Johannes Seppänen

LOHKOKETJUTEKNOLOGIAN HAASTEET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Seppänen, Johannes
Lohkoketjuteknologian haasteet
Jyväskylä: Jyväskylän yliopisto, 2021, 27 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Taipalus, Toni

Lohkoketjuteknologiaa on kuvattu maailmaa mullistavaksi teknologiaksi, uuden sukupolven internetiksi ja muilla ylentävillä tavoilla. On kuitenkin selvää, että näinkin uudella teknologialla on hehkutuksesta huolimatta haasteita, jotka täytyy pystyä ratkaisemaan. Tutkielman tarkoituksena on selvittää lohkoketjuteknologian haasteita ja niiden ratkaisuja. Tutkielma toteutettiin kirjallisuuskatsauksena. Tutkimuksen keskeisinä tuloksina voidaan esitellä, että lohkoketjuteknologialla on ollut ja on edelleen useita haasteita. Erilaisia haasteita on paljon ja ne voidaan jakaa useisiin eri kategorioihin, kuten teknologisiin, organisatorisiin ja ympäristöllisiin. Teknologiset haasteet ovat erityisen suuressa roolissa haasteita tarkastellessa ja niihin paneudutaan tarkemmin tutkielmassa. Löydettyihin haasteisiin on kehitetty useita ratkaisuja, jotka ovat vastanneet osittain haasteisiin. Ratkaisuja on monenlaisia ja osa niistä keskittyy yhden tietyn ongelman ratkaisemiseen, kun taas osa keskittyy kokonaisuuksien kehittämiseen, kuten konsensusmekanismien muuttamiseen.

Asiasanat: lohkoketjuteknologia, haasteet, ratkaisut

ABSTRACT

Seppänen, Johannes
Challenges of blockchain technology
Jyväskylä: University of Jyväskylä, 2021, 27 pp.
Information systems, Bachelor's thesis
Supervisor: Taipalus, Toni

Blockchain technology has been described as revolutionizing technology, the new generation of the Internet and other uplifting ways. However, such a new technology has its own challenges that need to be met. The purpose of the thesis is to find out the challenges of blockchain technology and solutions to them. The study was conducted as a literature review. The main results of the study can be presented that blockchain technology has had and still has several challenges. There are many different challenges, and they can be divided into several different categories, such as technological, organizational and environmental. Technological challenges play a particularly important role in examining the challenges and will be addressed in more detail in the thesis. Several solutions have been developed to the identified challenges, which have partially met them. There are many solutions, and some of them focus on solving one problem, while some focus on developing blockchain as a whole, such as changing consensus mechanisms.

Keywords: blockchain technology, challenges, solutions

KUVIOT

SISÄLLYS

1 JOHDANTO

Lohkoketju toimii eräänlaisena muuttumattomana tilikirjana tai tietokantana, joka toimii vertaisverkossa. Se mahdollistaa erilaisten hajautettujen tietokantojen ylläpitämisen ja transaktioiden suorittamisen hajautetulla tavalla. Lohkoketjupohjaiset sovellukset ovat lisääntyneet huomattavasti ja ne kattavat useita aloja, kuten rahoituspalveluja, esineiden internetiä ja niin edelleen (Zheng, Xie, Dai, Chen & Wang, 2018). Zheng ym. (2018) mukaan lohkoketju mahdollistaa maksujen suorittamisen ilman pankkeja tai muita välittäjiä, ja sitä voidaan käyttää myös useisiin muihin taloudellisiin palveluihin, kuten digitaalisiin omaisuuseriin, rahalähetyksiin ja verkkomaksuihin. Sitä voidaan käyttää myös muilla aloilla, kuten älykäissä sopimuksissa, julkispalveluissa, IoT:ssa, mainejärjestelmissä ja turvallisuuspalveluissa. (Zheng ym., 2018) Lohkoketjuteknologiaa on kuvailtu esimerkiksi uuden sukupolven internetiksi ja uudenlaiseksi ratkaisuksi ikivanhaan luottamuksen ongelmaan (Shermin, 2017).

Lohkoketjuteknologian ympärillä, kuten monella muullakin uudella teknologialla on ollut ja on edelleen huomattavaa hehkutusta. Kietzmann ja Archer-Brown (2019) käyvät sitä läpi artikkelissaan. Siinä esitetään Gartnerin (Panetta, 2018) esittämä kaavio, jonka mukaan jokainen uusi teknologia noudattaa samanlaista kypsyys- ja käyttöönottomallia. Ajan mittaan uuden teknologian suorituskykyodotukset käyvät läpi ennustettavissa olevia nousu- ja laskusykliä. Kun jokin teknologia julkaistaan ensimmäisen kerran, se on yleensä kaupallisesti kannattamaton. Kuitenkin varsinkin mullistavien teknologioiden yhteydessä innovaatiot laukaisevat nopean kuluttajien ennakoinnin ja uskomuksen välittömistä muutoksista vallitsevaan tilanteeseen. Teknologian hehkutus kasvaa, mutta lopulta ihmiset tajuavat, että odotukset olivat liian suuret. Paisutettujen odotusten huipulla saavutetaan käännekohta, jossa ihmiset tunnistavat, ettei teknologia vastaakaan odotuksia. Kiinnostus laskee ja odotukset teknologialta laskevat. Ajan myötä teknologioiden kehittyessä ilmenee kuitenkin enemmän käyttötapauksia, kuinka teknologiaa voidaan hyödyntää. Lopulta, yleensä toisen tai kolmannen sukupolven aikana teknologioista tulee todellisuutta ja ne siirtyvät valtavirtaan. Kaikki uudet teknologiat käyvät läpi nämä vaiheet eri nopeuksilla, eikä lohkoketjuteknologia ole poikkeus tästä. Sen heh-

kutuksen vaihtelua voidaan tarkastella helposti esimerkiksi tarkastelemalla Bitcoin kryptovaluutan kurssia, joka on vaihdellut erittäin suuresti viime vuosien aikana.

Lohkoketjuteknologialla on kuitenkin hehkutuksesta huolimatta useita haasteita ja ongelmia. Sen mahdollisuuksista hehkuttamisen sijaan on kuitenkin tärkeää tutkia sen haasteita. Haasteiden selvittäminen ja ratkaiseminen on erittäin tärkeää lohkoketjuteknologian yleistymisen kannalta. Lohkoketjuteknologian haasteita voidaan tarkastella kolmesta näkökulmasta, jotka ovat teknologinen, organisatorinen ja ympäristöllinen (Batubara, Ubacht & Janssen, 2018). Tutkielmassa keskitytään erityisesti teknologisiin haasteisiin, joita ovat esimerkiksi turvallisuus, skaalautuvuus, käytettävyys, yhteensopivuus, luotettavuus, kustannustehokkuus, varastointitila ja kypsymättömyys (Batubara ym., 2018). Teknologiset haasteet ovat erityisen suuressa osassa lohkoketjuteknologian haasteita tarkastellessa, minkä vuoksi niihin paneudutaan tarkemmin tutkielmassa. Tutkielma toteutetaan kirjallisuuskatsauksena ja siinä pyritään lähdekirjallisuuden perusteella vastaamaan kahteen tutkimuskysymykseen, jotka ovat:

1. Mitä ovat lohkoketjuteknologian suurimmat haasteet?

2. Minkälaisia ratkaisuja on kehitetty vastaamaan haasteisiin?

Kirjallisuuskatsauksen tietokantoina on käytetty IEEE Xplorea, ACM Digital Librarya, Science Directiä ja Google Scholaria. Hakusanoina on käytetty erilaisia englanninkielisiä hakusanoja, kuten ”blockchain”, ”blockchain consensus” ja ”challenges of blockchain”. Tietyissä tilanteissa lähteinä on käytetty myös nettisivuja, jotka tarkastelevat eri lohkoketjuja.

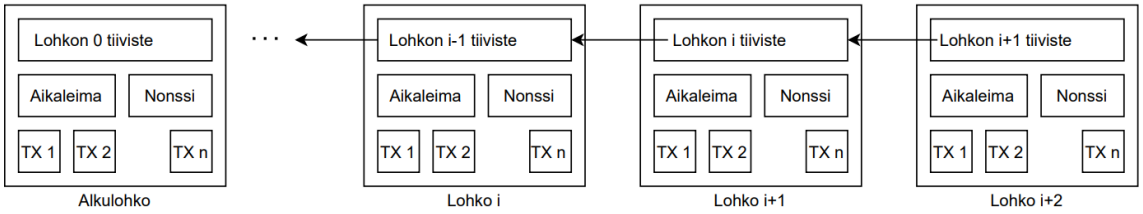
Tutkielma on jaettu neljään lukuun. Johdannon jälkeen tutkielman toisessa luvussa esitellään lohkoketjuteknologia yleisesti keskittyen sen rakenteeseen. Tämän jälkeen käsitellään konsensusta lohkoketjuissa ja esitellään kaksi eri konsensusmekanismia, jotka ovat Proof of Work ja Proof of Stake. Viimeisenä käsitellään lohkoketjuteknologian laajennuksia kryptovaluuttojen ulkopuolelle. Laajennuksissa keskitytään älysopimuksiin ja lohkoketjuihin, jotka mahdollistavat älysopimuksien käytön.

Kolmannessa luvussa pyritään vastaamaan tutkielman tutkimuskysymyksiin, eli mitä ovat lohkoketjuteknologian suurimmat haasteet ja millaisia ratkaisuja niihin on kehitetty. Luvun alussa esitellään haasteita yleisesti, minkä jälkeen paneudutaan tarkemmin kolmeen haasteeseen, jotka ovat energian kulutus, skaalautuvuus ja turvallisuus. Nämä kolme on valittu tarkasteltavaksi, sillä ne ovat suuresti esillä lähdekirjallisuudessa. Haasteiden esittelyn jälkeen keskitytään niihin kehitettyjen ja ehdotettujen ratkaisujen tarkastelemiseen. Tutkielman viimeisessä luvussa tehdään yhteenveto tutkielmasta, sen tuloksista ja mahdollisista rajoitteista tutkielmassa. Tämän jälkeen pohditaan tulosten merkitystä lohkoketjuteknologian kehityksen kannalta ja mahdollisia jatkotutkimusaiheita.

2 LOHKOKETJUTEKNOLOGIA YLEISESTI

Lohkoketjuteknologialla tarkoitetaan tekniikkaa, joka mahdollistaa toisilleen vieraiden toimijoiden yhteisen hajautetun tietokannan ilman kolmansia osapuolia. Lohkoketju toimii eräänlaisena useiden tietokoneiden verkkoon säilöttynä tilikirjana, joka on avoin, hajautettu ja kryptografisesti ketjutettu. Se toimii siis täysin hajautetusti tuhansien tietokoneiden muodostamassa vertaisverkossa ilman yhtä keskuskontrollikoneistoa. (Honkanen, 2017)

Lohkoketju muodostuu tietojoukoista, jotka koostuvat tietopakettiketjusta eli lohkoista, joissa lohko sisältää useita transaktioita. Sitä laajennetaan jokaisella uudella lohkolla ja se edustaa tapahtumahistorian täydellistä tilikirjaa. Transaktioiden lisäksi lohkot sisältävät aikaleiman, edellisen lohkon tiivisteen ja nonssin, joka on satunnainen luku tiivisteen tarkistamiseksi. Tämä konsepti varmistaa koko lohkoketjun eheyden ensimmäiseen lohkon asti. Lohkoketjun rakennetta on havainnollistettu kuviossa 1 (kuvio 1). Tiivisteet ovat ainutlaatuisia ja lohkoketjun muutokset voidaan estää tehokkaasti, koska lohkossa tapahtuvat muutokset muuttavat välittömästi vastaavaa tiivistettä. Jos suurin osa verkon solmuista ovat samaa mieltä konsensusmekanismin avulla lohkon tapahtumien paikkaansa pitävyydestä, se voidaan lisätä lohkoketjuun. Konsensusmekanismi on prosessi, jossa suurin osa verkon solmuista pääsee yhteisymmärrykseen lohkoketjun tilasta. Se on joukko sääntöjä ja menettelytapoja, mitkä mahdollistavat yhdenmukaisen tosiseikkojen ylläpitämisen useiden osallistuvien solmujen välillä. Konsensusmekanismin takia uusia tapahtumia ei lisätä automaattisesti lohkoketjuun. Se varmistaa, että tapahtumat tallennetaan lohkoon tietyksi ajaksi ennen niiden siirtymistä lohkoketjuun, jonne tallennettuja tietoja ei voida muuttaa enää jälkeenpäin. Bitcoinin tapauksessa lohkot luodaan louhijoiden toimesta, jotka palkitaan bitcoineilla lohkojen validoinnista. (Nofer, Gomber, Hinz & Schiereck, 2017)



KUVIO 1 Lohkoketjun rakenne (Zheng ym., 2018)

2.1 Konsensus

Hajautetussa tietojenkäsittelyssä hajautettu verkko johtaa väistämättä verkkojen väliseen epäluottamukseen. Verkon luotettavuuden varmistamiseksi järjestelmät neuvottelevat asiaankuuluvien protokollien kautta päästäkseen konsensukseen ja johdonmukaisuuteen. Tätä kutsutaan konsensusmekanismiksi. (Zhang, Wu & Wang, 2020) Konsensuksen saavuttamiseen on useita lähestymistapoja. Nämä lähestymistavat voidaan luokitella karkeasti avoimiin lohkoketjuihin, joita käyttävät esimerkiksi Bitcoin ja muut avoimet lohkoketjut, sekä luvanvaraisiin lohkoketjuihin, jotka soveltuvat paremmin hallituille yksityisille ympäristöille. (Gupta, Hellings, Rahnama & Sadoghi, 2020) Tässä tutkielmassa keskitytään avoimiin lohkoketjuihin.

Konsensusmekanismia käytetään hajautettujen järjestelmien johdonmukaisuusongelman ratkaisemiseen. Konsensusalgoritmilla rajoitetun ajan suojattu operaatio on johdonmukainen, hyväksytty ja turvattu hajautetussa verkossa. Sen ydin on ratkaista hajauttamisen luottamusongelma. Lohkoketjujärjestelmien luominen on edistänyt konsensusmekanismien tehokasta kehittämistä Proof of Work (PoW)-mekanismista eteenpäin. Lohkoketjua ehdotettiin alun perin Bitcoin-järjestelmän yhteydessä. Lohkoketju on Bitcoinin taustalla oleva toteutus, jolla on hajauttamisen, nimettömyyden, turvallisuuden ja uskottavuuden edut. Pohjimmiltaan se on hajautettu tilikirja. Hajauttaminen on ainutlaatuinen idea, jonka se on tuonut. Aikaisemmin tapahtumat tapahtuivat keskitetyissä ympäristöissä, usein hallituksen tai muiden järjestöjen valvonnassa ja hallinnassa. Lohkoketjuteknologian toteuttamassa verkkoympäristössä ei ole erilaisien keskitettyjen organisaatioiden valvontaa, vaan reiluus ja oikeudenmukaisuus kunkin solmun välillä. Näin ollen jokaisen solmun välillä tarvitaan yksimielisyys, jotta voidaan toteuttaa kaupan laillisuus ja niiden hajauttaminen. Konsensusmekanismi on lohkoketjuteknologian ydin. Sen tehokkuus määrittää suoraan lohkoketjujärjestelmän vakaan ja turvallisen toiminnan. Tehokas konsensusmekanismi antaa lohkoketjulle mahdollisuuden muodostaa yhtenäisen rakenteen tehokkaasti. (Zhang ym., 2020) Seuraavaksi esitellään PoW- ja PoS-konsensusmekanismit. On huomattava, että erilaisia konsensusmekanismeja on useita ja niitä kaikkia ei käsitellä tässä tutkielmassa. PoW ja PoS ovat kuitenkin erittäin yleisesti käytettyjä suurimmissa lohkoketjuissa, minkä takia ne on valittu esiteltäväksi.

2.1.1 Proof of Work-konsensusmekanismi

Nakamoto (2008) esitteli ensimmäistä kertaa Proof of Work (PoW)-konsensusmekanismin Bitcoin-lohkoketjujärjestelmän yhteydessä. PoW-konsensusmekanismin ydinajatuksena on varmistaa datan yhtenäisyys ja konsensuksen turvallisuus kilpailemalla hajautettujen solmujen laskentateholla. Bitcoin-järjestelmässä jokainen tapahtuma on kirjattava lohkoon. Konsensusmekanismin perusteella solmut voivat todeta tapahtumat päteväksi yksimielisesti.

Käytännössä tämä tapahtuu siten, että uudet transaktiot lähetetään kaikille solmuille, jonka jälkeen jokainen solmu kerää transaktioita lohkoon. Tämän jälkeen solmut pyrkivät laskemaan oikean tiivisteen lohkolleen. Jonkun solmun löytäessä tiivisteen, se lähettää lohkonsa kaikille muille solmuille. Muut solmut hyväksyvät lohkon, jos se sisältää vain kelvollisia transaktioita, eikä niitä ole aikaisemmin lähetetty. Solmut ilmaisevat hyväksyntänsä uudelle lohkolle alkamalla työstämään seuraavaa lohkoa käyttämällä hyväksytyn lohkon tiivistettä edellisenä tiivisteenä. (Nakamoto, 2008) Tämä toimintatapa johtaa helposti myös transaktioiden jumittumiseen ja kuluilla kilpailemiseen, sillä solmut valitsevat luomiinsa lohkoihin luonnollisesti mieluiten niitä transaktioita, joiden lähettäjä maksaa solmulle enemmän lähettämisestä. Verkon ruuhkautuessa lähettäjien täytyy siis maksaa enemmän lähettämisestä, jos he haluavat transaktiot lähetettyä nopeasti.

PoW-mekanismilla siis saavutetaan koko verkon yksimielisyys laskemalla ja ratkaisemalla vaikeita ongelmia, mikä toteuttaa hajauttamisen, estää kaksinkertaisen maksamisen ja saavuttaa tapahtuman sopimisen rajoitetussa ajassa, mikä varmistaa järjestelmän vakaan toiminnan. PoW-mekanismissa on kuitenkin useita puutteita ja ongelmia, kuten se, että mekanismi vaatii paljon resursseja. Yhden louhijan onnistuessa louhinnassa kaikkien muiden louhijoiden laskentaan käyttämä energia menee hukkaan. Lisäksi tapahtumien vahvistusajat ovat pitkiä ja samanaikaisuus on vähäistä. Louhijayhteisöt ovat lisäksi riski hajauttamiselle. Tällä hetkellä viisi suurinta louhijayhteisöä kattaa yli 50 % Bitcoin-verkon laskentatehosta. (Zhang ym., 2020)

2.1.2 Proof of Stake-konsensusmekanismi

Proof of Stake (PoS)-konsensusmekanismissa lohkojen validoijat valitaan laskentatehon sijaan heidän omistamiensa panosten perusteella. Panospohjaisen valinnan takia validoijien ei tarvitse kuluttaa suurta määrää energiaa laskentatehon saavuttamiseen, mikä vähentää huomattavasti energian kulutusta vertaillessa PoS- ja PoW-mekanismeja. Lohkojen luominen ja transaktioiden varmistaminen on yleensä myös huomattavasti nopeampaa PoS-lohkoketjuissa verrattuna PoW-lohkoketjuihin. Tämä johtuu siitä, että PoW-ketjut pitävät lohkonmuodostus- ja transaktioiden vahvistusnopeudet suhteellisen pienenä turvallisuuden takaamiseksi, koska louhijoiden ehdottamia lohkoja on suuri määrä. PoS-mekanismikierroksella luodaan vain yksi lohko, mikä nopeuttaa prosessia

huomattavasti. PoS-konsensusmekanismissa solmun panos on sen hallussa olevien tai tallettamien digitaalisten rahakkeiden, esimerkiksi kryptovaluutoissa olevien rahakkeiden määrä. Sen sijaan, että kulutettaisiin paljon energiaa hakuprosessiin, kuten PoW-mekanismissa, validoija valitaan esimerkiksi sen panosten perusteella painotetun satunnaisen valinnan avulla. Suurimmalla panoksella on suurin mahdollisuus päästä lohkon validoijaksi ja täten saada lohkonluontipalkkio. (Nguyen ym., 2019) PoS-mekanismista on erilaisia variaatioita, joiden toiminnallisuudet ja ominaisuudet vaihtelevat. Kaikissa on kuitenkin yhtenäistä se, että uusien lohkojen validoijat valitaan laskentatehon sijaan heidän panosten perusteella.

Tendermint on esimerkki PoS-konsensusprotokollasta. Siinä valitaan joku validoijista ehdokkaaksi, joka vastaa lohkon luomisesta ja ehdottamisesta nykyiselle kierrokselle. Validoijien on lukittava rahakkeensa eli panoksensa tietyksi ajaksi. Jos validoijan todetaan osallistuneen haitalliseen toimintaan tämän aikana, sitä voidaan rangaista viemällä sen panostamat rahakkeet. Ajan jälkeen panokset vapautetaan ja palautetaan validoijille. (Thin, Dong, Bai & Dong, 2018) Ethereum on siirtymässä Casper-protokollaan tällä hetkellä käyttämästään PoW-mekanismista. Casper käyttää samankaltaisia tapoja Tendermintin kanssa haitallisen toiminnan estämiseksi. Näitä tapoja ovat esimerkiksi validoijan panoksen vieminen sen rikkoessa tiettyjä ehtoja (Buterin & Griffith, 2017).

2.2 Laajennukset

Lohkoketjuteknologia sai alkunsa Nakamoton (2008) julkaistessa kryptovaluutta Bitcoinin. Sen jälkeen lohkoketjuteknologia on laajentanut kattamaan monia muitakin osa-alueita, kuten älykkäitä sopimuksia. Szabo (1996) esitteli ensimmäisenä älykkäät sopimukset, jotka ovat tietokoneprotokollia, jotka on kirjoitettu ohjelmointikielillä. Älykkäät sopimukset ovat mullistavia, koska erilaiset sopimusehdot voidaan sisällyttää ohjelmistoihin tai laitteistoihin. Kun ennalta asetetut ehdot täyttyvät, sopimukset suoritetaan automaattisesti. (Li, Zheng & Dai, 2021) Ethereum oli ensimmäinen lohkoketju, joka otti käyttöön älykkäät sopimukset. Ethereum on julkinen hajautettu alusta, jossa käyttäjät voivat luoda transaktioita anonyymisti. Ethereum tarjoaa Turing-täydellisen ohjelmointikielen Solidityn, jolla voidaan kehittää älykkäitä sopimuksia ja sen jälkeen asentaa sopimukset Ethereumin lohkoketjuun suoritettavaksi. (Buterin, 2014)

Ethereum suunniteltiin aluksi päivitetyksi versioksi kryptovaluutasta, joka tarjoaa edistyneempiä ominaisuuksia, kuten nostorajoja, rahoitussopimuksia, uhkapelimarkkinoita ja muita vastaavia yleisen ohjelmointikielen kautta. Ethereum ei tue mitään sovelluksia suoraan, mutta Turing-täydellisen ohjelmointikielen olemassaolo tarkoittaa, että teoreettisesti voidaan luoda millaisia tahansa sopimuksia mille tahansa tapahtumalle tai sovellukselle. Ethereum on paljon pidemmälle viety kuin pelkkä kryptovaluutta. Protokollilla ja hajautetuilla sovelluksilla on potentiaalia lisätä huomattavasti tietojenkäsittelyalan tehokkuutta ja auttaa muitakin vertaisverkkoprotokollia. (Buterin, 2014) Ethereumin jäl-

keen on julkaistu monia muita lohkoketjuja, joissa pystytään suorittamaan älykkäitä sopimuksia, kuten EOS, Neo, Qtum ja IOTA (Li ym., 2021).

3 Lohkoketjuteknologian haasteet

Tässä luvussa tarkastellaan lohkoketjuteknologian haasteita ja ratkaisuja niihin. Haasteita tarkastellaan useista näkökulmista painottuen teknologisiin haasteisiin. Yleisesittelyn jälkeen keskitytään tarkemmin kolmeen eri haasteeseen, jotka ovat energian kulutus, skaalautuvuus ja turvallisuus. Nämä kolme haastetta on valittu tarkasteltavaksi, sillä ne ovat suuresti esillä tarkastellussa kirjallisuudessa. Haasteiden ja niiden vaikutusten tarkastelemisen jälkeen käsitellään niihin ehdotettuja ratkaisuja.

Lohkoketjujen haasteita voidaan tarkastella kolmesta näkökulmasta, joita ovat teknologiset-, organisatoriset- ja ympäristölliset haasteet. (Batubara ym., 2018) Myös Toufaily, Zalan ja Dhaou (2021) jakavat lohkoketjuteknologiaan kohdistuvat haasteet näihin näkökulmiin. Ali, Jaradat, Kulakli ja Abuhalimeh (2021) taas jakavat haasteet teknologisiin, organisatorisiin, operatiivisiin, omaksumisen ja ympäristöllisiin haasteisiin. Kaikki näkökulmat kuitenkin sisältävät useita haasteita, joihin lohkoketjuteknologian täytyy pystyä vastaamaan.

Teknologisia haasteita ovat esimerkiksi turvallisuus, skaalautuvuus, yhteensopivuus, luotettavuus ja kustannustehokkuus, joista suurimmat haasteet liittyvät turvallisuuteen ja skaalautuvuuteen (Batubara ym., 2018). Swan (2015) jakaa teknologiset haasteet seuraaviin: suorituskyky, viive, koko ja kaistanleveys, käytettävyys, turvallisuus, tuhlatut resurssit ja haarautumat. Fournier & Petrillo (2020) esittelevät kolmeksi suureksi haasteeksi skaalautuvuuden, turvallisuuden ja konsensusprotokollat. Yleisesti ottaen teknologian kypsymättömyys on syynä kaikkiin teknologisiin haasteisiin, mikä on yleistä kaikissa uusissa teknologioissa. Tutkimuskehitys on näiden haasteiden voittamiseksi kuitenkin varsin lupaavaa. (Batubara ym., 2018)

Organisatorisesta näkökulmasta suurimmat haasteet liittyvät hyväksyttävyyteen ja uusien hallintomallien tarvitsemiseen. Koska lohkoketjualustat vaativat useiden instituutioiden ja sidosryhmien yhteistyötä, tarvitaan uusia hallintomalleja. (Batubara ym., 2018) Toufaily ym. (2021) erottelevat kolme suurinta organisatorista estettä lohkoketjujen adoptiolle: hallintojen ja johtajien valmiuden, liiketoimintamallien mukauttamisen lohkoketjuihin ja organisaatioiden valmiuden. Kaiken kaikkiaan organisatorinen valmius on tärkeää lohkoketjujen

adoptiossa ja teknologian käyttöönoton tarkoituksena on muuttaa organisaatioita niin, että ne voivat parantaa suorituskykyään ja tehokkuuttaan (Batubara ym., 2018).

Ympäristöllisiin haasteisiin liittyvinä tärkeimpinä tekijöinä voidaan pitää lakeja ja sääntelyä, mitkä tukevat lohkoketjuteknologian käyttöönottoa. Laki ja sääntely ovat välttämättömiä sen varmistamiseksi, että käyttäjillä on varmuus sopimuspuolten oikeuksia ja velvollisuuksia määritellessä. (Batubara ym., 2018) Upadhyay (2020) esittää, että hallituksien haluttomuus säännellä ja linjata lohkoketjuteknologian aloitteita rajoittaa lohkoketjuteknologian käyttöönottoa. Myös Toufaily ym. (2021) esittävät, että sääntelyn epävarmuus on keskeinen haaste, joka hidastaa ja estää lohkoketjuteknologian käyttöönottoa.

3.1 Teknologiset haasteet

Teknologiset haasteet ovat erittäin suuressa osassa lohkoketjujen haasteita tarkastellessa. Seuraavaksi esitellään tarkemmin kolme teknologista haastetta, jotka ovat energian kulutus, skaalautuvuus ja turvallisuus.

3.1.1 Energian kulutus

Useat lohkoketjut käyttävät hyvin suurta energiamäärää. Esimerkiksi Bitcoinin energiankulutus on arvioitu tällä hetkellä olevan noin 80 terawattituntia vuodessa (Digiconomist, 2021). Lohkoketjuteknologian energiankulutukseen liittyvässä tutkimuksessa (Sedlmeir, Buhl, Fridgen & Keller, 2020) arvioidaan Bitcoinin energiankulutuksen olevan noin 60–125 terawattituntia vuodessa. Suomen energiankulutus on noin 85 TWh vuodessa, joten Bitcoinin louhintaan käytetään lähes saman verran energiaa kuin koko Suomen energiankulutukseen vuosittain (Digiconomist, 2021). On myös huomattava, että arvioihin ei sisälly muuhun kuin louhintaan käytettävä energia. Energian kulutusta lisää myös esimerkiksi laitteiston ja rakennusten jäähdytyskustannukset.

Louhintaan käytettävä energia voidaan laskea esimerkiksi kaavalla: energian kulutus ≥ kokonaislaskentateho × minimissään käytetty energia per laskenta. Tällä kaavalla saadaan hyvin tarkka minimikulutus. Yksittäiseen laskentaan käytetty energia riippuu käytettävästä laitteistosta, joka vaihtelee. Eri lohkoketjut käyttävät eri algoritmeja, esimerkiksi Bitcoin käyttää SHA256-algoritmia, jolle on olemassa mikropiirejä, jotka ovat erittäin optimoituja tiivistearvojen laskemiseen. Tämän ansiosta Bitcoinin minimienergian kulutus on helppo laskea aikaisemmalla kaavalla. On kuitenkin huomioitava, että kaikki louhijat eivät käytä parhaimpia mahdollisia laitteita, joten laskettu energian kulutus on vain arvio. Kaikki lohkoketjut eivät myöskään käytä algoritmeja, joille on suunniteltu optimoidut louhintalaitteet. Esimerkiksi Ethereum on suunniteltu estämään erittäin spesifisten louhintalaitteiden käytön, joten lou-

hintaan voidaan käyttää yleiskäyttöisiä grafiikkasuorittimia. (Sedlmeir ym., 2020)

Kaikki lohkoketjut eivät kuitenkaan tarvitse suurta määrää energiaa niiden ylläpitämiseen. Tiettyjen lohkoketjujen, kuten Bitcoinin ja Ethereumin suuri energiankulutus johtuu niiden käyttämästä PoW-konsensusalgoritmista. PoW-algoritmissa selvitettävien matemaattisten ongelmien ratkaiseminen, jota jokainen louhija ratkaisee, vaatii huomattavaa laskentatehoa. Tämä johtaa suureen energian kulutukseen. (Cole & Cheng, 2018) Sedlmeir ym., (2020) huomauttaa, että PoW-lohkoketjujen suuri energiankulutus ei johdu tehottomista algoritmeista tai vanhentuneista laitteista, vaan siitä, että ne ovat suunniteltu sellaisiksi. Suuri energian kulutus suojaa PoW-lohkoketjuja hyökkäyksiltä, sillä hyökkääjällä olisi oltava suuri osa laskentatehosta hallitakseen lohkoketjua.

3.1.2 Skaalautuvuus

Skaalautuvuus on yksi lohkoketjuteknologian suurista ongelmista. Yang, Long, Xu ja Peng (2020) mainitsevat skaalautuvuusongelmasta erityisesti sen, että lohkoketjuilla on usein matala transaktiotehokkuus ja korkea transaktioiden vahvistusviive. Artikkelissa mainitaan esimerkiksi, että Bitcoin pystyy suorittamaan 7 transaktiota sekunnissa ja Ethereum noin 30 transaktiota sekunnissa. Kyseiset transaktiomäärät ovat erittäin pieniä verrattaessa esimerkiksi Visaan, joka suorittaa keskimäärin 150 miljoonaa transaktiota päivässä, eli noin 1700 transaktiota sekunnissa (Visa, 2010). Vukolić (2015) toteaa myös, että bitcoin pystyy suorittamaan noin 7 transaktiota sekunnissa, kun taas suurimmat luottokorttiyhtiöt suorittavat keskimäärin noin 2000 transaktiota sekunnissa.

Transaktioiden vahvistusviive on myös huomattavan korkea lohkoketjuissa. Bitcoinin lohkoketjussa luodaan uusi lohko noin kymmenen minuutin välein (Blockchain.com, 2021), joten transaktioiden vahvistusviive on vähintään 10 minuuttia. Yleensä kuitenkin vaaditaan useamman lohkon vahvistus transaktioille, jolloin transaktion vahvistaminen kestää useita kymmeniä minuutteja. Myös Ethereumissa, joka on huomattavasti Bitcoinia nopeampi, vahvistaminen kestää noin 18 sekuntia. (Yang ym., 2020) Etherscan.io (2021) verkkosivulta selviää, että Ethereumin keskimäärinen lohkoaika viimeisen vuoden aikana on ollut noin 13 sekuntia. Lohkoajat kuitenkin nousevat ajoittain, esimerkiksi helmikuussa 2019 lohkoajat olivat jopa 20 sekuntia. Tämä tarkoittaa, että jos transaktion lopulliseen varmistamiseen vaaditaan esimerkiksi 10 lohkovarmistusta, kestää transaktion vahvistamisessa yli kaksi minuuttia. Transaktioiden hitauteen liittyy myös se, että lohkokoko on esimerkiksi Bitcoinin tapauksessa rajattu yhteen megatavuun, joka rajoittaa transaktioiden määrää lohkossa (Xie ym., 2019). Tämä tarkoittaa, että transaktioita mahtuu yhteen lohkoon keskimäärin noin 2000 kappaletta. Skaalautuvuusongelmat johtuvat siis rajoitetusta lohkokoosta, pitkästä lohkoajasta ja nykyisistä konsensusmenetelmistä, joissa jokainen verkon solmu vahvistaa peräkkäin tapahtuman ennen kuin se viedään lohkoketjuun (Chauhan, Malviya, Verma & Mor, 2018).

3.1.3 Turvallisuus

Lohkoketjuilla on useita turvallisuusuhkia, jotka voidaan luokitella yleisesti ottaen seuraaviin: kaksinkertaisen kulutuksen uhat, verkkouhat, louhijayhteisöjen uhat ja lompakkojen turvallisuusuhat (Bhushan, Sinha, Sagayam & Andrew, 2020). Kaksinkertainen kulutus tarkoittaa sitä, että joku lähettää saman transaktion useamman kuin kerran ja täten käyttää enemmän rahaa kuin hänellä oikeasti on (Gervais ym., 2016). Hyökkäyksen, joka mahdollistaa kaksinkertaisen kulutuksen voi suorittaa monella eri tapaa, mutta yksi tunnetuimmista on 51% hyökkäys.

51% hyökkäys on hyökkäys erityisesti PoW-lohkoketjuja vastaan, missä hyökkääjä, joka hallitsee suurinta osaa, vähintään 51% verkon laskentatehosta pystyy hylkäämään muiden louhijoiden lohkot asettamalla etusijalle omat lohkonsa. Tällainen hyökkäys ei salli hyökkääjän luoda rahaa tyhjästä, mutta se antaa mahdollisuuden kaksinkertaiseen kuluttamiseen. Käytännössä tällaiset hyökkäykset ovat erittäin kalliita suurille verkoille, joilla on korkea hajautusaste, kuten Bitcoinilla. (Amiet, 2021)

Verkkoon kohdistuvia uhkia on myös useita, kuten transaktioiden muokattavuushyökkäys, sybil-hyökkäys ja eclipse-hyökkäys. Muokattavuushyökkäyksessä hyökkääjät yrittävät saada kohteen uskomaan, että tietty transaktio on epäonnistunut, ja pyytää toistamaan saman tapahtuman muuttamalla transaktion tiivistettä ennen sen vahvistamista. Tällaista voidaan pitää eräänlaisena kaksinkertaisena kuluttamisena, jossa hyökkääjät eivät ole tapahtuman varmentajia. Sybil-hyökkäys keskittyy mainejärjestelmän heikentämiseen tuomalla väärennettyjä identiteettejä verkkoon. Hyökkääjät hajottavat mainejärjestelmän luomalla lukuisia pseudonyymejä identiteettejä ja hyödyntämällä niitä valtavan vaikutusvallan saamiseksi. Eclipse-hyökkäyksessä hyökkääjä hallitsee valtavaa määrää IP-osoitteita ja monopolisoi kaikki yhteydet yhteen uhrisolmuun. Tällä tavalla hyökkääjä voi estää solmua näkemästä, mitä verkossa oikeasti tapahtuu ja hyödyntää tätä erilaisiin hyökkäyksiin, kuten itsekkääseen louhintaan ja kaksinkertaiseen kuluttamiseen. (Bhushan ym., 2020)

Louhijayhteisöihin kohdistuvia uhkia ovat erilaiset hyökkäykset, jotka hyödyntävät yhteisön haavoittuvuuksia käynnistääkseen sekä ulkoisia että sisäisiä hyökkäyksiä louhijayhteisöön. Näitä hyökkäystyyppejä ovat esimerkiksi itsekkään louhinnan hyökkäys ja lohkon löytämisen panttaaminen yhteisöltä. (Bhushan ym., 2020) Lisäksi louhijayhteisöjen koon kasvaminen liian isoksi on riski hajauttamisen kannalta, koska se mahdollistaa myös erilaiset hyökkäykset, kuten 51 %-hyökkäyksen. (Zhang ym., 2020) Lompakkojen turvallisuusuhkiin kuuluu esimerkiksi haavoittuva allekirjoitus, virheellinen avainten luominen, osoitteen luomisen hallinnan puuttuminen ja preimage-hyökkäys (Bhushan ym., 2020).

3.2 Mahdollisia ratkaisuja haasteisiin

Lohkoketjuteknologialla on selvästi useita haasteita ja ongelmia, joista on esitelty osa tässä tutkielmassa. Näihin haasteisiin on kuitenkin ehdotettu ja kehitetty erilaisia ratkaisuja, joita käsittelemme tässä luvussa.

3.2.1 Energian kulutus

Erittäin suuri energian kulutus on yksi suurimpia lohkoketjuteknologian ongelmia, Digiconomist (2021) on arvioinut yhden Bitcoin transaktion käyttävän noin 800 kWh sähköä, joka on miltei saman verran kuin keskimääräinen kotitalouden sähkönkulutus kuukaudessa Yhdysvalloissa. ING pankin raportissa (2017) arvioidaan sen hetkisen energiankulutuksen yhteen transaktioon olevan 200 kWh Bitcoin-verkossa, 37 kWh Ethereum-verkossa ja 0.01 kWh Visan suorittamissa transaktioissa. Cole ja Cheng (2018) vertailivat artikkelissaan neljän eri lohkoketjun energiankulutusta transaktioissa. Artikkelin mukaan arvioitu energiankulutus yhdessä Bitcoin transaktiossa vaihtelee 200 kWh ja 950 kWh välillä, kun taas Ethereumin verkossa yksi transaktio kuluttaa noin 75 kWh. Bitcoin ja Ethereum käyttävät PoW-konsensusmekanismia. Ripple protokollan konsensusalgoritmi oli artikkelin mukaan huomattavasti vähemmän energiaa kuluttava, sillä se käytti vain 0,5Wh yhteen transaktioon ja Stellar konsensusprotokolla vielä vähemmän. Ilmeisin ratkaisu on siirtyä PoW-konsensusmekanismista johonkin muuhun vähemmän energiaa vaativaan mekanismiin.

PoS-konsensusmekanismi yrittää ratkaista PoW-lohkoketjujen energiankulutusongelman. Tämän saavuttaakseen PoS-mekanismi korvaa PoW-mekanismin laskentateholla kilpailemisen valitsemalla satunnaisesti seuraavan lohkon luojan (Saleh, 2018). Sedlmeir ym. (2020) esittävät artikkelissaan, että luultavasti paras jo tunnettu ratkaisu PoW-konsensusmekanismin korvaajaksi on PoS-konsensusmekanismi. Artikkelissa mainitaan, että Ethereum, joka on toiseksi suurin lohkoketju markkina-arvoltaan, on siirtymässä PoW-mekanismista PoS-mekanismiin. PoS-mekanismin käyttöönotosta ja toimivuudesta on jo useita esimerkkejä, kuten EOS, Tezos ja Tron. Irresberger, John ja Saleh (2020) mainitsevat artikkelissaan, että yli 50 PoS-lohkoketjua on julkistettu vuoden 2015 jälkeen ja käyttöönotetut PoS-lohkoketjut ovat enemmän käytettyjä kuin PoW-lohkoketjut.

Konsensusmenetelmää muuttamalla voidaan muuttaa energian kulutusta huomattavasti pienemmäksi, mutta on myös muita asioita, millä sitä voidaan pienentää. Energian kulutusta voidaan pienentää huomattavasti vähentämällä tarpeetonta työtä. Yksi usein mainittu ratkaisu ylimääräisen työn vähentämiseen on niin kutsuttu sirpaloituminen. Siinä lohkoketju jaetaan osajoukkoihin ja tiettyjen transaktioiden prosessointi tapahtuu vain yhdessä osajoukossa, mikä vähentää turhaa työtä, koska jokaisen solmun ei tarvitse käsitellä jokaista transaktiota. Sirpaloituminen on lisäksi helpompaa toteuttaa PoS-lohkoketjussa

kuin PoW-lohkoketjussa, mikä lisää PoS-konsensusmekanismien etua verrattuna PoW-konsensusmekanismeihin. (Sedlmeir ym., 2020)

3.2.2 Skaalautuvuus

Lohkoketjujen skaalautuvuusongelmaan on esitetty lukemattomia eri ratkaisuja, joista käymme osan läpi tässä kappaleessa. Ratkaisuja on lukematon määrä, mutta ne voidaan jakaa osiin. Zhou, Huang, Zheng ja Bian (2020) ovat jakaneet skaalautumisratkaisut kolmeen eri tasoon: ketjun sisäisiin, ketjun ulkopuolisiin ja muihin. Kim, Kwon ja Cho (2018) taas jakavat skaalautumisratkaisut viiteen eri osaan, jotka ovat ketjun sisäiset-, ketjun ulkopuoliset-, sivuketju-, lapsiketjuja ketjujen väliset ratkaisut. Yang ym. (2020) esittelevät artikkelissaan neljä tunnettua ratkaisua skaalautuvuusongelmaan: sirpaloitumisen, DAG-teknologian, lohkoketjun ulkopuoliset transaktiot ja lohkoketjujen välisen tekniikan. Jokaiseen edellä mainittuun osaan kuuluu useita erilaisia lähestymistapoja, mutta artikkelien perusteella mikään ei ole yksin täydellinen ratkaisu ongelmaan.

Esimerkiksi vuonna 2017 Bitcoin jakautui kahteen eri lohkoketjuun, Bitcoiniin ja Bitcoin Cashiin lohkokoon kasvattamisen yhteydessä. Bitcoin säilytti alkuperäisen 1 megatavun lohkokokonsa ja Bitcoin Cash otti käyttöön uuden 8 megatavun lohkokoon. Tämä haarautuma tehtiin skaalautuvuusongelman ratkaisemiseksi ja myöhemmin Bitcoin Cash-ketjun lohkokokoa kasvatettiin edelleen 32 megatavuun. Lohkokoon kasvattaminen ratkaisi osittain skaalautuvuusongelman, mutta ei ilman haittavaikutuksia. Lohkokoon kasvattaminen mahdollistaa sen, että enemmän transaktioita mahtuu yhteen lohkoon, mikä kasvattaa transaktioiden määrää. Kuitenkin se aiheuttaa samalla sen, että lohkojen siirtäminen vaikeutuu lohkojen koon vuoksi ja lohkoketjujen sisäisen kaistanleveyden vuoksi. (Zhou ym., 2020) Lohkokoon kasvattamisella, joka on helpolta tuntuva ratkaisu skaalautuvuusongelman ratkaisemiseen, on myös muita haittapuolia. Yksi ongelma on se, että suurempien lohkojen prosessointi vaatii tehokkaampia laitteita. Tämä voi johtaa siihen, että louhijoiden määrä laskee ja louhinnasta tulee keskitettyä, mikä vähentää lohkoketjuteknologian hajautunutta luonnetta. (BitFury Group, 2015) Toinen yksinkertainen ratkaisu ongelmaan on lyhentää lohkojen intervallia, jolloin luodaan enemmän lohkoja ja täten varmennetaan enemmän transaktioita. Lohkojen intervallin lyhentäminen kuitenkin vaikuttaa järjestelmän turvallisuuteen, sillä se kasvattaa haarautumien syntymistä (Zhou ym., 2020).

Suurin osa lohkoketjujen skaalautuvuutta ja tietoturvaongelmia koskevista tutkimuksista ovat samaa mieltä siitä, että suurin ongelman aiheuttaja on PoW-konsensusmekanismi, jota Bitcoin ja monet muut lohkoketjut käyttävät. Niin kauan kuin Nakamoto-protokollaa ei muuteta voimakkaasti tai korvata kokonaan jollain toisella konsensusprotokollalla, Bitcoinin tapahtuma-ajat tulevat olemaan hitaita. Siksi sopivan konsensusprotokollan valitsemisella on paljon merkittävämpi rooli, kuin lohkoketjujen uudelleenparametrisoinnilla. Ideaalissa tilanteessa uusi konsensusprotokolla poistaisi skaalautuvuuden ja turvallisuuden välisen kompromissin. (Fournier & Petrillo, 2020)

3.2.3 Turvallisuus

Lohkoketjuilla on lukemattomia turvallisuusuhkia, joista kävimme osan läpi aikaisemmin. Lohkoketjujen turvallisuusuhkiin on kuitenkin useita ratkaisuja: 51% hyökkäys on teoriassa helppo estää estämällä mitään tahoa saamasta suurinta osaa louhintatehoa verkosta (Bhushan ym., 2020). Sen estäminen ei kuitenkaan välttämättä ole mahdollista, joten tarvitaan myös muitakin suojia mahdollisille hyökkäyksille. Artikkelissaan Rosenfeld (2014) esittää, että hyökkääjät eivät välttämättä tarvitse edes 51% koko laskentatehosta, vaan hyökkäys voi onnistua millä tahansa osuudella koko laskentatehosta. Onnistumisesta vain tulee epätodennäköisempää, mitä pienemmällä laskentateholla hyökkäys tapahtuu (Rosenfeld, 2014). Artikkelissaan Sayeed ja Marco-Gisbert (2019) esittelevät viisi tunnettua tekniikkaa, joilla voidaan vähentää 51% hyökkäyksiä. He selvittivät, että mikään näistä viidestä ei kuitenkaan tarjoa riittävää suojaa hyökkäystä vastaan, vaan lohkoketjujen on otettava lisäksi käyttöön turvallisuuskäytäntöjä, jotka vaikeuttavat ja estävät hyökkäyksen toteuttamisen. Tärkein käytäntö ovat se, että konsensusprotokollan on hyväksyttävä lohkoketjuun tuotavaksi vain tietty rajoitettu määrä lohkoja kerrallaan. Tämä estää hyökkääjiä tuomasta lohkoketjuun rajoittamatonta määrää uusia lohkoja lyhyellä aikavälillä ja täten estää hyökkääjiä saamasta pisintä ketjua ja lohkoketjun hallintaa itselleen. (Sayeed & Marco-Gisbert, 2019)

Muihin aiemmin esitettyihin turvallisuusuhkiin on myös kehitetty ratkaisuja. BIP 62 (Bitcoin Impromevent Proposal) on tehokas vastatoimenpide transaktioiden muokattavuushyökkäystä vastaan, sillä se sisältää useita tapahtumanvahvistustietoja uusien tapahtumien vahvistamista varten (Bhushan ym., 2020). Swathi, Modi & Patel (2019) ovat esittäneet Sybil-hyökkäysten estämiseksi järjestelmää, joka seuraa muiden solmujen käyttäytymistä ja tarkistaa solmut, jotka välittävät vain tietyn käyttäjän lohkoja. Louhijoita ja louhijayhteisöjä koskevia uhkia vastaan on kehitetty myös ratkaisuja. Saad, Njilla, Kamhoua ja Mohaisen (2019) ovat kehittäneet ratkaisun itsekästä louhintaa vastaan. Artikkelin mukaan heidän kehittämä algoritmi estää tehokkaasti itsekästä louhintaa ja kannustaa oikeanlaisiin louhintakäytäntöihin. Myös lohkon panttaamista vastaan on kehitetty ratkaisuja: Lee ja Kim (2019) esittelevät artikkelissaan vastatoimen lohkon panttaamista vastaan, minkä louhijayhteisöt voivat ottaa helposti käyttöön.

Lohkoketjujen turvallisuusuhkia vastaan on kehitetty monia eri ratkaisuja, mutta se ei tarkoita, että ne olisivat täysin turvallisia. Suurimpia ja käytetyimpiäkin lohkoketjuja vastaan on onnistuneita hyökkäyksiä, kuten 2016 vuoden DAO-hyökkäys. DAO oli älysopimus, joka otettiin käyttöön Ethereumin verkossa. Se ehti toimia 20 päivää, kunnes sitä vastaan tehtiin onnistunut hyökkäys, jossa hyökkääjä varasti noin 60 miljoonan dollarin edestä Etheriä. Hyökkäys ei kuitenkaan tapahtunut Ethereum-verkkoon vaan DAO-älysopimukseen hyödyntämällä sen haavoittuvuuksia. Tämäntyyppiset tapaukset kuitenkin osoittavat, että kokeneetkin kehittäjät voivat jättää järjestelmän vakavasti alttiiksi

hyökkääjille, jotka pyrkivät hyödyntämään haavoittuvuuksia älysopimuksissa. (Singh, Hosen & Yoon, 2021)

4 Yhteenveto

Tässä tutkielmassa tarkasteltiin lohkoketjuteknologian haasteita ja ratkaisuja niihin. Ensin tutkielmassa esiteltiin, mitä lohkoketjuteknologia on, jonka jälkeen tarkasteltiin konsensusmekanismeja ja lohkoketjuteknologian laajennuksia kryptovaluuttojen ulkopuolelle. Tämän jälkeen käytiin läpi lohkoketjuteknologian haasteita kolmesta eri näkökulmasta, jotka olivat teknologinen, ympäristöllinen ja organisatorinen. Teknologisiin haasteisiin kiinnitettiin erityistä huomiota, sillä ne olivat eniten esillä kirjallisuutta tarkastellessa. Teknologisista haasteista esiteltiin tarkemmin kolme haastetta, jotka olivat energian kulutus, skaalautuvuus ja turvallisuus. Haasteiden tarkastelun jälkeen käytiin läpi niihin kehitettyjä ratkaisuja.

Tutkielman ensimmäinen tutkimuskysymys oli ”Mitä ovat lohkoketjuteknologian suurimmat haasteet,” ja tarkastellun kirjallisuuden mukaan energian kulutus, skaalautuvuus ja turvallisuus kuuluvat niihin. Nämä kolme kuuluvat lohkoketjuteknologian suurimpiin haasteisiin, mutta lohkoketjuilla on valtavasti muitakin haasteita, joita tutkielmassa käytiin läpi lyhyesti. Ei voida myöskään perusteltavasti sanoa, että juuri nämä kolme haastetta ovat ne suurimmat haasteet. Yleisesti ottaen teknologian kypsymättömyys on syynä kaikkiin teknologisiin haasteisiin, mikä on yleistä kaikissa uusissa teknologioissa (Batubara ym., 2018).

Toinen tutkimuskysymys oli ”Minkälaisia ratkaisuja on kehitetty vastaamaan haasteisiin,” ja selvisi, että haasteisiin on ehdotettu ja kehitetty monenlaisia ratkaisuja. Kuitenkin suurimmassa osassa tapauksista päädyttiin lopulta ratkaisuun, että konsensusmekanismilla on suurin rooli haasteiden ratkaisemisen kannalta (Fournier & Petrillo, 2020; Cole & Cheng, 2018). Tämä korostuu varsinkin PoW-lohkoketjujen kohdalla, koska niiden perusominaisuuksiin kuuluu esimerkiksi suuri energian kulutus. PoW-lohkoketjujen skaalautuvuutta on myös vaikea parantaa merkittävästi ilman haittavaikutuksia. PoW-konsensusmekanismin korvaajaksi paras tämänhetkinen ratkaisu on PoS-konsensusmekanismi (Sedlmeir ym., 2020; Saleh, 2018).

Lohkoketjuteknologian haasteiden ratkaisemiseksi ei ole selvää yhteisymmärrystä, vaan haasteisiin on ehdotettu useita ratkaisuja ja mahdollisuuksia.

Eri lohkoketjut implementoivat eri ratkaisuja ja erilaisia versioita konsensusmekanismeista, mikä auttaa ratkaisujen arvioimista. Ei ole olemassa kuitenkaan yhtä täydellistä ratkaisua, joka vastaisi kaikkiin haasteisiin ilman negatiivisia vaikutuksia. Esimerkiksi usein ehdotetussa PoS-konsensusmekanismissa, joka onnistuu vähentämään energiankulutuksen merkityksettömälle tasolle ja auttaa suuresti skaalautuvuusongelmassa, on omat ongelmansa (Saleh, 2018). On todennäköistä, että lohkoketjujen täytyy implementoida useita eri ratkaisuja ratkaistakseen haasteet. Lohkoketjuja on lisäksi paljon, ja ne ovat lähtökohtaisesti erilaisia toisiin vertaillessa. Tämä voi johtaa siihen, että mahdollisia ratkaisuja ei pystytä yleistämään useisiin lohkoketjuihin, vaan jokaisen lohkoketjun täytyy muuttaa ratkaisuja itselleen sopiviksi.

Tutkielma sisältää useita rajoitteita, mitkä voivat vaikuttaa tuloksiin. Tutkimusaiheen laajuus rajoittaa tutkimuksen syvyyttä ja tutkielman tarkoituksena on antaa yleiskuva lohkoketjuteknologian haasteiden eri osa-alueista ja niiden laajuudesta. Yleiskuvan lisäksi käsiteltiin tarkemmin vain kolmea eri haastetta ja niiden ratkaisuja. Nämä kolme ovat itsessään erittäin moniulotteisia ja ei voida olettaa, että ne käsiteltiin kokonaisvaltaisesti. Varsinkin ehdotettuja ratkaisuja on valtavasti ja eri lohkoketjut implementoivat eri ratkaisuja ratkaisemaan samankaltaisia ongelmia. Tutkielman perusteella voidaan kuitenkin mainita erityisesti se, että konsensusmekanismeilla ja niiden muuttamisella on suurin rooli haasteiden ratkaisemisen kannalta. Hyviä jatkotutkimusaiheita ovat tämän perusteella erityisesti eri konsensusmekanismeihin kohdistuvat tutkimukset.

Lohkoketjuja ja niiden konsensusmekanismeja muutettaessa on kuitenkin mietittävä, miten paljon ja millä tavalla niitä voidaan muuttaa. Lohkoketjujen ominaisuuksiin kuuluva hajautettu luonne ei saa kärsiä muutoksista. Lohkoketjut ovat esitelty luottamuksen ongelman ratkaisijoina, joka johtuu suoraan niiden hajautetusta luonteesta ja yhden keskuskontrollin puutteesta. Erittäin keskitetyistä lohkoketjuista on useita esimerkkejä, kuten Binance Smart Chain (BSC). BSC on hyvin pitkälle samanlainen lohkoketju kuin Ethereum, ja myös se mahdollistaa erilaisten älykkäiden sopimusten luomisen lohkoketjuun. BSC käyttää kuitenkin Proof of Authority (PoA)-konsensusmekanismia, toisin kuin Ethereum, joka käyttää tällä hetkellä PoW-mekanismia ja on siirtymässä PoS-mekanismiin. PoA-konsensusmekanismissa lohkokoko voidaan pitää suhteellisen suurena ja lohkoaika lyhyenä, jolloin transaktioiden määrä voi olla erittäin suuri ilman että lohkoketju ruuhkautuu ja transaktiokulut kasvavat. Tällä on kuitenkin hintansa, sillä BSC lohkoketjulla on vain 21 validoijaa, joka on erittäin vähän verrattuna esimerkiksi Bitcoinin ja Ethereumin tuhansiin louhijoihin. Tämä johtaa väistämättä kysymyksiin BSC-ketjun luonteesta ja sen luotettavuudesta, koska sitä ei voi sanoa millään tasolla hajautetuksi.

On mielenkiintoista huomata, että vaikka BSC on erittäin keskitetty ja rikkoo lohkoketjuteknologian perustavanlaatuisia ominaisuuksia, sillä on erittäin paljon käyttäjiä. Esimerkiksi 21.4.2021 BSC:lla oli yli miljoona aktiivista osoitetta (BscScan.com, 2021), kun taas Ethereumilla oli samana päivänä hieman yli 700000 aktiivista osoitetta (Etherscan.io, 2021). BSC lohkoketjussa on myös suoritettu huomattavasti enemmän transaktioita viime kuukausina kuin Ethereu-

min lohkoketjussa. Nämä huomiot ovat lyhyeltä ajalta, joten niistä ei voi päätellä mitään lopullista, sillä tilanne voi muuttua nopeasti. Ne kuitenkin johtavat myös kysymyksiin siitä, että onko käyttäjille lopulta merkitystä hajauttamisella tai muilla lohkoketjuteknologian mahdollistamilla perustavanlaatuisilla ominaisuuksilla. Voiko tämänkaltaisia lohkoketjuja, jotka eivät ole hajautettuja tai ovat muuten suuresti erilaisia alkuperäiseen lohkoketjuideaan verrattuna enää kutsua lohkoketjuiksi? Nakamoton (2008) liikkeelle laskema ajatus hajautetusta ja kontrolloimattomasta valuutasta on kasvanut ja laajentunut vuosien varrella suuresti. Sen perusajatuksina olleet luottamuksen takaajien tarpeettomuus ja lohkoketjun muuttumattomuus ovat tärkeitä asioita, jotka ovat tuoneet lohkoketjuteknologian suureen tietoisuuteen. Lohkoketjut kattavat nykyään hajautetun valuutan lisäksi lukemattomia muita mahdollisuuksia, mutta niiden perustavanlaatuisten ominaisuuksien on pysyttävä samankaltaisina kuin aikaisemmin.

LÄHTEET

Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. IEEE Access, 9, 12730-12749.

Amiet, N. (2021). Blockchain Vulnerabilities in Practice. *Digital Threats: Research and Practice*, *2*(2), 1-7.

Batubara, F. R., Ubacht, J., & Janssen, M. (2018, May). Challenges of blockchain technology adoption for e-government: a systematic literature review. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (pp. 1-9).

Bhushan, B., Sinha, P., Sagayam, K. M., & Andrew, J. (2020). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, 106897.

BitFury Group (2015) Haettu 10.4.2021 osoitteesta https://bitfury.com/content/downloads/block-size-1.1.1.pdf

Blockchain.com (2021) Haettu 8.4.2021 osoitteesta https://www.blockchain.com/charts/median-confirmation-time

BscScan.com (2021) Haettu 28.4.2021 osoitteesta https://bscscan.com/chart/active-address

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37).

Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*.

Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018, July). Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 122-128). IEEE.

Cole, R., & Cheng, L. (2018, July). Modeling the energy consumption of blockchain consensus algorithms. In *2018 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)* (pp. 1691-1696). IEEE.

Digiconomist (2021) Haettu 25.3.2021 osoitteesta https://digiconomist.net/bitcoin-energy-consumption/

Etherscan.io (2021) Haettu 5.4.2021 osoitteesta https://etherscan.io/chart/blocktime

Etherscan.io (2021) Haettu 28.4.2021 osoitteesta https://etherscan.io/chart/active-address

Fournier, G., & Petrillo, F. (2020, June). Architecting Blockchain Systems: A Systematic Literature Review. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops* (pp. 664-670).

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 3-16).

Gupta, S., Hellings, J., Rahnama, S., & Sadoghi, M. (2020, July). Blockchain consensus unraveled: virtues and limitations. In *Proceedings of the 14th ACM International Conference on Distributed and Event-based Systems* (pp. 218-221).

Honkanen, P. (2017). Lohkoketjuteknologian lupaus.

ING (2017) Haettu 9.4.2021 osoitteesta https://think.ing.com/opinions/why-bitcoin-transactions-are-more-expensive-than-you-think

Irresberger, F., John, K., & Saleh, F. (2020). The public blockchain ecosystem: An empirical analysis. *NYU Stern School of Business*.

Kietzmann, J., & Archer-Brown, C. (2019). From hype to reality: Blockchain grows up. *Business Horizons*, *62*(3), 269-271.

Kim, S., Kwon, Y., & Cho, S. (2018, October). A survey of scalability solutions on blockchain. In 2018 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1204-1207). IEEE.

Lee, S., & Kim, S. (2019, April). Countering block withholding attack efficiently. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 330-335). IEEE.

Li, X., Zheng, Z., & Dai, H. N. (2021). When services computing meets blockchain: Challenges and opportunities. Journal of Parallel and Distributed Computing, 150, 1-14.

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

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*, *7*, 85727-85745.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187.

Panetta (2018) Haettu 18.3.2021 osoitteesta https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Rosenfeld, M. (2014). Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009.

Saad, M., Njilla, L., Kamhoua, C., & Mohaisen, A. (2019, February). Countering selfish mining in blockchains. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 360-364). IEEE.

Saleh, F. (2018). Blockchain without waste: Proof-of-stake. The Review of Financial Studies.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. Applied Sciences, 9(9), 1788.

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: beyond myth. *Business & Information Systems Engineering*, *62*(6), 599-608.

Shermin, V. (2017). Disrupting governance with blockchains and smart contracts. Strategic Change, 26(5), 499-509.

Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. IEEE Access, 9, 13938-13959.

Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

Swathi, P., Modi, C., & Patel, D. (2019, July). Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

Szabo, N. (1996). Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16), 18(2).

Thin, W. Y. M. M., Dong, N., Bai, G., & Dong, J. S. (2018, December). Formal analysis of a proof-of-stake blockchain. In *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)* (pp. 197-200). IEEE.

Toufaily, E., Zalan, T., & Dhaou, S. B. (2021). A framework of blockchain technology adoption: An investigation of challenges and expected value. Information & Management, 58(3), 103444.

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management, 54, 102120.

Visa (2010) Haettu 8.4.2021 osoitteesta https://usa.visa.com/run-your-business/small-business-tools/retail.html

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International workshop on open problems in network security (pp. 112-125). Springer, Cham.

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A survey on the scalability of blockchain systems. *IEEE Network*, *33*(5), 166-173.

Yang, D., Long, C., Xu, H., & Peng, S. (2020, March). A review on scalability of blockchain. In *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology* (pp. 1-6).

Zhang, C., Wu, C., & Wang, X. (2020, May). Overview of Blockchain consensus mechanism. In *Proceedings of the 2020 2nd International Conference on Big Data Engineering* (pp. 7-12).

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. IEEE Access, 8, 16440-16455.