Panu Suuronen

LOHKOKETJUTEKNOLOGIAN TEKNOLOGISET HAASTEET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Suuronen, Panu
Lohkoketjuteknologian teknologiset haasteet
Jyväskylä: Jyväskylän yliopisto, 2023, 26 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Vuorinen, Jukka

Lohkoketjuteknologian ensimmäinen julkinen ja hajautettu toteutus syntyi vuonna 2008, kun ”Satoshi Nakamoto” -nimimerkkiä käyttänyt taho julkaisi artikkelin ”Bitcoin: A Peer-to-Peer Electronic Cash System”. Lohkoketjuteknologia on sen julkaisusta lähtien herättänyt ympärilleen suurta mielenkiintoa. Sen mahdollistamien tosielämän käyttötapauksien, kuten nopeiden globaalien transaktioiden, älysopimuksien, muuttumattomuuden ja läpinäkyvyyden ansiosta, lohkoketjuteknologiaa pidetään yhtenä suurimpana teknologisena innovaationa. On kuitenkin selvää, että lohkoketjuteknologian ollessa melko uusi tekniikka, sillä on edessä useita haasteita, jotka tulisi ratkaista ennen laajempaa käyttöönottoa. Tämän tutkielman tarkoituksena on esittää kirjallisuuskatsauksen kautta löydettyjä lohkoketjuteknologian teknologisia haasteita ja niiden mahdollisia ratkaisuja. Tutkielmassa käsitellään myös lohkoketjuteknologian yleistä toimintaperiaatetta ja eri konsensusalgoritmeja. Lohkoketjuteknologian haasteita on valtavasti ja ne voidaan kategorisoida esimerkiksi teknologisiin, organisatorisiin ja ympäristöllisiin haasteisiin. Haasteita tarkastellessa, teknologiset haasteet nousevat vahvasti esille, ja niiden ratkaisemista pidetään tärkeänä lohkoketjuteknologian kehityksen kannalta. Tutkielmassa tarkasteltavat haasteet nousevat useasti esille kirjallisuudessa ja niihin on kehitetty erilaisia mahdollisia ratkaisuja. Ratkaisut näihin haasteisiin voivat kohdistua tiettyjen ongelmien ratkaisemiseen, tai pyrkiä parantamaan lohkoketjuteknologian laajempia kokonaisuuksia, kuten konsensusalgoritmeja.

Asiasanat: lohkoketjuteknologia, haasteet, ratkaisut, konsensusalgoritmit

ABSTRACT

Suuronen, Panu
Technological challenges of blockchain technology
Jyväskylä: University of Jyväskylä, 2020, 26 pp.
Information Systems, Bachelor's thesis
Supervisor: Vuorinen, Jukka

The first public and decentralized implementation of blockchain technology was created in 2008 when an individual or a group using the pseudonym "Satoshi Nakamoto" published an article titled "Bitcoin: A Peer-to-Peer Electronic Cash System." Since its release, blockchain technology has generated significant interest due to its real-world applications, such as fast global transactions, smart contracts, immutability, and transparency, making it one of the biggest technological innovations. However, as blockchain technology is still a relatively new technology, it faces several challenges that need to be addressed before wider adoption. The purpose of this thesis is to present the technological challenges of blockchain technology and their potential solutions through a literature review. The thesis also discusses the general operating principle of blockchain technology and various consensus algorithms. There are numerous challenges associated with blockchain technology, which can be categorized into technological, organizational, and environmental challenges. When examining these challenges, specifically the technological challenges emerge frequently, and solving them is considered essential for the development of blockchain technology. The challenges examined in this thesis appear frequently in the literature, and different potential solutions have been developed for them. Solutions to these challenges may target specific problems or seek to improve the broader entities of blockchain technology, such as the consensus algorithms.

Keywords: blockchain technology, challenges, solutions, consensus algorithms

KUVIOT

SISÄLLYS

1 JOHDANTO

Lohkoketjuteknologia on viime vuosina noussut otsikoihin sekä mediassa että tutkimuskirjallisuudessa. Alun perin Bitcoinin yhteydessä julkaistu ensimmäinen julkinen ja hajautettu lohkoketju on herättänyt suuren mielenkiinnon lohkoketjuteknologiaa kohtaan. Lohkoketjuteknologian uskotaan vaikuttavan laajasti useisiin eri aloihin, kuten terveydenhuoltoon, rahoitusalaan ja teollisuusalaan (Ahram ym., 2017).

Suuresta hehkutuksesta huolimatta lohkoketjuteknologialla on edessään lukemattomia haasteita, jotka tulisi ratkaista. Näitä haasteita on tärkeä tutkia, sillä lohkoketjuteknologian sanotaan olevan yksi suurimpia teknologisia innovaatiota. Siksi ennen laajempaa käyttöönottoa olisi tärkeää ymmärtää, mitä haasteita lohkoketjuteknologialla on vielä edessä ja millaisia ratkaisuja näihin haasteisiin on jo kehitetty. Tämän tiedon avulla lohkoketjuteknologiaa voidaan kehittää eteenpäin ratkaisemalla kyseiset haasteet.

Tässä kirjallisuuskatsauksessa pyritään vastaamaan seuraaviin tutkimuskysymyksiin lähdekirjallisuuden pohjalta:

1. Mitkä ovat lohkoketjuteknologian suurimmat teknologiset haasteet?

2. Minkälaisia ratkaisuja kyseisiin haasteisiin on kehitetty?

Kirjallisuuskatsauksen lähteitä on haettu Google Scholar-, ScienceDirect-, IEEE Xplore-, ResearchGate-, ACM Digital Library -tietokannoista. Hakusanoina on käytetty muun muassa seuraavia: ”blockchain challenges”, ”consensus algorithms”, ”blockchain scalability”, ”blockchain energy consumption”, ”blockchain interoperability” ja ”blockchain security”. Katsauksessa on pyritty mahdollisimman relevanttien ja laadukkaiden lähteiden valintaa, joten lähteiden valinnassa on otettu huomioon viittausten määrä, vertaisarvioinnit sekä suomalaisen tieteellisten julkaisukanavien luokitusjärjestelmän, Julkaisufoorumin, subjektiivinen laatuarviointi. Osa lähteistä on konferenssipapereita tai systemaattisia kirjallisuuskatsauksia, joissa viitataan muihin tutkimuksiin.

Lisäksi tutkielmassa on käytetty lähteinä verkkosivustoja niiden ollessa relevantteja tutkielman kannalta.

Tutkielma on jaettu neljään lukuun: johdanto, lohkoketjuteknologia, lohkoketjuteknologian teknologiset haasteet ja yhteenveto. Johdannon jälkeen toisessa luvussa käsitellään lohkoketjuteknologian toimintaa yleisesti, jotta lukijalla on tarpeeksi laaja käsitys lohkoketjujen toiminnasta, jotta lukija saa lohkoketjujen toiminnasta niiden haasteiden ymmärtämiseen riittävän käsityksen. Tämän jälkeen esitellään erilaisia konsensusalgoritmeja ja niiden toimintaa, joista laajemmin käydään läpi ”Proof of Work” ja ”Proof of Stake”. Tutkielman kolmannessa luvussa esitellään eri haasteiden kategorioita, joista keskitytään teknologisiin haasteisiin julkisten lohkoketjujen näkökulmasta. Luvussa pyritään vastaamaan tutkielman tutkimuskysymyksiin. Luku alkaa erilaisten haasteiden yleisellä esittelyllä, jonka jälkeen keskitytään neljään eri haasteeseen tarkemmin. Nämä neljä haastetta ovat: skaalautuvuus, energiankulutus, turvallisuus ja yhteentoimivuus. Haasteisiin tutustumisen jälkeen esitellään niihin ehdotettuja ratkaisuja lähdekirjallisuuden pohjalta. Nämä haasteet valikoituivat tarkasteltaviksi, sillä ne ovat useasti esillä lähdekirjallisuudessa ja niiden ratkaisemista voidaan pitää kriittisenä lohkoketjuteknologian kehityksen kannalta.

”Yhteenveto” on tutkielman viimeinen luku, jossa käydään läpi tutkielman tulokset ja johtopäätökset. Luvussa käsitellään myös tutkielman mahdollisia rajoitteita ja jatkotutkimusaiheita tulevaisuutta varten.

2 LOHKOKETJUTEKNOLOGIA

Tässä luvussa käsitellään lohkoketjuteknologian perusteet ja toimintaperiaate. Jotta lohkoketjuteknologian haasteita voidaan esitellä ja tarjota niihin ratkaisuja, lukijan täytyy ymmärtää lohkoketjuteknologian toiminnan perusperiaatteet. Lohkoketjuteknologian esittelyssä keskitytään tämän tutkielman kannalta sen tärkeimpiin ominaisuuksiin ja käsittely rajataan siten, että lohkoketjuteknologian toiminnan pääpiirteet tulevat selviksi. Ensimmäisessä alaluvussa käsitellään, mikä on lohkoketjuteknologia ja kuinka se toimii. Toisessa alaluvussa käsitellään konsensusalgoritmeja ja niiden merkitystä yleisellä tasolla.

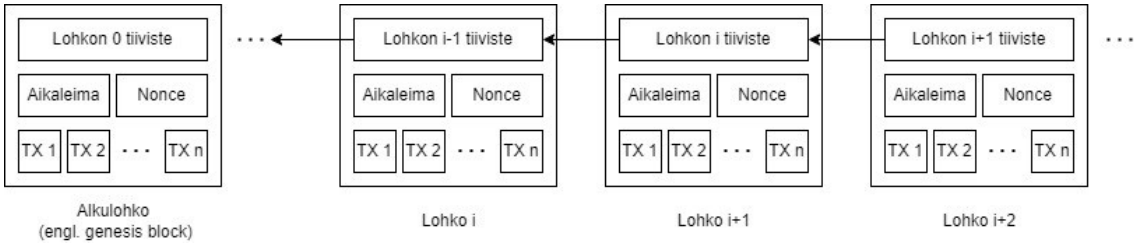
2.1 Lohkoketjuteknologian perusteet ja toimintaperiaate

Habibin ym. (2022) mukaan lohkoketjuteknologiaa pidetään innovatiivisena ja vallankumouksellisena teknologiana, joka tarjoaa mahdollisuuden vähentää tietoturvariskejä, poistaa petoksia ja lisätä läpinäkyvyyttä aiempaa suuremmassa mittakaavassa. Vaikka lohkoketjuteknologia tuli alun perin tunnetuksi kryptovaluutan ja NFT:iden yhteydessä 2010-luvulla, sitä voidaan nykyään käyttää monilla eri aloilla moniin eri tarkoituksiin, kuten elintarviketoimitusketjujen läpinäkyvyyden tarjoamiseen, terveydenhuollon tietojen turvaamiseen, pelialan uudistamiseen ja datan ja omistajuuden käsittelytavan muuttamiseen. Käyttämällä lohkoketjuteknologiaa digitaalinen omaisuus ja tiedot voivat siirtyä suoraan käyttäjältä toiselle ilman keskitetyn välittäjän tai kolmannen osapuolen osallistumista. (Habib ym., 2022.)

Lohkoketjuteknologian ensimmäinen julkinen ja hajautettu toteutus sai alkunsa vuonna 2008, kun ”Satoshi Nakamoto”-nimimerkkiä käyttänyt taho julkaisi artikkelin ”Bitcoin: A Peer-to-Peer Electronic Cash System” (Monrat, Schelén & Andersson, 2019). Artikkeli käsitteli hajautetun (engl. decentralization) digitaalisen valuutan, nimeltä Bitcoin, luomista ja sen toimintaa. Artikkelissa esiteltiin uusi hajautetun tietokannan teknologia, jota kutsutaan lohkoketjuteknologiaksi (tunnetaan myös nimellä hajautettu kirjanpitoteknologia tai

DLT), joka mahdollisti Bitcoin-verkon toiminnan ilman keskitettyä viranomaista tai pankkia. (Nakamoto, 2008.) Ensimmäinen Bitcoin-verkon transaktio suoritettiin vuonna 2009 Hal Finneyn toimesta (Monrat ym., 2019).

Monratin ym. (2019) lohkoketjuteknologia perustuu hajautettuun tietokantajärjestelmään, jossa tiedot tallennetaan hajautetusti usealle eri tietokoneelle. Tällaista verkkoa voidaan kutsua vertaisverkoksi (engl. peer-to-peer tai P2P). Näin ollen tietokannan hallinta on hajautettu eri solmuille (engl. node), eikä yhdellä keskitetyllä palvelimella ole täyttä hallintavaltaa tietokantaan. Tämä tarjoaa turvallisen ja läpinäkyvän tavan tallentaa ja varmentaa tapahtumia kuten transaktioita osapuolten välillä ilman kolmatta osapuolta. Lohkoketjuteknologia toimii siis tietokantaa yhdessä ylläpitävien tietokoneiden verkoston kautta. Jokainen uusi tapahtuma lisätään lohkoon ja liitetään edellisiin lohkoihin kryptografisilla tiivisteillä (engl. cryptographic hash). Kryptografinen tiiviste on yksisuuntainen funktio, joka ottaa minkä tahansa pituisen datan syötteenään, kuten numeroita, tekstiä, merkkijonoja tai jopa tiedostoja, ja tuottaa siitä ainutlaatuisen ja kiinteän pituisen hajautusarvon. Tämä tiiviste on tärkeä osa lohkoketjuteknologiaa, koska se mahdollistaa lohkoketjun lohkojen eheyden ja autenttisuuden tarkistamisen. Näin luodaan muutoksilta suojattu rekisteri kaikista verkon tapahtumista, sillä yritys muuttaa aikaisempaa lohkoa edellyttäisi myös kaikkien myöhempien lohkojen muuttamista ketjussa. (Monrat ym., 2019.) Lohkoketjun rakennetta on havainnollistettu kuviossa 1 (kuvio 1).



KUVIO 1 Yksinkertaistettu lohkoketjun rakenne (Zheng ym., 2018)

Lohkoketjuteknologia toimii käytännössä hajautettuna tietokantana, joka tallentaa tietoa ketjumaisesti järjestettyihin lohkoihin, luoden lohkoketjun. Jokaisella lohkolla on ainutlaatuinen tunniste eli tiiviste ja lohkot sisältävät tietoa, kuten transaktioita, sopimuksia tai muita tietoja, jotka on tallennettu lohkon luomisen yhteydessä. Nämä tiedot voivat käytännössä olla esimerkiksi siirretyn valuutan määrä, lähettäjän ja vastaanottajan osoitteet ja aikaleima. Koska lohkoketju muodostuu useamman tietokoneen hajautetusta verkostosta, lohkoketjuteknologia myös mahdollistaa tietojen tallentamisen hajautetusti useisiin tietokoneisiin, jotka on kytketty toisiinsa verkon kautta. Näitä tietokoneita kutsutaan solmuiksi. Jokainen solmu sisältää oman kopionsa lohkoketjusta ja tarkistaa jatkuvasti, että sen oma kopio on yhdenmukainen muiden solmujen kanssa. Tämän avulla varmistetaan lohkoketjun eheys ja vältetään väärinkäytökset. Jos yksi solmu sisältää virheellisen lohkon tai väärää tietoa, se voi aiheuttaa epäyhtenäisyyttä lohkoketjussa ja johtaa siihen, että muut solmut eivät hyväksy sitä. Tämä tarkistusprosessi on tärkeä, koska se takaa, että lohkoketju on luotettava ja

turvallinen käyttää. Uusien lohkojen luominen tapahtuu, kun verkon käyttäjät eli henkilöt tai organisaatiot käyttävät lohkoketjuun liittyviä sovelluksia ja tekevät uusia transaktioita. Transaktiot varmennetaan ja lisätään uuteen lohkoon konsensusalgoritmien avulla. Kun lohko on lisätty ketjuun, se on pysyvästi tallennettu kaikkiin solmuihin, eikä sitä voi enää muuttaa. (Habib ym., 2022.)

Zhang & Lee (2020) nimeävät kolme lohkoketjun perustyyppiä: julkinen lohkoketju, konsortion lohkoketju ja yksityinen lohkoketju. Eri lohkoketjutyypeillä on erilaiset sovellusskenaariot, joten valitun konsensusalgoritmin tulee vastata tietyn sovellusskenaarion vaatimuksiin. Yksityiset ja konsortion lohkoketjut eivät ole yhtä hajautuneita kuin julkiset lohkoketjut. (Zhang & Lee, 2020.) Tämä tutkielma tarkastelee lohkoketjuja julkisten lohkoketjujen näkökulmasta, sillä lohkoketjujen yhtenä perusajatuksena pidetään hajautuneisuutta, jota Nakamoton (2008) artikkeli myös käsitteli. Lohkoketjujen hajautuneisuus mahdollistaa esimerkiksi transaktiot käyttäjien välillä hajautetusti, mikä eliminoi perinteisten välittäjien vaatimukset validoida ja todentaa transaktiot (Monrat ym., 2019).

2.2 Konsensusalgoritmit

Tässä alaluvussa tarkastellaan, mitä ovat lohkoketjun konsensusalgoritmit ja niiden toimintaa yleisesti. Luvussa käydään läpi tunnetuimpia konsensusalgoritmeja, kuten Proof of Work (PoW) ja Proof of Stake (PoS), sekä lyhyesti muita vähemmän tunnettuja konsensusalgoritmeja. Luvun tavoitteena on antaa lukijalle ymmärrys siitä, miksi konsensusalgoritmeja käytetään, sekä selventää eri konsensusalgoritmien toimintaperiaatteita ja niiden vahvuuksia ja heikkouksia. Konsensusalgoritmien käsittelyn laajuus rajataan siten, että lukija ymmärtää niiden toiminnan yleisellä tasolla, jotta seuraavassa luvussa voidaan esitellä lohkoketjuteknologian teknologisia haasteita. Lohkoketjun konsensusalgoritmit ovat keskeinen osa lohkoketjuteknologiaa, ja niiden ymmärtäminen on tärkeää, kun pyritään arvioimaan lohkoketjuteknologian soveltuvuutta eri käyttökohteisiin ja kehittämään uusia sovelluksia.

Zhengin ym. (2018) mukaan lohkoketjun konsensus tarkoittaa sitä, että kaikki solmut ylläpitävät samaa hajautettua tilikirjaa (engl. Ledger). Keskuspalvelimen ollessa olemassa konsensuksen saavuttaminen ei juurikaan ole ongelma, sillä muut solmut seuraavat keskuspalvelimen tilikirjaa. Hajautetussa verkossa, kuten lohkoketjussa, haaste syntyy siitä, että siinä ei ole keskuspalvelinta, vaan verkko koostuu tasavertaisista solmuista. Jokaisen solmun on vaihdettava tietoja muiden solmujen kanssa, jotta päästään konsensukseen. Osa solmuista voi olla alhaalla tai offline-tilassa sekä osa solmuista voi olla haitallisia vaikuttaen negatiivisesti konsensuksen saavuttamiseen. Konsensusalgoritmien avulla näitä haittavaikutuksia pyritään minimoimaan, jotta ne eivät vaikuta lopulliseen konsensukseen. Konsensusalgoritmin tulee olla sopiva järjestelmän käyttämälle lohkoketjutyypille. Nämä algoritmit vaihtelevat lohkoketjujen

välillä riippuen siitä onko lohkoketju julkinen, yksityinen vai konsortion lohkoketju. (Zheng ym., 2018.)

Konsensuksen saavuttaminen lohkoketjussa ei siis aina ole yksinkertaista. Tämän ongelman ratkaisemiseksi on luotu erilaisia konsensusalgoritmeja. Lohkoketjussa konsensuksen saavuttamista epäluotettavien solmujen kesken usein kuvataan muunnokseksi bysanttilaisen kenraalin ongelmasta (engl. Byzantine fault). Ongelma kuvaa kuinka hajautetussa ympäristössä sen osapuolten on vaikea päästä yhteisymmärrykseen ilman luotettavaa keskitettyä auktoriteettia, sillä ympäristön osapuolet eivät voi luottaa toisiinsa. Lohkoketjun kontekstissa siis haasteeksi syntyy konsensuksen muodostaminen solmujen kesken. (Zheng ym., 2018.) Zhang & Lee (2020) kertovat, että konsensusalgoritmi on lohkoketjuteknologian yksi keskeisimmistä elementeistä, sillä se mahdollistaa lohkoketjun toiminnan hajautetusti ilman keskitettyä hallintoa. Konsensusalgoritmi tarkoittaa siis menetelmää, jolla lohkoketjun eri solmut pääsevät yhteisymmärrykseen uusien transaktioiden lisäämisestä lohkoihin ja lohkojen liittämisestä ketjuun.

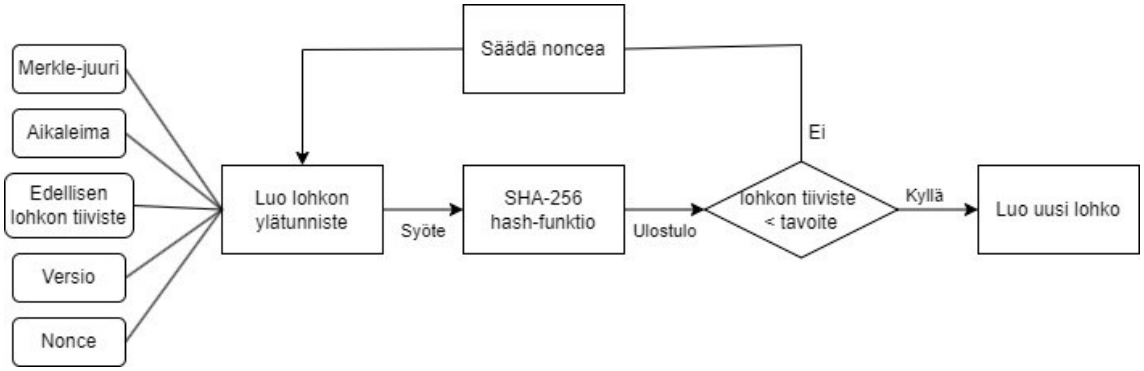
Kuten mainittu suurimpina konsensusalgoritmeina pidetään Proof of Work (PoW) ja Proof of Stake (PoS) -konsensusalgoritmeja (Nguyen & Kim, 2018). Seuraavaksi siirrytään tarkastelemaan kuinka kyseiset konsensusalgoritmit toimivat. Tämän jälkeen tarkastelemme lyhyesti muita konsensusalgoritmeja.

2.2.1 Proof of work -konsensusalgoritmi

Vuonna 2008 ”Satoshi Nakamoto” -pseudonyymiä käyttänyt taho esitteli Proof of work (PoW) -konsensusalgoritmin, joka on alun perin suunniteltu varmistamaan lohkoketjuun tallennettavien tapahtumien oikeellisuus ja eheys Bitcoin-järjestelmässä. PoW-menetelmä vaatii tietokonelaskentaa, sillä lohkojen lisääminen suoritetaan kilpailullisesti louhinnan (engl. mining) kautta. (Nakamoto, 2008.)

Nguyenin ja Kimin (2018) mukaan Proof of Work -konsensusalgoritmi toimii siten, että jokaisen verkon louhijan eli louhijasolmun on ratkaistava vaikea matemaattinen tehtävä, jotta he voivat lisätä uuden lohkon lohkoketjuun. Ennen kuin solmut voivat ratkaista tehtävän, he vahvistavat lohkoon sisältyvät tapahtumat ja muut tiedot, kuten edellisen hash-arvon eli kynnysarvon ja aikaleiman, ja lisäävät ne lohkoon. Ratkaisua varten solmut arvaavat salaisen arvon, joka on ”nonce”-kenttä, ja lisäävät sen lohkoon. Lohkon kaikki tiedot yhdistetään ja syötetään SHA-256 hash-funktioon. Jos kynnysarvon tulos on pienempi kuin vaikeustasoon liittyvä kynnysarvo, arvaus hyväksytään ja solmulla on oikeus lisätä uusi lohko lohkoketjuun. Muussa tapauksessa solmun on arvattava uusi salainen arvo, kunnes oikea arvo on löytynyt. Bitcoin-verkossa tehtävän vaikeustasoa säädetään siten, että uuden lohkon lisäämisen nopeus on keskimäärin yksi lohko kymmenessä minuutissa, ja kynnysarvo pienenee sitä mukaa kun tehtävän vaikeustaso kasvaa. Kun solmu löytää oikean salaisen arvon, se lähettää ehdotetun lohkon muiden solmujen tarkistettavaksi ja lisättäväksi lohkoketjuun. Muut solmut tarkistavat lohkon tapahtumat ja edellisen kynnysarvon oikeellisuuden. Jos tarkistukset ovat oikein, ehdotettu lohko lisätään ketjuun ja solmut aloittavat uuden tehtävän ratkaisun. Tätä prosessia jatketaan toistuvasti kasvattaen

lohkoketjua. (Nguyen & Kim, 2018.) Lohkojen luomista PoW-konsensusalgoritmissa on havainnollistettu kuviossa 2 (kuvio 2).



KUVIO 2 Vuokaavio lohkon luomisesta PoW-konsensusalgoritmissa (Zhang & Lee, 2020)

PoW-konsensusalgoritmi on suunniteltu siten, että sen avulla verkon osallistujat voivat varmistaa lohkoketjun oikeellisuuden ja estää huijaamisen. Laskentatehon tarve tekee lohkon löytämisen erittäin vaikeaksi, mikä estää yksittäistä henkilöä tai ryhmää hallitsemasta verkkoa ja estää lohkoketjun manipuloinnin. Tämä tekee PoW-konsensusalgoritmia käyttävistä järjestelmistä turvallisen ja luotettavan tavan siirtää arvoa verkossa. (Nguyen & Kim, 2018.)

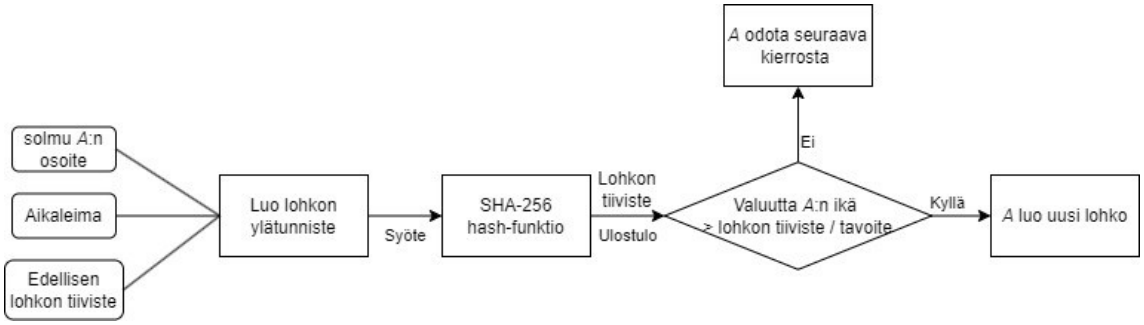
Wang ym. (2020) nimeävät PoW-konsensusalgoritmin vahvuuksiksi sen korkean hajautuneisuuden ja korkean turvallisuustason. PoW on yksinkertainen toteuttaa, mikä mahdollistaa solmujen vapaan liittymisen, mikä myös lisää hajautuneisuutta. PoW:n korkea turvallisuustaso on peräisin siitä, että järjestelmän vahingoittaminen vaatii valtavia investointeja laskentatehoon ja sähköön. Lisäksi algoritmin ansiosta lohkoketjussa tallennettujen tapahtumien oikeellisuus on taattu matemaattisesti ilman ihmisten osallistumista, mikä voi lisätä luottamusta järjestelmää kohtaan. (Zhang & Lee, 2020.)

Wang ym. (2020) mainitsevat PoW:n heikkouksiksi muun muassa sen pitkät vahvistusajat. Järjestelmän hajauttamisen varmistamiseksi vahvistusajan lyhentäminen on hankalaa. PoW:n hidas vahvistusaika voi myös aiheuttaa skaalautuvuus ongelmia. Lisäksi PoW kuluttaa huomattavan määrän resursseja, koska louhiminen vaatii paljon laskentatehoa ja sähköä, mikä voi olla ympäristölle haitallista. (Wang ym., 2020.)

2.2.2 Proof of stake -konsensusalgoritmi

Pian Bitcoin-järjestelmän syntymisen jälkeen, aloitettiin etsimään ratkaisuja PoW-konsensusalgoritmin haasteisiin esimerkiksi energiankulutuksen kanssa. Tämän pohjalta Sunny King ja Scott Nadal (2012) kehittivät Proof of Stake (PoS) -konsensusalgoritmin, jonka ensimmäinen julkinen toteutus julkaistiin PPCoin kryptovaluutan yhteydessä vuonna 2012. PoS-konsensusalgoritmi nähtiin alun perin energiatehokkaana vaihtoehtona PoW:lle. (King & Nadal, 2012) PPCoin ei kuitenkaan vielä täysin käyttänyt yksinomaisesti PoS:ia vaan PoW:n ja PoS:n hybridiä. (Nguyen & Kim, 2018.)

PoS-konsensusalgoritmi käyttää vähemmän energiaa kuin PoW. Sen sijaan, että lohkoketjun verifioinnin suorittaisivat louhijat ratkaisemalla monimutkaisia matemaattisia ongelmia, PoS:issa tapahtuu sattumanvarainen valinta seuraavasta lohkon luojasta. Lohkon luojia kutsutaan PoS:issa validaattoreiksi (engl. validator). Valintaan vaikuttaa käyttäjän omistama kyseisen valuutan määrä, jota kutsutaan panokseksi (engl. stake). Mitä suurempi panos käyttäjällä on, sitä suurempi todennäköisyys hänellä on tulla valituksi seuraavan lohkon luojaksi. Tämä on suunniteltu estämään hyökkäykset, koska hyökkääjän täytyisi omistaa suuri määrä valuuttaa, mikä olisi kallis investointi. (Nguyen & Kim, 2018.) Lohkojen luomista PoS-konsensusalgoritmissa on havainnollistettu kuviossa 3 (kuvio 3)



KUVIO 3 Vuokaavio lohkon luomisesta PoS-konsensusalgoritmissa (Zhang & Lee, 2020)

PoS:issa lohkot eivät enää olekaan louhintakilpailun tulos, vaan ne on luotu sattumanvaraisesti panoksen perusteella. Validaattorit toimivat verkon "vartijoina" ja tarkastavat transaktioiden ja lohkoketjun eheyden. Ne, jotka ovat aktiivisia lohkoketjun tarkkailussa, palkitaan kyseisen lohkoketjun valuutalla. Toisin kuin PoW:issa, joka palkitsee louhijat louhintakilpailun voittamisesta, PoS:issa palkitseminen perustuu käyttäjän panokseen ja sitoutumiseen verkon turvallisuuden ylläpitämisestä. (Nguyen & Kim, 2018.)

Wang ym. (2020) kertovat PoS:n yhdeksi eduksi resurssien säästön, koska validaattorit ei kuluta sähköä, sillä PoS:issa PoW:n louhinnan sijaan, lohkon luojat valitaan steikkauksen (engl. staking) kautta. Toinen PoS:n etu on nopeampi lohkojen vahvistusaika. Louhiminen ei vaadi yhtä vaativia laskelmia, vaan lähinnä pääoman todistamista, mikä vähentää konsensusvahvistuksen aikaa. (Wang ym., 2020.)

Haittoina Wang ym. (2020) mainitsevat muun muassa algoritmin monimutkaisuuden ja mahdollisuuden luoda tietoturva-aukkoja monimutkaisen toteutuksen vuoksi. Toinen haittapuoli on Matteus-vaikutus (engl. Matthew effect), joka johtaa siihen, että rikkaiden validaattorien pääoma kasvaa kasvamistaan, koska suurempi osuus kaikesta steikatusta pääomasta takaa enemmän palkkiota validaattoreille. (Wang ym., 2020.)

2.2.3 Muut konsensusalgoritmit

PoW ja PoS ovat kaksi yleisintä konsensusalgoritmia, joita käytetään lohkoketjuteknologian toiminnan varmistamiseen. Nämä konsensusalgoritmit

kategorisoidaan ”Proof-based” -konsensusalgoritmeiksi. Proof-based-konsensusalgoritmit edellyttävät, että verkon verifiointiin liittyvät solmut osoittavat olevansa pätevämpiä kuin muut, saadakseen oikeuden suorittaa konsensusalgoritmiin asetettu tehtävä palkkiota vastaan. (Nguyen & Kim, 2018.)

Proof-based-konsensusalgoritmeja on valtavasti ja useat perustuvat PoW:iin, PoS:iin tai niiden yhdistelmiin. Nguyen ja Kim (2018) luettelevat tutkimuksessaan useita eri proof-based-konsensusalgoritmeja, joista esimerkkejä PoW:iin perustuvista konsensusalgoritmeista ovat muun muassa ”Cuckoo hash function-based PoW”, ”Prime number finding-based PoW”, ”Double puzzles-based PoW” ja ”Generalized PoW”. Esimerkkejä PoS:iin perustuvista konsensusalgoritmeista ovat muun muassa ”Delegated PoS” ja ”State of the block-based PoS”. PoS:n ja PoW:n yhdistelmiin perustuvia konsensusalgoritmeja ovat heidän mukaansa muun muassa ”Proof of Activity”, ”Coin age-based PoW difficulty re-designation” ja ”Stake-based PoW difficulty re-designation”. (Nguyen & Kim, 2018.)

Nguyen ja Kim (2018) luettelevat myös tutkimuksessaan muita proof-based-konsensusalgoritmeja kuin PoW ja PoS, joita ovat muun muassa ”Proof of burn”, ”Proof of space”, ”Proof of elapsed time” ja ”Proof of luck”.

Nguyen ja Kimin (2018) mukaan Proof-based-konsensusalgoritmien lisäksi on myös ”Vote-based”-konsensusalgoritmeja. Vote-based-konsesusalgoritmeissa solmut viestivät keskenään tehdäkseen sopimuksen tilikirjaan liitettävistä lohkoista tai tapahtumista. Nguyen ja Kim (2018) jakavat vote-based-konsensusalgoritmit ”Byzantine fault tolerance-based” ja ”Crash fault tolerance-based”-konsensusalgoritmeihin. Byzantine fault tolerance-based konsensus on konsensus, joka voisi estää kaatuvien solmujen ja kumoutuneiden solmujen tapaukset. ”Crash fault tolerance-based” konsensus on taas konsensus, joka voisi estää vain kaatuvien solmujen tapaukset. Kaikkien näitä kahta konsensusta käyttävien konsensusalgoritmien on luotettava, että tietty määrä solmuista toimii normaalisti, joka tekee niiden käytöstä haastavaa julkisessa hajauttetussa ympäristössä. (Nguyen & Kim, 2018.)

Proof-based- ja vote-based-konsensusalgoritmien lisäksi on olemassa muihin toimintoihin perustuvia konsensusalgoritmeja, kuten esimerkiksi ”Federated Byzantine Agreement” (FBA) (Florian, Henningsen, Ndolo & Scheuermann 2022).

3 LOHKOKETJUTEKNOLOGIAN TEKNOLOGISET HAASTEET

Tässä luvussa tarkastellaan muutamia lohkoketjuteknologian teknologisia haasteita ja niihin esitettyjä ratkaisuja lähdekirjallisuuden pohjalta. Käsiteltäviksi haasteiksi valikoituivat seuraavat: skaalautuvuus, energiankulutus, turvallisuus ja yhteentoimivuus. Nämä haasteet valikoituivat tarkasteltaviksi, sillä ne esiintyivät lähdekirjallisuudessa useasti ja niitä voidaan pitää lohkoketjun toiminnan ja käyttöönoton kannalta kriittisinä haasteina. Riippuen kriteereistä on kuitenkin tärkeä huomata, että ei ole selvää ovatko valikoidut haasteet juuri ne suurimmat tai kriittisimmät haasteet. Näkemykset haasteiden suuruudesta tai kriittisyydestä voivat vaihdella riippuen lähteestä.

Lohkoketjuteknologia tarjoaa monia etuja, kuten avoimuuden, läpinäkyvyyden, turvallisuuden ja hajautetun hallinnan. Se soveltuu erityisesti transaktioiden hallintaan ja seurantaan, kuten kryptovaluuttojen siirtoihin. Lohkoketjuteknologiaa voidaan myös soveltaa laajemmin eri teollisuudenaloilla, kuten terveydenhuollossa tai tuotantoteollisuudessa. (Ahram ym., 2017.) Kuitenkaan lohkoketjuteknologia ei tule ilman haasteita, ja nämä haasteet tulisi ratkaista ennen sen laajempaa käyttöönottoa.

Lohkoketjuteknologian haasteita voidaan tarkastella useasta eri näkökulmasta. Ali ym. (2021) jakavat haasteet teknologisiin, organisatorisiin, omaksumisen, operatiivisiin ja ympäristön ja kestävän kehityksen haasteisiin. Batubara, Ubacht ja Janssen (2018) taas jakavat haasteet teknologisiin, organisatorisiin ja ympäristöllisiin haasteisiin. Myös Toufaily, Zalan ja Dhaou (2021) jakavat haasteet näihin kolmeen edellä mainittuun näkökulmaan (teknologiset, organisatoriset ja ympäristölliset haasteet) kuten Batubara, Ubacht ja Janssen.

Ali ym. (2021) mukaan teknologisia haasteita ovat esimerkiksi turvallisuus, yksityisyys ja integraatio. Organisatorisia haasteita ovat esimerkiksi rakenteellinen suunnittelu ja organisaation valmius ja muutos. Omaksumisen haasteiksi he mainitsevat muun muassa yhteensopivuuden, yhteentoimivuuden ja säännöstelyn haasteet. Operatiivisiin haasteisiin he listaavat muun muassa lohkoketjun ylläpidon, skaalautuvuuden, latenssin ja suorituskyvyn. Ympäristön ja

kestävän kehityksen haasteiksi he mainitsevat muun muassa lakien ja säännösten tuen ja kestävän kehityksen huolet. (Ali ym., 2021.)

Batubara ym. (2018) jakaessa haasteet kolmeen eri näkökulmaan, he näkevät teknologisina haasteina muun muassa turvallisuuden, skaalautuvuuden, yhteentoimivuuden ja laskennan tehokkuuden. Organisatorisina haasteina he näkevät esimerkiksi luotettavuuden ja auditoinnin. Ympäristöllisillä haasteilla Batubara ym. (2018) tarkoittavat käyttöympäristön (ulkoisia) haasteita. Tällaisia haasteita ovat heidän mukaansa esimerkiksi haasteet liittyen lakeihin ja säännöstelyyn ja tuki-infrastruktuuriin. Kuten mainittu myös Toufaily ym. (2021) jakavat lohkoketjuteknologian haasteet näihin kolmeen näkökulmaan (teknologiset, organisatoriset ja ympäristölliset haasteet). Kuitenkin se mihin näkökulmaan tietty haaste on kategorisoitu, vaihtelee lähteiden välillä.

Tässä tutkielmassa käsiteltävät haasteet on lähteiden mukaan kategorisoitu teknologisiksi haasteiksi. Seuraavaksi siirrytään tarkastelemaan näitä teknologisia haasteita ja niiden ratkaisuja tarkemmin.

3.1 Skaalautuvuus

Hafidin, Senhaji Hafidin ja Samihin (2020) mukaan lohkoketjun skaalautuvuudella viitataan sen kykyyn käsitellä suuria määriä tietoa ja transaktioita nopeasti ja tehokkaasti ilman että lohkoketjun turvallisuus ja hajautuneisuus heikkenee merkittävästi. Tämä on tärkeä ominaisuus, sillä mitä enemmän käyttäjiä ja transaktioita lohkoketjussa on, sitä suurempi on riski, että lohkoketjun suorituskyky hidastuu. Skaalautuvan lohkoketjun avulla voidaan mahdollistaa laajempi käyttö ja sovellukset. (Hafid ym., 2020.)

Lohkoketjun skaalautuvuuteen vaikuttavat useat tekijät. Yksi tärkeimmistä tekijöistä on suoritusteho (engl. throughput), joka kuvaa vahvistettujen transaktioiden määrää sekunnissa. Julkisissa lohkoketjuissa suoritusteho voi olla hyvin pieni verrattuna muihin järjestelmiin. Esimerkiksi Bitcoin-järjestelmä pystyy käsittelemään enintään 7 transaktiota sekunnissa, kun taas Visa pystyy käsittelemään 1700 ja PayPal 193 transaktiota sekunnissa. (Hafid ym., 2020.)

Toinen tärkeä tekijä on tallennustilan tarve. Jos kaikki transaktiot tallennetaan lohkoketjuun, sen koko kasvaa merkittävästi ja tallennustilan tarve kasvaa huomattavasti. Tämä myös luonnollisesti lisää lohkoketjun lataamiseen tarvittavaa aikaa. (Hafid ym., 2020.)

Kustannukset ovat myös merkittävä tekijä, sillä käyttäjä maksaa transaktiomaksun louhijalle, joka sisällyttää transaktion uuteen lohkoon. Tämän vuoksi käyttäjien on kustannustehokkaampaa suorittaa mahdollisimman monta transaktiota lohkoketjun ulkopuolella ja kirjata ne myöhemmin yhtenä transaktiona lohkoketjussa. (Hafid ym., 2020.)

Lisäksi viive tai vahvistusaika (engl. confirmation time) eli aika transaktion lähetyksen ja sen hyväksymisen välillä on tärkeä skaalautuvuustekijä. Mitä enemmän käyttäjiä lähettää transaktioita lohkoketjussa, sitä suuremmaksi transaktion vahvistusaika kasvaa, sillä jokainen transaktio vaati vertaisverkon

varmennuksen. Esimerkiksi Bitcoin-järjestelmässä uusi lohko pyritään lisäämään lohkoketjuun noin 10 minuutin välein, joten vahvistusaika on vähintään 10 minuuttia. (Hafid ym., 2020.)

Skaalautuvuuden parantaminen ei kuitenkaan ole niin yksinkertaista. Haaste syntyy vastakkaisten vaatimusten vuorovaikutuksesta lohkoketjun perusteellisesta suunnittelusta. Ethereumin perustaja, Vitalik Buterin, on luonnehtinut tätä ongelmaa ”lohkoketjun skaalautusvuustrilemmalla” (engl. blockchain trilemma). (Monte ym., 2020.) Tämä trilemma muodostuu kolmesta näkökohdasta: hajauttamisesta, turvallisuudesta ja skaalautuvuudesta. Hajautuneisuus on lohkoketjun ydin ja luonne, turvallisuus on olennainen ominaisuus, kun taas skaalautuvuus on suurin haaste. (Hafid ym., 2020.) Lohkoketjun skaalautuvuustrilemmassa todetaan, että kaikki parannukset joko skaalautumiseen, turvallisuuteen tai hajauttamiseen vaikuttavat negatiivisesti ainakin toiseen kahdesta muusta näkökohdasta (Monte ym., 2020).

Lohkoketjun skaalautuvuustrilemmaan on esitetty lukemattomia eri ratkaisuja, joista osa käydään seuraavaksi läpi. Hafidin ym. (2020) mukaan skaalautuvuustrilemman ratkaisut voidaan jakaa ns. ensimmäisen kerroksen (engl. first layer) ja toisen kerroksen (engl. second layer) ratkaisuihin. Ensimmäisen kerroksen eli on-chain-ratkaisuilla tarkoitetaan ratkaisuja, joissa lohkoketjun teknistä toteutusta muutetaan, parantaen lohkoketjun suorituskykyä. On-chain-ratkaisuja ovat esimerkiksi pirstaloiminen (engl. sharding), lohkojen koon kasvatus, eri konsensusalgoritmien käyttö ja suunnattu syklitön verkko eli DAG (engl. directed acyclic graph). (Hafid ym., 2020.)

Toisen kerroksen eli off-chain-ratkaisuilla taas tarkoitetaan ratkaisuja, joilla luodaan mekanismeja lohkoketjun ulkopuolelle. Näiden mekanismien avulla voidaan esimerkiksi käsitellä tiettyjä transaktioita lohkoketjun ulkopuolella, jolloin vain tärkeimmät transaktiot tallentuvat lohkoketjuun. Hafidin ym. (2020) mukaan off-chain-ratkaisut voidaan luokitella sivuketjuihin (engl. sidechains) ja maksukanaviin (engl. payment channels). (Hafid ym., 2020.)

Wangin ym. (2019) mukaan erityisesti sirpalointi on noussut hyväksi ehdokkaaksi skaalautuvuuden haasteiden ratkaisemiseksi lohkoketjuissa. Lohkoketjujen sirpaloinnilla tarkoitetaan tilannetta, jossa lohkoketju jakautuu useisiin erillisiin osiin tai osajärjestelmiin, joita kutsutaan sirpaleiksi (engl. shard). Sirpalointi on siis tekniikka, jossa lohkoketju jaetaan pienempiin osiin eli sirpaleisiin tietyn kriteerin perusteella, kuten esimerkiksi transaktioiden määrän tai lohkojen koon perusteella. Tämä tekniikka auttaa parantamaan lohkoketjun suorituskykyä ja skaalautuvuutta. Sirpalointi voi vähentää verkon kuormitusta ja lisätä transaktioiden suoritusnopeutta jakamalla tietokannan hallinnan useille solmuille. Jokaisella sirpaleella voi olla oma lohkoketjunsa, joka käsittelee vain siihen liittyviä transaktioita. Sirpaleet voivat myös kommunikoida keskenään, jotta tiedot voidaan siirtää sirpaleiden välillä tarvittaessa. Lohkoketjun sirpalointi voi kuitenkin aiheuttaa joitakin haasteita. Esimerkiksi sirpaleiden välisen yhteistyön ja yhtenäisyyden ylläpitäminen voi olla vaikeaa. (Wang ym., 2019.) Sirpalointi myös altistaa verkon ns. 1 %-hyökkäykselle eli koko verkko voidaan murtaa, jos yksikin sirpale murretaan. Täten tietoturva on suunniteltava huolellisesti, jotta

varmistetaan lohkoketjun eheys ja estetään mahdolliset hyökkäykset. (Hafid ym., 2020.)

Skaalautuvuusongelmien ratkaiseminen lohkoketjuissa on kuitenkin monimutkainen haaste, joka vaatii kokonaisvaltaisen lähestymistavan. Useita ratkaisuja on esitetty ja kehitetty skaalautuvuuden haasteisiin, mutta ne tuovat mukanaan myös omat haasteensa. Potentiaalisimmiksi ratkaisuiksi kuitenkin nousevat vaihtoehtoiset konsensusalgoritmit, sirpalointi sekä ensimmäisen ja toisen kerroksen ratkaisujen yhdistäminen. (Hafid ym., 2020.)

3.2 Energiankulutus

Useat lohkoketjut kuluttavat erittäin suuria määriä energiaa. Esimerkiksi heinäkuussa 2021 Digiconomist on arvioinut Bitcoin-verkon energiankulutuksen (sähkönkulutuksen) vaihtelevan välillä 29,96–135,12 terawattituntia vuodessa (Kohli ym., 2023). Digiconomistin tuoreimpien arvioiden mukaan Bitcoin-verkon energiankulutuksen arvioidaan olevan vähintään 99,11 terawattituntia vuodessa (Digiconomist, 2023). Cambridge Bitcoin Electricity Consumption Indexin (CBECI) tuorein arvio estimoi, että Bitcoin-verkon vuosittainen sähkönkulutus on 137,79 terawattituntia vuodessa. CBECI:n arvion mukaan Bitcoin-verkon hypoteettinen sähkönkulutus vaihtelee välillä 64,58–239,79 terawattituntia vuodessa. Suomen sähkönkulutus oli tilastokeskukseen mukaan vuonna 2022 n. 82 terawattituntia vuodessa (Tilastokeskus, 2023). Näiden arvioiden pohjalta Bitcoin-verkko kuluttaa vuodessa enemmän sähköä kuin koko Suomi.

Bitcoin-verkon suuri energiankulutus pohjautuu PoW-konsensusalgoritmiin. PoW-konsensusalgoritmin vaatiessa suuria määriä laskentatehoa, se luonnostaan kuluttaa myös suuren määrän energiaa. PoW:n suurta energiankulutusta on pyritty ratkaisemaan muun muassa redundanssin vähentämisellä, optimaalisilla louhintalaitteilla ja uusiutuvilla energianlähteillä vähentäen energiankulutuksen haittapuolia. Energiankulutusta voidaan kuitenkin parhaiten vähentää käyttämällä energiatehokkaampia konsensusalgoritmeja, sillä heikko energiatehokkuus johtuu useasti konsensusalgoritmin olennaisesta suunnittelusta. (Kohli ym., 2023.) Esimerkiksi PoS luotiin alun perin parantamaan PoW:n suurta energiankulutusta (Zheng ym., 2018). PoS:issa energiankulutus on pienempää, sillä lohkojen lisääminen lohkoketjuun ei tapahdu laskentatehoa vaativan pulman kautta vaan validaattorien panoksen steikkauksesta lohkoketjuun. Tämä vähentää energiankulutusta ja hiilidioksidipäästöjä huomattavasti. (Kohli ym., 2023.) Esimerkiksi Kapengutin ja Mizrachin (2023) mukaan Ethereumin siirtyessä PoW:ista PoS:iin, sen energiankulutus laski 99,98 %.

3.3 Turvallisuus

Lohkoketjuilla on useita turvallisuus- ja haavoittuvuusuhkia. Alam Khanin ym. (2020) nimeävät seuraavat turvallisuusuhat: 51 %-hyökkäys, kaksinkertainen kulutus (engl. double spending), Eclipse attack -hyökkäykset ja identiteettivarkaudet.

51 %-hyökkäys on merkittävä turvallisuusuhka, sillä se toimii muiden hyökkäysten pohjana. 51 %-hyökkäyksessä yksi solmu tai solmujen joukko pyrkii saavuttamaan 51 % lohkoketjun laskentatehosta. Jos hyökkäävät solmut saavuttaisivat 51 % laskentatehosta, he pystyisivät muokkaamaan transaktioiden tietoja siten, että kaksinkertainen kulutus olisi mahdollista. (Alam Khan ym., 2020.) Kaksinkertainen kulutus tarkoittaa sitä, että sama valuutta esimerkiksi Bitcoin, voidaan käyttää useamman kerran (Heilman ym., 2015). Kaksinkertaisen kulutuksen lisäksi kyseiset solmut voisivat estää lohkojen louhimisen. Tällaisessa tilanteessa kyseisillä solmuilla on käytännössä valta koko lohkoketjun toiminnasta ja he voisivat mahdollisesti pysäyttää jopa koko lohkoketjun toiminnan. (Lin & Liao, 2017.) Yhden henkilön tai joukon on kuitenkin hyvin vaikea toteuttaa 51 %-hyökkäys vakiintuneissa ja tunnetuissa lohkoketjuissa, sillä se vaatisi valtavan määrän investointeja suurella riskillä. Vakiintuneissa lohkoketjuissa on kuitenkin myös riski 51 %-hyökkäykselle. Lohkoketjun louhijoiden kasvaessa, louhiminen yksin ei ole kannattavaa taloudellisesti, sillä mahdollisuus valikoitua lohkon luojaksi on erittäin pieni. Tällöin yksittäinen louhija voi liittyä louhintasyndikaattiin (engl. mining pool), joka muodostuu yksittäisistä louhijoista luoden louhijoiden joukon. Louhintasyndikaateissa palkkiot lohkon luomisesta jaetaan tasan louhijoiden kesken. Louhintasyndikaatin kasvaessa kasvaa myös mahdollisuus sille, että jokin syndikaatin louhijoista tulee valituksi. Syndikaatin kasvaessa, mahdollisuus 51 %-hyökkäykselle kasvaa. Esimerkiksi vuonna 2014 GHASH.IO -louhintasyndikaatti oli lähellä saavuttaa 51 % asema verkosta, jonka takia iso osa louhijoista lähti kyseisestä syndikaatista. (Alam Khan ym., 2020.)

Vaikka 51 %-hyökkäys on todella vaikea toteuttaa käytännössä, parhaimmat ratkaisut 51 %-hyökkäyksien estämiseksi on käyttää konsensusalgoritmeja, joissa tällaiset hyökkäykset ovat vielä haastavampia toteuttaa. PoS-konsensusalgoritmissa 51 %-hyökkäys nähdään epätodennäköisempänä kuin PoW:issa. PoW:issa hyökkääjän tulisi omistaa 51 % verkon laskentatehosta. Vastaavasti PoS:issa hyökkääjän tulisi omistaa vähintään 51 % kaikista verkon panoksista, joka voi olla erittäin suuri investointi riippuen lohkoketjun koosta. Tämän vaatimuksen lisäksi uskotaan, että henkilö, jolla on iso osa verkon panoksista, tuskin haluaa ryhtyä pahantahtoisiin toimiin, sillä se vaikuttaisi hänen tuottoihinsa negatiivisesti. (Nguyen & Kim, 2018.)

Toinen tunnettu mutta harvinainen hyökkäys on Eclipse attack. Eclipse attack -nimisessä hyökkäyksessä hyökkääjä ottaa haltuunsa uhrien tulevat ja lähtevät yhteydet eristäen heidät muista vertaisverkon käyttäjistä. Hyökkääjä voi suodattaa uhrien näkymän lohkoketjusta, pakottaen uhrin käyttämään laskentatehoa vanhentuneisiin näkymiin lohkoketjusta tai käyttää uhrien laskentatehoa

omiin tarkoituksiinsa. (Heilman ym., 2015.) Eclipse attack -hyökkäyksiin on esitetty ratkaisuksi esimerkiksi aluepohjaista naapurisolmun valintamenetelmää. Tällaisessa menetelmässä kukin solmu valitsee naapurinsa satunnaisesti tietyn alueen sisältä ja ulkopuolelta, johon solmu kuuluu. (Matsuura, Goto & Sao, 2021.) Kuitenkin helpoin ja yksinkertaisin tapa välttyä Eclipse attack -hyökkäyksiltä on, että solmut rajoittavat saapuvia yhteyksiä ja ovat tietoisia muiden solmujen kanssa luoduista yhteyksistä (Gemini, 2023).

Lohkoketjuissa on myös uhka identiteettivarkauksille. Lohkoketjujen säilyttäessä käyttäjien anonymiteetin ja yksityisyyden, lohkoketjussa säilytettävät omaisuudet turvataan yksityisellä avaimella (engl. private key). Tällä avaimella käyttäjät voivat todistaa olevansa lompakon omistaja. Kuitenkin jos yksityinen avain varastetaan tai hukataan, kukaan kolmas osapuoli ei voi palauttaa sitä alkuperäiselle omistajalle. Tällaisessa tilanteessa kaikki omistajan varat voivat hävitä, ja varkaustilanteissa varasta on lähes mahdotonta tunnistaa. Tämän seurauksena identiteettivarkaus voidaan toteuttaa hyvin pienellä kiinnijäämisen riskillä. (Xu, 2016.) Yksityisen avaimen varastaminen on kuitenkin hyvin vaikeaa, mutta ei täysin mahdotonta. Nykyiset salausstandardit eivät myöskään ole täysin murtumattomia, ja kvanttilaskennan kehityksen myötä, on mahdollista, että kryptografiset avaimet voidaan murtaa. Tämän seurauksena koko lohkoketjun perusta tuhoutuisi. Tämän takia on suunniteltu lohkoketjuja, jotka kestävät kvanttihyökkäykset. (Fernández-Caramès & Fraga-Lamas, 2020.)

3.4 Yhteentoimivuus

Pillain, Biswasin ja Muthukkumaran (2019) mukaan lohkoketjuteknologian tulevaisuus riippuu pitkälti sen kyvystä olla vuorovaikutuksessa ja integroitua muihin järjestelmiin. Siksi lohkoketjujen yhteentoimivuuteen tulisi panostaa. Yhteentoimivat lohkoketjut sallisivat tiedonsiirron lohkoketjusta toiseen lohkoketjuun (Lafourcade & Lombard-Platet, 2020). Lohkoketjujen välinen yhteentoimivuus parantaisi täten lohkoketjujen skaalautuvuutta kokonaiskuvassa, sillä tämä mahdollistaisi tehokkaasti skaalautuvien lohkoketjujen saumattoman toiminnan yhdessä heikosti skaalautuvien lohkoketjujen kanssa (Monika & Bhatia, 2020). Lafourcaden ja Lombard-Platetin (2020) mukaan ei ole suoraa tapaa saavuttaa lohkoketjujen välistä yhteentoimivuutta ainakaan ilman luotettavaa kolmatta osapuolta. Tällä hetkellä käyttäjän halutessa vaihtaa eri lohkoketjun kryptovaluutasta toiseen, hänen tulee käyttää kolmannen osapuolen ”escrow” -tyyppisiä palveluita. (Lafourcade & Lombard-Platet, 2020.) Joissain tapauksissa yhteentoimivuutta on pyritty ratkaisemaan erilaisten vaihtokauppa menetelmien avulla, kuten ”atomic swap” ja ”bridging” -ratkaisujen kautta (Monika & Bhatia, 2020).

Lafourcade ja Lombard-Platet (2020) väittävät, että klassisen määritelmän mukaan lohkoketjujen on mahdoton olla vuorovaikutuksessa minkään muun lohkoketjun kuin itsensä kanssa. Kuitenkin heidän mukaansa kevennetyllä määritelmällä, yhteentoimivat lohkoketjut vastaisi ”2-in-1” -lohkoketjua. ”2-in-1” -

lohkoketjut olisivat heidän mukaansa lohkoketjuja, joissa tilikirja on jaettu kahteen erilliseen rekisteriin. (Lafourcade & Lombard-Platet, 2020.)

Lafourcaden ja Lombard-Platetin (2020) mukaan myös kaikki tähän mennessä luodut käytännön toteutukset yhteentoimivuudesta lohkoketjujen välillä toimivat vaihtamalla valmiiksi luotuja tokeneita tai kryptovaluuttaa kahden eri lohkoketjun välillä. Tämä ei kuitenkaan tarjoa mahdollisuutta siirtää juuri tiettyjä tokeneita ja kryptovaluuttaa yhdestä lohkoketjusta toiseen. Toteutus, jossa saumaton siirto olisi mahdollista, tarkoittaisi molempien lohkoketjujen luotujen tokeneiden ja kryptovaluutan kokonaismäärän tasapainon muuttumista (Lafourcade & Lombard-Platet, 2020). Saumaton siirto ei siis käytännössä ole mahdollista, sillä se vaatisi tokeneiden tai kryptovaluuttojen luonnin tyhjästä vaihtojen yhteydessä.

Yhteentoimivuus lohkoketjujen välillä on tähän mennessä toteutettu valuutanvaihdon tapaan yleensä kolmansien osapuolien kautta. (Lafourcade & Lombard-Platet, 2020.) Valuutanvaihdossa henkilö A lähettää tietyn lohkoketjun tokeneita tai kryptovaluuttaa henkilölle B, jolloin henkilö A saa vastineeksi toisessa lohkoketjussa olevia varoja henkilöltä B. Tämä ei kuitenkaan tarkoita sitä, että lohkoketjut olisivat vuorovaikutuksessa toistensa kanssa, sillä varat pysyvät vastaavissa lohkoketjuissaan ja ne siirretään vain tililtä toiselle, joka vaatii ulkoisia muuttujia. Tällaista valuutanvaihtoa voidaan kutsua ”asset exchangeksi”. (Monika & Bhatia, 2020.)

Lafourcaden ja Lombard-Platetin (2020) väittämän pohjalta voidaan todeta, että jos todellinen yhteentoimivuus haluttaisiin toteuttaa, lohkoketjujen varojen tulisi olla mahdollista vaihtaa lohkoketjusta toiseen saumattomasti. Siirtoa varten molempien lohkoketjujen varojen tulisi olla yhteensopivia keskenään. Siirron aikana varat poltettaisiin toisessa lohkoketjussa ja luotaisi toisessa lohkoketjussa, jolloin varojen kokonaismäärä pysyisi samana. Kuten mainittu tällainen toteutus on käytännössä mahdoton toteuttaa, sillä varojen luominen tyhjästä tällaisen vaihtokaupan yhteydessä ei ole mahdollista. Haasteena tällaisessa toteutuksessa olisi myös se, että ei ole arviota siitä, kuinka paljon kryptovaluutta A on kryptovaluuttaa B. Tämänhetkisissä käytännön ratkaisuissa arviot tapahtuvat kryptovaluutta kurssien mukaan, jotka vaativat kolmannen osapuolen pörssejä. On kuitenkin tärkeä huomata, että lohkoketjujen yhteentoimivuus on laajempi kokonaisuus kuin pelkästään kryptovaluuttojen ketjujen välinen siirtäminen, ja sitä tulisi tutkia tulevaisuudessa enemmän (Belchior ym., 2022).

4 YHTEENVETO

Tässä tutkielmassa käsiteltiin lohkoketjuteknologiaa ja sen teknologisia haasteita sekä kyseisiin haasteisiin esitettyjä ratkaisuja julkisten lohkoketjujen näkökulmasta. Tutkielman alussa käsiteltiin lohkoketjuteknologian toimintaa yleisesti: kuinka lohkoketjuteknologia toimii ja kuinka lohkoketju rakentuu. Lohkoketjun toiminta pohjautuu konsensusalgoritmeihin, joista käsiteltiin laajemmin Proof of Work (PoW) sekä Proof of Stake (PoS) -konsensusalgoritmeja. Seuraavissa luvuissa käsiteltiin lohkoketjuteknologian haasteita. Haasteet oli jaettu muun muassa teknologisiin, ympäristöllisiin ja organisatorisiin haasteisiin. Näistä haasteista keskityttiin teknologisiin haasteisiin. Teknologisista haasteista esiteltiin neljä keskeisintä: skaalautuvuus, energiankulutus, turvallisuus ja yhteentoimivuus.

Tutkielman ensimmäinen tutkimuskysymys oli "Mitkä ovat lohkoketjuteknologian suurimmat teknologiset haasteet?". Lähdekirjallisuuden perusteella skaalautuvuus, energiankulutus, turvallisuus ja yhteentoimivuus olivat neljä suurinta haastetta. On kuitenkin huomattava, että haasteiden suuruus ja kriittisyys vaihtelevat lähdekirjallisuudesta ja näkemyksistä riippuen. Toisin sanoen, yksimielisesti ei voida väittää, että juuri nämä neljä haastetta ovat lohkoketjuteknologian suurimmat teknologiset haasteet. Lisäksi on huomattava, että lohkoketjuteknologialla on myös muita merkittäviä haasteita, joita ei tutkielmassa käsitellä. Näiden haasteiden huomiotta jättäminen voi kuitenkin vääristää kuvaa lohkoketjuteknologian teknologisesta kehityksestä ja sen mahdollisista sovelluksista tulevaisuudessa. Siksi on tärkeää pitää mielessä, että lohkoketjuteknologian haasteita on monia ja uusia haasteita voi syntyä teknologian kehittyessä ja sitä sovellettaessa eri aloilla.

Tutkielman toinen tutkimuskysymys oli "Minkälaisia ratkaisuja kyseisiin haasteisiin on kehitetty?". Lähdekirjallisuuden perusteella voidaan todeta, että haasteisiin on kehitetty useita eri ratkaisuja. Kehitetyt ratkaisut riippuvat pitkälti siitä, mihin haasteeseen pyritään vastaamaan. Voidaan kuitenkin todeta, että ratkaisuja on kehitetty skaalautuvuuden, energiankulutuksen ja turvallisuuden haasteisiin. Yhteentoimivuuden ratkaisut ovat kuitenkin jossain määrin haasteellisia, sillä Lafourcaden ja Lombard-Platetin (2020) mukaan todellista yhteentoimivuutta ei voida saavuttaa lohkoketjujen välillä lohkoketjujen perimmäisen luonteen vuoksi. Yhteentoimivuus voi kuitenkin olla mahdollista erilaisten ratkaisujen avulla, riippuen yhteentoimivuuden määritelmästä (Lafourcade & Lombard-Platet, 2020; Monika & Bhatia, 2020).

Haasteiden ratkaisuja tarkastellessa on myös tärkeä huomata, että haasteet kuten skaalautuvuus ja energiankulutus ovat vahvasti esillä PoW-konsensusalgoritmissa (Kohli ym., 2023; Kapengut & Mizrach, 2023). PoS-konsensusalgoritmi voisi olla hyvä ratkaisu PoW-konsensusalgoritmin korvaamiseen, sillä PoS:issa energiankulutus on huomattavasti pienempi ja skaalautuvuus merkittävästi parempi (Kohli ym., 2023; Kapengut & Mizrach, 2023; Wang ym., 2020). On

kuitenkin tärkeä huomata, että PoS-konsensusalgoritmi tuo mukanaan myös omia haasteitaan, joita tässä tutkielmassa ei käyty syvällisesti läpi.

Tutkielman tulosten pohjalta vaikuttaa siltä, että lohkoketjuteknologian haasteet riippuvat pitkälti lohkoketjujen konsensusalgoritmeista, ja haasteet vaihtelevat laajasti konsensusalgoritmien välillä. Myöskään eri haasteiden ratkaisemiseksi ei ole selvää yhteisymmärrystä siitä, kuinka kyseiset haasteet tulisi ratkaista.

Tutkielma sisältää useita rajoitteita, jotka voivat vaikuttaa tuloksiin. Tutkimusaihe on todella laaja, joten aihetta on rajattu merkittävästi. Tämä tutkielma toimii pitkälti yleiskatsauksena lohkoketjuteknologian teknologisista haasteista. Neljä tarkemmin käsiteltyä haastetta ovat jo itsessään erittäin laajoja ja moniulotteisia, joten ei voida olettaa, että ne olisi käsitelty täysin holistisesti. Vastaavasti kyseisten haasteiden ratkaisut ovat myös erittäin laajoja. Kuitenkin tutkielman pohjalta voidaan mainita se, että konsensusalgoritmit vaikuttavat olevan suuressa roolissa haasteiden ratkaisemisessa. Tämän perusteella eri konsensusalgoritmien rooli haasteiden ratkaisuissa voisi olla mielenkiintoinen jatkotutkimusaihe.

LÄHTEET

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, 137–141. https://doi.org/10.1109/TEMSCON.2017.7998367

Alam Khan, F., Asif, M., Ahmad, A., Alharbi, M. & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, *55*, 102018. https://doi.org/10.1016/j.scs.2020.102018

Ali, O., Jaradat, A., Kulakli, A. & Abuhalimeh, A. (2021). A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. *IEEE Access*, *9*, 12730–12749. https://doi.org/10.1109/ACCESS.2021.3050241

Batubara, F. R., Ubacht, J. & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 1–9. https://doi.org/10.1145/3209281.3209317

Belchior, R., Vasconcelos, A., Guerreiro, S. & Correia, M. (2022). A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Computing Surveys*, *54*(8), 1–41. https://doi.org/10.1145/3471140

Bitcoin Energy Consumption Index. (2023). Digiconomist. Haettu 25.4.2023 osoitteesta https://digiconomist.net/bitcoin-energy-consumption/

Cambridge Bitcoin Electricity Consumption Index (CBECI). (2023). Haettu 25.4.2023 osoitteesta https://ccaf.io/cbeci/index

Eclipse Attacks Explained: What Are They? (2023). Gemini. Haettu 28.4.2023 osoitteesta https://www.gemini.com/cryptopedia/eclipse-attacks-defense-bitcoin

Energian kokonaiskulutus väheni 5 % vuonna 2022 - Tilastokeskus. (18.4.2023). Haettu 25.4.2023 osoitteesta https://www.stat.fi/julkaisu/cl8lnt36ar51h0duts69hbekz

Fernández-Caramès, T. M. & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, *8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985

Florian, M., Henningsen, S., Ndolo, C. & Scheuermann, B. (2022). The sum of its parts: Analysis of federated byzantine agreement systems. *Distributed Computing*, *35*(5), 399–417. https://doi.org/10.1007/s00446-022-00430-0

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S. & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, *14*(11), 341. https://doi.org/10.3390/fi14110341

Hafid, A., Senhaji Hafid, A. & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access*, *PP*. https://doi.org/10.1109/ACCESS.2020.3007251

Heilman, E., Kendler, A., Zohar, A. & Goldberg, S. (2015). *Eclipse Attacks on Bitcoin's Peer-to-Peer Network*.

Kapengut, E. & Mizrach, B. (2023). An Event Study of the Ethereum Transition to Proof-of-Stake. *Commodities*, *2*(2), 96–110. https://doi.org/10.3390/commodities2020006

King, S. & Nadal, S. (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*.

Kohli, V., Chakravarty, S., Chamola, V., Sangwan, K. S. & Zeadally, S. (2023). An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions. *Digital Communications and Networks*, *9*(1), 79–89. https://doi.org/10.1016/j.dcan.2022.06.017

Lafourcade, P. & Lombard-Platet, M. (2020). About blockchain interoperability. *Information Processing Letters*, *161*, 105976. https://doi.org/10.1016/j.ipl.2020.105976

Matsuura, H., Goto, Y. & Sao, H. (2021). Region-based Neighbor Selection in Blockchain Networks. *2021 IEEE International Conference on Blockchain (Blockchain)*, 21–28. https://doi.org/10.1109/Blockchain53845.2021.00015

Monika & Bhatia, R. (2020). Interoperability Solutions for Blockchain. *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, 381–385. https://doi.org/10.1109/ICSTCEE49637.2020.9277054

Monrat, A. A., Schelén, O. & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access*, *7*, 117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094

Monte, G. D., Pennino, D. & Pizzonia, M. (2020). Scaling blockchains without giving up decentralization and security: a solution to the blockchain scalability trilemma. *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 71–76. https://doi.org/10.1145/3410699.3413800

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Nguyen, T. & Kim, K. (2018). A survey about consensus algorithms used in Blockchain. *Journal of Information Processing Systems*, *14*, 101–128. https://doi.org/10.3745/JIPS.01.0024

Pillai, B., Biswas, K. & Muthukkumarasamy, V. (2019). *Blockchain Interoperable Digital Objects* (s. 80–94). https://doi.org/10.1007/978-3-030-23404-1_6

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. https://doi.org/10.1016/j.im.2021.103444

Wang, G., Shi, Z. J., Nixon, M. & Han, S. (2019). SoK: Sharding on Blockchain. *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 41–61. https://doi.org/10.1145/3318041.3355457

Wang, Q., Huang, J., Wang, S., Chen, Y., Zhang, P. & He, L. (2020). A Comparative Study of Blockchain Consensus Algorithms. *Journal of Physics: Conference Series*, *1437*(1), 012007. https://doi.org/10.1088/1742-6596/1437/1/012007

Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financial Innovation*, *2*(1), 25. https://doi.org/10.1186/s40854-016-0046-5

Zhang, S. & Lee, J.-H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express*, *6*(2), 93–97. https://doi.org/10.1016/j.icte.2019.08.001

Zheng, Z., Xie, S., Dai, H.-N., Chen, X. & Wang, H. (2018). *Blockchain Challenges and Opportunities: A Survey*.