Juho Rantala

Lohkoketjuteknologian yhteiskunta

Osa I: Bitcoinista Ethereumiin

Lohkoketjuteknologiasta (*blockchain technology*) on povattu internetin, talouden ja koko teknologia-alan uudistajaa. Se onkin otettu innostuneesti vastaan, kiitos noin kahdeksan vuotta sitten käynnistetyn, lohkoketjun varaan rakentuvan kryptovaluutta Bitcoinin (BTC)[1]. Bitcoinilla ja lohkoketjulla on myös kriitikkonsa: esimerkiksi Paul Krugmanin mukaan ensin mainittu ei toimi rahana, kun taas David Golumbia liittää molemmat valtiovastaisuuteen[2]. Osa kritiikistä tarttuu teknisiä innovaatioita ympäröivään retoriikkaan, jossa povataan uutta ja autuasta desentralisoitua maailmaa. Uudet digitaaliset valuutat riippuvatkin käytetystä teknologiasta. Samalla tämä teknologinen perusta aina ilmentää ja toisaalta muokkaa poliittista, sosiaalista ja yhteiskunnallista todellisuutta.

Lohkoketjusta on tullut nopeasti tunnetuin ja puhutuin ”hajautettuun tilikirjaan” perustuvista teknologioista (*Distributed Ledger Technology*). Hajautettuja tilikirjoja on monenlaisia, mutta erityisesti digitaalisessa maailmassa ne ovat käytännössä hajautettuja tietokantoja. Lohkoketju voi olla myös täysin desentralisoitu, kuten Bitcoinin tapauksessa.[3] Lohkoketjun toimintaperiaate on yleisellä tasolla hyvin yksinkertainen. Esimerkiksi Bitcoinissa jokainen valuutan siirto, ”transaktio”, tallentuu lohkoista muodostuvaan ketjuun, joka vuorostaan päivittyy kaikille käyttäjille jatkuvasti. Tämä lohkoketju rakentaa ikään kuin suuren historiallisen tilikirjan transaktioista. Tämä ”tilikirja” myös varmistaa aina transaktioiden oikeellisuuden. Näin estetään mahdollisuudet huijata tai toistaa transaktiot, koska kaikilla käyttäjillä on kopio ketjusta. Bitcoinissa transaktioiden suorittaminen edellyttää sekä *julkista* että *yksityistä* salausavainta ja osoitetta, jota käytetään joko valuutan vastaanottamiseen tai lähettämiseen. Tämä osoite määritetään julkisen avaimen avulla e-lompakossa, jollainen on oltava, jotta ”kolikoille” olisi jokin säilytyspaikka. Yksinkertaistaen voidaan sanoa, että prosessissa ikään kuin siirretään tietyn Bitcoinin käyttöoikeus osoitteesta toiseen. Bitcoinit ovatkin periaatteessa vain osoitteita, joihin joillakin on salausavaimet eli käyttöoikeus.[4]

Lohkoketjun ylläpito vaatii varmentamista (*proof-of-work*), jota Bitcoinin kohdalla kutsutaan louhinnaksi (*mining*). Samalla louhinnassa syntyy uusia Bitcoineja ”palkkiona” ketjua ja varmentamista ylläpitävän laskentatehon jakamisesta. Louhinnassa hajautetun verkoston koneet hyväksyvät kollektiivisesti muutoksia Bitcoinin tilikirjaan (tietokantaan).[5] Periaatteessa kuka tahansa voi louhia Bitcoineja omalla kotikoneellaan. Käytännössä louhinta kuitenkin vaikeutuu jatkuvasti, sillä louhijoiden lisääntyessä louhinta-algoritmi säätyy joka neljäs vuosi automaattisesti vaikeammaksi[6]. Samalla Bitcoineja on entistä niukemmin saatavilla[7]. Bitcoinien maksimimäärä on 21 miljoonaa, joista toukokuussa 2017 oli louhittu jo 16 miljoonaa. Yksi Bitcoin on tosin mahdollista jakaa pienempiin yksiköihin aina yhteen ”satoshiin” asti (0,00000001 BTC).

Louhinnan vaikeutuessa myös sen vaatima energia tulee nykyisessä energiajärjestelmässä kalliimmaksi kuin synnytettyjen kolikoiden arvo. Nykypäivänä yksittäisten käyttäjien kannattaakin kuulua ”louhintaryhmiin” (*mining pool*), joissa louhintateho ja synnytetyt kolikot jaetaan jäsenten kesken. Kun kaikki kolikot on louhittu (olettavasti vuonna 2040), transaktiopalkkioiden on tarkoitus toimia porkkanana verkoston ylläpitämisessä[8]. Bitcoineja on myös helppo kadottaa tai ”unohtaa”: jos e-lompakon salasanaa ei muista, rahat on menetetty. Onkin arvioitu, että näitä kadonneita ”zombikolikoita” olisi noin 1,6 miljoonaa tai jopa 30 prosenttia kaikista louhituista kolikoista[9].

Lohkoketjussa luottamus luodaan ilman ”kolmatta osapuolta” (pankkia tai vastaavaa instituutiota). *The Economist* tiivistää: se on ”luottamuskone”[10]. Tilikirja tai tietokanta on mahdollista jakaa kaikkien osanottajien kesken. Näin on mahdollista luoda tietoja ja solmia omistus- ja vaihtosuhteita ilman tarvetta löytää kolmatta osapuolta, jonka kaikki luottavat ”pitävän kirjaa” rehellisesti. On siis samantekevää, tuntevatko ihmiset toisensa, sillä turvallisuus ja luottamus perustuvat automaattisesti toimivaan teknologiaan sekä toisaalta yksilöiden mahdollisuuteen tai valintaan pitää yllä anonymiteettiaan.[11]

Isa Maaranen, *Ikuisuudet laatikoissaan* (2016), öljyväri ja tempera kankaalle, 160 x 150 cm. Valokuva: Tarmo Valmela

Melanie Swan onkin mahtipontisesti kuvannut lohkoketjuteknologiaa ”tasa-arvoteknologiaksi”: ketjut voivat ”laajentaa maailman kaikkien olentojen, niin koneiden kuin ihmistenkin, vapauksia, mahdollisuuksia, ilmaisua, ideointia ja niiden toteutumista”[12]. Vuoden 2008 finanssikriisin jälkeen markkinaluottamuksesta onkin ollut pulaa.

Suuri osa lohkoketjuteknologian sovelluksista pohjaa Bitcoinin tapaan avoimeen lähdekoodiin. Lähdekoodin pohjalta voi siis tuottaa uuden lohkoketjun tai vaikka digitaalisen valuutan. Kaikki lohkoketjut ja hajautetut kirjanpidot eivät kuitenkaan ole julkisia. On myös täysin yksityisiä tai vain rajatuille käyttäjille avoimia vaihtoehtoja.[13] Lohkoketjun yhteydessä voidaan myös karkeasti erotella hajautetut ja desentralistiset lohkoketjut. Hajautetussa järjestelmässä verkoston elementit noudattavat yleensä keskuksen ohjausta. Desentralisoidussa verkostossa taas ei ole mitään keskuksellista, päättävää elintä.[14] Voidaankin esittää, että mahdollisimman avoimet ja julkiset lohkoketjun sovellusratkaisut ovat ”desentralistisia”, kun taas suljetut ja yksityiset ja näin ollen rajatut pikemminkin ”hajautettuja”[15].

Hajautettuja tai desentralisoituja kirjanpitoteknologioita tai -tekniikoita on käytetty viimeisen parin vuoden aikana moniin tarkoituksiin: sopimusten allekirjoittamiseen, varainhallintaan sekä identiteetti-, patentti ja maineenhallintarekistereihin[16]. Terveydenhuollon tietojärjestelmiä ja koulutuksen moninaisia alustoja pidetään oivallisina kohteina ketjulle[17]. On todennäköistä, että jonkinlainen hajautettu tietokanta on myös lisätyn ja sekoitetun todellisuuden (*augmented reality*; *mixed reality*) teknologioiden, tavaroiden tai teollisen internetin (*Internet of Things*) sekä tekoälyn ytimessä[18]. Lisäksi on povattu, että tulevaisuudessa äänestysjärjestelmät voisivat hyödyntää lohkoketjua. Ensimmäinen kokeilu tehtiin viime vuonna, kun Etelä-Korean provinssi Gyeonggi-do käytti lohkoketjuteknologiaa julkisessa, paikallishankkeita koskevassa äänestyksessä.[19]

Innostuneita eivät ole vain uudet tekijät ja *startup*it. Esimerkiksi finanssialan vanhukset, kuten Suomessa Osuuspankki, sekä muutamat valtiot ovat kiinnostuneet saamaan oman ketjunsa – tai ainakin kryptovaluutan.[20] Viime kuukausina Euroopan keskuspankista on kuulunut toiveita digitaalivaluutasta ja myös Suomen Pankki on analysoinut kryptovaluuttaratkaisujen mahdollisuuksia[21]. Rahoittaja ja ohjelmistokehittäjä Olaf Carlson-Wee totesi *Wired*-lehdessä, että tulevaisuudessa nähdään luultavasti lohkoketjuun perustuvia yrityksiä, jotka omistavat itsensä ja toimivat itsenäisesti[22]. Lohkoketjua hyödyntäviä *prepaid*-luottokortteja, joita varten ei tarvitse luottotietoja tai pankkihistoriaa, on myönnetty turvapaikanhakijoille. Samalla kortit toimivat seurantavälineenä, ja EU onkin panostanut viime aikoina hajautetun tietokantajärjestelmän tutkimiseen juuri identiteettihallinnan ja seurannan näkökulmasta.[23]

Lohkoketju tekniikkana on itsessään vallankumouksellinen, mutta sen soveltaminen on vahvasti riippuvaista asiayhteydestä. Lohkoketju on kytkeytynyt ennen kaikkea talouteen ja se on syntynyt ”taloudellisena innovaationa”, joten sen pääasiallisia nykysovelluksia ovat kryptovaluutat sekä digitaaliset vaihtojärjestelmät, näistä tärkeimpinä Bitcoin ja Ethereum.

Teknologiaunelmat: lohkoketjuteknologian ja kryptovaluuttojen teknologinen tausta

Lohkoketjun kehittämistä inspiroivat laajat ja pitkään käydyt keskustelut yksilön ja instituutioiden suhteesta, desentralisaatiosta ja ihmisyhteisöjen spontaanista järjestäytymisestä. Nämä teemat ovat olleet tärkeitä myös niin sanotussa hakkerietiikassa. Tällainen etiikka kumpuaa vapaasta yhteisöllisestä luovuudesta, itsekorjaavuudesta, ongelmanratkaisusta ja halusta ymmärtää, miten asiat toimivat. Ohjelmistot ovat usein hyvin laaja-alaisia, jolloin niiden kehittäminen kannattaa hajauttaa: monta silmäparia luo ja kehittää koodia paremmin kuin yksi. Verkossa tuotanto on helppo desentralisoida, ja ohjelmoijat osallistuvat projekteihin usein ilman korvausta yhteisen hyvän vuoksi. Kuten Yochai Benkler toteaa, verkossa yhteistuotanto ei toimi markkinatalouden taustalle oletetun hintajärjestelmän tai yritysrakenteen pohjalta vaan vapaammin ja samalla tehokkaammin.[24]

Vaikka lohkoketjua pidetään helposti ”laadullisesti” täysin uutena keksintönä, se vaikuttaa pikemminkin olevan osa tai seuraava askel internetin kehityksessä[25]. Alkupisteenä ovat internetin alkuvuosien hakkereiden ideaalit, joihin kuuluvat esimerkiksi libertarismin yksilökeskeisyys ja yksilöiden välinen ”puolisosialistinen” yhteistyö ja vapaa jakaminen[26]. Tietysti myös itse internetin rakenne mukailee desentralisoitua verkostoa, jossa tosin on keskuksellisia pisteitä[27]. Samalla esimerkiksi avoimen lähdekoodin ohjelmistot ilmentävät jo lohkoketjun yhteisöllisyyttä. Toisin sanoen lohkoketju toimii ikään kuin avoimen lähdekoodin ohjelmistojen vapaan koodauksen ja suunnittelun verkoston automaattisena varmistajana.

Toiminnan hajauttaminen on teknologisesta näkökulmasta katsottuna juurtunut myös syvemmälle. Daniel Hillis tiivistää, että tietokoneiden prosessorien kehityksessä oli pakko ottaa käyttöön monisuoritinkoneet eli tietokoneet, joissa oli monia prosessoriytimiä. Kehityksen taustalla olivat kokeilut koneiden verkottamisesta ja tehtävien osien jakamisesta verkossa oleville yksittäisille koneille (”hajautettu tietojenkäsittely”).[28] Myös tekoälyä kehitettäessä on jo pidempään käsitelty niin sanottuja ”hajautettuja representaatioita”, varsinkin neuroverkkojen ja koneoppimisen yhteydessä. Niin ikään internetverkkoa hyödyntävät ohjelmistot ja palvelut ovat jo kauan pyrkineet soveltamaan hajautettuja arkkitehtuureita. Esimerkiksi hakukoneissa hyödynnetyissä neuroverkoissa yksittäiset tiedonkäsittelyn yksiköt (neuronit) voivat edustaa (representoida) jotain tiettyä asiaa, ja toisaalta ne voivat ”ottaa osaa” myös muiden asioiden tai käsitteiden representaatioihin. Näillä representaatioilla luodaan erilaisia rooleja, jotka ovat olemassa tiettyinä hetkinä verkostossa. Tämä roolittaminen perustuu oppimissäännöille. Esimerkiksi itseoppivan tekoälyn yhteydessä neuraaliverkko

”Neuroverkot, vertaisverkot ja PayPalin kaltaiset internetmaksupalvelut olivat pioneereja kryptovaluuttojen ja lohkoketjuteknologian kehityksessä.”

kykenee tekemään yleistyksiä erityisistä tilanteista. Samalla verkosto kykenee muokkautumaan toimintaympäristönsä mukaan.[29]

Hajauttaminen tai desentralisaatio sekä hallinnan kysymykset ovat olleet osa Norbert Wienerin kehittämää kybernetiikkaa aina 1900-luvun alkupuoliskolta lähtien. Alkunsa kybernetiikka sai niin sanotuista Macy-konferensseista, joita alettiin pitää vuonna 1942. Niissä kokoontuivat erityisesti matemaatikot, fysiologit ja insinöörit, jotka keskustelivat itsesääntelystä ja teleologisuudesta. Lopulta keskeisiksi nousivat koneelliset ja biologiset järjestelmät sekä sosiaaliset prosessit, joiden taustalla katsottiin olevan informaatio ja ”takaisinkytkentä” (*feedback*). Varsinkin armeija tarttui aihepiiriin, sillä se oli pitkään ollut huolissaan kommunikaatiojärjestelmien haavoittuvuudesta. Tosin esimerkiksi Ian Watson huomauttaa, että armeija ei alkujaan ollut mukana itse internetin kehityksessä, vaan erityisesti yliopistot pyrkivät tehostamaan rajallisten tietokoneresurssien käyttöä. Ratkaisuksi tarjottiin hajautettua kommunikaatiota, joka rakentui tasa-arvoisista keskuksista. Tiedonsiirrossa hyödynnettiin ”pakettikytkentää” (*packet switching*) eli data hajotettiin pieniksi ”paketeiksi”, jotka vuorostaan siirtyivät IP-protokollan hallitsemien verkko-osoitteiden mukaisesti. Internetin ”pohja” kehittyi 1969, kun neljä tietokonetta verkotettiin ARPANETiksi (*Advanced Research Projects Agency Network*).[30]

Yleisesti muotoiltuna kybernetiikka tarkoittaa tutkimusta kontrollin ja kommunikaation verkostoista, joissa ihminen ja ei-ihminen toimivat yhdessä. Samalla siinä pyritään luomaan ja ymmärtämään hallittuja itsesäätéleviä järjestelmiä, joita voivat olla lähes mitkä tahansa kokonaisuudet aina biologisista organismeista teknologisiin laitteisiin. Kybernetiikka on kuitenkin lopulta kääntynyt tutkimaan ja kehittämään informaation avulla sosiaalista hallintaa, joka kohdistuu niin ihmisiin kuin ei-inhimilliseen – ja nykyään kattaa niin *offline*n kuin *online*n.[31]

1990-luvun alkupuolella yleistyivät vertaisverkot (*peer-to-peer*). Niiden perusajatuksena on, että verkon käyttäjät toimivat yhtä aikaa asiakkaina *ja* palvelimina. Verkko on siis hajautettu käyttäjien kesken.[32] Uudella vuosituhannella vertaisverkko tuli laajemmin tunnetuksi, kun musiikinjakopalvelu Napsterin aiheuttamat tekijänoikeusrikkomukset nousivat otsikoihin. Samalla syntyi muita enemmän tai vähemmän laittomia palveluita.

Neuroverkot, vertaisverkot ja PayPalin kaltaiset internetmaksupalvelut olivat pioneereja kryptovaluuttojen ja lohkoketjuteknologian kehityksessä. Tosin jo 1983 David Chaum esitteli anonyymin elektronisen maksujärjestelmän, mutta vasta internetin nopeutuessa ja laaje-

”Rahoja kyettiin periaatteessa kopioimaan kuin mitä tahansa digitaalisia tiedostoja.”

tessa sekä mobiiliteknologian kehittyessä tällaiset haaveet alkoivat vaikuttaa realistisemmilta.[33] Tietysti myös tietokoneiden kehityksen mukana kulkenut kryptografia eli salaus on ollut tärkeässä osassa. Yksi tärkeä askel oli Cynthia Dworkin ja Moni Naorin kehittämä kryptografinen varmistus sähköpostia varten[34].

Digitaalisia tai elektronisia rahoja on ollut käytössä jo pitkään. 1990-luvulla monet pelit ja Second Lifen kaltaiset virtuaalimaailmat tarjosivat oman valuuttansa tai kokonaisen virtuaalitalouden[35]. Vuonna 1990 Chaum perusti DigiCashin, joka kuitenkin kaatui kahdeksan vuotta myöhemmin markkinoiden vähäisyyteen.[36] Bitcoinin kehityksessä erityisen tärkeitä ovat olleet Adam Backin kehittämä Hashcash, Hal Finneyn kokeilut Bitcoinia muistuttavilla kryptovaluuttarakenteilla sekä Wei Dain luoma B-money[37]. Esimerkiksi Hashcashin ajatus varmentamisesta (*proof-of-work*) on muuntunut louhinnaksi. Nakamoton mukaan Bitcoinin taustalla oli halu ratkaista ensimmäisiä digitaalivaluuttoja vaivannut ”kaksinkertaisen käytön ongelma” (*double-spend problem*)[38]. Rahoja nimittäin kyettiin periaatteessa kopioimaan kuin mitä tahansa digitaalisia tiedostoja: raha siis pystyttiin käyttämään useaan kertaan. Tähän ongelmaan Bitcoin pyrki vastaamaan yhdistämällä kryptosalauksen, lohkoketjun sekä louhinnan. Toisaalta louhinnan ja lohkoketjun yhteispelillä voidaan vastustaa myös ”Sybil-hyökkäystä” (*Sybil attack*), jossa yksittäinen käyttäjä luo joukon väärennettyjä käyttäjätunnuksia tai -identiteettejä ja nostattaa näin oman tunnuksensa, sivustonsa tai muun vastaavan arvoa verkoston silmissä, eli pyrkii saamaan haltuunsa enemmistön verkostosta. Samalla lohkoketjussa siirryttiin konetehon jakamiseen pohjautuvaan varmistamiseen, sillä hajautuneesta konetehosta oli vaikeampi saada enemmistö hallintaan kuin vaikkapa verkkoidentiteeteistä.[39]

Itse lohkoketjun tallennus- ja varmistusjärjestelmän taustalla oli todennäköisesti Stuart Haberin ja W. Scott Stornettan kehittämä dokumenttien aikaleimaus. Ajatuksena oli luoda leimaustapa, jolla dokumenttien muutosta ja kehitystä voitiin seurata. Leimausta ei kyennyt muuttamaan, sillä se tapahtui palvelimella, johon dokumentit lähetettiin. Palvelin liitti mukaan myös linkin aikaisempaan dokumenttiin, mutta linkin takaa löytyi pikemminkin dataa, joka toimi aikaleiman kanssa osana ”sertifikaattia”[40]. Lohkoketjua kokoava ja transaktioita verifioiva funktio perustui myös Nick Szabon kehittämään algoritmiin, joka muovasi valuutasta niukan resurssin[41]. Kun tähän liitettiin vertaisverkon hajautettu verkosto, siinsi uusi teknologia horisontissa.

Viime vuosina onkin kehittynyt ajatus jaetusta vertaisverkkoon perustuvasta taloudesta[42]. Näissä uusissa talouksissa arvonmuodostus tapahtuu avoimesti, samaan tapaan kuin avoimen lähdekoodin jakaminen. Ainakin

kahdenlaisia sovelluksia on syntynyt: yhtäältä Wikipedian kaltaisia vapaasti luettavia ja vapaasti päivitettäviä kokonaisuuksia sekä toisaalta ilmaiseksi käytettäviä ja käyttäjien tuottamasta sisällöstä rakentuvia palveluita kuten Facebook. Sovelluksia erottaa se, että esimerkiksi Wikipediassa arvo syntyy ja jaetaan kaikkien käyttäjien kesken. Facebookissa taas suuri osa arvosta kanavoituu – erityisesti mainostuloina – palvelua ylläpitävälle yritykselle.

Verkon ja käyttäjän anonymiteetista on tullut tärkeä tekijä. Onkin puhuttu identiteettitietojen henkilökohtaisesta pääomasta: ihmiset voisivat itse omistaa identiteettitietonsa, joita sitten jakaisivat esimerkiksi maksua vastaan[43]. Tiedot voisivat tallentua lohkoketjuun, johon ihmiset voisivat antaa käyttöoikeuden tietylle taholle tietyksi ajaksi. Identiteettitietojen vaihdannan on povattu jopa syrjäyttävän virtuaali- tai kryptovaluuttojen käytön[44].

Pääasiassa erityyppisiin lohkoketjurakenteisiin perustuvat kryptovaluutat ovat suosittuja, ja niitä onkin syntynyt paljon. Bitcoinin haastajista Ethereum on tällä hetkellä saavuttanut suuren markkinaosuuden. Muita valuuttoja ovat esimerkiksi Ripple, Litecoin ja Dash[45]. Suuren volatiliteetin takia Bitcoinin arvo on ollut yhtä vuoristorataa, vaikka viimeisen parin vuoden ajan se onkin kohonnut suhteellisen tasaisesti. Lähtöarvona vuonna 2009 oli vain 0,0005 euroa, ja kolme vuotta myöhemmin arvo oli noussut kuuteen dollariin. Tämän jälkeen alkoi nousukiito: vuosien 2013–2015 välillä arvo liikkui 140 dollarista 950 dollariin ja takaisin 220 dollariin. Tammikuussa 2017 yksi Bitcoin vastasi noin tuhatta dollaria. Kesäkuussa arvo oli kasvanut jo kolminkertaiseksi ylittäen lopulta elokuussa 4 000 dollarin rajapyykin. Loppusyksyä kohden arvon nousutahti kiihtyi ja marraskuun lopulla se oli jo yli 9 000 dollaria. Bitcoin-futuurien astuessa markkinoille joulukuun alkupuolella arvo kohosi entisestään, ja kuun puolen välin jälkeen yhden Bitcoinin hinta oli noin 19 000 dollaria. Loppukuusta ja vuoden 2018 alkupuolella nähtiin kuitenkin arvon voimakasta heittelyä, ja helmikuun viidentenä yhden Bitcoinin hinta oli noin 6 900 dollaria. Seuraavan kymmenen päivän aikana arvo kuitenkin ylitti taas 10 000 dollarin rajan.[46]

Ethereum ja tulevaisuus

Lohkoketju ei välttämättä – tai ainakaan kaikilta osin – ole mikään erillinen innovaatio. Swan toteaa osuvasti, että esimerkiksi Ethereum-lohkoketjujen älysopimukset (*smart contracts*) eivät oikeastaan tee mahdolliseksi mitään aikaisemmasta poikkeavaa, vaan ne vain helpottavat ja nopeuttavat sopimusten toimintaa[47]. Itse älysopimuksia käsitteli jo Szabo 1990-luvun puolessavälissä[48]. Uudet älysopimukset kuitenkin mahdollistavat sen, että lohkoketju voi suorittaa lyhyitä algoritmeja tai ohjelmia, ei pelkästään kerätä tietokantaa. Tällainen lohkoketju voi antaa myös hetkellisiä oikeuksia käyttää ketjun ulkopuolista identiteettidataa vaikkapa terveydenhuollossa.[49]

Ethereum onkin protokolla tai palvelualusta, jossa lohkoketjuteknologian avulla mahdollistetaan ohjelmien ja algoritmien suorittaminen sekä virtuaalivaluuttojen ja mainejärjestelmien kehittäminen. Ethereumia Vitalik Buterinin kanssa kehittäneen Gavin Woodin mukaan sen tarkoituksena on tuottaa yleinen teknologia, jonka päälle voidaan rakentaa kaikki vaihtoon perustuvat toiminnat (eli luoda *transaction-based state machine*). Tämä tarkoittaa käytännössä lohkoketjuteknologiaan perustuvaa ”Ethereumin maailmaa” eli tilakonetta, jossa kaikki laskennalliseen muotoon muunnettavissa olevat tilat ja niiden muutokset välittyvät tämän maailmaprotokollan avulla.[50]

Ethereum tarvitsee kuitenkin oman ”valuuttansa” tai resurssinsa, Etherin (ETH). Tätä valuuttaa käytetään kannusteena ylläpitää taustalla olevan lohkoketjua. Prosessi eroaa jonkin verran Bitcoinin louhinnasta, jossa jokainen uusi louhittu kolikko muodostuu ikään kuin ”käyttämättömäksi transaktioksi” tai, hieman yksinkertaistaen, koodiriviksi, johon tietyllä käyttäjällä on oikeus. Kun transaktio tapahtuu, syntyy uusi koodirivi, joka kertoo uuden käyttöoikeuden haltijan. Ethereum-ketju tallentaa jatkuvasti verkoston ”nykytilan” mukaan lukien käyttäjätilit ja niiden saldot. Transaktion tai muun tapahtuman oikeellisuus varmistetaan yksinkertaisesti: onko käyttäjällä tarpeeksi saldoa. Etherin tarkoitus *ei ole olla valuutta* vaan Ethereumin sisäinen resurssi. Tätä resurssia käytetään koodien ja älysopimusten suorittamiseen, eikä sillä ole rajoitettua kokonaismäärää kuten Bitcoinilla – tosin Etherin vuosittainen louhintaraja on 18 miljoonaa. Ether siis toimii öljyn kaltaisena koko alustaa vauhdittavana elementtinä. Ethereum-alustaa kuitenkin rajoitetaan *Gas*in (”polttoaineen”) avulla. Jos esimerkiksi älysopimus vie paljon kaistaa ja sen suorittaminen kestää kauan, *Gas*-luku on suuri, jolloin tarvitaan enemmän Etheriä. Näin on tarkoitus ”tasoittaa” lohkoketjua eli rajoittaa esimerkiksi paljon Etheriä omistavan tahon kykyä vaikuttaa ketjuun.

Itse asiassa juuri Ethereum- tai älysopimuspohjainen lohkoketju oli käytössä Gyeonggin maakunnan äänestyksessä[51]. Pierre Noizatin taas on ehdottanut Bitcoinin rakenteeseen pohjautuvaa sähköistä äänestystä. Tässä järjestelmässä äänen antaminen toimisi samoin kuin kryptovaluutan transaktio. Äänestäjällä olisi tietty määrä äänestysluottoa, joka kohdistettaisiin tiettyyn tai tiettyihin ehdokkaisiin tai ehdotuksiin riippuen äänestyksen sisällöstä. Lyhyesti sanottuna kolme julkista avainta yhdistettäisiin, jolloin tietyt ennalta luodut osoitteet tulisivat ”rahoitetuksi”, ja sen myötä ne näkyisivät ketjussa. Ketju voitaisiin lopuksi kääntää suoraan äänestystuloksiksi. Samalla jokainen voisi katsoa, onko hänen osoitteensa rahoitettu eli ääni mennyt läpi.[52]

Sähköisessä äänestyksessä on tietysti omat ongelmansa. Esimerkiksi Aalto-yliopiston professori Jarno Limnéll on todennut, että sähköinen äänestys lisää hybridisodan uhkaa. F-Securen tutkimusjohtaja Mikko Hyppönen on taas katsonut, ettei perinteisessä äänestämisessä ole mitään ongelmaa, joka ”digitalisaation olisi

”Oikeastaan koko internet on rakennettu hyvin hallintakeskeisesti.”

Iisa Maaranen, *Lapulta palaudumme samaan muotoon* (2017), tempera ja öljyväri kankaalle, 150 x 150 cm. Valokuva: Tarmo Valmela

ratkaistava”. ”Paperiäänestys” myös mahdollistaa helpon uudelleenlaskennan.[53] Noizat jakaa ainakin osittain saman näkemyksen: sähköisen äänestyksen ei olisi tarkoitus korvata perinteistä äänestystä vaan tarjota vaihtoehtoinen, rinnalla toimiva tapa[54]. Toisaalta kansalaisilla, äänestäjillä, pitäisi olla jonkinlainen mahdollisuus todeta tai varmentaa käytettävän koneen ja koodin (lohkoketjun) oikeellisuus. Monimutkaiset järjestelmät ovat viime kädessä suunnittelijoiden ja koodaajien tuotoksia, joihin ”tavallisen kansalaisen” on vaikea sanoa mitään.

Yksi Ethereumin kehittäjistä, Vitalik Buterin, on esitellyt uudenlaista varmistamisprosessia, joka poikkeaa Bitcoinin louhinnasta (*proof-of-work*). Todistus osakkuudesta tai ”osakkuusvarmennus” (*proof-of-stake*) on kehitetty Casper-projektissa, joka perustuu Ethereumiin. Varmistusprosessissa valitsijat äänestävät seuraavasta ketjun lohkosta, mutta jokaisen äänestäjän antaman *äänen painoarvo* riippuu tähän ääneen asetetusta resurssitalletuksesta. Casperissa tämä resurssi on Ether. Jokainen Etheriä omistava voi luoda erityisen transaktion, joka lukitsee halutun resurssimäärän talletukseen. Näin talletuksen tekijästä tulee valitsija, joka ottaa osaa uusien lohkojen kasaamiseen ja saa tästä tiettyjen algoritmisten sääntöjen mukaan palkkioita. Tällainen varmistamistapa säästää huomattavasti energiaa verrattuna louhinnan konetehojen jakamiseen perustuvaan varmistamiseen. Se myös tekee epätodennäköisemmäksi 51%-ongelman eli tilanteen, jossa yksittäinen taho kontrolloi yli puolta verkoston louhintatehosta luoden mahdollisuuden väärinkäytöksiin.[55]

Erityisesti Ethereumin kaltaiset monimutkaiset lohkoketjusovellukset ovat tulleet ryminällä myös Wall Streetille. *Wired*-lehti uutisoi Richard Craibin uudesta Numerai-yrityksestä, jossa osakekaupan hoitaa tekoäly. Yritys kerää yhteen tärkeimmät osakekauppatiedot, jotka sitten jaetaan tuhansien ohjelmoijien kesken. Heidän tarkoituksenaan on rakentaa tietojen pohjalta malleja, jotka hoitaisivat kaupat automaattisesti ja entistä paremmin tuloksin. Parhaista malleista palkkiona on Bitcoineja. Craibin mukaan ongelmana on kuitenkin itsekkyys: miksi voittanut ohjelmoija värväisi myös muita mukaan? Vastauksena tähän on uusi Numeraire-valuutta tai -rahake, jonka tarkoitus on muuttaa ”Wall Streetin kilpailu yhteistyöksi”.[56] Numerairella ohjelmoijat lyövät vetoa siitä, toimivatko heidän algoritminsa markkinoilla. Jos ne toimivat, he saavat Numerairensa takaisin sekä osinkoa Bitcoineina. Craibin mukaan Numerairen arvo kasvaa, kun rahaston varat kasvavat. Näin ohjelmoijat tavallaan puhaltavat yhteiseen hiileen. Tämä tietysti ta-

”NSA-vuodoissa paljastui, että Yhdysvallat oli kaapannut erinäisten reititinten tietoliikenteen kokonaisvaltaisesti.”

pahtuu yhden rahaston sisällä, joka käy kilpailua muita rahastoja vastaan.

Lohkoketjun ja sen sovellusten ongelmia

Tutkimusartikkeleissa ja -keskustelussa on kritisoitu laajasti lohkoketjuteknologiaa ja nostettu esiin sen ongelmia. Vaikka lohkoketju tähtää desentralisaatioon eli hajauttamiseen ja siten hallinnasta vapautumiseen, voidaan yleisemmällä tasolla katsoa, että oikeastaan koko internet on rakennettu hyvin hallintakeskeisesti. Alexander Galloway on esimerkiksi käsitellyt internetin liikennettä ja verkko-osoitteita ohjaavia protokollia (TCP/IP sekä DNS ja sähköposteissa käytetty STMP), jotka on muodostettu niin, että tietoliikenteen keskuksellinen hallinta on helppoa. Internetissä selkeät protokollarakenteet mahdollistavat tietojen luovuttamisen, mutta myös niiden suoran kaappaamisen, kuten NSA-vuodot ovat osoittaneet. Internetissä kaikki ”solmukohdat” (*node*; esimerkiksi tietokone) voivat luoda yhteyksiä keskenään ilman hierarkkista välittäjää. Tästä huolimatta näiden ”solmujen” on puhuttava ”samaa kieltä”, ja toisaalta ne kulkevat erinäisten ohjaavien laitteistojen, reititinten, kautta.[57] Järjestelmä siis jakaa protokollan, jolloin hallintamalli on sisäistetty verkkoon. NSA-vuodoissa paljastui, että Yhdysvallat oli kaapannut erinäisten reititinten tietoliikenteen kokonaisvaltaisesti. Vaikka Bitcoinissa luottamus pyritään siirtämään taustalla toimivaan lohkoketjuun ja tietysti myös louhintaprosessiin, luotto kohdistuu viime kädessä salausmekanismiin, koodiin ja kehittäjiin. Samalla päivitykset ja kehitystyö syntyvät tietyssä rajatussa yhteisössä.[58]

Vaikka lohkoketjua on kritisoitu ketjun hakkeroinnin helppoudesta, erityisesti julkisia ketjuja näyttää olevan vaikea muokata juuri niiden desentralisaation vuoksi. Toisaalta julkinen ketju ei kuitenkaan välttämättä takaa samanlaista yksityisyyttä kuin rajattu, yksityinen ketju. Jälkimmäisen ongelma on vuorostaan nimenomaan sen yksityisyydessä: lohkoketjun ”ideaali” perustuu suurelta osin vapaaseen itseorganisoitumiseen ja luottamukseen, johon sulkeutuminen, rajat ja määräävä ”keskus” eivät kuulu. Julkisissa ketjuissa ongelmana sen sijaan on, että käyttäjä- ja kehittäjärajapinnat eivät ole tasaveroisia. Vaikka julkinen ketju ei ole minkään tahon hallussa, järjestelmän kehittäjillä voi olla mahdollisuus vaikuttaa verkon toimintaan esimerkiksi uusilla päivityksillä. Eivätkä sen paremmin yksityiset kuin julkisetkaan teknologiat pelastu valtioiden tai yksityisten jätti-instituutioiden harjoittamalta verkkourkinnalta, vaikka tähän mennessä esimerkiksi Bitcoinin lohkoketjun salauksen murtaminen on osoittautunut vaikeaksi. Julkisissa verkoissa tai lohkoketjuissa data on aina kolmansien osa-

puolien analysoitavissa[59]. Lohkoketjussa syntyvästä ”kirjanpidon” historiasta voi olla mahdollista lukea, kuka ketjuun tallentuneet transaktiot on tehnyt. Henkilöllisyys voi paljastua, jos rinnalla on toinen tietokanta, johon verraten transaktiot ovat liitettävissä konkreettisiin tapahtumiin. Tietysti myös e-lompakon salasana on syytä pitää tallessa: mitään turvaa tai vakuutta kolikoille ei ole.[60]

Tere Vadén on summannut lohkoketjun yleisiä ongelmia. Ketju kärsii ei-ammattilaisen näkökulmasta käytettävyysongelmista: käyttöliittymä ja esimerkiksi anonymiteetin ylläpitäminen eivät ole yksinkertaisia asioita. Toisaalta ketjua ovat jo tuotteistamassa suuret toimijat, jolloin valta-asemat säilyvät, vaikka – Swania lainaten – ketjun piti olla tasa-arvoa tuottava teknologia. Näin ollen suuremman yleisön silmissä puheet vallankumouksellisuudesta ja uutuudesta näyttävät tyhjiltä lupauksilta, joissa kaikuvat aikaisempien vuosien vertaisverkkojen epäonnistumiset.[61] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park ja Kari Smolander ovat vuorostaan tiivistäneet osuvasti erityisesti Bitcoinin yhteydessä ilmenneitä teknisiä ongelmia. Heidän mukaansa yhtenä ongelmana on latenssi eli viive: Bitcoinin pääversiossa transaktioiden varmistus voi kestää jopa puoli tuntia, kun esimerkiksi Visalla asia hoituu muutamassa sekunnissa[62]. Samalla lohkoketjun kaista on rakennettu käsittelemään hyvin pieniä bittimääriä. Bitcoinin nykyisessä versiossa yhden lohkon koko voi olla yksi megatavu. Tosin esimerkiksi Ethereumissa ei tällaista rajoitetta ole. Erityisesti pienet lohkoketjut ovat todella alttiita 51%-hyökkäyksille.[63]

David Golumbia tiivistää 51%-ongelman teoreettiseksi mahdollisuudeksi vaikuttaa ketjun kokonaisuuteen, kun järjestelmästä 51 prosenttia on tietyn tahon hallussa. Ketjun uusi lohko ”hyväksytään”, jos suurin osa verkon solmukohdista varmistaa sen oikeaksi. Hallitseva taho kykenisi joko estämään transaktioiden varmistamisen tai hyödyntämään edellä mainittua ”kaksinkertaisen käytön ongelmaa”.[64] Vaikka pitkään arvioitiin, ettei 51%-ongelma toteudu, näin kuitenkin kävi vuonna 2014[65]. Valta onkin siirtynyt entistä enemmän käyttäjäverkostolta tietyille yksittäisille käyttäjille tai kollektiiveille, kun louhinta on jatkuvasti vaikeutunut. Nykyään hyödylliseen ja kustannustehokkaaseen louhintaan vaaditaan valtava määrä konetehoa ja energiaa. Alkuaikoina tuhansia ja satoja tuhansia kolikoita haalineet voivat entistä helpommin käyttää 51%-ongelmaa omaksi hyödykseen. Näyttäisi myös siltä, että hintaan on pyritty vaikuttamaan bottien avulla.[66]

Yksi suuri uhka uusille teknologioille on maailmanlaajuinen ekologinen kriisi. Steve Hucklen ja Martin Whiten mukaan Bitcoinin louhinnan energiankulutus oli vuonna 2014 noin 3,38 terawattituntia. Vertailukohdaksi he esittävät, että 2,72 miljoonan jamaikalaisen energiankulutus oli samaisena vuonna noin 3,03 terawattituntia. Esimerkiksi Visan järjestelmässä yksittäinen transaktio vie vain 0,0003 talouden verran energiaa. Energiankulutus on suosion mukana vain kasvanut. Lokakuussa 2017 Bitcoinin kulutusarvio oli noin 21,9 terawattituntia ja Ethereumin järjestelmän noin 5,7 terawattituntia. Will Martin arvioi Maailman talousfoorumin sivuilla, että yhden transaktion energiankulutuksella voitaisiin ylläpitää kotitaloutta neljän viikon ajan. Myös lohkoketjun läpinäkyvyys vaatii laajoja julkisia metadatamääriä ja niiden seurantaa, vaikka luottamus onkin osittain automatisoitu ketjun toimintaan.[67] Jeff Hecht huomautti *Nature*-lehden artikkelissaan, että jo nyt uusien informaatioteknologioiden tarvitsemia suuria nopeuksia on vaikea ylläpitää niiden vaatimien suurten energiamäärien takia[68]. Tällainen kulutus on väistämättä ongelma teknologian laajentumiselle maailmassa, jossa pitäisi leikata ilmastopäästöjä eli fossiilisten polttoaineiden kulutusta[69]. Yksi suuri syy Bitcoinin valtavalle energiankulutukselle on sen suunnittelussa ja laskennallistetussa luottamuksessa: Bitcoin-järjestelmän salaus- ja turvallisuusvaatimukset ja koko louhintaprosessi ovat raskaita ja konetehoa vaativia toimia.

Lopuksi

Lohkoketju on *tekniikka*, jota sovelletaan hyvin monin tavoin. Perusperiaate eli hajautettu tai desentralisoitu tietokanta tai tilikirja kuitenkin toistuu. Näin ollen ketju ”innovaationa” on sidoksissa sen soveltamistapaan, jolloin sen olemus riippuu juuri käyttöyhteydestä. Jos esimerkiksi haluttaisiin, että Bitcoin olisi toimiva *valuutta*, täytyisi sitä periaatteessa säännellä[70]. Tämä taas sotii osittain koko Bitcoinin ajatusta vastaan, mutta vaikuttaa samalla myös itse lohkoketjun toimintaan. Toisaalta täysin säätelystä vapaa kryptovaluutta kohtaa helposti 51%-ongelman, jolloin ajaudutaan jälleen keskukselliseen hallintaan, sääntelyyn.[71]

Ongelmistaan huolimatta lohkoketjulla on paikkansa yhteiskunnassa. Vaikka lohkoketju ja sen käytännölliset sovellukset eivät ole täysin lunastaneet lupauksiaan, näyttää sen tulevaisuus ruusuiselta – tai näin ainakin keskusteluissa povataan[72]. Vaikka ketju näyttää johdonmukaiselta kehitysaskeleelta 1900-luvun informaatioteknologian ja varsinkin internetin historiassa, siinä tiivistyy monia aikaisempia ajatuksia ja innovaatioita.

Poliittisista näkökulmista tai menneistä ja tulevista yhteisömalleista vapaata teknologiaa ei ole olemassa. On tärkeää ymmärtää, mihin koodia tai tiettyä teknologiaa käytetään, ja ennen kaikkea, mistä se tulee. Lohkoketju on hyvä esimerkki tästä. Sitä voi pitää jopa ajattelutapana, jolla lähestytään erityisesti ohjelmistokehitystä mutta myös monia ihmiselämän ja yhteiskunnallisen olemisen ongelmia ja niiden ratkaisuja.

Artikkelin jatko-osa ”Lohkoketjuteknologian yhteiskunta. Osa II: Lohkoketjun rajatut mutta desentralisoidut markkinat” on luettavissa numeron 1/2018 verkkosivuilla osoitteessa: www.netn.fi/lehti/niin-nain-118

Viitteet

1 Alkuperäinen Bitcoinin ”lanseerausartikkeli”, ks. Nakamoto 2008. Nimimerkin Satoshi Nakamoto taustalla on luultavasti useampi kuin yksi ihminen. O’Hagan (2016) esitti pitkässä artikkelissaan, että australialainen yrittäjä ja informaatiotieteilijä Craig Steven Wright on todennäköisesti ollut ainakin yksi näistä henkilöistä. Myös esimerkiksi suomalainen Martti Malmi auttoi Nakamotoa Bitcoinin käyttöliittymän kanssa (esim. Eklund 2015).

2 Krugman 2013; Feuer 2013; Golumbia 2016.

3 Esimerkiksi lukuisten rahoituslaitosten kanssa toimivan R3:n kehittämä Corda-järjestelmä (ks. Rutter 2017) sekä Hashgraph (ks. verkkosivu: hashgraph.com).

4 Esim. Nakamoto 2008; Swan 2015a; ks. myös hyvä tiivistys Tymoigne 2013.

5 Ks. Ethereum/Wiki, ”History”. Nykyään kryptovaluuttojen louhintaan on käytettävä keskusprosessorien (CPU) sijasta näytönohjaimia (GPU), joilla laskentatehoa voidaan hyödyntää paremmin. Bitcoinin louhinta taas on siirtynyt tähän tehtävään räätälöityyn ASIC-arkkitehtuuriin. Ks. esim. Karppinen 2015; blockchaintechnologies.com/blockchain-mining.

6 Algoritmi tarkoittaa yksinkertaisesti, Adrian Mackenzieta lainaten, ohjetta tai ”joukkoa askelia”, jotka on ilmaistu koodina, kuviona tai kuvaajana. Algoritmi siis tekee jotain eli suorittaa jonkin toimen. Se voi myös kantaa tai jakaa toimintoja eri ympäristöihin. (Mackenzie 2006, 43.)

7 Tschorsch & Scheuermann 2016, 2087.

8 Sama.

9 Guadamuz & Marsden 2015.

10 *The Economist* 2015.

11 Ks. Mallard ym. 2014.

12 Swan 2015b, 42.

13 Chester 2016.

14 Narayanan ym. 2016; Troncoso ym. 2017.

15 Esim. Swan 2015a, x; Tapscott & Tapscott 2016, I.I.

16 Ks. laaja luettelo lohkoketjuteknologian mahdollisuuksista esim. Swan 2015a; Honkanen 2017a ja 2017b. Myös OECD (2017) käsittelee raportissaan lohkoketjua tekoälyn rinnalla.

17 Esim. Honkanen 2017a, 13–16, 29–31; 2017b, 14.

18 Ks. Swan 2015b, 42; Reijers ym. 2016, 145. Laajemmin lohkoketjun käytöstä esineiden internetissä (IoT) Christidis & Devetsikiotis 2016. Lee & Pilkington (2017, 20) esittävät, että lohkoketju voisi alentaa hintoja, vahvistaa toimitusketjua, helpottaa erilaisten ongelmien (esim. ympäristövahinkojen) seurantaa ja tuoda läpinäkyvyyttä.

19 Das 2017. Tosin esimerkiksi Suomessa sähköinen äänestys on herättänyt paljon kritiikkiä (ks. Keränen 2016).

20 Ks. OP Ryhmä 2015; Elinkeinoelämän keskusliitto 2016. Esimerkiksi Tanska on suunnitellut e-kruunua (Levring 2016), kuten myös Norja (Nicolaisen 2017). Islanti kielsi Bitcoinin vuonna 2013, jolloin se otti laajaan käyttöön toisen digitaalisen valuutan, Auroracoinin (ks. Swan 2015a, 6–7). Ranskan pankki- ja finanssiryhmittymä Crédit Agricole on suunnitellut Bitcoinin hyväksymistä investoinneissa (Keirns 2017). Venäjä taas on alkanut kartoittaa lohkoketjun käyttöä julkisissa palveluissa (Higgins 2017).

21 Ks. Kastelein 2017; laajemmin Mersch 2017; Grym ym. 2017.

22 Metz 2017a. Ks. myös Carlson-Wee 2017.

23 Orcutt 2017; European Parliament 2017, 9–10; *CoinDesk* 2017.

24 Hakkerietiikasta sekä avoimesta ja vapaasta koodista esim. Vadén & Stallman 2002; Benkler 2006, 60–63; Thrift & French 2005, 171. Yksi tärkeimmistä esimerkeistä on Linus Torvaldsin alkujaan kehittämä ja sittemmin laajan verkoston synnyttänyt Linux-käyttöjärjestelmä (Benkler 2006, 65–66). Tätä avoimen lähdekoodin yhteistuotantoa voidaan kutsua myös lahjatalouden muunnelmaksi (Barbrook 1998).

25 Esim. Mougayar 2016, ”1. What is Blockchain?”

26 Huckle & White ovat kuvanneet (2016), lohkoketjuteknologian sosialistisia piirteitä. Poliittisesta monimuotoisuudesta myös Honkanen 2017b, 5–6.

27 Internetverkon rakenteesta esim. Watson 2012, luku 8. ”Weaving the Web”.

28 Hillis 1999, 145–147.

29 Hinton ym. 1990, 249–251; Musiani & Méadel 2016; Hillis 1999, luku 8; myös esim. Gere 2008, 58.

30 Watson 2012, 167–168; Gere 2008, 55–56, 71–72; Galloway 2014, 111–114; laajemmin Wiener 1985.

31 Esim. *Posthumanismi* 2014, 14–15; Tuusvuori 2010.

32 Esimerkiksi videotiedostoa ladattaessa vertaisverkko-ohjelmisto lataa samanaikaisesti monelta eri käyttäjältä osia videosta eli datapaketteja. Ratkaisu on tehokas, sillä verkon kaista on tavallaan jaettu käyttäjien kesken, eikä yhdeltä ”keskukselta” vaadita suuria määriä levytilaa tai nopeaa yhteyttä. Monet vertaisverkkopalveluista eivät ole sinänsä laittomia, mutta niissä jaetaan usein luvatta tekijänoikeuksilla suojattua materiaalia. Myös esimerkiksi 1990- ja 2000-lukujen vaihteessa aloitettu SETI@home-projekti hyödynsi käyttäjien konetehoa purkaessaan avaruudesta vastaanotettuja viestejä ja radiosignaaleja (Benkler 2006, 82; Korpela ym. 2001).

33 Swan 2015a, 11; Chaum 1983.

34 Ks. Dwork & Naor 1992.

35 Dierksmeier & Seele 2016; Boellstorff 2008. Myös esim. Edward Castronova kirjoitti jo vuonna 2002 virtuaalitalouksista.

36 Elektronisesta rahasta esim. Hart 2000, 261–270; Narayanan ym. 2016, 7–15. Kryptografiasta esim. Dupont 2014. DigiCashistä Pitta 1999.

37 Nakamoto 2008; Ethereum/Wiki, ”History”; O’Hagan 2016. Myös Suomessa on 1990-luvun puolivälissä vaikuttanut Digicash-yrityksen Ecash, jonka suomalaisena levittäjänä toimi EUnet ja jonka transaktiot kulkivat Meritan (nyk. Nordea) kautta. Tarkoituksena oli ilmeisesti ”ladata” rahaa (enimmillään sata markkaa) e-lompakkoon, jolla voitiin sitten maksaa ostoksia. (Narayanan ym. 2016, 11–14. Ks. myös netlab.tkk.fi/opetus/s38118/s98/htyo/49/ecash.shtml.)

38 Ks. Hoepman 2008. *Double-spend*-ongelmaa ja sen vertaisverkkoratkaisuja ovat käsitelleet jo 2007–2008 esim. Opiskov ym. 2007.

39 Tschorsch & Scheuermann 2016, 2084–2086; Ks. myös Ethereum/Wiki. ”History”.

40 Haber & Stornetta 1991; Narayanan ym. 2016, 16–17.

41 Karlstrøm 2014, 28; Lauslahti ym. 2017, 3.

42 Esim. Redlich & Moritz 2016, 27–29; myös esim. Jakonen 2015.

43 Esim. Pratt 2015; Swan 2015b, 42–43.

44 Smith 2016.

45 Esim. coinmarketcap.com. Syksyllä 2017 sivustolla oli listattuna yli 1 300 kryptovaluuttaa. Ks. laaja globaali tutkimus erityisesti suurimmista kryptovaluutoista, Hileman & Rauchs 2017.

46 Bitcoinin arvon kehitystä voi seurata reaaliaikaisesti osoitteessa: coindesk.com/price/.

47 Swan 2015a, 17. Reijers ym. (2016, 135) määrittelevät tämän älysopimusmallin desentralisoiduksi ”sopimusten pakottamiseksi”.

48 Esim. Szabo 1997.

49 Swan 2015b, 43.

50 Wood 2017; ks. Myös Ethereum/Wiki; CoinDesk 2016.

51 Das 2017.

52 Noizat 2015.

53 Keränen 2016; myös *Aalto.fi* 2016.

54 Noizat 2015, 453.

55 Esim. Buterin 2016.

56 Metz 2017b. Ks. Numeraista myös Metz 2016.

57 Galloway 2004, 7–9, 12; 2014, 111–113; Watson 2012, 168–172; Wilson 2015, esim. ”3. The Physical Structure of the Internet”; Narayanan ym. 2016, 59–60. Esimerkiksi internetissä data siirtyy paketteina, jotka kulkevat tehokkaasti eri reittejä pitkin. Ne siis pirstoutuvat ja ne kootaan taas protokollien osoitejärjestelmän mukaisesti yhteen.

58 Mallard ym. 2014; De Filippi & Loveluck 2016; Karlstrøm 2014, 31–32. Myös itse koodilla (koodikielellä ja binäärikoodilla) on materiaalinen eli sosiaalinen sekä ideologinen ulottuvuutensa (esim. Coeckelbergh & Reijers 2015; Evens 2015, 1). Myös vertaisverkot, hajautettu laskennallisuus ja hajautettu tietojenkäsittely ovat kohdanneet paljon kritiikkiä. Esimerkiksi vertaisverkoissa toistuvat yleensä yksittäisten solmujen prosessien tietämistä koskevat

Isa Maaranen, *Yhä uudelleen* (2016), öljyväri kankaalle, 200 × 150 cm

ongelmat ja keskinäisen synkronoinnin ja ongelmankäsittelyn heikkoudet. Näiden lisäksi ilmenee eräänlaisia aliongelmia esimerkiksi ajan synkronoinnissa tai lokaalien ja globaalien tasojen välisessä vuorovaikutuksessa. Monet ongelmista toistuvat lohkoketjuissa. Toisaalta lohkoketjurakenne pyrkii ohittamaan esimerkiksi verkon niukkojen resurssien ongelman siten, että laskentateho on periaatteessa kaikkien käytössä. (Ghosh 2007, 6–9. Hajautettujen järjestelmien kohtaamista ongelmista ja lohkoketjuteknologian eräistä korjausehdotuksista ks. Wattenhofer 2016.)

59 Ks. De Filippi 2016.

60 Kostakis & Giotitsas 2014, 436; Narayanan ym. 2016, 48–50. Guadamuz & Marsden 2015; De Filippi 2016, 48–50.

61 Vadén 2016; Swan 2015b, 42. De Filippi & Loveluck ovat tiivistäneet (2016) vertaisverkkoyhteisöjen (P2P) ongelmiksi yhteisön rajojen ja kannustimien määrittämisen, jäsenistön roolit ja konfliktien käsittelyn.

62 Toisaalta esimerkiksi pankkisiirrot eri pankkien välillä voivat kestää parikin päivää. Visalla ei myöskään voi siirtää rahaa suoraan ja välittömästi yksityishenkilöiden välillä, mutta esimerkiksi uudemmilla kryptovaluutoilla – kuten Litecoinilla ja Dashilla – voi.

63 Yli-Huumo ym. 2016. Kirjoittajat myös summaavat lohkoketjututkimusta. Siinä on keskitytty pääasiassa turvallisuuteen, resurssihukkaan ja käytettävyyteen. Esimerkiksi latenssista, moniketjuisuudesta, ketjun koosta, ketjun jakaantumisesta (*forking*) ja kaistanleveydestä ei kirjoittajien mukaan ole juurikaan tutkimuksia. He myös jatkavat, että moniakaan tutkimuksia ei ole julkaistu ”korkealaatuisissa aikakausjulkaisuissa” (sama, 22). Ks. tiiviisti myös O’Dwyer 2016.

64 Golumbia 2016. Louhijat lisäävät lohkoja ketjuun jatkuvasti, mutta huijari alkaa ikään kuin luoda omaa ketjua, joka haarautuu ”oikeasta ketjusta”. Bitcoinin yhteydessä pisin lohko voittaa tai hyväksytään ”oikeaksi”, joten huijarilla olisi oltava enemmän konetehoa kuin muilla louhijoilla (ks. Ethereum/Wiki, ”History”). Lohkojen tarkistuksen huijaamisesta ks. Narayanan ym. 2016, 59–60; Malmo 2015; Lanchester 2016.

65 Ks. Felten 2014. Dallyn (2017, 470) esittää, että vuonna 2016 noin 70 prosenttia louhinnasta hallitsi neljä kiinalaista louhintainstituuttia, jotka ovat myös pyrkineet estämään nykyisen megatavun lohkokoon suurentamisen.

66 Esim. Guadamuz & Marsden 2015.

67 De Filippi 2016; Huckle & White 2016; Malmo 2015; 2017; Martin 2017. Christopher Malmon mukaan Bitcoin pystyy käsittelemään noin 360 000 transaktiota päivittäin (vuonna 2015), mutta Visa taas noin 160 miljoonaa päivittäin (vuoden 2013 tiedot; Malmo 2015; Visa 2013). Malmo kritisoi myös Hass McCookin (2014) analyysiä, jonka mukaan Bitcoin tuottaisi moninkertaisesti vähemmän hiilidioksidia kuin perinteinen pankkijärjestelmä. McCook ei oikeastaan ollenkaan huomioi näiden järjestelmien kokoeroja. Bitcoinin ja Ethereumin energiankulutusta voi seurata osoitteessa: digiconomist.net.

68 Hecht 2016.

69 Lähde 2013.

70 Papadopoulos 2015, 168.

71 Ks. tiiviisti Bitcoinin järjestelmän desentralisaatiota rajoittavista piirteistä Böhme ym. 2015, 220–222.

72 Ks. käytännöllisten sovellusten vähäisyydestä ja innovaatiohypen ongelmista esim. Honkanen 2017a; b. Lisäksi on hyvä huomata, että yksityisillä lohkoketjuilla voidaan helpostikin tehostaa (ja onkin tehostettu) organisaatioiden toimintoja, mutta julkisia ketjuja – joiden tarkoitus oli juuri tuottaa todella desentralisoituja alustoja – on hyvin vaikea ottaa käyttöön.

Kirjallisuus

Aalto.fi, Sähköiset vaalit – uhka vai mahdollisuus? Aalto yliopisto 9.12.2016. Verkossa: aalto.fi/fi/current/news/2016-12-09/.

Barbrook, Richard, The Hi-Tech Gift Economy. *First Monday*. Vol. 3, No. 12, 1998. Verkossa: firstmonday.org/ojs/index.php/fm/article/view/631/552.

Benkler, Yochai, *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. Yale University Press, New Haven 2006.

Boellstorff, Tom, *Coming of Age in Second Life. An Anthropologist Explores the Virtually Human*. Princeton University Press, Princeton 2008.

Buterin, Vitalik, A Proof of Stake Design Philosophy. *Medium* 30.12.2016. Verkossa: medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51.

Böhme, Rainer, Christin, Nicolas, Edelman, Benjamin & Moore, Tyler, Bitcoin: Economics, Technology, and Governance. *Journal of Economics Perspectives*. Vol. 29, No. 2, 2015, 213–238.

Carlson-Wee, Olaf, The Future Is a Decentralized Internet. *Techcrunch* 8.1.2017. Verkossa: techcrunch.com/2017/01/08/the-future-is-a-decentralized-internet/.

Castronova, Edward, On Virtual Economies. *Cesifo Working Paper*. No. 752, vii/2002.

Chaum, David, Blind Signatures for Untraceable Payments. *Advances in Cryptology. Proceedings of Crypto 82*, 1983, 199–203.

Chester, Jonathan, The Blockchain Wars. How Startups and Enterprises are Competing to Create the Web 2.0. *Forbes* 14.4.2016. Verkossa: forbes.com/sites/jonathanchester/2016/04/14/the-blockchain-wars-how-startups-and-enterprises-are-competing-to-create-the-web-2-0/#28b6277b14a7.

Christidis, Konstantinos & Devetsikiotis, Michael, Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*. Vol. 4 – Special Section on the Plethora of Research in Internet of Things, 2016. Verkossa: ieeexplore.ieee.org/document/7467408/.

Coeckelbergh, Mark & Wessel Reijers, Cryptocurrencies as Narrative Technologies. *SIGCAS Computers & Society*. Vol. 45, No. 3, 2015, 172–178.

CoinDesk, Understanding Ethereum. 2016. Verkossa: coindesk.com/research/understanding-ethereum-report/.

CoinDesk, EU Politician Pushes Parliament to Test Blockchain Identity for Refugees. *coindesk.com* 31.8.2017. Verkossa: coindesk.com/eu-politician-pushes-parliament-test-blockchain-identity-refugees/.

Dallyn, Sam, Cryptocurrencies as Market Singularities. The Strange Case of Bitcoin. *Journal of Cultural Economy*. Vol. 10, No. 5, 2017, 462–473.

Das, Samburaj, A South Korean Province Used Blockchain Tech for Resident Voting. *Cryptocoinsnews.com* 8.3.2017. Verkossa: cryptocoinsnews.com/south-korean-province-used-blockchain-tech-resident-voting/.

De Filippi, Primavera, The Interplay Between Decentralization and Privacy. The Case of Blockchain Technologies. *Journal of Peer Production*. 9/ix 2016. Verkossa: peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/the-interplay-between-decentralization-and-privacy-the-case-of-blockchain-technologies/.

De Filippi, Primavera & Loveluck, Benjamin, The Invisible Politics of Bitcoin. Governance Crisis of a Decentralised Infrastructure. *Internet Policy Review*. Vol. 5, No. 3, 2016.

Dierksmeier, Claus & Seele, Peter, Cryptocurrencies and Business Ethics. *Journal of Business Ethics*. viii/2016.

DuPont, Quinn, The Politics of Cryptography. Bitcoin and the Ordering Machines. *Journal of Peer Production*. No. 4, 2014. Verkossa: peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/.

Dwork, Cynthia & Naor, Moni, Pricing Via Processing or Combatting Junk Mail. *hashcash.org* 1992. Verkossa: hashcash.org/papers/pvp.pdf.

The Economist, The Trust Machine. 31.10.2015. Verkossa: economist.com/node/21677198/.

Eklund, Henri, Virtuaalivaluutta Bitcoin. Vaihtoehtoinen maksuväline. Opinnäytetyö. Metropolia Ammattikorkeakoulu, Helsinki 2015. Verkossa: urn.fi/URN:NBN:fi:amk-201505127470.

Elinkeinoelämän keskusliitto, Lohkoketjut myllertävät maailmaa enemmän kuin internet. *ek.fi* 21.10.2016. Verkossa: ek.fi/ajankohtaista/uutiset/2016/10/21/lohkoketjut-myllertavat-maailmaa-enemman-kuin-internet/.

Ethereum/Wiki, White Paper. 2017. Verkossa: github.com/ethereum/wiki/wiki/White-Paper.

European Parliament, Budget Amendments 2018. Committee on Economic and

Monetary Affairs. 29.8.2017. Verkossa: europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-609.538&format=PDF&language=EN&secondRef=01.
Evens, Aden, *Logic of The Digital*. Bloomsbury Academic, London 2015.
Felten, Ed, Bitcoin Mining Now Dominated by One Pool. *Freedom to Tinker* 16.6.2014. Verkossa: freedom-to-tinker.com/2014/06/16/bitcoin-mining-now-dominated-by-one-pool/.
Feuer, Alan, The Bitcoin Ideology. *New York Times* 14.12.2013. Verkossa: nytimes.com/2013/12/15/sunday-review/the-bitcoin-ideology.html.
Galloway, Alexander R., *Protocol. How Control Exists after Decentralization*. MIT Press, Cambridge, Mass. 2004.
Galloway, Alexander R., The Cybernetic Hypothesis. *Differences. A Journal of Feminist Cultural Studies*. Vol. 25, No.1, 2014, 107–131.
Gere, Charlie, *Digital Culture*. Reaktion Books, London 2008.
Ghosh, Rishab, Network-centered is an Oxymoron. *First Monday*. Vol. 1, No. 1, 1996. Verkossa: firstmonday.org/ojs/index.php/fm/article/view/467/388.
Ghosh, Sukumar, *Distributed Systems. An Algorithmic Approach*. Chapman & Hall, Boca Raton 2007.
Golumbia, David, *The Politics of Bitcoin. Software as Right-Wing Extremism*. Minnesota UP, Minneapolis 2016.
Grym, Aleksi, Heikkinen, Päivi, Kauko, Karlo & Takala, Kari, Digitaalinen keskuspankkiraha. *BoF Economics Review* 4/2017. Verkossa: helda.helsinki.fi/bof/handle/123456789/14951.
Guadamuz, Andres & Marsden, Chris, Blockchains and Bitcoin. Regulatory Responses to Cryptocurrencies. *First Monday*. Vol. 20, No. 12, 2015. Verkossa: firstmonday.org/ojs/index.php/fm/article/view/6198/5163.
Gupta, Vinay, A Brief History of Blockchain. *Harvard Business Review* 28.2.2017. Verkossa: hbr.org/2017/02/a-brief-history-of-blockchain.
Haber, Stuart & Stornetta, W. Scott, How to Time-Stamp a Digital Document. *Journal of Cryptology*. Vol. 3, No. 2, 1991, 99–111.
Hart, Keith, *The Memory Bank. Money in an Unequal World*. Profile Books, London 2000.
Hecht, Jeff, The Bandwidth Bottleneck. *Nature*. Vol. 536, 2016, 139–142.
Higgins, Stan, Russian PM Orders Research on Public Sector Blockchain Use. *CoinDesk.com* 7.3.2017. Verkossa: coindesk.com/russian-pm-orders-government-research-public-sector-blockchain-use/.
Hileman, Garrick & Rauchs, Michel, *Global Cryptocurrency Benchmarking Study*. Center for Alternative Finance. University of Cambridge, Cambridge 2017.
Hillis, Daniel, *Miten tietokone toimii* (The Pattern on the Stone. The Simple Ideas That Make Computers Work, 1998). Suom. Risto Varteva. WSOY, Helsinki 1999.
Hinton, Geoffrey E., James L. McClelland & Rumelhart, David E., Distributed Representations. Teoksessa *The Philosophy of Artificial Intelligence*. Toim. Margaret A. Boden. Oxford UP, Oxford 1990, 248–280.
Hoepman, Jaap-Henk, Distributed Double Spending Prevention. 15th Workshop on Security Protocols. Cornell University 2008. Verkossa: arxiv.org/abs/0802.0832v1.
Honkanen, Petri, Lohkoketjuteknologian lupaus. *Arcada Working Papers* 1/2017a.
Honkanen, Petri, Lohkoketjuteknologia. Luottamuksen koodi hajautuneessa yhteiskunnassa. *Impulsseja*. Kalevi Sorsa säätiö 10/2017b.
Huckle, Steve & White, Martin, Socialism and the Blockchain. *Future Internet*. Vol. 8, No. 4, 2016.
Jakonen, Mikko, Talous ja työ prekaarissa yhteiskunnassa. Teoksessa *Talouden uudet muodot*.
Toim. Mikko Jakonen & Tiina Silvasti. Into, Helsinki 2015, 92–121.
Karlstrøm, Henrik, Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin. *Distinktion. Journal of Social Theory*. Vol. 15, No. 1, 2014, 23–36.
Karppinen, Juhani, Bitcoin-kryptovaluutta. Kandidaatintutkielma. Oulun yliopisto, Oulu 2015. Verkossa: urn.fi/URN:NBN:fi:oulu-201509222013.
Kastelein, Richard, European Central Bank Considering Digital Currency. Cryptocash. *Blockchain News* 18.1.2017. Verkossa: the-blockchain.com/2017/01/18/european-central-bank-considering-digital-currency-cryptocash.
Keirns, Garrett, Bitstamp Partners with Banking Giant for Bitcoin Investment On-Ramp. *CoinDesk.com* 8.3.2017. Verkossa: coindesk.com/bitstamp-partners-with-banking-giant-to-provide-bitcoin-investment-on-ramp/.
Keränen, Matti, Sähköinen äänestys haluttiin Suomeen, mutta asiantuntijat toppuuttelevat: ”lisää hybridisodan uhkaa”. *Tekniikka & Talous* 9.12.2016. Verkossa: tekniikkatalous.fi/tekniikka/ict/sahkoinen-aanestys-haluttiin-suomeen-mutta-asiantuntijat-toppuuttelevat-lisaa-hybridisodan-uhkaa-6606252.
Korpela, Eric, Werthimer, Dan, Anderson, David, Cobb, Jeff & Lebofsky, Matt, SETI@home. Massively Distributed Computing for SETI. *Computing in Science & Engineering*. Vol. 3, No. 1, 2001, 78–83.
Kostakis, Vasilis & Giotitsas, Chris, The (A) Political Economy of Bitcoin. *tripleC*. Vol. 12, No. 2, 2014, 431–440.
Krugman, Paul, Bitcoin is Evil. *The New York Times* 28.12.2013. Verkossa: krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=0.
Lanchester, John, When Bitcoin Grows Up. *London Review of Books*. Vol. 38, No. 8, 2016, 3–12.
Lauslahti, Kristian, Mattila, Juri & Seppälä, Timo, Smart Contracts – How Will Blockchain Technology Affect Contractual Practices? *ETLA Reports*. No. 68, 2017.
Lee, Jong-Hyouk & Pilkington, Marc, How the Blockchain Revolution Will Reshape the Consumer Electronics Industry. *IEEE Consumer Electronics Magazine*. 7/2017, 19–23.
Levring, Peter, Blockchain Lures Central Banks as Danes Consider Minting E-Krone. *Bloomberg* 11.12.2016. Verkossa:bloomberg.com/news/articles/2016-12-11/blockchain-lures-central-banks-as-danes-consider-minting-e-krone.
Lähde, Ville, *Niukkuuden maailmassa*. niin & näin, Tampere 2013.
Mackenzie, Adrian, *Cutting Code. Software and Sociality*. Peter Lang, New York 2006.
Mallard, Alexandre, Méadel, Cécile & Musiani, Francesca, The Paradoxes of Distributed Trust. Peer-To-Peer Architecture and User Confidence in Bitcoin. *Journal of Peer Production*. No. 4, 2014. Verkossa: peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-paradoxes-of-distributed-trust/.
Malmo, Christopher, Bitcoin is Unsustainable. *Motherboard* 29.6.2015. Verkossa: motherboard.vice.com/en_us/article/ae3p7e/bitcoin-is-unsustainable.
Malmo, Christopher, A Single Bitcoin Transaction Takes Thousands of Times More Energy Than a Credit Card Swipe. *Motherboard* 8.3.2017. Verkossa: motherboard.vice.com/en_us/article/ypkp3y/bitcoin-is-still-unsustainable.
Martin, Will, The Electricity Required for a Single Bitcoin Trade Could Power a House for a Whole month. *World Economic Forum* 16.10.2017. Verkossa: weforum.org/agenda/2017/10/the-electricity-required-for-a-single-bitcoin-trade-could-power-a-house-for-a-whole-month.
McCook, Hass, Under the Microscope: The True Cost of Banking. *coindesk.com* 12.7.2014. Verkossa: coindesk.com/microscope-true-costs-banking/.
Mersch, Yves, Speech by Yves Mersch, at the Farewell Ceremony for Pentti Hakkarainen. European Central Bank. *Neweurope.eu* 16.1.2017. Verkossa: neweurope.eu/press-release/speech-yves-mersch-digital-base-money-an-assessment-from-the-ecbs-perspective/.
Metz, Cade, 7500 Faceless Coders Paid in Bitcoin Built a Hedge Fund's Brain. *Wired* 12.12.2016. Verkossa: wired.com/2016/12/7500-faceless-coders-paid-bitcoin-built-hedge-funds-brain/.
Metz, Cade, Bitcoin Will Never Be a Currency. It's Something Way Weirder. *Wired* 6.1.2017a. Verkossa: wired.com/2017/01/bitcoin-will-never-currency-something-way-weirder/.
Metz, Cade, An AI Hedge Fund Created a New Currency to Make Wall Street Work Like Open Source. *Wired* 21.2.2017b. Verkossa: wired.com/2017/02/ai-hedge-fund-created-new-currency-make-wall-street-work-

like-open-source.
Mougayar, William, *The Business Blockchain. Promise, Practice, and Application of the Next Internet Technology*. Wiley, Hoboken (NJ) 2016.
Musiani, Francesca & Méadel, Cécile, "Reclaiming the Internet" With Distributed Architectures. An Introduction. *Frist Monday*. Vol. 21, No. 12, 2016. Verkossa: firstmonday.org/ojs/index.php/fm/article/view/7101/5654.
Nakamoto, Satoshi, Bitcoin. A Peer-to-Peer Electronic Cash System. *Bitcoin.org* 2008. Verkossa: bitcoin.org/en/bitcoin-paper.
Narayanan, Arvind, Bonneau, Joseph, Felten, Edward, Miller, Andrew & Goldfeder, Steven, *Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction.* Princeton University Press, Princeton 2016.
Nicolaisen, Jon, What Should the Future Form of Our Money Be? Puhe Norwegian Academy of Science and Letters -tapahtumassa, Oslo, 25.4.2017. Verkossa: bis.org/review/r170426d.pdf.
Noizat, Pierre, Blockchain Electronic Vote. Teoksessa *Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Big Data*. Toim. David Lee. Elsevier, Boston 2015, 453–461.
O'Dwyer, Rachel, Blockchains and Their Pitfalls. Teoksessa *Ours to Hack and to Own. The Rise of Platform Cooperativism, A New Vision for The Future of Work and A Fairer Internet*. Toim. Trebor Scholz & Nathan Schneider. O/R Books, London 2016, 228–233.
O'Hagan, Andrew, The Satoshi Affair. *London Review of Books*. Vol. 38, No. 13, 2016, 7–28. Verkossa: lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair.
OECD, *Digital Economy Outlook 2017*. OECD Publishing, Paris 2017. Verkossa: keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en#.WfNOPkwgmfU#page1.
OP Ryhmä, lehdistötiedote. *op.fi* 17.12.2015. Verkossa: op.fi/op?cid=-73775&srcpl=3.
Opiskov, Ivan, Vasserman, Eugene Y., Hopper, Nicholas & Kim, Yongdae, Combating Double-Spending Using Cooperative P2P Systems. Kokoelmassa *27th International Conference on Distributed Computing Systems, Toronto, Canada, 25–27 June*. IEEE Computer Society 2007. Verkossa: ieeexplore.ieee.org/document/4268195/.
Orcutt, Mike, How Blockchain Is Kickstarting the Financial Lives of Refugees. *MIT Technology Review* 5.9.2017. Verkossa: technologyreview.com/s/608764/how-blockchain-is-kickstarting-the-financial-lives-of-refugees/.
Pagliery, Jose, *Bitcoin and the Future of Money*. Triumph Books, Chicago 2014.
Papadopoulos, Georgios, Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies. Teoksessa *Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Big Data*. Toim. David Lee. Elsevier, Boston 2015, 153–172.
Pitta, Julie, Requiem for a Bright Idea. *Forbes* 11.1.1999. Verkossa: www.forbes.com/forbes/1999/1101/6411390a.html.
Posthumanismi. Toim. Karoliina Lummaa & Lea Rojola. Eetos, Turku 2014.
Pratt, Gill A., Is a Cambrian Explosion Coming for Robotics? *The Journal of Economic Perspectives*. Vol. 29, No. 3, 2015, 51–60.
Redlich, Tobias & Moritz, Manuel, Bottom-Up Economics. Foundations of a Theory of Distributed and Open Value Creation. Teoksessa *The Decentralized and Networked Future of Value Creation. 3D Printing and its Implications for Society, Industry, and Sustainable Development*. Toim. Jan-Peter Ferdinand, Ulrich Petschow & Sascha Dickel. Springer International, Heidelberg 2016, 27–58.
Reijers, Wessel, O'Brolcháin, Fiachra & Haynes, Paul, Governance in Blockchain Technologies & Social Contract Theories. *Ledger*. Vol. 1, 2016, 134–151.
Rutter, David E., When is a Blockchain not a Blockchain? *R3.com* 24.2.2017. Verkossa: r3.com/blog/2017/02/24/when-is-a-blockchain-not-a-blockchain/.
Smith, Aaron, Future of Money. Classifying Virtual Currency Systems. *bigthink.com* 2016. Verkossa: bigthink.com/hybrid-reality/future-of-money-classifying-virtual-currency-systems.
Swan, Melanie, *Blockchain. Blueprint for a New Economy*. O'Reilly Media, California 2015a.
Swan, Melanie, Blockchain Thinking. The Brain as Decentralized Autonomous Corporation. *IEEE Technology and Society Magazine*. No. 12, 2015b, 41–52.
Szabo, Nick, Formalizing and Securing Relationships on Public Networks. *First Monday*. Vol. 2, No. 9, 1997. Verkossa: firstmonday.org/ojs/index.php/fm/article/view/548/469.
Tapscott, Don & Tapscott, Alex, *Blockchain Revolution. How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin Random House, New York 2016.
Thrift, Nigel & French, Shaun, The Automatic Production of Space. Teoksessa *Knowing Capitalism*. Toim. Nigel Thrift. Sage Publications, London 2005, 153–181.
Troncoso, Carmela, Isaakidis, Marios, Danezis, George & Halpin, Harry, Systematizing Decentralization and Privacy: Lessons From 15 Years of Research and Deployments. *Proceedings on Privacy Enhancing Technologies*. Vol. 4, 2017, 307–329.
Tschorsch, Florian & Scheuermann, Björn, Bitcoin and Beyond. A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*. Vol. 18, No. 3, 2016, 2084–2123.
Tuusvuori, Jarkko S., Pickering teoriasta ja käytännöstä. *niin & näin* 4/2010. Verkossa: netn.fi/lehti/niin-nain-410/pickering-teoriasta-ja-kaytannosta.
Tymoigne, Eric, The Fair Price of a Bitcoin is Zero. *New Economic Perspectives* 2.12.2013. Verkossa: neweconomicperspectives.org/2013/12/fair-price-bitcoin-zero.html.
Vadén, Tere, Three Non-Technological Ways in Which Blockchains May Still "Fail". *A Medium Corporation* 1.11.2016. Verkossa: medium.com/economic-spacing/three-non-technological-ways-in-which-blockchains-may-still-fail-a8d3a7c-238be.
Vadén, Tere & Stallman, Richard M., *Koodi vapaaksi. Hakkerietiikan vaativuus*. Juvenes, Tampere 2002. Verkossa: free.yudu.com/item/details/11245/Koodi-vapaaksi.-Hakkerietiikan-vaativuus.
Watson, Ian, *The Universal Machine. From the Dawn of Computing to Digital Consciousness*. Copernicus Books, New York 2012.
Wattenhofer, Roger, *The Science of the Blockchain*. Inverted Forest Publishing 2016.
Wiener, Norbert, *Cybernetics, or Control and Communication in the Animal and the Machine*. The MIT Press, Cambridge (ma) 1985.
Wilson, Steven Lloyd, How to Control the Internet. Comparative Political Implications of the Internet's Engineering. *First Monday*. Vol. 20, No. 2, 2015. Verkossa: firstmonday.org/ojs/index.php/fm/article/view/5228/4204.
Visa, Annual Report 2013. Verkossa: s1.q4cdn.com/050606653/files/doc_downloads/annual%20meeting/Visa%20Annual%20Report%20%202013%20final%20website.pdf.
Wood, Gavin, Ethereum. A Secure Decentralised Generalised Transaction Ledger. *cryptopapers.net* 2017. Verkossa: cryptopapers.net/papers/ethereum-yellowpaper.pdf.
Yli-Huumo, Jesse, Ko, Deokyoon, Choi, Sujin, Park, Sooyong & Smolander, Kari, Where is Current Research on Blockchain Technology? A Systematic Review. *PLoS ONE*. Vol. 11, No. 10, 2016.