LOHKOKETJUTEKNOLOGIA YLEISKÄYTTÖISENÄ TEKNOLOGIANA JA SEN SOVELLUTUKSET

Jyväskylän yliopisto
Kauppakorkeakoulu

Pro gradu -tutkielma

2019

JYVÄSKYLÄN YLIOPISTO

Tekijä: Niklas Sanmark
Oppiaine: Taloustiede
Ohjaaja: Ari Hyytinen

TIIVISTELMÄ

Tekijä

Niklas Sanmark

Työn nimi

Lohkoketjuteknologia yleiskäyttöisenä teknologiana ja sen sovellutukset

Oppiaine	Työn laji
Taloustiede	Pro gradu -tutkielma
Aika (pvm.)	Sivumäärä
17.12.2019	89

Tiivistelmä – Abstract

Tämä työ on kirjallisuuteen pohjautuva arvio siitä, onko lohkoketjuteknologialla riittävästi piirteitä, joilla se voidaan tunnistaa yleiskäyttöiseksi teknologiaksi. Ensiksi määritellään käsite yleiskäyttöinen teknologia ja miten se eroaa tavanomaisesta yleishyödyllisestä teknologiasta. Tämän jälkeen tutustutaan lohkoketjuteknologiaan tarkemmin ja sen taloudellisiin ulottuvuuksiin. Tältä pohjalta pohditaan lohkoketjuteknologian nykyhetken etuja ja haittoja ja arvioidaan, onko lohkoketjuteknologia yleiskäyttöinen teknologia. Tässä annetaan esimerkkejä hyvin erilaisista toimialoista, joissa lohkoketjuteknologiaa voi hyödyntää. Seuraavaksi tutustutaan lohkoketjuteknologian potentiaalisiin uusiin sovellutuksiin. Lopuksi johtopäätöksissä todetaan, että etukäteen on hyvin vaikea todentaa, onko lohkoketjuteknologia seuraava yleiskäyttöinen teknologia, sillä monet työssä esitetyt yleiskäyttöisen teknologian ominaispiirteet ovat tunnistettavissa jälkikäteen havainnoimalla. Lisäksi lohkoketjuteknologiassa on teknologiana erilaisia haasteita, mikä itsessään antaa olettaa, ettei tulevaisuuden mahdollinen yleiskäyttöinen lohkoketjuteknologia perustu samoihin teknisiin ratkaisuihin, mitkä on tunnettu tämän työn kirjoittamisen hetkellä.

Asiasanat

Lohkoketjuteknologia, Yleiskäyttöinen teknologia, Älysopimukset, Nanomaksut, Alenevat transaktiokustannukset

Säilytyspaikka Jyväskylän yliopiston kirjasto

SISÄLLYS

TAULUKOT

KUVAT

1 JOHDANTO

1.1 Yleistä

Teknologinen kehitys on kautta aikojen ollut yksi talouskasvun tärkeimmistä tekijöistä (Helpman & Trajtenberg, 1994). Talouskasvu taas on tuonut hyvinvointia yhteiskuntaan. Teknologinen kehitys on mahdollistanut muun muassa tuottavuuden kasvun, entistä paremman ja terveemmän elämän sekä vapaa-ajan lisääntymisen. Erakkomaisesti elänyt ja usein nuorena kuollut metsästäjäkeräilijä oli kovin erilainen ihminen kuin nykyisin tiiviissä, urbaanissa ympäristössä elävä asiantuntijatyötä tekevä nykykaupunkilainen. Siinä missä osa teknologioista ja keksinnöistä on puhtaasti yksilön elämänlaatua parantavia, toiset teknologiat taas ovat globaalilla mittakaavalla saattaneet ihmisen uuteen aikakauteen. Tällaisia teknologioita, jotka vaikuttavat yhteiskunnan rakenteisiin ja toimintaan, kutsutaan yleiskäyttöisiksi teknologioiksi.

Vuonna 2008 pseudonyymi Satoshi Nakamoto julkaisi virtuaalivaluutta Bitcoinin vastalauseena keskuspankkien liikkeelle laskemalle rahalle. Bitcoinin todellinen innovaatio oli kuitenkin sen taustalla oleva lohkoketjuteknologia. Nakamoto kehitti lohkoketjuteknologian virtuaalivaluuttansa transaktioiden varmentamiseen, mutta tällä teknologialla on laajemminkin käyttöä tiedon käsittelyssä luotettavasti ilman kolmatta osapuolta.

1.2 Miksi aihe on tärkeä?

Nykyään lähes kaikessa digitaalisessa toiminnassa on kolmas osapuoli eli palveluntarjoaja, joka ottaa aina oman osuutensa välistä muodossa tai toisessa. Kun kolmas osapuoli poistetaan yhtälöstä, virtuaalivaluuttojen lisäksi

lohkoketjuteknologialla voisi muun muassa mahdollistaa älykkäät kahdenväliset sopimukset taikka sen avulla voitaisiin luoda esimerkiksi turvallinen äänestysjärjestelmä tai säilöä henkilörekisteritietoja.

Tutkimukseni aihe on ajankohtainen ja erittäin merkittävä, sillä yleiskäyttöinen teknologia määritelmänsä mukaisesti vaikuttaa globaalilla tavalla yhteiskuntarakenteita muuttavasti. Lohkoketjuteknologia on mahdollisesti seuraava yleiskäyttöinen teknologia. Aihepiirin mielenkiintoisuutta lisää sekin seikka, että aiheesta on vielä vähän tutkimusta, jossa on suoranaisesti otettu kantaa lohkoketjuteknologian potentiaaliin olla seuraava yleiskäyttöinen teknologia.

Aiheen ajankohtaisuudesta kielii myös se, että yli 70 maailman suurinta finanssi-instituutiota on liittoutunut R3-konsortioiksi varautuakseen siihen, että lohkoketjuteknologia olisi finanssimaailman seuraavana suuri läpimurto. Laajemmalla mittakaavalla koko FinTech-alan, eli finanssisektorin digitalisoitumisen arvioidaan kasvavan kokonaisarvoltaan 300 miljardin dollarin arvoiseksi alaksi vuoteen 2020 mennessä. FinTechillä tarkoitetaan laajasti ottaen kaikkea uutta teknologiaa, joka suoraan tarjoaa tai mahdollistaa erilaiset internetpohjaiset ratkaisut digitaalisessa kaupankäynnissä, maksamisessa tai startup-joukkorahoituksessa. (Forest & Rose 2015).

Yleiskäyttöiselle teknologialle on tyypillistä se, että sillä ei välttämättä ole suoranaista investointipotentiaalia tiettyyn yksittäiseen tuotteeseen, minä takia yleiskäyttöisen teknologian yleistyminen saattaa olla hidasta ja todennäköisesti siksi varsinaisia käytännön sovellutuksia on ilmestynyt vasta vähän. Lohkoketjuteknologian voisi siis sanoa olevan vielä tarkastelu- ja opetteluvaiheessa, jossa potentiaali tunnistetaan, mutta sitä ei osata vielä hyödyntää. Teknologialle löytyy kuitenkin valtavaa kiinnostusta erityisesti finanssisektorilta.

Riippumatta alasta millä lohkoketjuteknologia lyö itsensä läpi, yleiskäyttöisenä teknologiana se laajenisi pikkuhiljaa muillekin aloille ja näin ollen synnyttäisi pitkällä aikavälillä talouskasvua (Jovanovic & Rousseau, 2005). Tästäkin syystä aiheen taloustieteellinen tarkastelu on perusteltua.

1.3 Tutkimuskysymykset

Tässä opinnäytetyössä arvioidaan lohkoketjuteknologian taloudellista luonnetta ja erityisesti sitä, missä määrin lohkoketjuteknologiaa voidaan pitää yleiskäyttöisenä teknologiana. Työssä tarkastellaan, täyttääkö lohkoketjuteknologia tutkimuskirjallisuudessa määriteltyjä ehtoja, joita teknologian tulee täyttää, jotta sitä voidaan luonnehtia yleiskäyttöiseksi. Lisäksi työssä kuvataan konkreettisia esimerkkejä sovellusalueista, joilla lohkoketjuteknologiaa pyritään parhaillaan hyödyntämään. Esimerkkejä on pyritty löytämään siten, että niiden avulla saataisiin arvioitua, missä määrin lohkoketjuteknologiaa pyritään jo nyt hyödyntämään eri toimialoilla.

1.4 Työn rakenne

Työ etenee siten, että luvussa kaksi määritellään yleiskäyttöinen teknologia ja minkä ehtojen tulee täyttyä, jotta teknologiaa voidaan kutsua yleiskäyttöiseksi. Kolmannessa luvussa avataan lohkoketjuteknologian toimintaperiaatteita ja käydään läpi teknologian merkittävyyden kannalta oleellisimpia teknisiä ratkaisuja. Neljännessä luvussa pyritään löytämään vastaus sille, onko lohkoketjuteknologiasta uudeksi yleiskäyttöiseksi teknologiaksi. Viidennessä luvussa käydään esimerkkien kautta potentiaalisia lohkoketjuteknologian sovellutusalueita. Kuudennessa luvussa esitetään tämän tutkimuksen johtopäätökset.

2 YLEISKÄYTTÖINEN TEKNOLOGIA

2.1 Yleistä

Cummins ja Violante (2002) muotoilevat asian kuvailemalla yleiskäyttöisen teknologian olevan sellainen teknologia, joka kiihdyttää kasvuvauhtia yhtäläisesti kaikilla teollisuudenaloilla. Yleiskäyttöinen teknologia (General Purpose Technology, GPT) voidaan määritellä Lipsey ym. (2005) mukaan geneeriseksi tuotteeksi, prosessiksi tai organisaatiomuodoksi, joka ajan läpi tapahtuvasta kehittymisestä huolimatta pysyy yleispiirteiltään tunnistettavana. Esimerkiksi ensimmäiset kaappitietokoneet ovat täysin eri näköisiä kuin modernit kannettavat tietokoneet, mutta kummatkin ovat yhtä lailla tunnistettavissa tietokoneiksi. Bresnahan ja Trajtenberg (1995) taas toteavat Cumminsin ja Violanten ajatuksen hieman eri tavalla kuvaamalla yleiskäyttöisen teknologian sellaiseksi teknologiaksi, joka kiihdyttää teknologista kehitystä laaja-alaisesti taloudessa ja yhteiskunnassa. Hyytinen (2019) taas täsmentää yhden tärkeän syyn tälle olevan se, että ” yleiskäyttöinen teknologia sekä lisää monilla erilaisilla toimialoilla uusien tavaroiden ja palveluiden markkinoille tuloa että tehostaa erilaisten jo olemassa olevien tuotteiden tuotantoa”.

Yleisesti ottaen on helpompi tunnistaa asioita retrospektiivisesti kuin nykyajassa saatikka tulevaisuuteen päin tarkastellen. Yleiskäyttöisten teknologioiden tunnistaminen etukäteen on haastavaa, mutta välillä on myös vaikeaa taikka täysin mahdotonta tehdä menneisyydessä rajavetoa erilaisten yleiskäyttöisten teknologioiden välillä (Hyytinen, 2019). Hyytinen toteaakin, että aina ei ole selvää, onko jokin yleiskäyttöinen teknologia syy vai seuraus jostain toisesta yleiskäyttöisestä teknologiasta, ja milloin tietyn yleiskäyttöisen teknologian vaikutuksen voidaan katsoa alkaneen ja milloin päättyneen. Tämän havainnon valossa voisi siis peilata tutkimusongelmaa myös siten, että onko lohkoketjuteknologia uusi itsenäinen yleiskäyttöinen teknologia, vai onko kyseessä yleiskäyttöisen ICT-

teknologian johdannainen. Kuitenkin kyseessä on enemmänkin retrospektiivisesti tarkasteltava asia, mistä syystä tämä kysymys jätetään tässä työssä vain huomion asteelle.

Lipsey ym. (2005) toteavat, että ihmiskunnalla voidaan kuitenkin katsoa historiansa aikana olleen aidosti vain 24 yleiskäyttöistä teknologiaa, jotka ovat vaikuttaneet globaalisti ihmiskuntaan. Näistä aikaisin voidaan ajoittaa viljelyksen keksimiseen 9000-8000 eaa. ja viimeisin yhä käynnissä olevaan informaatioteknologian aikakauteen. Varsinainen yleiskäyttöisten teknologioiden kulta-aika alkoi sähköistymisen myötä 1800-luvun lopulla, sillä sähköistymisen jälkeen yleiskäyttöisiä teknologioita on syntynyt jo kymmenen eli noin 42 %:a kaikista yleiskäyttöisistä teknologioista ihmiskunnan historian aikana. Nämä 24 yleiskäyttöisen teknologian aikakautta on lueteltu alla olevassa taulukossa. Kuten taulukosta voi huomata, niin moni yleiskäyttöisistä teknologioista vaikuttaa aina myöhempien yleiskäyttöisten teknologioiden taustalla (esim. höyrykone – höyrylaiva, polttomoottori – moottoriajoneuvo & lentokone, sähkö – tietokone & internet ym.). Tästäkin syystä on mielestäni perusteltua pitää tarkastelu sellaisena, että käsittelemme tutkimusongelmaa siitä näkökulmasta, että, onko lohkoketjuteknologia seuraava eli (Lipsey ym. laskutavan mukaan) 25. yleiskäyttöinen teknologia.

Alla esitetty taulukko on suomennettu versio Lipsey ym. (2005) esittämästä taulukosta. Alkuperäinen taulukko on laadittu lähes 15 vuotta sitten, joten on hyvä huomata, että siitä puuttuu kokonaan 2010-luku.[1] Yleiskäyttöiset teknologiat on luokiteltu kolmeen luokkaan (prosessi, tuote ja organisaatio) sen mukaan, mikä kuvaa parhaiten teknologian luonnetta parhaiten. Huomionarvoista on myös se, että moni yleiskäyttöinen teknologia asettuu päällekkäisille ajanjaksoille. Jatkossa kun tässä pro gradu -tutkielmassa puhutaan yleiskäyttöisistä teknologioista, näitä tuotteita, prosesseja ja organisatorisia keksintöjä kutsutaan vain yksinkertaisesti teknologioiksi.

[1] Katso 2010-luvulle päivitetty, Lipsey ym. (2005) taulukkoa mukaileva taulukko Hyytisen (2019, s. 83) julkaisusta. Tässä taulukossa lohkoketjuteknologia on 28. yleiskäyttöinen teknologia. Toinen 2010-luvulle sijoittuva yleiskäyttöinen teknologia on koneoppiminen, järjestysnumero 29.

Nro	GPT	Ajanjakso	Tyyppi
1	Maanviljely	9000 - 8000 eaa.	Prosessi
2	Karjan kasvattaminen	8500 - 7500 eaa.	Prosessi
3	Malmin sulatus	8000 - 7000 eaa.	Prosessi
4	Pyörä	4000 - 3000 eaa.	Tuote
5	Kirjoitustaito	3400 -3200 eaa.	Prosessi
6	Pronssi	2800 eaa.	Tuote
7	Rauda	1200 eaa.	Tuote
8	Vesimylly	Varhainen keskiaika	Tuote
9	Kolmimastoinen purjelaiva	1400-luku	Tuote
10	Kirjapaino	1500-luku	Prosessi
11	Höyrykone	1700- & 1800-lukujen taite	Tuote
12	Tuotantotehdas-konsepti	1700- & 1800-lukujen taite	Organisaatio
13	Rautatie	1800-luvun puoliväli	Tuote
14	Höyrylaiva	1800-luvun puoliväli	Tuote
15	Polttomoottori	1800-luvun loppupuoli	Tuote
16	Sähkö	1800-luvun loppupuoli	Tuote
17	Moottoriajoneuvo	1900-luku	Tuote
18	Lentokone	1900-luku	Tuote
19	Massatuotanto	1900-luku	Organisaatio
20	Tietokone / ICT	1900-luku	Tuote
21	Lean-tuotantomalli	1900-luku	Organisaatio
22	Internet	1900-luku	Tuote
23	Bioteknologia	1900-luku	Prosessi
24	Nanoteknologia	2000-luku	Prosessi

Taulukko 1: Ihmiskunnan historian aikaiset yleiskäyttöiset teknologiat (Lähde: Lipsey ym. 2005, s. 132)

2.2 Makrotaloudellisia huomioita yleiskäyttöisestä teknologiasta

Yleiskäyttöinen teknologia on tunnistettavissa varmuudella vasta jälkikäteen ja etukäteen teknologian vielä kehittyessä sen ominaispiirteitä on vaikea havaita. Tämän vuoksi ei voidakaan etukäteen luotettavasti arvioda, että kohdennetaanko mahdollisen uuden yleiskäyttöisen teknologian kehittämisen resurssit yhteiskunnan kannalta tehokkaasti. Lisäksi yleiskäyttöiseen teknologiaan liittyy myös komplementaaristen keksintöjen ja innovaatioiden ketju, missä siis teknologiasta syntyvät sovellutukset itsessään tukevat teknologian jatkokehittämistä. (Hyytinen, 2019).

Jos selkeyden vuoksi puhumme siitä, että yleiskäyttöisellä teknologialla on epämääräisen ja tulkinnanvaraisen alun sijasta selkeämpi teknologian alkuajankohta, käy uusi yleiskäyttöinen teknologia Helpmanin ja Tratjenbergin (1994) mukaan läpi syklin, jossa heidän mukaansa on kaksi voimakasta makrotaloudellista vaihetta. Ensimmäinen yleiskäyttöisen teknologian vaihe yhteiskunnallisilta vaikutuksiltaan on ”kylvämisen aika” ja toinen on ”niittämisen aika”. Kylvämisen ajalle ominaista on, että resurssit ohjataan komplementaaristen tuotantopanosten kehittämiseen, jotka mahdollistaisivat uuden yleiskäyttöisen teknologian hyödyntämisen. Tämän aloitusvaiheen aikana alkuvaiheen tuotanto ja (mitattu) tuottavuuden kasvu hidastuu ja reaalipalkat jäävät stagnaatiotilaan.

Toinen vaihe, eli ”niittämisen aika” tulee kun komplementaariset tuotantopanokset ovat kehittyneet tarpeeksi, jotta uusi yleiskäyttöinen teknologia voidaan ottaa täysimääräisenä käyttöön ja hyödynnettäväksi. Tästä uuden yleiskäyttöisen teknologian tehokkaasta ja täysimääräisestä käytöstä laajalti yhteiskunnassa seuraa (mitatun) talouskasvun aikakausi, jolloin tuotanto, reaalipalkat ja voitot kasvavat. Kun syntyy uusi yleiskäyttöinen teknologia, toistuu tämä kaksivaiheinen sykli taas. (Helpman ja Tratjenberg, 1994).

Hyytisen (2019) mukaan taloustieteen ja taloushistoriallisen tutkimuskirjallisuuden mukaan voidaan jokseenkin kiistattomasti jälkikäteen arvioida, että monet yleiskäyttöiset teknologiat ovat ”nopeuttaneet teknologista kehitystä, kiihdyttäneet tuottavuuskasvua ja muokanneet laajasti yhteiskuntaa ja taloutta”. Hän kuitenkin tarkentaa, että on jossain määrin epäselvää, että missä määrin ja millaisilla mekanismeilla yleiskäyttöiset teknologiat ovat vaikuttaneet tekniseen ja taloudelliseen kehitykseen. Pitkän aikavälin talouskasvu kuitenkin perustuu talouden kokonaistuottavuuden kehittymiseen.[2]

---

[2] Perinteinen neoklassinen talousteoria kuvaa kasvumalleissaan teknologian eksogeeniseksi muuttujaksi. Tällainen teknologian käyttö taloudessa parantaa pääoman käyttöastetta, mikä johtaa myös työn tuottavuuden kasvuun tätä teknologiaa käyttävillä aloilla, mutta ei itsessään lisää kokonaistuottavuutta. Yleiskäyttöisen teknologian tiedetään lisäävän kokonaistuottavuutta, joten selitykseksi voidaan tarjota ns. läikkymisefektiä (spill-over) tai edellä mainittua komplementaaristen tuotantopanosten kehittymistä. (Basu & Fernald, 2006).

Yleiskäyttöisistä teknologioista puhuttaessa on vielä otettava huomioon mittausongelma eli se, onko kyseessä todellisesta vai mitatusta tuottavuuden kasvun hidastumisesta. Yleiskäyttöisen teknologian ominaispiirre on, että niiden vaiheittainen käyttöönotto nopetuttaa talouskasvua vasta viiveellä. Tätä pidetään yhtenä syynä sille, että pitkällä aikavälillä havaitaan talouskasvun nopeuden vaihtelua (ns. Kondratieffin syklit). Tämä tarkoittaa sitä, että yleiskäyttöinen teknologia voi aluksi hidastaa (mitattavaa) tuottavuutta. Syyksi tälle nähdään muun muassa se, että uuden yleiskäyttöisen teknologian hyödyntäminen vaatii eri toimijoilta sopeutumista ja toimintansa uudelleejärjestelyä, mikä itsessään sitoo resursseja. (komplementaariset investoinnit).

Toisekseen uusi yleiskäyttöinen teknologia on harvemmin suoraan käyttövalmis, vaan sen käyttöönottoa ja hyödyntämistä varten tulee kehittää uusia välituotteita. Tämä näkyy yleiskäyttöisen teknologian leviämistä kuvaavassa tilastoaineistoon perustuvassa kuvaajassa J:n muotoisena tuottavuuskehityksenä (x-akseli: aika, y-akseli: tuottavuuskehitys), mikä siis tukee väitettä siitä, että yleiskäyttöinen teknologia aluksi hidastaa tuottavuutta. Tämä kuitenkin saattaa osiltaan johtua mittausongelmista, sillä monet uuden teknologian investoinnit ovat aineettomia ja tulevat täten helposti tilastoissa aluksi aliarvioiduiksi ja myöhemmin yleiskäyttöisen teknologian ”hyötyasteen” noustessa tulevat yliarvioiduiksi. (Hyytinen, 2019).

Huomionarvoista on peilata tätä mittausongelmaa myös Lipsey ym. (2005) esittelemään tuottavuuden paradoksin myyttiin (the myth of the productivy paradox). Sen mukaan on virheellistä olettaa, että uusi yleiskäyttöinen teknologia automaattisesti tuottaa ennemmin tai myöhemmin tuottavuusbonusta. Yleiskäyttöisen teknologian tuottamat innovaatiot leviävät jopa vuosikymmenten aikajänteelle, eivätkä välttämättä ole ajallisessa yhteydessä toisiinsa. Näin ollen teknologia on vain tuottavuuden kasvun luonnollinen komponentti eikä se sisällä mitään erityisiä kasvuvauhtibonuksia.

Seuraavaksi käydään läpi niitä ominaispiirteitä, jotka erottavat laajasti käytetyn teknologisen ratkaisun varsinaisesta määritelmän mukaisesta yleiskäyttöisestä teknologiasta. Tämän jälkeen käymme läpi yleiskäyttöisen teknologian syklisyyttä ja tarkastelemme sitä niin Schumpeterilaisen kasvumallin kautta. Lopuksi tustumme case-tyyppisesti yleiskäyttöisen teknologian käyttön vaikutuksiin sähkön ja informaatioteknologian kautta.

2.3 Yleiskäyttöisen teknologian tunnuspiirteet

Millä voidaan sitten tunnistaa, että teknologia on juuri yleiskäyttöinen teknologia, eikä kyseessä ole muuten laajasti omaksuttu teknologia? Etukäteen tämä tunnistaminen onkin haastavaa, kuten edellä on jo todettu. Jälkikäteisessä tarkastelussa voidaan sen sijaan havaita, että pääominaispiirre yleiskäyttöiselle

teknologialle on se, että se johtaa perustavanlaatuisiin muutoksiin niissä tuotantoprosesseissa, jotka hyödyntävät uutta yleiskäyttöistä teknologiaa (Helpman ja Tratjenberg, 1996). Toisin sanoen kyseessä ei ole teknologia, joka hieman vain tehostaa tuotantoprosessia, vaan teknologia, joka muuttaa tapaa tehdä asioita. Toisessa tutkimuksessa Bresnahan ja Trajtenberg (1995) listaavat kolme tunnuspiirrettä, jotka teknologiasta tulisi löytyä, jotta sen voitaisiin katsoa täyttävän yleiskäyttöisen teknologian tunnusmerkistön erotuksena laajasti omaksuttuun (”normaaliin”) teknologiseen innovaatioon. Esimerkiksi jokainen taulukossa 1 esitetty teknologia sisältää nämä yleiskäyttöisen teknologian kolme tunnuspiirrettä[3].

1. Kokonaisvaltaisuus – GPT levittäytyy useimmille talouden ja yhteiskunnan aloille.

2. Kehittyminen – GPT kehittyy ajan kuluessa ja alentaa jalostuessaan käyttäjiensä kustannuksia.

3. Innovaatioiden syntyminen – GPT helpottaa uusien tuotteiden, prosessien ja sovellusinnovaatioiden keksimistä.

Kokonaisvaltaisuuden tunnuspiirre tarkoittaa sitä, että yleiskäyttöinen teknologia on laajalti käytössä yhteiskunnassa ja taloudessa mitä erilaisimmilla aloilla ja käyttötarkoituksissa. Voisi sanoa, että yleiskäyttöisen teknologian lopullista käyttökohdetta ei voi päätellä siitä, mikä teknologia on kyseessä. Tietysti eri yleiskäyttöiset teknologiat näyttelevät erilaista roolia talouden eri alueilla riippuen siitä mikä teknologia on kyseessä, eikä voi yleispätevästi todeta jotain tiettyä käyttöastetta tai prosenttia, mikä määriteltäisiin yleiskäyttöisen teknologian rajaksi. Kuitenkin teknologian kokonaisvaltaisuus erottaa yleiskäyttöisen teknologian muusta laajasti omaksutusta teknologiasta. Kehittymisen tunnuspiirre taas tarkoittaa sitä, että yleiskäyttöinen teknologia kehittyy ja jalostuu jatkuvasti, kun siitä kehitetään uusia versioita. Toisien sanoen se mukautuu ympäröivään maailmaan siinä, missä ympäröivä maailmakin mukautuu siihen, mutta perusidealtaan yleiskäyttöinen teknologia on sama kuin sen ensimmäinen versio, vaikka teknisesti olisikin vuosien tai vuosikymmenien aikana otettu huomattavia kehitysaskeleita. Kolmas tunnuspiirre eli innovaatioiden syntymisen tarkoittaa sitä, että yleiskäyttöisen teknologian ansioista keksitään täysin uusia tuotteita, prosesseja ja sovellusinnovaatioita eli voidaan sanoa yleiskäyttöisen teknologian mahdollistavan asioita, jotka eivät ennen ole olleet mahdollisia. Riippuen siitä, onko yleiskäyttöinen teknologia prosessi, tuote vai organisaatio (kts. Taulukon 1

[3] Kuten aiemmin jo todettu, ex ante -tarkastelussa nämä tunnuspiirteet voivat olla hyvinkin vaikeita havaita, vaikka ex post -tarkastelussa ne olisivatkin selvästi nähtävissä.

luokittelu), on sen tuottamat innovaatiot luonteeltaan erilaisia, eikä tässäkään voi yksiselitteisesti etukäteen ennustaa minkä tyyppisiä innovaatiota ne tuottavat. Sovellusinnovaatiot ovat ehkäpä helpoimpia visioitavia etukäteen, minkä vuoksi tämänkin työn viides luku keskittyy lohkoketjuteknologian sovellutuksiin. Kuitenkaan varmoja vastauksia ei saada kuin vasta jälkikäteisessä tarkastelussa vuosien tai vuosikymmenien päästä yleiskäyttöisen teknologian synnystä.

Mitä nämä kolme tunnuspiirrettä tarkoittavat sitten konkreettisesti? Otetaan yleiskäyttöisen teknologian esimerkkitapaukseksi tietokone. Voimme melko vaivattomasti ja yksiselitteisesti havaita kaikki kolme tunnuspiirrettä esimerkistämme, sillä -kuten jo useasti todettu- jälkikäteen historiaa tarkastellessa näiden tunnuspiirteiden havainnoiminen on melko helppoa. Vaikeampaa, ellei jopa mahdotonta, on löytää näitä piirteitä teknologioista, jotka ovat vasta tulossa käyttöön ja laajemmin saataville. Yleiskäyttöisen teknologian ensimmäinen tunnuspiirre tietokone-esimerkissämme on tietokoneiden kokonaisvaltainen käyttö yhteiskunnassa ja taloudessa, mikä on jo intuitiivisestikin nykyaikaan peilaten lähes itsestäänselvyys. Tietokoneet ovat levinneet kaikkialle: esimerkiksi teollisuuteen, koteihin, autoihin sekä yksittäisiin laitteisiin ja esineisiin. Siinä missä työpaikoilla ja kotona eri tarkoituksiin käytettävät perinteisen malliset tietokoneet ovat tietokoneita klassisimmillaan, löytyy tietokoneita esimerkiksi niin autojen turva- ja viihdejärjestelmistä kuin lasten leluista. Tästä päästäänkin yleiskäyttöisen teknologian toiseen tunnuspiirteeseen, joka sovellettuna esimerkkiimme on tietokoneiden kehittyminen: ensimmäiset tietokoneet olivat yksinkertaisia, kalliita ja huoneen kokoisia laskentakaappeja. Nykyisin tietokone voi olla hyvinkin edullinen ja mahtua taskuun taikka lelun sisälle ja se suorittaa moninkertaisen määrään laskentaoperaatioita sekunnissa verrattuna teknologian varhaisempiin versioihin. Yhtä lailla ”kaappitietokone” ja ”ultrabook-läppäri” ovat kuitenkin edelleen tunnistettavissa tietokoneiksi, joilla on sama teknologinen tausta. Myöskin kännykkä tai lelu on tunnistettavissa tietokoneiksi, kun kuorten alta paljastetaan piirilevy. Bresnahan ja Trajtenberg (1995) toteavatkin, että tämä ehtojen toinen tunnuspiirre käsittelee erityisesti yleiskäyttöisen teknologian tuottavuuden ja ”hyötysuhteen” kasvua ajassa. Tämä tarkoittaa sitä, että tuottavuuden kasvun kautta yksikkökustannuksen tulisi laskea ajan myötä teknologian kehittyessä ja yleiskäyttöisen teknologian käyttämisen kustannusten tulisi alentua. Kolmas yleiskäyttöisen teknologian tunnuspiirre tietokone-esimerkissämme on innovaatioiden syntyminen. Siinä, missä ensimmäiset tietokoneet olivat tutkimuskäytön lisäksi lähinnä sotilaskäytössä, ovat nykyaikaiset tietokoneet kokonaisvaltaisen leviämisen lisäksi synnyttäneet jopa uusia talouden aloja. Näistä uusista talouden aloista mainittakoon muun muassa graafinen mallintaminen (esim. pelit ja elokuvat), teollisuusrobotit- ja -automaatio sekä puhelimet ja älylaitteet. Bresnahan ja Trajtenberg (1995) huomauttavat kuitenkin, että kaikki yleiskäyttöiset teknologiat eivät yhtäläisesti synnytä monia uusia innovaatioita, vaan monet niistä pikemminkin tehostavat olemassa olevia prosesseja. Tässä mielessä tietokonetta voidaan pitää poikkeuksellisena yleiskäyttöisenä teknologiana, sillä se on tehostanut huomattavissa määrin niin olemassa olevia prosesseja kuin luonut paljon uusia keksintöjä.

Lopuksi on kuitenkin tärkeää huomata, että vaikka kaikki yleiskäyttöiset teknologiat täyttävät jälkikäteisessä tarkastelussa nämä kolme teknologialta vaadittua tunnuspiirrettä, niin jokainen yleiskäyttöinen teknologia etenee omalla vauhdillaan ja tavallaan yksilöllisenä kehityskaarena. Esimerkiksi sähkö yleiskäyttöisenä teknologiana eteni suhteellisen vauhdikkaasti ja kokonaisvaltaisesti siten, että sähkö otettiin laajalti käyttöön sen varhaisessa ”kantamuodossa” ja toiseen tunnuspiirteeseen peilaten kehityskaarensa alussa. ICT (Information and Communication Technology) taas on yleiskäyttöisenä teknologiana levittäytynyt pikemminkin kehittymisen ja innovaatioiden kautta muualle talouteen ja yhteiskuntaan. Toisin sanoen ICT-innovaatiot ja ICT:n kehittyminen ovat tuoneet siihen yleiskäyttöisenä teknologiana kokonaisvaltaisuutta, kun taas sähkö on kokonaisvaltaisuutensa vuoksi kehittynyt ja synnyttänyt uusia innovaatioita. (Jovanovic & Rosseau, 2005).

2.4 Yleiskäyttöisen teknologian syklisyys

Aghion ym. (2013) toteavat, että vaikka yleiskäyttöinen teknologia kasvattaa kokonaistuotantoa ja tuottavuutta pitkällä aikavälillä, voi se aiheuttaa syklistä heiluntaa sillä aikaa kuin talous sopeutuu kyseiseen yleiskäyttöiseen teknologiaan. Puhuttaessa pitkän aikavälin talouden kasvun kiihtymisistä ja hidastumisista korostaen juuri tätä syklistä heiluntaa, on kyseessä ns. Kondratieffin sykli ja yleiskäyttöisiä teknologioita pidetään Kondratieffin syklien todennäköisimpinä selittäjinä (Aghion ym., 2013). Tätä teemaa sivusimme jo luvun alkupuolella puhuessamme Helpmanin ja Trajtenberg (1994) esittelemistä kylvön ja niittämisen vaiheista. Vastoin oletusta, ensimmäinen ”positiivinen teknologiashokki” ei välttämättä nosta kokonaistatuotantoa, tuottavuutta ja työllisyyttä, vaan pikemminkin alentavat niitä (Ahgion ym., 2013).

Yleiskäyttöiset teknologiat ovat luonteeltaan Schumpeterilaisia, jossa uudet teknologiat syrjäyttävät vanhat ”luovan tuhon” kautta, joten ne tyypillisesti johtavat kokonaisvaltaisesti talouteen levittäytyessään vanhempien teknologioiden hylkäämiseen (Ahgion ym., 2013). Helpman ja Trajtenberg (1998) toteavatkin, että yleiskäyttöinen teknologia ei tule valmiina tarjolle, vaan vaatii ensiksi kalliita välituotteita, jotta se voidaan implementoida kokonaisvaltaisesti talouteen ja yhteiskuntaan. Jovanovic & Rosseau (2005) esittelevät tutkimuksessaan yleiskäyttöisen teknologian kolmen tunnuspiirteen lisäksi muiden aiemmin mainittujen tutkijoiden kanssa linjassa olevia huomioita siitä, että uusi yleiskäyttöinen teknologia aiheuttaa aluksi negatiivisia vaikutuksia taulouteen. Myös heidän mallinsa ennustavat, että tuottavuus tulee aluksi hidastumaan. Uusi teknologia ei välttämättä ole käyttäjäystävällistä ja tuotanto saattaa laskea hetkellisesti, kunnes talous sopeutuu tähän teknologiaan. Yleiskäyttöisen teknologian kanssa voikin myös olla ongelmana se, ettei alkuun välttämättä edes tunnisteta niitä käyttökohteita missä yleiskäyttöinen teknologia on omimmillaan. Uudet yleiskäyttöiset teknologiat ovat myös monesti työvoimakustannuksiltaan kalliita ottaa käyttöön

eli osaavan työvoiman preemio on korkea. Tämä johtuu siitä, että jos uusi teknologia ei ole käyttäjäystävällistä, on uuden teknologian saapuessa osaavan työvoiman kysyntä monesti huomattavasti tarjontaa suurempaa ja osaavat ammattilaiset voivat hinnoitella itsensä korkeammalle.

Schumpeterilaisen luovan tuhon teorian mukaan uuden yleiskäyttöisen teknologian tulo talouteen aiheuttaa varallisuuden uudelleenallokoitumista. Kyseisen mallin mukaan hyödyke tuottaa voittoa keksijälleen patentin suojaaman eksklusiivisen tuotantokäytön turvin (Aghion ym., 2013). Uusia yrityksiä astuu markkinoille, vanhoja poistuu ja ne yhdistyvät toisiin toimijoihin. Myöskään osakemarkkinat eivät selviä ilman uuden teknologian negatiivista vaikusta, sillä Jovanovic & Rosseau (2005) huomasivat myös, että osakekurssit laskevat aluksi. Tämä johtuu siitä, että vanhan pääoman arvo laskee, sillä uusi teknologia tekee monesti vanhaa teknologiaa turhaksi. Esimerkiksi höyrykoneilla toimivan tehtaan arvo laskee sen myötä, kun tehtaita varustetaan sähkömoottoreilla. Laskuvauhti korreloi sen kanssa, miten markkinat vastaanottavat uuden teknologian, eli uuden yleiskäyttöisen teknologian leviämisnopeus määrää osakemarkkinoiden notkahduksen jyrkkyyden. Tällaisessa toimikentässä monesti nuoret ja pienet yritykset pärjäävät paremmin, sillä yleiskäyttöisen teknologian adaptoimisessa nuoret yritykset ovat pääsääntöisesti vanhoja ja isoja yrityksiä ketterämpiä. Viimeisenä nostona Jovanovicin & Rosseaun (2005) tutkimuksesta on se, että korot nousevat ja kauppataseeseen syntyy vajetta. Uusi teknologia muokkaa monesti myös kulutustottumuksia ja uusi tuotanto ei välttämättä pysy halutun kulutuksen mukana.[4]

Miten Schumpeteriläinen kasvumalli sitten tulkitsee yleiskäyttöistä teknologiaa ja selittää sen syklisyyttä? Aghion ym. (2013) sekä Helpman & Trajtenberg (1998) mukaan saavuttaaksemme yleiskäyttöistä teknologiaa hyödyntävän lopputuotteet, tulee työntekijän käyttää työpanoksensa L joko tätä yleiskäyttöistä teknologiaa hyödyttävän välituotteen valmistamiseen tai siihen kohdistuvaan tutkimustyöhön. Oletuksena on, ettei tätä lopullista tuotetta voida saavuttaa ilman vähintään yhden välituotteen hyödyntämistä. Tämä on kaksivaiheinen prosessi, jossa uuden yleiskäyttöisen teknologian täytyy ensiksi syntyä, jotta voidaan kehittää tätä teknologiaa paremmin talouteen implementoivia tuotteita. Kumpikaan vaiheista ei voi tulla toisessa järjestyksessä. Kylvämisen ja niittämisen sykli –kuten Helpman & Trajtenberg sitä kuvaavat- alkaa uuden yleiskäyttöisen teknologian saapumisella, jolloin työvoimaa L kohdistetaan näiden välituotteiden kehittämiseen (kylväminen). Tänä aikana talouskehitys on laskusuhdanteista, kunnes ajan t kuluttua keksitään niitä välituotteita, joilla pystytään implementoimaan yleiskäyttöinen teknologia kokonaisvaltaisesti talouteen. Tällöin työvoima L kohdistuu kyseisten välituotteiden valmistamiseen ja taloudessa on noususuhdanne (niittäminen). Lasku- ja noususuhdanteen sykli alkaa alusta,

[4] Tässä opinnäytetyössä ei paneuduta kovin tarkasti edellä esitettyjen mallien empiiriseen tarkasteluun, joten empiiriset tulokset käydään läpi vain löydösten kommentointina. Jovanovic & Rosseau (2005) käyttävät empiriassaan aineistoa, joka käsittelee sähköistämisen ja ICT:n aikakautta.

kun keksitään uusi yleiskäyttöinen teknologia, jonka implementointi talouteen aloitetaan välituotteiden kehittämisestä.

Aiemmin tässä kappaleessa puhuttiin osaavan työvoiman preemiosta yleiskäyttöisen teknologian hyödyntämisessä. Tarkastellaan tätä vielä Aghionin ym. (2013) sekä Helpmanin & Trajtenbergin (1998) kautta. He jakavat työvoiman kahteen luokkaan: koulutettuihin ja kouluttamattomiin. Koulutetut voivat työskennellä niin tuotekehityksessä kuin itse tuotannossa. Kouluttautumattomat voivat työskennellä pelkästään tuotannossa. Syklin ensimmäisessä vaiheessa koulutettu työvoima hakeutuu kehittämään korkean tuottavuuden komplementaarisia tuotteita (välituotteita) yleiskäyttöisen teknologian implementoimiseksi ja kouluttautumaton työvoima kohdistuu tuotantoon. Samaan aikaan laskusuhdanteessa työvoimapanos kuitenkin kohdistuu kehittämiseen, jolloin tuotannon työpaikkojen tarjonta vähenee, eikä kaikelle kouluttamattomalle työvoimalle riitä töitä. Kun yleiskäyttöisen teknologian implementoimiseen tarvittava välituote on keksitty ja työvoima kohdistuu enemmän tämän välituotteen tuotantoon, kilpailevat noususuhdanteessa koulutetut ja kouluttamattomat samoista tuotannon työpaikoista. Kun asetamme koulutetun työvoiman tuottavuuden suhteutettuna palkkaan korkeammalle kuin kouluttamattoman, menee tuotannonkin työpaikat noususuhdanteessa ensisijaisesti koulutetulle työvoimalle. Tämä aiheuttaa sen, että uusi yleiskäyttöinen teknologia tuo koulutetulle työvoimalle palkkaan taitopreemion ja kouluttamatton työvoima jää häviäjän rooliin. Lisäksi Hyytinen (2019) toteaa, että mikäli uudella yleiskäyttöisellä teknologialla korvattavissa olevien työvaiheiden tai tehtävien pääomahyödykkeen hinta on riittävän alhainen, korvaavat kyseiset pääomahyödykkeet työvoimaa.

2.5 Yleiskäyttöisen teknologian vaikutus käytännössä

Jovanovic & Rosseau (2005) pitävät sähköä ja informaatioteknologiaa (IT) kahtena kautta aikojen vaikuttavimmista ja tärkeimmistä yleiskäyttöisistä teknologioista ja näin ollen ovat tutkineet, miten nämä kaksi yleiskäyttöistä teknologiaa ovat vaikuttaneet Yhdysvaltojen talouteen. Sen lisäksi, että sähkö ja IT ovat oleellisimmat yleiskäyttöiset teknologiat, on niiden tarkastelu mielekästä senkin johdosta, että yleiskäyttöisen teknologian kolme tunnuspiirrettä on helppo hahmottaa näissä esimerkeissä. Aghion ym. (2013) ottavat esimerkiksi sen, että 1990-luvun puolivälistä alkaen Amerikan tuottavuuden ja BKT:n kasvu alkoi kiihtymään. Selitykseksi tälle on annettu yleiskäyttöisen teknologian ja erityisesti IT-teknologian leviämistä kokonaisvaltaisesti talouteen.

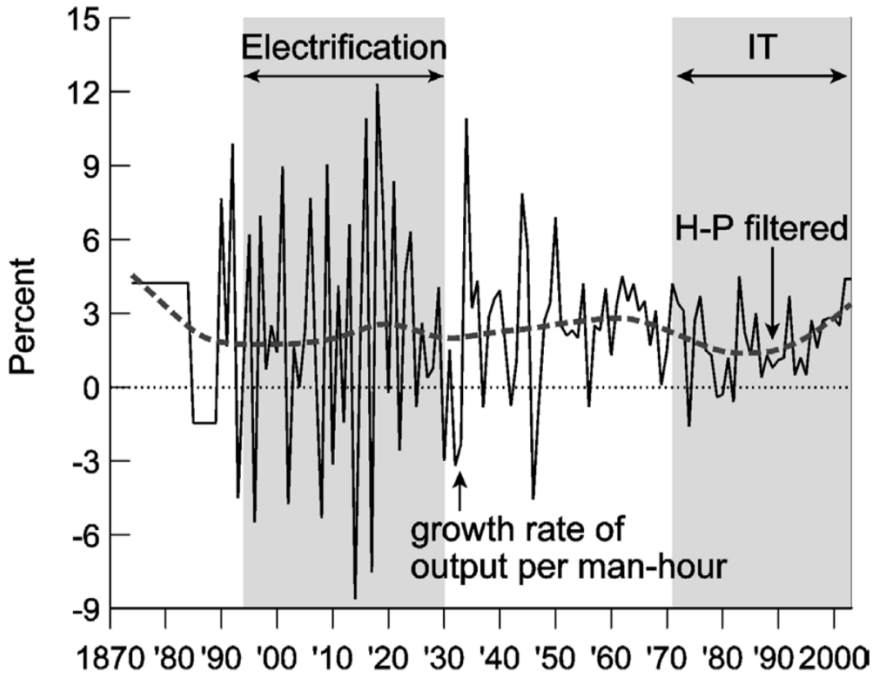
Sähkö yleiskäyttöisen teknologian ajanjaksona voidaan ajoittaa aikavälille 1894-1930 ja IT-ajanjakson alkaneen vuodesta 1971 jatkuen nykypäivään. Kuten aiemmin jo tässä luvussa on mainittu, ei jonkun tietyn yleiskäyttöisen teknologian ajoittaminen tarkasti tiettyyn ajanjaksoon ole aina yksiselitteistä. Jovanovic & Rosseau (2005) huomauttavatkin, ettei sähköistämisen vuotta 1894 ja IT:n vuotta 1971 voi pitää ehdottomina kyseisten yleiskäyttöisten teknologioiden

syntyhetkinä, sillä esimerkiksi New Yorkiin oli rakennettu sähkövoimala 12 vuotta ennen Niagaran putouksen sähkövoimalan avaamista vuonna 1894. Samaten IT:n yleiskäyttöisen teknologian syntyhetkenä pidetään Intelin 4004-mikroprosessorin keksimistä 1971, vaikkakin tietokoneita oli käytetty ensimmäistä kertaa jo pari vuosikymmentä aikaisemmin. Myöskin, kuten alla olevasta kuvaajasta näkyy, on tuottavuuden kasvu alkanut jo vuosikymmen ennen IT:n yleiskäyttöisen teknologian aikakauden alkua. Jovanovic & Rosseau tarkentavatkin yleiskäyttöisen teknologian syntymääritystä siten, että tietyn yleiskäyttöisen teknologian ajanjakso alkaa siitä, kun yleiskäyttöinen teknologian käyttöönottoprosentti on yksi tai yli tyypillisellä (mediaanilla) toimialla.

Jovanovicin & Rosseaun (2005) päähuomiot tässä case-tutkimuksessa olivat, että näiden kahden yleiskäyttöisten teknologian ajanjaksolla tuottavuuden kasvu vaikutti olevan matalampaa erityisesti ajanjaksojen alkuvaiheilla kuin muissa vaiheissa sykliä. Tuotannon taso oli kuitenkin aina aikakauden lopussa korkeammalla kuin aikakauden alussa, joten tuottavuuden kasvu oli kuitenkin positiivista, vaikkakin hidastunutta. Jovanovic & Rosseau huomioivat myös, että kummatkin yleiskäyttöiset teknologiat olivat kokonaisvaltaisesti käytössä taloudessa, mutta sähkön käyttöönotto tapahtui nopeammin läpi toimialojen. Tämän lisäksi kumpikin yleiskäyttöinen teknologia kehittyi sitä mukaan, kun niitä otettiin käyttöön, käyttäjiensä kustannuksia alentava vaikutus oli voimakkaampi informaatioteknologiassa kuin sähkön kohdalla. Kumpikin yleiskäyttöinen teknologia täyttää yleiskäyttöisen teknologian kolmannenkin ominaispiirteen, eli ne ovat myös synnyttäneet laajasti innovaatioita, IT enemmän verrattaessa patenttien ja tuotesuojien määrää. Uudelle yleiskäyttöiselle teknologialle tyypilliseen tapaan teknologian tulo ravisteli tuotannon rakenteita ja kumpikin ajanjakso toi mukanaan Schumpeterilaisen luovan tuhon ja turbulenssin, kun tarkastellaan asiaa pääomamarkkinoiden ja yritysten toimintaympäristöjen muutosten kannalta. Helpman & Trajtenberg (1994) toteavat, että komplementaaristen innovaatioiden eli välituotteiden alhaisempi määrä kasvattaa todennäköisyyttä jonkin yleiskäyttöisen teknologian aikaisemmalle implementaatiolle taloudessa. Vastavuoroisesti isompi komplementaaristen tuotteiden määrä hidastaa yleiskäyttöisten teknologian leviämistä talouteen ja yhteiskuntaan. Subjektiivisesti tarkastellen, Helpmanin ja Tratjenbergin näkemys on linjassa Jovanovicin ja Rosseaun havaintoihin.

Alla olevasta kuvasta 1 yksi voidaan myös huomata, että yleiskäyttöisen teknologian syklit ovat helposti tunnistettavissa trendiviivasta. IT-teknologian kohdalla on selkeä kylvön ajan laskukausi ja sitä seuraava niiton ajan nousukausi. Sähkön kohdalla tämä sykli on myös tunnistettavissa, mutta se on maltillisempi. Myöskin vuosivaihtelu on IT:n kohdalla pienempää ja siitä on helpommin tunnistettavissa J:n muotoinen tuottavuuskehitys. Tämä saattaa viitata mittausongelmaan, jossa aineettomien investointia aikaansaama tuottavuus aliarvioidaan ja panostuksen pääomaan yliarvioidaan noususuhdanteessa (Hyytinen, 2019). Brynjolfsson (2018) huomauttaa, että J:n muotoinen tuottavuuskehitys saattaa olla myös seurausta klassisesta Solow'n tuottavuuden paradoksista, jossa uuden

yleiskäyttöisen teknologian alkuaikoina tarvittavat aineettoman pääoman investoinnit eivät näy tuottavuuden kehityksenä ollenkaan.



Kuva 1: Vuosittainen tuotannon kasvu miestuntia kohden, 1874-2004 (Lähde: Jovanovic & Rosseau 2005)

Sähköistämisen ja IT:n aikakauden samankaltaisuuksia vertaillessa huomionarvoista on myös, että kummankin aikakauden tuottavuuden kasvun alenema on selkeästi nähtävissä tilastollisesta aineistosta ja tarkasteltavana oleviin yleiskäyttöisen teknologian aikakausiin lähdetään korkeamman tuottavuuden kasvun tilasta. Yleiskäyttöisen teknologian aikakauden tuottavuuden kasvu on kuitenkin aina kauden lopussa korkeampaa kuin kauden alussa. Täytyy kuitenkin muistaa, että yleiskäyttöisten teknologioiden rajat ovat epämääräisiä ja esimerkiksi kuvassa näkyvä tuottavuuden kasvun heikentyminen selvästi ennen sähköistymisen aikakautta saattaa viitata jonkin toisen limittäisen yleiskäyttöisen teknologian kylvön aikakauteen.

Jovanovic & Rosseau (2005) havaitsivat tutkimuksessaan myös, että kyseisten yleiskäyttöisten teknologioiden ajankohtina yrityksiä listautui pörssiin ja poistui sieltä enemmän kuin muina ajankohtina. Lisäksi yrityksiin investoitiin enemmän sekä patenttien ja tavaramerkkien myöntöjen määrä kasvoi verrattuna kyseisten aikakausien ulkopuolisiin ajanjaksoihin. Tämä johtuu hyvin paljolti siitä, että uusi yleiskäyttöinen teknologia muokkaa talouden rakenteita laajasti, jolloin on vain luonnollista, että uutta teknologiaa hyödyntävät yrityksen

listautuvat pörssiin ja vanhat sopeutumattomat toimivat poistuvat sieltä. Esimerkiksi sähköistymisen aikakaudella sähkömoottorin keksimisen myötä oli vain luonnollista, että höyrykoneet poistuvat jollain aikavälillä käytöstä. Tämän seurauksena Yhdysvaltojen talouden suurimpien yritysten keski-ikä laski. Jovanovic & Rosseau tekivät myös huomion, että yksityinen kulutus nousee vähitellen yleiskäyttöisen teknologian aikakaudella. Teknologian kehittymisen myötä sen kustannukset alenevat ja tulevat yhä useampien saataville -kulutusmahdollisuudet siis kasvavat. Viimeisenä nostona he huomioivat, että reaalikorot ovat kutakuinkin samat kummankin yleiskäyttöisen teknologian aikakauden aikana ja noin 3% korkeammalla kuin näiden kahden ajanjakson välillä (1930-1970).

Olemme tähän mennessä tunnistaneet yleiskäyttöisen teknologian sykleille ominaisia yhteisiä piirteitä. Kuten aiemmin todettu, on jokaisen yleiskäyttöisen teknologian kehityskaari yksilöllinen. Jovanovic & Rosseau (2005) löysivät sähköistämisen ja IT:n aikakausille viisi eriäväisyyttä. Ensinnäkin innovaatioiden määrä kasvoi huomattavasti nopeammin IT-aikakauden aikana. Patentteja ja tavaramerkkejä haettiin huomattavasti enemmän IT-aikakauden aikana kuin sähköistämisen aikakaudella. Toiseksi IT-tuotteiden kustannukset laskivat sata kertaa nopeammin kuin sähkön kustannukset. Kolmanneksi IT levittäytyi huomattavasti hitaammin kuin sähköistäminen eteni ja käsitti pienemmän osan pääomakannasta. IT:n nettoadoptoiminen jatkuu edelleen. Neljäntenä huomiona oli, että tuottavuuden hidastuminen oli vahvempaa IT-aikakaudella. IT:n adoptoiminen ei aluksi tapahtunut yhtä nopeasti ja laaja-alaisesti kuin sähkön. Viidentenä sähköistämisen ja IT:n aikakausien eroavaisuutena oli se, että sähköistämisen aikakausi tuotti ylijäämää Yhdysvaltojen kauppataseeseen. Tätä lukua tosin osittain vääristää Euroopassa käydyt maailmansodat, jolloin aseteollisuuden vienti vaikutti suuresti lukuihin. IT-aikakaudella sen sijaan Yhdysvaltojen kauppatase on johdonmukaisesti ollut alijäämäinen. Jovanovic & Rosseau toteavatkin, että todisteet selvästi tukevat väitettä, että teknologinen kehitys on epätasaista. Se tuo mukanaan yleiskäyttöisten teknologioiden jaksottaisen saapumisen, ja että nämä yleiskäyttöiset teknologiat tuovat mukanaan turbulenssia ja matalampaa kasvua alkuunsa (ns. kylvön aika), joka myöhemmin sitten vaihtuu korkeampaan kasvuun ja hyvinvointiin (ns. niiton aika). Yleiskäyttöisen teknologian levinneisyyden epätasaisuuteen ja adoptioherkkyyteen vaikuttaa sen vaatimien välituotteiden määrä ja laatu (Helpman & Trajtenberg, 1994).

Jovanovicin & Rosseaun (2005) mukaan empiria tukee teoriaa siitä, että tuottavuus hidastuu ensiksi ja kasvaa tämän jälkeen saavuttaen korkeamman tason kuin mitä se oli ennen yleiskäyttöisen teknologian sykliä. Näin kävi kummankin mainitun yleiskäyttöisen teknologian kohdalla ja esimerkiksi IT:n kohdalla tuottavuus nykypäivänä on paljon korkeampi kuin mitä se oli ennen IT:tä. Toisekseen palkkojen taitopreemion todetaan myös aikasarjojen perusteella olevan korkea kummankin yleiskäyttöisen teknologian alkuaikoina. Kolmanneksi varojen allokoinninkin suhteen tulokset näyttävät, että ne ovat hallitsevampia ajankohtina, jotka liittyvät kyseisiin ajanjaksoihin. Hieman mallin oletuksista poiketen löydösten perusteella sen sijaan osakekurssien laskua ei tapahtunut sähköistämisen alkuaikoina, mutta kurssit laskivat IT:n alkuaikoina.

Sähköistämisen kohdalla Jovanovic & Rosseau epäilevät syyn olleen ainakin osittain se, että 12 vuotta ennen Niagaran putouksen patoa rakennettu New Yorkin voimalaitos auttoi ymmärtämään uuden teknologian potentiaalin ja siirtyminen uuteen teknologiaan oli sulavampaa. Myöskin nuorten yritysten pärjäämisen suhteen tulokset ovat ristiriitaisia. Ne olivat silti kokonaisvaikutukseltaan positiivisia. Sen sijaan uuden teknologian saapuessa Yhdysvallat käyttäytyy uuden yleiskäyttöisen teknologian suhteen suljetun kansantalouden kaltaisesti. Kauppataseen alijäämän kasvu oli nopeampaa IT:n aikakaudella kuin sähköistämisen aikaudella. Kulutus taas kasvoi vähemmän sähköistämisen aikakaudella kuin IT:n aikakaudella. Lisäksi korot kasvoivat enemmän sähköistämisen aikakaudella.

3 LOHKOKETJUTEKNOLOGIA

3.1 Yleistä

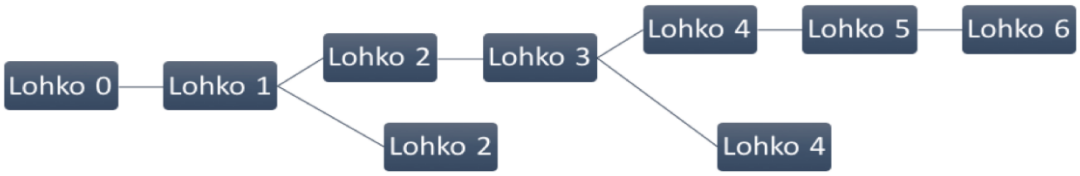
Ymmärtääksemme lohkoketjuteknologiaa yleiskäyttöisen teknologian näkökulmasta ja voidaksemme myöhemmässä luvussa arvioida lohkoketjuteknologian potentiaalisia sovellusinnovaatiota on aluksi ymmärrettävä hieman lohkoketjuteknologiaa ja sen toimintalogiikkaa. Tämän luvun alkupuoliskolla käyn läpi lohkoketjuteknologian toimintaperiaatteita painottaen niitä teknisiä ratkaisuja, jotka tekevät lohkoketjuteknologiasta potentiaalisen yleiskäyttöisen teknologian (GPT-tyyppi[5]: prosessi). Käyn siis läpi sen, miten transaktiot ja niihin oleellisesti liittyvä luottamus (ja luottamuksen kustannus) on lohkoketjuteknologiassa teknisesti ratkaistu. Nostan lisäksi esille muutamia tekniseen toteutukseen liittyviä haasteita, joiden vuoksi näkemykseni on, ettei lohkoketjuteknologia ole nykyisessä toteutusmuodossaan valmis leviämään kokonaisvaltaisesti talouteen ja yhteiskuntaan (GPT:n 1. tunnuspiirre). Kuitenkin osa tässä luvussa esittelemistäni teknisistä toteutuksista indikoi puolestaan, että lohkoketjuteknologia kehittyy ajassa (GPT:n 2. tunnuspiirre). Luvun loppupuoliskolla arvioidaan taloustieteellisestä näkökulmasta, että mikä on luottamuksen merkitys transaktioissa ylipäätänsä ja pyritään tätä kautta löytämään luottamuksen kustannus, mikä voidaan lohkoketjuteknologialla välttää. Lisäksi arvioidaan lohkoketjuteknologian taloudellisia ulottuvuuksia ja tehdään vielä lopuksi huomio siitä, että tietojen pysyvyys ja koskemattomuus ei aina ole positiivinen asia ja saattaa aiheuttaa lainsäätäjän puolelta haasteita lohkoketjuteknologian kokonaisvaltaiselle leviämiselle taloudessa ja yhteiskunnassa.

---

[5] Kts. Tarvittaessa taulukon 1 luokittelu yleiskäyttöisistä teknologioista.

3.2 Lohkoketju ja vertaisverkko

Lohkoketjuteknologialla tarkoitetaan teknologiaa, jossa vertaisverkossa toisilleen tuntemattomat osapuolet ylläpitävät hajautettua ja tietoturvallista tietokantaa ilman, että heidän tarvitsee tuntea tai luottaa toisiinsa. Lohkoketjuteknologia esiteltiin alun perin vuonna 2008 Satoshi Nakamoton toimesta osana Bitcoin-virtuaalivaluutan teknisiä ratkaisuja. Lohkoketjuteknologia oli Nakamotolle työkalu varmentaa Bitcoinin luotettavuus ja turvallisuus ilman, että tähän tarvittaisiin kolmatta osapuolta. Avaininnovaatio lohkoketjuteknologiassa on se, että vertaisverkkoon hajautetut lohkot muodostavat informaatioketjun – lohkoketjun, jossa osapuolten ei tarvitse tuntea toisiansa voidakseen luottaa lohkojen sisältämään informaatioon. Lohkoketju on aina yhtenäinen ketju, jossa lohkosta n voidaan aina palata katkeamattomasti ensimmäiseen lohkoon 0 saakka. Uusien lohkojen luomisprosessista johtuen samanaikaisia lohkoja voi syntyä useampia, jolloin pisin yhtenäinen ketju jää voimaan (Nakamoto 2008). Lohkoketjujen tarkempaan tekniseen toimintaan palataan teknisiä ominaisuuksia käsittelevässä kappaleessa.



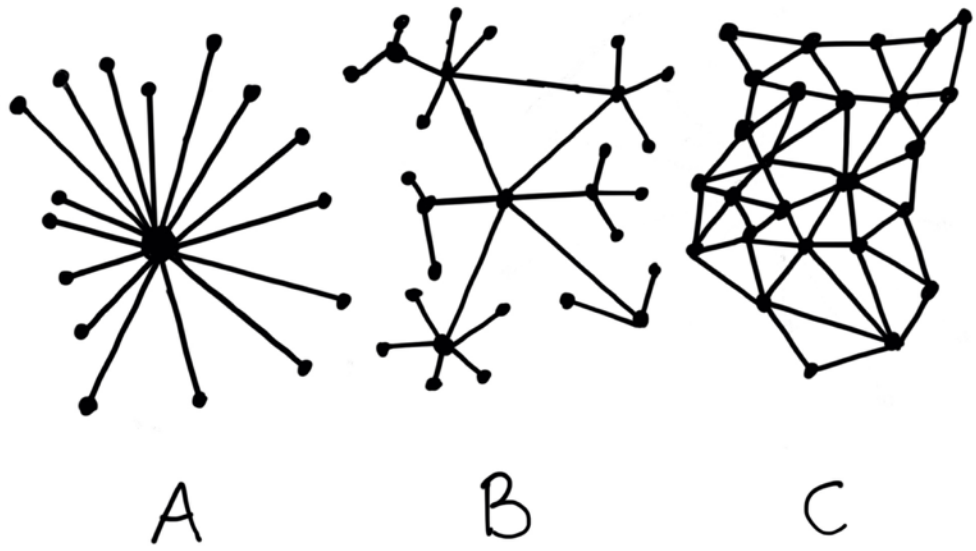
Kuva 2: Lohkoketju (Lähde: Nakamoto 2008)

Muun muassa Catalini & Gans (2016) esittävät tutkimuksessaan, että lohkoketjuteknologian suurimmat hyödyt saavutetaan kustannuksettomassa varmentamisessa sekä verkostoitumiskulujen pienemisenä. Ymmärtääksemme nämä hyödyt, käydään seuraavaksi lyhyesti läpi, miten nykyisenkaltainen järjestelmä toimii ja mikä on vertaisverkko.

Nykyinen järjestelmä perustuu kolmannen osapuolen, välittäjän toimintaan. Esimerkiksi kaupassa luottokortilla maksettaessa myyjä ja ostaja eivät maksun suhteen suoranaisesti asioi keskenään, vaan välikäden, luottokortin myöntäjän kanssa. Kun ostaja ostaa myyjän myymän tuotteen luottokortilla, luottokorttiyhtiö lupaa maksaa myyjälle tuotteen ostajan puolesta ja laskuttaa asiakkaalta tuotteen hinnan luottokorttilaskun yhteydessä. Ennen luottokortin myöntämistä, luottokorttiyhtiö on varmentanut ostajan luottokelpoisuuden. Luottokorttiyhtiö ottaa myyjältä transaktiosta myyjän ja luottokorttiyhtiön välisen sopimuksen mukaisen palkkion ja laskee korkoa ostajan luottokorttilaskulle

luottokorttiyhtiön ja ostajan välisen luottosopimuksen mukaisesti. Lohkoketjuteknologiaan nojautuvissa ratkaisuissa tällaista kallista kolmatta osapuolta ei tarvita, vaan osapuolten varmentaminen tehdään osapuolten välillä kustannuksitta.

Vertaisverkko taas on kokoelma verkkoon liitettyjä päätelaitteita, jotka toimivat sekä asiakkaana että palvelimena ilman varsinaista kiinteitä keskuspalvelimia tai dedikoituja asiakkaita (Rüdiger 2002). Hajautetut ja keskitetyt verkot toimivat taas niin, että niissä palvelimet toimivat solmukohtina, joiden kautta asiakkaat pääsevät käsiksi dataan. Keskitetyssä verkossa tällaisia solmukohtia on vain yksi, kun taas hajautetussa verkossa niitä on useampia. Tyypillisesti transaktiot internetissä nojaavat tällaisiin luotettuihin solmukohtiin ja välittäjiin (Catalin & Gans 2016). Luotetun ja tietoturvallisen solmukohdan ylläpito kuitenkin maksaa ja kustannus kohdistuu solmun ylläpitäjään. Vertaisverkossa jokainen lohkoketjun ylläpitoon osallistuva kone toimii tällaisena solmuna ja täten myös kustannukset jakautuva vertaisverkon kesken. Nakamoto (2008) esitteli julkaisussaan kannustimet, joilla käyttäjät saadaan osallistumaan vertaisverkon ylläpitoon. Näihin kannustimiinkin palataan seuraavassa kappaleessa.



Kuva 3: Keskitetty verkko (A), Hajautettu verkko (B) & Vertaisverkko (C) (Lähde: Nasville Medical News 2017)

3.3 Hajautettu tilikirja

Lohkoketjuteknologian perimmäisin innovaatio on hajautettu tilikirja (distributed ledger). Tämä toteutetaan sisällyttämällä kirjaukset verkkoon hajautettuihin

lohkoihin, jotka muodostavat katkeamattoman kirjausketjun, lohkoketjun. Yleisellä tasolla digitaalisten transaktioiden perimmäinen ongelma on kaksinkertaisen menon (double spend) ongelma. Kaksinkertaisessa menossa on kyse siitä, että henkilö ei voi käyttää samaa rahasummaa kahdesti, täten hänen menonsa on kirjattava johonkin ylös reaaliaikaisesti reagoimaan tehtyihin transaktioihin. Vallitsevassa systeemissä tämä tarkoittaa tietojen kirjaamista pankkien digitaalisiin tilikirjoihin (ledger). Nykyisen kaltainen systeemi kuitenkin edellyttää sitä, että tilikirjan haltija on aina luotettu taho, joka varmentaa tilikirjan tietoturvan sekä sen, että tilikirja on aina ajan tasalla. Lohkoketjuteknologialla hajautettu tilikirja taas on julkinen eli kaikkien saatavilla ja kuka tahansa pystyy varmentamaan transaktiot. Tämä poistaa keskusauktoriteettien tarpeen. (Barrdear 2014).

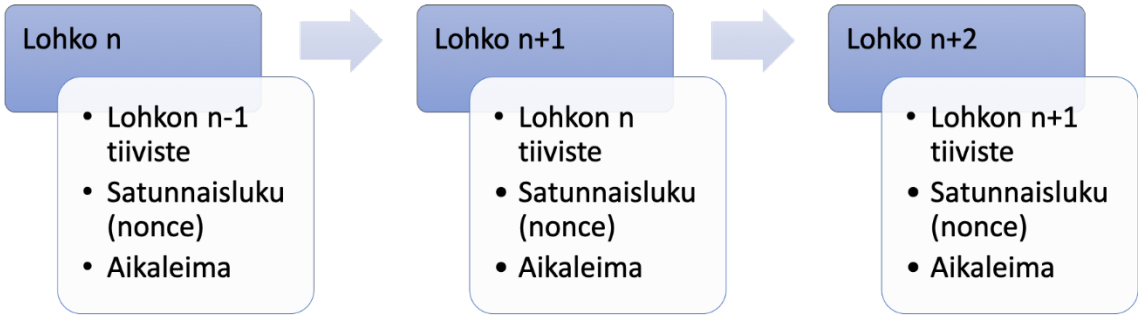
Lohkoketju on siis digitaalinen, ikuisesti laajeneva hajautettu tilikirja, jonka jokainen lohko sisältää tiivisteen (hash) edellisestä lohkosta. Näin ollen lohkoketju on katkeamaton ja muuntumaton, ja kuten aiemmin todettu, voidaan lohkosta n aina palata ensimmäiseen lohkoon 0 asti. Jokainen lohko on kryptattu ja digitaalisesti allekirjoitettu siten, että lohkon jälkikäteen muuttaminen mitätöi kaikki aiemmat lohkot aina lohkoon 0 asti ja estää täten tietyn lohkon tietojen peukaloimisen jälkikäteen. Tämä estää tehokkaasti lohkoketjun hakkeroimisen, ellei hakkeroijalla ole hallussaan yli 50%:a kaikista olemassa olevista lohkoista (ns. 51% –hyökkäys, jossain kirjallisuudessa 50% + 1 -hyökkäys). Lohkoketjuteknologiaan sisällytetyt kannustimet uusien lohkojen luomiseen ovat sellaiset, että laskentakapasiteetti on taloudellisesti järkevämpää käyttää uusien lohkojen luomiseen kuin olemassa olevien lohkojen väärentämiseen. Tämän turvallisuustekijän (51%–hyökkäyksen kannattamattomuus) takia lohkoketjujen sovellutukset ovat lähes rajattomat ja niitä voidaan finanssisektorin lisäksi käyttää muun muassa sähköisessä äänestämisessä, patenttien hallinnassa taikka autenttisuuden varmistavien sertifikaattien hallinnassa. Transparency International uskoo lohkoketjuteknologian jopa eliminoivan korruption vaaleissa tai kohdennettaessa apua, kun kaikki transaktiot ovat nähtävissä ja jäljitettävissä. (Forest & Rose 2015).

Kuva 4: Seuraava lohko sisältää aina edellisen lohkon tiivisteen (hash) (Lähde: Nakamoto 2008)

3.4 Proof of Work

Kuten edellisessä kappaleessa totesimme, kaksinkertaisen menon estämiseksi, jokainen transaktio tulee tarkistaa erikseen, ettei maksaja ole jo käyttänyt transaktioon vaadittuja varoja johonkin toiseen transaktioon. Nakamoton (2008) ratkaisu tähän ongelmaa on se, että meidän tulee tuntea kaikki aiemmat transaktiot. Jotta tämä olisi mahdollista, täytyy transaktioiden olla julkisia. Lohkoketjuteknologian turvallisuuden taustalla on siis se perusajatus, että koko verkko ja siihen liitetyt solmut ovat samaa mieltä tapahtumien oikeellisesta järjestyksestä. Tämä saavutetaan siten, että jokaisesta lohkosta luodaan tiiviste (hash), joka aikaleimataan ja sisällytetään seuraavaan lohkoon. Aikaleima todistaa, että lohkon on pakko olla ollut olemassa leimaamishetkellä, jotta se on ylipäänsä tullut sisällytetyksi tiivisteeseen (ja näin ollen jokainen tiiviste sisältää katekamattoman aikaleimojen ketjun taaksepäin).

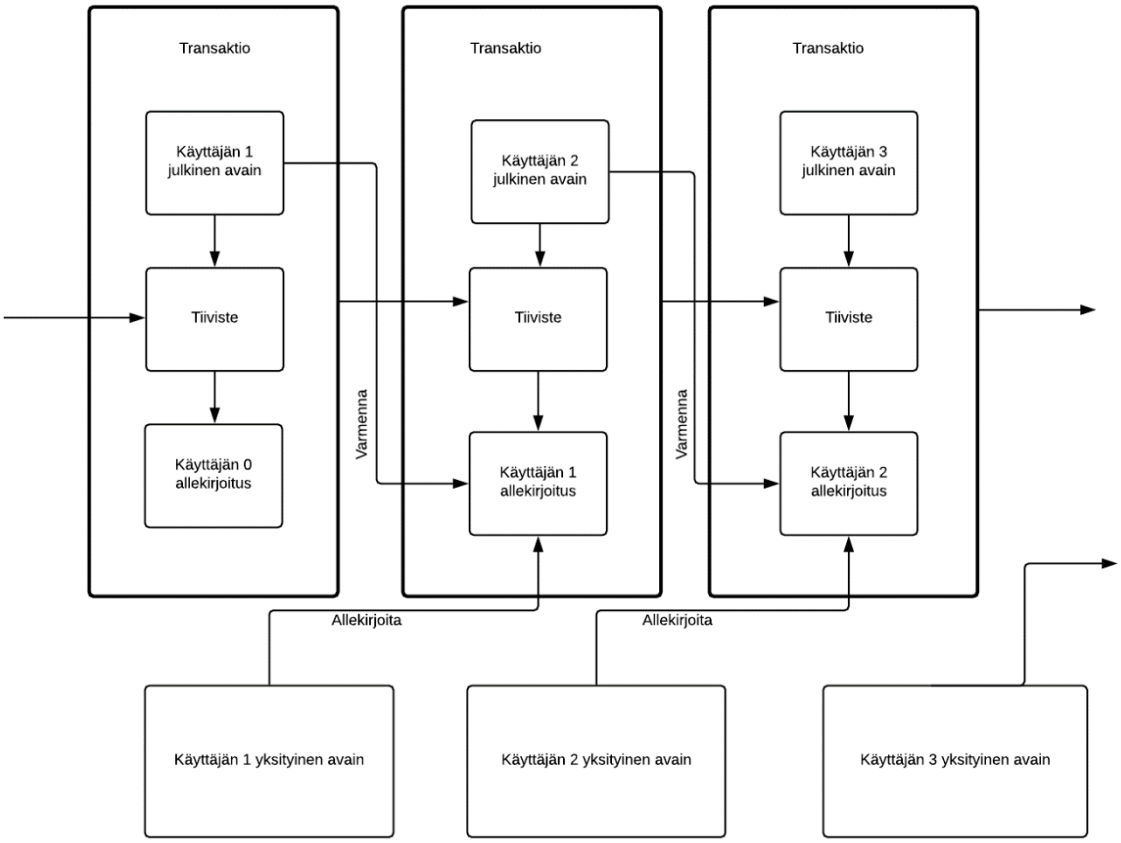
Transaktio varmistetaan louhimalla uusi lohko, johon kerätään uudet ja vielä vahvistamattomat transaktiot liitettäväksi yhtenä lohkona lohkoketjun jatkoksi. Louhinnalla tarkoitetaan prosessorilla suoritettavaa laskentaa, jossa arvataan muiden louhijoiden kanssa kilpaa edellisen lohkon uniikkia satunnaislukua (nonce) ja täten varmennetaan uuden luotavan lohkon aitous (Nakamoto 2008).



Kuva 5: Lohko sisältää aina edellisen lohkon tiivisteen (Lähde: Nakamoto 2008)

Louhinnan vaikeus (Narayanan ym., 2016) määritellään yleensä ”x määrä uusia lohkoja per tunti”-perusteella ja laskentatehon kasvaessa, laskentaa vaikeutetaan, jotta tämä määrä pysyisi vakiona. Uusia lohkoja on tarkoituksella raskas laskea, mutta laskentatuloksia on helppo varmentaa. Tätä kutsutaan Proof of Work –laskennaksi. Proof of Work -laskennan tehokkuuden perustana on juurikin se, että suurin laskentakapasiteetti on aina arvokkainta eli laskentaan käytetty laskentateho itsessään toimii todisteena ketjun rehellisyydestä. Tämä perustuu siihen, että Proof of Work -laskenta on pohjimmiltaan yksi prosessori – yksi ääni (one-CPU-one-vote) -käytöstä. Kun suurin laskentateho on käytetty

pisimpään ketjuun, tämä pisin ketju pitää hallussaan suurinta osaa rehellisiin solmuihin käytetystä laskentatehosta ja täten kasvaa nopeammin kuin muut kilpailevat ketjut (Nakamoto, 2008). Näin ollen, kun rehellisen lohkon luominen ketjuun on haastavaa, mutta sen tarkistaminen helppoa, laskentakapasiteettia ei kannata investoida väärennetyn tiedon luontiin ja järjestelmää vastaan hyökkäämiseen. Lohkoketjun pidetessä ja kilpailevien ketjujen ”kilpailuvoiman” laskiessa, kannattavampaa on juurikin investoida uusien rehellisten lohkojen luomiseen.



Kuva 6: Transaktioiden varmentaminen (Lähde: Nakamoto 2008)

Nakamoto (2008) hahmotteli julkaisussaan myös, kuinka lohkoketjuverkko toimii ja mitkä ovat lohkojen luomisen kuusi vaihetta:

1. Transaktioista sopiminen
2. Transaktiosanoman luominen
3. Transaktiosanoman allekirjoittaminen

4. Transaktiosanoman lähettäminen
5. Transaktion varmistaminen (louhinta)
6. Transaktion toteutuminen

Prosessissa saattaa syntyä päällekkäisiä samanaikaisia lohkoja, joiden ristiriidan Nakamoto ratkaisi edellä esitetyllä Proof of Work -menetelmällä. Lohkoketju luottaa aina pisimpään ketjuun ja täten verkko valitsee ne solmukohdat, jotka tuottavat pisimmän ketjun. Englannin keskuspankin julkaisussa (Barrdear, 2014) nämä ongelmat on selitetty laajemmin Nakamoton listan pohjalta:

1. *Transaktioista sopiminen.* Kahden toimijan välisestä transaktiosta sovittaessa sovitaan itse tuotteen / palvelun kauppahinnan lisäksi yleensä transaktiokorvauksen maksamisesta. Transaktiokorvaus ei ole pakollinen, mutta koska louhijat voivat päättää, mitä transaktioita he varmistavat, niin mitä suurempi transaktiokorvaus, sitä suurempi kannustin muilla louhijoilla on kyseisen kaupan varmistamiseen.

2. *Transaktiosanoman luominen*. Transaktiosanomaa luotaessa lohko ilmoittaa sisääntulona (input) henkilön omistaman varallisuuden ja ulostulona (output) maksetun suoritteen, mahdollisen transaktiokorvauksen sekä transaktion ”vaihtorahat” eli kirjanpidollisen kreditin. Näin ollen input ja output-puolet ovat tilikirjamaisesti tasan. Nämä tiedot ovat kenen tahansa julkisesti saatavissa.

3. *Transaktiosanoman allekirjoittaminen*. Transaktiosanoman allekirjoittamisessa maksaja digitaalisesti allekirjoittaa edellisessä vaiheessa luodun transaktiosanoman oikeudellisuuden. Tämä allekirjoitus koostuu digitaalisesta julkisesta crypto(salaus)-avaimesta sekä maksajan omasta henkilökohtaisesta yksityisestä crypto-avaimesta. Näiden avaimien avulla transaktion oikeellisuuden tarkistamisen tehtäväkseen ottava louhija voi varmentaa transaktion.

4. *Transaktiosanoman lähettäminen.* Allekirjoitettu transaktiosanoma lähetetään vertaisverkkoon varmennettavaksi. Viestiä ei kuitenkaan lähetetä kaikille vertaisverkon louhijoille samanaikaisesti, vaan satunnaisesti valituille osajoukoille.

5. *Transaktion varmistaminen (louhinta).* Transaktio varmennetaan louhimalla uusi lohko muiden uusien ja vielä varmentamattomien transaktioiden

kanssa ja lisätään lohkoketjun jatkoksi aiemmin kuvatun Proof of Work -laskennan edellytyksin.

6. *Transaktion toteutuminen.* Transaktion toteutuminen on kyseisen maksuprosessin viimeinen vaihe. Transaktiosanoman luoja maksaa transaktiosanoman varmentaneelle (louhijalle) transaktiokorvauksen sekä kyseinen varmentaja saa mahdollisen palkkion uuden lohkon luomisesta, mikäli kyseinen lohkoketjuteknologia jakaa kannustinpalkkioita louhinnasta. Kaupan toinen osapuoli saa suorittensa sekä nämä päivittyneet ”tilitiedot” lähetetään taas eteenpäin seuraavaan lohkoon varmennettavaksi (kohta 5).

Kuten huomaamme, transaktiot eivät ole täysin reaaliaikaisia, vaan varmentuvat lohkojen luomisvauhdin mukaisesti. Lohkojen luomisvauhti ja loh-kon laskentaan perustuvan turvallisuuden voidaankin sanoa olevan kääntäen verrannollisia. Mikäli lohkojen varmentamista (transaktioita) halutaan nopeuttaa, joudutaan joustamaan Proof of Work -laskennan vaikeudesta.

Myös toinen turvallisuuteen liittyvä huomio on yksityisyys. Koska lohkot ovat julkisia ja jokainen transaktio kuulutetaan verkkoon louhittavaksi ja varmennettavaksi, on jokainen transaktio kenen tahansa nähtävissä. Catalin & Gans (2016) huomauttavatkin, että täydellisen yksityisyyden sijaan transaktiot ovatkin pseudonyymejä. Jokainen transaktio on vain merkkijono, joten merkkijonon takana oleva henkilö on tunnettava, jotta hänen transaktionsa olisivat yhdistettävissä juuri kyseiseen henkilöön. Henkilöä ei kuitenkaan voida jäljittää ilman tätä tietoa. Lisäksi henkilö voi luoda itselleen uuden tunnuksen (merkkijonon) jokaista transaktiota varten.

Hayes (2015) ja de Vries (2018) taas ovat ottaneet kantaa lohkoketjuteknologian sähkönkulutukseen tarkastelemalla Bitcoin-verkon kuluttamaa sähköä.[6] Pelkästään Bitcoinin sähkönkulutus vastaa jo nyt tällä hetkellä joidenkin valtioiden kulutusta ja on jatkuvassa kasvussa. Tämänhetkinen Proof of Work -tapa varmentaa transaktioita on hidas, eikä millään tavalla kustannustehokas. Tältä osin Proof of Work –varmentamista on vaikea nähdä tulevaisuuden yleiskäyttöisen teknologian teknisenä ratkaisuna.

3.5 Proof of Stake

Toisin kuin Proof of Work, Proof of Stake ei käytä lohkoketjun laskentatehoa lohkoketjun oikeellisuuden määritteenä (ns. 51%:n hyökkäys), eikä näin ollen tuhlaa fyysisiä niukkoja resursseja, vaan sen idea perustuu mekanismiin, jossa

[6] Kts. tämän työn liite 2.

päätöksentekovoima annetaan niille, joilla on lohkoketjussa sillä hetkellä kolikoita (coins) (Bentov ym. 2016). Proof of Stake:n kantavana ajatuksena on se ideologia, että ne, joilla on oma osuutensa lohkoketjussa, ovat myös sopivia huolehtimaan systeemin turvallisuudesta, sillä heidän panoksensa arvo alenee, jos systeemin turvallisuus rapistuu (Bentov ym. 2016).

Bentov ym. (2016) puhuvatkin tutkimuksessaan puhtaasta (pure) Proof of Stake:sta erotuksena variantteihin, joissa on myös Proof of Work -elementtejä mukana. Siinä missä Proof of Work:sta tulee epäluotettava jonkun saavuttaessa 51% osuuden lohkoketjun laskentavoimasta, on Proof of Stake epäluotettava silloin, kun tarpeeksi lohkoketjun osakkaita päättää juonitella systeemiä vastaan. Koko lohkoketju menettää olemassaolonsa merkityksen silloin, kun enemmistö osakkaista päättää hyökätä sitä vastaan. Bentov ym. tunnistavatkin puhtaassa Proof of Stake -protokollassa kaksi ongelmaa: se antaa lohkoketjun ensimmäisille osakkaille suhteettoman suuren vaikutusvallan systeemiin (kolikoiden suhteellinen osuus suuri) sekä kaksinkertaisen kulutuksen lahjus; silloin, kun osakkaalla ei ole insentiiviä puolustaa lohkoketjun oikeellisuutta, lahjusten maksamisen kustannus ketjun väärentämisestä alenee.

Edellä mainitusta johtuen puhdas Proof of Stake -protokolla ei ole hajautetuissa lohkoketjuissa täysin turvallinen, vaan tarvitsee niukkojen fyysisten resurssien alenemisen komponentin pitämään totuuden tiukasti dominoivana strategiana, jota lohkoketjun osakkaiden kannattaa aina pelata. Bentov ym. (2016) tarjoavatkin tutkimuksessaan uudenlaista ratkaisua ongelmaan, jossa käytetään Proof of Stake -protokollaa, mutta niukkoja fyysisiä resursseja ei tarvitse käyttää systeemin varmentamiseen. He väittävät kehittämänsä protokollan tarjoavan parempaa turvallisuutta kuin mikään olemassa olevista protokollista. Väite jää kuitenkin tämän työn osalta vain maininnaksi, sillä tutkimuskysymyksen kannalta ei ole oleellista tarkastella eri protokollien paremmuutta. Seuraavissa luvuissa tarkastellaan tutkimusongelmaa sen oletuksen pohjalta, että systeemin insentiivit toimivat siten, että rehellinen toiminta on lohkoketjussa aina tiukasti dominoiva strategia.

3.6 Ethereum: lohkoketju 2.0

Ethereum on lohkoketjusovellusalusta (blockhain app platform). Sitä kutsutaan arkikielessä lohkoketju 2.0:ksi, sillä se on hajautettu sovellusalusta, joka toimii lohkoketjuteknologialla ja jolle kuka tahansa voi kehittää omia sovellutuksiaan. Siinä missä Bitcoinin taustalla ollut lohkoketjuteknologia oli puhtaasti kehitetty transaktioiden varmentamiseen, on Ethereum suunniteltu joustavaksi muutoksille ja jatkokehittelylle. Siinä voi olla edellä esitetyn kaltaisesti solmukohtia (nodes), joissa voidaan suorittaa käyttäjän omaa koodia tai ohjelmia. Nämä solmukohtien sovellukset ovat aina saatavilla, sillä sovellukset eivät ole riippuvaisia mistään tietystä serveristä, vaan ovat jakautuneet koko lohkoketjuun. Tämä tuottaa luotettavia ja aina ajan tasalla sekä saatavissa olevia sovelluksia. Näitä omaa

koodia suorittavia solmukohtia hyödyntävät muun muassa älysopimukset taikka erilaiset rekisterit. (Ethereum.org).

Älysopimukset eivät ole suinkaan ainoita mahdollisuuksia, joita käyttäjät voivat ajaa omissa solmukohdissaan, vaan Ethereumin sivut listaavat myös esimerkiksi hajautetun joukkorahoituksen työkalun ja esineiden internetin (IoT) sovellukset sekä autonomiset organisaatiot. Lisäksi Ethereumilla on oma valuutta Ether, jota voi käyttää transaktioihin eri sovellusten välillä Etherin oman kryptovaluuttalompakkosovelluksen kautta. Ether ei kuitenkaan ole ainoa Ethereumpohjainen kryptovaluutta, vaan niitä on paljon muitakin. Ethereumin voi siis käsittää ohjelmointirajapinnaksi. Myöskin kolmannen sukupolven lohkoketjuja kehitetäänkin jo kovaa vauhtia.

Ethereumin ongelma on sama kuin Bitcoinilla, eli transaktioiden nopeus sekunnissa on heikko ja ne kuluttavat paljon laskentatehoa. Proof of Work -toimintaperusteen ongelma on kuitenkin sama riippumatta siitä, minkä sukupolven lohkoketjusta puhutaan: Jokainen louhija kuluttaa fyysisiä, niukkoja resursseja sähkökulutuksen ja laitteiston kulumisen muodossa saaden vastineeksi kryptografisesti niukkaa resurssia (~krypotvaluutta), jota voi sitten käyttää systeemin sisällä (Bentov ym. 2016). Tämän vuoksi Bentov ym. (2016) kysyvätkin, että voiko hajautettu lohkoketjusysteemi olla turvallinen, jos osapuolet, jotka varmistavat lohkoketjun turvallisuutta laskentatehollaan, eivät kulutakkaan loppuun niukkoja fyysisiä resursseja (eli heidän suhteellinen laskentavoimansa koko lohkon laskentatehoon kasvaa)?

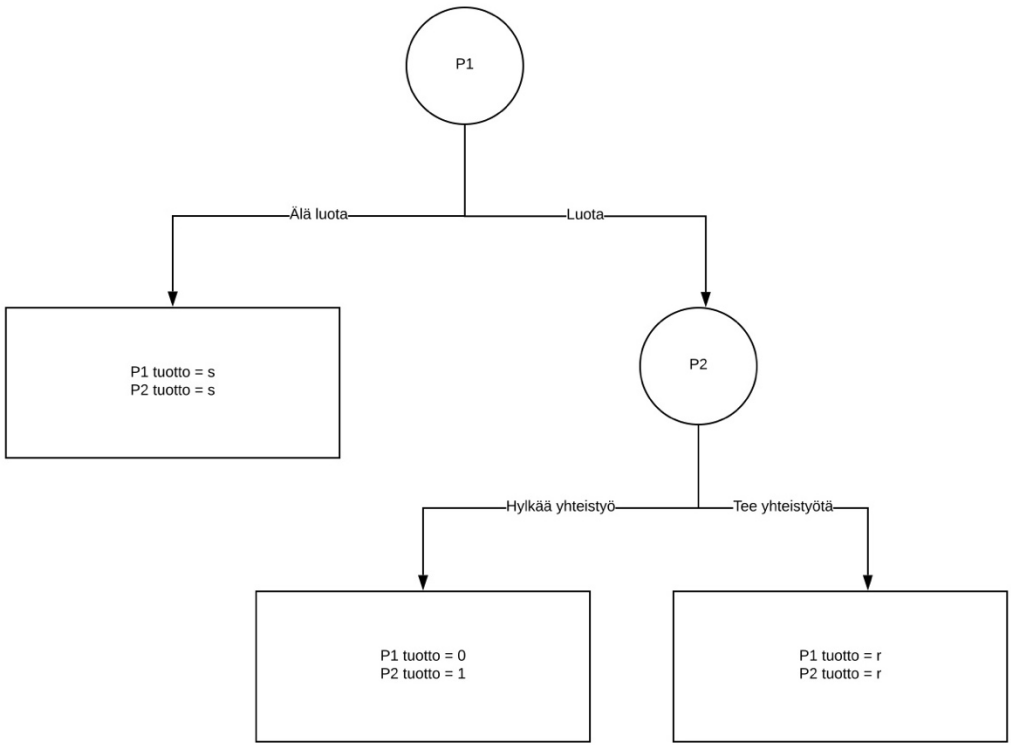
Proof of Work -varmennuksesta puhuttaessa, on vielä hyvä tehdä huomio tulevaisuuden kvanttitietokoneista. Niiden laskentateho ja tapa laskea on perinteiseen tietokoneeseen verrattuna huomattavan erilainen ja Proof of Work -tyyppisessä varmentamisessa varsin tehokas, mikä itsessään tuo oman haasteensa tulevaisuuden lohkoketjuteknologioiden kehittämiselle. Laajempi katsaus kvanttitietokoneiden asettamiin haasteisiin ja vaatimuksiin löytyy tämän työn liitteestä 1.

3.7 Luottamuksen merkitys transaktioissa

Lohkoketjuteknologian yksi suurimmista innovaatioista juurikin se, ettei se tarvitse luotettavaa kolmatta osapuolta transaktioiden varmentamiseen, vaan lohkoketjun luotettavuus perustuu edelle esiteltyihin Proof of Work ja Proof of Stake -ratkaisuihin. Koska transaktio määritelmällisesti tarkoittaa kahden henkilön tai muun toimijan välistä taloudellista toimintaa, on luottamus avainasemassa näissä toimissa. Seuraavaksi esitellään yksinkertaisena peliteoreettisena pelipuuna kaksi yhteistyöpeliä (cooperation game), joissa Pelaajat 1 ja 2 (P1 ja P2) käyvät kauppaa keskenään ja tekevät perättäisiä päätöksiä sen perusteella, miten toinen pelaaja on valinnut edellisessä solmukohdassa (node). Tällaista peliteoreettisen pelin muotoa kutsutaan peräkkäisten valintojen peliksi (sequential

game). Peräkkäisten valintojen pelissä olennaista on informaatio siitä, mitä edellinen pelaaja on valinnut ja kummankin pelaajan tuotto (payoffs) muodostuu näistä valinnoista. Luottamusta tarkastellaan kahdesta eri näkökulmasta: onko Pelaajalla 1 mahdollisuutta hankkia informaatiota Pelaajasta 2 ja kannattaako häneen luottaa. Tarkoituksena on havainnollistaa sitä, miten luottamus vaikuttaa pelin lopputulokseen. Pelipuu on kaksivaiheinen, eli siinä on kaksi solmukohtaa, jossa pelaajat tekevät päätöksiä: ensiksi Pelaaja 1 tekee valinnan, luottaako hän Pelaajaan 2 ja tämän jälkeen Pelaaja 2 tekee valinnan siitä, että aikooko hän olla tämän luottamuksen arvoinen ja tehdä yhteistyötä Pelaajan 1 kanssa vaiko pettää tämän luottamus ja hylätä yhteistyö. Alla olevat esimerkit perustuvat McNamara ym. (2009) tutkimukseen.

Pelaajat 1 ja 2 käyvät kauppaa keskenään. Aivan ensimmäiseksi Pelaaja 1 päättää, luottaako hän Pelaajaan 2. Jos Pelaaja 1 päättää, ettei hän luota Pelaajaan 2, peli päättyy ja kummatkin saavat pelin seurauksena tuoton *s*. Jos taas Pelaaja 1 päättää luottaa Pelaajaan 2, peli siirtyy seuraavaan vaiheeseen, jossa Pelaaja 2 päättää, tekeekö hän yhteistyötä Pelaajan 1 kanssa. Jos Pelaaja 2 tekee yhteistyötä, kumpikin pelaaja saa tuoton r. Jos taas Pelaaja 2 ei tee yhteistyötä, Pelaaja 2 saa tuoton 1 ja Pelaaja 1 ei saa mitään. Tuottojen arvojärjestys on $0 < s < r < 1$. Mikäli pelaajat eivät tunne toisiaan, eikä Pelaajalla 1 ole mitään informaatiota Pelaajasta 2, luottamustilanteessa Pelaajan 2 kannattaa aina hylätä yhteistyö saadakseen tuoton 1. Tämän vuoksi Pelaajan 1 paras strategia em. tilanteessa on aina olla luottamatta Pelaajaan 2, jolloin kummatkin saavat pelistä tuoton s. Jos he olisivat luottaneet toisiinsa, kumpikin olisi saanut pelistä korkeamman tuoton r.

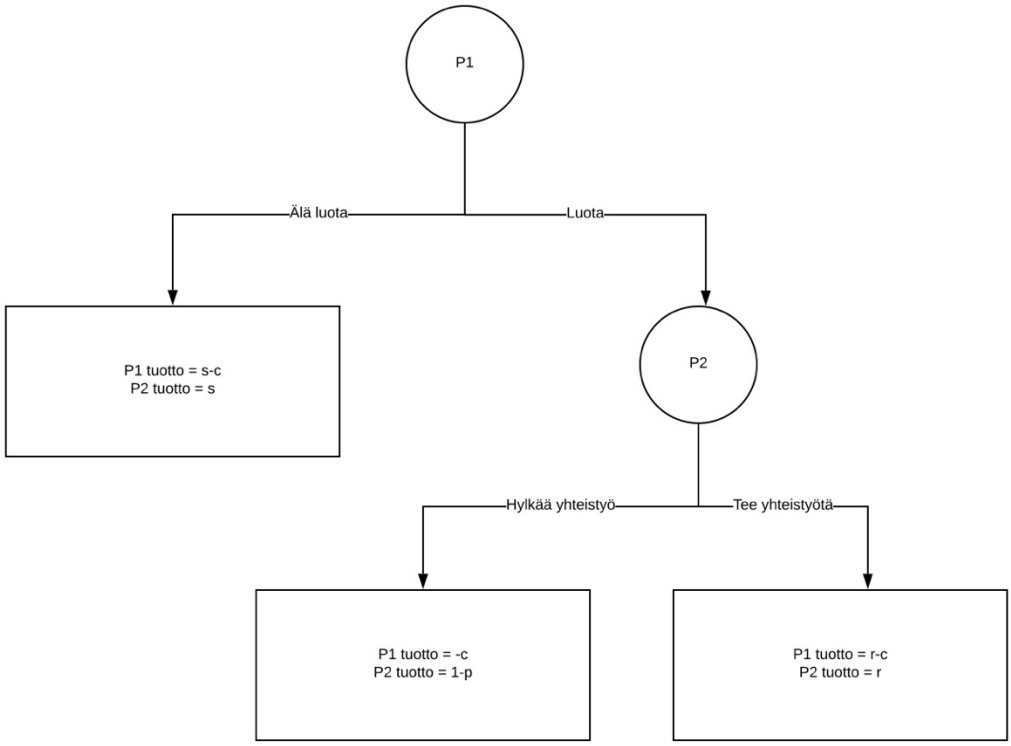


Kuva 7: Yksinkertainen valintapuu ja cooperation game (Lähde: McNamara ym. 2009)

Kun otamme peliin mukaan luottamuksen vaikutuksen ja sen kustannuksen (joka on lohkoketjuteknologian peruspilareista), niin Pelaajan 2 aiempi strategia aina hylätä yhteistyö Pelaajan 1 luottaessa häneen todennäköisesti muuttuu siten, että Pelaajan 2 kannattaakin tehdä yhteistyötä. Tämä johtuu siitä, että luottamuksen pettämisen kustannus on todennäköisesti niin korkea, että se itsessään on jo insentiivi tehdä yhteistyötä. Perinteisessä mielessä kustannuksen takana voi olla esimerkiksi kolmannen osapuolen rangaistus Pelaajaa 2 kohtaan. Lohkoketjuteknologiassa tämä insentiivi tulee sitä kautta, että vain rehellinen toiminta on taloudellisesti kannattavaa lohkoketjussa johtuen teknologian ominaispiirteistä. Näitä ominaispiirteitä on jo käyty tässä luvussa läpi ja tulevissa luvuissa tullaan käymään läpi mm. älysopimuksia ja niiden vaikutusta transaktiokustannuksiin.

McNamara ym. (2009) laajentavat yllä esitettyä pelipuuta (kuva 7) vielä ottamalla mukaan henkilöiden alitajuisen tendenssi tehdä yhteistyötä. Tämä he merkitsevät todennäköisyydellä p ($0 \leq p \leq 1$). Lisäksi todellisuudessa Pelaaja 1 yrittää saada Pelaajasta 2 informaatiota ennen kuin hän tekee päätöksen, luottaako hän tähän. Tämän informaation hankinnan kustannus on c ($0 \leq c \leq s$).

Kun otetaan huomioon nämä parametrilisäykset, saadaan yhteistyöpelistä ja pelipuusta alla olevan näköinen:



Kuva 8: Cooperation game informaatiokustannuksilla

Kuva on voimakas yksinkertaistus McNamara ym. (2009) tutkimuksessa käytetyistä parametreista, jossa huomioon otetaan henkilöiden psykologiset ominaisuudet, tendenssit alitajuisiin ja tiedostettuihin päätöksiin sekä näiden tendenssien tuottamat tuotto-odotukset. Kuitenkin lohkoketjuteknologian kannalta mielenkiintoisin parametri on informaation hankinnan kustannusparametri c. Tämä kustannusparametri kohdistuu pelissämme vain Pelaajaan 1 ja on seurausta informaation hankinnasta, jota Pelaaja tarvitsee luottamuspäätöksentekonsa muodostamiseen. Pelaajan 2 saamaan tuottoon informaation hankintakustannus c ei vaikuta missään pelin lopputulemassa. Mutta toisaalta Pelaaja 2 ei tee pelissämme päätöstä luottamuksen perusteella, vaan hän ottaa tilanteen annettuna Pelaajan 1 päätöksestä pelipuun aiemmassa solmukohdassa.

Pelaamamme pelin ja kuvan 8 perusteella Pelaajan 1 pelin mahdolliset lopputulemat ovat s-c, -c, r-c. Näiden yhteinen nimittävä tekijä on se, että Pelaaja 1 maksimoi joka tilanteessa tuottonsa (tai minimoi tappionsa) minimoimalla kustannuksen c. Seuraavassa luvussa 4 käymme läpi tarkemmin lohkoketjuteknologian transaktioita alentavaa vaikutusta, mutta voimme tässä vaiheessa jo todeta,

että luottamus maksaa ja lohkoketjuteknologia alentaa luottamukseen hintaa ja näin ollen alentaa transaktioiden kustannuksia.

3.8 Taloudelliset ulottuvuudet

Kuten jo edellä on mainittu, Catalin & Gans (2016) nostavat lohkoketjuteknologian suurimmaksi eduksi sen mahdollistaman kustannuksettoman varmentamisen sekä alentuneet verkostoitumiskustannukset. Kuitenkin tähän mennessä olemme käsitelleet vain tapauksia, joissa lohkoketju on hajautettu vertaisverkkoon eli alustana toimii internet ja verkon osapuolet louhivat (varmentavat) lohkoja kannustimia vastaan. Vaikka Nakamoto suunnittelikin lohkoketjuteknologian täysin avoimeksi, ei se ole välttämättä ideaali ratkaisu esimerkiksi yrityksiin, joissa ei ole tarvetta vahvalle proof-of-work -laskennalle ja sen tuomille rasitteille. Esimerkiksi luottokorttiyhtiö Visa pystyy käsittelemään yli 56 000 transaktiota sekunnissa (Visa, 2017), kun taas Bitcoin pystyy tällä hetkellä seitsemään transaktioon sekunnissa (Bitcoin Wiki, 2017).

Yksityinen, lupaa vaativa, lohkoketju muistuttaa hyvin paljon yritysten nykyisiä verkkoratkaisuja, mutta tarjoaa silti kustannuksettoman varmentamisen edut. Kun lohkoketju on yksityinen, ei lohkojen varmentamiseen eli louhimiseen tarvitse käyttää aikaa. Verkon käyttäjät ovat luotettuja. Tietysti hajautetun tilikirjan ja lohkojen luotettavuus on vain yhtä luotettava kuin yksityisen verkon tietoturva, joten alentuneita verkkokustannuksia tällä ratkaisulla ei välttämättä saavuteta. Tämän lisäksi lohkot ovat muokattavissa jälkikäteen, mutta tämä ei välttämättä ole huono asia. Siinä, missä Nakamoton näkemys lohkoketjuista on ehdoton ja aiheuttaa ongelmia esimerkiksi rahanpesulain tai asiakkaan tuntemisvaatimuksen kanssa, voidaan yksityisen lohkoketjun lohkoja muokata jälkikäteen lohkon käyttöoikeuksien haltijan toimesta. Paljon sääntelyä sisältävillä aloilla tämä helpottaa lohkoketjuteknologian käyttöönottoa. Lisäksi yksityisistä lohkoketjuista voi olla hyötyä aloilla, missä välikäsi on saavuttanut poikkeuksellisen suuren markkinavoiman transaktioissa. Tällöin pelkkä varmentamiskustannusten alentaminen hyödyttää osapuolia. Catalin & Gans (2016)

Kolmantena vaihtoehtona ovat puolijulkiset lohkoketjut. Nämä ovat yksityisiä lohkoketjuja, jotka on liitetty julkisiin lohkoketjuihin salauksen avulla. Tällöin lohkoketju toimii aikaleimasimena, koska lohkon peukalointi korruptoi lohkon ja katkaisee linkin yksityisen ja julkisen lohkoketjun välillä. Tällaiset puolijulkiset lohkoketjut ovat tällä hetkellä kiinnostuksen kohteena juurikin sen takia, että ne tarjoavat suhteellisen hyvää turvallisuutta säilyttäen kuitenkin lohkoketjun yksityisen osan hallinnan sen omistajalla. Tällöin lohkoketjun yksityisen osan omistaja voi suorittaa koodia, joka on tarkoitettu vain yksityisverkon osapuolten käyttöön, mutta esimerkiksi lopputulos tallennetaan osaksi julkista lohkoketjua. Catalin & Gans (2016)

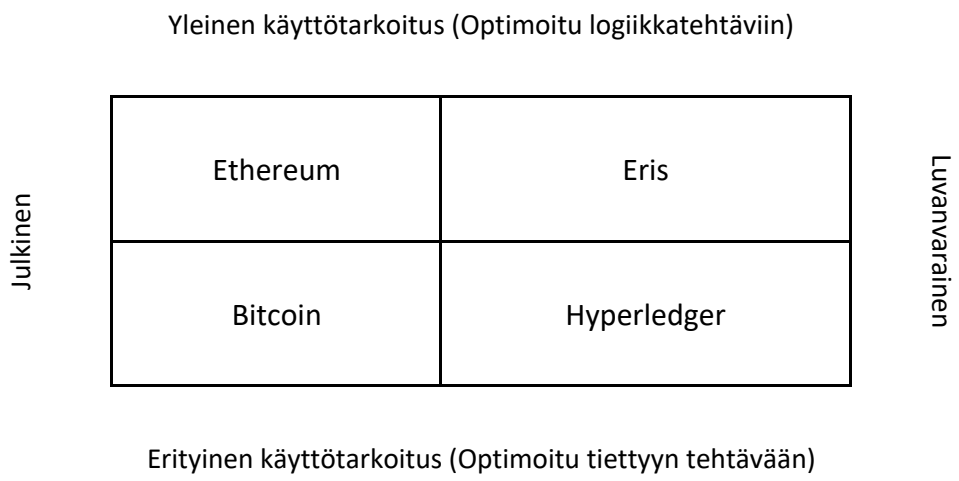
Mattila (2016) taas esittelee alla olevan kuvan mukaisesti, että lohkoketjuteknologia tarjoaa erilaisia hyötyjä siitä riippuen, että onko se kaikille julkinen vai onko sen käyttöä rajattu tietyn ryhmän sisälle. Kuten jo aiemmin todettu, täysin avoin lohkoketju tarjoaa erittäin tehokkaan suojan hakkerointia vastaan (ns. 51% hyökkäys) ja Nakamoton alkuperäisen idean mukaista luotettavuutta (läpinäkyvyyttä), mutta se on vaihtokauppa nopeuden, tehokkuuden ja skaalautuvuuden välillä. Kumpikaan ei ole toistansa parempi vaihtoehto, mutta ne ovat tarkoitettu eri tarkoituksiin. Yrityksen, joka tuntee (ja luottaa) kaikki verkon muut osapuolet, ei kannata käyttää omaa energiaansa ja resurssejansa transaktioiden ja niiden oikeellisuuden varmentamiseen, vaan käyttää resurssejansa mieluummin verkossa tapahtuvaan kaupankäyntiin ja muihin verkon spesifeihin tehtäviin. Julkisessa verkossa taas digitaalisen luottamuksen edellytys on kaikki kaikessa, jolloin verkon hitaampi toiminta on perusteltua transaktioiden oikeellisuuden varmistamiseksi. Kuitenkin verkon hitaus on muodostunut yhdeksi ongelmaksi julkisten lohkoketjujen yleistymiselle.

	LUVANVARAINEN	**JULKINEN**
NOPEUS	Nopea	Hidas
ENERGIATEHOKAS	Energiatehokkaampi	Energiasyöppö
SKAALAUTUVUUS	Helppo skaalata	Ennalta määritelty
SENSUROINTI-RESISTENTTI	Helppo sensuroida	Tieto kaikkien saatavilla, vaikea sensuroida
PEUKALOINTI-VARMA	Ei ole, jos vapaa pääsy muokata tiedostoja	Kyllä, Proof of Work

Taulukko 2: Luvanvaraisen ja julkisen lohkoketjun ominaisuudet (Lähde: Mattila, 2016)

Yllä esitellään taulukko, jonka mukaan lohkoketjuteknologia voidaan jakaa luvanvaraisiin ja pääsy-/käyttölupaa (permission) tarvitsemattomiin eli julkisiin lohkoketjuratkaisuihin. Siinä missä luvanvaraiset lohkoketjut ovat suljettuja, mutta nopeita ja tehokkaita, ovat taas pääsylupaa tarvitsemattomat eli julkiset lohkoketjut avoimia, mutta turvallisempia ja hitaampia. Tämän lisäksi lohkoketjut voidaan jakaa sen mukaan, ovatko ne suunniteltu tiettyihin erikoistehtäviin vai yleisiin loogisiin tehtäviin. Alkuperäinen Bitcoin ja sen taustalla ollut lohkoketju oli tarkoitettu juurikin näihin loogisiin matemaattisiin tehtäviin, kun taas esimerkiksi Ethereum, parannettu ”lohkoketjuteknologia 2.0”, voi sisällyttää lohkoketjuratkaisun eli alustan päällä ajettavaa koodia, jolla voidaan sitten suorittaa lohkoketjussa paikallisia prosesseja, kuten älysopimuksiin perustuvia transaktioita. Näin ollen Ethreum ja sen variaatiot ovat suunniteltu käytettävissä

erilaisissa etukäteen määritellyissä erityistehtävissä (Mattila, 2016). Alla olevassa nelikentässä esitetään vielä eri lohkoketjuteknologioiden jako julkinen – luvanvarainen sekä yleinen – erityinen käyttötarkoitus -akseleilla.



Taulukko 3: Esimerkkejä erilaisista lohkoketjuarkkitehtuureista (Lähde: Mattila, 2016)

3.9 Tietojen pysyvyyden varjopuoli

Lohkoketjuteknologian yksi suurimmista ongelmista on sama kuin sen suurin etu, nimittäin turvallisuus ja sormeiluvapaa (tamper proof) lohkoketju. Interpol kiinnitti jo vuonna 2015 huomiota siihen, että lohkoketjuja käytettiin haittaohjelmien (malwares) ja laittoman materiaalin levittämiseen juurikin siitä syystä, että kun lohko on varmennettu ja lisätty ketjun jatkoksi, on sitä jälkikäteen mahdotonta muokata. Näin ollen haittaohjelmien ja muun rikollisen materiaalin poistaminen oli käytännössä mahdotonta tuhoamatta itse lohkoketjua.

Roman ym. (2018) suorittivat tutkimuksessaan kvantitatiivisen analyysin Bitcoinin satunnaisen lohkoketjun sisällöstä. Heidän havainnoissaan yli 99% lohkoketjun sisällöstä oli teksti- ja kuvatiedostoja. Vaikka Bitcoin-lohkoketju on tarkoitettu transaktioiden varmentamiseen, on siihen teknisesti mahdollista lisätä muutakin sisältöä. Tutkimuksessa läpikäydystä lohkoketjun sisällöstä 1,4%:a oli sisältöä, jolla ei ollut tekemistä transaktioiden varmentamisen kanssa. Vaikka suurin osa tästä satunnaisesta sisällöstä oli harmitonta, mahtui mukaan myös laitonta materiaalia. Koska lohkoketjuteknologiassa data on hajautettu verkkoon, eli lohkoketjun käyttäjien koneille, tarkoittaa tämä monen maan lainsäädännön

mukaan sitä, että lohkoketjun laillisetkin käyttäjät saattavat syyllistyä rikokseen ja itseasiassa koko lohkoketju on laiton. Ja koska lohkoketjuteknologian ideana on juurikin tietojen jälkikäteisen peukaloinnin mahdottomuus, ei näitä laittomia tiedostoja pystytä poistamaan jälkikäteen lohkoketjusta. Tämä saattaa olla este lohkoketjujen laajemmalle yleistymiselle kokonaisvaltaisesti taloudessa ja yhteiskunnassa. Tässä ei riitä, että yhden maan lainsäädäntö huomioi lohkoketjun erikoispiirteet, vaan hajautetun rakenteensa vuoksi lohkoketju on todennäköisesti useamman maan vaikutuspiirissä ja eri maiden lainsäädännöt vaihtelevat pahimmillaan huomattavasti. Joissain maissa pelkästään se, ettei viranomainen pysty jälkikäteen puuttumaan lohkoketjun kautta leviävään tietoon, on este lohkoketjun laajemmalle leviämiselle. Mikäli lohkoketjuun taas tehtäisiin tekninen takaportti muuttaa tietoja jälkikäteen, häviää siinä vastavuoroisesti pahimmassa tapauksessa se ominaisuus, mikä tekee lohkoketjusta yleiskäyttöisen teknologian: prosessi, joka kasvattaa kokonaistuottavuutta alentamalla transaktion kustannuksia.

Laittoman materiaalin lisäksi tietojen pysyvyyden varjopuoli liittyy haitalliseen materiaaliin, kuten viruksiin. Interpol julkaisi jo vuonna 2015 huomion, että lohkoketjuihin sisällytetty virus jää lohkoketjuteknologiassa aiheuttamaan haittaa ikuisiksi ajoiksi, sillä lohkoketjua ei voi muokata jälkikäteen. Toistaiseksi näitä tapauksia ei pahemmin ole ollut, mutta lohkoketjujen yleistymisen myötä saatamme nähdä entistä enemmän tapauksia, jossa haittaohjelmat ottavat niskalenkin. Interpol paikansi ongelman teknisesti avoimiin lohkoketjuratkaisuihin, joihin kuka tahansa voi lisätä tietoa eli lohkoketjun julkiseen solmuun (node). Kun haittaohjelma tai rikollinen materiaali lisättiin, ja mikäli lohko louhittiin, päätyi se lopulta ikuisiksi ajoiksi osaksi lohkoketjua. Tämä avaa aivan uudenlaiset rikolliset markkinat. Nimittäin haittaohjelma voi sisältää pääsyn johonkin arkaluonteiseen tietoon ja pimeillä markkinoilla myydään sitten avaimia näiden haittaohjelmien käyttämiseen. Siinä missä Bitcoinia on syytetty pimeiden markkinoiden valuutaksi, se ei kuitenkaan ole itse rikollisuuden mahdollistaja samassa kontekstissa kuin saastunut lohkoketju. Bitcoin voidaan aina vaihtaa johonkin muuhun maksuvälineeseen, mutta pitkää ja paljon tärkeää informaatiota sisältävää saastunutta lohkoketjua ei voi vaihtaa (kustannustehokkaasti) toiseen.

4 ONKO LOHKOKETJUTEKNOLOGIA UUSI YLEISKÄYTTÖINEN TEKNOLOGIA?

4.1 Yleisesti

Tässä luvussa tarkastellaan, täyttääkö lohkoketjuteknologia edellä kuvattuja tutkimuskirjallisuudessa määriteltyjä ehtoja, joita teknologian tulee täyttää, jotta sitä voidaan luonnehtia yleiskäyttöiseksi teknologiaksi. Vertailun perustana on aiemmin luvussa kaksi esitetyt yleiskäyttöisen teknologian kolme tunnuspiirrettä. Tässä luvussa pyritään löytämään näitä ominaisuuksia lohkoketjuteknologiasta käyttäen apuna Mattilan (2016) esittelemiä esimerkkisovellutuksia

Lohkoketjuteknologian suurimpia etuja on käyttötarkoituksesta riippumatta transaktioiden kustannukseton varmentaminen ja verkkokustannusten laskeminen (Catalini & Gans 2016). Lohkoketjuteknologian ansioista ei ole enää tarvetta kalliille kolmansille osapuolille transaktioiden varmentajana. Ja myös lohkojen "sijoittaminen" vertaisverkkoon olemassa olevaan internetinfrastruktuuriin poistaa parhaimmillaan tarpeen yksityisille tietokantapalvelimille ja datakeskuksille. Lohkoketjuteknologia uudelleen määrittää termin "digitaalinen luottamus". Siinä missä digitaalinen luottamus on nykyisin pitkälti sen varassa, että osapuolella on hyvä maine, ei maineella ole lohkoketjujen ansiosta mitään merkitystä (Mattila 2016). Jos asia on varmennettu muiden toimesta, riittää vain, että ihmiset ovat keskimäärin luotettavia. Tällöin esimerkiksi osapuolten ei tarvitse enää maksaa kolmannelle osapuolelle siitä, että tämä varmentaa osapuolten luotettavuuden, kuten pankkitunnistautumisessa tehdään.

4.2 Aiempaa kirjallisuutta

Catalini & Gans (2016) ovatkin ensimmäisiä, jotka ovat selvästi tutkimuksessaan ottaneet kantaa lohkoketjuteknologian soveltuvuuteen yleiskäyttöisenä teknologiana. Heidän näkemyksensä on, että lohkoketjuteknologiasta todellakin olisi seuraavaksi yleiskäyttöiseksi teknologiaksi ja se tulee kaikkein todennäköisimmin näkymään siten, että lohkoketjuteknologia muuttaa välittäjien toimintakenttää alentamalla transaktion kustannuksia ja sitä kautta mahdollistamalla uudenlaisten markkinapaikkojen ja -alustojen syntymisen. Catalini & Gans (2016) löysivät tutkimuksessaan lohkoketjuteknologiasta yleiskäyttöisen teknologian ominaisuuksia. Lohkoketjuteknologialla on kaikki yleiskäyttöiseltä vaadittavat luonteenpiirteet eli kokonaisvaltaisuus, kehittyminen ja innovaatioiden syntyminen. Lohkoketjuteknologia ei ole rajoittanut vain palvelemaan Bitcoinia, vaan sitä voidaan hyödyntää laajemminkin esimerkiksi tallentamaan tietoa, jonka pitää olla turvassa tai yksityistä. Catalini & Gans toteavatkin tutkimuksessaan, että kuitenkin, koska kyseessä on yleiskäyttöinen teknologia, yksittäinen yritys ei pysty hyödyntämään kaikkea sen potentiaalia, ali-investointeja saattaa aluksi esiintyä. Bitcoinin leviämistä helpotti louhinnan kannustinjärjestelmä. He myös huomauttavat, että vaikka lohkoketjuteknologia loisikin läikkymisefektiä, antaa se vielä odottaa varsinaista läpimurtokohdettaan esimerkiksi turvallisuuden ja yksityisyyden saralla.

Myöskin Etlan tutkija Juri Mattila on ansioitunut lohkoketjuteknologian tutkija ja hän onkin monelta osin ottanut kantaa lohkoketjuteknologian potentiaaliin käytännön sovellutusten kautta. Mattila ym. (2016) on tutkinut useita lohkoketjuteknologian sovellutuksia ja erityisesti sitä, millä tavalla kyseinen teknologia muuttaa olemassa olevia asioita ja käytäntöjä. Hän käy tutkimuksissaan läpi niin lohkoketjuteknologian perusideologian eli luottamuksen tarpeettomuuden sovellutuksia (mm. varallisuusrekisterit, tietojen hallinta, äänestäminen, älysopimukset) kuin teollisuuden lohkoketjuja esimerkiksi energia-alalla.

Luvussa viisi paneudumme hieman tarkemmin lohkoketjuteknologian mahdollistamiin sovellutuksiin ja erityisesti siihen, millä tavalla ne muuttavat jo tuntemiamme asioita. Mutta ennen sitä on tärkeää ymmärtää, miten laajalle skaalalle elämän eri osa-alueita lohkoketjuteknologia voi tulevaisuudessa mahdollisesti ulottua.

4.3 Lohkoketjuteknologian markkinoita disruptoivat toiminnallisuudet

Kuten luvussa kaksi jo käytiin läpi, yleiskäyttöisen teknologian kolme ominaisvaatimusta ovat teknologian kokonaisvaltaisuus, kehittyminen ja innovaatioiden syntyminen. Alkuun on kuitenkin hyvä tehdä sellainen täsmennys, että tässä luvussa lohkoketjuteknologialla tarkoitetaan laajasti kaikkea

lohkoketjuteknologiaa ja sen arkkitehtuureja, eikä esitystä rajata koskemaan vain alkuperäistä Bitcoinin taustalla olevaa transaktioiden varmentamista.

Voimme sanoa elävämme informaatioyhteiskunnassa, jossa internet tarjoaa jatkuvaa informaatiovirtaa vuorokauden ympäri. Kuluttajat ovat valveutuneempia kuin koskaan aiemmin. Kuitenkin lohkoketjuteknologia lisää datan ja sitä kautta informaation saatavuutta radikaalisti. Siinä, missä jokainen toimija pitää tällä hetkellä yllä omaa tietokantaansa ja toimijan vastuulla on tietokannan oikeellisuus ja ajantasaisuus, lohkoketjuteknologian avulla kyseinen tietokanta kattaisi koko toimijaketjun, esimerkiksi tuotantoketjun. Näin ollen esimerkiksi tuotantoketjussa olisi koko ajan ajantasainen tieto siitä, että onko kylmätuotteen kylmäketju ollut katkeamaton taikka miltä tilalta raaka-aineet ovat lähtöisin. Kun kuluttajalle mahdollistetaan pääsy tähän dataan (avoin lohkoketju), voi se parhaassa tapauksessa ohjata niin kuluttajan käyttäytymistä ja sitä kautta koko tuotantoketjun käyttäytymistä esimerkiksi ympäristöystävällisempään suuntaan. Parhaassa tapauksessa kuluttaja pääsee itse päättämään keneltä tuottajalta ostaa hankkimansa lopputuotteen materiaalit. Markkina muuttuu kokonaisvaltaisesti, kun läpinäkyvyys ja informaatio lisääntyvät, ne myös kehittyvät vastaamaan paremmin markkinoiden uutta tilaa ja palvelemaan paremmin kuluttajien muuttuneita preferenssejä. Esimerkissä uusi innovaatio oli maksaa lopputuotteen materiaalit suoraan valitsemalleen tuottajalle.

Markkinoiden mullistuminen lohkoketjuteknologian avulla ei kuitenkaan ole näin yksioikoinen asia, sillä menestyäkseen lohkoketjuteknologia tarvitsee taaksensa isojen toimijoiden ja kehittäjien tuen. Mikään innovaatio ei menesty, vaikka se olisi teknisesti kuinka ylivertainen tahansa, ellei sille löydy kysyntää, siitä kilpailla, sekä tietoaitoa teknologian hyödyntämisestä (Mattila 2016). Toinen tämän hetken trendikkäistä puheenaiheista on esineiden internet, IoT (Internet of Things). Maalaisjärjellä ajateltuna esineiden internet hyötyisi hajautetusta lohkoketjuratkaisusta, jossa kaikkien IoT-laitteiden data sijaitsisi. Kuitenkin valmistajien etu on sitouttaa kuluttaja tämän omaan suljettuun systeemiin, sillä se takaa asiakasuskollisuuden laitteita päivittäessä ja uusia hankittaessa. Tässäkin tapauksessa uuteen teknologiaan ali-investoidaan.

Silloin, kun jokin teknologinen innovaatio muuttaa kokonaisvaltaisesti toimialaa, on tärkeää kiinnittää lainsäädäntöön ja sen vaatimuksiin huomiota. Nykyisen kaltaisessa järjestelmässä data on toimijan hallussa ja lainsäädäntö asettaa vaatimuksia datan käsittelylle niin tietoturvan ja -suojan kuin myös käytettävyyden osalta. Jos esimerkiksi henkilörekisteriin tehdään tietomurto, on lähtökohtaisesti rekisterinpitäjä vastuussa tästä. Hajautetun lohkoketjun tapauksessa ei kuitenkaan ole vastuutahoa. Vaikka itse datan peukalointi onkin lohkoketjuteknologiassa vaikeaa, on tämän hetken ratkaisut kuitenkin avoimuutensa osalta täysin kehittäjien omien ratkaisujen varassa. Entäpä jos täysin automatisoiduissa prosesseissa sattuu virhe? Kuka tästä vastaa, jos sopimuksen kumpikaan osapuoli ei ole ihminen? Näyttääkin siltä, että lainsäätäjä on ensimmäisten joukossa, jotka saavat kokea lohkoketjuteknologian synnyttämän disruption.

4.3.1 Nanomaksut

Ehkäpä eninten markkinoille disruptiota aiheuttava asia tulee kuitenkin lohkoketjujen myötä olemaan nanomaksut. Kun lohkoketjuteknologian myötä tarve (maksulliselle) kolmannelle osapuolelle varmistamaan ja välittämään maksuja poistuu, tulevat nanomaksut kannattaviksi. Nanomaksuilla tarkoitetaan maksuja, joiden suuruus on sentin murto-osa. Nanomaksuilla pystyy ohjamaan markkinoita yllättävän monipuolisesti. Erityisesti kun tarpeeksi moni ohjaa nanomaksuilla muiden käyttäytymistä toivottuun suuntaan, sillä pienistä rahapuroista syntyy lopulta suurempi joki. Esimerkiksi median ansaintamalli voisi nanomaksujen myötä perustua uutisessa vietettyyn aikaan mainosnäyttöjen sijaan, jolloin klikkiotsikoita ei tarvitsisi enää tehtailla ja kaikki voittaisivat. Yhtä lailla hyödyllistä tietoa internetissä jakavia voisi palkita nanomaksuilla. Siinä missä sentin murto-osan palkkion maksamista tuskin huomaa, saattaa vastapuoli useiden maksujen seurauksena saada insentiivin toimia samalla tavalla jatkossakin. Idea toimii myös kannustimena lopettaa haitallinen toiminta. Esimerkiksi jos sähköpostin lähettäminen maksaisi jotain, ei nanomaksu tuntuisi satunnaisia sähköposteja lähettävän lompakossa yhtään missään, mutta päivässä pahimmillaan satoja tuhansia sähköposteja lähettävän roskapostittajan lompakossa nanomaksut alkaisivat jo tuntumaan.

Kuten esimerkeistä kävikin ilmi, olisi nanomaksujen vaikutus ennen kaikkea suurimmillaan ohjaamassa käytöstä johonkin haluttuun suuntaan: yksittäinen kerta ei vielä vaikuta missään, mutta asian toisto alkaa näkyä positiivisessa tai negatiivisessa mielessä. Lisäksi nanomaksut tulevat todennäköisesti yleistymään myös tosiasiallisenkäytön mukaan laskutettavissa palveluissa, joissa samaa tuotetta tai palvelua käyttävän useammat henkilöt, esimerkiksi yhteiskäyttöautot. Nanomaksut kuitenkin voivat levittäytyä kokonaisvaltaisesti eri toimialoille, ne kehittyvät sitä mukaan, kun eri toimijat ottavat lohkoketjuteknologiaa käyttöönsä ja nanomaksujen ansiosta täysin uudet innovaatiot ja palvelut ovat mahdollisia. Nanomaksujen lisäksi voidaan puhua mikromaksuista. Niissä on sama logiikka, mutta kyseessä on kertaluokkaa suuremmat maksut.

4.3.2 Älysopimukset

Älysopimus eli smart contract on yksinkertaistettuna ennalta määritelty ehdollinen koodinpätkä, jossa määritellään, että jos X = Y, niin tapahtuu asia Z. Älysopimukset muokkaavat sopimisen kulttuuria aivan uudella tavalla. Siinä missä tähän asti sopimuksesta tai sopimuksen täytäntöönpanon ongelmista on riidelty viime kädessä oikeudessa juristien avustamana, älysopimuksissa sopimuksen ehdot ovat etukäteen määritelty ja sopimukset toteutuvat automaattisesti ehtojen täytyttyä. Kaikki tekemämme transaktiot ovat juridisessa mielessä sopimuksia, joten vain teknologian adoptoijien mielikuvitus on rajana.

Älysopimukset toimivat lohkoketjun solmukohdissa (nodes) suoritettavana ennalta määrättynä koodina. Ne voivat olla yllä esitetyn kaltaisia yksinkertaisia ehdollisia komentoja tai sitten hyvinkin monimutkaisia suoritusketjuja ehtojen täyttyessä. Sinänsä älysopimukseen ei tarvitse liittyä rahaa tai transaktiota, vaan sopimus saattaa olla lupa tarkastella esimerkiksi jotain tiettyä asiakirjaa. Mutta monimutkaisimmillaan se voi olla esimerkiksi kokonainen huutokauppaalusta.

4.3.3 Hajautetut autonomiset organisaatiot

Hajautetuilla autonomisilla organisaatioilla, decentralized autonomous organisations, DAO, tarkoitetaan lohkoketjuteknologian sovelluksen ja itsestään toteutuvien älysopimusten kombinaatiota (Mattila 2016). Hajautetussa autonomisessa organisaatiossa verkon solmut toimivat itsenäisesti toteuttaen transaktioita systeemien välillä ilman ihmisen ohjausta. Älysopimukset suorittavat itsensä ehtojen täyttyessä ja lohkoketju varmentaa transaktion, kun järjestelmä siirtää rahaa ilman ihmisen hyväksyntää. Tällaisia systeemejä voisivat olla esimerkiksi kauppojen automatisoidut tilausjärjestelmät, jotka osaisivat tilata hupenevaa tavaraa itsenäisesti taikka pankkien yön yli -korkojen talletustoiminnot.

	Ihmiset reunoilla	Automaatio reunoilla
Ihmiset keskiössä	Ihmisorganisaatiot	Robotisoidut systeemit
Automaatio keskiössä	Hajautetut autonomiset organisaatiot (DAO)	Täysin automatisoidut systeemit ja systeemien systeemit

Taulukko 4: Erilaisten automatisoitujen systeemien relaatiot (Lähde: Mattila 2016)

Lohkoketjuteknologian aiheuttamassa disruptiossa pääosaa näyttelee erityisesti itseään toteuttavat älysopimukset ja mikromaksut. Siinä missä ne luonnollisesti ilman ihmisen apua vähentävät transaktiokustannuksia, voivat ne luoda täysin uusia bisnesmalleja niin ihmisen ja koneen kuin koneen ja koneen välisissä sopimuksissa. Parhaassa tapauksessa yksittäiset komponentit tuottavat varallisuutta, jolla ne kustantavat omat huolto- ja kierrätyskustannuksensa.

Lohkoketjuteknologian kehityksen suunta näyttääkin olevan kohti automatisoitua taloutta.

4.3.4 Hajautetut ja ajantasaiset rekisterit

Toimivan kaupankäynnin perusta on se, että osapuolet voivat luottaa siihen, että transaktion kohde on sopimuksen mukainen ja että myyjä omistaa kauppaamansa tuotteen ja ostajalla on varaa ostaa se. Lisäksi transaktiosta tulee jäädä jälki, jotta mahdolliseen seuraavaan transaktioon olisi todiste ostajan omistusoikeudesta transaktion kohteeseen. Tällaisia todisteita ovat muun muassa kiinteistörekisteriote tai ajoneuvorekisteriote. Perinteisessä systeemissä viranomainen pitää yllä tämänkaltaisia rekistereitä. Tällöin nopeissa transaktioketjuissa viive voi olla informaatiokatkoksen aiheuttaja, taikka rekisteritodistus saattaa olla väärennös. Lohkoketjuteknologialla toteutetussa rekisterissä omistajan nimi vaihtuu parhaimmillaan samalla sekunnilla kuin transaktion kauppahinta maksetaan. Tieto on aina ajantasaista ja nopeasti saatavilla.

4.4 Teknologisen kehityksen jaottelu neoklassiseen ja institutionaaliseen muutokseen

Davidson ym. (2016a) esittelevät kaksi tapaa, jolla teknologista kehitystä tapahtuu: neoklassinen lähestymistapa sekä institutionaalinen eli hallintokeskeinen lähestymistapa. He toteavat tutkimuksessaan monimutkaisten (taloudellisten) systeemien kehityskaaren perinteisesti alkavan keskitetystä systeemistä kohti hajautettua systeemiä, sillä keskitetty systeemi on hyötysuhteeltaan paras ratkaisu aloittaa. Keskitetyssä taloudessa kuitenkin hierarkkinen valta johtaa lopulta inflaatioon, korruptioon ja pääomien uudelleenallokoitumiseen. Tällainen talouden kehityskaari johtaa Davidsonin ym. (2016a) mielestä kohti markkinoiden hajautumista ja tämän vuoksi hajautetut teknologiset ratkaisut tulevat olemaan tulevaisuudessa keskitettyjä ratkaisuja tehokkaampia.

Talous mielletään perinteisessä mielessä yksilöiden ja yritysten väliseksi yhteistyöksi. Lohkoketjuteknologian funktio on tässä toimia totuuden paljastajana tai varmennuskoneena (verification engine). Edellä mainittu tarkoittaa sitä, että Davidsonin ym. (2016b) mielestä lohkoketjuteknologia ei ole teknologinen innovaatio (=vaikuttaa tuotantofunktioon), vaan institutionaalinen innovaatio eli se vaikuttaa transaktiokustannuksiin. Erottelu ei ole heidän mukaansa pelkästään taksonomista semanttisuutta, vaan kuvaa sitä tapaa, jolla lohkoketjuteknologia disruptoi markkinoita ja millaisia uusia innovaatioita se mahdollistaa.

Neoklassisen lähestymistavan mukaan teknologinen kehitys alentaa tuotantokustannuksia ja aiheuttaa koordinaatistossa siirtymän oikealle kokonaistuotantofunktiossa. Yritykset siis allokoivat resurssejaan tehokkaammin ja tämän

seurauksena säästävät tuotantokustannuksissa sekä kokonaistuotanto kasvaa. Neoklassinen teknologianäkemys siis perustuu niukkojen resurssien uudelleenallokointiin lohkoketjuteknologian avulla. (Davidson ym. 2016a).

Hallintokeskeinen lähestymistapa luokittelee lohkoketjuteknologian uudeksi institutionaaliseksi teknologiaksi, joka alentaa markkinoiden hyödyntämisen transaktiokustannuksia. Institutionaalisessa lähestymistavassa teknologinen kehitys taas parantaa instituutioiden (esim. markkinat, yritykset ja julkinen valta) tehokkuutta, sillä markkinat muodostuvat tehokkaasta sekoituksesta talouden eri agentteja, jotka yrittävät säästää transaktiokustannuksista. Täten voidaankin todeta, että tuotantokustannuksissa säästäminen johtaa resurssien tehokkaaseen allokaatioon, mutta transaktiokustannuksista säästäminen johtaa talouden organisaatioiden ja hallinnon tehokkaaseen rakenteeseen. (Davidson ym. 2016a).

Davidson ym. (2016a) mukaan markkinat ovat yleensä tehokkaat yksittäisissä puhtaasti markkinaehtoisissa transaktioissa. Mutta silloin, kun markkinat vaativat koordinoituja investointeja aikahorisontti huomioiden, jatkuvan suhteen osapuolten välille taikka epävarmuus on läsnä yhtenä komponenttina, vaihtoehtoiset tavat organisoida taloudellista toimeliaisuutta voivat olla tehokkaampi tapa ehkäistä opportunismin vaaraa eli sitä, että joku yrittää hyväksikäyttää systeemiä. Lohkoketjuteknologian funktiona on juurikin ehkäistä kryptografisin mekanismein opportunismin riskiä mahdollistaen transaktiokustannuksiltaan tehokkaat markkinat aina ja kaikkialla. Mikäli julkinen valta päättää puuttua markkinoihin muusta syystä kuin opportunismin riskiä estääkseen, ei lohkoketjuteknologian vaikutus markkinoiden tehokkuuteen ole niin suuri kuin edellä.

Lohkoketjuteknologialla on markkina-alustalle tyypillisiä piirteitä, mutta se ei ole markkina-alusta kansantalouden näkökulmasta, vaan lohkoketjuteknologia fasilitoi transaktioita. Davidson ym. (2016a) mukaan yksi tapa katsoa lohkoketjuteknologiaa onkin juuri se, että se on uusi yleiskäyttöinen teknologia, joka on juuri varhaisessa vaiheessaan käymässä läpi Shumpeterilaisen prosessin vaiheita innovaation käyttöönotossa ja levittäytymisessä koko talouteen. Muuttuvat suhteelliset tuotantokustannukset kilpailevista teknologisista substituuteista tukevat teknologisen adaptaation prosessia, mistä voidaan juurikin tehdä tulkinta, että lohkoketjuteknologia on varhaisessa disruptoivassa vaiheessa oleva Shumpeterilainen luovan tuhon prosessi. (Davidson ym. 2016a).

4.5 Täyttyvätkö yleiskäyttöisen teknologian tunnusmerkit?

Alla olevassa taulukossa on tarkoitus havainnollistaa muutamin esimerkein eri toimialojen ratkaisuja ja verrata niitä yleiskäyttöiseen teknologiaan ominaispiirteisiin. Taulukko perustuu työn tekemisen aikana syntyneeseen näkemykseen lohkoketjuteknologian sovellettavuudesta eri kohteisiin ja seuraavassa luvussa esitettyihin esimerkkisovellutuksiin. Taulukon jokainen rivi kuvaa omaa

toimialaansa ja sarakkeissa on sovellutusesimerkki, GPT:n ominaispiirteet, sovellutuksen ja disruption aiheuttaminen nykytilanteeseen. Taulukko ei lähtökohtaisestikaan voi olla kovinkaan kattava, vaan tarkoitus on tarkistuslistatyyppisesti arvioida eri toimialoja samoilla kriteereillä. Seuraavassa luvussa taas kiinnitetään enemmän huomiota yksittäisiin mielenkiintoisen sovellutusaloihin.

	Innovaatiot	Kehittyminen	Kokonaisvaltaisuus	Lohkoketjusovellus
Finanssiala	Kyllä. Lohkoketjusovellutuksista on mahdollisuus löytää finanssialaa suurestikin muokkaavia innovaatioita, jotka muokkaavat markkinaa ja tapoja tehdä asioita.	Kyllä. Nykyiset ratkaisut ovat teknisesti vajaita, mutta lohkoketjuteknologialla toimiva sovellus on tunnistettavissa lohkoketjuteknologiaksi.	Kyllä. Finanssialan ratkaisut voitaisiin toteuttaa yhtä lailla lohkoketjuteknologiaa hyväksikäyttäen.	Hajautetut autonomiset organisaatiot. Pankit voivat lainata toisilleen yön yli rahaa ilman, että ihmistoimija on välissä.
Teollisuus	Kyllä. Uudenlaiset teollisuuden palvelut erityisesti prosessitehokkuudessa ovat varsinkin ensivaiheen lohkoketjuinnovaatioita.	Kyllä. Odotettavissa erityisesti tehokkuuden paranemista, mutta lohkoketjuteknologian toimintalogiikka säilyy.	Osittainen. Teollisuusprosesseissa laaja-alainen vaikutus, mutta teknologialla ei vaikutusta itse valmistusmenetelmiin.	Älysopimukset. Tuotantoprosessien tehokkuus paranee, kun esimerkiksi lohkoketju voi huolehtia varastoista automaattisesti (lean-periaate).
Palvelut	Kyllä. Mahdollistaa täysin uudenlaisia palveluita ja prosesseja.	Kyllä. Palvelut kehittyvät ja syntyy täysin uusia palveluita, mutta tekniikka niiden taustalla on tunnistettavissa.	Kyllä. Palvelut, niin uudet kuin vanhat voitaisiin kokonaisvaltaisesti toteuttaa lohkoketjuilla.	Nanomaksut. Palveluista voidaan maksaa kannattavasti käytön mukaan.

Taulukko 5: Lohkoketjusovellusten ominaispiirteitä eri toimialoilla

	Innovaatiot	Kehittyminen	Kokonaisvaltaisuus	Lohkoketjusovellus
Liikenne / liikkuminen	Kyllä. Erityisesti liikenteen tehokkuus ja palveluiden käyttäminen ja maksaminen.	Kyllä. Niin vanhojen palveluiden kuin uusien innovaatioiden kohdalla teknologia taustalla on tunnistettavissa.	Kyllä. Kaikki liikkumisen palvelut voidaan toteuttaa lohkoketjuilla.	Älysopimukset. Palveluiden automatisointi toimimaan älysopimusten pohjalta.
Sosiaali- ja terveysala	Kyllä. Uudenlainen diagnostiikka, joka perustuu lohkoketjujen mahdollistamaan data-analytiikkaan.	Kyllä. Dataa voidaan käyttää täysin uudella tavalla, mutta lohkoketjusovellusten toimintalogiikka pysyy samana.	Kyllä. Datan säilytys, hallinta ja analytiikka voidaan toteuttaa lohkoketjuteknologialla	Hajautetut tietokannat. Dataa yhdistelemällä eri tietokannoista voidaan tuottaa parempaa diagnostiikkaa.
Julkishallinto	Kyllä. Uudenlaiset palvelukonseptit ja viranomaistoiminnan tehostuminen	Kyllä. Viranomaistoiminnan laajamittaisesta kehittymisestä huolimatta teknologia taustalla on tunnistettavissa.	Kyllä. Palvelut, tiedonhallinta ja älysopimukset voidaan toteuttaa lohkoketjuilla.	Hajautetut autonomiset organisaatiot. Julkishallinnon mekaanista toimintaa voidaan automatisoida.

Taulukko 6: Lohkoketjusovellusten ominaispiirteitä eri toimialoilla

Kuten yllä olevasta taulukosta huomaa, niin vaikka lohkoketjuteknologia ei ole prosessi, vaan teknologia, niin sen vaikutusalue on suurimmillaan juuri prosesseissa. Lohkoketjuteknologiassa itsessään ei ole mitään sellaista, mikä automaattisesti parantaisi tuottavuutta tai tehokkuutta. Lohkoketjuteknologian voima on juurikin siinä, että tietoyhteiskuntaa voidaan linkittää yhteen entistä syvällisemmällä tasolla. Yleiskäyttöiselle teknologialle ominainen kokonaistuottavuuden kasvu saavutetaan juurikin prosessitehokkuuden ja data-analytiikan tehokkaamman hyödyntämisen kautta. Tämä tietysti edellyttää sitä, että lohkoketjuteknologian antamat mahdollisuudet, kuten esimerkiksi älysopimukset ja autonomiset hajautetut organisaatiot ovat tuettuina koko prosessin matkalta. Tai että dataan päästään käsiksi niin laajasti, että siitä voidaan tehdä esimerkiksi lääketieteessä tehdä data-analyysin perusteella ennusteita. Mikäli henkilö esimerkiksi estää oman datansa käytön, voi se vaikuttaa analytiikan tehokkuuteen tai luotettavuuteen myös yleisemmällä tasolla.

Syvempi linkittyminen tietoyhteiskuntaan on myös lohkoketjuteknologian yleistymisen suurin este. Jotta lohkoketjuteknologialla voitaisiin saavuttaa laaja-alainen, toimialoja ylittävä kattavuus ja sen tuoma tehokkuus, tarvitsee lohkoketjuteknologian olla tuettuina kaikilla prosessin osa-alueilla. Julkishyödykkeitä lukuun ottamatta investointipäätöstä uuteen teknologiaan ohjaa ainoastaan odotettavissa oleva tuotto ja ne kustannukset, mitkä uuden teknologian käyttöönotosta syntyvät. Välttämättä käyttöönottokustannus ei ole pelkästään rahassa mitattavaa, vaan se voi olla esimerkiksi juridinen ongelma -kuten GDPR:n tapauksessa näyttäisi olevan[7]. Tällöin investoinnin positiivinen nettonykyarvo ei välttämättä riitä uuteen teknologiaan investoimiseksi, mikä itsessään on omiaan hidastamaan uuden teknologian käyttöönottoa.

Esimerkin vuoksi ajatellaan skenaariota, jossa tarjolla on liikkumisen palvelu, jossa auton omistava henkilö lainaa autoaan eteenpäin aina, kun ei itse tarvitse sitä. Jos palvelu tuotetaan kokonaisvaltaisesti ja tehokkaasti lohkoketjuteknologialla, niin henkilöllä tulee olla useita linkityksiä lohkoketjuteknologian kautta: älysopimusmahdollisuus vuokraajan kanssa, sopimus pankin kanssa lohkoketjussa toimivasta lompakkopalvelusta, linkki verottajalle tulon automaattiseksi ilmoittamiseksi sekä nanomaksusopimus vakuutusyhtiöön, jossa maksetaan esimerkiksi erityistä vuokraajan vastuuvakuutusta siltä ajetulta ajalta, kun auto on vuokrattuna. Auton vuokraus käynnistäisi automaattisesti älysopimuksen kautta sopimussuhteen auton omistajan ja vuokraajan välillä, jossa syntyisi normaalien vuokrasopimusehtojen lisäksi laskutusoikeus vuokraajan lohkoketjussa sijaitsevaan lompakkoon. Auton omistajan saadessa suorituksen reaaliajassa omaan lohkoketjussa sijaitsevaan lompakkoonsa, lähtee tästä tieto verottajalle tulosta, sekä tieto vakuutusyhtiöön reaaliajassa vuokrakäytössä ajetuista

[7] Kts. tämän työn liite 3.

matkoista, jolloin vakuutusyhtiö voi reaaliajassa veloittaa tästä lisävastuuvakuutuksesta oikean käytön mukaan.

Vaikka esimerkillä ei vielä olekaan todellisuuspohjaa, tämä olisi erittäin tehotonta toimintaa, jos vuokraaja joutuisi esimerkiksi puolen tunnin käytön takia tekemään perinteisen ”paperisopimuksen” omistajan kanssa, maksamaan tilisiirtona jälkikäteen lasketun summan auton omistajalle, omistaja tekisi verottajalle erillisen pääomatuloveroilmoituksen, sekä ilmoittaisi vakuutusyhtiöön ne ajat, jolloin auto on ollut muun ihmisen käytössä ja vakuutusyhtiö tekisi näistä erillisen laskelman ja lähettäisi sen sitten omistajalle. Tässä vaiheessa ylimääräinen työ on jo niin suurta, että vuokraustoiminnan tulee olla laaja-alaista, jotta se olisi kannattavaa. Tämän vuoksi yksityishenkilö todennäköisesti tässä esimerkissä luopuisi siitä. Myöskään edellä esitetty tilanne ei tunnu kovin tehokkaalta, jos yksikin prosessin vaihe joudutaan toteuttamaan perinteisin menetelmin. Tämän vuoksi lohkoketjuteknologian potentiaalin saavuttaminen edellyttää, että se on laaja-alaisesti tuettu. Nykyinen lainsäädäntö esimerkiksi GDPR-sääntelyn kautta vaikeuttaa tätä kehitystä.

4.6 Yhteenveto

Kuten edellisessä kappaleessa 4.5 jo totesin, niin vaikka lohkoketjuteknologia katsotaan yleiskäyttöisten teknologioiden luokittelussa uudeksi teknologiaksi, ovat sen vaikutukset juuri prosesseihin kaikista suurimmat. Tämä havaintoa tukee myös Davidson ym. (2016a,b) esittämä väite siitä, että lohkoketjuteknologia on institutionaalinen innovaatio eli sellainen innovaatio, joka vaikuttaa tuotantokustannusten sijasta transaktiokustannuksiin.

Toki intuitiivisesti ajateltuna lohkoketjuteknologia on teknologinen innovaatio, mutta taloustieteen näkökulmasta se ei ole teknologiaa, joka siirtää kokonaistuotosta koordinaatistossa oikealle uuden teknisen keksinnön taikka prosessin avulla. Taloustieteessä talouden kasvua selitetään endogeenisilla kasvumalleilla, joissa talouden kasvu on peräisen talouden sisäisistä malleista, ei ulkoa annetusta teknologisesta kehityksestä (vrt. Solow’n kasvumalli). Endogeenisten mallien mukaan kasvu syntyy investoinneista henkiseen pääomaan (human capital) eli koulutukseen ja innovaatioihin (Romer, 1994). Nykyaikaisten taloustieteen mallien mukaan tuottavuus siis kasvaa, kun talouteen syntyy innovaatioita ja innovaatiot vaativat syntyäkseen henkistä pääomaa.

Innovaatiot voivat siis olla uusien tuotteiden lisäksi mm. prosessi-innovaatioita. Transaktiokustannusten aleneminenkin vaikuttaa tuottavuuteen, eikä lohkoketjuteknologian poikkeaminen perinteisestä ”fyysinen keksintö”-muotista millään tavalla sodi innovaatiopohjaisen talouskasvun näkemystä vastaan. Näkemykseni mukaan lohkoketjuteknologiaa ei voi kuitenkaan selittää uutena yleiskäyttöisenä teknologiana neoklassisen teknologisen kehityksen mallin kautta, vaan juurikin transaktiokustannuksia alentavana institutionaalisena eli

hallinnollisena innovaationa. Transaktiokustannusten merkittävyyden lohkoketjuteknologian perustavanlaatuisena innovaationa ovat tuoneet esille myös Catalini & Gans (2016).

Transaktiokustannusten alenemisen tuoman tehokkuushyödyn linkittämisen tuottavuuden kasvuun voi jakaa vielä kahteen osaan: olemassa olevien systeemien tehokkuuden paranemiseen ja uusin markkinaratkaisuihin. Toistaiseksi ratkaisemattomien teknisten rajoitteiden vuoksi tehokkuuden paranemisen näkökulmasta on otettu vasta kokeilevia askelia lohkoketjuteknologian käytössä, mutta uusia pienen mittakaavan markkina-alustoja on jo syntynyt. Tässä luvussa esitellyt nanomaksut ja älysopimukset ovat erittäin tehokas tapa parantaa tuottavuutta, sillä niin nanomaksut kuin älysopimuksetkin parantavat eritoten transaktiotehokkuutta. Mutta yhtä lailla, kun transaktiotehokkuus paranee nanomaksuilla ja älysopimuksilla, mahdollistavat ne myös uusia markkinapaikkoja sellaisille transaktioille, jotka kolmannen osapuolen varmentamina olisivat tulleet liian kalliiksi saavutettuun hyötyyn nähden.

Yleiskäyttöisen teknologian kolme ominaispiirrettä eli innovaatiot, kehittyminen ja kokonaisvaltaisuus täyttyvät lohkoketjuteknologian osalta. Transaktiokustannusten aleneminen vaikuttaa innovoivasti siten, että voidaan toteuttaa täysin uusia ratkaisuja olemassa oleviin asioihin, kuin myös luoda täysin uudenlaisia markkina-alustoja silloin. Esimerkiksi poistamalla kolmas osapuoli välistä, turvaten osapuolten kaupankäynti ja oikeusturva älysopimuksella sekä mahdollistamalla nanomaksujen avulla sellaiset transaktiot, jotka eivät olisi olleet välittäjän (ns. kolmas osapuoli) kautta taloudellisesti kannattavia, ts. transaktion kustannus olisi ylittänyt transaktion arvon. Kuten taulukoissa 5 ja 6 esitetään, voidaan näitä ratkaisuja toteuttaa laaja-alaisesti eri toimialoilla, eivätkä ratkaisut rajoitu pelkästään finanssialalle ja perinteiseksi koettuun kaupankäyntiin.

Yleiskäyttöisen teknologian toinen ominaispiirre eli teknologian kehittyminen on lohkoketjuteknologian suhteen ehkäpä helpoin hahmottaa näistä kolmesta piirteestä. Sillä siis tarkoitettiin sitä, että vaikka teknologia kehittyy, on se tunnistettavissa samaiseksi teknologiaksi. Koska lohkoketjuteknologia on transaktiokustannuksia alentava prosesseihin vaikuttava teknologia, ei sen muoto, toimintamalli ja tunnistettavuus muutu kovinkaan paljoa, vaikka tekniset ratkaisut sen taustalla muuttuisivat aivan täysin. Tästä voidaan ottaa esimerkiksi jo nykyhetki, jolloin on jo tarjolla Proof of Work ja Proof of Stake -tyylisiä varmentamistapoja ja tulevaisuudessa omat ratkaisunsa vaatii kvanttitietokoneet (liite 1). Näistä kaikista huolimatta jokaisessa tapauksessa lohkoketjuteknologia on tunnistettavissa samaiseksi teknologiaksi.

Kolmas yleiskäyttöisen teknologian edellytys on teknologian kokonaisvaltaisuus. Sen tulisi levittäytyä yleisesti talouteen. Kuten taulukoista 5 ja 6 näkee, on tämä mahdollista hyvin laaja-alaisesti eri toimialoilla ja sillä voidaan korvata monia sellaisia ratkaisuja, jotka tehdään tällä hetkellä eri tavalla. Tietysti yleiskäyttöiselle teknologialle tyypillisesti on täysin mahdotonta sanoa etukäteen, että millä tavalla se korvaa olemassa olevia ratkaisuja, mutta teknologisesta kyvykkyyttä peilaten ehdot teknologian kokonaisvaltaisuudesta täyttyvät.

Lohkoketjuteknologia tulee todennäköisesti leviämään sellaisten alojen kautta, joissa transaktiokustannusten madaltumisella voidaan maksimoida hyöty ja tuottavuus. Seuraavassa luvussa 5 esitellään tarkemmin erilaisia lohkoketjuteknologian potentiaalisia sovelluksia eri toimialoilta. Tarkoitus on havainnollistaa kyseisen teknologian kyvykkyyden lisäksi sitä, että lohkoketjuteknologia täyttää yleiskäyttöisenteknologian kokonaisvaltaisuuden vaatimuksen.

5 LOHKOKETJUTEKNOLOGIAN SOVELLUTUKSET

5.1 Yleistä

Tässä luvussa kuvataan konkreettisia esimerkkejä sovellutusalueista, joilla lohkoketjuteknologiaa pyritään parhaillaan hyödyntämään. Esimerkkejä on pyritty löytämään siten, että niiden avulla saataisiin arvioitua, missä määrin lohkoketjuteknologiaa voitaisiin jo nyt tai lähitulevaisuudessa hyödyntää eri toimialoilla. Esimerkit pohjautuvat mm. Etlan julkaisemiin arvioihin kyseisen teknologian sovellusmahdollisuuksista. Tässä luvussa asian esittämisen helpottamiseksi puhutaan lohkoketjusta tekevänä osapuolena, vaikkakin tarkemmin ottaen lohkoketjuteknologia mahdollistaa päällänsä ajettavia sovelluksia, jotka ovat alla olevissa esimerkeissä toimiva osapuoli.

Usein puheessa sekoitetaan lohkoketjuteknologia ja Bitcoin keskenään, mikä on toisaalta ymmärrettävääkin ottaen huomioon niiden toisiinsa kietoutunut historia. Kuten jo aiemmin tässä tutkielmassa on todettu, lohkoketjuteknologian taustalla oleva oivallus hajauttaa tieto turvallisesti ja kustannustehokkaasti verkkoon, ei kuitenkaan rajoitu vain virtuaalisiin valuuttoihin, vaan hyödyttää kaikkea tiedon hajauttamista. Luvussa neljä esitellyistä lohkoketjuteknologian soveltamismahdollisuuksista nostaisin ehkä yksittäisenä mielenkiintoisimpana mahdollisuutena juurikin älysopimukset, sillä älysopimusten mahdollistama prosessien automatisointi on helposti havainnoitava ja toteutettava askel.

Lohkoketjuteknologiasta puhuttaessa ei voi olla huomioimatta myöskään rahoitussektoria, joka R3-konsortion kautta vaikuttaa olevan liikkeellä ensimmäisten joukossa. Fintech eli financial techonolgy ei itsesään viittaa lohkoketjuteknologiaan, mutta monet tämän termin alle mahtuvat ideat olisivat aivan hyvin toteutettavissa lohkoketjuteknologialla. Vuoden 2018 alusta voimaan astunut uusi maksupalveludirektiivi PSD2 vaatii, että kolmansille osapuolille on asiakkaan suostumuksen valossa mahdollistettava pääsy asiakkaan tilille (Finanssivalvonta, 2018), mikä itsessään tuottaa hedelmällistä maaperää

lohkoketjuteknologialle juuri Fintechin alalla. Saksassa on saanut toimiluvan jo ensimmäinen BaaS-palvelu (Bankin as a Service), mikä tarkoittaa, että pankki toimii vain verkossa ja ettei kyseisellä pankilla ole perinteistä konttoria (Ventureskies 2016). BaaS-pankin palvelut ovat siis puhtaasti verkossa. Pankin tekninen toteutus ei ole selvillä, mutta tämäkin BaaS-palvelun voisi mahdollisesti tulevaisuudessa toteuttaa lohkoketjuteknologialla verkkoon hajautettuna.

5.2 Virtuaalivaluutat

Virtuaalivaluutat ovat ehkä perinteisin esimerkki lohkoketjuteknologian sovellutuksista. Lohkoketjuteknologialla virtuaalirahan tilikirja on hajautettu verkkoon ja se on murtovarma (ns. 51% hyökkäys) ja transaktiot tapahtuvat (lähes) reaaliajassa ympäri maailmaa ja tieto on aina ajantasaista. Transaktioiden väärentäminen on kannattamatonta ja virtuaalivaluuttalompakko voidaan liittää osaksi erilaisia sovelluksia, jolloin maksaminen ja ”kirjanpito” näissä helpottuu huomattavasti.

Bitcoin on vain yksi monista digitaalisista valuutoista, mutta ylivoimaisesti suosituin ja tunnetuin. Kyseisellä valuutalla ei ole keskuspankkilähtöistä liikkeellelaskijaa, vaan rahan enimmäismäärä on lukittu jo alkuvaiheessa ja sitä saadaan jatkuvasti lisää käyttöön louhimalla (mining). Mitä enemmän bitcoineja, cryptovaluuttaa, louhitaan sitä vaikeammaksi louhiminen käy ja hidastuu. Käytännössä tämä louhinta on uusien lohkojen luomista lohkoketjuun ja kiitokseksi tästä louhija saa itsellensä bitcoineja. Louhinnasta saatavien bitcoinien määrä puolittuu aina 210 000 lohkon välein ja on tällä hetkellä 12,5 bitcoinia per lohko. Seuraava puolittuminen tapahtuu vuonna 2020. Louhintapalkkioilla varmistetaan lohkoketjujen jatkuva lisääntyminen ja hajautuminen sekä kannustetaan käyttäjiä varmentamaan muiden käyttäjien transaktioita. (Barrdear, 2014).

Tällä hetkellä digitaalisilla valuutoilla ei voi ostaa kulutushyödykkeitä kovin laajalti, paitsi niin kutsutussa dark webissä, jossa bitcoin on rikollisten suosima maksutapa. Digitaalisella valuutalla onkin näin ollen muuntokurssi perinteisiin valuuttoihin nähden, joten täysin irti vanhasta keskuspankkirahasta digitaalisella valuutalla ei pääse. Finanssikriisi voimistutti esimerkiksi bitcoinin hintaa suhteessa dollariin ja bitcoin maksoi parhaimmillaan 17. joulukuuta 2017 $19 783,21 bitcoinilta (Coindesk, 2018). Bitcoinin suora ja ainoa hieman tunnetumpi kilpailija on Ethereum. Ethereum on Bitcoiniin nähden paljon joustavampi ja monipuolisempi lohkoketjuteknologiaan perustuva virtuaalivaluutta, joka sisältää mahdollisuuden tehdä myös älysopimuksia (Ethereum Homestead, 2017).

Kuitenkaan Bitcoinilla (eikä todennäköisesti Ethereumilla) ei ole nähtävissä kovinkaan valoisaa tulevaisuutta. Bitcoinin tapauksessa ongelmaksi muodostuu jo itsessään hupeneva rahavaranto (rahan määrä kiinteä), mutta tällä hetkellä markkinoilla olevia kryptovaluuttoja vaivaa yleisemminkin se, että ne eivät täytä rahan kolmea perustehtävää eli sitä, että raha on vaihdon väline, arvon säilyttäjä

ja arvon mitta. Kryptovaluutoilla voi käydä kauppaa vain hyvin rajoitetusta eivätkä heiluvat kurssit täytä arvon säilyttäjänkään vaatimusta. Lisäksi Bitcoinin kurssi on tällä hetkellä niin korkea, että Bitcoin ei toimi arvon mittanakaan kovin hyvin.

Raskin & Yermack (2016) esittävät, että yksi lohkoketjuteknologian hyödyntämisen mahdollisuuksista olisi niin sanottu ”Fedcoin” eli keskuspankkilähtöinen digitaalinen valuutta. Keskuspankkivaluutta vastaisi aikoinaan käytössä ollutta keskuspankkikultaa ja mahdollistaisi muutenkin rahan siirtämisen varmemmin ja halvemmalla tallettajien välillä. Keskuspankki voisi omien tilikirjojensa ohella hoitaa liikepankkienkin tilinpidon ja toimia kaikkien maksujen välittäjinä, jolloin Raskin & Yermack arvioivat mahdollisten kustannussäästöjen olevan jopa 50%-80% luokkaa.

Suuren volyyminsä ansiosta keskuspankki voisi valvojan asemasta toimia myös maksunvälittäjänä perinteisten pankkien lisäksi kotitalouksille ja yrityksille. Keskuspankit nauttivat myös yleisesti ottaen korkeasta julkisesta luottamuksesta. Erityisesti kansainväliset rahansiirrot ovat erittäin kalliita ja vuoden 2015 lopussa keskimääräinen kansainvälisen rahansiirron kustannus oli 7,37%. Keskuspankki pystyisi hoitamaan lohkoketjuteknologialla tämän ilman lukuisia nykyisin tarvittavia välikäsiä. Lisäksi lohkoketjuteknologian avulla keskuspankit pystyisivät taistelemaan paremmin kansainvälistä rahanpesua ja verojen välttelyä vastaan. (Raskin & Yermack 2016).

Toisena vaihtoehtoisena ratkaisuna Fedcoinista on puhuttu pankkien välisenä rahana, jolloin järjestelmä ei eroasi kovinkaan paljoa nykyisestä. Vain tapa kirjata asioita helpottuisi, kun jokainen pankkien välinen transaktio ei sisältäisi useita välivaiheita, vaan kirjautuisivat aina lohkoon (lähes) reaaliajassa.

Kummassakin tapauksessa lohkoketju toimisi turvallisena tietojen säilytyspaikkana ja kun siihen vielä lisätään älysopimusten ja hajautettujen autonomisten organisaatioiden ominaisuuksia, se voisi toimia varsin autonomisesti ennalta määrättyjen parametrien mukaan. Lohkoketjuteknologian transaktiokustannuksia alentava vaikutus on tämänkin sovellutuksen avainmahdollistaja, sillä tämän kokoluokan ratkaisu olisi perinteisin tavoin mahdotonta toteuttaa kustannustehokkaasti.

5.3 Älysopimukset

Automaattisesti etukäteen asetettujen parametrien toteuduttua täytäntöön pantaviin älysopimuksiin ei tarvita kolmatta osapuolta valvomaan sopimuksen noudattamista. Parhaimmassa tapauksessa älysopimus osaa toteuttaa itsensä (self-executing), jolloin älysopimus ehtojen täyttyessä hoitaa myös sopimukseen liittyvät transaktiovelvoitteet. Älysopimusten suurin hyöty saavutetaankin osana kokonaisprosessia, jossa prosessin eri vaiheita voidaan automatisoida itsestään toteutuvilla sopimusparametreilla ja näin ollen nopeuttaa prosessin

läpimenoaikaa. Älysopimuksilla tullee olemaan sopimusjuridiikan näkökulmasta suuri vaikutus toimialaan: siinä missä sopimusoikeudellisia asioita puidaan jälkikäteen riita-asioina, tulee painopiste älysopimusten myötä kallistumaan näiden sopimusparametrien määrittämiseen.

Älysopimukset voivat olla erittäin monimutkaisia ja pitkässä riippuvuussuhteessa muihin komponentteihin, mutta yksinkertaisimmillaan älysopimus esimerkiksi voi olla etämyynti-kuljetuspalvelu. Siinä lohkoketju lähettää maksun tavarantoimittajalle välittömästi, kun tavara on saapunut perille. Tämä saapuminen voidaan kuitata tapahtuneeksi esimerkiksi GPS-koordinaattien perusteella, joten tässäkään vaiheessa toimitusta ei tarvita ihmisosapuolta vastaanottamaan lähetystä. (Iansiti & Lakhani 2017).

Älysopimuksen ei tarvitse rajoittua pelkästään yksinkertaiseen transaktiosopimukseen, vaan se voi sisältää lisävelvoitteita ja jatkuvuutta. Mattila (2016) mainitsee esimerkkinä musiikkipalvelun, josta voi ostaa kappaleen omaan käyttöön kiinteällä rahasummalla, mutta jos sitä sopimusehtojen mukaan käyttää kaupallisessa toiminnassa, saa alkuperäinen artisti tuotosta tietyn osuuden x. Älysopimus tunnistaa, jos kappaletta käytetään kaupallisessa toiminnassa ja tilittää automaattisesti alkuperäiselle oikeuksien omistajalle lähes reaaliajassa sovitun tuotto-osuuden x. Lohkoketjuteknologian transaktioita alentava vaikutus mahdollistaa tämänkin tyyppisen markkinapaikan ja -ratkaisun luomisen, sillä edellä kerrottu ei olisi kustannustehokasta, mikäli kolmannen osapuolen tulisi jotenkin valvoa kappaleiden käyttöä kaupallisessa toiminnassa ja jokin osapuoli hoitaisi käyttöön perustuvan laskutuksen ja ylläpitäisi niihin liittyviä sopimuksia ja muita vaateita.

Toisena käytännön esimerkkinä R3-konsortio on esitellyt oman hajautetun tilikirjan ratkaisunsa R3 Cordan[8]. Corda on tarkoitettu tallentamaan ja hallinnoimaan rahoitussopimuksia. Corda ei ole kaikille avoin systeemi, vaan perustuu käyttöoikeuksiin ja sillä ei ole keskitettyä valvojaa. Siihen on kuitenkin sisäänrakennettu solmukohtia valvoville viranomaisille, eikä se sisällä omaa virtuaalivaluuttaa. Corda pystyy saavuttamaan yhteisymmärryksen eri yritysten välillä yksittäisissä sopimuksissa, mutta ei systeemin tasolla. (Hearn & Brown, 2016).

---

[8] OP Ryhmä julkaisi 22.11.2018 tiedotteen, jonka mukaan se kehittää yhdessä Nordean, Asiakastieto Groupin, Tiedon, Privanetin, Verohallinnon sekä Patentti- ja rekisterihallituksen kanssa Cordaan pohjautuvaa lohkoketjuteknologia-alustaa, jolla voitaisiin käydä kauppaa Suomen noin 300 000 listaamattoman yrityksen osakkeilla sekä hallinnoida näitä osakkeita ja osakeanteja sekä ylläpitää osakasrekisteriä. Tällä hetkellä edellä mainittuja tietoja ei ole laajasti ja helposti saatavilla, eivätkä välttämättä ollenkaan ajantasaisia. Osakeyhtiölaki ei vaadi tietojen ylläpitämistä mitenkään keskitetysti, joten tähän saakka tietojen oikeellisuus ja ajantasaisuus ovat olleet yrityksen puhtaasi vastuulla. Lohkoketjuteknologian avulla nämä tiedot hajautetaan lohkoketjuun, jolloin kaikki tieto on kaikkien saatavilla ja ajantasaista. Osakeomistukset sekä kaupankäynti päivittyvät reaaliaikaisesti. Tästä hyötyvät niin muut lohkoketjun käyttäjät kuin myös viranomaiset. Lisäksi täysin digitaalinen, reaaliaikainen kaupankäynti ilman kolmatta osapuolta lohkoketjussa mahdollistaa tehokkaamman rahoituksen hankinnan osakeantien muodossa kuin perinteiset kanavat.

5.4 Jakamistalous

Suomen Pankin maksuneuvoston julkaisussa (Kapanen & Nordlund, 2016) maalaillaan kuvaa siitä, että autokin on tulevaisuudessa lompakko ja kasa sopimuksia. Auto ei enää ole yksityisesti omistettu, vaan autonominen, sosiaalisen kollektiivin palvelutuote, joka hoitaa niin kalenterit ja varaukset kuin tankkaukset, huollot ja taloushallinnon. Ajatus on lohkoketjuteknologiankin kannalta mielenkiintoinen. Nimittäin nämä tulevaisuuden toiminnot voidaan hajauttaa verkkoon lohkoketjuteknologian avulla (Kapanen & Nordlund, 2016). Kun auton menee tankkaamaan, auto keskustelee verkon välityksellä bensapumpun kanssa ja hoitaa maksun ilman, että kuskin täytyy tehdä asialle mitään. Transaktio tapahtuu verkossa. Lisäksi, koska auto on kollektiivin omistuksessa, on tehty älysopimus, minkä perusteella auton käytön kustannukset jaetaan kollektiivin kesken ja esimerkiksi bensapumppu osaa suoraan tankatessa laskuttaa jokaista kollektiivin jäsentä auton tosiasiallisen käytön mukaan tai huolto- ja vakuutuskustannukset jaetaan reaaliajassa tosiasiallisen käytön mukaan– sillä älysopimus ja kollektiivin lompakot ovat hajautettuna verkossa. Huoltoon mentäessä auto on tietenkin varannut itselleen etukäteen huoltoajan perustuen kollektiivin kalentereihin ja siihen, kuka hyväksynyt huoltoon viennin vastuulleen jonkinmoista ”vaivannäön” hyvitystä vastaan.

Auto on tietenkin vain yksi esimerkki jakamistaloudesta ja sen mahdollisuuksista hyödyntää lohkoketjuteknologiaa. Jakamistalous-lohkoketjun toimivuuden kulmakiviksi muodostuvat juurikin älysopimukset ja lohkoketjulompakot. Älysopimuksen avulla on määritelty tarkasti kollektiivin osallisen oikeudet ja vastuut sekä hinnasto. Koska älysopimus toteuttaa itseään ennalta määrättyjen parametrien mukaan autonomisesti, ei kollektiivin käyttäjien välillä täydy olla luottamusta siitä, että jokainen kollektiivin osallinen ”pelaa reilua peliä”, vaan kaikella toiminnalla on etukäteen määrätty taksa, joka veloitetaan automaattisesti henkilön käyttäytymisen mukaan.

Jakamistaloudessa jakajia voi olla kaiken lisäksi hyvin monia ja jaettavan hyödykkeen käyttöasteet voivat vaihdella paljonkin eri jakajien välillä. Siksi onkin erittäin tärkeää, että kustannukset kohdistuvat oikein ja tarkasti jakamishyödykkeen käytön mukaisesti. Transaktiokustannusten aleneminen on tässäkin avainasemassa, sillä jaettavan hyödykkeen kustannusten jakamisesta ei tulisi syntyä kovinkaan suuria kustannuksia, jotta se ei karkottaisi jaettavan hyödykkeen satunnaiskäyttäjiä. Toisin sanoen hyödykkeen käyttö tulisi pystyä jyvittämään tarpeeksi tarkalla tasolla tosiasiallisen käytön mukaan, eikä tästä jyvittämisestä saisi syntyä ylimääräistä kulua, joka laskutettaisiin käytön päälle. Perinteisellä mallilla kolmannen osapuolen välittäjä tyypillisesti ottaa välityspalkkiona tietyn minimipalkkiontason riippumatta itse transaktion arvosta, jolloin se voi olla suhteellisesti varsinaisen transaktion arvoon nähden hyvinkin suuri.

5.5 Terveydenhoitopalvelut

Lohkoketju mahdollistaisi parhaimmillaan koko maan kattavan turvallisen tietokannan, jossa potilaan koko hoitohistoria olisi missä tahansa hoitopaikassa välittömästi saatavissa potilaan omalla digitaalisella allekirjoituksella. Lisäksi data-analytiikan kehittyminen on tuonut uusia mahdollisuuksia myös terveydenhuoltopalveluihin. Kun saatavilla on massiivinen data-aineisto erilaisten henkilöiden elintavoista ja sairauksista, voidaan tätä dataan hyödyntämällä ennustaa yksittäisen henkilön riskiä sairastua johonkin tiettyyn sairauteen ja parhaassa tapauksessa ennaltaehkäistä koko sairaus. Haasteena on kuitenkin tietosuoja ja tekninen toteutus tällaisen massiivisen data-aineiston hallinnoinnille ja ylläpidolle. Niissä lohkoketjuteknologia ratkaisee useita säilytykseen ja hallinnointiin liittyviä teknisiä ongelmia, mutta ei asian juridista problematiikkaa. Lohkoketjuteknologia-sovellutus parantaa niin potilaan hoitomahdollisuuksia kuin tiedon saatavuutta sekä madaltaa huomattavasti tiedon hallinnasta aiheutuvia kustannuksia, joten juridisen problematiikan ratkaisemiseen tarvitaan poliittista tahtoa.

Tietotekniikkayhtiö Oracle (2016) näkee lohkoketjuteknologian potentiaalin juurikin terveydenhoitopalveluiden tietokannoissa. Heidän näkemyksessään potilastiedot olisivat salatussa lohkoketjussa, johon pääsisivät käsiksi kaikki terveydenhoitoammattilaiset, jolle potilas on omalla henkilökohtaisella digitaalisella allekirjoituksellaan antanut luvan katsoa tietoja. Lisäksi katselulupa voisi olla vakuutusyhtiöillä ja sairaaloiden laskutuspalveluilla, jolloin sairaala voisi asioida maksuasioissa suoraan vakuutusyhtiön kanssa, mutta se myös toimisi taistelussa vakuutuspetoksia vastaan.

Jo nykyisellään vakuutusyhtiöt tekevät tiivistä yhteistyötä hoitolaitosten kanssa. Hoitolaitoskumppanuuksiin kuuluu tiiviinä osana maksusitoumukset, joissa vakuutusyhtiö arvioi hoitotietojen perusteella etukäteen hoidon korvattavuuden ja näin ollen korvattavassa tapahtumassa lupautuu maksamaan laskun suoraan hoitolaitokselle ilman, että vakuutetun tulee itse käyttää rahaa. Tämä prosessi on nykyisellään hyvin mekaaninen, missä hoitava lääkäri tekee vakuutusyhtiöön maksusitoumuspyynnön, vakuutusyhtiö käsittelee pyynnön ja arvioi korvattavuutta hoitotietojen perusteella. Tämän jälkeen vakuutusyhtiö myöntää maksusitoumuksen hoitolaitokselle, hoitolaitos ilmoittaa myönteisestä päätöksestä potilaalle ja varaa ajan hoitoon. Hoidon jälkeen hoitolaitos lähettää laskun vakuutusyhtiölle, jossa se maksetaan manuaalisesti. Koko prosessin voisi sujuvoittaa samassa lohkoketjussa toimivilla sovelluksilla, jossa koko edellä kuvattu prosessi toteutuisi samalla hetkellä kun potilas varaa ajan hoitoon: hoitolaitos saa lohkoketjusta tiedon, missä potilas on vakuutettu, vakuutusyhtiö saa lohkoketjusta potilaan hoitotiedot, joiden perusteella automatiikka tekee maksusitoumuspäätöksen välittömästi, hyväksytystä maksusitoumuksesta menee tieto sekä varausta tekevälle potilaalle sekä hoitolaitokselle sekunneissa ja lasku menee käynnin jälkeen välittömästi maksuun lohkoketjusta löytyvän vakuutusyhtiön ”lompakon” kautta. Siinä, missä manuaalisesti prosessissa kestäisi päiviä, tapahtuu lohkoketjun kautta sama prosessi sekunneissa.

Terveydenhuoltoesimerkeissä transaktiokustannusten alenemisen tulee nähdä implisiittisesti prosessin virtaviivaistumisen kustannusalentumana. Potilastietojen ja muiden henkilötietojen käsittelyssä tärkeintä on tietoturva ja vasta sen jälkeen kaikki muu. Kun tietoturva on ratkaistu, säästävät yllä esitellyt koneoppimiseen ja data-analytiikkaan perustuvat lohkoketjuratkaisut juuri välikäsien kustannuksissa. Kaikkea tietotyötä ei voida (ainakaan toistaiseksi) ulkoistaa tietokoneille, mutta vakiomuotoiset perustapaukset voidaan massana ohjata automaattisen käsittelyn piiriin, jolloin välikädet (ns. kolmannet osapuolet lähtöpisteen ja maalin välillä) poistuvat prosessista.

5.6 Energian tuotanto ja hallinta

Älysopimukset ja hajautetut autonomiset organisaatiot mahdollistaisivat jatkuvan sopimuksen kilpailuttamisen, jossa lohkoketju tauotta ja automaattisesti kilpailuttaisi ja vaihtaisi sopimusta kummankin osapuolen kannalta parhaaseen mahdolliseen vaihtoehtoon. Tämä muuttaisi sopimusten rakenteita, joissa nykyisin tehdään pitkiä määräaikaisia sopimuksia, hyvin lyhyen aikavälin sopimuksiksi. Jotta tällainen toiminta olisi taloudellisesti kannattavaa, ei sopimuksista voi syntyä kulua osapuolille, sekä transaktioiden tulee olla reaaliaikaisia ja luotettavia. Nanomaksut ovat tässäkin merkittävässä osassa, sillä sopimusten vaihtamisen nopea tahti edellyttää sitä, että pieninkin transaktio voidaan toteuttaa kuluitta ja taloudellisesti kannattavasti. Kustannusten hallinnan kannalta lohkoketjuteknologia loistaa erityisesti siinä, ettei siinä ole kolmatta osapuolta, välittäjää (markkinapaikkaa) ottamassa omaa välityspalkkiotansa.

Nykytilanteessa kuluttaja voi hankkia itselleen aurinkopaneelit tai tuulivoimalan ja varastoida saatua energiaa akustoon omaa käyttöä varten. Siinä vaiheessa, kun tuotanto ylittää kulutuksen ja akusto on täynnä, ei tätä ylimääräenergiaa saada talteen. Lisäksi kyseinen kuluttaja on todennäköisesti sähköyhtiön ja sähkönsiirtoyhtiön sopimusten kautta sidottu kiinteään kuukausimaksuun, joka tulee maksettavaksi siitä huolimatta, onko kotitalous omavarainen sillä hetkellä vai ei. Lisäksi sopimus voi olla määräaikainen, jolloin kyseinen kuluttaja ei voi edes vaihtaa sähkösopimustaan kesken sopimuskauden edullisempaan.

Toinen Oraclen (2016) näkemys lohkoketjuteknologian sovellutuksista käsittelee juurikin kotitalouksissa tuotettavaa sähköenergiaa (aurinkoenergia tai tuulienergia). Aurinkoisina / tuulisina päivinä energiaomavaraisuus saattaa ylittyä, jolloin järkevää on myydä ylijäämäenergia sähköverkkoon muille välitettäväksi muille sähkönostajille. Vastaavasti pilvisinä / tuulettomina päivinä, kun oma tuotanto ei riitä, kotitalous ostaa tarvitsemansa energian sähköverkosta. Lisäksi lohkoketju osaisi valita kenelle se myy ylijäämäsähköä sen mukaan, kuka maksaa sinä päivän sähköstä parhaan hinnan. Vastavuoroisesti lohkoketjuteknologiaan perustuvassa systeemissä ei välttämättä tehtäisi ollenkaan perinteistä sähkösopimusta, vaan älysopimusten avulla lohkoketju ostaisi aina päivän tai jopa tunnin hinnan perusteella halvinta sähköä. Ostamisen ja myymisen

jatkuvasti eri paikoista mahdollistaa nanomaksut, sillä niiden avulla mikään transaktio ei ole liian pieni käsiteltäväksi taloudellisesti kannattavalla tavalla ja kaikki ylijäämäsähkö kannattaa myydä verkkoon. Mikäli sähköyhtiölle tulisi ylimääräistä kulua jatkuvista pätkäsopimuksista, niin myynnin ja ostamisen suhteen, ei tällaista toimintaa harjoitettaisi markkinatalouden ehdoin. Juuri lohkoketjuteknologian mahdollistama transaktiokustannusten aleneminen ilman kolmannen osapuolen välittäjää mahdollistaa yllä kuvatun kaltaisen toiminnan ja markkina-alustan. Lisäksi tällaisessa ylijäämäsähkön myynnissä puhutaan lähes poikkeuksetta puhtaasti tuotetusta ylijäämäsähköstä, kuten esimerkin aurinko- ja tuulienergia.

5.7 Äänestysjärjestelmä

Internet-äänestäminen on tällä hetkellä ajankohtainen puheenaihe, sillä Suomessakin pohditaan mahdollisuutta äänestää internetin välityksellä. Suunnitelmat ovat kuitenkin jääneet toistaiseksi vaiheeseen, koska demokratian kannalta on erittäin tärkeää, että äänestysalusta on toimintavarma ja eikä sitä voi hakkeroida. Jos äänestysjärjestelmää vertaa aiemmin tässä luvuissa esitettyihin lohkoketjuteknologiasovellutus-esimerkkeihin, niin se on varsin yksinkertainen toiminnaltaan: kyseessä olisi hajautettu tietokanta, jossa olisi kaikkien äänioikeutettujen tiedot, kaikkien ehdokkaiden tiedot ja mahdollisuus äänestää haluamaansa ehdokasta. Mattila (2016) mainitseekin julkaisussaan lohkoketjupotentiaalin myös äänestysjärjestelmän alustana. Äänestysjärjestelmässä on erityisen tärkeää, ettei sitä voi hakkeroida, eikä kukaan pääse muutenkaan muuttamaan tuloksia jälkikäteen. Eli sen pitää olla äärimmäisen turvallinen, mutta samaan aikaan myöskin erittäin läpinäkyvä, jotta tulos voidaan varmentaa helposti ja vaalit todeta vilpittömiksi. Samalla myös järjestelmän tulee olla täysin anonyymi ja verkosta riippumaton.

Tässä mielessä lohkoketjun kaikista perinteisin ratkaisu on tarkoitukseen sopivin, missä korkea Proof of Work -työ on oleellisessa asemassa. Lohkoketjuteknologiassa turvallisuus saavutetaan tekemällä enemmän laskentatyötä kuin hyökkääjä (51% hyökkäys). Äänestysjärjestelmän tapauksessa Proof of Work -insentiivi hoidettaisiin siten, että sen sijaan, että henkilö louhisi saadakseen kryptovaluuttaa, henkilö louhii saadakseen oikeuden äänestää. Eli louhintatyöstä saisi palkkioksi äänestyslipukkeen. Lohkoketjuteknologian käyttäminen äänestämisessä on kuitenkin demokratian kannalta hieman ongelmallista, vaikka tekninen toteutus saataisiin kuntoon. Nimittäin vaikka näennäisesti lohkoketjun käyttö on ilmaista, syntyy siitä välillisiä kustannuksia laskennan käyttämän energian muodossa. Lisäksi äänestäminen on perusoikeus, jolloin tilanne, jossa jokaisen pitäisi louhia oma äänestyslipukkeensa, aiheuttaa eriarvoisuutta. Esimerkiksi vanhukselta, joka on koko elämänsä pärjännyt ilman tietotekniikkaa, saattaa olla kohtuutonta vaatia oman äänestyslipukkeensa louhintaa toteuttaakseen perusoikeuttansa äänestää. Ja siinä vaiheessa, kun osalta vaaditaan äänestämään

päästäkseen omakustanteista louhintaa ja osalle se tarjotaan annettuna, ollaan demokratian kannalta isojen kysymysten ääressä.

Vaikka ongelmaan löydettäisiin jokin toinen ratkaisu, jossa louhinnan palkkio ei ole äänestyslipuke, on -kuten yllä todettiin- demokratiaprosessin maksattaminen äänestäjillä hieman kyseenalaista. Vaikka nykyisenkaltainen lohkoketjuteknologia olisikin teknisesti oikein pätevä ratkaisu toteuttaa lohkoketjuteknologiaan perustuva äänestysjärjestelmä, ei se ole taas taloudellisessa mielessä kustannustehokas järjestelmä. Parhain mahdollinen ratkaisu olisi sellainen lohkoketjuteknologinen varmennustapa, jossa voitaisiin käyttää sähköisen äänestyspäätteen - on se sitten henkilön oma tietokone tai esimerkiksi kirjaston kone - laskentatehoa hetkellisesti ja samanaikaisesti itse äänestysprosessin kanssa. Koska normaalin internetsivun käyttö kuormittaa tietokoneen prosessoria vain muutaman prosentin luokkaa, voitaisiin tämä käytön aikana tyhjäkäynnillä oleva prosessori valjastaa laskemaan lohkoketjun varmennustyötä vain muutamaksi minuutiksi kerrallaan, jolloin kustannus äänestäjälle jää minimaaliseksi. Enää vain puuttuu sellainen lohkoketjuteknologia, jolla tämä onnistuu.

Transaktiokustannusten alenemisen näkökulmasta tilanne on tämän sovelluksen kohdalla hieman nurinkurinen nykytilanteeseen verrattuna. Lohkoketjuteknologia kyllä yllä esitetyn kaltaisilla ratkaisuilla alentaisi äänestyksen järjestäjän (valtio/kunta) kustannuksia huomattavasti, mutta vyöryttäisi äänestämisestä syntyviä välittömiä kustannuksia äänestäjille, kun nykyinen systeemi on synnyttänyt korkeintaan välillisiä kustannuksia äänestäjille äänestyspaikalle liikkumisen muodossa (ja toki äänestyksen järjestämisen kustannukset katetaan verovaroista). Uskoisin kuitenkin kokonaiskustannuksen jäävän matalammaksi kuin nykyisessä systeemissä, mutta kuten jo useaan kertaan todettu, välittömien kustannusten vyöryttäminen äänestäjille on demokratian näkökulmasta ongelmallista.

5.8 IPFS

IPFS eli Inter Planetary File System on lohkoketjuteknologiaan perustuva tiedostojärjestelmä, jolla kehittäjänsä pyrkivät kunnianhimoisesti korvaavaan nykyisenkaltaisen http-protokollaan perustuvan internetin (IPFS 2016). Http-protokollaan perustuvassa internetissä tietokone lähettää tietopyynnön palvelimelle, joka palauttaa pyydetyn datan tietokoneelle. On sitten kyseessä yksinkertainen internet-tekstisivu tai jokin videontoistopalvelu, täytyy pyydetty data säilöä jossain tietyssä palvelimessa. Ensiksi käyttäjän selaimen pitää löytää kyseinen serveri, jossa kyseinen tiedosto sijaistee ja sieltä sen pitää löytää myös tiensä takaisin ”internetin läpi” koneelle. Tässä ketjussa on paljon välityspalvelimia ja muitakin lenkkejä. Mikäli jokin vaihe tässä tiedonsiirtoketjussa on saavuttamattomissa, ei tiedoston tavoittaminen todennäköisesti onnistu. Arkielämästäkin on tuttua, että jokin verkkopalvelu on erinäisestä syystä kaatunut tai muuten

saavuttamattomissa. IPFS:ssä on lohkoketjuteknologian perusperiaatteiden mukaisesti kaikki tiedostot hajautettu turvallisesti ympäri verkkoa.

IPFS:n kehittäjät lupaavatkin teknologiasta edeltäjäänsä tehokkaamman ja halvemman. IPFS säästää jopa 60% käytettävästä tiedonsiirtokaistasta ja etsii ja poistaa tuplaversioita samoista tiedostoista aktiivisesti, jolloin myös tilaa säästyy. Jotta tiedostojen saatavuus on varmistettu, IPFS luo versiohistorioita tiedostoista, jolloin ne ovat paremmassa turvassa, koska inhimillinen virhe tai pahimmassa tapauksessa yhden solmukohdan tuhoutuminen ei tuhoa tiedostoja. Tämän lisäksi lohkoketjuteknologian perusperiaatteiden mukaisesti IPFS toimii vertaisverkossa eli se ei ole riippuvainen keskistetystä palveluntarjoajasta ja tämän palveluntarjoajan kapasiteetista sekä luotettavuudesta. Vertaisverkkoon hajauttaminen lisää niin toimintavarmuutta kuin riippumattomuutta ja alentaa kustannuksia. Edellä mainitut seikat on otettu huomioon jo verkon teknisessä rakenteessa, sillä IPFS luo joustavia verkkoyhteyksiä, joiden avulla se on resilientti esimerkiksi runkoverkon ongelmille. Mikäli IPFS tulee laajemmin käyttöön, tulee datan määrä kasvamaan aivan valtavaksi, jolloin järjestelmä tarvitsee tehokkaan indeksointityökalun, jotta tiedostoja löytyisi vertaisverkosta. Se, että kenen vastuulla tällaisen työkalun kehittäminen, ylläpitäminen ja kustantaminen on, on vielä ratkaisematon kysymys.

Transaktiokustannusten alenemisen näkökulmasta kyse on lohkoketjuteknologian perusajatuksesta eli poistaa kolmas osapuoli kuvioista ja alentaa tätä kautta transaktiokustannuksia. Tässä esimerkissä kolmas osapuoli ovat palvelinkeskukset ja muut internet-liikenteen solmukohtia hoitavat yritykset, jotka luonnollisesti laskuttavat palveluistaan ja datan säilömisestä. Myöskin nykyisen kaltaisessa kolmanteen osapuoleen perustuvissa ratkaisuissa datakeskuksen / palvelinhuoneen ylläpitäjä hyvin usein hajauttaa ainakin palvelunsa kriittiset komponentit maantieteellisesti, mikä aiheuttaa ylimääräisiä kustannuksia ylläpidon muodossa. Kustannukseton hajauttaminen on osa IPFS:n lohkoketjuteknologista ratkaisua.

5.9 Yhteenveto

Yleiskäyttöiselle teknologialle ominaispiirteeksi todettiin jo luvussa kaksi, että sen tulee levittäytyä laaja-alaisesti talouteen eri toimialoille ja lopulta kasvattaa näiden alojen tuottavuutta. Tyypillistä yleiskäyttöisille teknologioille on myös se, että aluksi tuottavuuden kasvu saattaa jopa hidastua uuden teknologian adaptoimisen haasteiden vuoksi, mutta lopulta saavutetaan tuottavuuden taso, joka on lähtötasoa korkeampi. Tässä luvussa esitellyt lohkoketjuteknologian sovellukset sopivat kumpaankin kuvaukseen: ne ovat laaja-alaisesti eri toimialoilta ja jokainen niistä on potentiaalinen ja mahdollinen toteuttaa, mutta teknologian adaptaatio saattaa olla hidasta ja haastavaa sekä teknisten että vastuukysymysten vuoksi. Hieman ironisesti hajautettu lohkoketjusysteemi, joka ei tarvitse keskitettyä hallintoa, tarvitsee kuitenkin ainakin alkuunsa keskitetyn kehittäjän tai

kehittäjäverkoston, jonka vastuulla systeemin kehittäminen ja ylläpitäminen on. Tässä tulee taas vastaan ns. early adopters -ongelma, jossa uuden teknologian aikaiset adoptoijat maksavat teknologian kehitys- ja testauskulut. Tämä on taloudellisessa mielessä kannattavaa vain tilanteissa, jossa odotettu tuotto uudesta teknologiasta ylittää uuden teknologian käyttöönoton kustannukset ja tuottaa kilpailuetua. Käytännön tasolla tämä tarkoittaa toimialoja, joissa transaktiokustannukset ovat merkittävässä roolissa kulurakenteessa eli kolmannen osapuolen välityspalkkiot ovat suuria suhteessa transaktioiden arvoihin.

Transaktiokustannukset liitetään mielikuvissa ensisijaisesti kaupankäynnin kustannuksiin, vaikka transaktioita on muunkinlaisia. Kuten tässäkin luvussa on tullut ilmi, niin transaktiokustannuksista voidaan puhua laajassa merkityksessä myös esimerkiksi datan hallinnan, käsittelyn ja siirtämisen kustannuksista (lohkoketjuteknologian äänestysjärjestelmä-, terveydenhoitopalvelusovellutukset sekä IPFS). Kuitenkin oman näkemykseni mukaan lohkoketjuteknologia tulee aivan ensimmäisenä lyömään läpi aloilla, joissa se alentaa kaupankäynnin transaktiokustannuksia. Tämä johtuu ensisijaisesti lohkoketjuteknologian mahdollistamista nanomaksuista ja älysopimuksista, joilla luodaan markkina-alustoja olemassa oleville asioille ja myös täysin uusia markkinoita asioille, jotka eivät ole ennen olleet mahdollisia toteuttaa taloudellisesti kannattavasti, vaikka niiden tekninen toteutus olisikin ollut mahdollista. Jälkimmäisestä nostaisin esille tässä luvussa esitellyt jakamistalouden ja energiakaupan sovellutukset.

Ylijäämäenergian myynti takaisin verkkoon ja yhteiskäyttöinen hyödyke ovat siinä mielessä erinomaisia esimerkkejä juurikin lohkoketjuteknologian eduista verrattuna johonkin muuhun teknologiseen ratkaisuun, joka teoriassa pystyisi seuraamaan kulujen syntyä tai tuottojen generoitumista eurosentin sadasosien tarkkuudella, sillä luottamus ja sen ylläpito ovat rahanarvoisia asioita taloudellisessa toimeliaisuudessa. Mikäli kolmas osapuoli hallinnoisi ylijäämäenergian myyntiä takaisin verkkoon parhaalla mahdollisella hinnalla ja nanomaksujen tilittämistä osapuolille taikka yhteiskäyttöauton kustannusten jyvittämistä äärimmäisellä tarkkuudella ja muita auton osaomistamiseen liittyviä velvoitteita, haluaisi tämä osapuoli tästä toiminnastaan palkkion riippumatta siitä, että synnyttääkö itse tekninen ratkaisu merkittäviä kustannuksia alustan ylläpitäjälle, kun sen kustannukset jyvitetään koko käyttäjäkunnan kesken. Älysopimuksilla ja lohkoketjuteknologialla alennetaan transaktion kustannuksia myös siten, että luottamuksesta ei tarvitse maksaa.

Lohkoketjuteknologian potentiaali on siinä, että teknologian päälle voi rakentaa kokonaisvaltaisia sovellusratkaisuja. Kuten jo useampaankin kertaan tässä työssä on todettu, vaikuttaa lohkoketjuteknologia prosesseihin, eikä yritä keksiä ns. pyörää uudelleen, vaan keskittyy -samaa vertausta jatkaen- renkaan ajo-ominaisuuksiin. Jokaiselle tässäkin luvussa esitetylle sovellukselle voi keksiä monia vaihtoehtoisia teknologisia tapoja päästä haluttuun lopputulokseen, mutta ongelmat syntyvät siinä, kun nämä ratkaisut halutaan nivoa yhteen saumattomasti toimivaksi kokonaisuudeksi ja tehdä tämä vielä

kustannustehokkaasti ja skaalautuvaksi. Kun luottamus on rakennettu sisälle lohkoketjusysteemiin, niin kallista kolmatta osapuolta ei tarvita, eikä tämän valvojan kustannus kasva alustan koon kasvaessa, vaan älysopimukset skaalautuvat kustannustehokkaasti.

6 JOHTOPÄÄTELMÄT

Jo tämän työn alkupuolella totesin, että asioiden ennustaminen on huomattavasti vaikeampaa kuin jälkikäteinen havainnointi. Menee vielä todennäköisesti vuosikymmeniä, ennen kuin voimme havainnoimalla todeta historiallisesta datasta, että täyttääkö lohkoketjuteknologia yleiskäyttöiselle teknologialle asetetut ehdot. Näin ollen varmuudella vastausta kysymykseen ”onko lohkoketjuteknologia seuraava yleiskäyttöinen teknologia?” on mahdotonta antaa tässä vaiheessa. Aiheesta tähän mennessä julkaistut tutkimukset kuitenkin viittaavat siihen, että lohkoketjuteknologia olisi sellainen – tai sillä ainakin olisi potentiaalia siihen. Lohkoketjuteknologia kasvattaa kokonaistuotantoa teknologisen kehityksen kautta tapahtuvan tuottavuuden parantumisen kautta.

Suurin ongelma uuden teknologian yleistymisessä on se, että aikaisen vaiheen adoptoijat joutuvat monesti ”maksamaan oppirahat” ja toimimaan ns. betatestaajina teknologialle. Monesti tämä näkyy niin kasvaneina kuluina kuin tuottavuudenkin kasvun alenemisena. Niinpä uusi teknologia monesti odottaa yhtä läpimurtotuotettansa tai -hittiänsä, jonka kautta se sitten lopulta leviää laajemmalle käyttöön. Tällaisen läpimurtotuotteen uskotaan tulevan lohkoketjuteknologian kohdalla finanssisektorilta, mutta tätä opinnäytettä tehdessä sellaista ei kuitenkaan vielä ollut ilmaantunut. Mikään ei tietenkään vaadi tai edellytä, että läpimurto tulee rahoitusmaailmasta, mutta se on tällä hetkellä toimiala, joka panostaa huomattavasti lohkoketjuteknologiaan. Kuitenkin lohkoketjuteknologian luonteen vuoksi eli sen transaktiokustannuksia alentavasta vaikutuksesta johtuen tämä läpimurtoala tai -tuote on mitä todennäköisimmin sellainen toimiala, jossa transaktiokustannukset ovat suuri ja huonosti käyttäjämääriin skaalautuva kustannuserä. Kuten edellä jo mainitsin, on lohkoketjuteknologian potentiaali sen teknologisista ominaispiirteistä huolimatta erityisesti prosessien parantamisessa ja tehostamisessa. Prosessin läpimenon tehostumiseksi tarvitaan tehokkuutta jokaiseen prosessin vaiheeseen. Niinpä on melko turvallista ennustaa, että tuottavuusloikka tulee vasta siinä vaiheessa, kun teknologia on levinnyt niin

laajalle, että sillä voidaan toteuttaa alusta loppuun kaikki prosessin eri vaiheet välivaiheineen ja ulkoisine liityntäkohtineen (nodes).

Tässä vaiheessa on kuitenkin mielestäni myöskin melko turvallista olettaa, että riippumatta siitä, minkä toimialan kautta lohkoketjuteknologia lyö läpi, ovat tulevaisuuden lohkoketjut teknisesti jotain muuta kuin tämän hetken ratkaisut tai ne, millaisiksi Nakamoto ne kymmenen vuotta sitten suunnitteli. Ajatusta voi verrata siihen, että 1800-luvun sähköteknologiset ratkaisut ovat varsin erilaisia kuin nykypäivän ratkaistut, mutta silti ne ovat edelleen tunnistettavissa samaksi teknologiaksi (GPT:n ehdot). Täytyy muistaa, että Nakamotolle lohkoketju oli vain keino päästä tavoitteeseen, eli varmentaa bitcoinien ja transaktioiden aitous. Sitä ei ollut tarkoitettu yleiskäyttöiseksi teknologiaksi tai tekemään yhtään mitään muutakaan, mitä luvussa viisi on esitelty lohkoketjuteknologian potentiaalisiksi tulevaisuuden lohkoketjusovellutuksiksi. Tämä onkin jo verrattain lyhyessä ajassa aiheuttanut monia ongelmia, joista yksi merkittävimmistä on transaktioiden varmentamisnopeus, tai siis pikemminkin niiden hitaus, ja ulkopuolisten hallitun pääsyn mahdollistavien rajapintojen puute. Tietynlaisesta likinäköisyydestä kielii myös lohkoketjuteknologian kannalta se, että bitcoineille asetetiin jo alusta alkaen enimmäismäärä, jonka täyteen tuleminen ajankohta on ollut alusta asti tiedossa.

Bitcoinin kilpailevana virtuaalivaluuttana onkin kehitetty vuonna 2015 Ethereum, jonka lohkoketjuteknologisissa ratkaisuissa on korjattu näitä puutteita. Ethereumista puhutaankin monesti arkikielessä ”lohkoketjuteknologia 2.0:na”. Ja aivan kulman takana odottaa jo esimerkiksi Icon ja muut ”lohkoketjuteknologia 3.0” -ratkaisut. Tarkoitus ei ole enää tutustua näihin teknologisiin kehitysaskeliin tarkemmin, vaan pelkästään havainnollistaa kuinka nopeaa kehitys on jo kymmenessä vuodessa ollut teknologialle, jolle ei ole vielä löydetty mitään varsinaista käyttökohdetta virtuaalivaluuttojen ulkopuolella. Proof of Work -pohjaisessa varmentamisessa on suurena ongelma valtava laskentatehon ja sähkönkulutuksen tarve (liite 2), sekä sen heikkous tulevaisuuden tietokoneita vastaan (liite1). Hieman ironisesti hajautettu systeemi on ajautunut vain harvojen käsiin, kun vain isoilla toimijoilla on varaa ja taloudellisia kannustimia harjoittaa Proof of Work -laskentaa. Tällä hetkellä kehitetään / on kehitetty vaihtoehtoisia varmentamisratkaisuja, joista Proof of Stake -varmentaminen on valmiimpia ratkaisu tällä hetkellä ja ehkäpä siitä syystä esillä julkisuudessa. Kuitenkaan menemättä yhtään syvemmälle tämän ratkaisun tekniseen toteutukseen kuin mitä luvussa kolme on jo esitetty, todettakoon vielä, että kyseinen ratkaisu on osaltaan saanut sen laatuista kritiikkiä, että Proof of Stake -laskennalla on tuskin tulevaisuutta, joten läpimurtoratkaisua joudumme vielä odottamaan.

Tämä lohkoketjuteknologian teknisen kehityksen muutosvauhti osoittaa toisaalta sen, että teknologia kehittyy ja reagoi nopeasti muuttuviin tarpeisiin. Mutta toisaalta jatkuvassa muutostilassa oleminen vaikeuttaa sen käyttöönottoa, sillä teknologia, jonka määritykset eivät ole vakiintuneet (standardoituneet) kärsii standardien puutteista käytännön jatkokehitysprojektien mahdottomuutena. Kuten yleisesti tiedämme, uusien työkalujen tai teknologioiden käyttöönotto

vaatii aina ensiksi työkalun / teknologian määrittelyn ja testaamisen ennen kuin se voidaan ottaa niin sanotusti tuotantoon. Riippuen projektin suuruudesta ja monimutkaisuudesta, määrittelyvaihe ja testaaminen voivat kestää hyvinkin pitkään. Tällöin erityisesti jatkuvassa muutoksessa oleva teknologia on projektin onnistumisen kannalta riski tai jopa mahdottomuus. Kun huomioon otetaan vielä digitalisaatioon muutenkin liittyvä ja mahdollistava huima innovointivauhti, täytyy läpimurtotuotteen olla todella ylivoimainen, jotta projektin riski jatkuvassa muutoksessa kannattaa ottaa.

Huomionarvoista on kuitenkin myös se, että yleiskäyttöisen teknologian ehtojen mukaisesti yleiskäyttöisen teknologian tulee kehittyä ajan kuluessa (ja alentaa käyttäjällensä aiheutuneita kustannuksia). Näin ollen edellisessä kappaleessa lausuttu ei tarkoita sitä, etteikö lohkoketjuteknologia saisi (ja pitäisi) kehittyä ajan kuluessa. Innovointi ja kehittyminen kulkevat monesti myös käsi kädessä sekä tukevat ja mahdollistavat toisiaan. Monesti jonkin tekniikan standardointiprosessissa oleellisena osana on tavoite siitä mitä standardoidun version pitäisi osata tehdä. Kun fokus tästä tavoitteesta on vielä hämärän peitossa ja lohkoketjuteknologiaa kehitetään suhteellisen lavealla tavoitteella: ”parempi kuin aiemmin”, niin on hyvinkin luonnollista, että teknologia hakee muutenkin muotoaan. Oleellista on siis se, että lohkoketjuteknologia tarvitsee raamit, tietokonetermein ”release candidate” -version, jota lähdetään yhdessä sovittujen määritysten pohjalta kehittämään eteenpäin. Tilanne on kuitenkin hieman erilainen kuin verrattuna esimerkiksi aiempaan yleiskäyttöiseen teknologiaan; tietokoneeseen. Se oli uusi teknologinen innovaatio, jolle keksittiin käytännön sovellutuksia sitä mukaan, kun sen potentiaalia ymmärrettiin ja tekniikan kehitys mahdollisti. Lohkoketjuteknologian kohdalla mielestäni teknologian potentiaali eli prosessien tehostumin ja transaktiokustannusten aleneminen kuitenkin ymmärretään melko hyvin jo valmiiksi ja tämän nyt vain odotetaan lohkoketjuteknologian teknologista kehittymistä vastaamaan paremmin näihin jo olemassa oleviin odotuksiin.

Jotta näihin lohkoketjuteknologian teknologisiin odotuksiin voitaisiin vastata, vaatii kaikkia toimialoja palvelevien raamien muodostaminen keskitetyn organisaation vetämään projektia ja olemaan siitä vastuussa. Kuten jo aiemmin mainittu, tämä on taas hieman ironisesti ideologisessa ristiriidassa koko lohkoketjuteknologian hajauttamisen ja keskushallinnon puutteen ajatuksen kanssa. Nykyinen tilanne, jossa jokainen toimija – tai yhteenliittymä, konsortio - kehittää omaa teknologiaansa, ei edistä yleiskäyttöisen teknologian ydinajatusta ”ihmiskuntaa eteenpäin vievänä suurena teknologisena harppauksena”. Vaan kyseessä on mitä todennäköisimmin selviytymistaistelu, jossa vahvin kehittäjäryhmä saa määrätä kehityksen suunnan riippumatta siitä, että onko ratkaisu teknologisesti kaikkein parhain ja universaalein sovellettavuudeltaan. Kuten Mattilakin (2016) toteaa: tekninen ylivertaisuus ei itsessään ole tae menestymiselle, vaan menestyäkseen lohkoketjuteknologia tarvitsee kysyntää, kilpailua ja tietotaitoa. Esimerkiksi tietokoneiden mikroprosessorit käyttävät edelleen Intelin 70-luvulla kehittämää x86-suoritinarkkitehtuuria, sillä Intel on de facto -suoritinvalmistajana saanut määrätä kehityksen suunnan. Monesti voidaan sanoa, että kilpailu tuottaa

parhaat innovaatiot, mutta lohkoketjuteknologian tapauksessa esimerkiksi finanssialan R3-konsortion tuote Cordana ei tarkalleen ottaen ole edes teknisesti puhdas lohkoketjuteknologia, vaan se on suljetun systeemin ja lohkoketjuteknologian hybridi. Se on varmasti finanssialan näkökulmasta teknisesti paras ratkaisu, mutta tässä tilanteessa se ei edistä uuden yleiskäyttöisen teknologian syntymistä.

Edellä mainitut seikat ja haasteet huomioiden on mahdotonta sanoa, tuleeko lohkoketjuteknologia olemaan seuraava yleiskäyttöinen teknologia. Sillä on valtavasti potentiaalia ollakseen sellainen ja se täyttää yleiskäyttöiselle teknologialle asetetut määritelmälliset tunnuspiirteet. Lisäksi lohkoketjuteknologia näyttää noudattavan Schumpeterilaisen kasvuteorian kaksivaiheista sykliä, jossa tuottavuus on alentunut niin kauan kuin työvoimaa kohdistetaan välituotteiden kehittämiseen ja että kyseinen yleiskäyttöinen teknologia saadaan implementoitua kokonaisvaltaisesti talouteen ja yhteiskuntaan. Mikäli lohkoketjuteknologia on yleiskäyttöinen teknologia, olemme tässä ensimmäisessä laskevan tuottavuuden vaiheessa, kylvön ajassa.

Lohkoketjuteknologian nykyisten teknisten ratkaisujen Proof of Work -laskenta on energiasyöppö lohkojen oikeellisuuden varmentamistapa, jolle ei voi nykyisenkaltaisena toteutuksena taloudellisten realiteettien valossa odottaa pitkää ikää. Kuitenkaan vielä ei ole esitetty uskottavaa vaihtoehtoa Proof of Work -laskennalle. Lohkoketjuteknologian yleistymistä hidastaa myöskin se, että todennäköisesti alun innovoinnit kohdistuvat juurikin prosessitehokkuuden parantamiseen eli lohkoketjuteknologian avulla monia jo olemassa olevia asioita voitaisiin tehdä transaktiokustannuksia pienentäen, ei siis aluksi välttämättä keksitä uusia asioita, synnytetä uusia markkinoita tai markkina-alustoja. Mutta ilman varsinaista hittiä, markkinoiden läpimurtotuotetta, jolla saataisiin lohkoketjuteknologia kaikkien huulille, voi lohkoketjuteknologia jäädä kaikesta kyvykkyydestään huolimatta historian unholaan. Nykyaikaisessa yhteiskunnassa ei enää riitä, että tuote / teknologia on hyvä, vaan sen pitää olla mahdollisimman tuottava heti alusta alkaen – asetelma, joka sotii yleiskäyttöisen teknologian alentuneen alkutuottavuuden tunnuspiirrettä vastaan. Sovellusinnovaatiota ehkäpä tärkeämpää on se, millaisia välituotteita kehitetään, joilla implementoidaan itse yleiskäyttöinen teknologia osaksi taloutta ja yhteiskuntaa.

LÄHTEET

Aghion, P., Akcigit, U., Howitt, P., 2013, What Do We Learn from Schumpeterian Growth Theory? Handbook of Economic Growth, 2014, Volume 2, 515–563.

Barrdear, J., 2014, Innovations in Payment Technologies and the Emergence of Digital Currencies. Bank of England, Quarterly Bulletin, 2014, Q3, Volume 54 No. 3, 262-272.

Basu, S., Fernald, J., 2006, Information and Communications Technology as a General-Purpose Technology: Evidence from U.S Industry Data. Federal Reserve Bank of San Francisco. Working Paper Series 2006-29.

Benet, J. 2018, IPFS – Content Addressed, Versioned, P2P File System (Draft 3).

Bentov, I., Gabizon, A., Mizrahi, A. 2016, Cryptocurrencies Without Proof of Work. In International Conference on Financial Cryptography and Data Security, Springer, 142–157 .

Bresnahan, T., Trajtenberg, M., 1995, General Purpose Technologies: Engines of Growth?. Journal of Econometrics, 65, 83–108.

Brown, R., Carlyle, J., Grigg, I., Hearn, M., 2016, Corda: An Introduction. Whitepaper.

Brynjolfsson, E., Rock, D. ja Syverson, C., 2018, The Productivity J-curve: How Intangibles Complement General Purpose Technologies, NBER WP no. 25148.

Catalini, C., Gans, J., 2016, Some Simple Economics of the Blockchain. MIT

Cummins, J., Violante, G., 2002, Investment Specific Technical Change in the United States (1947–2000): Measurement and Macroeconomic Consequences. Review of Economic Dynamics 5, Issue 2, 243–284.

Davidson, S., De Filippi, P., Potts, J., 2016a, Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology. SSRN Working Paper.

Davidson, S., De Filippi, P., Potts, J., 2016b, Economics of Blockchain. SSRN Working Paper.

de Vries, A., 2018, Bitcoin's Growing Energy Problem. Joule, Volume 2, Issue 5, 801 – 805.

Divesh, Gavin et al., 2017, Quantum Attacks on Bitcoin, and How to Protect Against Them.

Sinclair, D., De Filippi, P., Potts, J., 2016, Economics of Blockchain. School of Economics, Finance & Marketing, RMIT University.

Forest, H., Rose, D., 2015, Digitalisation and the Future of Commercial Banking, Deutche Bank.

Hayes, A., 2015, Cost of Production Model for Bitcoin. The New School for Social Research, Department of Economics, Working Paper 05/2015.

Hearn, M., Brown, R., 2016, Corda: A Distributed Ledger.

Helpman, E., Trajtenberg, M., 1994, General Purpose Technologies and Economic Growth, Helpman, E., ed., Cambridge: MIT Press, 1998.

Helpman, E., Trajtenberg, M., 1996, Diffusion of General Purpose Technologies, No 5773, NBER Working Papers, National Bureau of Economic Research, Inc.

Helpman, E., Trajtenberg, M., 1998, A Time to Sow and A Time to Reap: Growth Based on General Purpose Technologies. Helpman, E. (toim.) General Purpose Technologies and Economic Growth, MIT Press.

Hyytinen, A., 2019, Yleiskäyttöiset teknologiat ja koneoppiminen talouskasvun lähteenä. Teoksessa: Suomen kasvu – Mikä määrää tahdin muuttuvassa maailmassa?, Honkapohja, S., Vihriälä, V. (toim.), ETLA.

Iansiti, M., Lakhani, K., 2017, The Truth About Blockchain. Harward Business Review.

Kane, E., 2017, Is Blockchain a General Purpose Technology? School of Economics, Finance & Marketing, RMIT University.

Trautman, L., 2016, Is Disruptive Blockchain Technology the Future of Financial Services? The Consumer Finance Law Quarterly Report 232.

Jovanovic B., Rousseau P.L., 2005. General Purpose Technologies. Handbook of Economic Growth, Volume 1B. Aghion, P., Durlauf, S. (toim.).

Kapanen, H., Nordlund, S., 2016, Millä tavoin maksamme 2020-luvulla? Näkökulmia tulevaisuuden maksamisratkaisuihin. Suomen Pankin maksuneuvosto.

Lauslahti, K., Mattila, J., Seppälä, T., 2016, Älykäs sopimus – Miten blockchain muuttaa sopimuskäytäntöjä? ETLA Raportit No 57.

Lipsey, R., Carlaw, K., Clifford, B., 2005, Economic Transformations: General Purpose Technologies and Long Term Economic Growth. Oxford University Press.

Mattila, J., 2016, The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures. ETLA Working Papers No 38.

Mattila, J., Seppälä, T., Naucler, C., Stahl, R., Tikkanen, M., Bådenlid, A., Seppälä, J., 2016, Industrial Blockchain Pla orms: An Exercise in Use Case Development in the Energy Industry. ETLA Working Papers No 43.

McNamara, J., Stephens, P., Dall, S., Houston, A., 2009, Evolution of trust and trustworthiness: social awareness favours personality differences. Proceedings of the Royal Society of London B: Biological Sciences, 276(1657), 605–613.

Nakamoto, S., 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/en/bitcoin-paper.

Narayanan, A. Bonneau, J. Felten, E. Miller, A. Goldfeder, S. Clark, J., 2016, Bitcoin and cryptocurrency technologies.

Raskin, M., Yermack, D., 2016, Digital Currencies, Decentralized Ledgers, and the Future of Central Banking. NBER Working Paper No. 22238.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Roman, M., Hiller, J., Henze, M., Ziegeldorf, J., Müllmann, D., Hohlfeld, O., Wehrle, K., 2018, A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin.

Romer, P., 1994, The Origins of Endogenous Growth. Journal of Economic Perspectives, 8(1), 3-22.

Schollmeier, R., 2002, A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, Proceedings of the First International Conference on Peer-to-Peer Computing.

SÄHKÖISET LÄHTEET:

Bitcoin Wiki (2017): Scalability https://en.bitcoin.it/wiki/Scalability [Luettu 5.2.2017]

BitcoinAvarage (2016) https://bitcoinaverage.com/en/bitcoin-price/btc-to-usd [Luettu 25.11.2016]

Bloomberg (2018): Is Your Blockchain Business Doomed? https://www.bloomberg.com/news/articles/2018-03-22/is-your-blockchain- business-doomed [Luettu 26.5.2018]

Coindesk (2018): From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited/ [Luettu 21.3.2018]

Cryptocompare (2018): Mining Calculator https://www.cryptocompare.com/mining/calculator [Luettu 27.3.2018]

Ethereum (2018) https://www.ethereum.org [Luettu 26.3.2018]

Ethereum Homestead (2016): What is ethereum? http://ethdocs.org/en/latest/introduction/what-is-ethereum.html#a-next-generation-blockchain [Luettu 18.2.2017]

Finanssivalvonta (2018): Uusi maksupalveludirektiivi – Payment Services Directive, PSD2 http://www.finanssivalvonta.fi/fi/Saantely/Saantelyhankkeet/PSD2/Pages/Default.aspx [Luettu 3.5.2018]

Interpol (2018): INTERPOL cyber research identifies malware threat to virtual currencies https://www.interpol.int/News-and-media/News/2015/N2015-033 [Luettu 27.3.2018]

IPFS (2018) https://ipfs.io Luettu [27.3.2018]

Nashville Medical News Blog (2017): Blockchain Technology and Applications for Healthcare: A conversation with Kristen Johns https://nashvillemedicalnews.blog/2017/01/03/blockchain-technology-and-applications-for-healthcare-a-conversation-with-kristen-johns/ [Luettu 26.5.2018]

OP Media (2018): Pian osakekauppaa voi käydä listaamattomilla yrityksillä https://op.media/yrityselama/startupit/pian-osakekauppaa-voidaan-kayda-listaamattomilla-yrityksilla-543874d1c7c34f4a82f122976272e0b5?fbclid=IwAR2fsb6ZW5BglPfkV381ahVgiBoVcLFT99BBgedof8u8X86P4mKxx2Gjtrg [Luettu 22.11.2018]

Oracle (2016): The Benefits of Blockhain Across Industries http://www.oracle.com/us/corporate/profit/big-ideas/041316-siyer-2982371.html?utm_content=buffer1904a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer [Luettu 10.2.2017]

Tietosuojavaltuutetun toimisto (2018): Rekisteröidyn oikeudet https://tietosuoja.fi/rekisteroidyn-oikeudet [Luettu 26.5.2018]

Venture Skies (2016): Banking as a Service – what you need to know http://www.ventureskies.com/blog/banking-as-a-service-categorizing-the-services [Luettu 17.2.2017]

Visa (2015) http://visatechmatters.tumblr.com/post/108952718025/56582-transaction -messages-per-second [Luettu 5.2.2017]

LIITTEET

Liite1: Kvanttitietokoneet tulevaisuuden uhka lohkoketjuille?

Wikipedia toteaa kvanttitietokoneen olevan tietokone, joka perinteisten bittien (0 tai 1) sijaan hyödyntää kvanttitilojen superpositioita. Tällainen tietokone on huomattavasti nopeampi esimerkiksi salausavainten laskennassa kuin perinteinen tietokone. Kuten tässä luvussa jo aiemmin todettiin, voidaan lohkoketju väärentää vain ns. 51% -hyökkäyksen avulla, jossa väärentäjällä on hallussaan yli 50%:a verkon laskentakapasiteetista. Tällä hetkellä taloudellinen insentiivi on louhinnan eli Proof of Work -laskennan puolella, sillä louhintakapasiteettiin investoitujen laitteiden tuotto-odotus on parempi kuin lohkoketjua vastaan hyökkäämisestä odotettavissa oleva tuotto. Divesh ym. (2017) ovat kuitenkin tutkimuksessaan ”Quantum attacks on Bitcoin, and how to protect against them” esittäneet, että lohkoketjuteknologian turvallisuus on uhattuna, kun tulevaisuuden kvanttitietokoneet kehittyvät tarpeeksi.

Divesh ym. (2017) toteavat kuitenkin, että varsinainen Proof of Work -laskenta on toistaiseksi hyvinkin resilienttiä kvanttitietokoneita vastaan, sillä ”perinteisten tietokoneiden” suorittamassa louhinnassa käytetty ASIC-laskenta on todella nopeaa verrattuna tällä hetkellä suunnittelussa oleviin kvanttitietokoneisiin nähden. Teoriassa kvanttitietokoneet voisivat saavuttaa jopa 100 GHz:n porttinopeuden, mikä tarkoittaisi satakertaista Proof of Work -laskentatehoa nykyiseen teknologiaan nähden. Tämänkaltaiset kvanttitietokoneet eivät kuitenkaan todennäköisesti ole saatavilla aivan lähitulevaisuudessa, joten emme voi ennustaa, miten perinteiset tietokoneet skaalautuvat tulevaisuudessa, tai miten yleisiä kvanttitietokoneet ovat, eli ovatko kvanttitietokoneet tarpeeksi yleisiä, jotta niillä voitaisiin muodostaa kokonaisia lohkoketjuja.

Suurempi ongelma Divesh ym. (2017) mukaan on kuitenkin lohkojen louhinnassa luotu yksityinen salausavain. Jokaista lohkon julkista salausavainta vastaan on olemassa yksityinen salausavain, jotta voidaan tehdä Proof of Work -tarkastuslaskentaa. Kvanttitietokoneet pystyvät kuitenkin erittäin tehokkaasti laskemaan julkisesta salausavaimesta yksityisen salausavaimen. Esimerkiksi Bitcoinin tapauksessa lohkojen louhintanopeus on vakioitu 10 minuuttiin. Diveshin et al. mukaan kvanttitietokoneet saavuttavat tämän raja-arvon vuosikymmenessä, jolloin salausavaimet muuttuvat turvattomiksi. Kyseessä ei ole edellä esitetyn Proof of Work -laskennan kaltainen raa’an laskentatehon ongelma, vaan nykyinen kryptografinen menetelmä eli elliptisen käyrän digitaalisen allekirjoituksen algoritmi (Elliptic Curve Digital Signature Algorithm) vaarantaa kaikki nykyisin olemassa olevat salausavaimet.

Vaikka tässä työssä ei ole mielekästä lähteä arvailemaan kvanttitietokoneiden tulevaisuutta, on kuitenkin melko turvallista sanoa, että lohkoketjuteknologia on suuressa murroksessa, mikä itsessään haittaa lohkoketjujen käytännön

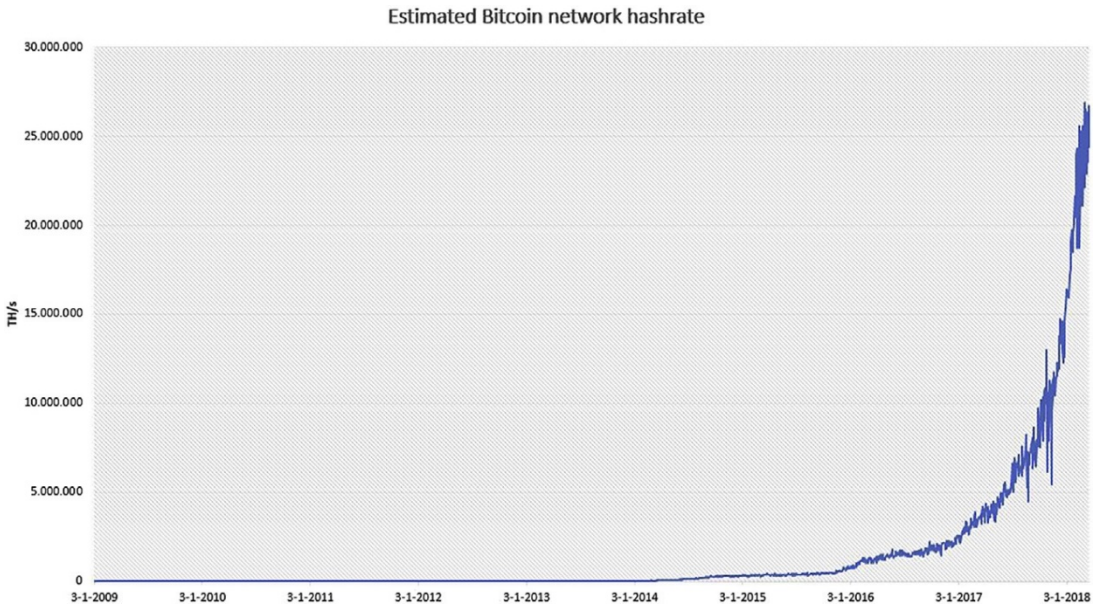
sovellutusten yleistymistä. Vaikka Divesh ym. esittivätkin tutkielmassaan ratkaisuja ongelman korjaamiseen, kuten laskennan vaikeustason nosto, Proof of Workin asymmetrisyys ja Proof of Workin siirtäminen muisti-intensiiviseksi, jolloin kvanttitietokoneen laskentanopeudesta ei ole hyötyä, vaativat nämäkin korjauskeinot täysin uudenlaisten lohkoketjujen luomista. Nykyisenkaltainen Bitcoinin tai Ethereumin lohkoketju on tällöin jo auttamattomasti vanhentunutta teknologiaa.

Liite 2: Sähkönkulutus on ongelma

Vaikka lohkoketjuteknologia itsessään mahdollistaa kolmannen osapuolen poistamisen yhtälöstä ja tätä kautta näennäisesti kuluttoman ratkaisun, täytyy muistaa, ettei teknologian taustalla oleva rauta (laskentayksiköt, palvelimet, tilat, sähkö jne.) ole missään nimessä ilmaista. Itseasiassa vaadittava laskentateho ja sähkönkulutus ovat tällä hetkellä valtavia ongelmia lohkoketjuteknologiaan perustuvien ratkaisujen kohdalla.

Hayes (2015) esitti, että Bitcoinien louhinta on yksinkertaisuudessaan laskevan rajatuotoksen funktio, jossa rajakustannuksen tulee kilpailluilla markkinoilla vastata myyntihintaa. Eli koska kustannukset ovat päivätasolla ilmaistuna dollaria ($) per päivä (d) ja tuotos taas Bitcoinia (BTC) per päivä (d), joten hintataso $/BTC on (kustannuksen per päivä) ja (BTC/d) suhde. Täten tasapainohintataso p* ($/BTC) on päivän sähkökustannus E jaettuna tuotannolla (BTC/d), eli p* = E / (BTC/d*). Sähkön kustannus päivätasolla taas määräytyy kWh-hinnan ja louhintakapasiteetin sähkönkulutuksen tulona. Kun markkinahinta laskee alle tasapainotason, poistuvat kannattamattomat louhijat verkosta. Täytyy muistaa, että kaikki louhintaan osallistuvat eivät saa louhintapalkkiota, vaan ainoastaan se, jonka louhima ketju verifioidaan lohkoketjun jatkoksi. Tämä taas kannustaa jatkuvasti panostamaan louhintakapasiteettiin. Tällä hetkellä tehokkaimpia louhijoita ovat ns. ASIC-louhintatietokoneet.

Alex de Vries on tutkimuksessaan ”Bitcoin’s Growing Energy Problem” (2018) ottanut lähtökohdaksi edellä esitetyn Hayesin tutkielman. Hayes kuitenkin jätti huomiotta louhintakapasiteettiin tarvittavat investoinnit ja keskittyi vain sähkönkulutukseen. Kuitenkin esimerkiksi Bitcoinin tapauksessa uusi lohko on vakioitu syntyväksi noin 10 minuutin välein, joten verkon laskentakapasiteetin kasvaessa, tarvitaan entistä tehokkaampia laskentayksiköitä. Kuitenkin on todettava, että sähkönkulutus on erittäin merkittävä tekijä lohkoketjujen kustannuksissa. Tällä hetkellä pelkästään Bitcoin lohkoketjuverkon on arvioitu kuluttavan 2,55 gigawattia sähköä tällä hetkellä ja mahdollisesti 7,67 GW vuoden 2018 loppuun mennessä. Vertailun vuoksi: Irlannin kuluttama sähköteho on keskimäärin 3,1 GW ja Itävallan 8,2 GW. Lohkoketjuteknologioiden Proof of Work -työ perustuu hash-arvojen laskemiseen. Hash-arvolla kuvataan sitä, kuinka monta SHA-256 laskentaa suoritetaan sekunnissa eli käytännössä lohkoketjuverkon laskentakapasiteettia.



Kuva 9: Bitcoin-verkon laskentavaatimusten kasvukäyrä (Lähde: de Vries, 2018)

Maaliskuun puolivälissä 2018 suoritettiin arviolta 26 kvintiljoonaa hash-laskentaoperaatiota sekunnissa jatkuvalla syötöllä. Samaan aikaan Bitcoin-verkko käsitteli vain 2-3 transaktiota per sekunti eli noin 200 000 transaktiota päivän aikana. Näillä luvuilla hash-laskennan suhdeluku oli jokaista käsiteltyä transaktiota kohden 8,7 kvintiljoonaa: 1. Tätä tehosuhteeltaan heikkoa verkostoa pidetään yllä massiivisella sähkönkulutuksella. Alla olevissa taulukoissa de Vries esittelee tämän hetken tehokkaimpia hash-laskentaa erikoistuneita ASIC-tietokoneita ja laskee niistä tehokkaimman Antminerin eli S9:n kustannukset 1, 1,5 ja 2 vuoden pitoajalla. Huomionarvoista on, että kyseinen Antminer S9 suoriutuu 14 Terahash-operaatiosta sekunnissa, kun pelkästään Bitcoin-verkon laskentateho oli maaliskuun puolivälissä 2018 26 kvintiljoonaa hash-operaatiota sekunnissa. (de Vries, 2018).

Tietokone	Hashrate (TH/s)	Sähkönkulutus (W)	Energiatehokkuus (J/GH)
Antminer S9	14	1372	0,098
Antminer T9	12,5	1576	0,126
Antminer T9+	10,50	1332	0,127
Antminer V9	4	1027	0,257
Antimner S7	4,73	1293	0,273
AvalonMiner 821	11	1200	0,109
AvalonMiner 761	8,8	1320	0,150
AvalonMiner 741	7,3	1150	0,160
Bitfury B8 Black	55	5600	0,11
Bitfury B8	47	6400	0,13

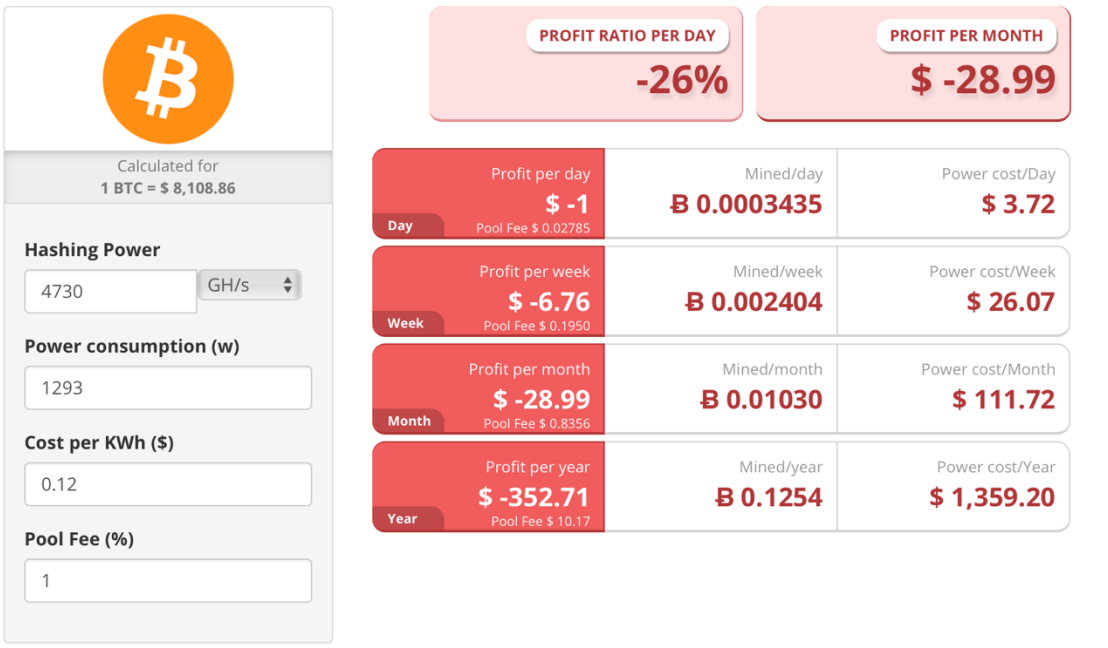
Taulukko 7: Esimerkkejä saatavilla olevista ASIC-louhijoista (Lähde: de Vries, 2018)

Tietokone	Antminer S9	Antminer S9	Antminer S9
Oletettu käyttöikä vuosina	2	1,5	1
Arvioitu tuotanto-kustannus ($)	500	500	500
Elinkaaren sähkönkulutus (kWh)	24037	18028	12019
Elinkaaren sähkön kustannus ($)	1202	901	601
Elinkaaren kokonaiskustannukset	1702	1401	1101
Sähkön kustannus / kokonaiskust.	70,6	64,3	54,6

Taulukko 8: Esimerkkilaskelma Antminer S9 -ASIC-louhijan elinkaarikustannuksista (Lähde: de Vries, 2018)

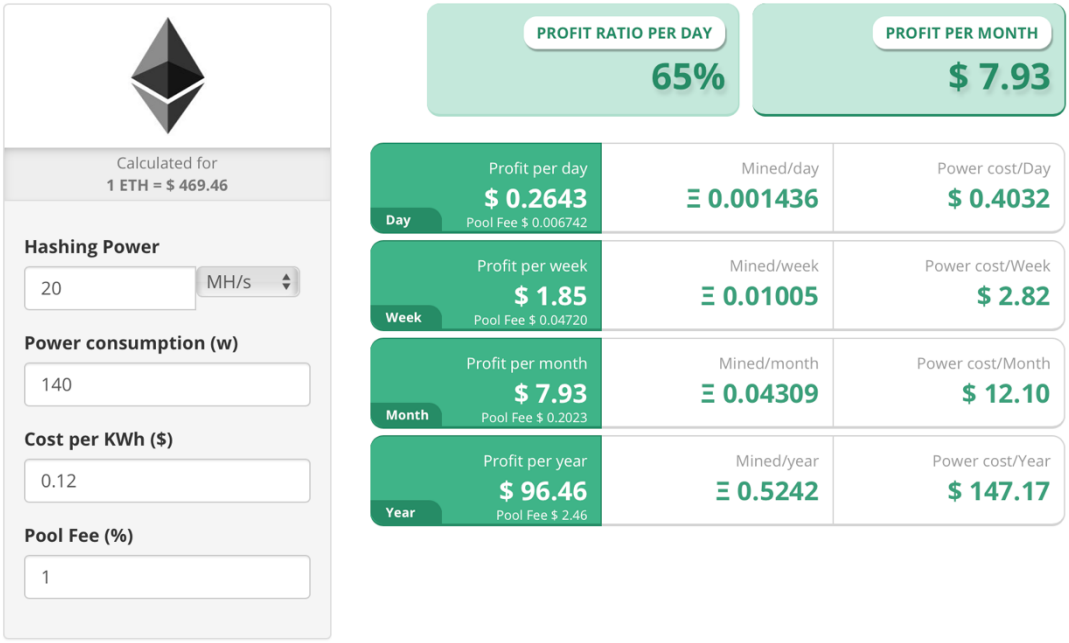
Kaiken kattavaa kululaskelmaa on täysin mahdotonta antaa, mutta yllä olevan taulukon mukaisesti sähkönkulutuksen kustannus on joka tapauksessa huomattava laiteinvestointeihin nähden. Kuitenkaan laiteinvestointeja ei voi jättää huomiotta, mikä on aiheuttanut sen, että Bitcoinin ja monen muun kryptovaluutan tapauksessa louhinta on keskittynyt serverifarmeille. Mikäli markkinahinta laskee alle tasapainohinnan, on monella serverifarmilla käsissään kannattamaton valtava laiteinvestointi.

Kun puhutaan taas ”tavallisten ihmisten” osallistumisesta louhintaan, on alla esimerkkeinä otettu kaksi tapausta (Bitcoin ja Ether). Cryptocompare.com-sivuston esimerkkilaskurista saatuja tuloksia vuoden 2018 maaliskuun 27. arvoilla Bitcoinin ja Etherin kannattavuuksista. Arvot perustuvat Bitcoinin ja Etherin noteerattuihin kursseihin ja kummankin kryptovaluutan edellyttämään laskennalliseen hash-arvoon (hash rate) suhteutettuna koko verkon laskentakapasiteettiin. Bitcoinin ja Etherin kovin erilaiset arvot johtuvat siitä, että ne käyttävät erilaista lohkoketjuteknologiaa ja siinä missä uuden lohkon luomisintervalli Bitcoinissa on 10 minuuttia, on se Etherissä vain 15 sekuntia. Lisäksi, kuten yllä olevasta kuvasta numero 11 näkee, on Bitcoinin hash-arvo kasvava käyrä, joten tulevaisuudessa myös Etherin vaatima laskentateho nousee, mikäli Etherin markkinahinta on tasapainohintaa korkeampi. Kuvista voi kuitenkin tehdä sellaisen johtopäätöksen edellä esitettyjen tietojen valossa, että Bitcoin ei ole enää kannattavaa toimintaa kuluttajille. Tämän vahvistaa myös uutiset Bitcoinin louhinnan keskittymisestä serverifarmeille. Tuskin joudumme kovinkaan kauaa odottamaan, että Ether siirtyy myös skaalaetujen vuoksi farmien louhittaviksi. Mikäli trendi on kaikkien lohkoketjuvaluuttojen kannalta tämänkaltainen, ei välttämättä louhintapalkkio ole tulevaisuuden lohkoketjuteknologiassa se insentiivi, joka tarvitaan kyseisen teknologian läpimurtoon ja tätä kautta saavuttaakseen yleiskäyttöisen teknologian aseman.



Kuva 10: Esimerkkilaskelma Bitcoinin kannattavuudesta (Lähde: Cryptocompare, 2018)

Kuvan 8 esimerkkilaskelmassa louhinnan arvot perustuvat seuraaviin parametreihin: verkon hash-rate on 24 786 222 093 GH/s ja Bitcoinin ja US-dollarin vaihtosuhde on 1BTC = $ 8108,86. Lohkon palkkiotaso on tällä hetkellä kiinteä 12,5 Bitcoinia jokaista uutta luotua lohkoa kohden, eikä laskelmassa ole otettu huomioon tulevaisuudessa tapahtuvaa palkkion puolittumista. Keskimääräinen laskenta-aika uudelle lohkolle on 600 sekuntia. Sähkön hinta on laskettu käyttämällä arvoa $ 0,12 / kWh. Koska Bitcoinin kurssi elää jatkuvasti ja verkon laskentateho kasvaa, on esimerkkilaskelman tulos kuvaus vain tietysti ajanhetkestä (27.3.2018) ja näin ollen vain suuntaa antava. Syksyllä 2018 Bitcoinin arvo oli laskenut huomattavasti ja samaan aikaan verkon laskentakyky kasvanut, mikä tarkoittaa entistä heikompaa louhinnan kannattavuutta. (Cryptocompare 2018).



Kuva 11: Esimerkkilaskelma Etherin kannattavuudesta (Lähde: Cryptocompare, 2018)

Kuvan 9 esimerkkilaskelmassa louhinnan arvot perustuvat seuraaviin parametreihin: verkon hash-rate on 240 639 GH/s ja Ethereumin ja US-dollarin vaihtosuhde on 1ETH = $ 469,46. Lohkon palkkiotaso on tällä hetkellä kiinteä 3 Ethereumia jokaista uutta luotua lohkoa kohden, eikä laskelmassa ole otettu huomioon tulevaisuudessa tapahtuvaa palkkion vähenemistä. Keskimääräinen laskenta-aika uudelle lohkolle on 15 sekuntia. Sähkön hinta on laskettu käyttämällä arvoa $ 0,12 / kWh. Koska Ethereumin kurssi elää jatkuvasti ja verkon laskentateho kasvaa, on esimerkkilaskelman tulos kuvaus vain tietysti ajanhetkestä (27.3.2018) ja näin ollen vain suuntaa antava. Syksyllä 2018 Ethereumin arvo oli laskenut huomattavasti ja samaan aikaan verkon laskentakyky kasvanut, mikä tarkoittaa entistä heikompaa louhinnan kannattavuutta. (Cryptocompare 2018).

Vaikka yllä olevia taulukoita ei voi yleistää koskemaan kaikkea lohkoketjuteknologiaa, kuvaavat ne hyvin sitä, että tilanteissa, jossa ei ole rahallisia kannustimia louhintaan, on lohkoketjuteknologia kaikkea muuta kuin ilmaista käyttää. Kuten taulukoista pystyy päättelemään, pienetkin nousut sähkönkulutuksessa ja sähkön hinnassa vaikuttavat merkittävästi louhinnan kannattavuuteen. Sähkön hintaan kuluttaja voi vaikuttaa vain pienissä määrin, mutta toisaalta jatkuva sähköntarpeen lisääntymien (kysyntä) nostaa talousteorioiden perusteella sähkön tasapainohintaa. Lisäksi lohkoketjuteknologian keskeisimpiä ideoita on proof-of-work -laskenta, mikä tarkoittaa aina 51% laskentatehoa lohkojen varmentamiseen, jotta ne ovat turvallisia ja luotettavia. Kun verkon kokonaislaskentateho eli hash rate -kasvaa, vaaditaan verkkoon kytketyiltä laitteita entistä korkeampaa laskentatehoa. Tämä taas on suoraan verrannollinen sähkönkulutuksen kasvuun ja laskentatehon kasvattamiseen tarvittaviin investointeihin. Vastaavasti kasvava hinta monesti vähentää puolestaan kysyntää, jolloin lyhyellä aikavälillä investointeja ovat valmiita tekemään ne, jotka ovat valmiita maksamaan kalliimman

hinnan. Tätä päätelmäketjua myöten louhiminen taas keskittyy ammattimaisten louhijoiden / serverifarmien käsiin, mikä omalta osaltaan puhuu sen puolesta, ettei louhintapalkkiot välttämättä ole lohkoketjuteknologian yleistymisen kannalta paras tapa palkita lohkoketjun louhintaan osallistumisesta silloin, kun halutaan laajentaa lohkoketjuteknologiaa muihinkin toimintoihin kuin kryptovaluuttoihin.

Liite 3: Euroopan Unionin tietosuoja-asetus, GDPR

Toukokuun lopulla 2018 koko Euroopan Unionin astui kahden vuoden siirtymäajan jälkeen voimaan uusi tietosuoja-asetus (EU 2016/679), joka radikaalilla tavalla uudistaa kuluttajan tietosuojaa ja oikeutta omiin tietoihinsa. Asetuksesta käytetään varsinkin julkisuudessa paljon sen englanninkielistä lyhennettä GDPR – General Data Protection Regulation. Asetus laajentaa käsitettä siitä, mikä on henkilötieto koskemaan kaikkea sitä tietoa, mistä henkilö on tunnistettavissa. ”Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero, sijaintitiedot ja isovanhempien perinnöllisiä sairauksia koskevat tiedot” (Tietosuojavaltuutetun toimisto). Tämä tarkoittaa sitä, että suurella todennäköisyydellä lohkoketju saattaa sisältää henkilötietoja, jolloin se kuuluu GDPR-sääntelyn piiriin. Bloombergille (2018) antamassaan haastattelussa Oxfordin yliopiston EU-oikeuden luennoitsija Michèle Finck toteaa, että lohkoketjuteknologia on nykymuodossaan epäyhteensopiva GDPR-sääntelyn kanssa.

GDPR tuo mukanaan kuluttajalle paljon oikeuksia sitä tahoa kohtaan, joka käsittelee hänen henkilötietojaan, eli rekisterinpitäjää kohtaan. Hajautetussa lohkoketjuteknologiassa ensimmäinen ongelma syntyy jo siinä, että rekisterinpitäjä saattaa olla vaikea nimetä. Jos rekisterinpitäjä kuitenkin pystytään osoittamaan ja lohkoketjuteknologia sisältää henkilötietoja, on rekisterinpitäjällä ankaran sakkorangaistuksen uhalla velvollisuus tarjota kuluttajalle seuraavat GDPR:n suomat oikeudet (Tietosuojavaltuutetun toimisto):

Henkilöllä on oikeus

- saada tietoa henkilötietojensa käsittelystä
- saada pääsy tietoihin
- oikaista tietoja
- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi

Lisäksi rekisterinpitäjän vastuulla on, että henkilötietojen käsittelyssä noudatetaan aina tietosuojalainsäädännön mukaisia tietosuojaperiaatteita (Tietosuojavaltuutetun toimisto):

Tietosuojaperiaatteiden mukaan henkilötietoja on

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

GDPR-sääntely on ollut voimassa vasta niin lyhyen aikaa, ettei käytännön esimerkkejä vielä ole siitä, miten viranomaiset tulkitsevat sääntelyä. Lain tavoite on kuitenkin selkeä: vahvistaa kuluttajan oikeuksia omiin tietoihinsa ja heikentää rekisterinpitäjän valtaa näihin tietoihin. Teknisesti tarkasteltuna GDPR-sääntelyyn on helppo mukautua niissä vaatimuksissa, jotka kohdistuvat olemassa olevan tiedon tarkasteluun, siirtämiseen tai läpinäkyvään käsittelyyn ja keräämiseen. Lohkoketjuteknologia itsessään tukee jo monilta osin näitä periaatteita avoimuutensa puolesta. Ja lohkoketjussa ajettavat sovellukset voidaan tehdä keräämään vain sellaista tietoa ja siinä määrin, että tietosuojasääntelyä noudatetaan.

Ongelma syntyykin tietosuoja-asetuksen vaatimuksista, jotka edellyttävät jo louhitun tiedon muokkaamista tai poistamista. Nimittäin, kuten jo monesti todettu, lohkoketjuteknologian perusperiaate, tietojen jälkikäteisen muokkaamisen mahdottomuus, estää tietojen jälkikäteisen oikaisun tai poistamisen. Lisäksi mikäli tieto on jo päätynyt osaksi lohkoketjua, sen jälkikäteinen rajoittaminenkin tai jopa tiedonkäsittelyn kokonaan vastustaminen saattaa varsinkin avointen lohkoketjujen tapauksessa olla täysin mahdotonta, sillä avoimuuden takia mikään ei estä käyttämästä jo lohkoon päätynyttä tietoa, johon on annettu lupa lohkon luomisen hetkellä. Kuluttajan oikeus olla joutumatta automaattisen päätöksenteon kohteeksi on yhtä ongelmallinen, sillä esimerkiksi älysopimukset perustuvat juurikin loppuun asti menevään automaatioon. Ja kun lohko on luotu, manuaalisella uudelleenkäsittelyllä ei ole enää merkitystä. Ja vaikka oletettaisiin, että uudelleenkäsittely on teknisesti mahdollista, alati kasvavassa ja laajenevassa lohkojen ketjussa tällainen manuaalityö ei olisi edes millään tavalla lohkoketjujen funktiot

huomioon ottaen mielekästä tai käytännössä mahdollista. Louhintanopeus voi nimittäin olla nopeimmillaan sekunteja ja tällaisessa tahdissa ihmisen manuaalinen puuttuminen käytännössä tarkoittaisi sitä, että uusien lohkojen luonti pitäisi keskeyttää manuaalikäsittelyn ajaksi. Käytännössä tarpeeksi monella oikaisuvaatimuksella lohkoketju voitaisiin pysäyttää loputtomaksi aikaa. Mikäli lohkoketjuteknologiaan tehtäisiin sellaisia teknisiä ratkaisuja, jotka taipuvat GDPR-sääntelyn muottiin, niin tällainen ratkaisu ei mielestäni enää ole lohkoketju siinä merkityksessä, mistä lohkoketjuista yleisesti ottaen puhutaan.

Euroopan Unionissa asuu yli puoli miljardia ihmistä ja se on maailman mittakaavassa yksi suurimmista talousalueista, joten GDPR-sääntelyllä on jo nyt ollut huomattavia globaaleja vaikutuksia. Yritykset eivät voi toimia Euroopan talousalueella, elleivät ne alistu EU-sääntelyyn. Tämän vuoksi käytännössä kaikki globaalit yritykset ainakin jossain määrin noudattavat GDPR-sääntelyä (tai jos eivät noudata, ne poistuvat eurooppalaisten kuluttajien saatavilta, kuten joidenkin amerikkalaisten verkkosanomalehtien kohdalla kävi sääntelyn astuttua voimaan). Tämä taas ohjaa yrityksiä tekemään investointeja, jotka ovat niille kannattavia koko toiminnan mittakaavassa. Mikäli EU:n kokoinen markkina toteaa, että jokin lohkoketjuteknologiaan perustuva sovellus rikkoo sen laidansääntöä, globaali yritys tuskin investoi tällaiseen teknologiaan. Yleiskäyttöinen teknologia lähtee yleensä leviämään yhden läpimurtotuotteen kautta. Nyt, kun yritykset GDPR-lainsäädännön takia joutuvat olemaan lohkoketjuteknologian kanssa varovaisia, kasvaa riski sille, ettei markkina näe lähiaikoina lohkoketjuteknologiaan perustuvaa läpimurtosovellusta - ellei lohkoketjuteknologian teknisissä ratkaisuissa taikka GDPR-asetuksessa tai sen soveltamisalassa tapahdu jotain mullistavaa.