ASIANTUNTIJALAUSUNTO EDUSKUNNAN TULEVAISUUSVALIOKUNNALLE
2.10.2018

Juho Rantala, väitöskirjatutkija, Tampereen yliopisto

Aihe: Valiokunta on erityisesti kiinnostunut kuulemaan lohkoketjujen ja kryptovaluuttojen yhteiskunnallisesta merkityksestä.

Tiivistelmä

Eduskunnan tulevaisuusvaliokunta on pyytänyt allekirjoittaneelta asiantuntijalausuntoa liittyen aiheeseen ”lohkoketjujen ja kryptovaluuttojen yhteiskunnallisesta merkityksestä”. Seuraavassa lausunnossa esitän lyhyesti näkemyksiäni lohkoketjujen merkityksestä yhteiskunnalle, yhteiskunnan instituutioille, markkinatoimijoille sekä kansalaisille. Lopussa tarjoan myös joitain tärkeitä ongelmia liittyen lohkoketjuihin ja niiden soveltamiseen.

Lohkoketjusta on noussut nopeasti puhuttu ja *hype*tetty teknologia, jonka vaikutuksia on jopa verrattu internetin tuomiin mullistuksiin. Myös esimerkiksi OECD nosti digitaalista taloutta käsittelevässä raportissaan vuonna 2017 lohkoketjun tulevaisuuden tärkeimmäksi innovaatioksi tekoälyn rinnalle. Tästä huolimatta on hyvä huomata, että suuri osa lohkoketjun sovelluksista on kuitenkin vielä kehitys- ja kokeiluasteella, varsinkin kun kyseessä on niin sanotut julkiset, desentralisoidut alustat.

Tällä hetkellä tärkein kontribuutio, jonka lohkoketjut voivat tuoda yhteiskunnalle liittyy tiettyjen institutionaalisten toimien automatisointiin. Samalla lohkoketjut tarjoavat alustan yksilöltä yksilölle (*peer-to-peer*) tapahtuvalle vertaistaloudelle, jossa ei tarvita ”kolmatta osapuolta” (esim. instituutiota tai organisaatiota). Näin ollen ne myös luovat haasteita perinteisille, hiearkkisille organisaatiorakenteille sekä tällaisten organisaatioiden toimille ja tehtäville. Lohkoketjulla on myös mahdollisuuksia toimia tasa-arvoistavien toimien työkaluina, vaikka ne eivät tietysti vielä itsessään tuota tasa-arvoa ja pura hierarkkisia valtarakenteita.

Lohkoketju lyhyesti

Lohkoketjun voi katsoa olevan eräänlainen *tekniikka*, jolla on monenlaisia teknologisia *sovelluksia*. Tunnetuimmat näistä ovat luultavasti kryptovaluutta Bitcoin sekä ”digitaaliympäristö” Ethereum. Tiivistäen lohkoketju on desentralisoitu tietokanta, jota ylläpidetään vertaisverkkoperiaatteella. Se on siis aina hajautunut kaikkien käyttäjien kesken ja se myös päivittyy kaikille käyttäjille jatkuvasti. Desentralisoitu tarkoittaa tässä yhteydessä sitä, ettei lohkoketjujärjestelmää hallitse mikään yksittäinen taho – sillä ei siis ole keskusauktoriteettia. Samalla monimutkaiset kryptografiset salaustekniikat varmistavat, että – esimerkiksi Bitcoinin tapauksessa – järjestelmässä tehdyt transaktiot pysyvät salaisina ja ne ovat valideja.

Lohkoketjujärjestelmä tarvitsee toimiakseen myös *varmentamista*, joka tapahtuu käytännössä hieman eri tavoin riippuen siitä, mikä lohkoketjusovellus on kyseessä. Esimerkiksi Bitcoinissa niin sanotut louhijat (*miners*) ylläpitävät verkostoa (”louhivat”; *mining*) ja jakamalla konetehoaan verkoston käyttöön kytkevät uudet transaktiot osaksi

vanhempaa ketjua.[1] Näin varmistetaan, että samaa digitaalista valuuttaa ei käytetä kahteen kertaan, luodaan luottamusta salausmekanismein ja pidetään koko järjestelmää käynnissä. Samalla lohkoketjujärjestelmä synnyttää nopeimmin louhineelle taholle uusia Bitcoineja. Louhinta perustuu ennalta määrättyihin matemaattisiin ongelmiin, jotka vaikeutuvat ajan kuluessa.

Bitcoinin järjestelmä on yksi esimerkki *julkisesta* lohkoketjusta, jonka lisäksi on *yksityisiä* ja *puolijulkisia* ketjuja. Jälkimmäiset eivät ole desentralisoituja, vaan niitä hallitsee jokin keskusauktoriteetti. Kaikki nämä lohkoketjumuodot perustuvat yleensä vapaasti jaettavaan (*open source*) lähdekoodiin, joka alleviivaa järjestelmän toimintaperiaatteiden läpinäkyvyyttä. Näin esimerkiksi Bitcoinin ja Ethereumin lähdekoodin pohjalta rakennetaan jatkuvasti uusia sovelluksia mitä erilaisimpiin tarkoituksiin. Julkisten lohkoketjujen rakennetta ei voi oikeastaan muuttaa, paitsi niin, että kaikista louhijoista yli 50 prosenttia hyväksyy muutoksen. Tällaisessa lohkoketjussa tapahtumat, olivat ne sitten transaktioita tai vaikkapa suoritettuja älysopimuksia, ovat käytännössä peruuttamattomia ja lopullisia.

Uudemmat lohkoketjun sovellukset tarjoavat kuitenkin muutakin kuin kryptovaluutan. Esimerkiksi Ethereum ja erityisesti sen uudemmat sovellukset voivat toimia monimutkaisina ja automatisoituina järjestelminä tai ”ympäristöinä”. Ethereum tutustutti lohkoketjuun älysopimukset (*smart contracts*), jotka nimensä mukaisesti ovat koodattuja ja automatisoituja sopimuksia. Käyttäjät voivat itse määritellä sopimuksen (algoritmiset) ehdot ja sen, millä aikavälillä sopimus on voimassa ja niin edelleen. Tärkein asia älysopimuksissa on kuitenkin se, että ne *mahdollistavat koodin ja ohjelmiston suorittamisen lohkoketjun sisällä*. (Esimerkiksi Bitcoinissa lohkoketjuun tallentuivat vain lyhyet tiedot tehdyistä transaktioista.)

Lohkoketjuteknologian mahdollisuuksista ja merkityksistä

Markkinoilla lohkoketjuteknologia mahdollistaa digitaalisen vertaistalouden. Monissa kryptovaluuttoja ja lohkoketjuja puolustavissa puheenvuoroissa on nostettu esille, että ihmiset voitaisiin nostaa köyhyydestä lohkoketjujärjestelmien avulla. Esimerkiksi monilla kolmannen maailman asukkailla on kännykät, mutta ei pankkitiliä. Ruohonjuuritason vertaistaloudella he voisivat ottaa osaa markkinoille tai jopa tuottaa itse markkinat. Alustat mahdollistavat myös joukkorahoituskampanjoita, joissa projektia tai yritystä voidaan rahoittaa esimerkiksi niin sanotun *initial coin offering*:n (ICO) avulla. Tämä tarkoittaa, että lohkoketjujärjestelmän omaa kryptovaluuttaa lasketaan liikkeelle, eli yleensä sitä ostetaan. Samalla luodaan kysyntää kyseiselle valuutalle ja toisaalta rahoitetaan itse järjestelmän kehittänyttä organisaatiota.

Erityisesti uudempien, monimutkaisempien lohkoketjujen yhteydessä on suunniteltu ”desentralisoituja autonomisia organisaatioita” (*decentralized autonomous organization*; DAO) tai yrityksiä (*decentralized autonomous company*; DAC). Erityisesti Ethereum-lohkoketjua hyväksi käyttävät DAO:t ja DAC:t voivat, ainakin teoriassa, omistaa itse itsensä ja toimia automaattisesti. Näiden säännöt voidaan esimerkiksi äänestää järjestelmän kehitysvaiheessa. Äänioikeus taas voidaan määrittää sen mukaan, kuka on hankkinut ICO-vaiheessa lohkoketjualustan kryptovaluuttaa (tai ”rahaketta”). Toisaalta äänestys voi muodostua myös muulla tavalla, kuten esimerkiksi jatkuvalla äänestyksellä

[1] Bitcoinin yhteydessä louhintavarmistusta kutsutaan ”työvarmennukseksi” (*proof-of-work*), mutta esimerkiksi Ethereum-lohkoketjujärjestelmän uudemmat sovellukset voivat käyttää ”osakkuusvarmennusta” (*proof-of-stake*), jonka tarkoitus on muun muassa vähentää konetehojen käyttöä.

kaikkien käyttäjien kesken. Lohkoketjututkija Quinn Dupont on esittänyt hypoteettisen valaanpelastusorganisaation, joka toimisi DAO-periaatteella. Organisaatio voisi tunnistaa tietyllä alueella tapahtuvan öljyonnettomuuden, jonka johdosta se voisi allokoida automaattisesti varoja kyseisen alueen pelastus- ja puhdistustahoille. Näin organisaatio ikään kuin olisi toimija valaiden puolesta (tai työkalu valaille taistella ihmistä vastaan), ja se asettaisi ihmiset suoraan ja automaattisesti vastuuseen teoistaan.

Yritykset ja organisaatiot voivat hyödyntää yksityisiä lohkoketjuja, joilla voidaan hajauttaa toimintoja mutta säilyttää kuitenkin yhtenäinen dokumentointi. Lisäksi yritykset voivat tuottaa jaettuja ja puolijulkisia ketjuja, jotka voivat ylläpitää yritysten keskinäistä kaupankäyntiä sekä vaihtaa monenlaista dataa vaikkapa logistiikkaketjuista. Yksi puhutuimpia lohkoketjun sovelluskohteita onkin ”tavaroiden internet” tai ”teollinen internet”. Ketjut voisivat parantaa esimerkiksi laajojen ylikansallisten tuotanto- ja logistiikkaketjujen läpinäkyvyyttä. Myös älykaupungit tarjoavat lukuisia erilaisia sovellusyhteyksiä, ja toisaalta juuri lohkoketju mahdollistaa älykaupungit yhdistämällä moniulotteiset datankeruu- ja seurantajärjestelmät samalle alustalle.

Lohkoketjut mahdollistavat myös alustoja jakamistaloutta varten. Esimerkiksi Uberin ja Airbnb kaltaisten palveluiden toiminta voidaan tuottaa lohkoketjun pohjalta. Toisaalta ketjut voivat tuoda uusia tapoja järjestää jakamistaloutta: maksut onnistuvat alustan omalla kryptovaluutalla ja alusta mahdollistaa myös mainejärjestelmän, jolla arvioida yrittäjiä ja rakentaa luottamusta. Älysopimuksella taas vuokrattava auto tai asunto voi automaattisesti avautua tietyksi aikaväliksi. Näiden lisäksi myös monenlaisia sähkön vertaistuotantojärjestelmiä on suunnitteilla.

Toisaalta lohkoketjuteknologian ympärille on syntynyt monenlaisia uusia palveluita ainakin muutamalla tasolla. On niitä, jotka suoraan tarjoavat uusia lohkoketjujärjestelmiä sekä tahoja, jotka tuottavat palveluita lohkoketjujärjestelmien käyttäjille (esimerkiksi tarjoavat e-lompakon tai vastaavan, johon kryptovaluutat voi tallentaa). Näiden lisäksi on esimerkiksi ”louhintapooleja”, jotka antavat yksittäisille käyttäjille mahdollisuuden ottaa osaa louhintaan ja saada käsiinsä Bitcoineja. Tällaiset ”poolit” yleensä verottavat osan uusista Bitcoineista sekä saattavat vaatia joitain muita maksuja.

Lohkoketju mahdollistaa myös osakekaupan suoraviivaistamisen esimerkiksi tallentamalla jatkuvasti uudet kauppatiedot yhteen rekisteriin. Tämä rekisteri voi olla julkinen niin, että sen (julkiseksi tarkoitetut) tiedot ovat kaikkien tai rajatun joukon luettavissa. Älysopimuksilla voidaan myös luoda algoritmisia johdannaisia. Kryptovaluutat vuorostaan eivät täytä rahan kaikkia ominaisuuksia (vaihdannan väline, arvon mitta, arvon säilyttäjä), vaan viittaavat juuri vaihdannan väline -attribuuttiin. Tästä huolimatta nämä digitaaliset valuutat vaikuttavat monin tavoin yhteiskuntaan. Esimerkiksi verotus vaikeutuu, kun monissa kryptovaluutoissa – kuten esimerkiksi Bitcoinissa – transaktiot ovat anonyymejä, eikä desentralisoitua järjestelmää muutenkaan hallita.

Itse asiassa lohkoketjujärjestelmässä on mahdollista luoda algoritmiset säännöt, joilla verotus tai muu varallisuuden uudelleenjakaminen onnistuu. Toisaalta on mahdollista toteuttaa myös desentralisoidut, hajautetut markkinat, joissa yksilöt voivat vapaasti vaihtaa keskenään ja saada tietoonsa näitä markkinoita koskevan informaation. Mutta koska lohkoketjujärjestelmässä on mahdollista tallentaa kaikki informaatio – ja se aina kiertää järjestelmän kautta –, on mahdollista luoda myös suunnitelmatalouteen perustuva markkina-alusta.

Myös lohkoketjun käytöstä identiteettidatan yhteydessä on keskusteltu laajasti. Esimerkiksi internetin eri palveluiden salasanatiedot voitaisiin asettaa yhden ja saman lohkoketju-ID:n taakse, jolloin ei tarvitsisi muistaa suurta joukkoa salasanoja. Toisaalta monet yhteiskunnassa kerätyt tiedot kansalaisesta (esim. terveystiedot) voitaisiin yhdistää yhteen ja samaan järjestelmään helpottamaan kanssakäymistä instituutioiden kanssa. Automatisoidut sopimukset voisivat huomioida, onko esimerkiksi tietty henkilö oikeutettu ostamaan asetta tai vuokraamaan autoa (onko ajokorttia/menettänyt ajokortin). Älysopimukset siis mahdollistavat myös muunlaisia lakiteknisiä sovelluksia kuin pelkästään käyttäjältä käyttäjälle tarkoitetun automatisoidun sopimusoikeuden. Äärimmäisenä ja vielä teoreettisena ajatuksena on ollut erilaisten lakipykälien automatisointi. Lisäksi lohkoketjua hyödyntävä sähköinen äänestys on viety läpi ainakin Etelä-Koreassa.

Lohkoketjun ja sen soveltamisen ongelmia

Lohkoketjujen kohdalla ja niitä ympäröivässä, yleensä puolustavassa retoriikassa ilmenee kuitenkin paljon ongelmia ja virheellisiä olettamuksia. Olen listannut seuraavaan joitain esimerkkejä.

1. Lohkoketjun ylläpito eli varmentamistoiminnot kuluttavat valtavia määriä energiaa. Esimerkiksi Bitcoin-verkon louhinnan, joka perustuu konetehon jakamiselle, arvioitiin syyskuussa 2018 kuluttavan noin 73 terawattituntia (/vuosi).
2. Suuri osa lohkoketjuteknologioista on vasta kehitys- ja suunnitteluasteella.
3. Lohkoketjuja vaivaa siis lähes samankaltainen *hype*, kuin internetiä vaivasi sen ”boomivuosina” 1990-luvun lopussa ja 2000-luvun alussa.
4. *Hype* on tuonut mukanaan myös keinottelua ja suoranaista huijausta. Esimerkiksi jotkin ICO:t ovat tarjonneet sijoituskohteena kryptovaluuttaa tai rahaketta, jolla ei ole ollut oikeastaan mitään muuta funktiota.
5. Lohkoketjuilla on myös monia teknisiä ongelmia ja heikkouksia, joita kuitenkin jatkuvasti pyritään parantamaan ja ylittämään, esimerkiksi uusilla järjestelmillä.
6. Esimerkiksi Bitcoinin kohdalla järjestelmää ei voida muokata, ellei ympäri maailmaa hajautunut louhiajoukko saavuta konsensusta (eli yli 50 prosenttia louhintaan allokoidusta konetehosta on ”samaa mieltä” siitä, miten louhitaan seuraavat transaktiot osaksi vanhaa ketjua). Vuonna 2016 kourallinen kiinalaisia louhintainstituutteja hallitsi jopa 70 prosenttia Bitcoin verkoston louhinnasta, joten heillä on ollut ainakin teoreettinen mahdollisuus vaikuttaa järjestelmään eli esimerkiksi käyttää kahteen kertaan jo kerran siirretyt valuutat.
7. Usein julkisiin ketjuihin ajetaan päivityksiä konsensuksen avulla. Päivitykset on kuitenkin tuottanut jokin kehittäjätaho tai -joukko, jolloin niiden sisällöstä on oltava hyvin perillä.
8. Vaikka esimerkiksi Bitcoinin transaktiot ovat salattuja siinä, ettei niistä tiedä *kuka* on lähettänyt *kenelle* valuuttaa, voi olla mahdollista selvittää tekijästä jotain vertaamalla lohkoketjun julkisia tietoja johonkin toiseen julkiseen tietokantaan, joka vuorostaan voidaan kytkeä konkreettisiin tapahtumiin.
9. E-lompakon, jossa Bitcoineja (tai muita kryptovaluuttoja) säilytetään, salasanaa ei kannata unohtaa. Kun ei ole mitään keskusauktoriteettia, on e-lompakon murtaminen lähes mahdotonta. Onkin arvioitu, että unohdettuja tai kadotettuja Bitcoineja eli ”zombiekolikoita” on järjestelmässä jopa 30 prosenttia kaikista louhituista kolikoista.
10. Älysopimukset eivät välttämättä tuo mitään laadullisesti uutta sopimusoikeuteen, vaan pikemminkin tehostavat vanhoja toimintoja. Ne voivat esimerkiksi

automatisoida joitain notaarin hoitamia tehtäviä, kuten allekirjoitusten ja asiakirjojen oikeaksi todistamisen.

11. Samalla on hyvä huomata, kuten muutamat tutkijat ovat esittäneet, että älysopimuksia ympäröivässä retoriikassa ei yleensä ymmärretä ihmisten välisten sopimusten luonnetta sekä sen kytköksiä oikeudellisiin prosesseihin – saati näiden toteutumista todellisessa käytännön elämässä.
12. Älysopimukset voivat toisaalta tuoda mukanaan uusia lakeja ja näin ollen entisestään monimutkaistaan organisaatioprosesseja.
13. Jos älysopimuksilla luodaan laajempia ja jopa lakia automatisoivia järjestelmiä, kuinka pitäisi toteuttaa suunnittelu ja ohjelmointivaiheessa järjestelmän pohjasäännöt? Käyttäjien, kansalaisten, siis äänestäjien olisi periaatteessa kyettävä ymmärtämään sitä, mihin ja millaisille algoritmisille koodatuille säännöille järjestelmä perustuu. Näin on todennäköisesti esimerkiksi sähköisen äänestyksen kohdalla.
14. Samalla myös tuomioistuinten, oikeusavustajien ja lainsäädäntöön keskittyneiden juristien olisi kyettävä arvioimaan älysopimuksia ja niiden koodia. Vielä vuonna 2017 ei oikeastaan ollut ennakkotapauksia, jotka voisivat osoittaa, miten tällaiset tapaukset pitäisi käsitellä.
15. Sopimusten ja lain automatisointiin liittyy myös toisenlainen ongelma. Perinteinen laki ei kykene pakottamaan lain tottelemiseen, vaan se rankaisee jälkikäteen. Tämä onkin ollut tärkeä osa erityisesti länsimaista oikeuskäsitystä. Koodatut, automatisoidut sopimukset tai lait, erityisesti lohkoketjualustalla, ovat kuitenkin *lopullisia* eli peruuttamattomia, yksilö ei siis voi päättää totteleeko sopimusta tai lakia. Näin yksilö ei näyttäydy vapaasti valitsevana toimijana lain edessä, ja toisaalta koko lain henki saa ainakin jossain mielessä uuden merkityksen.
16. Samalla kun koodista tulee sopimus (tai laki), myös kaikki koodissa olevat virheet kuuluvat osaksi sopimusta (tai lakia). Joissain tapauksissa, kun joku on onnistunut varastamaan kryptovaluuttoja hyödyntämällä järjestelmän teknistä heikkoutta, on tätä puolusteltu sillä, että toiminta oli järjestelmän sääntöjen puitteissa tapahtuvaa toimintaa.
17. Julkisen lohkoketjujärjestelmän kohdalla nousee myös kysymys vastuusta: Jos koko järjestelmä on desentralisoitu, eikä sillä ole mitään keskushallintoa, kuka voidaan saattaa vastuuseen järjestelmästä? Toisin sanoen, kuka voidaan kutsua oikeuden eteen vastaamaan järjestelmän tuottamista ongelmista tai haitoista?
18. Samalla nousee kysymys, joka varjostaa monia erityisesti alkuvuosien lohkoketju- ja Bitcoin-kehittäjien retoriikasta: mitä tapahtuu luottamukselle? Monet näistä kehittäjistä alleviivasivat, että ihmiset ovat lähtökohtaisesti epäluotettavia, joten on parempi siirtää luottamus (kuvitellusti) politiikasta ja ideologiasta vapaan teknologian harteille. Yksilöt vain käyvät ”toisistaan erossa yhdessä” kauppaa, eikä heidän tarvitse luottaa toisiinsa. Teknologia vain pakottaa tietynlaisen joukon toimia ja valintoja toteutumaan. Kiinnostavaa on, että mitä tämä ”luottamuksen automatisointi” tarkoittaa yhteiskunnallisten instituutioiden näkökulmasta, onhan luottamus yksi tärkeimmistä sosiaalista elämää rakentavista asioista.

Kirjallisuutta

Bambara, Joseph J. & Allen, Paul R., *Blockchain. A Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw-Hill Education 2018.

De Filippi, Primavera & Wright, Aaron, *Blockchain and the Law – The Rule of Code*. Harvard University Press, Cambridge & London 2018.

OECD, *Digital Economy Outlook 2017*. OECD Publishing, Paris 2017. Verkossa: https://read.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en#page1

Narayanan, Arvind, Bonneau, Joseph, Felten, Edward, Miller, Andrew & Goldfeder, Steven, *Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction*. Princeton University Press, Princeton & Oxford 2016.

Rantala, Juho, Lohkoketjuteknologian yhteiskunta. Osa I: Bitcoinista Ethereumiin. *niin & näin* 1/2018a, 45–58. Verkossa: http://netn.fi/node/7283.

Rantala, Juho, Lohkoketjuteknologian yhteiskunta. Osa II: Rajatut, desentralisoidut markkinat. *niin & näin* 1/2018b [Verkkoteksti]. Verkossa: http://netn.fi/node/7293.

Rantala, Juho, Koodin ja ohjelmiston filosofiasta. *niin & näin* 1/2018c, 101–108.

Rantala, Juho, Lohkoketjun hallitsema yhteiskunta – automatisoitu laki ja hallinta. Teoksessa *Informaatioteknologian filosofia 2*. [TULOSSA 2018/2019]

Rantala, Juho, Lohkoketjuteknologian yhteiskunta. Osa III: ihmiskuva ja politiikka. *niin & näin*. [TULOSSA]