteknologian hyödyntämisessä aiheuttaa etenkin skaalautuvuus. Mainontaverkot toteuttavat yli 100 000 toimintoa sekunnissa, kun esimerkiksi Bitcoin-verkko 7 toimintoa sekunnissa (Swan, 2015 s. 82). Kuitenkin jo olemassa olevista lohkoketjupohjaisista mainontaverkoista Adshares kertoo järjestelmänsä pystyvän jopa 10 000:een toimintoon ja 100 000:een siirtotapahtumaan sekunnissa (Zemlo & Rychlewski, 2017). Tämä ei vielä pysty vastamaan perinteisten verkkomainontaverkkojen määriin, mutta lohkoketjupohjaisia ratkaisuja ei ole vielä kehitetty muutamia vuosia kauempaa sekä kehittävät tahot eivät omista samanlaisia resursseja kehitykseen kuin Googlen ja Facebookin kaltaiset yritykset. Kunhan skaalautuvuusongelmat pystytään ratkaisemaan, on lohkoketjuteknologiaan pohjautuvia järjestelmiä mahdollista hyödyntää lähes millä tahansa alalla (Pärssinen, ym., 2018).

Toinen suuri ongelma on, kuinka etenkin avoimissa lohkoketjuissa kopio lohkoketjusta on jaettuna kaikille käyttäjille tiedon ollen pysyvää ja jäljitettävää (Walport, 2016). Tämä voi aiheuttaa ongelmia lainsäädännön kanssa (Fink, 2019). Käyttäjien yksityisyys onkin jopa helpompi saavuttaa perinteisissä tietokannoissa, koska läpinäkyvyyttä ja varmistettavuutta ei vaadita näiltä järjestelmiltä (Wüst & Gervais, 2018).

Osaan haasteista on jo pyritty vastaamaan teoriassa, mutta käytännössä toteutetut järjestelmät puuttuvat toistaiseksi. Zyskin ja Nathan (2015) ovat kehittäneet lohkoketjuteknologiaan perustuvan mallin, jossa henkilökohtainen data on käyttäjän hallinnoitavissa ja omistuksessa, mutta samalla säilyttäen datan turvallisuuden rajoittamatta kuitenkaan yritysten mahdollisuutta kohdistettuihin palveluihin. Tämänkaltaisessa ratkaisussa käyttäjien ei tarvitse luottaa kolmansiin osapuoliin ollen tietoisia kerättävästä datasta ja sen käytöstä, koska lohkoketju tunnistaa käyttäjän oman datan omistajakseen (Zyskind & Nathan, 2015). Tämä helpottaisi myös yritysten toimintaa sillä niiden ei tarvitse huolehtia datan turvaamisesta sekä lisäksi lait ja säädökset voitaisiin ohjelmoida suoraan itse lohkoketjun toimintalogiikkaan, joka estäisi väärinkäytökset (Zyskind & Nathan, 2015). Myös älysopimuksista on kehitetty malli, jossa tapahtumia ei jaeta julkisesti, jolloin tapahtumien yksityisyys säilyy (Kosba, Miller, Shi, Wen & Papamanthou, 2016).

Toistaiseksi nykyisillä käytössä olevilla lohkoketjujärjestelmillä ei kuitenkaan voida korvata vielä kokonaisia mainosverkostoja ja mainosjärjestelmiä (Pärssinen, ym., 2018), mutta joidenkin järjestelmien osa-alueiden toteutuksessa lohkoketjuteknologiaa voitaisiin hyödyntää. Nykyiset lohkoketjuteknologiaan perustuvat järjestelmät ovat siis vielä riittämättömiä, mutta potentiaali on suuri (Pärssinen, ym., 2018).

5 YHTEENVETO

Tässä tutkielmassa käsiteltiin lohkoketjuteknologian mahdollisuuksia kohdennetussa verkkomainonnassa. Niin lohkoketjuteknologia kuin kohdennettu verkkomainonta ovat hyvin ajankohtaisia aiheita, jotka sisältävät paljon lupauksia. Lähes kaikki verkossa oleva mainonta on kohdennettua mainosten ollessa elinehto monelle nykyiselle palvelulle; lohkoketjuteknologian kuitenkin ennustetaan muuttavan nykyiset liiketoimintamallit. Tutkielma toteutettiin kirjallisuuskatsauksena, joten tulokset muodostettiin lähdekirjallisuuden perusteella. Tutkielman alussa perusteltiin ja muodostettiin tutkimuskysymys:

- Miten lohkoketjuteknologian avulla voidaan ratkaista kohdennetun verkkomainonnan haasteita?

Johdantoluvun jälkeen määriteltiin kohdennettu verkkomainonta ja lohkoketjuteknologia, mitkä ovat niiden vahvuudet sekä mitkä ovat niiden haasteet. Kohdennettu verkkomainonta on verkossa tapahtuvaa mainontaa, joka kohdennetaan käyttäjälle hänestä saatavien tietojen perusteella. Kohdennetun verkkomainonnan vahvuudeksi tunnistettiin etenkin sen tehokkuus verrattuna kohdentamattomaan. Haasteita kohdennetussa verkkomainonnassa aiheuttaa lähdekirjallisuuden perusteella erityisesti kolmansien osapuolten runsas määrä, luottamuksen puute osapuolten välillä sekä mainontaan liittyvät huijaukset. Lohkoketjuteknologia on käyttäjien kesken hajautettu tietokanta, jossa tiedon oikeellisuus vahvistetaan käyttäjien toimesta. Tämän kaltaisessa toteutustavassa ei välttämättä tarvita kolmatta osapuolta ylläpitämään tietokantaa. Erilaiset lohkoketjut voidaan vielä niiden ominaisuuksien perusteella jaotella yksityisiin ja avoimiin. Teknologian vahvuudet ja haasteet vaihtelevat jonkin verran näiden toteutustapojen välillä.

Tutkielman tavoitteena oli tunnistaa, miten lohkoketjuteknologiaa voitaisiin hyödyntää kohdennetussa verkkomainonnassa. Kirjallisuuskatsauksen perusteella lohkoketjuteknologia voisi tarjota ratkaisuja useisiin kohdennetun verkkomainonnan haasteisiin. Lohkoketjuteknologian hyödyntäminen voisi korjata ongelmia käyttäjien tunnistautumisessa poistaen verkkomainonnalle ongelmallisen keinotekoisen liikenteen aiheuttamat kuluja. Lohkoketjuteknolo-

gia voisi poistaa kolmansia osapuolia tehden mainonnasta tehokkaampaa yrityksille vähentäen turhia osapuolia. Kolmansien osapuolten vähentyminen voisi palauttaa yksityisyyden tunnetta kuluttajille, mikä on oleellista mainonnan toimivuuden kannalta. Lisäksi lainsäädäntö olisi mahdollista ohjelmoida suoraan lohkoketjuun. Lohkoketjupohjaisia korvaajia nykyisille järjestelmille ei ole kuitenkaan vielä onnistuttu toteuttamaan. Suurimpia ongelmia aiheuttaa järjestelmien skaalautuvuus tarpeeksi suuriksi, sekä lisäksi lainsäädäntö lohkoketjuteknologian ympärillä on vielä sekavaa. Nykyiset lohkoketjuteknologiaan perustuvat järjestelmät ovat siis vielä riittämättömiä, mutta niissä uskotaan olevan potentiaalia.

Jatkossa tarvitaan lisää kehitystyötä, että lohkoketjupohjaiset järjestelmät pystyisivät korvaamaan nykyiset järjestelmät kohdennetun verkkomainonnan alalla. Lohkoketjuteknologia saattaa tulevaisuudessa tarjota ratkaisuja myös kohdennettuun verkkomainontaan, kuten moniin muihinkin aloihin. Yksi tärkeimpiä jatkotutkimuskohteita onkin miten saada lohkoketju kannattavaksi ja skaalautumaan, sillä nykyiset järjestelmät ovat suuressa mittakaavassa toteutettuna melko raskaita verrattuna perinteisiin.

Jatkotutkimusta tarvitaan lisäksi lohkoketjupohjaisten järjestelmien yksityisyyden osalta sekä lohkoketjuteknologian uutuudesta ja ominaisuuksista johtuen sen käytöstä lainsäädännön näkökulmasta täytyy saada lisää selkeyttä. Täytyy myös tutkia, onko lohkoketjuteknologian yhdistäminen kohdennettuun mainontaan tarpeellista vai pystytäänkö samat hyödyt saavuttamaan muilla ratkaisuilla, kuten lainsäädännöllä.

Gilad Edelman kirjoittaa artikkelissaan Wired-lehdessä (2020) kuinka ainut keino palauttaa kuluttajien yksityisyys olisi kieltää kohdennettu mainonta. Tällä hetkellä kuitenkin lukuisten suurten ja pienempien yritysten liiketoimintamallit perustuvat kohdennettuun verkkomainontaan, joten ennen kuin kuluttajat ovat valmiita maksamaan palveluista mieluummin rahalla kuin omilla tiedoillaan tai lainsäädäntöä vaihdeta, ei tätä muutosta nykyisestä tulla näkemään.

LÄHTEET

AdLedger. (2018). Blockchain & Advertising Special Report in Partnership with TV[R]EV. Haettu osoitteesta https://adledger.org/

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K. & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing,* 91(1), 34-49. Haettu osoitteesta https://www.sciencedirect.com/science/article/pii/S0022435914000669

Ansari, A. & Mela, C. F. (2003). E-customization. *Journal of marketing research,* 40(2), 131-145. Haettu osoitteesta https://journals.sagepub.com/doi/abs/10.1509/jmkr.40.2.131.19224

Bleier, A. & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing,* 91(3), 390-409. Haettu osoitteesta https://www.sciencedirect.com/science/article/pii/S0022435915000263

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchaintechnology: Beyond bitcoin. *Applied Innovation,* 2(6-10), 71. Haettu osoitteesta https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

Daswani, N., Mysen, C., Rao, V., Weis, S., Gharachorloo, K. & Ghosemajumder, S. (2008). Online advertising fraud. *Crimeware: understanding new attacks and defenses,* 40(2), 1-28. Haettu osoitteeesta https://neildaswani.com/assets/pdf/publications/crimeware.pdf

Edelman, G. (2020). Why Don't We Just Ban Targeted Advertising? Haettu osoitteesta https://www.wired.com/story/why-dont-we-just-ban-targeted-advertising/

Enberg, J. (28.3.2019). Global Digital Ad Spending 2019. Haettu osoitteesta https://www.emarketer.com/content/global-digital-ad-spending-2019

Euroopan unionin virallinen lehti. (2016). EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679. Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Englehardt, S. & Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. *In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (s. 1388-1401). Haettu osoitteesta https://dl.acm.org/doi/abs/10.1145/2976749.2978313

Facebook. (2020). Evästeet ja muut tallennustekniikat. Haettu osoitteesta https://www.facebook.com/policies/cookies

Facebook. (2020). Tietokäytäntö. Haettu osoitteesta https://www.facebook.com/about/privacy

Fink, M. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? Haettu osoitteesta

https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445

Goldfarb, A. & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management science,* 57(1), 57-71. Haettu osoitteesta https://pubsonline.informs.org/doi/abs/10.1287/mnsc.1100.1246

Google. (2020). Evästeiden poistaminen, käyttöönotto ja hallinnointi Chromessa. Haettu osoitteesta https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=fi

Google. (2020). Googlen käyttämät evästetyypit. Haettu osoitteesta https://policies.google.com/technologies/types?hl=fi

Harvey, C. R., Moorman, C. & Toledo, M. (2018). How Blockchain Will Change Marketing As We Know It. Haettu osoitteesta https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3257511

Isaak, J. & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer,* 51(8), 56-59. Haettu osoitteesta https://ieeexplore.ieee.org/abstract/document/8436400

Jeffries, D. (2019). What Will It Take for Crypto to Boom Again? Haettu osoitteesta https://hackernoon.com/what-will-it-take-for-crypto-to-boom-again-a7ef9c2ef982

Kinnunen, T. K., Leviäkangas, P., Kostiainen, J., Nykänen, L., Rouhiainen, K. & Finlow-Bates, K. (2017). Lohkoketjuteknologian soveltaminen ja vaikutukset liikenteessä ja viestinnässä. Haettu osoitteesta http://julkaisut.valtioneuvosto.fi/handle/10024/80667

Kosba, A., Miller, A., Shi, E., Wen, Z. & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *In 2016 IEEE symposium on security and privacy (SP)*, 839-858. Haettu osoitteesta https://ieeexplore.ieee.org/abstract/document/7546538

Lambrecht, A. & Tucker, C. (2013). When does retargeting work? Information specificity in online advertising. *Journal of Marketing research*, 50(5), 561-576. Haettu osoitteesta https://journals.sagepub.com/doi/pdf/10.1509/jmr.11.0503

Laurence, T. (2017). *Blockchain fur Dummies.* John Wiley & Sons Incorporated.

Luu, L., Chu, D. H., Olickel, H., Saxena, P. & Hobor, A. (2016). Making smart contracts smarter. *In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security,* 254-269. Haettu osoitteesta https://dl.acm.org/doi/abs/10.1145/2976749.2978309?casa_token=Qgf1zs0026YAAAAA:39gtdQzzf-z5G0M2wnTAJJRQmoyliPpBHnzqd8YGij6IplETtwA-TDnUWsoGsIVzN3dHFFksRKba

Mattila, J. (2016). The blockchain phenomenon–the disruptive potential of distributed consensus architectures (No. 38). *ETLA working papers.* Haettu osoitteesta: https://brie.berkeley.edu/sites/default/files/juri-mattila-.pdf

Mattila, J., Seppälä, T., Hukkinen, T., Laikari, A., Markkanen, K., Koulu, R. & Jia, K. (2019). Lohkoketjuteknologian hyödyntämismahdollisuudet palkkatulojen verotuksessa. Haettu osoitteesta http://julkaisut.valtioneuvosto.fi/handle/10024/161543

Murthi, B. P. S. & Sarkar, S. (2003). The role of the management sciences in research on personalization. *Management Science,* 49(10), 1344-1362. Haettu osoitteesta https://pubsonline.informs.org/doi/abs/10.1287/mnsc.49.10.1344.17313

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

Nithyanand, R., Khattak, S., Javed, M., Vallina-Rodriguez, N., Falahrastegar, M., Powles, J. E., De Cristofaro, E., Haddadi, H. & Murdoch, S. J. (2016). Adblocking and counter blocking: A slice of the arms race. *In 6th {USENIX} Workshop on Free and Open Communications on the Internet.* Haettu osoitteesta https://www.usenix.org/conference/foci16/workshop-program/presentation/nithyanand

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering,* 59(3), 183-187. Haettu osoitteesta https://link.springer.com/article/10.1007/s12599-017-0467-3

Plummer, J., Rappaport, S. D., Hall, T. & Barocci, R. (2007). *The online advertising playbook: Proven strategies and tested tactics from the advertising research foundation.* John Wiley & Sons.

Pärssinen, M., Kotila, M., Rumin, R. C., Phansalkar, A. & Manner, J. (2018). Is Blockchain Ready to Revolutionize Online Advertising?. *IEEE Access*, 6, 54884-54899. Haettu osoitteesta: https://ieeexplore.ieee.org/abstract/document/8478235

Rossi, P. E., McCulloch, R. E. & Allenby, G. M. (1996). The value of purchase history data in target marketing. *Marketing Science,* 15(4), 321-340. Haettu osoitteesta https://pubsonline.informs.org/doi/abs/10.1287/mksc.15.4.321

Rust, R. T. & Chung, T. S. (2006). Marketing models of service and relationships. *Marketing science,* 25(6), 560-580. Haettu osoitteesta https://pubsonline.informs.org/doi/abs/10.1287/mksc.1050.0139

Schlee, C. (2013). *Targeted Advertising Technologies in the ICT Space: A Use Case Driven Analysis.* Springer Fachmedien Wiesbaden 2013.

Song, J. H., & Zinkhan, G. M. (2008). Determinants of perceived web site interactivity. *Journal of marketing,* 72(2), 99-113. Haettu osoitteesta https://journals.sagepub.com/doi/abs/10.1509/jmkg.72.2.99

Stone-Gross, B., Stevens, R., Zarras, A., Kemmerer, R., Kruegel, C. & Vigna, G. (2011). Understanding fraudulent activities in online ad exchanges. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference,* 279-294. Haettu osoitteesta https://dl.acm.org/doi/abs/10.1145/2068816.2068843?casa_token=-dOxypTDd-wAAAAA:NXyTxOq4YkAa2OJ2Pj4L1hV6JDu-vCCIA3-WCRQW6UvbP_47adWjnG0qkuHMjJNfsmWc1v2Wl-wk

Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology innovation management review,* 7(10), 6-13. Haettu osoitteesta https://pdfs.semanticscholar.org/ced3/b8dcf8636a0de6a39ff32dfc78a5028c8207.pdf#page=6

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

Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A. & Alghamdi, T. (2019). A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access*, 7, 176838-176869. Haettu osoitteesta https://ieeexplore.ieee.org/abstract/document/8922632

Tam, K. Y. & Ho, S. Y. (2006). Understanding the impact of web personalization on user information processing and decision outcomes. *MIS quarterly*, 865-890. Haettu osoitteesta https://www.jstor.org/stable/25148757?seq=1 - metadata_info_tab_contents

Tapscott, D. & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.* Penguin.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research,* 51(5), 546-562. Haettu osoitteesta https://journals.sagepub.com/doi/full/10.1509/jmr.10.0355

Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing.* Haettu osoitteesta https://www.emerald.com/insight/content/doi/10.1108/03090560710737534/full/html

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current opinion in environmental sustainability*, 28, 1-9. Haettu osoitteesta https://www.sciencedirect.com/science/article/abs/pii/S1877343517300015

Walport, M. (2016) Distributed Ledger Technology: Beyond Block Chain, Government Office for Science, London. Haettu osoitteesta https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

Wüst, K. & Gervais, A. (2018). Do you need a blockchain? *In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT),* 45-54. Haettu osoitteesta https://ieeexplore.ieee.org/abstract/document/8525392

Zemlo, J. & Rychlewski, L. (2017). Adshares Whitepaper. Haettu osoitteesta https://adshares.net/docs/adshares_whitepaper.pdf

Zhang, J., & Wedel, M. (2009). The effectiveness of customized promotions in online and offline stores. *Journal of marketing research*, 46(2), 190-206. Haettu osoitteesta https://journals.sagepub.com/doi/abs/10.1509/jmkr.46.2.190

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *In 2017 IEEE international congress on big data (BigData congress)*, 557-564. Haettu osoitteesta https://ieeexplore.ieee.org/abstract/document/8029379

Zyskind, G. & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *In 2015 IEEE Security and Privacy Workshops,* 180-184. Haettu osoitteesta https://ieeexplore.ieee.org/abstract/document/7163223