Krista Määttä

Lohkoketjuteknologian sovellusmahdollisuudet osana infrastruktuuria

Tietotekniikan kandidaatintutkielma

14. toukokuuta 2018

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Krista Määttä

Yhteystiedot: krista.s.maatta@student.jyu.fi

Työn nimi: Lohkoketjuteknologian sovellusmahdollisuudet osana infrastruktuuria

Title in English: Blockchain technology applications as part of the infrastructure

Työ: Kandidaatintutkielma

Sivumäärä: 32+0

Tiivistelmä: Tutkielman aiheena on perehtyä lohkoketjuteknologiaan ja tarkastella sen mahdollisia sovellutuksia osana tietoyhteiskunnan infrastruktuuria: Millaisiin ongelmiin tämä voisi tuoda ratkaisuja ja miten sitä voitaisiin soveltaa yhteiskunnan rakenteessa? Mitä lohkoketjuteknologialla tarkoitetaan, kuinka ne toimivat ja miten ne ovat kehitetty? Millaisia haasteita lohkoketjujen soveltamiseen liittyy? Tutkimus toteutettiin kirjallisuuskatsauksena. Keskeisenä tuloksena voidaan teknologialla todeta olevan runsaasti potentiaalia tulla sovelletuksi monilla infrastruktuurin osa-alueilla. Lohkoketjun avainetuna on sen mahdollistama tiedon muuttumattomuus ja hajautettavuus, mutta ennen kaikkea läpinäkyvyys ja siten perinteisesti luottamuksen taanneen kolmannen osapuolen tarpeen poistaminen.

Avainsanat: lohkoketju, Bitcoin. sovellus, infrastruktuuri, yhteiskunta

Abstract: The subject of the thesis is to explore blockchain technology and survey its potential application as part of the information society's infrastructure: What kind of problems could the technology bring solutions to, and how could it be applied in a society's infrastructure? What blockchain is, how it works and how it has been developed? What sort of challenges are related to applying blockchain? The study was conducted as a literature review. As the key result, it can be said that blockchain technology has plenty of potential to be applied in many areas of infrastructure. The key advantage of the technology is in its ability to provide permanence, distribution and transparency to information, of which the latter can be used to remove the need of the traditionally trusted third-party.

Keywords: blockchain, Bitcoin, application, infrastructure, society

Kuviot

Sisältö

1 Johdanto

Tutkielman aiheena on perehtyä lohkoketjuteknologioihin ja niiden mahdollisiin lohkoketjusovelluksiin yhteiskunnan infrastruktuurisillista ongelmakohdista tarkasteltuna, kuitenkin pääsääntöisesti tietoyhteiskunnan näkökulmasta tarkasteltuna. Huoltovarmuuskeskuksen toimialojen mukaan infrastruktuurit voidaan jakaa Suomessa seuraavasti tietoyhteiskuntaan, logistiikkaan, energiahuoltoon, elintarvikehuoltoon, terveydenhuoltoon, rahoitushuoltoon ja kriittiseen teollisuustuotantoon (Huoltovarmuuskeskus). Tutkielmassa käsitellään lohkoketjuteknologian mahdollistamia keinoja vaikuttaa edellämainittuihin toimialoihin muun muassa vaihtoehtovaluuttojen, älysopimusten, tuotteiden alkuperän todentamisen tai julkisen tiedon, kuten omistusoikeuksien, tallentamisen avulla.

Lohkoketjuteknologian sovellusmahdollisuudet ovat nykyisessä valossa runsaat, mutta myös todennäköisesti myös vielä pitkälti tutkimattomat. Vaihtoehtovaluutat lohkoteknologia taustallaan voisivat nopeuttaa niin perinteisten pankkien transaktioita kuin myös toimia entistä sujuvammissa mikromaksuissa. Myös musiikin tekijänoikeuksien turvaaminen voitaisiin toteuttaa teoriassa lohkoketjuilla sekä siihen voitaisiin yhdistää lähitulevaisuudessa myös mahdollisuus mikromaksuihin, jotka menevät suoraan tekijöille ilman välikäsiä, joka itsessään on yksi mullistavimmista lohkoketjuteknologian mahdollistamista aspekteista rahoitusalalla: raha voi virrata hajautetusti suoraan maksajalta saajalle ilman välikäsiä. Samaa periaatetta hyödynnetään myös älysopimuksissa: sopimukset koodataan suoraan lohkoketjuun, jolloin niitä ei voi muuttaa ja maksut menevät sopimusehtojen täytyttyä. Esimerkiksi kuriiripalvelun kuitattua lähetys vastaanotetuksi, maksu menisi automaattisesti suoraan kuluttajalta kuriiripalvelulle, jonka lisäksi lohkoketjulla voitaisiin varmentaa lähetyksen alkuperä jopa raaka-aineiden alkuperästä eri vaiheiden kautta lopputuotteeksi. Ruoan alkuperän todentamiselle on yhä lisääntyvää tarvetta, etenkin raaka-ainehuijausten yleistyessä sekä kylmäketjun pysyvyyden todentamisessa. Tämä voitaisiin toteuttaa esimerkiksi RFID-tekniikkaa sekä lohkoketjuja hyödyntäen (Tian 2016). Lisäksi, älysopimuksia voitaisiin soveltaa perinteisimmissä sopimuksissa, kuten esimerkiksi sähkösopimuksissa sekä vakuutuksissa. Julkisen tiedon tallentamista voitaisiin puolestaan soveltaa esimerkiksi kansalaisten identiteettien tallentamisessa väestörekisteriin sekä tunnistamisessa liittyen sähköiseen äänestämiseen. Lohkoket-

juun perustuvalla kansalaisten identifioinnilla on paljon mahdollisuuksia, mutta myös toteutuksellisia haasteita sekä väärinkäytön uhkia, mikä tekee aiheesta kiinnostavan tutkimuksen kohteen. Esimerkiksi kansalaisten opintosuoritukset, terveystiedot ja omistusoikeudet maanomistuksesta arvoesineisiin voitaisiin tallentaa helposti saataville lohkoketjuun, mikä vähentäisi eri tahojen toisiinsa luottamattomuudesta johtuvia ongelmia sekä byrokratiaa, mutta toisaalta aiheuttasi mahdollisesti yksilönvapauteen ja eettisyyteen liittyviä ongelmia.

Lisäksi on huomioitava itse lohkoketjuteknologiaan liittyvät mahdolliset ongelmat, jotka liittyvät todennäköisesti ketjujen skaalaatuvuuteen: ketjun käyttäjien määrän lisääntyminen voi johtaa tämänhetkisillä teknologioilla sekä salaustekniikoilla toteutettujen ketjujen hidastumiseen sekä samalla energiankulutuksen kasvamiseen, mikä voi osaltansa vaikuttaa louhijien motivointiin liittyviin ongelmiin, etenkin jos louhimisesta saatavat korvaukset pienenevät tai loppuvat kokonaan ketjun kasvaessa. Herää kysymys siitä, kenen vastuulle louhiminen on siirrettävä: missä määrin ja millaisissa ketjuissa louhinta voidaan sallia yksityiselle sektorille? On myös huomioitava nykyisten salaustekniikoiden turvallisuuteen liittyvät näkökulmat: jos lohkoketjun perustana käytettävä salaustekniikka saadaan purettua, koko ketjun turvallisuus hajoaa perustavanlaatuisesti. Kvanttitietokoneiden kehityttyä suurin osa yleisimmistä nykyisitä salaustekniikoista, johon myös lohkoketjuteknologia perustuu, on tämänhetkisen tiedon perusteella purettavissa tulevaisuudessa kvanttitietokoneiden avulla (Aggarwal ym. 2017).

Tutkielman keskeisenä tutkimuskysymyksenä on löytää kirjallisuuskatsauksen keinoilla vastauksia seuraaviin kysymyksiin: Miten lohkoketjuteknologiaa voitaisiin soveltaa yhteiskunnan kehittämisessä, ja millaisiin ongelmiin lohkoketjuteknologia voisi tuoda ratkaisuja? Lisäksi toissijaisina tutkimuskysymyksinä ovat seuraavat: Mitä lohkoketjuteknologialla tarkoitetaan, kuinka se toimii ja kuinka se on kehitetty? Ensimmäisessä kappaleessa käsittellään lohkoketjuteknologiaa teknisestä näkökulmasta osana informaatiotieteen kehitystä. Toisessa kappaleessa tuodaan esille mahdollisia lohkoketjuteknologian sovellustapoja perustuen lohkoketjuteknologian kehitykseen, yhteiskunnalliset yhtymäkohdat huomioiden. Lopuksi, tutkielman kolmannessa kappaleessa, käsittelään mahdollisia lohkoketjuihin ja niiden soveltamiseen liittyviä ongelmakohtia ja haasteita, niin yksilötasolla, kuin globaalissa mittakaavassa.

2 Lohkoketjuteknologian tekniset perusteet

Lohkoketjuteknologialla *(eng. blockchain, block chain technology)* tarkoitetaan tekniikkaa, jolla toisilleen vieraat toimijat voivat ylläpitää yhteistä hajautettua tietokantaa ilman toimijoiden välissä perinteisesti toiminutta luottamuksen taannutta kolmatta osapuolta. Lohkoketjut ovat kaikille avoimia, useiden tietokoneiden verkkoon kryptografisesti linkitettyjä, hajautettuja tietokantoja. Tiedon hajautuneisuus mahdollistaa kaikille lohkoketjun käyttäjille sen sisältämien lokien tarkastelun sekä datan pysyvyyden; kerran lohkoketjuun tallennettua dataa ei ole mahdollista muuttaa tai poistaa, vaan se säilyy varmuuskopioituna lohkoketjuun kuuluvilla tietokoneilla. Lohkoketjujen väärentämättömyys puolestaan perustuu kryptografisesti varmennetuille konsensusmekanismeille (Honkanen 2017)

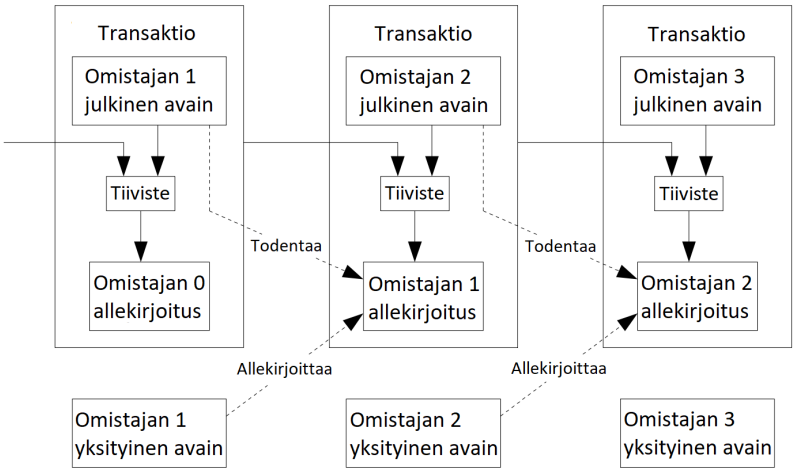
2.1 Historia

Lohkoketjuteknologian voidaan katsoa saaneen alkunsa vuonna 1991 Journal of Cryptocraphy tiedejulkaisussa julkaistusta Stornettan ja Haberin artikkelista “How to time-stamp a digital document”. Kyseisessä artikkelissa tuodaan esiin idea datan aikaleimaamisesta kryptografisia keinoja, kuten tiivisteitä, digitaalista allekirjoitusta ja linkitystä hyödyntäen niin, että aikaleimaa ei pysty manipuloimaan leimaushetkellä eikä jälkikäteen (Stornetta ja Haber 1991). Seuraavana vuonna edelliseen kuvaukseen yhdistettiin Merklen vuoden 1980 artikkelissaan kuvailema puumalli vähentämään vaadittavaa laskentatehoa mahdollistaen tehokkaamman, uudelleenkäytettävän aikaleimauksen (Merkle 1980), (Bayer, Haber ja Stornetta 1992). Vuonna 2002 kehitykseen tuotiin mukaan ajatus hajauttamisen käyttämisestä tietoturvan lisäämiseksi niin, että ketju itse olisi luotettava välittämättä epäluotettavista servereistä tai niille tunkeutujista (Mazieres ja Shasha 2002). Vaikka ajatus digitaalisesta valuutasta oli ollut olemassa kryptografian alalla jo 80-luvulta lähtien, kryptovaluutan kehitystä rajoittivat ratkaisemattomat ongelmat, kuten erityisesti kaksoiskulutuksen ongelma *(eng. double spending problem)* ja siihen oleellisesti liittyvä byzanttilaisen kenraalin ongelma *(eng. Byzantine general’s problem)*. Sakashi Nakamoto onnistui aikaisempaa tutkimusta hyödyntäen ratkaisemaan ongelman vuonna 2008, jonka seurauksena syntyi ensimmäinen merkittävä lohkoketjuteknologiaa käyttävä sovellus, kryptovaluutta Bitcoin (Nakamoto 2008).

2.2 Ideologia

Vaikka lohkoketjuteknologian historia alkaa tarpeesta kehittää toimiva digitaalinen valuutta, tulee lohkoketjuteknologia ensisijaisesti ajatella edistyneenä tapana tallentaa tietoa: Lin ja Liaon (2017) mukaan lohkoketjuteknologian etuja ovat sen mahdollistama datan hajautettuneisuus, muuttumattomuus ja läpinäkyvyys, joista erityisesti viimeksi mainittu mahdollistaa lohkoketjun luotettavuuden. Lohkoketjut ovat immuuneja useimpia hyökkäyksiä vastaan, jonka lisäksi lohkoketjut ovat toiminnaltaan autonomisia, joka lisää toimintavarmuutta. (Lin ja Liao 2017) Lohkoketjuteknologian merkittävimmät ominaisuudet teknologia-alan konsulttiyhtiö McKinseyn mukaan liittyvät lohkoketjun keskeisinpään ominaisuuteen, hajautettuun tietoverkkoon: Lohkoketjuteknologia mahdollistaa sellaisen ratkaisun kaksoiskulutuksen ongelmaan, joka ei vaadi kolmatta osapuolta. Kaksoiskulutuksen ongelman ratkaiseminen lohkoketjuteknologian avulla mahdollistaa puolestaan hajautetun, katkeamattoman luettelon kaikista transaktioista. Kryptografisten keinojen hyödyntäminen lohkoketjuissa takaa puolestaan yhdessä useiden datan varmuuskopioiden kanssa paremman tietoturvan, sekä prosessin yhtenäisyyden. (McKinsey ja Company 2017)

2.3 Transaktiot ja louhinta



Kuvio 1. Transaktio Bitcoin-lohkoketjussa. (Nakamoto 2008, 2)

Nakamoton Bitcoinia koskevan määritelmän mukaan kolikolla *(eng. coin)* tarkoitetaan digitaalisten allekirjoitusten ketjua, jossa jokainen omistaja siirtää kolikon seuraavalle alle-

kirjoittamalla edellisen transaktion, eli siirron, tiivisteen *(eng. hash)* ja seuraavan omistajan julkisen avaimen. Maksunsaaja näin voi todentaa allekirjoitukset varmistaakseen ketjun omistusoikeudet (Kuvio 1). Tiivisteellä tarkoitetaan transaktioista muodostuvan lohkon *(eng. block)* ensisijaista tunnistetta, eräänlaista digitaalista sormenjälkeä, joka saadaan hajauttamalla lohkon otsikko kahdesti SHA256-algoritmilla, luoden 32-bittisen merkkijonon, tiivisteen (Antonopoulos 2014). Maksunsaaja ei kuitenkaan voi tarkistaa, onko joku aiemmista omistajista käyttänyt kolikon useammin kuin kerran. Bitcoinin tapauksessa ongelma on ratkaistu julkaisemalla kaikki transaktiot aikaleimatuina vertaisverkossa ja hyödyntämällä siten Proof-of-Work-konsensusmekanismia (Nakamoto 2008). Bitcoinin lohkoketjussa transaktiot yhdistetään lohkoiksi louhinnaksi *(eng. mining)* kutsutussa prosessissa, jotka edellyttävät suurta laskentamäärää, mutta vaativat todentamiseensa vain vähän laskentatehoa. (Antonopoulos 2014) Antonopolous vertaa tätä prosessia sudoku-peliin, joka alustuu aina kun joku löytää siihen ratkaisun, ja joka muuntuu niin, että yhden pelin ratkaisemiseen kuluisi noin 10 minuuttia. Kuten sudokussa, myös louhinnassa ratkaistun lohkon varmentaminen on helpompaa kuin sen ratkaiseminen (2014).

2.4 Konsensusmekanismit

Lohkoketjut käyttävät konsensusmekanismeja *(eng. consensus mechanism)* kaksoiskulutuksen ongelman ratkaisemiseen. Kaksoiskulutuksella tarkoitetaan tilannetta, jossa yksi lähettäjä pystyy siirtämään yhden kolikon kahtena erillisenä transaktiona kahdelle eri vastaanottajalle. Jos edellä kuvailtu transaktio menisi molempien vastaanottajien kohdalla läpi, ajautuisi lohkoketju epävakaaseen tilaan. Perinteisessä pankkimallissa kaksoiskulutus on estetty pankin valvomien sarjanumeroiden käytöllä, estäen samanaikaisen tapahtumien käsittelyn. Hajautetussa mallissa, jossa kaksoiskulutus on estetty, transaktion ensimmäinen vastaanotto tallentuu julkiseen lokikirjaan lohkoketjuun, jolloin transaktion toinen vastaanotto tunnistetaan kaksoiskulutusyrityksenä. (Tschorsch ja Scheuermann 2016)

Bitcoin oli ensimmäinen, joka ratkaisi kaksoiskulutuksen ongelman tietoturvan kannalta kestävästi hajautetulla Proof-of-Work mekanismilla. Kaksoiskulutus on teoreettisesti edelleen mahdollista haaroittamalla *(eng. fork)* lohkoketju uudeksi haaraksi, mutta tähän vaaditaan, että hyökkääjällä on hallussaan vähintään 51 prosenttia lohkoketjun laskentatehosta

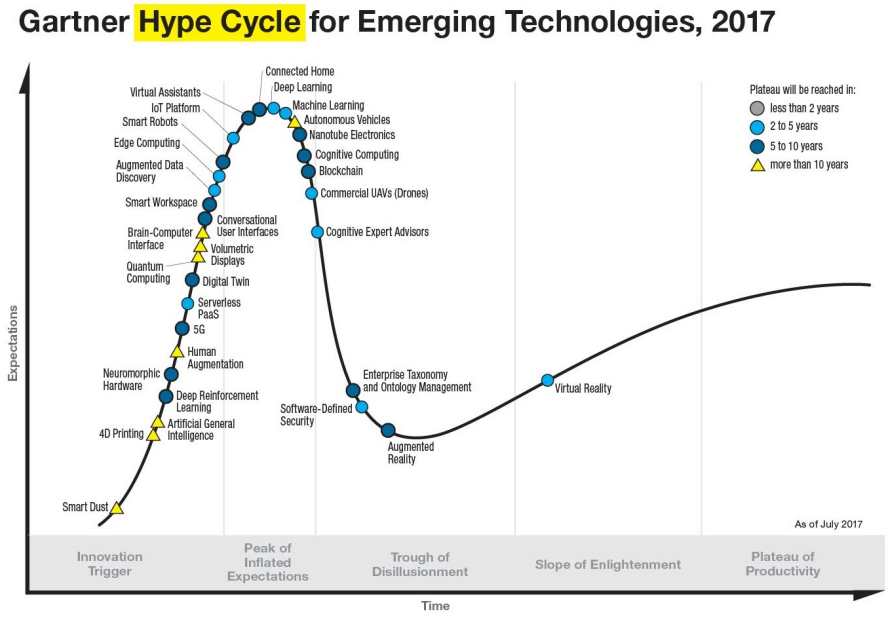
(Tschorsch ja Scheuermann 2016). Lohkoketjun haaroitus voi olla kuitenkin myös tarkoituksella toteutettu uusintahaaroitus ja se voidaan toteuttaa esimerkiksi lohkojen suuresta koosta johtuvan laskentaviiveen pienentämiseksi.

Proof-of-Work (lyh. PoW) konsensusmekanismissa kaikki verkossa olevat tietokoneen ovat velvollisia ylläpitämään lohkoketjun suojausta, pyrkimällä ratkaisemaan tiivistefunktiosta (eng. hash function), joka Bitcoinin tapauksessa on SHA-256-algoritmin mukainen, muodostuvan laskennallisen tehtävän. Tehtävä on tietokoneelle yksinkertainen, mutta erittäin toistuva ja siksi laskennallisesti kallis. Tehtävää voisi verrata ihmiset tietokoneista erottelemaan pyrkiviin CAPTCHA-kuvavarmennuksiin, sillä erotuksella, että lohkoketjun tapauksessa tehtävä on helppo tietokoneelle, kun taas kuvavarmennoksessa ihmisille. Tietokone, joka ratkaisee annetun tehtävän ja siten todistaa työn tehdyksi ensimmäisenä, saa lisätä transaktiolohkon lohkoketjuun ja Bitcoinin lohkoketjussa vastaanottaa lähettäjiltä kerätyistä lähetysmaksuista palkkion bitcoineissa. (Kostarev 2017) Ongelmana PoW-mekanismissa on suuren energiankulutuksen lisäksi louhijoiden pienenevät palkkiot, ja sen seurauksena mahdollisen motivaation puute louhintaan.

Suuren laskennallisen voiman tarpeen takia PoW kuluttaa paljon energiaa ja on siten kallis mekanismi. Eräs vaihtoehtoiseksi tavaksi noussut konsensusmekanismi on muun muassa Ethereum-lohkoketjussa käytettävä Proof-of-Stake (lyh. PoS), joka pyrkii ratkaisemaan energiankulutusongelman. PoS-mekanismissa tietokoneiden laskentaenergiaa kuluttava kilpailutus on korvattu valitsemalla satunnainen lohkoketjun osuuksien haltija *(eng. stake-holder)* uuden lohkon lisääjäksi lohkoketjuun. PoS-mekanismissa lohkoketjun osuuden haltijan todennäköisyys päästä lisäämään ketjuun uusi lohko kasvaa olemassa olevan omistusosuuden *(eng. stake)* mukaan. Tämä ei kuitenkaan lisää huijausten todennäköisyyttä, sillä lohkoketjua manipuloivalla tekijällä on riskinä menettää oma osuutensa lohkoketjusta. Vaikka PoS ratkaiseekin PoWin energiankulutusongelman, on sillä omat ongelmakohtansa: Koska lohkoketjun varmistamisen PoS-mekanismissa ei perustu suoriin kuluihin, on kynnys asettua ehdolle lohkon lisääjäksi samanaikaisesti useisiin lohkoketjun haaroihin matala, mikä voi haaroitustilanteessa *(eng. fork)* johtaa tyhjän osuuden ongelmaan *(eng. Nothing-at-Stake problem)*, jossa hyökkääjä saattaa voittaa haaran itselleen hyvinkin pienellä osuudella, kun muiden osuudet ovat pieniksi jakaantuneina useisiin eri haaroihin (Saleh 2017).

3 Lohkoketjuteknologian sovelluskohteita

ICT-alan konsulttiyhtiö Gartnerin vuosittain julkaistavan Nousevien teknologioiden kiinnostuksen kaari *(eng. Hype Cycle for Emerging Technologies)* -graafin mukaan vuonna 2017 lohkoketjuteknologia on lähestymässä inflatoituneiden odotusten huippua (eng. Peak of inflated expections), jonka aikana useat yritykset pyrkivät hyödyntämään teknologiaa, mutta toisaalta myös useat näistä yrityksistä epäonnistuvat, ja teknologia saa siten julkisuutta. Gartnerin arvion mukaan lohkoketjuteknologia saavuttaa tuotavuuden tason *(eng. Plateau of productivity)*, jolloin teknologia tunnetaan yleiseti ja sitä osataan hyödyntää tehokkaasti, noin 5-10 vuoden päästä. (Mukaillen kuvio 2)



Kuvio 2. Nousevien teknologioiden kiinnostuksen kaari. (Panetta 2017)

3.1 Lohkoketju 1.0: Valuutat

Kirjoitushetkellä Bitcoinin osuus kryptovaluuttamarkkinoista on 41.5%, mutta eri kokoisia kryptovaluuttaprojekteja on kehitteillä satoja, joiden joukkoon mahtuu hyvin erilaisiin tarpeisiin suunnattuja ratkaisuja, kuin myös huijauksia (*Cryptocurrency Market Capitalizations* 2018). Tällä hetkellä markkina-arvoltaan toiseksi suurin lohkoketju, vaikkakin ei alkujaan

ensisijaisesti kryptovaluutaksi tarkoitettu, Ethereum on avoimelle lähdekoodille perustuva hajautettu Turing-täydellinen alusta, joka on suunniteltu käytettäväksi erityisesti älysopimusten, mutta myös muiden lohkoketjusovellusten, kuten virtuallivaluuttojen, toteutuksissa. Ethereum eroaa muun muassa Bitcoinista siten, että se käyttää konsensusmekanisminaan Proof-of-Stake -mekanismia. Kolmanneksi suurimman markkina-arvon omaa tällä hetkellä erityisesti finanssialan tarpeisiin kehitetty Ripple. Antonopolouksen mukaan liikkeellä on myös vaihtoehtokolikoiksi *(eng. alt-coin)* kutsuttuja kryptovaluuttoja, jotka noudattavat pitkälti Bitcoinin toimintaperiaatteita, kuten esimerkiksi Bitcoinin 21 miljoonaan rajattua kolikoiden määrää, mutta parametrien arvoja muunnellen (2016). Yksi ensimmäisistä vaihtoehtokolikoista on vuonna 2011 julkaistu Litecoin, jonka haaroituksesta syntyi puolestaan Dogecoin vuonna 2013 (Antonopoulos 2014). Parametrien muunteluun perustuvien vaihtoehtokolikoiden lisäksi liikkeellä on myös valuuttoja, joiden konsensusmekanismit on suunniteltu uudestaan, sekä valuuttoja, joilla on tavoitteena olla muutakin kuin vain vaihdon väline. Esimerkiksi Curecoinin laskentatehoa hyödynnetään proteiinien simuloinnissa, kun taas osa säännöllisin väliajoin itsensä alustava CryptoNote pyrkii tarjoamaan käyttäjilleen entistäkin paremman anonymiteetin (Antonopoulos 2014).

3.2 Lohkoketju 2.0: Älysopimukset

Lohkoketjujen toisella sukupolvella viitataan lohkoketjujen hyödyntämiseen osana älykkäitä sopimuksia eli älysopimuksia (Swan 2015). Swanin (2015) mukaan älysopimuksella *(eng. smart contract)* tarkoitetaan kahden tai useamman osapuolen välistä itsestään toimivaa hajautettua sopimusta, jonka ehdot on kirjoitettu osaksi lohkoketjua, jolloin koodi toimii automaattisesti suorittaen ennalta määritellyt toimenpiteet sopimuksen ehtojen täyttyessä. Älysopimuksia voisivat hyödyntää niin yksityiset henkilöt kuin yrityksetkin. Älysopimusten avulla yksityisten henkilöiden olisi entistäkin helpompi solmia sopimuksia, kun sopimus voidaan vahvistaa ilman kolmatta osapuolta, joka on vielä nykyään useimmiten ulkopuolinen lainoppinut taho: "Havaintojemme perusteella näyttää siltä, että ainakin tietyn tyyppisten älykkäiden sopimusten välityksellä voidaan tehdä oikeustoimia. Sopimusten ja sopimuskulttuurin laajamittainen muutos on kuitenkin edessä yhteiskunnan digitalisaatiokehityksen kiihtyessä jatkuvasti."(Lauslahti, Mattila ja Seppälä 2016, 25). Erityisesti logistiikka-ala hyötyisi äly-

sopimuksista toimitusketjujen osana, mutta myös käyttöä olisi myös etenkin IoT-tekniikkaan yhdistettynä osana sähkö- ja kaupanalan toimitusketjuja. Lohkoketjuun perustuvassa toimitusketjussa jokainen verkon jäsen näkisi transaktion tapahtuneen, mutta vain transaktioon liittyvät osapuolet näkisivät sen datan yksityiskohtaisesti, jolloin virheiden tunnistaminen ja vastuun jäljittäminen helpottuu. Sen lisäksi, että kuljetusten turvallisuus lisääntyy vähentämällä mahdollista epärehellistä toimintaa, antaa läpinäkyvä toimitusketju kilpailukykyä myös eettisellä toiminnalla kilpailemiseen. (*Provenance: White Paper* 2015) Ethereumin lisäksi myös älysopimuksiin keskittyvä, Linux Foundationin alullepanema, Hyperledger on avoimeen lähdekoodin perustuva lohkoketjuprojekti, jonka tarkoituksena on toimia kattoterminä useille avoimen lähdekoodin lohkoketjusovelluksille (*About Hyperledger* 2018)

3.3 Lohkoketju 3.0: Muut sovellukset

Yksi kenties isoimmista lohkoketjukteknologian kolmannen aallon sovelluskohteista on tunnistautuminen, joka itsessään on laaja-alainen käsite, johon liittyy paljon vastuullista informaatiota ja oikeuksia. Tunnistautumalla voidaan turvata henkilön omistusoikeuksia liittyen muun muassa rahaan ja muuhun omaisuuteen, mutta tunnistautumisen taakse voidaan kätkeä muutakin henkilökohtaista tietoa, kuten henkilökohtaisia terveystietoja tai opintotodistuksia. Turvattua henkilökohtaista tunnistastumista tarvittaisiin myös esimerkiksi sähköistä äänestystä toteuttaessa, mutta turvallisesta tunnistautumisesta olisi hyötyä myös identiteettivarkauksilta suojautumisessa myös esimerkiksi sosiaalisessa medissa. Voitaisiin myös kysyä, voisiko lohkoketjuteknologia mahdollistaa tulevaisuudessa kenties selkärangan väestörekisteritasoiselle identiteettisuojalle henkilötunnuksen avulla ja jopa yhdistää eri alojen henkilötietokantoja selkeämmäksi kokonaisuudeksi. On myös huomioitava, että tunnistautumisella voidaan tunnistaa ihmisten lisäksi myös fyysistä että abstraktia omaisuutta; millaiset ovat lohkoketjuteknologian mahdollistamat keinot, joita voitaisiin hyödyntää esimerkiksi älysopimusten avulla omaisuuden ja korvausten vaihtaessaan omistajaa.

3.3.1 Alkuperän tunnistaminen

Elintarvikehuollon haasteisiin lukeutuvat ruoan turvallisuutta vaarantavat raaka-ainehuijaukset ovat viime vuosina yleistyneet etenkin kasvavilla talousalueilla, kuten Kiinassa: Hevosenli-

haa on myyty naudanlihana, kananmunia on valmistettu kemiallisesti ja maidonkorvikkeisiin on lisätty myrkyllisiä ainesosia (Tian 2016). Perinteisillä logistiikan keinoilla on vaikeuksia pysyä perässä alati kasvavilla markkinoilla, joten ratkaisuksi Tian (2016) ehdottaa lohkoketju- ja RFID-tekniikoita hyödyntävää toimitusketjun jäljitettävyysjärjestelmää. Tuotteiden alkuperän ja raaka-aineiden aitouden lisäksi jäljitettävyysjärjestelmällä voitaisiin seurata myös kylmäketjun katkeamattomuutta, mikä lisäisi entisestään ruoan turvallisuutta. RFID-tunnisteita käytetään jo yleisesti logistiikassa esimerkiksi tuotantoeläinten ja kuormalavojen tunnistamiseen, mutta ongelmana tutkimuksen mukaan laajemmassa käyttöönotossa jäljitettävyysjärjestelmien kehityksen suhteen on edelleen RFID-tunnisteiden hinta: RFID-tunniste maksaa edullisimmillaan 0,3 dollaria, kun taas tavallisen viivakoodin kustannukset Kiinassa on alle 0,01 dollaria. Tianin mukaan toinen merkittävä haaste liittyy lohkoketjuteknologian uutuuteen ja erityisesti ketjujen transaktioiden hitauteen.

Eräs eettisellä toiminnalla kilpaileva yritys on Provenance, jonka tarkoituksena on rakentaa tuotteiden toimistusketjujen ja elinkaaren läpinäkyvyyttä esiin tuova, lohkoketjua ja QR-skannausta hyödyntävä järjestelmä, pyrkimyksenään vastata kuluttajien kasvavaan kysyntään koskien tuotantoketjun läpinäkyvyyttä (*Provenance: White Paper* 2015). Lohkoketjuja voitaisiin soveltaa myös lääkkeiden aitouden todentamisessa ja siten lääkeväärennösten havaitsemisessa: lääkkeiden jäljittäminen on osa BlockRx-projektia, jonka tarkoituksena on luoda lohkoketjujärjestelmä yhdistämään terveydenhuollon tiedonkulkua (*BlockRx: White Paper* 2017).

3.3.2 Henkilöiden identifikaatio

Henkilötunnus ja väestörekisteri

Lohkoketjutietokantojen muuttumattomuutta ja hajautettuneisuutta voitaisiin hyödyntää identifikaatiossa ja maineenhallinnassa: Mattila & Seppälän (2016, 13) mukaan yleinen ongelma tämänhetkisessä digitaalisissa identifikaatiometodeissa on siinä, että nojaavat pitkälti luotettuihin välittäjiin todentaakseen identiteetin aitouden, jolloin välittäjällä on valta päättää sekä palvelumaksuista että siitä, mitkä palveluntarjoajat saavat käyttää identiteetinvarmennusta. Suomessa digitaalisen varmennuksen tarjoamisesta on tullut lähinnä rahoituslaitosten vas-

tuualuetta, jolloin jokaisen, joka haluaa tunnistaa itsensä digitaalisesti, täytyy antaa paljon enemmän informaatiota taloudellisesta tilanteestaan, kuin olisi todella tarpeen tunnistautumisen kannalta. Uudenlaisia tunnistautumisratkaisuja on kuitenkin jo kehitteillä: Bitnation on ensimmäinen projekti, joka lohkoketjuteknologiaan pohjautuen pyrkii tarjoamaan samoja palveluita kuin perinteiset hallitukset, mutta maailmanlaajuisesti hajautetusti. Bitnation on myöntänyt digitaalisia henkilötunnuksia vuodesta 2014, jonka jälkeen se on tarjonnut muun muassa notaaripalveluita sekä hätäapua pakolaisille. Vuodesta 2015 alkaen Bitnation on tehnyt yhteistyötä Viron hallituksen sähköisen oleskelulupaprojektin kanssa tarjoten luvanhaltioille mahdollisuuden tunnustaa Bitnationin palvelun avulla muun muassa syntymätodistuksia, avioliittoja, liiketoimintasopimuksia ja maanomistuksia (*Bitnation: Pangea White Paper* 2017)

Äänestäminen

"(Lohkoketju)teknologia on niin ikään hyvin soveltuva anonyymien, mutta julkisten tietokantojen luomiseen, jolloin esimerkiksi erilaisia sähköisiä äänestyksiä voitaisiin järjestää täysin läpinäkyvästi ilman, että äänestäjien anonymiteetti vaarantuu"(Mattila ja Seppälä 2015, 12). Joitakin sähköisen äänestyksen kokeiluja on tehty; muun muassa Tanskassa Liberty Partyn on uutisoitu käyttäneeneensä Bitcoin-lohkoketjuun perustuvaa sähköistä äänestystä puolueensa sisäisissä äänestyksissä. Mattila & Seppälän (2016, 17) mukaan sähköisten äänestysjärjestelmien rakentaminen on ongelmallista monimutkaisten neutraaliuden vaatimusten takia. Oikeudenmukaisten vaalien turvaamiseksi sähköisten äänestysjärjestelmien tulee pysyä anonyyminä ja väärentämiseltä suojattuna, mutta samalla tarkastuskelposena, mikä olisi toteutettavissa lohkoketjutekniikalla kryptovaluuttaa muistuttavalla järjestelmällä. Erona kryptovaluuttaan olisi kuitenkin se, että rahan sijasta transaktioissa siirrettäisiin äänestyslippuja. Koska lohkoketjun voi suunnitella julkiseksi, mutta anonyymeiksi, voivat äänestäjät tarkastaa äänen menneen perille samalla säilyttäen kuitenkin vaalisalaisuuden, mikä voisi auttaa vähentämään korruptiota ja vaalien manipulointia.

Sosiaalinen media

Sosiaalinen media on 2010-luvulla yhä kasvavissa määrin osana yhä useampien ihmisten arkea, ja eri palveluita löytyy erilaisiin tarpeisiin runsain mitoin. Sosiaaliset mediat käyttävät

taustallaan tietokantoja, joten voidaankin kysyä, voisiko lohkoketjuista olla hyötyä sosiaalisessa mediassa näkyviin ongelmiin, kuten häiriökäyttäytymiseen. Sekä sosiaalinen media että lohkoketjut ovat melko uusia innovaatiota, mutta jo nyt alalle on on syntynyt molempia edellä mainittuja yhdisteleviä projekteja, joista tällä hetkellä yksi isoimmista on Steem-tietokanta ja sen näkyvänä osana toimiva Steemit verkkosivusto. “Steem on lohkoketjutietokanta, jota tukee yhteisön rakentamista ja sosiaalista kanssakäymistä palkitsemalla kryptovaluutalla. Steemissä yhdistyvät eri sosiaalisten medioiden konseptit, kryptovaluuttojen ja niiden yhteisöjen rakentamisessa opittujen kokemusten pohjalta. Tärkeä osa yhteisön jäsenten osallistumisen motivoimiseen on reilu laskentasysteemi, josta näkee jokaisen henkilön tuoman työpanoksen. —” (Mukaillen *Steem: An incentivized, blockchain-based, public content platform.* 2017, 2) Steemin keskeisenä ajatuksena on siis luoda sisällöllisesti rikkaasta ja aktiivisesta käyttäjän tuottamasta sisällöstä palkitseva sosiaalinen media, jossa omaa näkyvyyttään voi jokainen nostaa itse omalla panoksellaan. Steemit-palvelun periaate on siis hyvin samanlainen perinteisiin blogi- ja sosiaalisen median uutispalveluihin verrattuna, mutta eroavana tekijänä on viestien tallennus lohkoketjuun, mikä mahdollistaa postauksista ja kommenteista palkitseminen kryptovaluutalla. Häiriökäyttäyminen puolestaan laskeen käyttäjän palkkioita, minkä voisi olettaa vähentävän sosiaalisessa mediassa yleistä häiriköintiä ja vihapuhetta. Rahallisten palkkioiden lisäksi Steemit-palvelussa on mahdollista äänestää ja kuratoida sisältöä, mutta tähän vaikutusvaltaan vaikuttaa käyttäjän maine palvelussa.

3.3.3 Omistusoikeudet

Lukuisista lahjoituksista ja kansallisista rahoitusprojekteista huolimatta pidemmän aikavälin maarekisterien toteutuksien onnistuminen kehittyvillä talousalueilla on ollut heikkoa. Maa- ja kiinteistörekisterit ovat kalliita kehittää sekä ylläpitää, ja ne vaativat asiantuntijoita hallinnointiin. Järjestelmien haasteiden lisäksi perustavanlaatuisen ongelmat kehittyvien maiden hallituksissa sekä virallisten tahojen vaikea tavoitettavuus etenkin köyhillä maaseuduilla vaikeuttavat tilannetta entisestään. (Anand, McKibbin ja Pichel 2016) Epävarmat maarekisterit voivat luoda korruptoituneille poliitikoille mahdollisuuksia siirtää kiinteistöjä haltuunsa muokkaamalla rekisterejä vilpillisesti (Lemieux 2016). Lemieuxin mukaan toinen nykyisiin maarekistereihin liittyvä ongelma on tietokantojen palvelimien elinkaarista riippuva lyhyti-

käisyys, vaikka tarve tiedon säilytykselle on pitkäaikainen. Tutkimustulosten mukaan lohkoketjutekniikkaa voidaan käyttää tietoturvatekijöihin liittyvissä kysymyksissä jo lähitulevaisuudessa, ja maailmanlaajuisesti muutamia projekteja on jo aluillaan: Hondurasissa on kehitteillä hallituksen aloitteesta Bitcoin-lohkoketjuun pohjautuva maarekisteriratkaisu yhdessä yhdysvaltalaisen Factomin kanssa, ja vastaavanalaisia projekteja on tekeillä myös muun muassa Georgiassa ja Ruotsissa (Shin 2017).

Henkilöidentiteetin ja tuotteiden tunnistamisen lisäksi lohkoketjuteknologiasta voi olla hyötyä myös abstraktien omistusoikeuksien takaamisessa tekijänoikeuksien muodossa: esimerkiksi muusikkojen tekijänoikeudellista asemaa voitaisiin parantaa yhdistämällä suoratoistopalveluihin lohkoketjuteknologiaa, ja näin mahdollistaa nopeat mikromaksut suoraan muusikoille soittokertojen mukaisesti, mikä olisi hyvinkin mullistavaa musiikkialalla sitten vertaisverkkotekniikan aiheuttamien mullistusten jälkeen (O'Dair 2016). Pro gradu tutkielmassaan Martén toteaa seuraavasti: "—lohkoketjuteknologia voisi mahdollisesti tarjota täydennystä DRM-teknologioihin (digitaaliset tekijänoikeuksien hallintajärjestelmät), tuoden jäljitettävyyttä, läpinäkyvyyttä, salausta sekä lohkoketjun tarjoama hajautettu tietokantamalli saattaisi mahdollistaa globaalin alustan digitaalisen musiikin sisällönhallinnalle" (Martén 2017, 3). Toisin sanoen, lohkoketjut voisivat tuoda ratkaisuja musiikkialalle internetin yleistymisen jälkeen yleistyneeseen musiikin vapaaseen jakeluun, ja sen myötä tuoda jälleen kohtuullisempia korvauksia suoraan musiikin tekijöille perinteisten levy-yhtiöiden sijaan. Musiikin lisäksi tekijänoikeudet ovat merkittävä tulonlähde myös muiden luovien alojen tekijöille, kuten kuvataiteilijoille ja valokuvaajille. Tällä hetkellä yrityksistä muun muassa Binded tarjoaa valokuvien omistusoikeuksien tallentamista, joka perustuu kuville luotujen tunnistetietojen tallentamiseen lohkoketjuun (*About Binded* 2018).

3.4 Yhteiskunnallinen näkökulma

Lohkoketjuteknologian mahdollisuuksia erityisesti suomalaisen yhteiskunnan kehityksen kannalta on käsitelty muun muassa useissa Elinkeinoelämän tutkimuslaitoksen ETLA-raporteissa. Erityisesti tutkijat Mattila ja Seppälä ovat käsitelleet lohkoketjuteknologiaa raporteissaan ja he ovat todenneet seuraavaa: "Lohkoketjuteknologia voikin mullistaa täysin teollisuuden ja yhteiskunnan digitalisaation ennakoidut ansaintalogiikat juuri siksi, että sen avulla älykkäät

komponentit voivat jakaa paljon muutakin kuin pelkkää dataa – esimerkiksi laskentatehoa, tallennustilaa, kaistanleveyttä tai vaikkapa energiaa" (Mattila ja Seppälä 2015, 9). "Avoimuutensa sekä luotettavuutensa johdosta lohkoketjuteknologialla voitaisiin myös merkittävästi parantaa julkishallinnon ohjautuvuutta, mikä osaltaan edesauttaisi kustannusrakenteen keventämistä julkisella sektorilla" (Mattila ja Seppälä 2015, 12). Lisäksi, yhtenä kattavimmista kotimaisista lohkoketjuteknologian käyttökohteita tutkineesta raporteista voisi mainita Petri Honkasen raportin "Lohkoketjuteknologian lupaus", jossa Honkanen esittelee laajasti lohkoketjuteknologian mahdollisuuksia ja jo olemassa olevia sovelluskohteita (Honkanen 2017).

3.4.1 Koulutussektori

Tutkijoiden Sharples ja Dominguen mukaan lohkoketjuteknologialla on tarvittavat ominaisuudet tullakseen sovelletuksi myös koulutussektorilla, erityisesti tehdyn älyllisen työn todistamissa (eng. Proof of intellectual work), sillä lohkoketjussa kaikki tallennettu data on julkisesti saatavilla, mutta luettavissa ainoastaan digitaalisilla avaimilla, samalla kuitenkin hajautetusti varmuuskopioituna. Arvosanojen tallennusrekisterien tarpeisiin lohkoketjuteknologia sopii erityisen hyvin, koska kaikki lisäykset voidaan identifioida, mutta jo tallennettua tietoa, eli tässä tapauksessa arvosanoja ja työtodistuksia, ei voi enää jälkikäteen muuttaa. (Sharples ja Domingue 2016) Julkinen ansio- ja arvosanaluettelo selkeyttäisi muun muassa työnhakijoiden sekä opiskelemaan pyrkivien hakuprosesseja keskittämällä datan sijaintia.

Ajatus maailmanlaajuisesta digitaalisesta sähköisen julkaisemisen tallennuspaikasta on ollut olemassa jo 60-luvulta lähtien, mutta riittävää tekniikkaa ei ole ollut olemassa ongelmiin, jotka akateemisessa yhteisössä on perinteisesti ratkaistu tieteentekijöiden välisellä vertaisarvioinnilla. Lohkoketjuteknologian myötä vertaisarvioinnista voitaisiin tehdä julkisempaa ja helpompaa: rahavaluutan sijaan instutioiden ja yksityishenkilöiden suorittamina transaktioina voisi siirtyä jo valmiiksi akateemisessa maailmassa tavoiteltua valuuttaa, arvostusta *(eng. kudos)*. Korkeakouluista Nikosian yliopisto Kyproksella myöntää joakateemiset todistuksensa Bitcoin-lohkojen kautta todennettavina, ja Sony Global Education on ilmoittanut kehittävänsä lohkoketjua opintopisteiden tallentamista varten. (Sharples ja Domingue 2016) Myös muualla on kehitteillä lohkoketjuratkaisuja koulutusalan tarpeisiin: muun muas-

sa Glasgow'n yliopistossa on kehitty Ethereumin pohjalle toteutettua opintopisteiden talletusrekisteriä (Rooksby ja Dimitrov 2017).

3.4.2 Terveydenhuolto

Lohkoketjuun perustuva, jatkuvasti ajan tasalla oleva hajautettu tietokanta tuo monia etuja myös terveydenhuoltosektorille, jossa useilla eri osapuolilla on tarve päästä käsiksi samoihin tietoihin. Nykyisin potilaan hoitoon osallistuvien useiden eri yksikköjen käyttämät yhteensopimattomat rajapinnat ja viestintävälineet voivat johtaa itse hoidolta aikaa ja resursseja pois vieviin autentikaatioprosesseihin (Mettler 2016). Ongelmaan on kuitenkin kehitteillä lohkoketjuteknologiaan pohjautuvia ratkaisuja, sillä lohkoketju tarjoaa useita sovellusmahdollisuuksia hyödynnettäväksi potilaslähtöisen terveysdatan käsittelyssä: muun muassa yhdysvaltalainen startup-yritys Gemin kehittämä Gem Health Network on Ethereum-lohkoketjuteknologiaan perustuva kokonaisvaltainen terveydenhuoltosektorille suunnattu tiedonhallintaratkaisu, kun taas svetsiläinen startup Healthbank on lähestynyt samaa ongelmaa potilaslähtöisemmästä näkökulmasta kehittämällä potilastietokannanhallintaa niin, että potilas itse pääsee vaikuttamaan tietojensa näkyvyyteen ja hyödyntämiseen. Valtiollisen infrastruktuurin tasolla Viro on yhtenä ensimmäisistä maista ottanut käyttöön lohkoketjuteknologiaan pohjautuvan digitaalisen terveydenhuoltojärjestelmän, johon pääsevät käsiksi niin kansalaiset, terveydenhuollon ammattilaiset kuin myös vakuutusyhtiöt. (Mettler 2016)

3.4.3 Finanssisektori

Tutkijoiden Sharples ja Domingue mukaan maine *(eng. reputation)* on uuden digitaalisen talouden perusta, jota edustavat esimerkiksi yritykset AirBnB ja Über, jotka molemmat rakentavat luottamusta käyttäjiensä arvioihin ja arvosteluihin perustuen (Sharples ja Domingue 2016). Nykyiset uudet tekniikat muuttavat myös taloutta luomalla täysin uusia markkinoita ja tapoja hallita rahavirtoja, mutta myös konservatiisisena pidetyn pankkialan, on sopeuduttava muutokseen. Yhdysvaltalaisen suurpankin JP Morgan Chasen entisen toimitusjohtajan Blythe Mastersin mukaan lohkoketjutekniikka pitäisi ottaa yhtä vakavasti kuin internetin kehitys 1990-luvun alussa (Robinson ja Leising 2015). Vaikka kryptovaluuttojen kehitys voidaan nähdä vastareaktiona perinteiselle keskitetylle pankkimallille häivyttämällä valuutansiirtoja

älysopimuksien ja IoT-sovelluksien avulla, myös jo olemassa olevat pankit ovat kiinnostuneita uudesta tekniikasta. Lohkoketjutekniikkaa voitaisiinkin soveltaa muun muassa pankkien välisiin tilisiirtoihin. Nykyisen pankki-infrastruktuurin rajoitukset pakottavat käsittelemään maksut erissä, mikä johtaa korkeisiin prosessointikustannuksiin, pitkiin toimistusaikoihin ja huonoihin asiakaskokemuksiin (*Ripple: Solution Overview* 2018). Erityisesti pankkien tarpeisiin kehitetty Ripple saattaa olla olla vastaus hitaisiin rahasiirtoihin, tarjoamalla pankeille tehokkaamman tavan siirtää rahaa toisen pankkien, yritysasiakkaiden ja kuluttajien välillä.

3.4.4 Energiasektori

Lohkoketjuteknologian edut, kuten verkon hajautettuneisuus ja älykkäät sopimukset, saattavat muuttaa myös energiasektorin toimintaa mahdollistaen älykkäiden sähköverkkojen synnyn. Sähköverkot ovat toimineet historiansa alusta alkaen hieman pankkien toimintaa muistuttavalla, sähkövoimaloiden ympärille keskittyneellä keskitetylläsähköverkolla, jossa sähköyhtiö myy yksisuuntaisesti sähköä kuluttajille. Perinteinen tapa myydä sähköä ei ole kuitenkaan enää toimivin ratkaisu ekologisen ajattelun ja sen myötä uusiutuvien energiantuotantotapojen lisääntyessä. Älykäs sähköverkko on myös korjaustoimenpiteiden kannalta joustavampi ratkaisu ja sen modulaarisuus vähentää koko sähköverkon kaatumisen riskiä, etenkin jos tällaiseen verkkoon yhdistettäisiin ylijäämäenergian varastointi akkuihin. Talouden kannalta älykkäät sähköverkot avaavat energiamarkkinoita etenkin pienyrityksille ja lisäävät kilpailua etenkin uusiutuvien energiantuotantomuotojen markkinoilla. (Meyer 2016) Toisin sanoen, käytännön etuna hajautetun mallin sähköverkossa olisi muun muassa etenkin toimintavarmuuden lisääntyminen, kun verkko ei ole enää täysin riippuvainen keskussolmukohdan, eli yksittäisen sähkönjakelijan, toiminnasta. Lisäksi älykkäät sähköverkot mahdollistaisivat yhdistettynä esineiden internetiin kuluttajien aurinkopaneelien tuottaman ylijäämäsähkön myynnin toisille kuluttajille. Edellä mainittu peer-to-peer malli vähentäisi myös sähkönsiirron häviöitä, ja mahdollistaisi kuluttajille paremmat korvaukset sähkönmyynnistä.

Kehitys ei ole kuitenkaan jäänyt pelkän teorian tasolle, sillä muun muassa yhdysvaltalainen yritys LO3 kehittää mikroälyverkkoja erilaisiin tarpeisiin ympäri maailmaa. Kehitteillä on älyverkkoratkaisuja sekä tiheästi asutun New Yorkin Brooklynin kaupunginosan tarpeisiin, että harvaan asuttuun Etelä-Australiaan (*LO3 Energy: Innovations* 2018). Kaupallisten

projektien lisäksi lohkoketjutekniikaa on alettu myös soveltamaan hyväntekeväisyyteen, sillä lohkoketjut mahdollistavat suoran lahjoittamisen ilman välikäsiä: Yhdysvaltalainen yritys Bankymoon on kehittänyt yleisörahoitteisen hyväntekeväisyysprojektin asentamalla afrikkalaisiin kouluihin älykkäitä vesi-ja sähkömittareita, joiden kautta kuka tahansa voi osallistua auttamiseen lähettämällä rahaa suoraan mittareihin, ja samalla varmistua siitä, että apu menee suoraan apua tarvitseville (*Bankymoon: Social projects* 2018).

Myös Suomessa on kehitteillä erinäisiä lohkoketjusovelluksia osana tutkimusprojekteja sen energiasektorin tarpeisiin: yhtenä mainittavimmista kenties Aalto-yliopiston, ETLA:n ja Fortum Oyj:n yhteistyönä kehittämä Ethereum-lohkoketjua hyödyntävä sovellus, jonka avulla yksittäiset toimijat voisivat ostaa ja myydä sähköä ilman nykymuotoista keskitettyä markkinamekanismia. Ennen kaikkea kyseisen sovelluksen kehittämisessä on kuitenkin on ollut tavoitteena selvittää, voidaanko älykkäitä sopimuksia hyödyntää kuvatun kaltaisissa sovelluksissa teollisuudessa ja yhteiskunnassa laajemmin. (Mattila ym. 2017) Kyseinen tutkimus ei ollut kuitenkaan ensimmäinen laatuaan, sillä samaiset edellä mainitut kolme toimijaa olivat julkaisseet tuloksiaan jo aiemmin vuonna 2016 ETLA-raportissa, jossa käsiteltiin alustavasti lohkoketjua käyttötapauksena energiasektorin autonomisissa sähkökaupoissa käytännöllisestä näkökulmasta (Mattila ym. 2016, 2016).

4 Ongelmakohdat ja haasteet

4.1 Teknologiset haasteet

Swanin (2015) mukaan suurimpia lohkoketjuteknologiaan liittyvistä teknisistä haasteista suurimmat ovat suoritusteho, koko ja viive. Tällä hetkellä Bitcoin voi suorittaa 7 transaktiota/sekunti, kun taas VISA käsittelee 2000 transaktiota/sekunti. Kirjoitushetkellä yhden Bitcoin-lohkon transaktion varmentamiseen menee 10 minuuttia, mutta riittävä turvallisuus saavutetaan vasta tunnin kuluttua. Lisäksi Bitcoin-lohkoketjun koko on nyt 25 Gt, mutta sen koko kasvaa jatkuvasti lohkoketjun laajentuessa. Vaikka 25 Gt on nykyisellä big datan aikakaudella melko pieni luku, se vaikeuttaa saavutettavuutta. Toisaalta, edellä mainitut ongelmakohdat ovat Swanin mukaan Bitcoiniin keskittyneitä, ja ongelmakohtiin voitaisiinkin löytää ratkaisuja siirtymällä käyttämään muita lohkoketjuratkaisuja. Suurimpana turvallisuusuhkana Swan mainitsee 51%-hyökkäyksen, mutta myös muita turvallisuusuhkia on tuotu esiin tutkimuksissa: Lin & Liaon mukaan (2017) 51%-hyökkäyksen ohella suurimmat turvallisuusriskit liittyvät haaroitukseen liittyviin erimielisyyksiin. Swanin mukaan teknisten ongelmakohtien lisäksi haasteita lohkoketjuteknologian käyttöönotossa voi tulla esiin muun muassa niin liiketoimintamallien sovittamisessa uuden teknologian ympärille, kuin käyttäjien hyväksynnän saannissa. Huolimatta useista kiinnostavista potentiaalisista lohkoketjun käyttökohteista, yksi tärkeimmistä taidoista kehittyvällä alalla on nähdä milloin kryptovaluuttojen ja lohkoketjumallien käyttö on järkevää, sillä kaikki prosessit eivät tarvitse maksusysteemiä, vertaisverkkoa, hajauttamista tai julkista kirjanpitoa (Swan 2015).

Yleisimmät internetin ja finanssitransaktioiden varmistamiseen käytetyt salaustekniikkaprotokollat ovat uhattuina, kun riittävän tehokas kvanttitietokone saadaan kehitettyä. Kryptovaluuttamarkkinat, joiden tämän hetkinen arvo on yli 150 miljardia dollaria, ovat tällöin erityisen uhattuna. Aggarwal ym. (2017) arvion mukaan Bitcoinin käyttämä PoW-mekanismi on suhteellisen vastustuskykyinen kvanttitietokoneiden kehitykseen suhteutettuna seuraavan kymmenen vuoden ajan, mutta Bitcoinin käyttämä elliptisen käyrän allekirjoitusmenetelmä *(eng. elliptic curve signature scheme)* on sitäkin suuremmassa riskissä, ja optimististen arvioiden mukaan kvanttitietokoneen tuhottavissa aikaisintaan vuonna 2027.

4.2 Julkisen vallan sääntely ja rikollisuus

Jotta teknologiaa voitaisiin soveltaa valtiollisen tason infrastruktuuriin, tarvitaan monin paikoin muutoksia lainsäädäntöön, sillä useimmat nykyiset lait ovat suunniteltu perinteisen tietokantarakenteen pohjalle. Esimerkiksi terveydenhuoltosektoriin kuuluvassa sosiaali- ja terveydenhuollon asiakastietojen sähköistä käsittelyä koskevassa laissa todetaan seuraavaa: "Asiakastietojen käyttäjien käyttöoikeustiedot ja lokitiedot tulee hävittää, kun ne eivät enää ole tarpeen asiakastietojen käytön ja luovutuksen lainmukaisuuden seuraamiseksi." (L159/2007, 5§). Tämä ei kuitenkaan ole mahdollista lohkoketjussa, koska siitä ei voida jälkikäteen poistaa dataa ilman koko lohkoketjun tuhoamista. Lisäksi samaisen lain edeltävässä artiklassa todetaan: "Sähköisestä asiakasasiakirjasta tulee olla vain yksi alkuperäinen tunnisteella yksilöity kappale." (L159/2007, 4§). Koska lohkoketjut ovat hajautettuja tietokantoja, olisi sellaiseen perustuva potilastietokanta ristiriidassa kyseisen lain kanssa. Sen lisäksi, että lainsääntäntö voi olla rajoittavana tekijänä teknolopgiaa hyödyntävien ratkaisujen käyttöönotossa, on myös huomioitava vielä kirjoitushetkellä merkittävimmän sovelluskohteen, kryptovaluuttojen, sääntelytilanne maailmalla: Muutamat valtiot ovat kieltäneet Bitcoinin, kun taas Kiina on kieltänyt virtuaalivaluutat kokonaan. Useat maat yrittävät sovittaa kryptovaluuttoja jo olemassa olevaan sääntelyyn, mutta tilanne vaihtelee valtioittain. (Swan 2015)

Vaikka uusiin teknologioihin liittyy usein yhteiskuntaa yleisesti hyödyntäviä tekijöitä, on huomioitava, että myös rikollisuus adaptoi niitä käyttöönsä. Lohkoketjuteknologian ensimmäisen aallon, kryptovaluuttojen, tarjoama käyttäjän anonymiteetti on tehnyt siitä houkuttelevan vaihtoehdon etenkin rahanpesuun ja laittomaan kauppaan, mutta myös muihin kyberrikoksiin. Poliisi Steven Brownin mukaan lainvalvonta on jo tunnustanut nämä mahdollisuudet, mutta laajamittaista kryptovaluuttoihin liittyvää toimintaa ei ole vielä havaittu. Brownin mukaan tämä voi johtua valuuttoihin liitettävän teknisen osaamisen ja resurssien puutteesta. Toinen mahdollisuus on, että kryptovaluuttoja hyödynnetään jo laajamittaisesti rikollisuudessa, mutta se ei näy vielä kokonaisuudessaan rikosoikeudellisille tahoille (Brown 2016).

Hass McCookin mukaan fiat-valuuttat ovat edelleen ehdottomasti merkittävimpiä vaihdon välineitä sosioekonomisten kulujen, kuten korruption, rahanpesun ja mustien markettien suhteen. Laittomilla marketeilla liikkuu fiat-rahaa biljoonia dollareita; pelkästään rahanpesussa arviolta 2,65 biljoonaa dollaria. Kullan merkitys laittomien markettien vaihdon välineenä

on jo huomattavasti pienempi, vain 600 miljoonaa dollaria. McCook arvio Bitcoinin merkityksen kaikilla edellä mainituilla osa-alueilla merkityksettömän pieneksi. Bitcoinin historian suurin institutionaalinen petos oli Mt Gox -kryptovaluuttapörssin kaatuminen vuonna 2014 omistajien varastaessa käyttäjiensä Bitcoineja vajaan puolen biljoonan dollarin arvosta. Istitutionaalisiin huijauksiin liittyvä vastaava luku fiat-valuutalla on 3800 biljoonaa dollaria vuodessa. (Kuvio 3)

Comparison of Annual Economic Costs

	Gross Yearly Cost
Gold Mining	USD$105 billion
Gold Recycling	USD$40 billion
Paper Currency & Minting	USD$28 billion
Banking System Electricity Use	USD$63.8 billion
Banking System (All Expenses)	USD$1870 billion
Bitcoin Mining	USD$0.79 billion

Comparison of Annual Environmental Costs

	Energy Used (GJ)	Tonnes CO_2 Produced
Gold Mining	475 million	54 million
Gold Recycling	25 million	4 million
Paper Currency & Minting	39.6 million	6.7 million
Banking System	2340 million	390 million
Bitcoin Mining	3.6 million	0.6 million

Comparison of Annual Socioeconomic Costs

	Gold	Fiat Currency	Bitcoin
Worker Deaths	Over 50,000 historically recorded & Over 100 per year	0	0
Corruption	USD$600m	USD$1.60 trillion	Negligible
Money Laundering		USD$2.65 trillion	
Black Markets		USD$1.80 trillion	
Institutional Fraud / Theft	USD$21 billion across two single events & several billion historically recorded	USD$3800 billion/year & several trillion historically recorded	< USD$0.5 billion ever recorded
Transactional Fraud	N/A – all historical use of counterfeit gold	$190 billion	$0
Inflation	Deflationary (Long-term)	3.9% per year (*time to loss of 50% loss of value: 17.5 years*)	Deflationary (Long-term)

Kuvio 3. Bitcoinin kulut pankkialaan verrattuna. (McCook 2014, 1)

4.3 Eettiset kysymykset

4.3.1 Yksityisyys

Datan määrä maailmassa lisääntyy nopeasti kasvavissa määrin, joten myös yleiset huolenaiheet käyttäjien yksityisyyteen liittyen ovat entistäkin ajankohtaisempia. Arviolta 20 prosenttia kaikesta maailman datasta on kerätty viimeisten muutamien vuosien aikana. Facebook on kerännyt perustamisesta lähtien 300 petatavua henkilökohtaista dataa, mikä on satakertainen

määrä Yhdysvaltain kansalliskirjaston Kongressin kirjaston viimeisen 200 vuoden aikana keräämään dataan. Nykyään vallitsevalla big datan aikakaudella data on arvokas osa talouttamme. (Zyskind, Nathan ja Pentland 2015) Zyskind, Nathan ja Pentlandin mukaan henkilökohtaista dataa ei tulisi uskoa kolmannen osapuolen haltuun, vaan dataa tulisi voida hallita itse, turvallisuutta vaarantamatta: Tähän tarkoitukseen ollaan luomassa Enigma protokollaa, jossa itse sopimus toimii hajautetussa vertaisverkossa piilossa julkisuudesta (*Enigma's Ambition—Our Latest Roadmap* 2018).

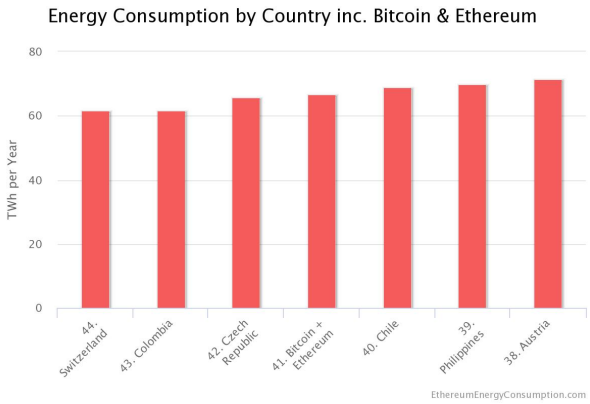
Yleisesti ottaen lohkoketjuissa data näkyy vain avainten haltijoille, transaktioiden tapahtuminen yleisesti kaikille verkon jäsenille, eli toisin sanoen vaikka ketju olisi julkinen, yksityinen data pysyy salaisena ellei käyttäjällä ole hallussaan dataa sisältävän lohkon avainta. Turvallisuutta voidaan parantaa myös tekemällä lohkoketjusta yksityinen, jolloin edes transaktiot eivät näy ulkopuolisille. Riskinä on edelleen yksityisten avaimien menetys, joka voi johtaa identiteettivarkauteen, samaan tapaan kuin tavallisen salasanankin kohdalla. Lin ja Liaon (2017) mukaan yksi lohkoketjujen avainominaisuuksista on mahdollistaa transaktioiden anonymiteetti käyttäjilleen.

Lohkoketjuista voi olla hyötyä erityisesti IoT-laiteiden yksityisyyden ja tietoturvan parantamisessa: Älykotien IoT-turvallisuuteen perehtyneessä tapaustutkimuksessa kehitetty Bitcoin-lohkoketjuun perustuvan metodi mahdollisti tutkimuksen mukaan huomattavia etuja liittyen tietoturvaan ja yksityisyyteen, samalla kuitenkin tarjoten perinteisiin IoT-tietoturvaratkaisuihin verrattain alhaiset kiinteät kustannukset (Dorri, Jurdak ja Kanhere 2017). Nykyiset tietoturvaratkaisut eivät välttämättä sovellu IoT-ratkaisuihin niiden korkean energiankulutuksen ja prosessointikustannuksien takia, sillä IoT-laitteet eivät tarjoa tarpeeksi resursseja.

4.3.2 Louhinnan ympäristövaikutukset

Bitcoin ja Ethereum, joka vastaa vajaata kolmasosaa Bitcoinin kulutuksesta, yhdistettynä kuluttavat energiaa keskikokoisen valtion verran; kulutus on tällä hetkellä 71.16TWh vuodessa, mikä on vain hieman enemmän kuin Filippiinien sähkönkulutus (Kuvio 4). Hass McCookin (2014) raportissa vertailtiin pankkisysteemiä Bitcoinin louhimiseen, huomioiden niiden taloudelliset ja sosioekonomiset kulut, sekä ympäristön kuormituksen. Raportin mu-

kaan Bitcoinin louhinnan aiheuttamat kulut ovat vielä pieniä: perinteisen pankkisysteemin kaikiksi taloudellisiksi kuluiksi maailmanlaajuisesti arvioitiin 1870 miljardia dollaria, kun taas Bitcoinin kuluiksi arvioitiin 790 miljoonaa dollaria. Lähimmäksi kuluarviossa Bitcoinia jäi käteisen painamisesta kertyvät kulut, joiksi arvioitiin 28 miljardia dollaria. Tutkimuksessa otettiin huomioon myös energiankulutus ja hiilijalanjälki: pankkisysteemin kokonaishiilijalanjäljen arvioitiin olevan noin 390 miljoonaa tonnia hiilidioksidia, kun taas Bitcoinin hiilijalanjälki jäi 0,6 miljoonaan tonniin. (Kuvio 3) Jos lohkoketjuteknologian avulla onnistutaan tehostamaan finanssi- ja pankkisektorin toimintaa, on tämä etenkin ympäristön kannalta merkittävää. Lisäksi energiasektorilla kehitettävät lohkoketjusovellukset voivat edistää uusiutuvien energiamuotojen käytön lisääntymistä älykkäiden sähköverkkojen myötä, mikä laajemmin katsottuna voi parantaa tuotantoketjun hiilijalanjälkeä.



Kuvio 4. Bitcoinin ja Ethereum energiankulutus valtioihin verrattuna. (Vries 2018)

Useissa tutkimuksissa on tuotu esille ideoita siitä, että suurta laskentatehoa konsensusmekanisminaan käyttävät lohkoketjut voitaisiin laittaa laskemaan jotain hyödyllistä, esimerkiksi alkulukuja: Primecoin kryptovaluutan lohkoketju perustuu Proof-of-Workiin, mutta sen tarkoituksena on lohkoketjun itsensä turvaamisen lisäksi laskea samanaikaisesti Cunninghamin ketjuun kuuluvia alkulukuja matematiikan tutkimuksen tarpeisiin (King 2013). Lisäksi syntyvä hukkalämpö voitaisiin ottaa serverihallien tapaan hyötykäyttöön lämmityksessä. Ensisijaisesti teknologian energiatehokkuuden parantamisessa tulisi kuitenkin siirtyä käyttämään Proof-of-Stakea. Lisäksi, yksityiset lohkoketjut saattaisivat vähentää Proof-of-Work mekanismia käyttävän louhinnan tarvetta rajoittamalla lohkoketjuun pääsyä ulkopuolisilta tahoilta.

5 Yhteenveto

Laajasti määriteltynä keskeisimpiä tutkimuskysymyksiä ovat kysymykset siitä, miten lohkoketjuteknologiaa voitaisiin soveltaa yhteiskunnan eri osa-alueiden kehittämisessä, millaisiin käytännön ongelmiin lohkoketjuteknologia voisi tuoda ratkaisuja, ja kuinka teknologiaa olisi tällöin hyödynnettävä. Lohkoketjujen avainetuna on niiden muuttumattomuus, hajautettavuus, mutta ennen kaikkea läpinäkyvyys. Viimeksi mainittu tiedon läpinäkyvyys lisää yleistä luotettavuutta ja nopeuttaa tiedon vapaata kulkua. Tutkielmassani keskiössä ovat kysymykset siitä, voisiko lohkoketjuista olla ratkaisuksi yleiseen luottamuspulaan ja jopa byrokratian vähentämiseen erityisesti tunnistautumiseen ja omistusoikeuksiin liittyvissä kysymyksissä. Yhteenvetona tutkielmani pohjalta voisi sanoa, että lohkoketjuteknologialla on paljon potentiaalia osana abstraktin omaisuuden, kuten esimerkiksi identiteetin, tekijänoikeuksien ja energian, todentamisessa, mutta tarvitaan lisää aiheeseen paneutuvia tutkimusprojekteja. Yllättävänä näkökulmana kirjallisuuskatsauksessa nousi esille lohkoketjuteknologian mahdollinen potentiaali tulla hyödynnetyksi hyväntekeväisyys- ja avustustyössä; lohkoketjuteknologian mahdollistaman läpinäkyvyyden, ja sen myötä luotettavuuden, avulla avustuksien päätyminen suoraan apua tarvitseville voitaisiin varmistaa entistä luotettavammin ilman kolmansia osapuolia.

On otettava myös huomioon toteutuksen haasteet; itse teknologian kohtaamisen ongelmien lisäksi on huomioitava myös yhteiskunnalliseen näkökulmaan ja etenkin yksityisyydensuojaan liittyvät eettiset ongelmakohdat. Suoraan lohkoketjuteknologiaan liittyvinä ongelmina voidaan mainita muun muassa lohkoketjujen skaalaatuvuusongelma, johon liittyy oleellisesti huoli ketjujen hidastumisesta mutta myös energiankulutuksen lisääntymisestä; kuka louhinnasta lopulta vastaa? Tulevissa tutkimuksissa olisi lisäksi hyvä pohtia, millaisia uusia skenarioita hyötyineen ja uhkakuvineen uudistukset toisivat mukanaan. Lisäksi muita kiehtovia kysymyksiä liittyen lohkoketjuteknologian mahdollisuuksiin on runsaasti; muun muassa tekoälyn ja neuroniverkkojen hyöndyntäminen yhdistettynä lohkoketjuteknologiaan voi avata vielä tässä vaiheessa tutkimattomia ovia täysin uudenlaisiin ongelmiin ja ratkaisuihin.

Lähteet

About Binded. 2018. https://binded.com/about.

About Hyperledger. 2018. https://www.hyperledger.org/about.

Aggarwal, Divesh, Gavin K. Brennen, Troy Lee, Miklos Santha ja Marco Tomamichel. 2017. "Quantum attacks on Bitcoin, and how to protect against them".

Anand, Aanchal, Matthew McKibbin ja Frank Pichel. 2016. "The 17th Annual World Bank Conference on Land and Poverty". Teoksessa *Colored Coins: Bitcoin, Blockchain, and Land Administration.* Washington DC.

Antonopoulos, Andreas M. 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* O'Reilly Media, Inc.

Bankymoon: Social projects. 2018. http://bankymoon.co.za/social-projects/.

Bayer, Dave, Stuart Haber ja W. Scott Stornetta. 1992. "Improving the Efficiency and Reliability of Digital Time-Stamping".

Bitnation: Pangea White Paper. 2017. https://tse.bitnation.co/documents/.

BlockRx: White Paper. 2017. https://www.blockrx.com/white-paper/.

Brown, Steven David. 2016. "Cryptocurrency and criminality: The Bitcoin opportunity". 89 (The Police Journal: Theory, Practice and Principles 4): 327–339.

Cryptocurrency Market Capitalizations. 2018. https://coinmarketcap.com/.

Dorri, Ali, Raja Jurdak ja Salil S. Kanhere. 2017. "Blockchain for IoT security and privacy: The case study of a smart home". Kona, HI, USA. doi:10.1109/PERCOMW.2017.7917634.

Enigma's Ambition—Our Latest Roadmap. 2018. https://blog.enigma.co/enigmas-ambition-our-latest-roadmap-8d50107ad314.

Honkanen, Petri. 2017. *Lohkoketjuteknologian lupaus.* Tekninen raportti 1. Arcada Working Papers.

Huoltovarmuuskeskus. *Toimialat.* https://www.huoltovarmuuskeskus.fi/toimialat/.

King, Sunny. 2013. "Primecoin: Cryptocurrency with Prime Number Proof-of-Work". https://bravenewcoin.com/assets/Whitepapers/primecoin-paper.pdf.

Kostarev, Gleb. 2017. *Review of blockchain consensus mechanisms.* https://blog.wavesplatform.com/review-of-blockchain-consensus-mechanisms-f575afae38f2.

L159/2007. *Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä.*

Lauslahti, Kristian, Juri Mattila ja Timo Seppälä. 2016. *Älykäs sopimus – Miten blockchain muuttaa sopimuskäytäntöjä?* Tekninen raportti 57. Elinkeinoelämän tutkimuslaitos. https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-57.pdf.

Lemieux, Victoria Louise. 2016. "Trusting records: is Blockchain technology the answer?" 26 (Records Management Journal 2): 110–139.

Lin, Iuon-Chang, ja Tzu-Chun Liao. 2017. "A Survey of Blockchain Security Issues and Challenges". 19 (International Journal of Network Security No.5): 653–659.

LO3 Energy: Innovations. 2018. https://lo3energy.com/innovations/.

Martén, Meiss. 2017. "Digital rights management - blockchain and digital music content management". Tutkielma.

Mattila, Juri, Taneli Hukkinen, Juuso Ilomäki ja Timo Seppälä. 2017. *A Blockchain Application in Energy.* Tekninen raportti 71. Elinkeinoelämän tutkimuslaitos.

Mattila, Juri, ja Timo Seppälä. 2015. *Laitteet pilveen – vai pilvi laitteisiin? Keskustelunavauksia teollisuuden ja yhteiskunnan digialustojen uusista kehitystrendeistä.* ETLA 44. Elinkeinoelämän tutkimuslaitos.

Mattila, Juri, Timo Seppälä, Catarina Naucler, Riitta Stahl, Marianne Tikkanen, Alexandra Bådenlid ja Jane Seppälä. 2016. *Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry.* ETLA 43. Elinkeinoelämän tutkimuslaitos.

Mazieres, David, ja Dennis Shasha. 2002. Teoksessa *Building secure file systems out of Byzantine storage,* 108–114.

McCook, Hass. 2014. "An Order-of-Magnitude Estimate of the Relative Sustainability of the Bitcoin Network". https://www.academia.edu/7666373/An_Order-of-Magnitude_Estimate_of_the_Relative_Sustainability_of_the_Bitcoin_Network_-_3rd_Edition.

McKinsey ja Company. 2017. *Blockchain Technology in the Insurance Sector.* Tekninen raportti. https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf.

Merkle, Ralph C. 1980. "A Digital Signature Based on a Conventional Encryption Function", 369–378.

Mettler, M. 2016. "Blockchain technology in healthcare: The revolution starts here". Teoksessa *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom),* 1–3. ID: 1.

Meyer, Andrew. 2016. "Why a Distributed Energy Grid is a Better Energy Grid". 2018 (3/5). www.swellenergy.com/blog/2016/05/20/why-a-distributed-energy-grid-is-a-better-energy-grid.

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system". http://bitcoin.org/bitcoin.pdf.

O'Dair, Marcus. 2016. *Music On The Blockchain Blockchain For Creative Industries Research Cluster.* Tekninen raportti Report N^{o} 1. Middlesex University.

Panetta, Kasey. 2017. "Top Trends in the Gartner Hype Cycle for Emerging Technologies". https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/.

Provenance: White Paper. 2015. https://www.provenance.org/how-it-works.

Ripple: Solution Overview. 2018. https://ripple.com/files/ripple_solutions_guide.pdf.

Robinson, Edward, ja Matthew Leising. 2015. “Blythe Masters Tells Banks the Blockchain Changes Everything”. *Bloomberg* 2018 (3/9).

Rooksby, John, ja Kristiyan Dimitrov. 2017. “Trustless Education? A Blockchain System for University Grades”. Edinburgh.

Saleh, Fahad. 2017. “Blockchain Without Waste: Proof-of-Stake”. New York University, Stern.

Sharples, Mike, ja John Domingue. 2016. “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward”. Teoksessa *Adaptive and Adaptable Learning,* toimittanut Katrien Verbert, Mike Sharples ja Tomas Klobucar, 490–496. ID: 10.1007/978-3-319-45153-4$_4$8. Cham: Springer International Publishing. ISBN: 978-3-319-45153-4.

Shin, Laura. 2017. “The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project”. *Forbes* 2018 (3/20).

Shrier, David, Weige Wu ja Alex Pentland. 2016. *Blockchain & Infrastructure (Identity, Data Security).* Tekninen raportti 3/4. Massachusetts Institute of Technology.

Steem: An incentivized, blockchain-based, public content platform. 2017. https://steem.io/SteemWhitePaper.pdf.

Stornetta, W. Scott, ja Stuart Haber. 1991. “How to Time-Stamp a Digital Document”. 3 (Journal of Cryptology): 99–111.

Swan, Melanie. 2015. *Blockchain: Blueprint for a New Economy.* 1st. O’Reilly Media, Inc. ISBN: 1491920491, 9781491920497.

Tian, Feng. 2016. “An agri-food supply chain traceability system for China based on RFID & blockchain technology”, nide 13th International Conference on Service Systems and Service Management (ICSSSM). Kunming, China.

Tschorsch, F., ja B. Scheuermann. 2016. “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies”. ID: 1, *IEEE Communications Surveys & Tutorials* 18 (3): 2084–2123.

Vries, Alex de. 2018. *Ethereum Energy Consumption Index (beta).* `https://digiconomist.net/ethereum-energy-cosumption`.

Zyskind, G., O. Nathan ja A. Pentland. 2015. “Decentralizing Privacy: Using Blockchain to Protect Personal Data”. Teoksessa *2015 IEEE Security and Privacy Workshops,* 180–184. ID: 1.