Jani Suoranta

Bitcoinin skaalautuvuusongelman ratkaisuehdotukset

Tietotekniikan kandidaatintutkielma

29. maaliskuuta 2019

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Jani Suoranta

Yhteystiedot: jatasuor@student.jyu.fi

Työn nimi: Bitcoinin skaalautuvuusongelman ratkaisuehdotukset

Title in English: Bitcoin's scalability problem and the proposed solutions

Työ: Kandidaatintutkielma

Sivumäärä: 29+0

Tiivistelmä: Tämä kandidaatintutkielma käsittelee hajautettujen ja julkisten lohkoketjujen skaalautuvuuden ongelmaa bitcoinin näkökulmasta. Lohkoketjuteknologiat mahdollistavat ilman luotettuja osapuolia toimivan verkoston, jota voidaan hyödyntää esimerkiksi arvonsiirrossa ja toisaalta lohkoketjuilla on laaja-alaista soveltamispotentiaalia myös muihin tarkoituksiin. Lohkoketjuteknologioiden laajempaa hyödyntämistä rajoittaa kuitenkin vielä lohkoketjun suorituskyvyn eli skaalautuvuuden ongelma, joka esiintyy bitcoinissa ja on osin yleistettävissä muihin hajautettuihin ja julkisiin lohkoketjuihin. Tutkielma tehtiin kirjallisuuskartoituksena bitcoinin skaalautuvuusongelmasta ja siitä, millaisia on- ja off-chain-ratkaisuja tähän ongelmaan on esitetty. Tutkielmassa selvisi, että bitcoin ei ole suorituskyvyltään skaalautuva, vaan transaktiokapasiteettia rajoittaa lohkokoko, verkon latenssi ja käytössä oleva Proof-of-Work-konsensus algoritmi. Tutkielmassa ilmeni myös, etteivät nykyiset on-chain-ratkaisut sellaisenaan yllä riittävään skaalautumiseen, eikä uudelleenparametrisoimalla latenssia tai lohkokokoa saavuteta riittävää skaalautumista. Toisaalta selvisi, että off-chain-ratkaisut ovat keino huomattavasti lisätä bitcoinin skaalautuvuutta, vaikka on-chain skaalautumisen parantaminen on silti keskeinen ongelma ratkaistavaksi. Off-chain-ratkaisu lightning network näyttäytyi tutkielman valossa parhaalta osaratkaisulta skaalautuvuuden ongelmaan. Tieteellisestä aineistosta oli havaittavissa myös ajatus siitä, että lohkoketjuprotokollien fundamentaalinen uudelleensuunnittelu on tarpeen skaalautuvuuden parantamiseksi.

Avainsanat: lohkoketju, bitcoin, skaalautuvuus, suorituskyky, hajautetut tietokannat

Abstract: This bachelor's thesis focuses on the scalability problem of decentralized and public blockchains from the perspective of bitcoin. Blockchain technologies enable a trustless network which can be used in for instance monetary value transfers besides which blockchain has great potential to be applied in many fields. For the blockchain technologies to be more widely adopted it still is restricted by the low performance and scalability problem which can be seen in bitcoin and can partly be generalized into other decentralized and public blockchains. This thesis was written as a literature review about bitcoin's scalability problem and the proposed solutions to fix that problem from the on-chain and off-chain perspectives. It was found in this study that bitcoin is not scalable by its performance because transaction capacity is restricted by block size, block frequency and the used Proof-of-Work-consensus algorithm. It was also found in this study that the current on-chain solutions won't reach sufficient scalability or that it won't be reached by reparametrizing block frequency or block size. On the other hand it was found out that off-chain solutions are a way to significantly improve bitcoin's scalability although improving on-chain scalability still remains an essential problem to be solved. In light of this study the off-chain solution lightning network seemed to be the best solution to the scalability problem. The thought about the need for a total fundamental redesign of blockchain protocols to improve the scalability could also be seen in the scientific literature.

Keywords: blockchain, bitcoin, scalability, performance, decentralized databases

Sisältö

1 Johdanto

Bitcoin on ensimmäinen julkinen lohkoketjualusta ja järjestelmä, jonka avulla voidaan suorittaa esimerkiksi arvonsiirtoja tai tallentaa informaatiota pitkäaikaisesti ilman luotettua kolmatta osapuolta. Bitcoinilla ja sen inspiroimana kehitetyillä julkisilla lohkoketjualustoilla on kuitenkin niiden käyttöä rajoittava skaalautuvuuden ongelma. Kuten Kim, Kwon ja Cho (2018) sekä Eberhardt ja Tai (2017) mainitsevat, lohkoketjuteknologiat ovat herättäneet niiden monipuolisen sovellettavuutensa vuoksi paljon huomiota, mutta näiden teknologioiden laajamittaiseksi käyttöönottamiseksi skaalautuvuuden ongelma täytyy ensin ratkaista. Bitcoinin skaalautuvuuden ongelma voidaan kiteyttää alhaiseen transaktiokapasiteettiin eli transaktiomäärään, jonka bitcoin pystyy prosessoimaan sekunnissa, ja korkeaan latenssiin eli transaktion varmistusaikaan. Nämä mitattavat ominaisuudet eivät esimerkiksi Zhangin ja Jacobsenin (2018) mukaan parane alustan ylläpitoon eli louhintaan kulutetun energian kasvaessa, mikä tarkoittaa että bitcoin ei ole tästä näkökulmasta skaalautuva.

Skaalautuvuus ei Cromanin ym. (2016) mukaan ole tarkasti määritelty hajautetun järjestelmän ominaisuus vaan kvantitatiivinen termi, joka yhdistää montaa eri suorituskyvyn ja turvallisuuden ominaisuutta. Vukolić (2016) sanoo teknisestä näkökulmastaan, että lohkoketjun skaalautuvuutta eli asiakasohjelmien ja solmujen määrää verkossa ei voi erottaa lohkoketjun latenssista eli transaktion varmistumiseen kuluvasta ajasta ja transaktionopeudesta, koska ne molemmat vaikuttavat paljon toisiinsa. Tässä tutkielmassa skaalautuvuudella tarkoitetaan bitcoinin suorituskyvyn laajennettavuutta, jossa siis yhdistyy edellä mainitut ominaisuudet eli asiakasohjelmien ja solmujen määrä verkossa, verkon latenssi ja verkon transaktionopeus. Sanoilla ”lohkoketju” ja ”lohkoketjuteknologia” viitataan tässä tutkielmassa hajautettuihin ja julkisiin lohkoketjuihin sekä lohkoketjuteknologioihin huomioimatta yksityisiä- ja konsortiolohkoketjuja. Viitatessa Bitcoiniin isolla etukirjaimel-

la tarkoitetaan virtuaalivara[1] Bitcoinia ja viitatessa pienellä kirjoitettuna bitcoiniin tarkoitetaan bitcoinia lohkoketjualustana (Bitcoin Wiki, 2018). Lohkoketjualustalla tässä tutkielmassa viitataan lohkoketjun ylläpitoon osallistuvien solmujen muodostamaan verkkoon, jolla on oma ohjelmointikielensä, jonka avulla lohkoketjua voidaan käyttää sovellusalustana.

Tässä tutkielmassa keskitytään bitcoiniin sovellukset mahdollistavana lohkoketjualustana ja siten osaltaan myös virtuaalivarana, jolloin bitcoinilla on huomattava tarve kehittyä suorituskyvyn osalta, kuten Vukolićin (2016) ja Chauhanin ym. (2018) mukaan kaikilla lohkoketjualustoilla, jotka mahdollistavat hajautettujen sovellusten ja älysopimusten käytön ja siten uudenlaisia tapoja toteuttaa liiketoimintaa. Koska skaalautuvuusongelmaa käsitellään bitcoinin näkökulmasta, niin tutkielman tulosten sovellettavuus rajautuu Proof-of-Work-konsensus algoritmia käyttäviin lohkoketjualustoihin. Tutkielmasta rajautui pois myös erilaiset protokollaehdotukset, kuten Bitcoin-NG tai Bitcoin Cash, joiden käsittely oli tämän tutkielman laajuuden ulkopuolella. Bitcoinin skaalautuvuuden keskeisiä ratkaisuehdotuksia oli siis tutkielman näkökulmasta ne, jotka voidaan bitcoiniin implementoida huomioonottaen bitcoinin luonne avoimen lähdekoodin järjestelmänä. Cromanin ym. (2016) mukaan bitcoinin ollessa avoimen lähdekoodin ja kehittäjien järjestelmä on erilaisten näkemyksien ristiriitaisuus yhteisön sisällä vaikeuttanut yhtenevää päätöksentekoa skaalautuvuuden ongelmien ratkaisuvaihtoehdoista. Myös Back ym. (2014) huomauttivat, että bitcoinin maine toimivana protokollana on aina muutoksia tehtäessä riskeerattuna, joten tehtävät muutokset tehdään aina erittäin harkitusti, varovaisuudella ja yhteisön selkeällä hyväksynnällä.

Lohkoketjuteknologioiden skaalautuvuuteen liittyvän tutkimuksen tärkeyttä korostavat esimerkiksi Kim ym. (2018) huomauttaessaan myös vanhan tiedon ja ratkai-

[1]Termi ”virtuaalivara” Antti-Juhani Kaijanaho. Lohkoketjun avulla toimivien virtuaali- eli kryptovaluuttojen monipuolisuutta paremmin kuvaavaa termiä ”kryptovara” käytti tiettävästi ensimmäisenä Suomen Pankin neuvonantaja Karlo Kauko Kauppalehden kirjoituksessaan `https://www.kauppalehti.fi/uutiset/debatti-kryptovaluutat-ovat-fiat-rahaa-puhtaimmillaan/e49a4b86-e8e8-3a23-9d62-c86f734cc04a`. Viitattu 19.1.2019.

suehdotusten analysoinnin olevan keskeisessä roolissa. Toisaalta myös Sompolinsky ja Zohar (2015) sanovat skaalautuvuuden ongelmien olevan tietoteknisestä näkökulmasta merkittäviä ongelmia ratkaistavaksi. Bitcoinin perustavaa laatua oleva skaalautuvuuden ongelma esiintyy myös muissa julkisissa lohkoketjuteknologioissa, jonka vuoksi on tärkeää ymmärtää bitcoinin skaalautuvuusongelman syyt. Tässä tutkielmassa pyritään vastaamaan bitcoinin skaalautuvuutta koskeviin kysymyksiin kuten ”Mikä rajaa bitcoinin skaalautuvuuden nykyiseen tasoon?” ja ”Mitä ratkaisuja skaalautuvuuden parantamiseksi on esitetty?”. Skaalautuvuusongelman syiden lisäksi pyritään siis kattavasti esittämään myös ongelman ratkaisuehdotuksia. Vastaavaa skaalautuvuuden ongelmia kokoavaa ja yhteenvetävää tutkimusta on tehnyt esimerkiksi Kim ym. (2018) sekä Chauhan ym. (2018) ja toisaalta useissa tutkimuksissa skaalautuvuusongelmaan viitataan ja siitä kerrotaan lyhyesti. Tämä kandidaatintutkielma pyrkii kontribuoimaan tähän keskeiseen skaalautuvuuden keskusteluun yhteenvetävänä ja ongelman laatua selkeyttävänä kirjallisuuskartoituksena, jonka avulla on myös helpompi ymmärtää bitcoinin skaalautuvuuden parantamisen kannalta keskeisiä ratkaisuehdotuksia. Valitsin tämän aiheen tutkielmalleni, koska olen kiinnostunut lohkoketjuteknologioista ja uskon niiden kehittyvän tulevaisuudessa keskeiseksi osaksi maailmanlaajuista älykkäiden ja autonomisten tietoverkkojen infrastruktuuria.

Tämä tutkielma toteutettiin kirjallisuuskartoituksena pääosin vertaisarvioitua ja tieteellistä aineistoa hyödyntäen. Lähdeaineiston etsinnässä hyödynnettiin tietokantoja, kuten Google Scholar, Scopus ja IEEE Xplore. Bitcoinin skaalautuvuuteen liittyvä lähdeaineisto etsittiin käyttäen edellä mainituissa tietokannoissa hakusanoja ”bitcoin scalability” ja ”blockchain scalability”, sekä etsimällä lisäaineistoa löytyneiden lähteiden lähdeaineistoista. Tarkempaa tietoa eri alakäsitteistä ja niihin liittyvästä tutkimuksesta etsittiin myös mainituista tietokannoista kyseisiä alakäsitteitä hakusanoina hyödyntäen, kuten esimerkiksi ”blockchain sharding”.

Tutkielmassa selvisi, että bitcoin ei ole suorituskyvyllisesti skaalautuva, vaan transaktiokapasiteettia nykyiseen tasoon rajoittaa lohkokoko ja verkon latenssi. Toisaalta tuloksista ilmeni, etteivät nykyiset on-chain-ratkaisut sellaisenaan yllä riittävään

skaalautumiseen, eikä uudelleenparametrisoimalla latenssia tai lohkokokoa voida saavuttaa riittävää skaalautumista. Toisaalta off-chain-ratkaisut ovat keino huomattavasti lisätä lohkoketjualustan skaalautuvuutta ja Eberhardtin ja Tain (2017) mukaan ne ovat keskeisiä työkaluja lohkoketjualustoihin liittyvien sovellusten kehittämisessä. On-chain skaalautuminen säilyy silti keskeisenä ongelmana vailla ratkaisua. Bitcoinin skaalautuvuuden parantamiseksi on siis esitetty esimerkiksi sirpalointia, joka on bitcoinin osalta vielä teorian asteella ja toisaalta sivuketjujen käyttöä, joka on esimerkiksi Rootstock -sivuketjuteknologian myötä kehitetty huomattavan pitkälle käytäntöön. Off-chain-ratkaisuista lightning network luo merkittäviä parannuksia bitcoinin käytettävyyteen mikrotransaktioissa, vaikka sillä on omat käyttöönottoon liittyvät heikkoutensa. Tutkielman tulosten valossa näyttää siltä, että lightning network on skaalautuvuusratkaisuista parhain, mutta toisaalta lisää skaalautuvuuden parantamiseksi ehdotettuja ratkaisuja yhdistelevää tutkimusta tarvitaan. Voidaan Cromanin ym. (2016) mukaisesti kiteyttää, että lohkoketjualustojen skaalautuvuuden, turvallisuuden ja hajautettavuuden trilemmaa ei nykyisillä ratkaisuilla pystytä tarpeeksi tyydyttävästi ratkaisemaan, joten fundamentaalinen lohkoketjuprotokollien uudelleensuunnittelu on tarpeen skaalautuvuuden parantamiseksi säilyttäen nykyinen järjestelmän hajautuneisuuden taso.

Seuraavassa luvussa 2 kuvataan tutkielman kannalta bitcoinin lohkoketjun keskeiset käsitteet ja toiminta. Sitten luvussa 3 esitellään bitcoinin skaalautuvuuteen liittyvät ongelmat ja sen alaluvuissa käsitellään bitcoinin transaktiokapasiteettia, latenssia ja lohkokokoa. Luvussa 4 esitellään ensin muutamia skaalautuvuuden parantamiseksi kehitettyjä ratkaisuja yleisemmällä tasolla ja sitten tarkemmin kahdentyyppisiä eli on- ja off-chain-ratkaisuja. On-chain-ratkaisuista esitellään sirpalointi luvussa 4.1.1, sivuketjut luvussa 4.1.2 ja off-chain-ratkaisuista lightning network luvussa 4.2.1. Luku 5 on tutkielman yhteenveto, jossa esitellään johtopäätöksiä ja tuloksia.

2 Bitcoinin lohkoketjun perusrakenteet

Tässä luvussa esitellään tutkielman kannalta keskeiset bitcoinin lohkoketjun perusrakenteet. Aloitetaan siis lohkoketjusta, joka muodostuu edeltäjäänsä linkittyvistä yksittäisistä lohkoista, joita louhijat laskevat ketjun jatkoksi Proof-of-Work-konsensus algoritmin mukaisesti (Nakamoto, 2008). Lohko on Antonopoulosin (2015, s. xix) määritelmän mukaisesti aikaleimattu joukko transaktioita, joka transaktiodatan lisäksi sisältää viittauksen edelliseen lohkoon. Transaktion Antonopoulos (2015, s. xx) määrittelee tarkoittavan arvon, esimerkiksi Bitcoinin, tai muun signeeratun datarakenteen siirtoa lohkoketjussa olevasta julkisesta osoitteesta toiseen, joka suoritettaessa louhijoille maksetaan transaktion louhintapalkkio. Transaktio saa lohkoon verifioituessaan yhden varmistuksen ja varmistukset lisääntyvät sitä myöten, kun saman ketjun uusia lohkoja validoidaan transaktion lohkon jälkeen lisää. Lohkoissa on myös ylätunniste, joka on yhteenveto lohkon tiedoista ja se lasketaan hajautusfunktiolla saaden näin aikaan proof-of-work, joka on vaikeasti tuotettavaa, mutta helposti verifioitavaa dataa (Antonopoulos, 2015, s. xix). Tämä data on numeerinen ratkaisu SHA256-algoritmin luomaan salaukseen, jonka laskemisen haastavuus eli sen laskemiseen tarvittava louhintateho kasvaa bitcoinin verkon asettaman louhinnan vaikeustason lisääntyessä. Louhijat taas ovat verkkoon liittyneitä ja siinä toimivia solmuja, jotka louhivat eli etsivät seuraavalle uudelle lohkolle tuota validia proof-of-workiä laskemalla hajautusfunktiota jatkuvasti uudelleen, jonka lisäksi louhijat huolehtivat myös verkon transaktioiden ja lohkojen verifioinnista. (Antonopoulos, 2015, s. xx.) Louhijoiden lisäksi verkkoon liittyneenä voi olla asiakasohjelmien käyttäjiä, joita ovat louhijat poislukien kaikki muut bitcoinin verkkoon oman päätteensä kautta liittyneet toimijat (Antonopoulos, 2015, s. 6).

Nakamoton (2008) alkuperäisen määritelmän mukaisesti bitcoinin louhinta toimii pisimmän ketjun säännön mukaan, joka tarkoittaa että pisin lohkojen muodostama ketju on aina validein pääketju, jota louhijat pyrkivät jatkamaan uusilla lohkoilla. Käytännössä sääntö siis tarkoittaa, että louhijan saadessa tiedon kahdesta eriävästä lohkosta hän valitsee pidempään ketjuun kuuluvan lohkon ja jatkaa louhimista

tuon tiedon pohjalta (Sompolinsky & Zohar, 2015). Lohkojen valintaan liittyy myös haarautumat, joita verkossa syntyy kun toisiinsa kaukaisesti liittyvät louhijat löytävät samoihin aikoihin uuden lohkon ja välittävät siitä tiedon muille verkon solmuille, jolloin kumpikaan juuri löydetty lohko ei viittaa toiseensa vanhempilohkona (Sompolinsky & Zohar, 2015). Tällöin louhijat alkavat louhia ensimmäisenä saamansa lohkon mukaisesti seuraavaa lohkoa, kunnes uuden proof-of-workin löytyessä ja seuraavan lohkon siten validoituessa näistä kahdesta ristiriitaisesta lohkosta valitaan pidempään ketjuun kuuluva haara louhittavaksi (Nakamoto, 2008). 51 % -hyökkäyksellä tarkoitetaan Zhaon ym. (2016) mukaan ketjuun kohdistuvan louhintatehon jakaumaa, jossa yksittäinen toimija hallitsee louhintatehosta 51 % tai enemmän, joka näin käytännössä mahdollistaa ketjun lohkojen uudelleenlaskennan ja siten myös transaktiohistorian muuttamisen.

3 Bitcoinin skaalautuvuuden keskeiset ongelmat

Käydään lyhyesti läpi bitcoinin skaalautuvuuteen liittyvien ongelmien laatu ensin tarkastellen, mitä tarkoittaa skaalautuva lohkoketju. Skaalautuvan lohkoketjun Ren ym. (2018) määrittelevät lohkoketjuna, jonka transaktiota varten vaadittava kommunikaation määrä ei riipu verkkoon käytettävien resurssien tai verkkoon kuuluvien solmujen määrästä. Tämän määritelmän mukaan bitcoinia voi siis pitää myös tällä hetkellä skaalautuvana kuten Vukolić (2016), jonka mukaan Proof-of-Work-lohkoketjut tarjoavat tehokasta solmujen skaalautuvuutta heikolla suorituskyvyllä. Toisaalta taas Zhang ja Jacobsen (2018) määrittelevät lohkoketjun ideaalin skaalautuvuuden korkeana transaktionopeutena, matalana latenssina ja näiden ominaisuuksien skaalautuvuutena lohkoketjuun osallistuvien resurssien ja solmujen määrän mukaisesti, joka on tässä tutkielmassa käytettävä skaalautuvuuden määritelmä.

Lohkoketjuteknologioiden skaalautuvuuden rajoittuneisuus kiteytyy Wangin (2018) mukaan siihen, että hajautettavuutta, turvallisuutta ja skaalautuvuutta ei voida saavuttaa samanaikaisesti. Samoin Ren ym. (2018) argumentoivat, että bitcoinin tasoisella turvallisuudella tai verkon hajautuneisuudella on mahdotonta saavuttaa skaalautuva suorituskyky, koska kaksinkertaisen maksun ongelma ratkeaa vain globaalilla konsensuksella ja koska lohkoketjujen luotettavuus sekä turvallisuus parantuvat verkon koon ja hajautuneisuuden asteen kasvaessa. Samasta kolmiosaisesta CAP-teoreemaa analogioivasta rajoittuneisuudesta puhuu myös Zhang ja Jacobsen (2018) luokitellessaan turvallisuuden sijaan johdonmukaisuutta, joka tarkoittaa, että lohkoketjussa olevan datan tulisi olla kaikilla käyttäjillä kaikkina aikoina yhtäläistä. Tämä CAP-teoreemaa analogioiva rajoittuneisuus tarkoittaa siis sitä, että jos kaksi asetettua ehtoa täyttyy, niin kolmatta ei onnistuta täyttämään ja toisaalta jos yhtä ominaisuutta parannetaan niin muut ominaisuudet heikkenevät.

Lohkoketjujen skaalautuvuuden ongelman ydin on Wangia (2018) mukaillen siinä, että jokaisen ketjun konsensukseen osallistuvan solmun täytyy verifioida ketjussa oleva data, jonka määrää rajoittaa lohkokoko, joka taas siten rajoittaa transaktiokapasiteettia. Samoin bitcoinin suorituskyvyn rajoittuneisuutta luonnehtii Croman

ym. (2016) sanoessaan datan prosessoinnin näkökulmasta lohkoketjun maksimaalisen suorituskyvyn olevan yksinkertaisesti lohkokoko jaettuna latenssilla. Verkon solmujen näkökulmasta skaalautuvuuden ongelman on tiivistänyt Chauhan ym. (2018) ja Ethereum wiki (2019), joiden mukaan myös bitcoinin skaalautuvuuden keskeisin ongelma johtuu perusperiaatteesta, että jokainen verkossa louhiva solmu tallentaa tiedon kaikista transaktioista, jolloin koko verkko ei pysty prosessoimaan enempää transaktioita kuin yksi solmu. Näin ollen Kanin ym. (2018) mukaan transaktiokapasiteettia ei voida nostaa verkon solmujen määrää lisäämällä, joka tosin mahdollistuisi myös Renin ym. (2018) mukaan mikäli jokaista transaktiota ei verifioisi jokainen solmu. Myös Gervais ym. (2016) sekä Feng ym. (2018) sanovat, että käytettävä konsensus algoritmi pitkälti määrittää lohkoketjualustan skaalautuvuuden, kun Sompolinsky, Lewenberg ja Zohar (2016) ja myöhemmin Chu ja Wang (2018) osoittavat, miten bitcoinin konsensus algoritmi ja pisimmän ketjun-sääntö väistämättä luovat skaalautuvuuden pullonkaulan. Nakamoton (2008) alkuperäisen bitcoinin määritelmän mukaan jokainen bitcoinin solmu verifioi jokaisen transaktion myös tänä päivänä, mutta esimerkiksi luvussa 4.1.1 esitellään sirpalointia, joka bitcoiniin implementoitaessa mahdollistaisi sen ettei jokaisen solmun tarvitse verifioida jokaista transaktiota.

Bitcoinin skaalautuvuuden parantamista lohkokoon ja latenssin uudelleenparametrisoinnilla on tutkinut Croman ym. (2016), joiden mukaan se tulisi ajatella vain ensiaskeleena kohti parempaa skaalautuvuutta, koska bitcoinin hajautetun luonteen vuoksi lohkokoon ja latenssin uudelleenparametrisoinnilla voidaan saavuttaa vain rajallinen ratkaisu skaalautuvuuden ongelmaan, jolloin paras suorituskyky jää kauas verkon teoreettisesta maksimista. Tällä hetkellä bitcoinin latenssi on Block Explorerin (2019) mukaan noin 10 minuuttia ja lohkokoko noin 1 megatavu Cromanin ym. (2016) mukaan uudelleenparametrisoinnilla olisi mahdollista yltää 27 transaktioon sekunnissa ja 12 sekunnin latenssiin, jolloin tosin kohdattaisiin muita tämän kappaleen alaosioissa esiteltäviä ongelmia. Toisaalta Gervais ym. (2016) osoittivat tutkimuksessaan, että Proof-of-Work-ketjujen lohkokoko muuttamalla keskimäärin 1 megatavuun ja latenssi 1 minuuttiin voisi esimerkiksi bitcoinissa yltää noin 60 transaktioon sekunnissa, ilman että ketjun turvallisuus kärsisi merkittävästi. Erilaisesta

näkökulmasta Croman ym. (2016) esittävät myös, että yksi bitcoinin transaktioiden prosessoinnin pullonkauloista on mahdollisesti se, että koko verkossa käytettävissä olevaa kaistanleveyttä ei täysin hyödynnetä.

Tämän luvun alaosioissa esitellään bitcoinin suorituskykyyn liittyvien ongelmien piirteitä eli mitä transaktionopeus, latenssi ja lohkokoko tarkoittavat, miten ne liittyvät skaalautuvuuteen ja mitä ongelmia näihin ominaisuuksiin liittyy.

3.1 Suorituskyky eli transaktiokapasiteetti ja latenssi

Transaktiokapasiteetin määrittelevät Sompolinsky ja Zohar (2015), Kiayias ja Panagiotakos (2016) sekä Gervais ym. (2016) transaktioina sekunnissa, joka tarkoittaa maksimaalista suoritustehoa, jolla bitcoinin lohkoketju pystyy transaktioita verifioimaan ja lisäämään pääketjuun. Latenssilla taas tarkoitetaan Cromanin ym. (2016) ja Vukolićin (2016) sekä Chun ja Wangin (2018) mukaan aikaa, joka kuluu transaktion yhden varmistuksen saantiin. Kuitenkin käytännössä Bitcoinia käytettäessä latenssi on useamman kuin 1 transaktion latenssi, sillä esimerkiksi laajasti käytetty vaihtoalusta Coinbase (2019) vaatii transaktion sinetöimiseksi 3 varmistusta, jolloin Bitcoin transaktion latenssi on keskimäärin 30 minuuttia.

Latenssi eli lohkojen ketjuun lisäämistaajuus tarkoittaa Gervaisia ym. (2016) mukaillen viivettä, jolla lohkoja lisätään pääketjuun. Latenssia pienentämällä eli lisäämällä ketjuun lohkoja useammin voidaan saavuttaa korkeampi transaktiokapasiteetti, mutta tämä johtaa Sompolinskyn ja Zoharin (2015) sekä Kimin ym. (2018) mukaan siihen, että syntyy useampia orpolohkoja eli haaroja pääketjuun, joka taas Gervaisin ym. (2016) mukaan heikentää ketjun turvallisuutta ja suorituskykyä. Orpolohkot siis tarkoittavat lohkoja, jotka aiheuttavat ketjun haarautumia, jotka eivät lopulta pääty osaksi pääketjua, jolloin näiden haarautumien prosessointiin kuluneen louhintatehon voidaan ajatella menneen hukkaan. Orpolohkojen aiheuttamat haarautumat aiheuttavat myös Deckerin ja Wattenhoferin (2013) mukaan lisää viivettä lohkojen lisäämisessä pääketjuun. Transaktiokapasiteetti sekunnissa ja latenssi liittyvät siis keskeisesti toisiinsa ja näihin kahteen taas liittyy lohkokoko, jota käsitellään seuraa-

vassa osiossa.

3.2 Lohkokoko

Lohkokoolla tarkoitetaan maksimimäärää dataa, joka lohkoon voidaan kaikkinensa sisällyttää. Monen lohkoketjun suorituskykyä rajaa Kimin ym. (2018) mukaan lohkokoon rajoitus, koska tällöin transaktion lisäämistä lohkoon ja lohkon lisäämistä ketjuun joudutaan odottamaan tilan puutteen vuoksi pidempään. Proof-of-Work-ketjuissa Gervaisia ym. (2016) mukaillen lohkokoko määrittelee verkon transaktiokapasiteetin sekunnissa eli lohkokokoa kasvattamalla voidaan nostaa transaktiokapasiteettia, mutta toisaalta suuremmat lohkot tarkoittavat korkeampaa latenssia, joka johtaa lisääntyneeseen orpolohkojen määrään ja siten heikompaan verkon turvallisuuteen. Näin ollen lohkokoon kasvattaminen ei ole Kimin ym. (2018) tai Zhengin ym. (2018) mukaan hyvä skaalautuvuusongelman ratkaisu, koska latenssi ja ketjun ylläpitokustannukset nousisivat. Myös Vukolićin (2016) mukaan latenssi nousisi lohkokokoa kasvatettaessa, koska yhä enemmän dataa eli isompia lohkoja pitäisi jakaa kaikkien verkon solmujen kesken ja samalla ketjun turvallisuus heikentyisi, kuten tapahtuisi myös Sompolinskyn ja Zoharin (2015) mukaan silloin, kun transaktiokapasiteettia kasvatettaisiin louhinnan vaikeusastetta madaltamalla.

Gervaisin ym. (2016) tekemä simulointitutkimus osoitti latenssin kohoavan lineaarisesti suhteessa lohkokokoon 4 megatavun lohkoihin asti, jonka jälkeen lohkokoon ehdottomaksi ylärajaksi ketjun turvallisuuden näkökulmasta voidaan määritellä 8 megatavua, jonka jälkeen latenssi ja orpolohkojen esiintymistiheys kohoavat eksponentiaalisesti lohkokoon kasvaessa. Lohkoketjun koon loppumattomaan suurenemiseen liittyy myös Kimin ym. (2018) kuvaama ongelma, kun kaikki transaktiot lohkoketjuun tallennettaessa sen koko kasvaa lopulta liian suureksi, jotta sitä voitaisiin ylläpitää, joka voisi Poonin ja Dryjan (2016) sekä Backin ym. (2014) mukaan johtaa solmujen ja louhintatehon keskittymiseen eli kasvaneeseen 51 % -hyökkäyksen riskiin, koska entistä harvempi omaisi tarvittavat teknologiset resurssit louhijana toimimiseen. Tällä hetkellä bitcoinin lohkoketjun koko on Block Explorerin (2019) graafien mukaan noin 205 gigatavua ja oletettavasti ketjun koko tulee jatkamaan

kasvamista lineaarisesti ellei lohkokokoon tule huomattavia muutoksia. Lohkokokoon ongelma on monisyinen, kuten Zheng ym. (2018) havainnollistavat sanoen, että bitcoinin lohkokoon ollessa rajattu monet pienemmät transaktiot saattavat jäädä prosessoimatta louhijoiden suosiessa korkeamman louhintapalkkion maksavia isompia transaktioita, jolloin latenssi pienillä transaktioilla voi kasvaa huomattavan suureksi. Tämän ongelman ratkaisemiseen on erityisesti keskitytty luvussa 4.2.1 esiteltävässä lightning networkin off-chain-ratkaisussa. Yhteenvetävästi voidaan todeta, että lohkokoon kasvattaminen erityisesti yli 8 megatavun ei ole skaalautuvuusongelmaan toimiva ratkaisu, koska se tuo mukanaan kohonnutta järjestelmän keskittymisen riskiä ja latenssia.

4 Bitcoinin skaalautuvuuden ratkaisuehdotuksia

Edeltävien kappaleiden pohjalta ymmärretään, miten haastava ongelma bitcoinin skaalautuvuuden parantaminen on. Tässä kappaleessa käsitellään ensin relevanttien esimerkkien kautta erilaisten ratkaisuehdotusten tyyppejä ja sitten kahdessa alaosiossa erilaisia skaalautuvuuden parantamisen on- ja off-chain-ratkaisuehdotuksia. On-chain-ratkaisut muokkaavat itse pääketjua skaalautuvammaksi, kun off-chain-ratkaisut tarkoittavat nimenomaan lisäjärjestelmiä, joiden avulla voidaan suorittaa ketjun toiminnallisuuksia ”off-chain” eli fyysisesti pääketjun ulkopuolella, mutta kuitenkin sen turvaamana. On-chain-ratkaisut nähdään usein lohkoketjuteknologioiden tulevaisuuden kannalta tärkeämpinä, mutta niiden monimutkaisen luonteen vuoksi haastavampina, kun taas off-chain-ratkaisujen on ajateltu soveltuvan skaalautuvuuden parantamiseen erityisesti pienten ja usein toistuvien transaktioiden osalta.

Esimerkkinä skaalautuvuuden parantamiseksi implementoidusta ratkaisusta voidaan mainita SegWit (2018), joka muun muassa poisti bitcoinin lohkokoon rajoitukset ja transaktioiden ID:tä koskevan muokattavuusongelman, näin mahdollistaen luvussa 4.2.1 esiteltävän lightning networkin. SegWit kasvattaa Kimin ym. (2018) mukaan ketjun transaktiokapasiteetin noin 2-kertaiseksi samalla kun käyttökustannukset madaltuvat. SegWit siis paransi skaalautuvuutta hieman ja mahdollisti off-chain-ratkaisujen monipuolisemman toteuttamisen.

Toisaalta myös tilankäyttöä optimoivilla ratkaisuilla voidaan lisätä skaalautuvuutta tiettyyn pisteeseen asti. Esimerkkinä tilankäytön optimointiratkaisusta on bitcoinin skriptiä pakkaava ja siten tilankäyttöä optimoiva ratkaisu on Laun (2016) esittämä Merkle-puuta ja abstraktia syntaksipuuta yhdistelevä MAST-metodi, joka muodostaa bitcoinin skriptistä Merkle-puun. Bitcoinin skriptit ovat transaktioissa olevia rajoitteita, joiden mukaan vastaanottaja voi transaktion sisältöä käyttää (Bitcoin Wiki, 2018). Merkle-puun avulla isompi määrä dataa saadaan mahdutettua yhteen tiivisteeseen, joka siten mahdollistaa bitcoinin lohkoketjun käytön pienemmällä muistikapasiteetilla ja toisaalta Kimin ym. (2018) mukaan pienentää louhijoille koituvaa

kuormaa. MAST tullaan todennäköisesti implementoimaan bitcoiniin, koska SegWit on jo pitkälti adoptoitu ja se oli edellytys MASTin implementoinnille. Toinen esimerkki tilankäyttöä optimoivasta ratkaisusta on Maxwellin ym. (2018) esittelemä Bellaren ja Nevenin (2006) työstä muunneltu protokolla, joka mahdollistaa usean eri transaktioon liittyvän toimijan luoda lyhyt yhteinen signatuuri. Bitcoinin nykyisen skriptikielen käyttö moniosaisissa signatuureissa on Maxwellin ym. (2018) mukaan joustavaa, mutta tarvittavan laskennan määrän ja koon näkökulmista tehotonta. Bitcoinin nykyisen mallin sijaan, jossa signatuuri tulee jokaista syötettä kohden, Maxwell ym. (2018) ehdottavat, että jokaista transaktiota kohden olisi vain yksi signatuuri. Näin voitaisiin päästä Maxwellin ym. (2018) arviota tulkiten noin 25 % pienempään lohkoketjun kokoon ja siten optimoida käytössä olevaa lohkokapasiteettia näin saavuttaen korkeampi transaktiokapasiteetti.

Toisaalta myös ketjun turvallisuutta parantamalla voidaan edistää skaalautuvuutta, kuten Sompolinskyn ja Zoharin (2015) GHOST-protokollassa (engl. The Greedy Heaviest-Observed Sub-Tree), joka korvaisi bitcoinin nykyisen louhinnassa käytettävän pisimmän ketjun-säännön. GHOSTin avulla osa orpolohkoihin kohdistuvasta ja siten hukkaan menevästä louhintatehosta pystyttäisiin Vukolićin (2016) mukaan ohjaamaan ketjun turvallisuuden parantamiseen, kun kaikki annettuun lohkoon liittyvät ketjun haarat arvioitaisiin vain pisimmän haaran sijaan. GHOST implementoimalla voitaisiin Sompolinskyn ja Zoharin (2015) mukaan saavuttaa matalampi latenssi säilyttämällä nykyinen turvallisuuden taso, joka siten mahdollistaisi korkeamman transaktiokapasiteetin. Toisaalta GHOSTia käytettäessä Kiayiasin ja Panagiotakosin (2016) mukaan louhintateholla toteutettavan optimaalisen hyökkäyksen tilanteessa ketjun latenssi on huomattavasti nykyistä bitcoinin toteutusta heikompi useilla eri parametreilla testattuna. Lisäksi GHOSTin ongelmana on Kiayiasin ja Panagiotakosin (2016) mukaan se, että useampien solmuyhteyksien kautta verkkoon liittyvät louhijat saavat hieman louhintatehoaan vastaavaa suurempia osuuksia louhintapalkkioista ja toisaalta Lewenbergin, Sompolinskyn ja Zoharin (2015) mukaan pienemmällä teholla louhivat toimijat voisivat toimia itsekkäiden louhintastrategioiden mukaisesti, joka voisi johtaa louhintatehon keskittymiin.

Skaalautuvuutta voidaan siis parantaa optimoimalla esimerkiksi datan pakkaamista, kuten Lau (2016) sekä Maxwell ym. (2018) ehdottivat tai SegWitin tapaisesti monta pienempää erilaista parannusta tekemällä. Sompolinskyn ja Zoharin (2015) ehdotuksen mukaan myös turvallisuutta parantamalla voidaan saavuttaa parempaa skaalautuvuutta, mutta kuten GHOSTin kritiikistä huomataan, niin skaalautuvuuden, hajautuneisuuden ja turvallisuuden trilemma on aina läsnä skaalautuvuuden parannuksia tehtäessä. Tämän trilemman purkamiseksi Chu ja Wang (2018) huomauttivat, että transaktiokeskeiseen skaalautumisen parantamiseen keskittymisen sijaan tulisi fokusoida vaihtoehtoisiin tapoihin luoda luottamuksettomia järjestelmiä tavoilla, joissa hajauttaminen ei ole ainut luottamuksettomuutta luova tekijä. Esimerkiksi varmistettua laitteistoa ja todennettua laskentaa käyttämällä voitaisiin Chun ja Wangin (2018) mukaan saada lohkoketjualustan solmut toimimaan luotettavan koodin kautta muuten luottamuksettomilla alustoilla. Toisesta näkökulmasta solmujen toimintaa voisi tehostaa Pazmiñon ja Rodriguesin (2015) tekemän ehdotuksen pohjalta, jossa saavutettiin lokaalilla bitcoinin solmun osittamisella parhaillaan 70 % parannuksia transaktioiden varmistusaikaan. Hajautettujen lohkoketjualustojen skaalautuvuuden ongelmaan ei kuitenkaan ole vielä keksitty pitkäaikaista ratkaisua, jonka löytäminen esimerkiksi Cromanin ym. (2016) mukaan vaatii lohkoketjun teknisen perustan uudelleensuunnittelua. Tarkastellaan seuraavassa alaosiossa bitcoinin skaalautuvuuden edistämiseksi kehiteltyjä on-chain-ratkaisuehdotuksia.

4.1 On-chain-ratkaisuehdotukset

On-chain-ratkaisut keskittyvät parantamaan skaalautuvuutta muuttamalla lohkoketjun teknistä toteutusta ja siten ketjun toimintatapaa tehokkaammaksi (Kim, 2018). Tarkastellaan tämän luvun alaosioissa sirpalointia ja sivuketjutekniikkaa, jotka ovat varteenotettavia bitcoinin skaalautuvuusongelman ratkaisuehdotuksia.

4.1.1 Sharding eli sirpalointi

Croman ym. (2016) ovat ehdottaneet lohkoketjun skaalautuvuuden parantamiseksi sharding eli sirpalointi-tekniikan käyttöä, jota hyödyntävät hajautetut tietokannat kuten MongoDB ja MySQL. Lohkoketjun sirpalointi tarkoittaa Cromanin ym. (2016) mukaan konsensustehtävien osiksi jakamista eri solmuryhmien eli sirpaleiden kesken, jotta solmukohtaiset prosessointi- ja tilavaatimukset laskevat ja ketjun transaktiokapasiteetti kasvaa lohkojen prosessointia rinnakkaistamalla usealle eri sirpaleelle. Bitcoinin tapauksessa sirpalointi tarkoittaisi Kimin ym. (2018) mukaan sitä, että yksittäiset solmut eivät tallenna kaikkia lohkoja, vaan pienemmät solmujen muodostamat sirpaleet prosessoivat lohkoja, jolloin louhijoille kohdistuva kuorma pienenee ja ketjun transaktiokapasiteetti kasvaa rinnakkaistettaessa lohkojen ja transaktioiden prosessointi usealle sirpaleelle.

Chu ja Wang (2018) sanovat sirpaloinnilla päästävän transaktiokapasiteettiin kt, kun t olisi lohkoketjun transaktiokapasiteetti sekunnissa ilman sirpalointia ja k sirpaleiden määrä, johon ketju on tasaisesti sirpaloitu. Louhinnan keskittymisen näkökulmasta sirpalointi tarkoittaisi Chun ja Wangin (2018) mukaan pahimmassa tapauksessa sitä, että tasaisesti sirpaloidussa ketjussa louhijoiden keskittymisen määrä pysyy vakiona, mutta epätasaisesti osioidussa ketjussa syntyisi enemmän louhijoiden keskittymistä tai transaktiokapasiteetti kärsisi. Tähän louhijoiden keskittymiseen liittyy Chauhanin ym. (2018) kuvailema sirpaloinnin keskeinen ongelma, kun yksittäiseen sirpaleeseen 51 %-hyökkäyksen toteuttaminen ei vaatii louhintatehoa vain suhteessa tuon yksittäisen sirpaleen louhintatehoon. Yksittäisen sirpaleen haltuunsa saadessaan hyökkääjä voi esimerkiksi toteuttaa koko verkossa valideina pidettäviä, mutta todellisuudessa virheellisiä transaktioita. Tämä tosin voidaan Chauhanin ym. (2018) mukaan korjata satunnaistamalla eri sirpaleisiin kohdistuva otanta, mutta tällöin taas ketjun transaktiokapasiteetti hieman kärsii satunnaistamisesta. Toisaalta Ren ym. (2018) sanovat, että sirpalointi on toimiva ratkaisu vain kun verkossa on vähän hyökkäysaikeisia louhijoita ja ettei mikään keksitty sirpalointiratkaisu ole osoittautunut transaktiokapasiteetin osalta solmujen määrän mukaan skaalautuvaksi.

4.1.2 Sivuketjut

Sivuketjuja Croman ym. (2016) luonnehtivat alemmiksi konsensustasoiksi, jotka voidaan toteuttaa pienemmällä hajautuneisuuden tasolla kuin pääketju johon ne liittyvät. Skaalautuvuuden ratkaiseminen käyttämällä sivuketjuja tarkoittaa Kimin ym. (2018) sekä de Kruijffin ja Weigandin (2017) määritelmien mukaan eri lohkoketjujen toiminnallisuuksien hyödyntämistä ristiin eli tällöin esimerkiksi kahden eri ketjun virtuaalivaroja voidaan liikutella sivuketjujen välillä. Hyötyä sivuketjujen käytöstä voi olla de Kruijffin ja Weigandin (2017) mukaan silloin, kun dataa ei voida tallentaa esimerkiksi kalliin hinnan vuoksi pääketjuun ja toisaalta transaktiokapasiteettia voidaan lisätä sivuketjujen avulla. Sivuketjut verifioivat omat transaktionsa, kunnes ne päivitetään aina väliajoin pääketjuun, josta seuraa myös sivuketjujen hyödyntämistä rajoittava keskeinen ongelma, kun yksittäisten sivuketjujen verifiointivastuu kasautuu louhijoille, joka voi Backin ym. (2014) mukaan johtaa verkon turvallisuuden ja toimivuuden kannalta epäedullisiin louhintatehon keskittymiin. Backin ym. (2014) ja Maxwellin ym. (2018) tutkimuksissa mukana ollut Wuille (2015) kommentoi, ettei sivuketjutekniikka ole skaalautuvuusongelmaan lohkokoon kasvattamista parempi vaihtoehto, koska sivuketjuille saman turvallisuuden saavuttaminen vaatii saman verran louhintatehoa ja resursseja, jonka lisäksi sivuketjut tuovat mukanaan muut omat ongelmansa. Tärkeää on huomata, että sivuketjut eivät pääse pakoon hajautettavuuden, turvallisuuden ja skaalautuvuuden trilemmaa, joten ne kohtaavat väistämättä samoja skaalautuvuuden ongelmia.

Bitcoiniin on Lernerin (2015) esittelemän Rootstock-sivuketjulla tullut mahdollisuus käyttää bitcoinia älysopimus- ja sovellusalustana, kun samalla Rootstock parantaa ainakin kuvauksen mukaan bitcoinin skaalautuvuutta monikymmenkertaisella transaktiokapasiteetillaan. Wuillen (2015) kuvaaman ongelman Rootstock ratkaisee ristiinlouhinnalla, joka tarkoittaa, että bitcoinin louhijat prosessoivat ja turvaavat samalla Rootstockin toimintaa. Rootstock on ollut käytettävissä useita kuukausia, mutta siihen liittyvää akateemista tutkimusta ei vielä ole tiettävästi julkaistu.

4.2 Off-chain-ratkaisuehdotukset

Off-chain-ratkaisuissa Kimin ym. (2018) mukaan lohkoketjun skaalautuvuutta parannetaan suorittamalla transaktioita tai muita toimintoja pääketjun ulkopuolella lisäten vain lopputulemat itse pääketjuun, jolloin pääketjun latenssin aiheuttama viivästys voidaan pitkälti syrjäyttää. Off-chain-ratkaisuja kutsutaan myös tilakanavaratkaisuiksi, koska ne Kimiä ym. (2018) mukaillen ylläpitävät pääketjun viimeisintä tilaa lopulta lisäten siihen omilla maksukanavillaan tapahtuneet transaktiot, jotka johdetaan ennalta luotuja ja vakuutettuja maksukanavia pitkin lähettäjältä vastaanottajalle. Näin käyttäjät voivat vastaanottaa ja lähettää olemassa olevien kanavien puitteissa maksuja, jotka viimeistellään pääketjuun vasta, kun lähettäjän ja vastaanottajan välinen kanava päätetään sulkea. Off-chain-ratkaisuilla on skaalautuvuudessa keskeinen rooli Xun ym. (2016) mukaan myös siksi, että niiden avulla saadaan aikaan säästöjä, kun sovelluksissa pelkän lohkoketjun käyttö datan tallentamiseen ja laskentaan on kallista. Off-chain-ratkaisut rajoittuvat Cromanin ym. (2016) mukaan niiden oman verkon transaktionopeuteen, latenssiin ja muihin ominaisuuksiin eivätkä lohkoketjualustan ominaisuuksiin. Toisaalta Croman ym. (2016) huomauttavat maksukanavien käyttöön liittyvän hajautuneisuuden ja yksityisyyden menettämisen ongelmia, koska ne hyödyntävät keskitettyä ”hub-and-spoke”-topologiaa. Näistä heikkouksista huolimatta hajautettujen sovellusten rakentaminen lohkoketjualustoille on Chauhanin ym. (2018) mukaan lisännyt alustoihin kohdistuvia vaatimuksia, joka on lisännyt off-chain-ratkaisujen käyttöönottoa.

4.2.1 Lightning network -mikrotransaktioverkko

Lohkoketjun avulla arvonsiirto on edullista suurempia varoja siirrettäessä, mutta toisaalta samalla esimerkiksi Bitcoinin käyttäminen pieniin ja usein toistuviin maksuihin on epäkäytännöllistä, koska latenssi on korkea ja lisäksi käyttäjän täytyy maksaa transaktiokulu louhijoille. Tähän mikrotransaktioiden ongelmaan Poon ja Dryja (2016) ehdottivat bitcoinin skaalautuvuuden osaratkaisuksi lightning network-mikrotransaktioverkkoa, jonka avulla bitcoinin luotettavuutta ja muita hyviä puolia pystytään hyödyntämään samalla Kimin ym. (2018) mukaan yltäen korkeaan tran-

saktiokapasiteettiin alhaisin kuluin. Mikrotransaktioverkon käytöllä pystytään vähentämään pääketjulle kertyvää kuormaa, käyttäjien odotteluaikoja ja transaktiokuluja erityisesti mikrotransaktioissa, kun Poonin ja Dryjan (2016) mukaan verkon transaktiokapasiteetti on useita kymmeniä tuhansia. Toisaalta transaktiokapasiteetti on riippuvainen avoinna olevien maksukanavien määrästä, näiden kanavien saldosta ja niiden muodostamista yhteyksistä, jolloin se voi olla verkon tilanteesta riippuen myös korkeampi tai matalampi.

Lightning network hyödyntää maksukanavia, jotka täytyy aukaista ja sulkea bitcoinin verkossa tapahtuvalla transaktiolla, joka on Kimin ym. (2018) mukaan tehotonta, koska tällöin transaktiokulu joudutaan maksamaan ja odottamaan bitcoinin latenssin mukainen transaktion varmistusaika, mutta toisaalta maksukanavia ei toistuvissa mikrotransaktioissa tarvitse välttämättä koskaan sulkea, jolloin bitcoinin korkea latenssi ja kulut eivät ole ongelma. Toisaalta kuten Chauhan ym. (2018) huomauttavat, niin verkossa tulee olla tarpeeksi kytkettynä olevia ja riittävästi saldoa sisältäviä maksukanavia, jotta verkon käyttäjät pääsevät suorittamaan haluamansa suuruisia transaktioita. Maksukanavien saldo määrää siis transaktion maksimaalisen suuruuden, joka on yksi mikrotransaktioverkon keskeisimmistä rajoitteista. Toisaalta myös mikrotransaktioverkon käyttöönotto ja käyttö on melko monimutkainen tehtävä, joten laajemman yleisön näkökulmasta käytön yleistyminen vaatii vielä kehitystä helppokäyttöisyydessä. Huolimatta ongelmistaan lightning network on huomattavalla transaktiokapasiteetillaan merkittävä parannus bitcoinin skaalautuvuuteen.

5 Yhteenveto

Bitcoin on ensimmäisenä julkisena lohkoketjualustana toiminut esimerkkinä muille hajautetuille lohkoketjualustoille, joiden avulla voidaan rakentaa täysin luottamuksettomia järjestelmiä. Bitcoinin inspiroimana kehitetyillä julkisilla lohkoketjualustoilla on kuitenkin niiden käytettävyyttä rajoittava skaalautuvuuden ongelma, jonka ratkaiseminen mahdollistaisi näiden teknologioiden laajamittaisemman käyttöönottamisen. Skaalautuvuusongelmaa on luonnehdittu merkittäväksi julkisten lohkoketjujen ongelmaksi, jonka vuoksi siihen liittyvä tutkimus ja ratkaisuehdotusten analysointi on tärkeää. Tämä tutkielma keskittyi bitcoinin skaalautuvuuden ongelmaan, joka voidaan kiteyttää alhaiseen transaktiokapasiteettiin ja korkeaan latenssiin eli transaktion varmistusaikaan, jotka eivät parannu esimerkiksi bitcoinin verkon muodostavien louhijoiden lisääntyessä. Bitcoinilla on huomattava tarve kehittyä skaalautuvammaksi mikäli sitä halutaan hyödyntää hajautettuna sovellusalustana osana uudenlaisia tapoja tehdä liiketoimintaa.

Skaalautuvuuden ongelma on määriteltävissä monella tavalla, mutta tässä tutkielmassa skaalautuvuudella tarkoitettiin bitcoinin suorituskyvyn laajennettavuutta, jossa yhdistyy bitcoinin verkon ominaisuudet, kuten asiakasohjelmien ja solmujen määrä, latenssi ja transaktiokapasiteetti. Näitä edellä mainittuja ominaisuuksia käsiteltiin yhdessä, koska niitä ei voida selkeästi lohkoketjun skaalautuvuuden mielessä erottaa toisistaan. On myös huomattava, että skaalautuvuus ei ole tarkasti määritelty järjestelmän ominaisuus vaan kvantitatiivinen termi, jossa yhdistyy monta eri suorituskyvyn ja turvallisuuden ominaisuutta.

Koska skaalautuvuusongelmaa käsiteltiin bitcoinin näkökulmasta, niin tutkielman tulosten sovellettavuus rajautui Proof-of-Work-konsensus algoritmia käyttäviin julkisiin lohkoketjualustoihin, vaikka myös muilla konsensus algoritmeilla toimivilla lohkoketjuilla esiintyy sama hajautettavuuden, turvallisuuden ja skaalautuvuuden trilemma. Tutkielmassa ei täten myöskään huomioitu yksityisiä- tai konsortiolohkoketjuja. Lisäksi tutkielmasta rajautui pois erilaiset protokollaehdotukset, koska niiden käsitteleminen oli tämän tutkielman laajuuden ulkopuolella. Tutkielman näkö-

kulmasta keskeisiä skaalautuvuusongelman ratkaisuja olivat siis bitcoiniin implementoitavissa olevat skaalautuvuuden ratkaisuehdotukset huomioiden bitcoinin luonne avoimen lähdekoodin järjestelmänä.

Tässä tutkielmassa pyrittiin vastaamaan bitcoinin skaalautuvuutta käsitteleviin kysymyksiin, kuten mikä rajaa bitcoinin skaalautuvuuden nykyiseen tasoon ja toisaalta mitä ratkaisuja skaalautuvuuden parantamiseksi on esitetty. Vastaavissa aiemmissa tutkimuksissa on käsitelty skaalautuvuusongelmaa lyhyehkösti tai melko yleisellä tasolla ja toisaalta ongelmaan usein viitataan tutkimuksissa lähinnä maininnan omaisesti. Varsinaisesti useita tutkimuksia yhteenvetävää ja tuloksia analysoivaa tutkimusta tai kirjallisuuskatsausta ei bitcoinin skaalautuvuuden osalta ole nähtävästi tehty, vaikka toisaalta monelle asiaan perehtyneelle skaalautuvuuden ongelman syyt ja relevanteimmat ratkaisuehdotukset ovat tiedossa. Toisaalta tämä kirjallisuuskartoitus onnistui asetettuihin tutkimusongelmiin vastaamisessa, mutta vielä syvällisempi ja kokonaisvaltaisempi eri ratkaisuihin perehtyminen ja niiden käsitteleminen olisi vaatinut tarkempaa rajausta tutkimuskysymysten osalta. Tämä kirjallisuuskartoitus kuitenkin kontribuoi keskeiseen skaalautuvuuden keskusteluun yhteenvetävänä ja bitcoinin skaalautuvuusongelman laatua selkeyttäen, näin ollen edistäen myös muiden Proof-of-Work-lohkoketjualustojen skaalautuvuusongelman ymmärtämistä. Tutkielmassa esiteltiin ensin bitcoinin lohkoketjun perusrakenne, jonka pohjalta tarkasteltiin bitcoinin skaalautuvuuden ongelman eri syitä. Ongelman syiden selvittyä siirryttiin tarkastelemaan eri ratkaisuehdotuksia, joita skaalautuvuuden parantamiseksi on esitetty. Osa skaalautuvuuden on-chain-ratkaisuista esiteltiin yleisluontoisemmin, kun sirpalointiin ja sivuketjuihin keskityttiin hieman tarkemmin. Tämän jälkeen tarkasteltiin viimeisenä off-chain-ratkaisuehdotuksien luonnetta ja syvennyttiin tarkemmin lightning network-ratkaisun tarkasteluun.

Tutkielmassa selvisi, että bitcoinia ja muita julkisia sekä hajautettuja lohkoketjualustoja rajoittaa hajautettavuuden, turvallisuuden ja skaalautuvuuden trilemma, joka tarkoittaa että näitä kolmea ominaisuutta ei voida saavuttaa tai ainakaan parantaa samanaikaisesti ilman, että yhden parantuessa muut eivät heikkenisi. Bitcoinin osal-

ta selvisi, että se ei ole suorituskyvyllisesti skaalautuva, vaan transaktiokapasiteettia rajoittaa lohkokoko ja latenssi, joita uudelleenparametrisoimalla ei toisaalta voida saavuttaa pitkäaikaista ratkaisua skaalautumisen ongelmaan. Esimerkiksi lohkokoon kasvattaminen varsinkaan yli 8 megatavun ei ole skaalautuvuusongelmaan toimiva ratkaisu, koska se tuo mukanaan kohonnutta järjestelmän keskittymisen riskiä ja latenssia. Toisaalta pienempiä parannuksia yhdistellen voidaan saavuttaa hieman parempaa skaalautuvuutta, kuten implementoidussa SegWit-ratkaisussa. Lisäksi erilaisin tilankäyttöä optimoivin ratkaisuin, kuten MAST-metodilla tai signatuureja optimoimalla voidaan lisätä transaktiokapasiteettia. Lopulta kuitenkin yhteenvetävästi voidaan todeta, että mikään on-chain-ratkaisu ei tällä hetkellä näytä riittävältä ratkaisulta skaalautuvuuden ongelmaan, vaikka sirpalointi tai sivuketjuteknologiat ovat lupaavia vaihtoehtoja, mutta niiden implementoinnin mukana tulee omat vielä ratkaisemattomat ongelmansa. Toisaalta taas off-chain-ratkaisuilla voidaan huomattavasti parantaa lohkoketjun skaalautuvuutta ja lightning network parantaa Bitcoinin käytettävyyttä mikrotransaktioissa huomattavasti. Voidaan todeta, että lightning network lienee tämän hetken skaalautuvuusratkaisuista parhain ja tehokkain, mutta toisaalta on-chain skaalautumisen parantamisen ongelma on silti edelleen relevantti. Teoreettisesti ajatellen jos on-chain skaalautumiseen löydetään tehokas ratkaisu, niin off-chain-ratkaisuja ei välttämättä edes tarvita. Lisäksi mainittakoon, että tieteellisessä aineistossa esiintyi myös ajatus siitä, että lohkoketjuprotokollien skaalautuvuusongelman ratkaisemiseksi tarvitaan protokollien huomattavaa fundamentaalisen tason uudelleensuunnittelua ja näin asia näyttäisi olevan on-chain skaalautumisen osalta.

Kirjallisuutta

Antonopoulos, A. M. (2015). *Mastering Bitcoin: unlocking digital cryptocurrencies*. Sebastopol: O'Reilly Media, Inc.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., & Wuille, P. (2014). *Enabling blockchain innovations with pegged sidechains*. Saatavilla WWW-muodossa: `http://www.bubifans.com/ueditor/php/upload/file/20181015/1539599182599463.pdf`. Viitattu 24.1.2019.

Bellare, M., & Neven, G. (2006). *Multi-signatures in the plain public-key model and a general forking lemma*. Teoksessa Proceedings of the 13th ACM conference on Computer and communications security. New York: ACM, s. 390–399.

Bitcoin Wiki. (2018). *Bitcoin Wiki*. Saatavilla WWW-muodossa: `https://en.bitcoin.it/wiki`. Viitattu 29.3.2019.

Blockchain Explorer. (2019). *Blockchain - The Most Trusted Crypto Company*. Saatavilla WWW-muodossa: `https://www.blockchain.com/explorer`. Viitattu 21.2.2019.

Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018). *Blockchain and scalability*. Teoksessa 2018 IEEE International Conference on Software Quality, Reliability and Security Companion. Lissabon: IEEE, s. 122–128.

Chu, S., & Wang, S. (2018). *The Curses of Blockchain Decentralization*. arXiv preprint. arXiv:1810.02937.

Coinbase. (2019). *Coinbase | Bitcoin Glossary*. Saatavilla WWW-muodossa: `https://support.coinbase.com/customer/portal/articles/1833695-bitcoin-glossary`. Viitattu 18.2.2019.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D., & Wattenhofer, R. (2016). *On Scaling Decentralized Blockchains*. Teoksessa International Conference on Financial Cryptography and Data Security. Clark, J., Meiklejohn, S., Ryan, P., Wallach, D., Brenner, M. & Rohloff, K. (toim.), Lecture Notes in Computer Science, 9604(1). Berlin: Springer, s. 106–125.

Decker, C., & Wattenhofer, R. (2013). *Information propagation in the bitcoin network*.

Teoksessa 13th IEEE International Conference on Peer-to-Peer Computing. Trento: IEEE, s. 1–10.

de Kruijff, J., & Weigand, H. (2017). *Understanding the blockchain using enterprise ontology*. Teoksessa International Conference on Advanced Information Systems Engineering. Cham: Springer, s. 29–43).

Eberhardt, J., & Tai, S. (2017). *On or off the blockchain? Insights on off-chaining computation and data*. Teoksessa European Conference on Service-Oriented and Cloud Computing. Cham: Springer, s. 3–15.

Ethereum wiki. (2019). *Sharding FAQs*. Saatavilla WWW-muodossa: `https://github.com/ethereum/wiki/wiki/Sharding-FAQs`. Viitattu 31.1.2019.

Feng, L., Zhang, H., Chen, Y., & Lou, L. (2018). *Scalable Dynamic Multi-Agent Practical Byzantine Fault-Tolerant Consensus in Permissioned Blockchain*. Applied Sciences, 8(10), nro. 1919. Basel: MDPI AG.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). *On the security and performance of proof of work blockchains*. Teoksessa Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, s. 3–16.

Kan, L., Wei, Y., Muhammad, A. H., Siyuan, W., Linchao, G., & Kai, H. (2018). *A Multiple Blockchains Architecture on Inter-Blockchain Communication*. Teoksessa 2018 IEEE International Conference on Software Quality, Reliability and Security Companion. Lissabon: IEEE, s. 139–145.

Kiayias, A., & Panagiotakos, G. (2016). *On Trees, Chains and Fast Transactions in the Blockchain*. IACR Cryptology ePrint Archive, nro. 545.

Kim, S., Kwon, Y., & Cho, S. (2018). *A Survey of Scalability Solutions on Blockchain*. Teoksessa 2018 International Conference on Information and Communication Technology Convergence. Jeju: IEEE, s. 1204–1207.

Lau, J. (2016, 30. marraskuuta). *Merkelized Abstract Syntax Tree*. Saatavilla WWW-muodossa: `https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki`. Viitattu 30.6.2018.

Lerner, S. D. (2015, 19. marraskuuta). *RSK White Paper Overview*. Saatavilla WWW-muodossa: `https://docs.rsk.co/RSK_White_Paper-Overview.`

pdf. Viitattu 25.1.2019.

Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015). *Inclusive block chain protocols*. Teoksessa International Conference on Financial Cryptography and Data Security. Berlin: Springer, s. 528–547.

Maxwell, G., Poelstra, A., Seurin, Y., & Wuille, P. (2018). *Simple schnorr multi-signatures with applications to bitcoin*. Designs, Codes and Cryptography, 1-26.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Saatavilla WWW-muodossa: https://bitcoin.org/bitcoin.pdf. Viitattu 15.2.2019.

Pazmiño, J. E., & Rodrigues, C. K. S. (2015). *Simply dividing a Bitcoin network node may reduce transaction verification time*. Teoksessa The SIJ Transactions on Computer Networks & Communication Engineering 3(2). Coimbatore: CNCE, s. 17–21.

Poon, J., & Dryja, T. (2016, 14. tammikuuta). *The bitcoin lightning network: Scalable off-chain instant payments*. Saatavilla WWW-muodossa: https://lightning.network/lightning-network-paper.pdf. Viitattu 21.1.2019.

Ren, Z., Cong, K., Aerts, T., de Jonge, B., Morais, A., & Erkin, Z. (2018). *A scale-out blockchain for value transfer with spontaneous sharding*. Teoksessa 2018 Crypto Valley Conference on Blockchain Technology. Zug: IEEE, s. 1–10.

SegWit. (2018). *SegWit, bip-0141.mediawiki*. Saatavilla WWW-muodossa: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. Viitattu 22.2.2019.

Sompolinsky, Y., Lewenberg, Y., & Zohar, A. (2016). *SPECTRE: A Fast and Scalable Cryptocurrency Protocol*. IACR Cryptology ePrint Archive, 1159.

Sompolinsky, Y., & Zohar, A. (2015). *Secure high-rate transaction processing in bitcoin*. Teoksessa Financial Cryptography and Data Security. Berliini: Springer, s. 507–527.

Vukolić, M. (2016). *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*. Teoksessa Open Problems in Network Security. Camenisch, J. & Kesdoğan, D. (toim.), Lecture Notes in Computer Science, 9591(1). Cham: Springer, s. 112–125.

Wang, W. (2018). *A Vision for Trust, Security and Privacy of Blockchain*. Teoksessa International Conference on Smart Blockchain. Qiu, M. (toim.), Lecture Notes in

Computer Science, 11373(1). Cham: Springer, s. 93–98.

Wuille, P. (5.10.2015). *Bitcoin stackexchange*. Saatavilla WWW-muodossa: `https://bitcoin.stackexchange.com/a/40772`. Viitattu 15.2.2019.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). *The blockchain as a software connector*. Teoksessa 2016 13th Working IEEE/IFIP Conference on Software Architecture. Venetsia: IEEE, s. 182–191.

Zhang, K., & Jacobsen, H. A. (2018). *Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains*. Teoksessa 2018 IEEE 38th International Conference on Distributed Computing Systems. Wien: IEEE, s. 1337–1346.

Zhao, J.L., Fan, S., & Yan, J. (2016). *Overview of business innovations and research opportunities in blockchain and introduction to the special issue*. Financial Innovation, 2(28).

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). *Blockchain Challenges and Opportunities: A Survey*. Teoksessa International Journal of Web and Grid Services, 14(4). Geneve: Inderscience Enterprises, s. 352–375.