Olli Soininen

LOHKOKETJUTEKNOLOGIAN HAASTEET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Soininen, Olli
Lohkoketjuteknologian haasteet
Jyväskylä: Jyväskylän yliopisto, 2020, 20 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Kollanus, Sami; Kyppö, Jorma

Lohkoketjuteknologia on herättänyt ympärilleen suurta hehkutusta. Teknologia on ilmiönä uusi ja sen on sanottu olevan suurin juttu sitten internetin. Julkisuuteen lohkoketjuteknologia on noussut enimmäkseen kryptovaluuttojen, kuten Bitcoinin, suuren taloudellisen arvon nousun myötä. Lohkoketjuteknologia on kuitenkin itsessään kryptovaluuttoja suurempi kokonaisuus, joka mahdollistaa eri asioiden tekemisen uudella tavalla. Koska lohkoketjuteknologia on ilmiönä tuore, sillä on haasteita edessään, sekä teknologian sisäisiä että ulkoisia, jotka täytyy ratkaista ennen teknologian laajempaa käyttöönottoa. Tässä tutkielmassa käydään läpi, kuinka lohkoketjuteknologia käytännössä rakentuu, sisäiset haasteet, kuten haavoittuvuus ja skaalautuvuus sekä ulkoiset haasteet, esimerkiksi lakisääteiset asiat. Tutkielma on toteutettu kirjallisuuskatsauksena.

Asiasanat: lohkoketjuteknologia, haasteet, GDPR, Bitcoin, Ethereum

ABSTRACT

Soininen, Olli
The issues blockchain technology is facing
Jyväskylä: University of Jyväskylä, 2020, 20 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Kollanus, Sami; Kyppö, Jorma

Blockchain technology has created a big hype around itself. Technology is a new phenomenon and it is said that it's the next big thing since the internet. Blockchain technology has gained publicity mostly due to cryptocurrencies, such as Bitcoin, and their increased economic value. Blockchain as a technology is far greater than only the cryptocurrencies, which allows us to do many things in a whole new way. Because the technology as a phenomenon is a new one, it faces many challenges, both internal and external, which must be resolved before a greater implementation of the technology. This thesis will review how blockchain technology practically consists of, the internal issues such as vulnerabilities ja scalability and the external issues for example legal challenges. The thesis was done as a literature review.

Keywords: blockchain technology, challenges, GDPR, Bitcoin, Ethereum

KUVIOT

SISÄLLYS

1 JOHDANTO

Lohkoketjuteknologia sai alkunsa Bitcoinin anonyyminä pysyneen perustajan tai perustajaryhmän, Satoshi Nakamoton (2008), julkaisusta. Kyseessä oli ensimmäinen lohkoketjuteknologiaan liittyvä julkaisu, jonka päälle Bitcoin on rakennettu. Bitcoin on kryptovaluutta, joka toimii mm. maksuvälineenä esimerkiksi joissain verkkokaupoissa. Bitcoinin rahaan verrattavan arvon nousun myötä teknologian ympärille kasvoi suuri mielenkiinto sekä tutkimus- että sijoituskohteena. Lohkoketjuteknologia pitää sisällään kuitenkin paljon muutakin, kuin kryptovaluutat. Teknologian sanotaan kykenevän mullistamaan internetin ja myötävaikuttamaan useilla aloilla, kuten julkisella sektorilla, esineiden internetissä ja pankkitoiminnassa (A. Balaskas & V. N. L. Franqueira, 2018).

Bitcoin-ilmiön myötä tutkimuksia lohkoketjuista on tullut satoja muutaman vuoden sisällä. Tämä tutkielma on tehty kirjallisuuskatsauksena ilmiön myötä syntyneistä lähteistä. Lähteitä on etsitty Google Scholarista sekä IEEE:n tietokannasta. Lähteiden arvosteluun on vaikuttanut viittausten määrä ja julkaisufoorumista tarkastettu julkaisijan laatuarviointi. Lähteiden valikoinnissa on myös tarkasteltu julkaisun tutkimukseen perustuvaa näkökulmaa. Lohkoketjuteknologiasta ilmestyneistä lähteistä suuri osa on konferenssijulkaisuja, ja näissäkin tutkielmassa viitataan jo todistettuihin asioihin, kuten olemassa olevaan teknologiaan ja lakipykäliin.

Tutkielma pyrkii vastaamaan seuraavaan kysymykseen: ”Mitä haasteita lohkoketjuteknologialla on edessään ennen laajempaa käyttöönottoa?” Motiivina tutkimukseen on lohkoketjuteknologian potentiaali. Kuten Balaskas ym. (2018) mainitsivat, on teknologialla mahdollisuus mullistaa useaa eri alaa. Siksi on tärkeää ymmärtää, tämänhetkiset ongelmat ja haasteet, jotta lohkoketjuteknologia voi kehittyä oikeaan suuntaan ja toimia apuvälineenä usean yrityksen ja toimijan arjessa. Tällä hetkellä lohkoketjut ovat pyörineet suurimmissa osin omien kryptovaluuttojensa ympärillä.

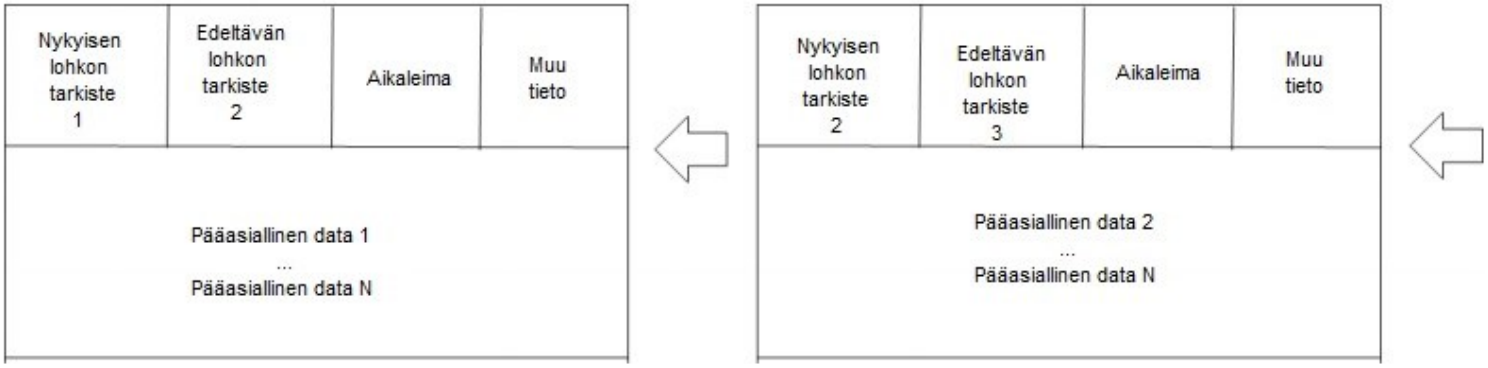
Jotta tutkimuskysymykseen saisi mahdollisimman ymmärrettävän ratkaisun, on tiedettävä mikä on lohkoketjuteknologia ja kuinka se käytännössä rakentuu. Tästä syystä tutkielman alussa, luvussa 2, käydään läpi, kuinka lohkoketjuteknologia käytännössä rakentuu ja mitä se pitää sisällään. On tärkeää ymmärtää,

kuinka teknologia toimii haasteiden hahmottamiseksi. Luvuissa 3 ja 4 tarkastellaan tutkimuskysymykseen vastaavia eri haasteita. Luvussa 3 tarkastellaan teknologian sisäisiä pulmia, kuten eri haavoittuvaisuuksia ja skaalautuvuusongelmaa. Luvussa 4 puolestaan ulkoisia haasteita, kuten lakiasioita ja kryptovaluuttamarkkinoiden aaltoilevuutta bitcoinin näkökulmasta. Luku 5 on yhteenvetokappale, jossa käydään läpi, mitä tutkielma on pitänyt sisällään.

2 LOHKOKETJU

Lohkoketjut voivat toimia toisistaan eri tavalla. Tutkielmassa tarkastellaan lohkoketjua pääosin Bitcoinin näkökulmasta, koska sitä varten Nakamoto (Nakamoto, 2008) sen alun perin julkaisi. Lohkoketju on nimensä mukaisesti kasa tai ketju lohkoja. Jokaiseen lohkoon on tallennettu kyseisen sekä edeltävän lohkon tarkisteet (engl. hash), aikaleima ja vaihteleva määrä yleistä dataa (S. Singh & N. Singh, 2016). Se on ikään kuin tilikirja, joka on turvallinen, läpinäkyvä ja todistettava ja rakentuu käyttäjältä käyttäjälle hajautettuun vertaisverkkoon. Hyötynä tässä, verrattavissa olemassa oleviin teknologioihin, on se, että käyttäjät voivat tehdä transaktioita keskenään ilman kolmatta osapuolta. (M. Dabbagh, M. Sookhak, & N. S. Safa, 2019). Itse vertaisverkko rakentuu palvelimista, eli solmuista. Käytännössä ketju toimii seuraavasti: lähettävä solmu tallettaa uutta dataa ja lähettää sen verkolle. Vastaanottava solmu tarkistaa tiedon oikeellisuuden ja lisää sen lohkoon. Tämän jälkeen kaikki vastaanottavat käyttäjät, eli louhijat, verkossa suorittavat joko Proof of Work (PoW) tai Proof of Stake (PoS) algoritmin lohkolle. Näiden algoritmien ansiosta varmistetaan, että ketjussa säilyy konsensus, eli yhteisymmärrys. Algoritmien suorittamista kutsutaan louhimiseksi. Louhimista suorittavat käyttäjät palkitaan osalla uudesta syntyneestä bitcoinista. Kun algoritmit on suoritettu ja yhteisymmärrys säilyy, lohko lisätään ketjun jatkoksi ja solmut jatkavat lohkoketjun kasvattamista tästä uudesta syntyneestä lohkosta. (Lin & Liao, 2017). Kuviossa 1 on havainnollistettu lohkoketjun rakennetta.

Pierro (M. D. Pierro, 2017) avaa lohkoketjua, lohkoja ja niiden transaktioita asuntokauppavertauksella. Asuntokaupoissa, kuten lohkoketjussa, tapahtumat jäävät ylös rekistereihin. Tieto omistuksista ja transaktioista tallennetaan yhteen luotettavaan tilikirjaan. Ongelmana tässä kuitenkin on se, ettei yksi keskitetty tilikirja välttämättä pysty vastaamaan useaan samanaikaiseen transaktioon ja edellyttää luottamusta tilikirjan ylläpitäjään. Pierro sanookin, että Nakamoto ratkaisee lohkoketjuteknologialla luottamuskysymyksen, kun tilikirjalla ei olekaan keskitettyä ylläpitäjää vaan se on hajautettu kaikkien ketjussa mukana olevien käyttäjien ylläpidettäväksi, joissa useampi toimija vahtii ketjun oikeellisuutta ja pystyy varmistamaan transaktiot ja ettei niitä ole koitettu vääristää. (M. D. Pierro, 2017).



Kuva 1 Lohkoketjun rakenne (Lin & Liao, 2017)

Lohkoketjun perusominaisuuksiin kuuluu jo aiemmin mainitut hajautettu vertaisverkko, läpinäkyvyys ja niiden lisäksi avoin lähdekoodi, autonomisuus, muuttumattomuus ja anonyymius. Hajautetun verkon hyötynä on, että jokainen verkossa toimiva solmu pystyy tallettamaan ja päivittämään tietoa ketjuun, eikä käyttäjien tarvitse luottaa vain yhteen keskitettyyn toimijaan. Hajautettu verkko tuo mukanaan myös ketjun autonomisuuden: koska ketju perustuu konsensuksen säilyttämiseen, käyttäjät luottavat vain yhden hallitsevan solmun sijaan koko ketjuun. Ketjulla ja sen käyttäjillä on siis vakiintunut itsehallinto, eikä tarvetta päättävälle elimelle ole. Läpinäkyvyyden hyötynä on, että kaikki ketjuun päivittyvä data on käyttäjien nähtävillä, joka nostaa luotettavuutta. (Lin & Liao, 2017)

Avoin lähdekoodi mahdollistaa ketjuun liittymisen kaikille. Jokainen teknologiasta kiinnostunut voi tarkistaa rekisteriä julkisesti ja käyttää lohkoketjua esimerkiksi omien sovelluksien kehittämiseen. Muuttumattomuudella viitataan siihen, että kaikki merkinnät ketjuun on tallennettu sinne lopullisesti, eikä niitä pystytä vaihtamaan. Muuttumattomuuteen liittyy yksi haavoittuvuus, 51 prosentin hyökkäys, mutta siitä lisää seuraavassa luvussa. Viimeinen perusominaisuus on anonyymius ketjussa. Koska ketju itsessään ratkaisee luotettavuuteen liittyvät ongelmat, ketjussa voi siirtää dataa tai tehdä transaktiot täysin anonyymisti. Ainoa asia, joka käyttäjien tarvitsee tietää, on henkilön osoite lohkoketjussa. Osoite lohkoketjussa on osa henkilön yleisavainta, joka toimii tunnistimena ketjussa. (Lin & Liao, 2017)

2.1 Louhimisalgoritmit (Proof of Work ja Proof of Stake)

Lohkoketjuissa louhiminen tapahtuu algoritmien läpikäymisellä tietokoneella. Proof of Workin (PoW) Bitcoinin tapauksessa louhijat laskevat edeltävän lohkon tiivisteen arvoa. Kun joku solmuista saavuttaa löytää tiivisteen kohdearvon, se lähettää sen muille lohkoille varmennettavaksi. Jos lohko on varmennettu, muut louhijat lisäävät tämän uuden lohkon osaksi lohkoketjuaan. Solmuja, jotka

suorittavat louhimista, kutsutaan louhijoiksi, ja algoritmin suorittamista louhimiseksi. (Z. Zheng, S. Xie, H. Dai, X. Chen, & H. Wang, 2017).

Proof of Stake (PoS) on energiaystävällisempi vaihtoehto Proof of Workiin nähden. Kyseisessä toimenpiteessä louhijoiden on todistettava kryptovaluutan omistajuus. Kuluttaessaan vähemmän energiaa, PoS on alttiimpi hyökkäyksille louhimiskulujen ollessa lähellä nollaa. Eri kryptovaluutat käyttävät erilaisia implementaatioita Proof of Stakesta, ja sen ollessa tehokkaampi vaihtoehto, moni lohkoketju aloittaa PoW:llä, vaihtaen asteittain kohti PoS:a. (Z. Zheng et al., 2017).

2.2 Älysopimukset

Toinen suosituksi lohkoketjuksi Bitcoinin kanssa on noussut Ethereum. Ethereum julkaistiin Woodin (Wood, 2014) julkaisussa Ethereum: A secure decentralised generalised transaction ledger. Siinä missä Bitcoinin transaktiot liittyvät lähinnä bitcoinien liikkumista paikasta A paikkaan B, esimerkiksi käyttäjän lompakosta toisen käyttäjän lompakkoon, Ethereumissa transaktioihin liittyy älysopimukset: niiden luonti ja niiden perintä. (G. Destefanis et al., 2018).

Älysopimuksia on ollut olemassa jo vuodesta 1997 lähtien. Esimerkki älysopimuksesta on esimerkiksi joukkorahoituskampanja. Älysopimus tallettaa kampanjan tukijan lahjoituksen ja jos kampanjan tavoite täyttyy, siirtää älysopimus rahat joukkorahoitusprojektille. Lohkoketjujen julkaisun myötä älysopimuksia voidaan toteuttaa sen avulla. Käytännössä kyseessä on siis sopimus osapuolien välillä, jonka ehdot tietokoneohjelma toteuttaa. Ethereum-älysopimus tallentuu lohkoketjuun sopimusta luodessa. Se koostuu omasta muististaan sekä määrästä kryptovaluuttaa, joka sopimukseen on asetettu. (G. Destefanis et al., 2018; K. Christidis & M. Devetsikiotis, 2016).

3 SISÄISET HAASTEET

Luvussa 3 käsitellään lohkoketjuteknologian sisäisiä haasteita. Luvussa perehdytään kuitenkin vain muutamiin, kandidaatin tutkielman raameihin sopiviin pulmiin. Käsiteltäviin haasteisiin tutkielmassa valittiin 51 % hyökkäys, tuplakulutus sekä skaalautuvuushankaluudet. Tässä vaiheessa olisi hyvä ymmärtää pääpiirteittäin, kuinka lohkoketjuteknologia käytännössä toimii, jotta pystyy hahmottamaan, kuinka nämä haasteet vaikeuttavat lohkoketjun tulemista laajemmaksi työkaluksi eri toimialoille.

3.1 51 % hyökkäys ja tuplakulutus

Bitcoinin haavoittuvuuksiin tällä hetkellä kuuluu ns. 51 % hyökkäys. Hyökkäys on periaatteessa mahdollinen, mutta käytännössä sen toteuttaminen vaatisi lähes mahdottoman suurta panostusta. 51 % hyökkäyksessä on kyse siitä, että käyttäjä tai kartelli käyttäjiä saisi haltuunsa yli puolet verkosta. Yli 50 % hallinta verkosta rikkoisi konsensukseen perustuvan Bitcoinin ja käyttäjä tai käyttäjäryhmä pystyisi täten muuttamaan protokollia ja hankkimaan itselleen edun uusien Bitcoinien louhimiseen. Mikäli tällainen skenaario toteutuisi, voisi se olla bitcoinin loppu valuuttana. (J. Bonneau et al., 2015; J. G. Fraser & A. Bouridane, 2017).

Syy, miksi kyseinen hyökkäys on todella epätodennäköinen, pohjautuu Bitcoin-verkoston suureen kokoon. Bitcoin-verkossa on miljoonia solmuja louhimassa ja jotta verkostosta saisi enemmistön itselleen, vaatisi se todella paljon resursseja. Bonneau (J. Bonneau et al., 2015) kuitenkin huomauttaa, että koska louhimisprosessi muuttuu koko ajan entistä monimutkaisemmaksi, on uusien louhijoiden vaikeampi päästä verkkoon mukaan. Tästäkin huolimatta, vaikka joidenkin louhijaryhmien koko onkin kasvanut jo suureksi, puhtaasti verkon ja solmujen suuren määrän vuoksi heidän on vaikea saada verkkoa itselleen (J. G. Fraser & A. Bouridane, 2017).

Onnistunut 51 % hyökkäys kasvattaisi bitcoinien tuplakulutuksen mahdollisuutta. Tuplakulutus on mahdollista myös alle 50 % hallinnalla, mutta se vaatii todella hyvää onnea ja resursseja, jotta se onnistuisi. Tuplakulutuksessa on kyse siitä, että käyttäjä käyttää samaa bitcoinia useammassa eri transaktiossa. Vastaanottava osapuoli pystyy varmistamaan vain sen, että lähettäjä on lähettänyt transaktion. Tämä johtuu siitä, että ainoastaan oikeelliseksi todistetut transaktiot tallennetaan tilikirjaan. Lähettäjä on kuitenkin voinut samaa bitcoinia käyttäen lähettää useammalle eri osapuolelle saman transaktion. Bitcoinissa ei ole laadittu toimenpidettä, miten tuplakulutuksen tapauksissa toimitaan ja mikä transaktio ketjuun kirjataan ja täten tuplakulutuksen arviointi jää vastaanottavana osapuolen vastuulle. (H. Lee, M. Shin, K. S. Kim, Y. Kang, & J. Kim, 2018).

3.2 Skaalautuvuus

Suuremmat lohkoketjut, kuten Bitcoin ja Ethereum, molemmat kohtaavat skaalautuvuuden haasteen. Bitcoinin ja Ethereumin suosion kasvaessa, yhä useampi käyttäjä on vuosien varrella liittynyt mukaan lohkoketjuun. Tämä on johtanut myös ketjuun rekisteröitävien transaktioiden eksponentiaaliseen kasvuun. (A. Chauhan, O. P. Malviya, M. Verma, & T. S. Mor, 2018).

Bitcoinin ilmestyttyä, vuonna 2009, transaktioita tapahtui keskimäärin 5000 kuukaudessa. Tämä määrä kuitenkin nousi jo vuoden 2010 puoleen väliin mennessä n. 50 000:n ja vuoden 2011 puoleen väliin mennessä jo 500 000 transaktioon. Määrä on jatkanut kasvamistaan ja vuonna 2017, transaktioita tapahtui jo lähes 10 miljoonaa kappaletta kuukautta kohden. Ethereuminkin tapauksessa transaktioiden määrä on kasvanut lokakuulta 2015 noin 5000 transaktiosta lähes 500 000:n transaktioon vuoden 2017 syksyyn mennessä. Kryptovaluuttojen tukijat ovatkin kiistelleet vaihtavansa uusien kryptovaluuttojen louhimiseen, mutta vastaavat ongelmat seuraisivat heidän mukanaan, jos uuden valuutan suosio kasvaisi. (A. Chauhan et al., 2018)

Skaalautuvuuden ongelman voi jakaa kolmeen osaan: läpivientiin (engl. throughput), kustannuksiin ja kapasiteettiin. Läpiviennin ongelma liittyy lohkojen rajoitettuun kokoon. Koska lohkoketju joutuu odottamaan transaktioiden varmistusta lohkoon ennen sen lisäämistä ketjuun, aiheutuu ruuhkaa. Lohkoja ei voida myöskään synnyttää nykyistä tahtia nopeammin, sillä se aiheuttaisi haarukkaefektin, eli lohko uhkaisi hajautua useampaan suuntaan. Konsensus perustuu uusien lohkojen syöttämisen pisimpään lohkoon, joten haarautuneet lohkot häviäisivät. Läpivientiä on rajoitettu tästä syystä. Kustannuksissa ongelman aiheuttavat transaktioihin liittyvät maksut: käyttäjä joutuu maksamaan transaktiokustannuksen sekä louhijalle, mutta häneltä veloitetaan myös mikromaksuja. Kun kaikki nämä transaktiot tallennetaan ketjuun, ketjun kapasiteetti kasvaa todella suureksi. Vuonna 2018 Bitcoinin lohkoketjun koko oli 163.34GB ja Ethereumin 667.10GB. (S. Kim, Y. Kwon, & S. Cho, 2018). Tämä nostaa kynnystä lohkoketjun ominaisuudeksi tarkoitetun avoin lähdekoodin toteutumista, sillä louhijoilta vaadittavien resurssien määrä nousee jatkuvasti.

4 ULKOISET HAASTEET

Lohkoketjuteknologiaa ja sen käyttöä vaikeuttaa teknologian ulkopuoleltakin tulevat haasteet. Luvussa 4 esitettävät haasteet liittyvät pitkälti teknologian toteutukseen, jotka eivät olisi pulmallisia, ilman esimerkiksi teknologian periaatteista poikkeavaa lainsäädäntöä. Kryptovaluuttamarkkinoiden aaltoilevuutta tarkastellaan bitcoinin näkökulmasta

4.1 Lainsäädäntö ja EU:n tietosuoja-asetus

EU:n uusi tietosuoja-asetus (engl. General Data Protection Regulation eli GDPR) asetettiin vuonna 2016 ja sen oli oltava täysin käytössä toukokuussa 2018. Tietosuoja-asetus määrittelee henkilötiedot tiedoiksi, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Tällaisia tietoja ovat mm. nimi, kotiosoite, sähköpostiosoite, auton rekisterinumero ja IP-osoite. (EUR-Lex, 2016). Tietosuoja-asetuksen mukana ihmisille tuli oikeus tulla unohdetuksi. Tämä tarkoittaa käytännössä sitä, että henkilöllä on oikeus vaatia tietojaan poistettavaksi, kun prosessointi ei vaadi enää tunnistautumista. (D. Schmelz, G. Fischer, P. Niemeier, L. Zhu, & T. Grechenig, 2018).

Lohkoketjuihin tallentuu tietoja mm. käyttäjien avaimista, eli tunnistimista. Schmelz ym. (2018) pohtivatkin, onko lohkoihin tallennettujen tietojen avulla mahdollista löytää ja tunnistaa käyttäjä varmuudella. Bitcoinilla oli ennen käytössä funktio, joka mahdollisti bitcoinien siirron suoraan IP-osoitteen perusteella. Vaikkakin tämä funktio on jo otettu käytöstä, lohkoketjuissa on käytetty henkilötietoja maksutapahtumien suorittamista varten.

Esimerkkinä Ethereumin tapauksessa henkilötietojen käytöstä, on auton ajettujen kilometrien mittarilukeman seuraaminen huijauksien estämiseksi, käyttäen auton rekisterinumeroa tunnistimena. Ethereumin älysopimukseen tallentuva tieto mittarilukemasta olisi julkisesti nähtävillä, eikä se olisi käyttäjien muutettavissa. Koska auton rekisterinumero on henkilötieto, on tässäkin otettava huomioon EU:n tietosuoja-asetuksen asettamat raamit henkilötietojen käyttöön. Lohkoketjuteknologia voi ratkaista ongelman vaatimalla käyttäjiään hyväksymään heidän henkilötietojen käytön esimerkiksi älysopimuksia tehdessä. Ongelmaksi muodostuu kuitenkin, jos älysopimuksella tarkkailtavan auton omistaja vaihtuu, eikä uusi omistaja suostu ehtoihin, on hänen henkilötietonsa, tässä tapauksessa auton rekisterinumero, tallentuneena ja näkyvillä ketjussa määrittelemättömän ajan. (D. Schmelz et al., 2018).

Toinen lainsäädäntöön perustuva ongelma pohjautuu lohkoketjujen autonomisuuteen. Fabiano (2017) huomauttaa, että Nakamoton (2008) Bitcoinin alkuperäisjulkaisussa on henkilöiden yksityisyyteen liittyvä ristiriita, jossa Nakamoto toteaa henkilöiden yksityisyyden olevan turvattu, kun heidän yleisavaimensa

pidetään anonyymeina. Kuitenkin Nakamoto toteaa, että jos avaimen omistaja selviäisi, voisi se paljastaa muita transaktioita, joita avaimen omistaja on tehnyt. Asiasta herää kysymys, kuka vastaa lohkoketjun turvallisuudesta käyttäjälle. Koska lohkoketju on autonominen ja perustuu konsensuksen säilymiseen yhden keskitetyn toimijan sijaan, käyttäjät eivät tarkalleen tiedä kuka heidän dataansa käsittelee. (N. Fabiano, 2017).

Lainsäädäntöä vaikeuttaa myös lohkoketjun ominaisuuksiin kuuluva hajautettu vertaisverkko. Yksityisyyden rikkoutumisen esimerkkiä jatkaen, on käyttäjän myös mahdotonta tietää, missä maantieteellisesti hänen tietojaan on tallentunut (N. Fabiano, 2017). Eri maissa pätevät eri lait, ja se minkä maan lakeja missäkin tapauksissa sovelletaan, on harmaalla alueella. Lisäksi GDPR:n tapauksessa, jos eurooppalaisen tietoa on tallennettu esimerkiksi Euroopan ulkopuolella, toimisiko GDPR tässä asiassa samalla tavalla ja tehokkuudella, kuin esim. tavallisessa yrityksen ja asiakkaan välisessä suhteessa.

4.2 Kryptovaluuttakurssien ailahtelu

Lohkoketjuteknologian pyöriessä tällä hetkellä suuresti eri kryptovaluuttojen ympärillä, kryptovaluuttakurssien aaltoilu herättää epävarmuutta, voiko teknologiaan luottaa. Bitcoin-kryptovaluutan hinta nousi vuonna 2017 räjähdysmäisesti alla tuhannesta eurosta jo lähes 20 000 euroon. Hinta on kuitenkin tippunut helmikuuhun 2019 mennessä jo n. 3 500 euroon. Brito & Schadab ja Castillon (2015) kyseessä on kuitenkin verrattain uusi valuutta, joka etsii vielä arvoaan. Kryptovaluutta-markkinoita ei ole kuitenkaan säännelty minkään ulkoisen toimijan toimesta, joka lisää markkinoilla epävakautta.

Vaikkakin bitcoinin arvo on aaltoillut yli 10 000 eurolla, useat toimijat hyväksyvät bitcoinin maksuvälineenä. Vastaanottava osapuoli pystyy kuitenkin heti maksun saatuaan vaihtaa bitcoinin rahaksi, joten he eivät ole alttiita bitcoinin hinnan romahtamiselle. Hintavaihteluun vaikuttaakin mm. suuret yritykset, ja heidän suhtautumisensa bitcoiniin: mikäli he sallivat sen maksuvälineenä, markkinahinnalla on tapana nousta ja päinvastoin. (Brito et al., 2015).

Markkinoiden ailahteluun vaikuttaa yritysten lisäksi myös sekä teknologia itsessään ja siihen liittyvät haavoittuvuudet, että valtioiden linjaukset liittyen kryptovaluuttoihin. Kuitenkin on hyvä huomata, että itse Bitcoin-protokolla on vain kerran vaikuttanut negatiivisesti sen hintaan vuonna 2013. Tällöin kyseiset ongelmat johtuivat ohjelmistopäivityksestä ja solmujen välisistä eri versioista. Kyseessä on tähän mennessä ainoa tapaus, kun itse Bitcoin-protokolla on kokenut häiriön. Huomioitavaa on kuitenkin, että jos vastaava tapahtuisi tänä päivänä, olisivat seuraukset huomattavasti suuremmat, kun Silk Roadin tai Mt. Goxin tapaukset, joista seuraavaksi kerrotaan. (J. G. Fraser & A. Bouridane, 2017).

Tähän mennessä bitcoinin hinnan laskemiseen ovat eniten vaikuttaneet teknologian ulkoiset tekijät. Eräs suurimmista oli Silk Road -nimisen palvelun sulkeminen vuonna 2013. Kyseessä oli siihen aikaan yksi ainoista paikoista, jossa

bitcoinia pystyi käyttämään maksuvälineenä. Silk Road oli vastaavasti yksi bitcoinin hinnan suurimpia nostattajia, mutta heidän toimistaan paljastui FBI:n tutkinnoissa laittomuuksia. Palvelun romahtaminen sai ihmiset epäilemään, onko itse valuutasta lainkaan hyötyä, kun siihen aikaan bitcoin ei käynyt yleisenä maksuvälineenä missään. (J. G. Fraser & A. Bouridane, 2017).

Laiton toiminta on ajanut myös valtioita, esimerkiksi Kiinaa, suhtautumaan skeptisesti kryptovaluuttoihin. Sen pelätään helpottavan esimerkiksi rahan pesua. Kryptovaluutan arvon nousun ei haluta kilpailevan valtion oman valuutan kanssa. Vuonna 2017 Kiina laittoikin kapuloita bitcoinmarkkinoiden rattaisiin, joka pysäytti Kiinan markkinat ja sai bitcoinin hinnan tippumaan. (J. G. Fraser & A. Bouridane, 2017). Kiina ei ole kuitenkaan lailla kieltänyt kryptovaluuttoja.

Vaikkakaan Bitcoiniin itseensä ei ole murtauduttu ja tähän mennessä ainoa ongelmatapaus on ollut edellä mainittu ohjelmistopäivitys, bitcoinien parissa asioivien palveluihin on kohdistunut onnistuneita hyökkäyksiä. Mt. Gox -nimiseen valuutanvaihtopalveluun kohdistunut hyökkäys helmikuussa 2014 johti n. 750 000 bitcoinin menetykseen, arvoltaan 400 miljoonaa Yhdysvaltain dollaria. Myös Bitfinexin-alustan romahtaminen tapahtuessaan vaikutti hinnan putoamiseen, muttei niin radikaalisti, kuin Mt. Gox. (J. G. Fraser & A. Bouridane, 2017).

5 YHTEENVETO

Tutkielmassa käsiteltiin lohkoketjuteknologiaa, ja mitä haasteita sillä on edessään, jotta teknologia saisi suuremman jalansijan nyky-yhteiskunnassa. Tutkielman alussa käytiin läpi lohkoketjuteknologian perusperiaatetta, kuinka se rakentuu ja kuinka se käytännössä toimii. Seuraavissa luvuissa käsiteltiin haasteita lohkoketjuteknologialle. Haasteet oli jaettu sisäisiin- ja ulkoisiin haasteisiin. Tutkielmassa lohkoketjua tarkasteltiin lähinnä Bitcoinin näkökulmasta, sillä lohkoketjuteknologia luotiin alun perin Bitcoinia varten Satoshi Nakamoton toimesta.

Lohkoketju on lohkoista rakentuva ketju. Lohkoja syntyy, kun solmut lähettävät dataa louhijoille. Kun datan oikeellisuus on tarkistettu, lisätään lohko ketjun jatkoksi. Jokaisessa lohkossa on viite edeltävään lohkoon. Louhijat ovat lohkoketjussa olevat käyttäjät, jotka Proof of Work -algoritmia käyttäen tarkistavat datan oikeellisuuden. Lohkoketju perustuu siihen, ettei sillä ole yhtä suurta omistajaa tai hallitsijaa, vaan ketju itsessään ylläpitää konsensusta eli yhteisymmärrystä ja täten mahdollistaa käyttäjien luottamuksen ketjua kohtaan, sillä väärinkäyttö- ja huijausyritykset huomattaisiin nopeasti konsensuksen häiriintyessä. Muita lohkoketjun pääominaisuuksia on avoin lähdekoodi, anonyymius, muuttumattomuus, läpinäkyvyys ja hajautettu vertaisverkko.

Lohkoketjuteknologia pyörii tällä hetkellä pitkälti kryptovaluuttojen ympärillä. Tällä hetkellä suurimmat valuutat ovat Bitcoin ja Ethereumin ether. Siinä missä Bitcoinin teknologia keskittyy lähinnä valuutan transaktioihin, Ethereum on älysopimuksien suurin tukija. Älysopimuksilla tarkoitetaan sopimusta, joka toteutuessaan menee tietokoneen toimesta automaattisesti käytäntöön.

Sisäisistä haasteista tutkielmassa käytiin läpi 51% hyökkäys, tuplakulutus ja skaalautuvuusvaikeudet. 51% hyökkäyksessä kyse on siitä, että käyttäjä tai käyttäjäjoukko saa enemmistön lohkoketjusta haltuunsa ja pääsisi täten vaikuttamaan konsensukseen. Tuplakulutuksessa kyse on saman bitcoinin käyttöä useammassa transaktiossa. Skaalautuvuuden ongelmat ovat sekä transaktioiden määrän eksponentiaalinen kasvu sekä ketjun kasvava koko ja muistivaatimus.

Ulkoisia, tutkielmassa käsiteltyjä haasteita lohkoketjuteknologialle ovat mm. lakipykälät esimerkiksi EU:n tietosuojavaatimus ja kryptovaluuttakurssien ailahtelevuus. Koska teknologia on niin nopeasti kehittyvää, on lakipykälien hankala pysyä mukana. Lohkoketjujen tapauksessa, ketjujen ollessa autonomisia kokonaisuuksia, joissa käyttäjät ovat anonyymejä, lakien soveltaminen on hankalaa, mutta kuitenkin tarvittavaa. Kryptovaluutat, jotka ovat nostattaneet lohkoketjuteknologian näkyvyyttä mediassa, eivät ole arvoltaan stabiileja vaan arvon aaltoilua tapahtuu runsaasti. Vaikkakin useat toimijat ovat ottaneet esimerkiksi bitcoinin sallituksi maksuvälineeksi, olisi markkinat hyvä saada tasapainottumaan madaltaakseen sekä asiakkaiden että yritysten kynnystä liittyä teknologian tukemiseen mukaan.

Lohkoketjuteknologialla on potentiaalia muuttaa tapaa, kuinka asioita tällä hetkellä tehdään. Uudeksi teknologiaksi sillä on kuitenkin vielä kasvettavaa, jotta sen paikka vakiintuisi esimerkiksi yritysarkkitehtuurissa. Tulevia hyviä

tutkimussuuntia on, kuinka teknologiaa voidaan kehittää, jotta se palvelisi suurempaa osaa ihmisistä ja saataisiin osaksi myös heidän arkeaan, sijoittajien ja teknologian parissa työskentelevien henkilöiden lisäksi.

LÄHTEET

A. Balaskas, & V. N. L. Franqueira. (2018). (2018). Analytical tools for blockchain: Review, taxonomy and open challenges. Paper presented at the *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* 1-8. doi:10.1109/CyberSecPODS.2018.8560672

A. Chauhan, O. P. Malviya, M. Verma, & T. S. Mor. (2018). (2018). Blockchain and scalability. Paper presented at the *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C),* 122-128. doi:10.1109/QRS-C.2018.00034

Brito, J., Shadab, H. B., & Castillo, A. (2015). Bitcoin financial regulation: Securities, derivatives, prediction markets, and gambling.

D. Schmelz, G. Fischer, P. Niemeier, L. Zhu, & T. Grechenig. (2018). (2018). Towards using public blockchain in information-centric networks: Challenges imposed by the european union's general data protection regulation. Paper presented at the *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN),* 223-228. doi:10.1109/HOTICN.2018.8606000

G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, & R. Hierons. (2018). (2018). Smart contracts vulnerabilities: A call for blockchain software engineering? Paper presented at the *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE),* 19-25. doi:10.1109/IWBOSE.2018.8327567

H. Lee, M. Shin, K. S. Kim, Y. Kang, & J. Kim. (2018). (2018). Recipient-oriented transaction for preventing double spending attacks in private blockchain. Paper presented at the *2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON),* 1-2. doi:10.1109/SAHCN.2018.8397151

J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, & E. W. Felten. (2015). (2015). SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. Paper presented at the *2015 IEEE Symposium on Security and Privacy,* 104-121. doi:10.1109/SP.2015.14

J. G. Fraser, & A. Bouridane. (2017). (2017). Have the security flaws surrounding BITCOIN effected the currency's value? Paper presented at the *2017 Seventh International Conference on Emerging Security Technologies (EST),* 50-55. doi:10.1109/EST.2017.8090398

K. Christidis, & M. Devetsikiotis. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292-2303. doi:10.1109/ACCESS.2016.2566339

Lin, I., & Liao, T. (2017). A survey of blockchain security issues and challenges. *IJ Network Security, 19*(5), 653-659.

M. D. Pierro. (2017). What is the blockchain? *Computing in Science & Engineering, 19*(5), 92-95. doi:10.1109/MCSE.2017.3421554

M. Dabbagh, M. Sookhak, & N. S. Safa. (2019). *The evolution of blockchain: A bibliometric study* doi:10.1109/ACCESS.2019.2895646

N. Fabiano. (2017). (2017). Internet of things and blockchain: Legal issues and privacy. the challenge for a privacy standard. Paper presented at the *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* 727-734. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.112

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

S. Kim, Y. Kwon, & S. Cho. (2018). (2018). A survey of scalability solutions on blockchain. Paper presented at the *2018 International Conference on Information and Communication Technology Convergence (ICTC),* 1204-1207. doi:10.1109/ICTC.2018.8539529

S. Singh, & N. Singh. (2016). (2016). Blockchain: Future of financial and cyber security. Paper presented at the *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I),* 463-467. doi:10.1109/IC3I.2016.7918009

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper, 151*, 1-32.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). (2017). An overview of blockchain technology: Architecture, consensus, and future trends. Paper presented at the *2017 IEEE International Congress on Big Data (BigData Congress),* 557-564.