Lohkoketjut ja muut hajautetut tietokannat: niiden ideologia, käyttökohteet ja energiankulutus

Asiantuntijalausunto eduskunnan tulevaisuusvaliokunnalle

U 69/2018 vp

Janne M. Korhonen
DI, FT
Turun yliopiston kauppakorkeakoulu / Aalto-yliopiston kauppakorkeakoulu
janne@jmkorhonen.fi
041 501 8481

Sisällysluettelo

Johdanto ja tiivistelmä....2
Tausta asiantuntemukselleni ja sidonnaisuudet....5
Lohkoketjuteknologia ja sen ideologinen ja teknologinen tausta....6
Lohkoketjujen ja kryptovaluuttojen todellisuus....9
Hajautettu tietokanta kansallisen muistin turvana?....12
Lohkoketjuteknologian energiankulutus ja ympäristövaikutukset....13
Yksityisyys, tietoturva, älysopimukset ja etiikka....16
Lähteet....19

Johdanto ja tiivistelmä

Kiitän tilaisuudesta kommentoida kirjelmää U 69/2018 vp aiheesta **lohkoketjut ja energiankulutus**. Kaksi vuotta aihetta tutkineena pidän kysymystä ajankohtaisena ja nähdäkseni on hyvin mahdollista, että eduskunta ja/tai Euroopan parlamentti ja neuvosto joutuvat ottamaan asiaan liittyviin kysymyksiin kantaa lähitulevaisuudessa. Aiheesta liikkuu myös paljon erisuuntaisia mielipiteitä ja kokonaisuutena ilmiössä on havaittavissa erittäin suuria hypekuplan merkkejä. On myös selviä merkkejä siitä, että lohkoketjuteknologian edistämisestä taloudellisesti hyötyvät ja teknologiaan ideologisista syistä varsin kritiikittömästi suhtautuvat tahot pyrkivät vaikuttamaan lainsäätäjiin niin, että lohkoketjuteknologioiden kannalta ongelmallista regulaatiota purettaisiin. Teknologian erityinen suosiminen ei kuitenkaan mitenkään välttämättä ole yleisen edun mukaista. Näistä syistä kriittisten asiantuntijoiden – myös muiden kuin allekirjoittaneen – lausunnoille on syytä antaa asiassa merkittävä painoarvo.

Tämän raportin tarkoitus ei ole vastustaa uuden tekniikan kehitystä, vaan antaa kriittinen näkökulma aiheeseen, josta puhuvat ennen kaikkea teknologiaan erittäin positiivisesti suhtautuvat ja sen edistämisestä hyötyvät tahot.

Tiivistettynä keskeiset huomioni ovat seuraavat:

1. Aikamme ylivoimaisesti keskeisimmän poliittisen kysymyksen eli sivilisaatiomme ja mahdollisesti lajimme tulevaisuuden vaarantavan ilmastonmuutoksen ja elinympäristöjen tuhon estämisen näkökulmasta lohkoketjuteknologioilla on tällä hetkellä lähinnä negatiivisia vaikutuksia, mutta teknologiassa on nähtävissä pieniä mahdollisuuksia mm. jakamistalouden ja yhteisöllisempien, pienimuotoisempien ja vähemmän ympäristörasitusta aiheuttavien talouden ja yhteiselon muotojen edistämiseksi.
2. Lohkoketju (blockchain) on lyhyesti sanottuna eräs tapa toteuttaa monen käyttäjän hajautettu tietokanta, johon tallennetun tiedon luotettavuuden voi periaatteessa kuka tahansa varmentaa ilman, että tietokannalla olisi yhtään varsinaista ”ylläpitäjää” tai muuten sen luotettavuudesta takuuseen menevää tahoa. Yleensä kyseiset tietokannat ovat myös sellaisia, joihin on mahdollista lisätä tietoa, mutta joista tietojen poistaminen on vaikeaa. Tämä muuttamattomuus on omiaan aiheuttamaan ongelmia mm. yksityisyyden suojan ja tietoturvan kanssa.
3. Yleisemmin voidaan puhua *monen käyttäjän hajautetuista tietokannoista* (distributed ledger technology). Lohkoketju on yksi tekninen tapa toteuttaa tällainen tietokanta.
4. Teknologia kehitettiin ratkaisemaan hajautetun, anonyymin elektronisen valuutan kehittämisestä kiinnostuneiden kohtaama ongelma: miten toteuttaa luotettava tietokanta kunkin käyttäjän omistuksista ilman, että tietokannalla olisi ylläpitäjä, jonka toiminnan viranomaiset voisivat esimerkiksi rahanpesuepäilyjä selvitellessään lopettaa? Tämän ongelman ratkaiseminen vaati tiettyjä teknisiä ratkaisuja, jotka tekevät lohkoketjuista ja useimmista muista hajautetuista tietokannoista huonosti sopivia muunlaisten ongelmien ratkaisemiseksi. Hajautettu tietokanta onkin teknisesti kiinnostava ratkaisu ongelmiin, joita on lähinnä niillä, jotka pitävät ideologisista syistä kaikkia ”keskitettyjä” palveluja lähtökohtaisesti epäluotettavina.

5. Tietokanta, jonka luotettavuus voidaan varmentaa hajautetusti, on potentiaalisesti arvokas teknologia. Tällä hetkellä lähes kaikki hajautetuilla tietokannoilla toteutettavaksi kaavaillut lailliset palvelut voitaisiin kuitenkin toteuttaa, usein helpommin ja halvemmalla, perinteisillä tekniikoilla. Tekniikkaan sisältyy vakavia sisäsyntyisiä rajoitteita, mukaanlukien vaikeasti ratkaistavia juridisia ongelmia, ja sitä kehitetään vahvasti teknologian ja teknologiasta innostuneiden ehdoilla, usein pysähtymättä miettimään, ratkaiseeko tekniikka mitään sellaista ongelmaa, mitä a) suuremmalla joukolla ihmisiä on ja b) jota ei voitaisi ratkaista paremmin jotenkin muuten. Hyvä tapa ajatella lohkoketjuteknologiaa on nähdä se hitaana, monen käyttäjän tietokantana: jos jokin ongelma ei ole ratkaistavissa tietokannalla, se tuskin on ratkaistavissa myöskään lohkoketjuilla.
6. Yhdeksän vuoden kehitystyöstä huolimatta varsinaisessa ”tuotantokäytössä” on lähinnä erilaisia kryptovaluuttoja ja olemassaolevaa sijoituslainsäädäntöä kiertäviä *de facto* sijoitusinstrumentteja, ns. ICOja. Kryptovaluuttojen pääasiallinen käyttökohde on edelleen äkkirikastumisen toivossa tehty spekulaatio ja rikollisiin tarkoituksiin tehdyt rahansiirrot; tekniset rajoitteet ja spekulaatiosta sekä todennäköisesti markkinamanipulaatiosta johtuva korkea volatiliteetti ovat johtaneet siihen, että edes teknologiakehittäjien omat konferenssit eivät välttämättä hyväksy kryptovaluuttoja maksuvälineenä. Teknologiaa kehittävien ja siitä innostuneiden väitteet teknologian käyttökohteista vastaavat todellisuutta vain harvoin, ja jopa suuret yritykset antavat lausuntoja, joiden totuusarvo on kyseenalainen. Ala on sääntelemätön ja suuri osa tarjoomuksista on suoria huijauksia, useiden muiden muistuttaessa enemmän tai vähemmän uhkapelejä tai pyramidihuijauksia. Kuluttajansuojaa ei käytännössä ole, ja toimijat esittävät mitä villimpiä väitteitä tarjoomustensa hyödyistä. Useat tarjoomukset ja niistä esitetyt väitteet ovat eri maiden viranomaisten tutkittavina ja tuomioita on odotettavissa tulevaisuudessa.
7. Teknologian ympärille kehittynyt hypekupla on monin suhtein pahempi kuin 1990-luvun lopun IT-kupla. Hypekuplan ja useiden teknologiaa edistävien vahvan ideologisen (yleensä libertaristisen ja valtiovastaisen) latauksen seurauksena lähes kaikki julkisuudessa saatavilla oleva materiaali on värittynyttä. Teknologian kritiikki herättää teknologiayhteisössä vahvan torjuntareaktion, ja väitteitä kyseenalaistavien on syytä varautua voimakkaisiin reaktioihin.
8. Teknologian kannattajilla on vahva taipumus esittää asiansa niin, että teknologia itsessään on erinomainen ratkaisu mitä moninaisimpiin yhteiskunnallisiin ongelmiin, ja että lainsäätäjien tulisi kiireellisesti purkaa kaikki regulaatioesteet sen käyttöönotolta. Näitä esityksiä tehostetaan vetoomuksilla mm. pysäyttämättömästä kehityksestä, teknologisen kehityksen kelkasta putoamisesta ja edelläkävijyyden eduista.
9. Kaikkiin teknologiaa kauppaavien esittämiin väitteisiin, myös suurten yritysten edustajien esittämiin, on syytä suhtautua huomattavan kriittisesti ja näyttöä ja demonstraatioita vaatien. Esitettyjä teknologioita ei välttämättä ole edes olemassa, saati tuotantokäytössä.
10. On kuitenkin mahdollista, että tapahtuvan kehitystyön myötä monen käyttäjän hajautetuista tietokannoista saadaan tulevaisuudessa käyttökelpoisempia ja niiden käytännöllistä soveltamisalaa voidaan laajentaa käytännössä ainoasta todella kilpailukykyisestä käyttökohteesta, kryptovaluutoista (tunnetuin esimerkki Bitcoin), muille alueille. *Lohkoketjuteknologian kenties suurin lupaus on siinä, että sitä käyttäen voi olla mahdollista kokeilla ja prototypoida vertaisverkoissa pienin kustannuksin sellaisia palveluita, joiden kokeilu aikaisemmin vaati vakavaraista, luotettavaa kolmatta osapuolta.*

11. Teknologian keskeisin mukanaan tuomat ”uudistukset” ovat a) laajentunut ymmärrys siitä, että tietokantoihin tallennettu tieto voidaan haluttaessa varmentaa niin, että tietokannan peukaloinnista jää jälki, ja b) kiinnostus tietokantojen hajauttamista kohtaan. Tietojen varmentamiseen käytetty ”Merkle tree”-rakenne on tosin tunnettu jo vuodesta 1979, ja monen käyttäjän hajautettuihin tietokantoihin tarvittavia algoritmeja on ollut olemassa vuodesta 1989. Teknisistä rajoitteista johtuen näitä rakenteita ei ole käytetty kovin paljon.
12. Eräs potentiaalisesti merkittävä hajautettuja tietokantoja hyödyntävä sovelluskohde voisi olla julkisten ja kansallisten digitaalisten arkistojen varmentaminen mm. kyberhyökkäyksiä vastaan. Peukalointiyritykset paljastava, aikaleimattu tietokanta voisi ehkäistä esimerkiksi arkistotietojen, uutisten tai peräti historian vääristelyllä poliittista vaikuttamista pyrkimään tekevät kyberhyökkäykset.
13. Mikäli niin päätetään, lainsäätäjä ja viranomaiset kykenevät halutessaan lähes pysäyttämään kryptovaluuttojen ja sijoitusinstrumenttien omaisten palveluiden käytön esimerkiksi a) hankaloittamalla oikeaa rahaa vastaanottavien tai tarjoavien välittäjien toimintaa, b) kiristämällä kryptovaluuttojen ja spekulatiivisten sijoitusinstrumenttien verokohtelua, c) määrittelemällä kyseisten valuuttojen vastaanoton vähittäiskaupassa laittomaksi ja d) ohjeistamalla Tullia ja muita viranomaisia pysäyttämään kuljetukset, jotka tulevat epäillyiltä ulkomaisilta kryptovaluuttoja hyväksyviltä kauppiailta. Teknologiaa itsessään on vaikea kieltää, mutta sen käyttämisestä on mahdollista tehdä vaikeaa ja paljastumisriskistä suurta.
14. Hajautettujen tietokantojen ja erityisesti lohkoketjuteknologian energiankulutus on teknologian suorituskykyyn nähden suuri tai erittäin suuri. Kulutus on myös joustamatonta, vaikeuttaen sähköverkon dekarbonisointia. Esitetyt ratkaisut energiankulutuksen vähentämiseen tuovat mukanaan muita haasteita.

Olen käytettävissä mikäli haluatte lisätietoja tässä tai muissa osaamiseni piiriin kuuluvissa asioissa.

Tausta asiantuntemukselleni ja sidonnaisuudet

Olen Teknillisestä korkeakoulusta 2009 diplomi-insinööriksi ja Aalto-yliopiston kauppakorkeakoulusta 2017 filosofian tohtoriksi valmistunut tutkija, jonka erikoisalaa on tieteen- ja teknologiantutkimus (science and technology studies). Olen julkaissut aihepiiristä tutkimuksia arvostetuissa kansainvälisissä julkaisuissa, kuten teknologian historian johtavassa lehdessä *Technology & Culture*ssa sekä *Ecological Economic*sissa. Tutkimustyön lisäksi minulla on kokemusta mm. käyttäjälähtöisestä tuotekehityksestä: olen ollut 2007-2010 suunnittelutoimisto Seos Designin perustajaosakas. Elokuusta 2016 elokuuhun 2018 olen työskennellyt täysipäiväisenä tutkijana Aalto-yliopiston Tekes-rahoitteisessa ReCon-projektissa. Projektin tarkoituksena oli tutkia lohkoketjuteknologioiden ja hajautettujen tietokantojen vaikutuksia erityisesti suomalaiseen yhteiskuntaan ja yrityksiin. Tätä kirjoittaessa projektin loppuraportin kirjoittaminen on vielä kesken. Projektin tulosten julkaiseminen kirjamuodossa sai äskettäin Tiedonjulkistamisen neuvottelukunnan apurahan. Tällä hetkellä olen Turun kauppakorkeakoulussa tutkijana (research fellow) ja opettajana.

Taloudelliset sidonnaisuuteni ovat seuraavat: kirjoitushetken kurssilla omistan teoriassa n. 10 000 € arvosta kryptovaluutta Etheriä (ETH) ja n. 100 € arvosta kryptovaluutta LiteCoinia. Omistusten arvo on kuitenkin voimakkaasti heittelevä ja arvostus lähinnä teoreettista. Huomautan, että kritiikkini kryptovaluuttoja kohtaan pätee myös omistamiini kryptovaluuttoihin, ja että yleisen edun nimissä myös näiden valuuttojen sääntely on paikallaan. Ehdotuksillani ei pitäisi olla positiivisia vaikutuksia mihinkään muihin omistuksiini.

Lohkoketjuteknologia ja sen ideologinen ja teknologinen tausta

Kuva 1: Bitcoin selitettynä yhdellä twiitillä.

Lohkoketjuteknologia (blockchain) on yksi tekninen toteutus niinsanotulle hajautetulle tietokannalle (distributed ledger). Kaikki lohkoketjut ovat hajautettuja tietokantoja, mutta kaikki hajautetut tietokannat eivät ole lohkoketjuja. ”Lohkoketju” on kuitenkin muodostunut yleiskäsitteeksi ja on tällä hetkellä tunnetuin esimerkki hajautetusta tietokannasta. Käsite on myös erityisesti teknologioita markkinoivien suosiossa, ja lainsäätäjä todennäköisimmin törmää juuri tähän termiin. Teknologioiden erot eivät myöskään ole tällä hetkellä välttämättä lainsäätäjän näkökulmasta merkittäviä.

Lohkoketju on lyhyesti sanoen tietokanta, jonka tietueet (block) on sidottu toisiinsa ketjuksi (chain) käyttäen niinsanottua Merkle tree-tekniikkaa (keksitty 1979) niin, että tietueiden jälkikäteinen muokkaaminen esim. epärehellisen käyttäjän toimesta paljastuu. ”Perinteinen” lohkoketjutietokanta perustuu tietokannan hajautukseen kaikille tai suurelle osalle käyttäjiä, ja kannustinjärjestelmään, jolla palkitaan tietokannan ylläpitämiseen tietokoneaikaa ja sähköä uhraavia käyttäjiä.

Lohkoketjuteknologia keksittiin vuonna 2008 ratkaisuksi niinsanottujen kryptoanarkistien ja äärimmäistä sääntelyn purkamista ajavien anarkokapitalistien 1980-luvulta saakka pohtimaan ongelmaan: *miten toteuttaa anonyymi, hajautettu elektroninen valuutta, jonka toimivuus ei riipu mistään yksittäisestä ylläpitäjästä jonka toiminnan viranomaiset voivat keskeyttää?*

Salaus- ja yksityisyydensuojateknologioita ihmisten vapauksien tärkeinä tukipylväinä pitävien kryptoanarkistien ajattelussa tällainen anonyymi elektroninen valuutta olisi keskeinen valtiosta

vapautumisen työkalu. Mikäli valtiot eivät kykene kontrolloimaan käytettyä valuuttaa, kryptoanarkistit ajattelevat, ne eivät myöskään kykene kontrolloimaan ihmisiä. Lohkoketjuteknologian tunnetuin käyttökohde, niinsanottu ”kryptovaluutta” Bitcoin, syntyi ratkaisuksi juuri tähän koettuun ongelmaan, vaihtoehtona 1990-luvulla kokeilluille elektronisen rahan palveluille kuten eGoldille, jotka viranomaiset olivat sulkeneet rahanpesun ja huumekaupan välineinä (Popper, 2015). Teknologia on siis alusta alkaen ollut ensisijaisesti poliittinen projekti, jonka tekniset ominaisuudet ovat olleet alusta saakka alisteisia sen kehittäjien ideologialle.

Anonymiteetin (tosiasiassa pseudonymiteetin: kaikki transaktiot tallentuvat ja käyttäjätilit on mahdollista yhdistää todellisiin henkilöihin) ja hajauttamisen lisäksi Bitcoinin kehittäjän **Satoshi Nakamoton** (tätä kirjoittaessa ei ole tiedossa, onko kyseessä yksittäinen henkilö vai ryhmä kehittäjiä) tavoitteena oli luoda valuutta, joka noudattaisi anarkokapitalistisia, ts. kaikkea markkinoiden sääntelyä vastustavia, ja valtavirtaisen taloustieteen ulkopuolelle jääneen ns. itävaltalaisen koulukunnan libertaareja eli äärimmäisen markkinaliberaaleja talousteoreettisia oppeja sekä toisintaisi kultakantaan perustuneen valuutan ominaisuudet. Kuten Bitcoinin ja sen keskeisten kehittäjien aatemaailmaa ja aatemailman historiaa tutkinut Virginian yliopiston professori **David Golumbia** on kirjassaan *The Politics of Bitcoin: Software as Right-Wing Extremism* (2016) osoittanut, Bitcoinin kehittäjiä on ajanut ideologia, jonka mukaan suuri osa maailman ongelmista johtuu kultakannasta luopumisesta ja niinsanotusta keskuspankki- tai ”fiat-rahasta”. Ideologia on peräisin Yhdysvaltojen laitaoikeistolta ja sen historia ulottuu Yhdysvaltojen keskuspankki Fed’in perustamista vuonna 1913 koskeneisiin riitoihin. Vaikka useimmat Bitcoinia kehittävät eivät ole asiasta tietoisia, kultakannan väitetyt edut ja keskuspankkirahan väitetyt ongelmallisuudet ovat olleet 1950-luvulta lähtien osa juutalaisvastaista äärioikeistolaista propagandaa: kuten Golumbia (2016) osoittaa, toisen maailmansodan jälkeen amerikkalaiset antisemiitit kuten kommunistien maailmanlaajuisesta salaliitosta saarnannut, jopa presidentti **Eisenhoweria** kommunistina pitänyt John Birch Society korvasivat sanan ”juutalainen” yleisesti sanalla ”pankkiiri” ja ”juutalaisten salaliitto” sanoilla ”keskuspankkien salaliitto”. Eufenismi oli aikalaisille selvä, mutta kun kyseisistä, kultakantaa puolustavista teoksista otettiin amerikkalaisten libertaarien toimesta 1990-luvulla uusia painoksia, ajattelun historia jäi suurelta osin unohduksiin (Golumbia, 2016).

Lohkoketjut ja kryptovaluutat ovatkin löytäneet kannattajia erityisesti libertaarien ja anarkokapitalistien parista. Näissä jokseenkin marginaalisissa ja sekä ideologisesti että maantieteellisesti hajanaisissa mutta Internetin myötä yhteyttä pitävissä ajatussuunnissa valtiot ja niiden harjoittama sääntely ovat kaiken pahan alku ja juuri, ja utopia saavutetaan tuhoamalla valtioiden rooli kaikessa muussa paitsi omistusoikeuksien turvaamisessa. Teknologiaa tällä hetkellä kannattavista hyvin suuri osa on poliittiselta ideologialtaan valtiovastaisia libertaareja tai anarkokapitalisteja. Tekniikan kehittäjistä huomattava osa on kryptoanarkisteja, joiden tavoitteena on kehittää täysin nykyisille instituutioille rinnakkainen ja teoriassa ihmisten (tai ainakin parhaimmin toimeentulevien) vapaasti valittavissa oleva ”government as a service”-malli. Tässä idealisoidussa utopiassa ihmiset kilpailuttaisivat myös hallituksia sen mukaan, mikä instituutio takaa heille parhaat edut.

Lohkoketjuteknologioiden ideologisen taustan vuoksi kaikenlaiset päätöksentekoa keskittävät *tekniset* ratkaisut ovat teknologiaa kehittävien mielessä lähtökohtaisesti epäluotettavia, ja tämä vaikuttaa tehtyihin teknologisiin ratkaisuihin. Kuten todettua, lohkoketjutekniikan tekninen tausta on kysymyksessä, miten toteuttaa luotettava kirjanpito esimerkiksi juuri ”pankkitilien” saldon

varmentamiseksi ja peukalointiyritysten ehkäisemiseksi ilman, että käyttäjien täytyy luottaa joko toisiinsa tai mihinkään keskitettyyn tahoon. Tämän sinänsä mielenkiintoisen teknisen ongelman ratkaisemiseksi suurin osa lohkoketjuteknologioista vaatii monimutkaisia, usein energiaa tuhlailevia järjestelyjä. Esimerkiksi Bitcoinin ”tilikirjojen” luotettavuuden varmentamiseksi järjestelmän ylläpitoon osallistuvat ”louhijat” käytännössä pakotetaan tuhlaamaan arvokasta resurssia – sähköä ja laskenta-aikaa. Jos tämänkaltaiseen tuhlailevaisuuteen ei pakotettaisi, järjestelmän pseudonyymisyyden vuoksi vihamielinen hyökkääjä voisi varsin helposti kaapata tai vääristää järjestelmän toiminnan. Seurauksena on tarkasta teknisestä toteutuksesta riippumatta järjestelmä, jonka resurssienkäyttö on tehotonta tai erittäin tehotonta verrattuna esimerkiksi tilanteeseen, jossa kirjanpito annettaisiin yksittäisen luotetun tahon hoidettavaksi. Toinen vastaava esimerkki löytyy tietokannan peruuttamattomuudesta: jotta Bitcoin vastaisi ominaisuuksiltaan kultakantaa ja olisi sekä ”sensuurivapaa” (viranomaistoimien ulottumattomissa) että ”itsenäinen” keskuspankkien tai muiden poliittisten toimijoiden painostuksesta, järjestelmässä ei ole teoriassa mahdollista perua tai muuttaa jo tehtyjä transaktioita, eikä tietokantaan kirjoitettua tietoa pysty periaatteessa poistamaan. Muutokset ovat kuitenkin käytännössä mahdollisia, mikäli enemmistö järjestelmää käytännössä hallitsevista ylläpitäjistä pääsee sopimukseen tietojen poistamisesta tai muuttamisesta. Äskettäin julkisuuteen tulleen tiedon mukaan myös Bitcoinin keskeiset kehittäjät olivat valmiit ”rullaamaan takaisin” tietokantaa eli perumaan transaktioita, mikäli erästä yllättäen havaittua kriittistä bugia olisi ehditty väärinkäyttää ennen sen korjaamista.[1]

Mielenkiintoista kylläkin, teknologiakehittäjien epäluulo päätöksenteon keskittämistä kohtaan ulottuu lähinnä teknologisiin ratkaisuihin. Käytännössä esimerkiksi Bitcoinin kehittäminen lepää varsin pienen, lähinnä teknisen osaamisen ja mielenkiinnon perusteella valikoituneen ja demokraattisen kontrollin ja valvontakäytäntöjen ulkopuolella toimivan sisäpiirin harteilla (mm. Böhme, Christin, Edelman, & Moore, 2015; Bohr & Bashir, 2014; Golumbia, 2016; Popper, 2015). Asiantilan potentiaalinen ongelmallisuus on kuitenkin herättänyt käyttäjien keskuudessa laajempaa keskustelua vasta viime aikoina.

1 Kts. esim. keskustelu https://www.reddit.com/r/btc/comments/9hq27d/theymos_on_rbitcoin_if_the_bug_was_exploited_they/

Lohkoketjujen ja kryptovaluuttojen todellisuus

> *We have elected to put our money and faith in a mathematical framework that is free of politics and human error.*
>
> -*Tyler Winklevoss, varhainen Facebook-sijoittaja,* New York Times*, 11.4.2013*
>
> *Someone ‘Accidentally’ Locked Away $150M Worth of Other People's Ethereum Funds*
>
> -*Otsikko,* VICE Motherboard*, 7.11.2017*

Teknologiaa kehittävien ja käyttävien suurista visioista ja liki kymmenen vuoden kehitystyöstä huolimatta lohkoketjuteknologiaa ei käytetä juuri mihinkään muuhun kuin spekulatiivisten sijoitusinstrumenttien toteuttamiseen. Tällä hetkellä käytössä olevat sovellukset voidaankin jakaa 1) kryptovaluuttoihin kuten Bitcoiniin, 2) sijoituslainsäädännön rajoja koetteleviin piensijoitusinstrumentteihin ICOihin, ja 3) teknologiademoihin.

Kryptovaluutat (*cryptocurrency*) kuten Bitcoin, Ether, Litecoin, Monero ja Dogecoin (muutamia tunnetumpia mainitakseni) ovat sääntelemättömiä sähköisiä maksuvälineitä. Alkuperäisen Bitcoinin ominaisuuksiin tai kehittäjäyhteisöön tyytymättömät kehittäjät ovat vuosien varrella lanseeranneet Bitcoinille useita vaihtoehtoja. Koska Bitcoinin ja lähes kaikkien muiden kryptovaluuttojen kirjanpitoa pyörittävän ohjelmiston lähdekoodi on avointa, uusien kryptovaluuttojen lanseeraaminen on erittäin helppoa, ja tätä kirjoittaessa liikkeellä on yli 1600 erilaista kryptovaluuttaa. Lähes kaikki näistä ovat kuitenkin liki täysin vailla käyttäjiä ja arvoa, ja suuri osa niistä on lanseerattu puhtaasti rahastustarkoituksessa. Bitcoinin ja muiden kryptovaluuttojen arvon nopea nousu onkin houkutellut mukaan sekä äkkirikastumisesta haaveilevia että äkkirikastumisesta haaveilevien kustannuksella rikastumisesta haaveilevia.

On olemassa vahvaa näyttöä siitä, että kryptovaluuttojen kurssia manipuloidaan tietoisesti (Griffin & Shams, 2018). Esimerkiksi Bitcoinin kurssia on erittäin todennäköisesti manipuloitu sopivasti ajoitetuilla ostoilla, johon on käytetty toista, väitetysti dollareihin sidottua kryptovaluuttaa Tetheriä. Tetherin kehittäjät eivät kuitenkaan ole lukuisista pyynnöistä ja vaatimuksista huolimatta kyenneet edelleenkään toimittamaan kunnollista kirjanpitoselvitystä, joka varmistaisi Tetherin olevan todella sidottu dollariin (ts. että jokaista liikkeellelaskettua Tetheriä vastaisi yhden dollarin talletus) ja on hyviä syitä uskoa, että mitään tällaisia takeita ei ole koskaan ollutkaan olemassa. Yhdysvaltojen oikeusministeriön on ilmoitettu tutkivan Tetherin ja sitä liikkeelle laskevan Bitfinex-kauppapaikan toimintaa.[2]

Spekulaation ohella kryptovaluuttojen keskeisin käyttökohde on edelleen niinsanotuissa ”high counterparty risk”-rahansiirroissa, eli suomeksi sanottuna muissa kuin laillisissa transaktioissa. Näihin kuuluvat huumekaupan lisäksi esimerkiksi kiristäjille maksetut maksut mm. viime vuosina

2 Esim. https://www.businessinsider.com/why-cryptocurrencies-are-susceptible-to-market-manipulation-2018-5?IR=T

yleistyneistä, käyttäjien tiedot lukitsevista haittaohjelmista, sekä erilaiset rahansiirrot valuuttakontrollien ulkopuolella. Kryptovaluuttojen korkean volatiliteetin, suurten transaktiokustannusten ja teknisten vaikeuksien vuoksi jopa kryptovaluuttaa kehittävien omissa konferensseissa on jouduttu kieltäytymään kryptovaluutoista maksuvälineinä, ja useimmat kryptovaluuttoja hyväksyneet lailliset liikeyritykset ovat luopuneet niiden käytöstä maksuvälineinä. Kryptovaluuttojen tärkein yksittäinen käyttökohde spekulaation lisäksi onkin huumekaupassa: arviolta vähintään neljännes Bitcoin-käyttäjistä ja puolet Bitcoin-transaktioista liittyy huumekauppaan (Foley, Karlsen, & Putniņš, 2018). Bitcoinin ominaisuudet, kuten kaikkien transaktioiden tallentuminen, tekevät siitä kuitenkin epätäydellisen välineen laittomaan kauppaan, ja Bitcoinin osuus etenkin salatussa Tor-verkossa tapahtuvasta huumekaupasta on laskussa paremmin salattujen kryptovaluuttojen kuten Moneron kasvattaessa suosiotaan.

Toinen lohkoketjuteknologian käyttökohde löytyy niinsanottujen rahakkeiden liikkeellelaskusta (*Initial Coin Offering, ICO*). ICO on useimmiten tapa toteuttaa sääntelemätön joukkorahoituskampanja niin, että rahoitusta hakeva taho laskee liikkeelle lohkoketjutekniikkaan perustuvaa kirjanpitoa hyödyntäviä digitaalisia rahakkeita. Näin toimimalla halutaan erityisesti kiertää osakkeiden liikkeellelaskuun liittyviä raportointi- ja kirjanpitovelvoitteita. Useissa hankkeissa rahakkeita olisi tarkoitus käyttää tulevan palvelun maksuvälineenä, myös palvelutarjoomuksissa, joissa erillisten rahakkeiden käytölle ei vaikuta olevan rahoituksen keräämisen ja teknologian rajoitteiden ohella mitään muuta käytännön syytä.

Kenties hienoin esimerkki sekä teknologian rajoitteista, tekniikkaa kehittävien ajattelutavasta ja suhtautumisen kritiikittömyydestä on DentaCoin. Kyseessä on palvelu, jonka liiketoimintaidea voidaan tiivistää näin: *maailman ongelma on se, että ei ole olemassa erikseen ostettavaa, arvoltaan vaihtelevaa rahaketta, jota voisi käyttää vain ja ainoastaan hammaslääkärilaskujen maksamiseen.* Ilmeisistä kysymysmerkeistä huolimatta DentaCoinia on pidetty yleisesti yhtenä lupaavimmista lohkoketjutekniikkaa ICOissa soveltavista palveluista, ja jopa luotettavina pidetyt tiedotusvälineet ovat suhtautuneet yritykseen ja sen liikeideaan lähes täysin kritiikittömästi.

Sijoittajat ostavat rahakkeita lähinnä spekuloidakseen niiden arvolla: harva palvelu on vielä edennyt toteutusvaiheeseen. Sääntelemättömänä rahoitusinstrumenttina ICOt ovat hämäräperäisten yrittäjien ja suorien huijareiden suosiossa, ja alle puolet kaikista ICOista on ylipäätään olemassa neljä kuukautta liikkeellelaskun jälkeen.[3] Useiden maiden rahoitusmarkkinaviranomaiset ovat aloittaneet ICOihin liittyviä rikostutkintoja, ja joissain maissa, kuten Kiinassa ja Etelä-Koreassa, ne on kielletty kokonaan. On kuitenkin mahdollista, että säännellyt ICOt tulevat jossain vaiheessa olemaan käyttökelpoinen joukkorahoitusinstrumentti muiden joukkorahoitusmuotojen joukossa.

Lohkoketjuteknologian käyttö mihinkään muihin tarkoituksiin on jäänyt runsaasta puheesta huolimatta vähäiseksi. Teknologian käytännön varjopuolet, kuten kehitysympäristöjen kehittymättömyys, pysyviin tietokantoihin sisäsyntyisesti liittyvät tietoturva- ja yksityisyydensuojaongelmat ja käytön hankaluus, ovat saaneet monet teknologiaa kokeilleetkin tahot peräytymään hankkeistaan. Raskaaseen liiketoimintakäyttöön sopivia enterprise-luokan ratkaisuja ei ole tätä kirjoittaessa olemassa, eikä välttämättä edes koekäytössä. Monia väitetysti lohkoketjutekniikkaan perustuvia kokeiluhankkeita

3 https://www.bloomberg.com/news/articles/2018-07-09/half-of-icos-die-within-four-months-after-token-sales-finalized

tarkemmin tutkiessa voidaan myös huomata, että nimitys ”lohkoketju” on saatettu ottaa käyttöön puhtaasti sen markkinointiarvon vuoksi. (Esimerkiksi Viron ”lohkoketju”hankkeen selkärankana pidetty KSI Blockchain ei todellisuudessa ole lohkoketjutekniikkaa, mutta sen nimi muutettiin vuonna 2012 lohkoketjuksi. Parhaana esimerkkinä muotisanan arvosta, alkoholitonta Long Island Ice Tea-drinkkisekoitusta valmistavan yrityksen pörssikurssi liki *nelinkertaistui* kun se yksinkertaisesti muutti nimensä ”Long Blockchain”iksi.[4]) Huolimatta siitä, että myös suuret yritykset ovat innostuneet myymään erilaisia enemmän tai vähemmän nimellisesti lohkoketjuun perustuvia palveluita ja tekniikkaa on koekäytetty useissa eri kohteissa, varsinaiset kaupalliset sovellukset ovat vielä hyvin vähäisiä elleivät olemattomia.

Pitkällä tähtäimellä teknologian todennäköisesti lupaavin käyttökohde on kuitenkin aivan uudenlaisten palvelujen kehittämisen alustana. Lohkoketjujen ja niiden inspiroimien hajautettujen tietokantateknologioiden mahdollistama luotettavan mutta hajautetun tietokannan rakentaminen ilman tarvetta sopia kaikille toimijoille sopivasta luotettavasta osapuolesta voisi parhaimmillaan toimia uusien palveluiden kehittämisessä samalla tavoin kuin 3D-tulostus on toiminut tuotekehityksessä: kun uusien palveluiden kehittäminen toimiviksi prototyypeiksi saakka helpottuu, saatamme vielä nähdä monia nyt vaikeasti kuviteltavissa olevia elektronisia palveluita.

Esimerkiksi suomalainen Arvotakomo-osuuskunta pyrkii rakentamaan teknologian avulla kehittyneen ”aikapankki”järjestelmän, jossa yksittäiset ihmiset voisivat ”luotottaa” ja ”jäädä velkaa” toisilleen periaatteessa mistä tahansa asiasta, työtunneista tavaraan. Rahallisten sijasta ihmiset voisivat tallentaa järjestelmään esimerkiksi aika- tai tavaraluottoja (”Matti luottaa Maijaan kahden työtunnin ja kolmen kaljan verran”). Mikä tärkeintä, järjestelmä mahdollistaisi ”maksujen” välittämisen toisiaan tuntemattomien ihmisten välillä: mikäli Mikko haluaisi tarjota Maijalle kaljan kiitokseksi hyvästä blogikirjoituksesta mutta tuntisi vain Matin, järjestelmä osaisi yhdistää Mikon Maijaan Matin kautta ja kehottaisi Mattia tarjoamaan Maijalle oluen. Vaikka järjestelmän toiminta on vaikea kuvata tiiviisti, vastaava järjestely on todennäköisesti ollut alunperin rahatalouden syntymisen taustalla (Graeber, 2011), ja kehittynyt teknologia mahdollistaisi tällä tavoin tietynasteisen irtautumisen yksinomaan rahasta sosiaalisen vaihdannan välineenä tilanteissa, joissa vaihtajat eivät tunne toisiaan. Järjestelmällä voisi siten olla positiivisia implikaatioita esimerkiksi vertais- ja jakamistalouden edistämisen kannalta.

Tällä hetkellä näyttää luultavalta, että ”perinteiset,” täysin hajautetut lohkoketjuteknologiat eivät tule missään vaiheessa olemaan merkittäviä teknologioita muissa kuin kryptovaluuttojen kaltaisissa erikoiskohteissa: ”luotetun osapuolen” käyttämisestä on edelleen merkittäviä etuja. Tekniikan pohjalta luotuja ratkaisuja voidaan kuitenkin hyödyntää tavoiteltaessa hajautetumpia, paremmin varmennettuja tietokantoja ja esimerkiksi tietokantoja, joiden hallintaoikeus on jaettu useamman luotetun käyttäjän kesken.

4 https://www.bloomberg.com/news/articles/2017-12-21/crypto-craze-sees-long-island-iced-tea-rename-as-long-blockchain

Hajautettu tietokanta kansallisen muistin turvana?

> *Joka hallitsee menneisyyttä, hallitsee tulevaisuutta; joka hallitsee nykyisyyttä, hallitsee menneisyyttä.*
>
> *-George Orwell,* 1984

Erityismaininnan ansaitsee lohkoketjujen tai vastaavien hajautettujen tietokantateknologioiden käyttö kansallisten digitaalisten arkistojen ja muiden yhteiskunnalliselle muistille tärkeiden arkistojen, kuten lehtien arkistojen, varmentamisessa. Kyberhyökkäyskykyjen kehittyessä on pidettävä mahdollisena, että hyökkääjä tai tahaton vahinko saattaa vaikuttaa merkittäviin kansallisiin arkistoihin vaarantaen arkistoidun tiedon luotettavuuden. Arkistoista voidaan poistaa suunnitelmallisesti tiettyjä tietoja tai niihin saatetaan ujuttaa virheellisiä tietoja. Koska arkistoja ei välttämättä seurata aktiivisesti eikä kansallisen muistin kannalta keskeisiä arkistoja ole haastattelujemme mukaan erityisesti vahvistettu kyberuhkia vastaan, hyökkäys ei mitenkään välttämättä paljastu ennen kuin on liian myöhäistä, ja on täysin mahdollista, että hyökkäys näin vaarantaisi myös varmuuskopioitavien tietojen luotettavuuden.

Tämänkaltaisen hyökkäyksen mahdollisuudet esimerkiksi levittää disinformaatiota tai yleisesti hämmennystä ja epäluottamusta julkisia tahoja ja toimijoita kohtaan ovat suuret. Nyt jo on lukuisia esimerkkejä tapauksista, joissa esimerkiksi Wikipedian artikkeleita pyritään editoimaan virheellisen tiedon lisäämiseksi yleiseen tietoisuuteen. Nämä hyökkäykset olisivat merkittävästi tehokkaampia, mikäli esimerkiksi lehtien arkistojen luotettavuus saataisiin horjumaan.

Yksi erittäin mahdollinen, teknisesti toteutettavissa oleva tapa vähentää tämänkaltaisten historiaa väärentämään pyrkivien hyökkäysten riskiä ja hallita niiden tuhoja olisi tallentaa arkistot vaikeasti väärennettävään lohkoketju- tai vastaavaan tietokantaan ja hajauttaa tietokanta useiden toimijoiden, kenties useiden valtioiden hallintaan. Tietokantaan voitaisiin tallentaa joko täydelliset dokumentit tai, todennäköisemmin, pelkästään niinsanottu hash-varmenne alkuperäisistä dokumenteista. Hash-varmenne toimii kuin henkilötunnuksen viimeinen tarkistusmerkki: se on alkuperäisestä tiedostosta laskettu tarkistussumma, jonka avulla voidaan luotettavasti todentaa, että tarkasteltava tiedosto vastaa alkuperäistä. Varmenteesta itsestään ei kuitenkaan voida palauttaa tiedoston sisältöä sen enempää kuin henkilötunnuksen viimeisestä merkistä voidaan päätellä koko henkilötunnusta. Tällainen ”varmistusleimajärjestelmä” olisi yksinkertaista ulottaa myös esimerkiksi lehtikirjoitusten ja vaikka yksityisten kansalaistenkin blogi- ym. kirjoitusten tarkistussummien tallentamista varten.

Olemme selvittäneet projektin osana arkistojen varmentamisjärjestelmän toteutettavuutta ja mahdollisuuksia. Järjestelmään on kiinnostusta mm. Kansallisarkistossa, ja se on teknisesti täysin toteutettavissa. Järjestelmä kuitenkin kannattaisi toteuttaa monikansallisena yhteistyönä, esimerkiksi koko EU:n tai Pohjoismaiden ja/tai Baltian maiden kansallisten arkistojen kanssa. Nämä kansalliset arkistot voisivat toimia luotettuina tahoina, jotka ylläpitäisivät järjestelmää ja tallentaisivat toistensa varmennearkistot, jotta mahdollisen hyökkäyksen tai onnettomuuden seurauksena varmenteet voitaisiin palauttaa. Arkistojen tai vastaavien julkisten instituutioiden käyttäminen luotettuina tahoina ratkaisisi myös lohkoketjuteknologiaan usein liittyvät tehokkuus- ja energiankulutusongelmat.

Lohkoketjuteknologian energiankulutus ja ympäristövaikutukset

Tällä hetkellä lohkoketjuteknologioiden vaikutus ympäristöön on lähinnä negatiivinen. Ympäristövaikutuksista ylivoimainen valtaosa tulee Bitcoin-kryptovaluutan ”louhimiseen” käytettyjen datakeskusten sähkönkulutuksesta. Tämä sähkönkulutus muodostaa sähköverkkoon vahvasti joustamattoman 24/7 kuorman, vaikeuttaen osaltaan sähköverkon dekarbonisointia.

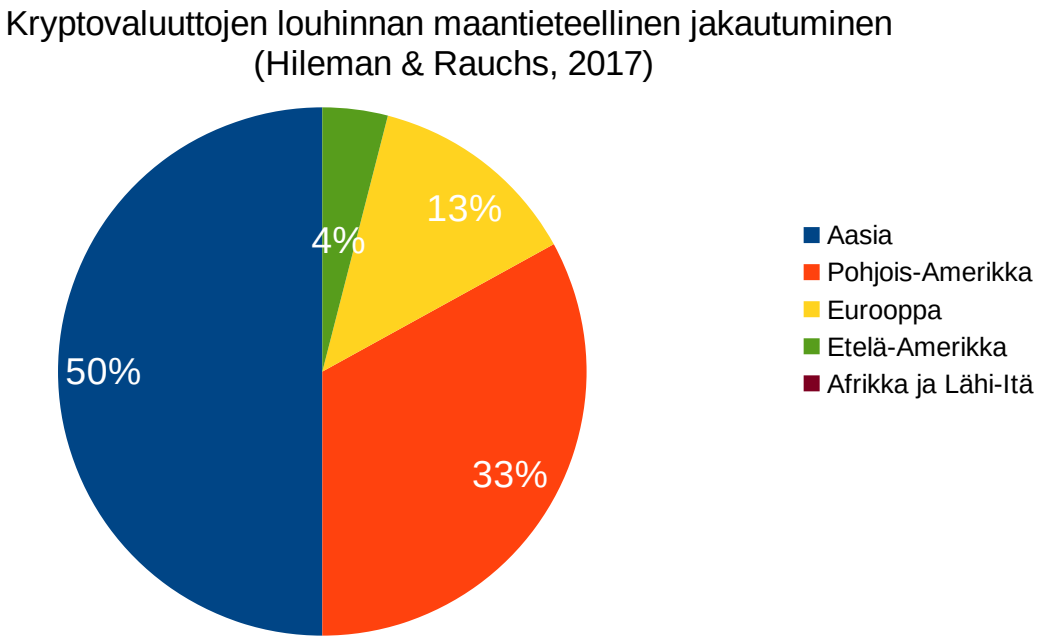
Lohkoketjutekniikoiden energiankulutus on palvelun ominaisuuksiin nähden suurta tai erittäin suurta, etenkin täysin hajautettujen ja anonyymien kryptovaluuttojen ja vastaavien lohkoketjupalvelujen tapauksessa. (Palvelut, jotka hyödyntävät ylläpitäjinä luotettuja tahoja, eivät tarvitse anonyymien kryptovaluuttojen kaltaisia tuhlailevia järjestelmiä väärennösten ehkäisemiseksi: luotetun osapuolen oletetaan olevan luotettu. Nämä järjestelmät eivät eroa esim. lainsäädännön tai käytännön näkökulmasta juurikaan perinteisistä tietokantatekniikoista.) Vaikka ehdotuksia resurssiongelman ratkaisemiseksi on esitetty, on edelleen hyvin epäselvää, miten hyvin nyt käytössä olevat teknologiat voivat skaalautua: esimerkiksi Bitcoinin jälkeen toiseksi merkittävin lohkoketjupalvelu, yleiskäyttöisemmäksi tietokannaksi ja ohjelmointialustaksi suunniteltu Ethereum, hyytyi joulukuussa 2017, kun ”kryptolemmikkien” (eräänlaisia moderneja Tamagotcheja) osto- ja hoitopeli CryptoKitties aiheutti muutamien päivien kuluessa noin 22 000 odottamatonta transaktiota.[5] Vertailun vuoksi, esimerkiksi yksin luottokorttiyhtiö Visa kykenee tiettävästi hoitamaan 56 000 transaktiota *sekunnissa*, siinä missä Bitcoinilla on vaikeuksia hoitaa seitsemää transaktiota ja Ethereumilla 20 transaktiota sekunnissa. Näistä rajoitteista huolimatta järjestelmien energiankulutus on massiivista: yksin Bitcoin saattaa tällä hetkellä kuluttaa sähköä pessimistisempien arvioiden mukaan jopa 70 terawattituntia vuodessa, lähestyen siis koko Suomen vuotuista sähkönkulutusta (de Vries, 2018; Giungato, Rana, Tarabella, & Tricase, 2017; Vranken, 2017).

Keskeinen syy transaktioiden määrään suunnattomassa energiankulutuksessa piilee lohkoketjutekniikan ja Bitcoinin alkuperäisten kehittäjien ideologisessa halussa välttää kaikkia ”keskitettyjä” luotettavia tahoja ja sen sijaan ”hajauttaa” verkon toiminta mahdollisimman pitkälle. Jotta hajautus tuntemattomien käyttäjien välille voidaan toteuttaa niin, että tietokannan luotettavuus säilyy, ts. jotta käyttäjät eivät pääse peukaloimaan tietokantaa, kirjoitusoikeudet tietokantaan jaetaan useimmissa tapauksissa eräänlaisen kilpailun perusteella. Kilpailussa kyseisiä kryptovaluuttoja ”louhivat” tietokoneet pyrkivät käytännössä arvaamaan oikean numeron erittäin suuresta numeroiden joukosta. Ensimmäisinä oikean numeron arvaava tietokone saa oikeuden kirjoittaa seuraavan tietueen, ja palkinnoksi tietyn summan kryptovaluuttaa. Näin toimimalla vältetään mm. uhka siitä, että pahantahtoinen käyttäjä perustaisi joukon valetilejä ja näiden toimintaa koordinoimalla voisi vaikuttaa tietokannan sisältöön omaksi edukseen: tilejä voi nyt luoda miten paljon tahansa, mutta kirjoitusoikeuksien luotettava voittaminen vaatii valtavasti laskentatehoa ja sitä kautta sähköä. Järjestelmät on myös suunniteltu toimimaan niin, että mitä enemmän laskentatehoa verkossa on, sitä vaikeampaa arvaamisesta tulee. Näin ollen järjestelmien *energiankulutus riippuu ensisijaisesti kryptovaluuttojen hinnasta:* mitä arvokkaampia kryptovaluutat ovat, sitä enemmän niiden louhimiseen

5 https://www.bloomberg.com/news/articles/2017-12-04/cryptokitties-quickly-becomes-most-widely-used-ethereum-app

kannattaa käyttää energiaa ja koneaikaa. On tärkeä huomata, että joitain kokeellisia yrityksiä huolimatta koneaikaa ei käytetä mihinkään erityisesti hyödylliseen laskentaan, ja että kryptovaluuttojen louhintaan käytetään pääasiassa erityisesti tätä tarkoitusta varten rakennettuja, muunlaiseen käyttöön täysin käyttökelvottomia louhintakoneita (ns. Application Specific Integrated Circuit, ASIC).

Koska energiankulutus on erittäin merkittävä osa kryptovaluuttojen louhinnan kustannusta, louhinta sijoittuu alueille, joilla on saatavissa edullista energiaa. Tarkkoja tietoja louhinnan sijoittumisesta on erittäin vaikea saada, mutta tiedämme suuren osan tapahtuvan Kiinassa (Hileman & Rauchs, 2017). Euroopassa louhintaa on ennen kaikkea Islannissa, mutta myös Suomessa on ollut suunnitelmia louhintakeskusten perustamisesta (Nikkanen, 2018).



Vielä toistaiseksi julkaisematon tutkimusartikkelini tarkastelee Bitcoinin ja muiden niinsanottujen ”Proof of Work”-varmentamistapaan perustuvien kryptovaluuttojen energiankulutuksen ympäristövaikutuksia, todeten, että esimerkiksi Bitcoinin CO2-päästöt ovat olleet joulukuun 2014 ja kesäkuun 2018 välillä vähintään noin 3 000 000 – 8 000 000 tonnia, olettaen että kaikki ”louhinta” on tapahtunut energiatehokkaimmilla saatavissa olleilla laitteilla, ja maksimimäärä on todennäköisesti alle 10 kertaa minimin. (Vertailun vuoksi, kyseiset hiilidioksidipäästöt vastaavat noin 400 000 – 1 200 000 auton vuosittaisia päästöjä.) Laskelma perustuu niinsanottuun marginaaliseen päästökertoimeen (Hawkes, 2014; Olkkonen & Syri, 2016), jossa päästöt lasketaan olettamalla, että sähköverkkoon tuleva uusi kuorma lisää verkon ajojärjestyksessä viimeisenä olevan ”marginaalisen” voimalan käyttöä. Käytännössä nämä marginaaliset voimalat ovat useimmilla alueilla, Suomi mukaanlukien, fossiilisia polttavia hiili- ja kaasuvoimaloita. Kryptovaluuttojen puolustajat esittävät usein väitteitä siitä, että kryptovaluuttojen louhijat ostaisivat sähkönsä kestävistä lähteistä kuten vesi- ja tuulivoimaloilta. Väitteen todenperäisyyttä laajemmassa mitassa on kuitenkin mahdoton todentaa, ja louhintaan käytetty puhdas sähkö on joka tapauksessa poissa fossiilisten lähteiden korvaamisesta muualla.

Kryptovaluuttojen louhinnan kulutusprofiili on myös omiaan vaikeuttamaan sähköverkon dekarbonisointia. Koska louhimiseen tarvittavat erikoistuneet ASIC-laskentakoneet ovat merkittävä investointi, louhijoiden intresseissä on maksimoida niiden käyttöaste ja pyrkiä toimimaan niin, että louhintaan olisi käytössä mahdollisimman tasaisesti edullista sähköä. Tämä tavoite on ristiriidassa mm. uusiutuvan tuotannon lisäämisen vaatiman kulutusjouston lisäämiseen pyrkivän energiapolitiikan kanssa. Maailman sähköstä tällä hetkellä noin kaksi prosenttia ja vuonna 2025 mahdollisesti jopa kymmenen prosenttia kuluttavien datakeskusten kestävyys on jo nyt kasvavassa määrin huolenaiheena, ja voidaan kysyä, missä määrin poliitikkojen tulisi puuttua lähinnä spekulaation ja laittoman kaupan mahdollistamiseen tarvittavien kryptovaluuttojen louhintakeskusten toimintaan.

Energiankulutuksen haasteisiin on olemassa teknisiä ratkaisuja, mutta kaikki ne vaatisivat kryptovaluuttojen muuttamista muodossa tai toisessa keskitetymmiksi palveluiksi ts. yksityisiksi valuutoiksi, joiden toiminta olisi *de facto* joidenkin luotettujen toimijoiden varassa. On epäselvää, missä määrin teknologiaan ideologisesti suhtautuvat kehittäjät ja käyttäjät hyväksyisivät tällaiset muutokset.

Yksityisyys, tietoturva, älysopimukset ja etiikka

Yksi keskeisiä lohkoketjutekniikoiden ja hajautettujen tietokantateknologioiden haasteista liittyy yksityisyyden suojaan ja tietoturvaan. Etenkin ”perinteinen” lohkoketjutekniikka on suunniteltu lähtökohtaisesti niin, että tietokantoihin tallennettava tieto on muuttamatonta (immutability): sitä voi muuttaa eikä poistaa. Muuttamattomuus on ollut tärkeää etenkin ideologisista syistä, koska lohkoketjun alkuperäisen käyttökohteen Bitcoinin kehittäjä(t) halusivat luoda järjestelmän, jossa kellään toimijalla ei ole mahdollisuutta tehdä rahapolitiikkaa esim. lisäämällä liikenteessä olevan rahan määrää. Kun teknologiaa ryhdyttiin ehdottamaan kryptovaluuttojen lisäksi muihin käyttökohteisiin, muuttamattomuutta käytettiin argumenttina korostamaan tietokantojen luotettavuutta verrattuna ”perinteisiin” tietokantoihin. Kuten useimmille lohkoketjuteknologioiden käytännön käyttökohteita miettiville on tähän mennessä käynyt selväksi, muuttamaton tietokanta ei kuitenkaan ole yksinomaan etu, vaan voi olla jopa käytön estävä haitta.

Kaikesta lohkoketjuihin liitetystä ”luottamus”hypetyksestä huolimatta julkisessa keskustelussa ei ole juuri nähty kriittisiä kysymyksiä siitä, mitä lohkoketjujen väitetty luotettavuus todella tarkoittaa: tässä tapauksessa luotettavuus tarkoittaa vain sitä, että *tietokantaan tallennettua tietoa on vaikea muuttaa.* Tekniikka ei millään tavoin varmista sitä, että esimerkiksi *tallennettava tieto olisi luotettavaa*. Tiedon tallentamisessa voidaan tehdä erehdyksiä, tai tietokantaan voidaan tallentaa tarkoituksella harhaanjohtavaa tietoa, jonka poistaminen tai korjaaminen jälkikäteen on vaikeaa tai mahdotonta. Mainiona, joskin onneksi vasta huvittavana esimerkkinä englantilainen tietotekniikkakonsultti **Terence Eden** tallensi taideteosten tekijätietojen varmentamista ja alkuperäsertifikaatteja tarjoavan Verisart-yrityksen tietokantaan muuttamattoman tiedon siitä, että hän on Mona Lisan tekijä.[6]

Kyseessä ei siis ole ainoastaan teoreettinen ongelma. Kryptovaluutoilla tapahtuvia virheellisiä rahansiirtoja ei ole mahdollista perua, ja on täysin mahdollista esimerkiksi siirtää rahaa tilille, jota ei ole olemassa: tässä tapauksessa raha katoaa olemasta. Kenties vielä uhkaavampi esimerkki on kuitenkin tarkoituksellisesti ongelmallisen tiedon tallentaminen: esimerkiksi Bitcoinin julkisesti ladattavissa olevaan tietokantaan (johon on mahdollista tallentaa transaktiotiedon lisäksi myös vapaamuotoista dataa) on jo tallennettu mm. lapsipornosivuille vieviä nettiosoitteita. Tätä kirjoittaessa ei ole tietoa, onko mihinkään laajemmassa käytössä olevaan lohkoketjuun tallennettu lähtökohtaisesti laitonta dataa (esim. lapsipornokuvia) tai dataa, jonka jokin tuomioistuin saattaisi vaatia poistettavaksi (esim. kunniaa loukkaava materiaali). Tekniset edellytykset tähän ovat kuitenkin olemassa, ja todennäköisesti on vain ajan kysymys, ennen kuin ongelma konkretisoituu.

Lohkoketjutekniikan yhteensopivuutta GDPR-lainsäädännön kanssa tarkastellut **Cagla Salmensuu** toteaa artikkelissaan (Salmensuu, 2018), että lohkoketjutietokantojen toteuttaminen GDPR:n ja muiden yksityisyyden suojaa sääntelevien lakien kanssa yhteensopivasti on mahdollista, mutta muuttamattomuus tekee tästä vaikeaa. Käytännössä tietokantaa suunniteltaessa olisi varmistettava – esimerkiksi sallimalla vain määrämuotoisen tiedon tallentaminen – ettei tietokantaa voida käyttää esimerkiksi yksityisyyttä loukkaavan tiedon tallentamiseen ja levittämiseen. Joillekin ”pääkäyttäjille”

6 https://verisart.com/works/23f2c64a-08c6-4a42-8013-84ac8422dffb

olisi luultavasti myös luotava oikeus, ja velvollisuus, poistaa esimerkiksi tuomioistuimien poistettavaksi määräämät tiedot. Lisäongelmia koituu siitä, että GDPR-asetuksen silmissä erityisen tarkasti silmälläpidettäviä tietoja ovat myös sellaiset tiedot, joita toisiin tietoihin yhdistelmällä voidaan tehdä päätelmiä ihmisten toiminnasta. Esimerkiksi Bitcoinin julkinen transaktiotietokanta on tällainen, ja tutkijat ovat jo demonstroineet, miten pelkästään julkisia tietoja yhdistämällä on mahdollista osoittaa todellisten henkilöiden esimerkiksi ostaneen huumeita Silk Road-kauppapaikalta (Jawaheri & Sabah, 2018).

Lohkoketjutekniikoista on periaatteessa mahdollista saada yhteensopivia yksityisyyslainsäädännön kanssa ja useita ratkaisuja on esitetty, mutta kaikki niistä johtaisivat teknologiayhteisön epäilyttävinä ja vastustettavina pitämään keskittymiseen. Merkittävä osa teknologian kehittäjistä onkin valinnut strategiakseen lobbaamisen sen puolesta, että lohkoketjuteknologiat vapautettaisiin niitä rajoittavasta lainsäädännöstä.

Vastaava ajattelutapa - ”tekniikka on matemaattisen täydellistä, ongelma on vain politiikassa” - on yleistä myös esityksissä hyödyntää niinsanottuja **älysopimuksia** (*smart contracts*). Älysopimukset ovat lyhyesti sanoen sopimuksia, jotka on luonnollisen kielen asemasta kirjoitettu tietokoneen ymmärtämällä ohjelmointikielellä. Näin olisi periaatteessa mahdollista, että älysopimukset toteuttaisivat sovittujen ehtojen täyttyessä itsensä ilman ihmisen väliintuloa. Tämäkään idea ei ole uusi: esimerkiksi laskun eräpäivän asettaminen tulevaisuuteen tavallisessa verkkopankissa on esimerkki ideasta, jollaisia nyt markkinoidaan älysopimuksina ja yhteiskunnan tulevaisuutena.

On kuitenkin helppo nähdä, että älysopimuksiin liittyy monenlaisia ongelmia. Etenkin jos sopimukset tallennetaan muuttamattomaan tietokantaan, mitä teknologian puolestapuhujat pitävät suorastaan keskeisenä kilpailutekijänä, on ilmiselvää, että sopimukset todennäköisesti aiheuttaisivat enemmän vaikeuksia kuin niitä ratkaisevat. Muuttamattoman, tietokoneen automaattisesti tulkitseman sopimuksen on oltava täydellinen ja bugiton: valitettavasti eräs tietojenkäsittelytieteen perusaksioomista kertoo, että monimutkaisen ohjelman bugittomuutta on mahdoton varmentaa etukäteen. Tämän raportin alkuosassa lainattu otsikko 150 miljoonan dollarin kadottamisesta johtui bugista älysopimuksessa. Kadottajana oli tässä tapauksessa yksi älysopimuksiin yleisimmin käytetyn ohjelmointikielen Solidiumin suunnittelijoista – edes hän ei osannut tehdä bugitonta älysopimusta, vaikka pelissä oli satoja miljoonia dollareita. Vaikka sopimusautomaatio todennäköisesti tuleekin lisääntymään ja siten vähentämään esimerkiksi paperityötä, älysopimukset ovat parhaimmillaan ehkä esimerkkitapauksena siitä, miksi oikeusjärjestyksemme on sellainen kuin se on, ja miksi sopimuksissa on lähes aina tulkinnanvaraa.

Lopuksi, lohkoketjuteknologiaan liittyy tiettyjä kysymyksiä, joihin lainsäätäjät saattavat joutua ottamaan lähitulevaisuudessa kantaa. Näihin liittyvät mm. kysymykset siitä, missä määrin ja millä keinoin lohkoketjutekniikoihin vahvasti liittyvään spekulaatioon ja suoriin huijauksiin tulisi puuttua; millainen on lohkoketjutekniikoiden ja erityisesti kryptovaluuttojen ja ICOiden kuluttajansuoja; ja kuinka ja missä määrin puututaan kryptovaluuttojen käyttöön laittoman maksuliikenteen välineenä.

Mikäli lainsäätäjät haluavat aktiivisesti hillitä esimerkiksi kryptovaluuttojen käyttöä, todennäköisesti haavoittuvimmat kohteet löytyvät rajapinnoista, joissa liikkuu oikeaa rahaa tai tavaraa. Esimerkiksi kryptovaluuttoja oikeaan rahaan vaihtavien markkinapaikkojen toimintaa on täysin mahdollista

kontrolloida nykyistä tiukemmin, ja kryptovaluuttoja maksuvälineinä hyväksyvät yritykset on mahdollista asettaa tiukemman tarkkailun alle. Verottajaa voidaan ohjeistaa puuttumaan tarkemmin kryptovaluuttojen käyttöön, ja ääritapauksessa esimerkiksi Tullia on mahdollista ohjeistaa puuttumaan tunnettujen ja epäiltyjen kryptovaluuttaa hyväksyvien ulkomaisten yritysten lähettämiin paketteihin. Mikään näistä toimista ei ole aukoton, mutta mikäli demokraattisessa järjestyksessä päätämme hillitä kryptovaluuttojen käyttöä, niiden yksin ja yhdessä aiheuttamat lisähankaluudet todennäköisesti vähentävät valuuttojen käyttöä tehokkaasti.

Kuten teknologian tutkimus meille kertoo, teknologiat sinänsä eivät ole positiivisia eivätkä negatiivisia, mutta ne eivät ole koskaan myöskään neutraaleja. Tietynlaisillla teknologioilla on yhteiskuntaan tietynlaisia vaikutuksia, ja äärimmäisen oikeistolibertaristisen, individualistisen, omaisuuksien ja vallan keskittymistä voimakkaasti edistävän ja lähtökohtaisesti valtioiden tuhoa ajavan ideologian maailmaan loihtima lohkoketjuteknologia voi tuottaa hyvin tietynlaisia vaikutuksia, mikäli sen ja sen puolestapuhujien lupauksiin ei osata suhtautua terveen kriittisesti. Teknologian kieltäminen itsessään on mahdotonta, mutta lainsäätäjillä ei ole mitään velvollisuutta nöyrtyä iskulauseilla ja muotitermeillä puhuvien teknologialähettiläiden vaatimusten edessä. Suomi tai Eurooppa eivät jää takapajuloiksi, vaikka kaikkia lohkoketjutekniikoiden ja muiden vastaavien teknologiaprojektien puolestapuhujien vaatimia lainsäädännöllisiä ja muita helpotuksia ei täysimääräisesti ja välittömästi toteutettaisikaan.

Lähteet

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives—Volume, 29*(2—Spring), 213–238. https://doi.org/10.1257/jep.29.2.213

Bohr, J., & Bashir, M. (2014). Who Uses Bitcoin? An exploration of the Bitcoin community. In *2014 12th Annual Conference on Privacy, Security and Trust, PST 2014* (pp. 94–101). https://doi.org/10.1109/PST.2014.6890928

de Vries, A. (2018). Bitcoin ' s Growing Energy Problem. *Joule*, *2*(5), 801–805. https://doi.org/10.1016/j.joule.2018.04.016

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

Giungato, P., Rana, R., Tarabella, A., & Tricase, C. (2017). Current trends in sustainability of bitcoins and related blockchain technology. *Sustainability (Switzerland)*, *9*(12). https://doi.org/10.3390/su9122214

Golumbia, D. (2016). *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis: University of Minnesota Press.

Graeber, D. (2011). *Debt: The First 5,000 Years*. New York: Melville House.

Griffin, J. M., & Shams, A. (2018). Is Bitcoin Really Un-Tethered ? *SSRN Electronic Journal*.

Hawkes, A. D. (2014). Long-run marginal CO2 emissions factors in national electricity systems. *Applied Energy*, *125*, 197–205. https://doi.org/10.1016/j.apenergy.2014.03.060

Hileman, G., & Rauchs, M. (2017). 2017 Global Cryptocurrency Benchmarking Study. *SSRN Electronic Journal*, *44*(0). https://doi.org/10.2139/ssrn.2965436

Jawaheri, H. Al, & Sabah, M. Al. (2018). *When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis*.

Nikkanen, H. (2018, April). Long Play 64: Missä louhimme kerran. *Long Play*.

Olkkonen, V., & Syri, S. (2016). Spatial and temporal variations of marginal electricity generation: The case of the Finnish, Nordic, and European energy systems up to 2030. *Journal of Cleaner Production, 126*, 515–525. https://doi.org/10.1016/j.jclepro.2016.03.112

Popper, N. (2015). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (Kindle ed.). New York: HarperCollins.

Salmensuu, C. (2018). General Data Protection Regulation and the Blockchains. *Liikejuridiikka*, (1), 92.

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability, 28*, 1–9. https://doi.org/10.1016/j.cosust.2017.04.011