Miikka Kivinen

LOHKOKETJUSOVELLUKSET JA HAASTEET NIIDEN KÄYTTÖÖNOTOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Kivinen, Miikka
Lohkoketjusovellukset ja haasteet niiden käyttöönotossa
Jyväskylä: Jyväskylän yliopisto, 2019, 29 s.
Tietojärjestelmätiede, Kandidaatin tutkielma
Ohjaaja(t): Seppänen, Ville

Lohkoketjut ovat P2P-verkossa toimivia hajautettuja tietokantoja, jotka tallentavat käyttäjien luomat digitaalisesti allekirjoitetut transaktiot ketjun lohkoihin. Lohkoketjussa toimivat verkon solmut vahvistavat ja kokoavat transaktiot lohkoihin, jotka linkitetään toisiinsa ja lisätään ketjuun konsensusprotokollaa avuksi käyttäen. Jokainen verkon solmu pitää itsellään kopiota ketjusta, jolloin datan muuttaminen jälkikäteen on mahdotonta. Hajautetun luonteen ja kryptografiaan perustuvan linkityksen ansiosta tarjotaan teoriassa muuttumaton ja luotettava tilikirja. Lohkoketjut ovat lähivuosina saaneet paljon huomiota monilta tahoilta ja niistä on povattu perinteisten tietokantojen korvaajaa monilla toimialoilla. Teknologia on kuitenkin nuori ja siihen liittyy vielä monia ongelmakohtia. Esimerkiksi erilaiset turvallisuuteen ja skaalautuvuuteen liittyvät ongelmat vaikuttavat lohkoketjuratkaisujen käyttöönottoon, jolloin niiden syitä ja ratkaisuja on syytä tutkia. Lisäksi lohkoketjun käyttö ei ole aina järkevää, sillä se eroaa perinteisistä tietokannoista välillä perustavanlaatuisesti. Tässä tutkielmassa pyritään selvittämään mitkä tekijät vaikuttavat lohkoketjuratkaisujen käyttöönottoon yrityksissä. Kirjallisuuskatsauksessa selvitetään käyttöönottoon vaikuttavat turvallisuustekijät, skaalautuvuuden tärkeys sekä yleiskuva mahdollisen lohkoketjuratkaisun tuomista kustannuksista. Lisäksi tutkielmassa esitetään päätöspuumalli, jolla voidaan perustella tarve lohkoketjun käytölle.

Asiasanat: lohkoketju, Bitcoin, Ethereum, turvallisuus, skaalautuvuus, implementointi, yksityisyys

ABSTRACT

Kivinen, Miikka
Blockchain Solutions and Challenges of Implementation
Jyväskylä: University of Jyväskylä, 2019, 29 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Seppänen, Ville

Blockchain is a distributed ledger that operates in P2P network. It stores digitally signed transactions into blocks that are validated and broadcasted to the network by nodes that operate in the blockchain. Blocks are linked to each other with cryptographically created hashes and they are added to the blockchain through consensus mechanism. Every node holds a copy of the blockchain so tampering the data is practically impossible. Due to blockchain's distributed nature and strong linking of the blocks, blockchain is an immutable and trusted ledger. In recent years, blockchain solutions have gained lot of attention from different entities. They have been proposed to replace traditional database systems in many industries, although the technology is still very young. Now, blockchain solutions face many issues concerning privacy, security and scalability, which hinders the further adoption. Additionally, blockchain is not suitable for all its proposed use cases, since it considerably differs from traditional databases. This study aims to find out the factors that have an influence on implementing a blockchain solution to enterprise systems. The paper discusses some security and privacy issues, importance of scalability and general expected cost structure of implementing a blockchain solution. Additionally, a decision tree model on justification of implementing a blockchain solution is proposed.

Keywords: blockchain, Bitcoin, Ethereum, security, scalability, implementation, privacy

KUVIOT

SISÄLLYS

1 JOHDANTO

Lohkoketju on hajautettu P2P-verkossa toimiva tietokanta, joka kirjaa käyttäjien digitaalisesti allekirjoittamia transaktioita lohkoihin ketjua ylläpitävien verkon solmujen avulla. Lohkoketjut poikkeavat perinteisistä tietokannoista siinä, että niiden ylläpitämiseen ei tarvita tietokantaa ylläpitävää yksittäistä tahoa. Lohkoketjuissa käytetään kryptografiaan perustuvia salausmenetelmiä, joilla pyritään turvaamaan ketjussa tapahtuvat transaktiot sekä säilyttämään ketjun datan oikeellisuus. Ketjun solmut tallentavat itselleen kopion lohkoketjusta, jolloin ne pystyvät tiivisteiden avulla vahvistamaan transaktioiden oikeellisuuden ja takaamaan, että ketjun dataa ei pystytä jälkikäteen muokkaamaan. Näin ollen tarjotaan luotettava ja muuttumaton tilikirja kahden osapuolen välisistä transaktioista. (Zhang, Xue & Liu, 2019)

Nuoresta iästään huolimatta lohkoketjut ovat herättäneet kiinnostusta niin yrityksissä, kuluttajissa kuin myös valtiollisella tasolla. On ennustettu, että lohkoketjuihin perustuvien yritysapplikaatioiden arvo tulee olemaan 19,9 miljardia dollaria vuoteen 2025 mennessä. Vuonna 2016 lohkoketjuihin perustuvien yritysapplikaatioiden arvo oli 2,5 miljardia ja näin ollen alalle ennustetaan 26,2 prosentin vuosittaista kasvua (Zhang ym., 2019). Koska lohkoketjuratkaisuille on povattu käyttöä esimerkiksi jakeluketjussa, IoT-järjestelmissä, terveydenhuollossa ja finanssialalla (Mohanta, Panda & Jena, 2018), on syytä tarkastella niiden ominaisuuksia ja soveltuvuutta eri toimialoille. Tässä tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin.

- Mitkä tekijät vaikuttavat lohkoketjuteknologioiden käyttöönottoon yrityksissä?
- Milloin lohkoketjuun pohjautuvan ratkaisun käyttö on perusteltua?

Tutkimus suoritettiin systemaattisena kirjallisuuskatsauksena tarkastelemalla hakuehtojen perusteella löytynyttä lähdemateriaalia ja kokoamalla sen perusteella käsitys lohkoketjuratkaisua koskevista haasteista. Lisäksi tutkielmassa pyrittiin muodostamaan malli, jonka avulla voidaan selvittää, onko lohkoketjuratkaisun valinnalle perusteluja. Lähdemateriaalia haettiin tieteellisten julkaisujen osalta IEEE Xploren, AIS eLibraryn ja ACM Digital Libraryn tieto-

kannoista. Hakusanoina käytettiin sanoja blockchain, implementation, security, critical, scalability, use case ja privacy. Haku suoritettiin lohkoketjuihin suuntautuvan lähdemateriaalin rajaamiseksi niin, että sana blockchain on jokaisessa haussa, jonka jälkeen käytettiin AND-operaattoria ja vaihtoehtoisesti muita hakusanoja. Tieteellisten julkaisujen lisäksi tutkielmassa käytettiin Bitcoinin alkuperäistä suunnitelmaa sekä yleisten tilastojen osalta lohkoketjuihin erikoistuneiden nettijulkaisuiden sekä statistiikkasivujen sisältöjä. Hakuprosessin jälkeen koottu lähdemateriaali arvioitiin ja hyväksyttiin lopulliseksi lähdemateriaaliksi, mikäli niiden sisältö oli tarpeeksi kattava ja kieliasu hyvä.

Tutkielman toisessa luvussa käydään yleisesti läpi lohkoketjujen toiminta ja niiden historia sekä lohkoketjuihin liittyvä keskeinen terminologia. Luvussa tarkastellaan myös älysopimusten toimintaa Ethereum-alustalla toimivien älysopimusten pohjalta. Lopuksi ensimmäisessä luvussa vertaillaan perinteisien tietokantojen ja lohkoketjuratkaisujen eroja. Kolmannessa luvussa käsitellään lohkoketjuihin yleisesti liittyviä ongelmia ja niiden vaikutusta yritysjärjestelmiin implementointiin. Ensiksi käydään läpi turvallisuuteen vaikuttavat lohkoketjujen fragmentaatio ja ongelmat anonymiteetissa. Seuraavaksi tarkastellaan lohkoketjuja yleisesti vaivaavaa skaalautuvuuden puutetta. Lopuksi muodostetaan käsitys lohkoketjuratkaisun mukana tuomista kustannuksista vertaamalla sitä perinteisen tietojärjestelmän käyttöönottoon. Neljännessä luvussa pohditaan aikaisemmin tutkimuksessa esiintyviä havaintoja ja tarkastellaan tutkielmassa esitellyn kolmijakoisen mallin pohjalta, mitkä ratkaisut ovat yritysten kannalta järkevimpiä. Lopuksi esitellään aikaisempaan tutkimukseen perustuva päätöspuumalli, joka ottaa huomioon tutkielmassa esiintyneet päätelmät. Viimeisessä luvussa tutkielman johtopäätökset kootaan yhteen. Johtopäätösten mukaan lohkoketjuratkaisujen käyttöönotossa on tällä hetkellä paljon haasteita ja lohkoketjujen luonteen takia niiden käyttö ei sovellu kaikkialle, mikä rajaa mielekkäitä käyttötapauksia paljon. Yhteenvedossa arvioidaan myös käytettyä lähdemateriaalia ja esitetään tutkielman aikana esiin nousseita jatkotutkimusaiheita.

2 Lohkoketjuteknologiat

Lohkoketju on hajautettu tietokanta ja tilikirja, joka kirjaa käyttäjien transaktioita hierarkkisesti lohkoihin ilman keskitettyä lohkoketjua hallitsevaa entiteettiä. Transaktiot toimitetaan lohkoketjua ylläpitävän verkon solmuille, jossa ne hyväksytään ja lisätään lohkoon. Uusia lohkoja ei voida lisätä ilman solmujen ylläpitämää konsensusta. Lohko suojataan kryptografiaan perustuvalla suojauksella ja sille annetaan lohkon sisältöön perustuva tiiviste, joka osoittaa lohkoista koostuvan ketjun osaan, johon data on varastoitu. Solmut ylläpitävät datan oikeellisuutta pitämällä tallessa kopiota osasta tai koko ketjusta. Näin ollen ketjuun lisättyjä transaktioita ei voida jälkikäteen muuttaa ja teoriassa tarjotaan luotettava ja muuttumaton tilikirja kahden osapuolen välisistä transaktioista. (Zhang ym., 2019)

Ensimmäinen dokumentoitu suunnitelma lohkoketjusovelluksesta on peräisin vuodelta 2008 ja ensimmäinen käytännön implementointi on vuodelta 2009 kun Bitcoinin liikkeellelasku aloitettiin. Bitcoin on tunnustettu laajalti ensimmäiseksi lohkoketjuksi, joka tukee yksinkertaisia älysopimuksia (Wang, Ouyang, Yuan, Ni, Han & Wang, 2019). Vuonna 2015 liikkeelle laskettiin julkinen lohkoketjualusta, Ethereum, joka mahdollisti monimutkaisempien ja kustomoitujen älysopimusten ohjelmoinnin (Wang ym., 2019). Vuoden 2015 jälkeen lohkoketjusovellusten määrä on vain kasvanut ja esimerkiksi Ethereum-alustalla toimivia ERC-20-rahakkeita on luotu yli 200 000 kappaletta (Ledger, 2019).

2.1 Lohkoketjun toiminta

Lohkoketju toimii hajautettuna ja suojattuna tietokantana käyttäjien transaktioille. Bitcoin on tällä hetkellä markkinaosuudeltaan suurin lohkoketjusovellus (CoinMarketCap, 2019) ja se on toiminut mallina monien muiden lohkoketjusovellusten kehityksessä (Zhang ym., 2019). Näin ollen tässä luvussa tarkastellaan lohkoketjun toimintaa Bitcoinin näkökulmasta.

Kahden osapuolen välinen transaktio tapahtuu Bitcoin-verkossa luomalla uusi transaktio toisen osapuolen toimesta. Kyseinen transaktio lähetetään verkon jokaiselle solmulle, joissa transaktiot kootaan lohkoksi. Lohkon sisältämien transaktioiden oikeellisuus varmistetaan ja se lähetetään julkiseen Bitcoin-verkkoon käyttäen konsensusprotokollaa. Bitcoin käyttää konsensusprotokollana proof-of-work-menetelmää lohkon oikeellisuuden tarkistamiseen (Bitcoin, 2019), ja kun lohkon sisältämät transaktiot on hyväksytty koko verkossa, lohko lisätään ketjuun. Kahden osapuolen välinen transaktio on aito vasta, kun ketjuun lisääminen on tapahtunut. Bitcoin käyttää lohkojen oikeellisuuden ja muuttumattomuuden takaamiseen tiivisteketjua, Merkle-puuta, digitaalista allekirjoitusta sekä konsensusmenetelmiä, joilla ehkäistään esimerkiksi valuutan kaksoiskuluttaminen. Lisäksi turvallisuusmenetelmillä taataan, että lohkoketjua ei voida muuttaa ilman kohtuutonta määrää työtä. (Zhang ym., 2019)

Bitcoin-verkossa lohkot linkitetään toisiinsa käyttämällä tiivisteosoittimia. Tiivisteosoitin on lohkon sisältämästä datasta kryptologian menetelmiä käyttäen luotu tiiviste, joka osoittaa dataan. Tiivisteen avulla voidaan tarkistaa, onko dataa muutettu jälkikäteen, sillä muutetusta datasta luotu tiiviste eroaa alkuperäisestä tiivisteestä. Tiivisteosoitin sisältää myös informaation edeltävän lohkon datan sijainnista, jolloin lohkoketju saadaan organisoitua ja oikeellisuus varmistettua. (Zhang ym., 2019)

Merkle-puu on datarakenne, jota käytetään lohkojen oikeellisuuden tarkistamiseen. Kahden alemman tason lohkon tiivisteet linkitetään ylemmän tason vanhempilohkoon ja prosessia toistetaan puun juurisolmuun asti. Datan oikeellisuus voidaan tarkastaa Merkle-puussa vertaamalla lehtisolmun tiivistettä juuritiivisteeseen ja näin saadaan selville mahdolliset muutokset lohkojen dataan. Lisäksi kyseinen datarakenne on kustannustehokas, sillä tiivisteiden ansiosta tarkistus voidaan suorittaa logaritmisessa ajassa. (Zhang ym., 2019)

Transaktioiden suorittamiseen Bitcoin-verkossa käytetään digitaalista allekirjoitusta, joka koostuu kolmesta käytettävästä algoritmista. Ensimmäinen näistä on avaimia generoiva algoritmi, joka luo käyttäjälle julkisen ja yksityisen avaimen. Yksityisellä avaimella allekirjoitetaan transaktiot ja julkisella avaimella varmistetaan, että transaktiot on suoritettu käyttämällä vastaavaa yksityistä avainta. Toisella, allekirjoitusalgoritmilla, luodaan yksityistä avainta vastaavaan transaktioon allekirjoitus. Kolmas algoritmi vahvistaa transaktion allekirjoituksen käyttämällä syötteenä saatuja julkista avainta, allekirjoitusta sekä transaktion sisältämää viestiä. (Zhang ym., 2019)

2.2 Älysopimukset

Älysopimukset ovat protokollia, joilla helpotetaan, suoritetaan ja vahvistetaan lohkoketjussa tapahtuvia useiden tahojen välisiä sopimuksia. Sopimus sisältää tiedot sen toiminnasta, kuten käynnistysehdoista ja sitä seuraavista toimenpiteistä. Älysopimuksen osalliset hyväksyvät sopimuksen toiminnan ja se lähetetään lohkoketjuun, jossa solmut vahvistavat sen ja lisäävät lohkoon. Käyttäjät

voivat suorittaa sopimuksen yleensä tekemällä transaktion sopimukseen, jossa oleva koodi suoritetaan, mikäli käynnistysehdot täyttyvät. (Wang ym., 2019). Älysopimukset mahdollistavat siis koodin suorittamisen lohkoketjussa, jolloin alustalle voidaan rakentaa applikaatioita.

Wangin ym., (2019) mukaan Ethereum on tällä hetkellä laajimmin käytetty alusta älysopimusten luomiseen ja suorittamiseen, joten tarkastellaan lyhyesti älysopimuksen suorittamista Ethereum-lohkoketjussa. Älysopimukset toimivat Ethereum-alustalla kahdenlaisten tilien pohjalta. Ensimmäinen tilityyppi on käyttäjätili, joka toimii lohkoketjun loppukäyttäjän hallinnoimana. Toinen tilityyppi on sopimustili, jonka hallinta tapahtuu älysopimuksen sisältämän koodin avulla. Käyttäjä voi aktivoida sopimuksen hallinnoimansa tilin avulla lähettämällä transaktiona sopimuksen tarvitseman tietosisällön sekä Etheriä, jota käytetään lohkoketjussa maksuvälineenä. Mikäli sopimuksen käynnistysehdot täyttyvät, sopimuksen koodi suoritetaan ja transaktio toimitetaan lohkoketjuun, jossa ketjun solmut louhivat sen. Lohkoketjun väärinkäytön, kuten verkon ylikuormittamisen, ehkäisemiseksi jokainen toiminto lohkoketjussa vaatii pienen maksun, jota kutsutaan Ethereum-verkossa kaasuksi. Näitä toimintoja ovat muun muassa operaatioiden suorittaminen Ethereumin virtuaalikoneessa (EVM) ja sopimusten luonti sekä niiden toteuttaminen.

2.3 Erot perinteisiin tietokantoihin

Lohkoketjut toimivat hajautettuina tietokantoina, jotka tallentavat käyttäjien transaktiota peräkkäisiin lohkoihin ketjun asettamien sääntöjen puitteissa. Näin ollen on sopivaa verrata lohkoketjun tuomia ominaisuuksia perinteisten tietokantojen ominaisuuksiin.

Perinteisissä tietokannoissa on usein pääkäyttäjä tai muu vastaava rooli, joka pystyy tekemään muutoksia tietokantaan. Mikäli tietokantaan tarvitaan luottamukseton tila käyttäjien välille, tarvitaan näin ollen kolmas osapuoli, johon muut osapuolet luottavat. Lohkoketjussa suoritettavien konsensusprotokollien vuoksi lohkoketjuissa on mahdollisuus saavuttaa osapuolten välinen konsensus ketjun tilasta ilman kolmatta luotettua osapuolta (Chowdhury, Colman, Kabir, Han & Sarda, 2018). Lohkoketjussa jokaisella verkon osallisella on samat oikeudet tarkastella ketjussa tapahtuneita transaktioita ja niiden dataa, ellei niitä ole erikseen rajoitettu esimerkiksi datan salausmekanismien tai yksityisessä lohkoketjussa roolien avulla. Näin ollen esimerkiksi kahden jakeluketjun tietokantaa käyttävän osapuolen ei tarvitse luottamuksen puuttuessa etsiä kolmatta osapuolta hallinnoimaan informaatiota, mikäli käytetään lohkoketjuun perustuvaa ratkaisua.

Kun saavutetaan hajautettu konsensus ketjun tilasta suuremmalla määrällä solmuja, voidaan myös varmistaa ketjussa olevan informaation muuttumattomuus, sillä jokainen ketjun solmu sisältää tiedon datasta. Dataa ei näin ollen voi jälkikäteen muuttaa yhden osapuolen toimesta ilman, että se huomataan muualla lohkoketjussa. Solmujen määrän vaikutusta tarkastellaan myöhemmin

tässä tutkielmassa. Kun monet lohkoketjun solmut pitävät sisällään tiedon ketjun datasta, saavutetaan myös datan yhteneväisyys. Mitä laajemmin lohkoketju on hajautettu, sitä vastustuskykyisempi se on esimerkiksi DoS-hyökkäyksiä vastaan, sillä vaikka hyökkääjä saisi ajettua alas osan verkon solmuista muut solmut voivat silti jatkaa ketjun ylläpitoa.

Datan alkuperä on vahvistettavissa lohkoketjusta, sillä datan varastointiprosessi toteutetaan transaktioilla. Koska jokainen transaktio täytyy vahvistaa lohkoketjujen käyttämällä digitaalisella allekirjoituksella, voidaan varmistua datan alkuperästä (Chowdhury ym., 2018). Lohkoketjuun tehdyn transaktion osapuolet ja data ovat tallennettuna lohkoon, eikä niitä voida ketjun hajautetun luonteen takia muuttaa jälkikäteen toisin kuin perinteisessä tietokannassa, jossa tarvittavat oikeudet omistava taho voi teoriassa muuttaa tietokannan dataa (Wessling, Ehmke, Hesenius & Gruhn, 2018). Lohkoketjut ja perinteiset tietokannat kohtaavat myös erilaisia turvallisuusriskejä. Siinä missä lohkoketjut ovat hajautetun luonteensa vuoksi jotakuinkin immuuneja DoS-hyökkäyksille, perinteiset tietokannat ovat tämän mallisille hyökkäyksille alttiimpia. Toisaalta perinteisissä tietokannoissa dataa voi muokata epärehellisessä tarkoituksessa vain, jos hyökkääjällä on tarvittavat oikeudet muokkauksiin, kun taas lohkoketjualustoilla on niiden demokraattisen luonteen takia mahdollista toteuttaa epärehellisiä transaktioita esimerkiksi hallitsemalla tarvittavan suurta osaa verkon laskentatehosta. Lohkoketjujen turvallisuuskysymyksiä käsitellään lisää seuraavassa luvussa.

3 HAASTEET KÄYTTÖÖNOTOSSA

Tässä luvussa tarkastellaan lohkoketjusovellusten käyttöönottoon liittyviä mahdollisia haasteita lohkoketjujen kolmijakoisen luokittelun pohjalta. Lohkoketjut voidaan jakaa ketjua hallitsevien ja käyttävien tahojen perusteella kolmeen eri luokkaan (Zhang ym., 2019). Ensimmäinen luokka on julkinen lohkoketju, joka on toiminnaltaan avoin kaikille. Julkisen lohkoketjun käyttäjät voivat suorittaa lukuoperaatioita, lähettää ja vastaanottaa transaktioita sekä osallistua halutessaan konsensusprosessiin luomalla laitteelleen lohkoketjua ylläpitävän solmun. Toinen luokka on konsortiolohkoketju, joka rajoittaa konsensusprosessiin osallistuvat tahot yleensä ennalta määrättyyn ryhmään. Lukuoperaatiot ovat kuitenkin avoimia jokaiselle verkon osalliselle. Kolmas luokka on yksityinen lohkoketju, jonka konsensusprosessia hallitsee yksittäinen taho. Lukuoperaatiot voivat olla yksityisessä lohkoketjussa joko julkisia tai rajoitettuja tietylle ennalta määrätylle käyttäjäryhmälle. Yhteistä näille kaikille luokille on, että ne käyttävät P2P-verkkoja, joissa tehtävät, konsensusprotokollalla vahvistettavat, transaktiot on allekirjoitettava digitaalisella allekirjoituksella sekä jokainen verkon solmu pitää itsellään kopiota lohkoketjusta. Tässä tutkielmassa lohkoketjuja on järkevää käsitellä tämän mallin pohjalta, sillä kolmijakoisen mallin eri luokat sisältävät ominaisuuksia ja käyttökohteita, joita on mielekästä tarkastella yrityssovellusten implementoinnin kannalta. Luvussa käsitellään ensiksi lohkoketjuihin liittyviä turvallisuusriskejä, jonka jälkeen siirrytään tarkastelemaan ongelmia skaalautuvuudessa. Lopuksi muodostetaan käsitys lohkoketjuratkaisun käyttöön liittyvistä kustannuksista.

3.1 Turvallisuus

Jotta lohkoketjusovelluksia voitaisiin implementoida mukaan yritysten toimintaan, on niiden toteutettava tietyt yleiset turvallisuuskriteerit sekä käyttökohteen mukaan muita ominaisuuksia. Lohkoketjujen periaatteen mukaisesti ketjun tulisi säilyttää oikeellinen tieto tapahtuneista transaktioista eikä syötetyn

datan tulisi olla muokattavissa epärehellisin keinoin. Koska digitaalinen data on melko helposti replikoitavissa, kohdistuu lohkoketjuihin uhkia, kuten valuutan kaksoiskuluttaminen ja konsensushyökkäykset. Lisäksi lohkoketjujen määrän lisääntyminen kasvattaa onnistuneiden hyökkäyksien todennäköisyyttä fragmentaatio-ongelman muodossa. Käyttökohteen luonteen mukaan lohkoketjulla on myös oltava mahdollisuus käyttäjän anonymiteettiin käyttäjän todellisen henkilöllisyyden ja hänen tekemien transaktioiden osalta. Tässä alaluvussa tarkastellaan lohkoketjujen turvallisuusriskejä, verrataan niitä aiemmin esitettyyn kolmijakoiseen malliin ja pohditaan, mitkä ratkaisut ovat järkevimpiä yritystoiminnan kannalta.

3.1.1 Fragmentaatio-ongelma

Bitcoinin alkuperäisessä suunnitelmassa on laskettu lohkoketjuun hyökkäävän tahon mahdollisuutta luoda vaihtoehtoinen ketju oikean rinnalle. Hyökkäyksen onnistuessakaan hyökkääjä ei pystyisi viemään arvoa osapuolelta, jonka kanssa hän ei ole tehnyt transaktioita, eikä luomaan ketjuun uutta arvoa. Sen sijaan hyökkääjä pystyisi onnistuessaan peruuttamaan tekemänsä transaktion ja näin ollen saamaan kulutetun balanssinsa takaisin. (Bitcoin, 2019)

Todennäköisyys hyökkääjän onnistumiselle on laskettu seuraavalla kaavalla, jossa p on todennäköisyys sille, että rehellinen solmu löytää seuraavan lohkon, q on todennäköisyys hyökkääjän onnistumiselle lohkon löytämisessä ja q_z on todennäköisyys, että hyökkääjä löytää uuden lohkon z lohkoa jäljessä.

$$q_z = \begin{cases} 1, & jos\ p \leq q, \\ (q/p)^z, & jos\ q < p \end{cases}$$

Hyökkääjä onnistuu siis muuttamaan ketjun itselleen edulliseksi sitä todennäköisemmin, mitä pienemmän määrän lohkoja hän on jäljessä, ja mitä suuremman määrän solmuja hän hallitsee olettaen, että jokaisen solmun todennäköisyys lohkon löytämiselle on suunnilleen sama.

Fragmentaatio-ongelma syntyy lohkoketjujen lisääntyessä, jolloin rehellisten solmujen määrä jakautuu suuremmalle määrälle ketjuja (Worley & Skjellum, 2018). Tällöin hyökkääjän on teoriassa helpompi saavuttaa tarpeeksi suuri määrä solmuja muutosten tekemiseen. Jos oletetaan, että lohkoketjuja on m määrä ja rehelliset solmut ovat jakautuneet tasaisesti niiden välille, saadaan kaavio, jossa hyökkääjän todennäköisyydet onnistua nousevat huomattavasti lohkoketjujen lisääntyessä.

$$q_z = \begin{cases} 1, & jos\ \frac{p}{m} \leq q, \\ (q/\frac{p}{m})^z, & jos\ q < \frac{p}{m} \end{cases}$$

Todellisuudessa lohkoketjujen solmut eivät kuitenkaan ole jakautuneet tasaisesti, vaan suurimmat lohkoketjusovellukset sisältävät huomattavasti enemmän

solmuja kuin uudemmat ja pienemmät sovellukset. Esimerkiksi Bitcoinilla on tällä hetkellä yli 9000 solmua (Bitnodes, 2019) ja Etherumilla yli 6500 (Etherscan, 2019), kun taas esimerkiksi markkinaosuudeltaan huomattavasti pienemmällä NEM:llä solmuja on vain 480 (Nemnodes, 2019). Näin ollen suurimmat lohkoketjualustat ovat fragmentaatio-ongelman kannalta turvallisimpia vaihtoehtoja. Turvallisuusongelmien lisäksi fragmentaatio kuormittaa sekä kehittäjien että ympäristön resursseja, sillä samasta sisällöllisestä arkkitehtuurista tehdään erilasten samaa funktiota toteuttavien sovellusten muodossa uusia versioita (Worley & Skjellum, 2018).

Fragmentaatio-ongelmaa lohkoketjujen kolmijakoisen luokittelun pohjalta tarkasteltaessa voidaan päätellä, että julkiset lohkoketjut ovat turvallisimpia, mikäli otetaan huomioon vain solmujen määrä. Julkisilla lohkoketjuilla on yleensä suurin määrä solmuja, jolloin niihin hyökkääminen on vaikeinta. Toisaalta julkisen lohkoketjun konsensusprosessiin voi osallistua kuka tahansa, jolloin hyökkääjän on helpompi saada hyökkäykseen tarvittavia solmuja haltuunsa. Uhka on suurempi, mitä vähemmän verkossa on laskentatehoa. Kahdessa jälkimmäisessä luokassa verkon solmujen määrä, ja sitä kautta lohkoketjun hajautus, on yleensä pienempi. Konsortiolohkoketjussa solmut on hajautettu ennalta määritellylle ryhmälle, jolloin hyökkääjän tulisi saada näistä solmuista tarvittava määrä haltuunsa hyökkäyksen onnistumiseksi. Mikäli ketjun solmuja hallinnoivat tahot ovat ”rehellisiä” eikä hyökkääjä saa manipuloitua solmuja omaan käyttönsä, voi konsortiolohkoketju olla julkista ketjua turvallisempi vaihtoehto. Yksityiset lohkoketjut ovat vain yhden tahon, esimerkiksi yhden tai useamman organisaation, hallitsemia lohkoketjuja, joissa konsensusprosessia ei ole hajautettu ulkopuolisille tahoille. Lisäksi ulkopuolisilla tai rajoitetulla käyttäjäryhmällä on valtuus suorittaa vain operaatioita vain oikeuksiensa mukaan, jolloin organisaation ulkopuolisen hyökkääjän on käytännössä mahdoton suorittaa hyökkäystä. Davenportin, Shettyn ja Liangin (2018) mukaan näiden ominaisuuksien avulla voidaan pitkälti välttyä laskentatehon väärinkäytöstä johtuvilta hyökkäyksiltä, mutta toisaalta samalla uhrataan lohkoketjun hajautettua perusperiaatetta ja menetetään luottamukseton tila ketjua hallinnoivan tahon ollessa keskitetty lohkoketjua hallitseva entiteetti.

3.1.2 Anonymiteetti

Koska lohkoketjun tyypistä riippuen käyttäjillä on oikeus tarkastella ketjussa tapahtuvia transaktioita, on käyttökohteen mukaan turvattava käyttäjän anonymiteetti. Tämä tarkoittaa sitä, että transaktiot eivät ole yhdistettävissä tiettyyn käyttäjään ja käyttäjän todellinen identiteetti ei ole julkisesti tarkasteltavissa. Lisäksi käyttökohteen mukaan transaktion sisältämä data tulisi voida salata, jotta luottamuksellinen data ei olisi kaikkien saatavilla ja transaktioita ei voi yhdistää tiettyyn käyttäjään. Anonymiteetti ja datan yksityisyys korostuu erityisesti ketjuissa, joissa liikkuu luottamuksellista tietoa sekä Bitcoinin kaltaisissa julkisissa lohkoketjuissa, joiden tarkoitus on toimia julkisena valuuttajärjestelmänä.

Lohkoketjut käyttävät yleisesti kahta erilaista transaktiomallia, joista ensimmäinen on esimerkiksi Bitcoinin käyttämä UTXO-malli (Zhang ym., 2019). Kyseisessä mallissa käyttäjän ”lompakko” pitää kirjaa osoitteista, joissa on käyttäjän hallinnoimaa käyttämätöntä valuuttaa. Jokaisen transaktion syötteenä lähetetään koko osoitteen sisältämä balanssi, josta vähennetään lähetettävä määrä. Tulosteena vastaanottaja saa lähetettävän määrän valuuttaa hallinnoimaansa osoitteeseen ja jäljelle jäänyt balanssi palautetaan lähettävälle uuteen osoitteeseen. Näin ollen osoitteet on tarkoitettu UTXO-mallissa kertakäyttöiseksi ja käyttäjien balanssi muodostuu käyttäjille palautetuista käyttämättömän valuutan tulosteista. Anonymiteetin kannalta UTXO-malli on seuraavaksi käsiteltävää tilimallia parempi, sillä käyttäjä voi omistaa saman lompakon alla monta valuutan instanssia yhdistämättä niitä yhdeksi julkiseksi balanssiksi. Käyttäjä pystyy näin ollen suorittamaan transaktioita toiselle osapuolelle vain tietyistä hallinnoimistaan instansseista paljastamatta kaikkia hallinnoimia osoitteitaan ja näin saavutetaan näennäisesti vaikeampi käyttäjän todellisen balanssin selvitys. Kuitenkin, vaikka UTXO-mallia käyttävät lohkoketjut onnistuvat tarjoamaan käyttäjälle pseudonymiteetin lompakon generoidun osoitteen muodossa, ne eivät voi taata käyttäjän tekemien transaktioiden yksityisyyttä ilman transaktion sisällön salaamista tai transaktion maskeeraamista muilla keinoilla. Esimerkiksi Bitcoinin tapauksessa kaikki transaktiot kirjataan lohkoketjuun, jossa kuka tahansa voi tarkastella niitä ja kohdeosoitteista tehtävän tilastollisen analyysin perusteella selvittää käyttäjän pseudonymiteetin ja balanssin (Balaskas & Franqueira, 2018). Mahdollinen reaalimaailman taustatieto lisäämällä voidaan myös selvittää käyttäjän todellinen henkilöllisyys. Toinen transaktiomalli on esimerkiksi Etherumin käyttämä tilimalli, joka muistuttaa enemmän perinteistä pankkijärjestelmän mallia (Zhang ym., 2019). Käyttäjän tili pitää kirjaa kokonaisbalanssista ja tilin informaatio on tallennettu lohkoketjuun UTXO-mallin erillisten balanssitulosteiden sijaan, jolloin saavutetaan lohkoketjun nopeampi toiminta ja kevyempi datarakenne. Anonymiteetin kannalta tilimalli on kuitenkin UTXO-mallia heikompi, sillä vaikka tilimallinkin tarjotessa pseudonymiteetin, uusia osoitteita ei luoda jokaiselle transaktiolle erikseen. Kuten Bitcoinin tapauksessa, myös Ethereumin transaktiot ovat julkisia eikä näin ollen voida taata, ettei transaktioita voitaisi linkittää tiettyyn käyttäjään ja dataa tarkastella.

Zhangin ym. (2019) mukaan todellisen anonymiteetin voi saavuttaa lohkoketjussa vain pseudonymiteetin sekä transaktioiden linkittämättömyyden avulla. Lohkoketjuihin on mahdollista implementoida vaihtoehtoisia turvallisuusmenetelmiä, jotka joko salaavat transaktion sisällön tai sekoittavat transaktioita keskenään, jotta niiden linkittäminen tiettyyn käyttäjään vaikeutuisi. Transaktioiden todellisen tekijän salaamiseksi on kehitetty digitaalisen allekirjoituksen anonymisoivia tekniikoita, kuten ryhmäallekirjoitus (*group signature*) ja kehäallekirjoitus (*ring signature*). Ryhmäallekirjoituksessa kuka tahansa jäsen voi allekirjoittaa ryhmän kautta tapahtuva transaktion ja kuka tahansa ryhmän jäsen voi vahvistaa sen käyttämällä ryhmä julkista avainta saaden transaktion todellisen tekijän pseudonyymin sijaan vain vahvistuksen transaktion tekijän kuulumisesta ryhmään. Ryhmässä täytyy kuitenkin olla taho, joka hallitsee

ryhmää ja näin ollen ryhmää hallinnoivalla taholla on mahdollisuus nähdä transaktion alkuperäinen allekirjoittaja. Kehäallekirjoitus taas perustuu algoritmiin, jossa ryhmäallekirjoituksen tavoin, kuka tahansa voi allekirjoittaa transaktion. Erona ryhmäallekirjoitukseen on, että kehäallekirjoituksessa ei tarvita yksittäistä tahoa hallitsemaan kehässä tapahtuvia transaktioita, jolloin alkuperäistä lähettäjää ei voida tunnistaa kuin arvaamalla. Allekirjoituksen anonymisoinnin lisäksi anonymiteetin takaamiseksi on olemassa erilaisia enkryptaustekniikoita, joilla salataan transaktion sisältämä data. (Zhang ym., 2019) Transaktion sisältämän datan salaaminen on oleellista joidenkin yrityssovellusten kannalta, sillä lohkoketjujen sisältämän datan julkisuus on ollut lohkoketjusovellusten käyttöönoton este monille mahdollisille käyttäjille (Sadhya & Sadhya, 2018). Julkisten lohkoketjujen transaktioiden sisällön salaaminen on kuitenkin ongelmallista, sillä vaikka data salattaisi ennen sen toimittamista ketjuun, verkon transaktioita voidaan tarkastella ja oppia tietynlaisten transaktioiden ominaispiirteet (Li, Sforzin, Fedorov & Karame, 2017). Tämä mahdollistaa transaktioiden linkittämisen tiettyyn käyttäjään tai ryhmään.

Mikäli lohkoketjujen anonymiteettiä tarkastellaan lohkoketjujen kolmijakoisen mallin pohjalta, julkiset lohkoketjut ovat useimmiten vähiten houkutteleva vaihtoehto yritysten kannalta. Suurimpien alustojen transaktiot ovat julkisia ja niiden sisältämä data on oletusarvoisesti kaikkien saatavilla, sillä ne eivät ole implementoineet pääketjuihinsa dataa tai transaktioita salaavia ominaisuuksia. Konsortiolohkoketjuissa on mahdollisuus samoille puutteille kuin julkisissa vastaavissa, mutta jotkin transaktioita suojaavat menetelmät on helpompi toteuttaa kuin julkisissa ketjuissa. Esimerkiksi ryhmäallekirjoitus soveltuu hyvin konsortiolohkoketjuille, sillä allekirjoitusmenetelmän tarvitsemat ryhmien haltijat on helppo asettaa ennalta määrättyjen konsensusosapuolien joukosta. Käyttökohteen mukaan sekä julkisissa- että konsortiolohkoketjuissa tulisi olla implementoituna myös datan salaavia metodeja, jotta ne olisivat luottamuksellisen tiedon välittämiseen käyttökelpoisia. Yksityisessä lohkoketjussa anonymiteetin takaus ketjun käyttäjälle ei ole yhtä suuressa roolissa kuin muissa tyypeissä, sillä ketjun yksityisyys itsessään takaa salauksen ulkopuolisilta tahoilta. Yksityiset lohkoketjut ovat usein yhden tai useamman yrityksen sisäisiä, ja niissä on ennalta määrätyt roolit ja oikeudet, jolloin ketjussa on tiedettävä transaktion tekijän rooli. Tällaisissa tapauksissa käyttäjien vahva anonymisointi ja transaktioiden salaus estävät käyttäjän tunnistamisen tehden ketjun epäkäytännölliseksi ja jopa käyttökelvottomaksi.

3.2 Skaalautuvuus

Lohkoketjujen skaalautuvuudesta on muodostunut käyttäjämäärien ja ketjujen koon takia ongelma lohkoketjujen laajemmassa käyttöönotossa (Worley & Skjellum, 2018). Koska lohkoketjun toiminta vaatii, että verkon jokainen solmu vahvistaa transaktion ja näin ollen säilyttää koko kopion lohkoketjusta, on skaalautuvuudesta tullut varsinkin suuremmilla käyttäjämäärillä yksi lohkoket-

jusovellusten suurimmista haasteista. Verkon solmut ovat siis tällä hetkellä ongelma lohkoketjujen suorituskyvyssä. Esimerkiksi Bitcoin-transaktion vahvistamiseen voi mennä aikaa kymmenestä minuutista ylöspäin sen mukaan onko verkossa muuta kuormittavaa aktiviteettia, kuten uudelleenhaaroittamista. Bitcoin pystyy käsittelemään seitsemän transaktiota sekunnissa. Sitä vasten perinteiset pankkijärjestelmien tietokannat, kuten Visan ja Mastercardin järjestelmät pystyvät hallitsemaan sekunnissa tuhansia transaktioita (Chowdhury ym., 2018). Lisäksi Gervaisin, Karamen, Wüstin, Glykantzisin, Ritzdorfin ja Capkunin (2016) tutkimustulokset osoittavat, että proof-of-work-menetelmällä toimiva lohkoketju pystyy käsittelemään vain 60 transaktiota sekunnissa ilman että ketjun turvallisuudesta tingitään. Tässä luvussa tarkastellaan lohkoketjujen skaalautuvuusongelman ratkaisuja sekä skaalautuvuuden merkitystä yritysten näkökulmasta käyttäen apuna aiemmin esiteltyä kolmijakoista mallia.

Vastauksena verkon solmujen luomaan pullonkaulaan on esitetty ratkaisuksi esimerkiksi Bitcoinin implementoimaa Lightning-protokollaa, jossa kaksi osapuolta luo pääketjun ulkopuolisen maksukanavan (Chauhan, Malviya, Verma & Mor, 2018). Käyttäjät lähettävät kahdenvälisiin transaktioihin suunnitellun määrän valuuttaa maksukanavan osoitteeseen, jossa se lukitaan pois pääketjusta ennalta määritetyksi ajaksi. Tämän jälkeen käyttäjät voivat suorittaa maksukanavassa tavallisesta osoitteestaan transaktioita, joihin vaaditaan kummankin osapuolen allekirjoitus. Maksukanava sulkeutuu ja osapuolten sen hetkiset balanssit palautetaan pääketjuun joko, kun ennalta määrätty aika umpeutuu ja suunnitellut transaktiot on tehty, tai toisen osapuolen vetäytyessä maksukanavasta, jolloin vetäytyneen osapuolen lähettämän balanssin palautukselle asetetaan tuhannen lohkon mittainen viive. Pääketjuun palautuu siis vain kaksi transaktiota ja näin ollen lohkoketju ei rasitu maksukanavan sisällä tehtävistä transaktioista. Maksukanavaa voi myös laajentaa rajoittamattomalle määrälle osapuolia, mikäli usean osapuolten maksukanavat linkittyvät mitä tahansa reittiä pitkin toisiinsa. Chauhanin ym. (2018) mukaan Lightning-protokollassa on kuitenkin ongelmia, kuten sen toimintaperiaate, joka rikkoo perinteisen lohkoketjun toimintaideologiaa vahvistamalla maksukanavissa tapahtuvat transaktiot ketjun ulkopuolella. Protokolla on osittain epäkäytännöllinen, sillä maksukanavan avaaminen ja balanssien palautus vaatii transaktion pääketjussa, joka vie saman ajan ja maksun kuin muut pääketjussa tapahtuvat transaktiot. Tämän lisäksi kanavan avaaminen vaatii osapuolet sitomaan balanssiaan maksukanavaan ennalta määritetyksi ajaksi sekä toisaalta sulkemaan kanavan ajan päättyessä, vaikka transaktioita olisi vielä jäljellä.

Toinen skaalautuvuusongelmiin esitetty ratkaisu on Ethereumin kehittäjien esittelemä lohkoketjun pirstalointi (*sharding*) (Chauhan ym., 2018). Pirstaloinnin tarkoituksena on jakaa pääketjun rasitusta ”pirstaleille”, jotka sisältävät oman transaktiohistoriansa ja tilansa. Solmujen työtä jaetaan niin, että vain tietyt verkon solmut käsittelevät tiettyjä pirstaleita, joiden sisältö lisätään myöhemmin pääketjuun. Transaktio kahden pirstaleen välillä tapahtuu lähettämällä transaktio pirstaleelle, joka vähentää lähetetyn määrän käyttäjän balanssista ja luo Merkle-juureen tallennettavan maksutositteen. Tosite lähetetään toiselle

pirstaleelle, joka lisää balanssin vastaanottajan tilille ja merkitsee maksutositteen käytetyksi. Yksinkertaistettuna pirstalointi tarkoittaa siis lohkoketjun jakamista moneksi pienemmäksi ketjuksi, jotka noudattavat pääketjun konsensusprotokollaa ja muita ominaisuuksia. Pirstaloinnin ongelmana on kuitenkin lohkoketjun jakamisesta johtuva transaktioita vahvistavien solmujen pienempi määrä, joka luo ketjuun turvallisuusriskin (Chauhan ym., 2018). Mahdollisen hyökkääjän on helpompi saada haltuunsa tarvittava määrä yhden pirstaleen solmuja kuin pääketjussa, ja tehdä itselleen edullisia transaktioita.

Koska skaalautuvuudesta tulee ongelma ketjun koon sekä käyttäjämäärien kasvaessa, on se otettava huomioon myös suunniteltaessa lohkoketjussa toimivia yrityssovelluksia. Julkisissa lohkoketjuissa käyttäjämäärät ovat suurimpia, jolloin myös pääketjua rasittavia transaktioita tapahtuu eniten. Lisäksi julkisissa ketjuissa transaktiot vahvistavia verkon solmuja on eniten, jolloin jokaisen solmun vahvistaessa uudet transaktiot konsensuksen saavuttaminen, ja näin ollen uusien lohkojen lisääminen ketjuun, hidastuu. Suuri määrä transaktioita myös kasvattaa ketjun koko nopeasti, jolloin konsensuksen saavuttaminen hidastuu entisestään. Tästä päätellen julkiset lohkoketjut eivät ole yrityssovellusten kannalta houkuttavia varsinkaan, jos alustalla ei käytetä mitään toimivaa ja tehokasta skaalausratkaisua. Konsortiolohkoketjuissa voi ketjun luonteen mukaan olla suuri määrä käyttäjiä, mutta solmuja on yleensä vähemmän, sillä ne on jaettu ennalta määritellylle joukolle. Näin ollen konsensuksen saavuttamiseen ei tarvita yhtä monen verkon solmun hyväksyntää kuin julkisessa lohkoketjussa. Ongelmana myös konsortiolohkoketjussa on ketjun koon kasvaminen ajan myötä. Koska konsensusprotokollat vaativat käytännössä koko ketjun historian transaktioiden vahvistamiseen, kasvava ketjun koko vaikuttaa toimintaan jatkuvasti ja näin ollen myös konsortiolohkoketjujen tapauksissa toimiva skaalausratkaisu on tarpeen, mikäli siihen aiotaan rakentaa pitkäikäinen sovellus. Yksityiset lohkoketjut noudattavat samaa kaavaa kuin julkiset- sekä konsortiolohkoketjut. Vaikka yksityisissä lohkoketjuissa on yleisesti vähiten verkon solmuja, jonka takia konsensuksen saavuttaminen ja ketjun toiminta on teoreettisesti nopeinta, vaativat nekin hyvän skaalautuvuuden pitkäikäisyyden takaamiseksi. Voidaan siis yleisesti sanoa, että lohkoketjun toimivuuden kannalta siihen on implementoitava jonkinnäköinen skaalausmenetelmä, jotta ketjun pohjalla toimivat sovellukset ovat käyttökelpoisia pidemmällä aikajaksolla.

3.3 Investoinnit

Lohkoketjuun pohjautuvan järjestelmän käyttöönotto vaatii joko oman ratkaisun kehittämistä tai tuotteen ostamista ulkoiselta palveluntarjoajalta. Yrityskäyttöisten lohkoketjusovellusten kustannusrakenteesta ei tutkielman kirjoitushetkellä löydy kattavaa tutkimustietoa, joten tässä luvussa peilataan lohkoketjun pohjalla toimivan järjestelmän käyttöönottoa perinteisen tietojärjestelmän käyttöönottoon. Lisäksi tarkastelussa otetaan huomioon muut erityisesti lohkoketjuissa kuluja aiheuttavat tekijät, kuten suuri energiankulutus. Lopuksi mah-

dollisia kustannuksia tarkastellaan aiemmin esitetyn kolmijakoisen mallin pohjalta.

Nikitovićin ja Mahmutovićin (2019) mukaan uuden järjestelmän käyttöönoton kustannukset voidaan jakaa neljään osaan. Ensimmäinen niistä on ohjelmistolisenssit, jotka voivat heidän mukaansa viedä 30-40 prosenttia koko prosessin kustannuksista. Lohkoketjujen osalta esimerkiksi IBM tarjoaa yrityksille omia lohkoketjuratkaisujaan, jotka on hinnoiteltu joko IBM:n SaaS-palvelun tuntikäytön perusteella tai muuhun järjestelmään integroitaessa erikseen sovittavalla hinnalla. IBM:n sivuilla on laskettu verkon solmut, klusterin ja fyysisen tietovaraston sisältävän esimerkkipaketin hinnaksi 1,90 dollaria tunnilta, joka aiheuttaa ympärivuorokautisessa käytössä yritykselle kustannuksia yli 1400 dollaria kuukaudessa (IBM, 2019). Lisäksi kustannukset voivat vaihdella verkon laajuuden ja verkossa tapahtuvien transaktioiden sekä niiden sisältämän datan perusteella. Toinen kustannuksia aiheuttava osa on järjestelmän ylläpito (Nikitović & Mahmutović, 2019). Lohkoketjuratkaisua tarjoavien yritysten SaaS-palveluja käytettäessä ylläpidon kustannukset pienenevät, sillä niitä tarjoava yritys hoitaa yleensä itse järjestelmässä tapahtuvat päivitykset ja toiminnan monitoroinnin. Ylläpidon suhteen kustannuksia lopputuotteen käyttäjälle aiheutuu SaaS-palveluissa verkon päivittämisestä omiin tarpeisiinsa. Mikäli käyttäjä haluaa hajauttaa verkkoaan tai hankkia lisää prosessoritehoa, hän joutuu päivittämään tilaustaan, mistä koituu luonnollisesti lisäkustannuksia. Jos loppukäyttäjän järjestelmä toimii kokonaan yrityksen omalla infrastruktuurilla, ylläpitokustannukset kasvavat päivitysten ja monitoroinnin langetessa loppukäyttäjän vastuuksi. Myös energiankulutuksesta koituu lohkoketjun ylläpitäjälle kustannuksia. Esimerkiksi surullisenkuuluisa Bitcoinin vuosittainen energiankulutus on arvioitu Bahrin ja Girdzijauskasin (2018) tutkimuksessa olevan 39 TWh, joka vastaa pienien maiden vuosittaista energiankulutusta. Mikäli lohkoketju toimii Bitcoinin käyttämällä proof-of-work-menetelmällä, energiakustannukset voivat olla ketjun käyttöasteen mukaan hyvin korkeat. Kolmas kustannuksia aiheuttava tekijä on myös lohkoketjun ylläpitämiseksi vaadittava laitteisto (Nikitović & Mahmutović, 2019). Lohkoketju vaatii toimiakseen enemmän tai vähemmän hajautetun verkon, joka sisältää ketjun toimintaa ylläpitävät solmut, jotka vaativat konsensusprotokollan mukaan tietyn määrän laskentatehoa sekä levytilan lohkoketjun kopion tallentamiseksi. Mitä enemmän verkkoa halutaan hajauttaa, sitä enemmän tarvitaan laitteistoa toimimaan verkon solmuina, jolloin myös laitteistokustannukset kasvavat. Neljäs ja suurin piilokustannuksia aiheuttava tekijä järjestelmän käyttöönotossa on itse implementointiprosessi (Nikitović & Mahmutović, 2019). Implementointi sisältää uuden järjestelmän kustomoinnin, testauksen ja integroinnin, järjestelmän käyttäjien koulutuksen, datan muuntamisen sekä konsultaation. Nikitovićin ja Mahmutovićin (2019) mukaan implementointi voi viedä jopa 40 prosenttia uuden järjestelmän kustannuksista. Lohkoketjujen tapauksessa käyttöönottoprosessi on haastava, sillä yritysten on joko kehitettävä järjestelmänsä lohkoketjualustan pohjalle tai muuntaa vanhat järjestelmät yhteensopiviksi lohkoketjualustan kanssa (Sadhya & Sadhya, 2018). Lisäksi vanhat järjestelmät eivät välttämättä ole helposti yh-

teensovitettavissa, jolloin käyttöönoton kustannukset kasvavat entisestään. Datan oikeellisuus ja sen muuntaminen uuden järjestelmän vaatimaan muotoon voi olla myös haastavaa, sillä muuntamisen automatisointi vaatii lisää ohjelmointityötä ja datan oikeellisuus on varmistettava ennen sen muuntamista useimmiten sellaisten henkilöiden toimesta, jotka ovat kyseisen datan kanssa jatkuvasti tekemisissä tai muuten tietävät sen rakenteesta eniten (Nikitović & Mahmutović, 2019). Järjestelmän teknisen integroinnin lisäksi kustannuksia aiheuttavat käyttäjien koulutus sekä konsultaatiotyö. Lohkoketjusovelluksessa tehtävät transaktiot vaativat nykyisellään aakkosnumeeriset julkisen ja yksityisen avaimen, joiden käyttö ei tavallisissa järjestelmän toiminnoissa ole välttämättä mielekästä. Lisäksi ei-selkokielisten avaimien käyttö altistaa käyttäjävirheille niiden monimutkaisuuden ja huonon muistettavuuden takia (Sadhya & Sadhya, 2018). Koska lohkoketjuteknologiat ovat vielä melko uusi aihealue, voi standardien ja säädösten puutteessa pätevän konsultaationkin löytäminen olla haasteellista.

Jos lohkoketjualustan käyttöönoton kustannuksia tarkastellaan aiemmin esitellyn kolmijakoisen mallin pohjalta, julkisista lohkoketjuista ei aiheudu kustannuksia ohjelmistolisenssien muodossa, sillä kuka tahansa voi liittyä niihin. Toisaalta julkisen lohkoketjun tapauksessa sovelluksen kehitystyö ja sen integroiminen muihin järjestelmiin lankeaa yrityksen vastuulle, josta aiheutuu lisäkustannuksia valmiiseen tuotteeseen verrattuna. Itse ketjun toiminta ja mahdolliset muutokset ovat myös täysin sen kehittäjien hallinnassa. Kun tähän lisätään aiemmin käsitellyt ongelmat turvallisuudessa ja skaalautuvuudessa, ei julkinen lohkoketju ole kovin mielekäs vaihtoehto yrityssovelluksen rakentamisen kannalta. Yritys kohtaa konsortiolohkoketjun kanssa samoja ongelmia kuin julkisen ketjun kanssa, mikäli yritys itse ei ole vähintään osa ketjun kehittäjäjoukkoa. Yrityksen omien toimintojen integrointi ei välttämättä ole mielekästä, mikäli ketjun toiminta ei noudata omia tarpeita. Kustannusnäkökulmasta yksityiset lohkoketjut ovat yrityksen kannalta mielekkäimpiä, sillä yleensä tarjolla on valmiita ratkaisuja, joita voidaan räätälöidä yritysten tarpeisiin. Käyttöönotto voi kuitenkin olla ongelmallinen, sillä kustannuksia tulee lisensseistä, laitteistosta, ylläpidosta sekä integrointiin liittyvistä töistä. On myös muistettava, että mikäli käytetään palveluntarjoajien SaaS-tuotteita, kaikki verkon solmut ovat periaatteessa palveluntarjoajan hallinnassa, jolloin on otettu mukaan luotettu kolmas osapuoli.

4 LOHKOKETJUN KÄYTÖN PERUSTELU

Lohkoketjut toimivat hajautettuina tietokantoina P2P-verkossa, jossa käyttäjien tekemät transaktiot vahvistetaan verkon solmujen toimesta ja lisätään ketjun uuteen lohkoon. Lohkoketju on oikein toimivana muuttumaton eli sinne tehtyjä transaktioita ei voi enää jälkikäteen muokata tai peruuttaa. Eri tyyppisillä lohkoketjuilla on eri ominaisuuksia, mitkä tekevät niistä enemmän tai vähemmän mielekkään vaihtoehdon perinteisellä tietokannoille yritysten näkökulmasta. Lohkoketjujen perinteisistä tietokannoista eroavien ominaisuuksien takia ne eivät sovellu kaikkiin käyttötapauksiin, jotka perinteisessä tietokannassa toimisivat. Muiden tutkielmassa esiintyneiden pointtien, kuten turvallisuuskysymysten ja skaalautuvuuden, lisäksi käyttötapauksia rajaa mahdolliset lait datan säilömiselle, kuten GDPR (Marsalek, Kollmann, Zefferer & Teufl, 2019). Tässä luvussa tarkastellaan tutkielmassa aiemmin esiintyneitä pointteja ja pohditaan, millaiset lohkoketjutoteutukset ovat yritysten kannalta järkeviä. Lisäksi tässä luvussa esitellään tämän tutkielman perusteella muokattu päätöspuu lohkoketjun käyttöönotosta yrityksissä.

4.1 Lohkoketjutyyppien soveltuvuus alustana

Kolmijakoinen malli jakaa lohkoketjut julkisiin, konsortio- ja yksityisiin lohkoketjuihin. Luokittelu perustuu ketjun käyttöoikeuksiin sekä sitä ylläpitävien solmujen hallitsijoihin. Jokainen lohkoketjutyyppi tarjoaa erilaisia ominaisuuksia, joista osa on yleensä mielekkäämpiä toteuttaa yritysjärjestelmiin implementoinnin kontekstissa. Tässä luvussa tarkastellaan edellä mainittuja lohkoketjutyyppejä ja niiden järkevyyttä yritysten näkökulmasta.

Ensimmäinen tyyppi on julkinen lohkoketju, jonka muista tyypeistä erottaviin ominaisuuksiin kuuluu sen avoimuus kaikille halukkaille osallistujille. Tämän tyyppisessä lohkoketjussa kuka tahansa voi tehdä transaktioita, jonka lisäksi on mahdollista muodostaa uusi solmu, jota käytetään verkon transaktioiden vahvistamiseen. Tutkimuksessa käsitellyt turvallisuusongelmat koskevat

etenkin julkisia lohkoketjuja, joten on syytä tarkastella niiden vaikutusta mahdollisen toteutuksen kannalta. Lohkoketjujen demokraattisen luonteen vuoksi niille muodostuu uhkaksi laskentatehon jakautuminen usealle eri alustalle, jonka vuoksi mahdollisen hyökkääjän on helpompi saada käyttöönsä tarvittava laskentateho vaihtoehtoisen ketjun luomiseksi. Tätä ilmiötä kutsutaan fragmentaatio-ongelmaksi ja siitä muodostuu suurempi uhka varsinkin pienemmille alustoille lohkoketjujen määrän kasvaessa. Koska uhka on suurin pienillä alustoilla, voidaan rajata mielekkäiksi tarkastelun kohteiksi vain suurimmat lohkoketjualustat, Bitcoin ja Ethereum, joilla fragmentaation uhka on pienin. Bitcoinin perusideana on toimia digitaalisena valuuttana, jolloin se ei lähtökohtaisesti sovellu applikaatioiden luomiseen alustalle. Bitcoinille on tosin luotu sivuketju nimeltä Rootstock, joka implementoi Ethereumin käyttämän Ethereum Virtual Machinen (EVM) mahdollistaen älysopimusten luomisen myös Bitcoin-alustalle ja näin ollen myös mahdollisuuden yritysapplikaatioille (Worley & Skjellum, 2018). Yritysapplikaatioissa liikkuu kuitenkin usein luottamuksellista tietoa, joka halutaan salata ulkopuolisilta, jolloin julkiset lohkoketjut eivät yleensä tarjoa tarpeellista suojausta transaktioissa liikkuvalle datalle. Vaikka transaktioiden data päästäisiin salaamaan, on ongelmana julkisten lohkoketjujen hitaus. Tämän hetkisten toteutusten suorituskyky ei vastaa toimialoilla totuttua nopeutta, vaan esimerkiksi Bitcoin-transaktion läpimeneminen voi viedä aikaa kymmenestä minuutista ylöspäin riippuen verkon kuormituksesta. Ethereumin alusta on suunniteltu älysopimusten luomiseen, joten se on luonnollisempi valinta ulkopuolisten applikaatioiden toteuttamiselle. Samat ongelmat turvallisuudessa ja skaalautuvuudessa tosin koskevat myös Ethereumia, jolloin sekään ei ole kovin mielekäs vaihtoehto yritysapplikaation luomiseksi. Kustannusnäkökulmasta julkisissa lohkoketjuissa säästetään ohjelmistolisenssien ja laitteiston suhteen, mutta lisäkustannuksia koituu itse applikaatioiden toteuttamisessa. Pohdinnan perusteella voidaan sanoa, että julkiset lohkoketjuratkaisut eivät ole turvallisuus- ja skaalautuvuuskysymysten takia yritysten kannalta mielekkäitä, joten niille ei ole järkevää lähteä rakentamaan yrityksen toimintaan integroitavaa järjestelmää.

Konsortiolohkoketjut ovat julkisen ja yksityisen lohkoketjun välimalleja, joissa verkkoa ylläpitävät solmut on jaettu ennalta määritetylle joukolle, mutta verkkoa pystyy tarkastelemaan kuka tahansa. Mikäli yritys rakentaa itse, tai on mukana rakentamassa, tämän tyyppistä lohkoketjua, voi se vaikuttaa verkon solmujen hallitsijoihin, jolloin vähennetään todennäköisyyttä verkon laskentatehon väärinkäyttöön perustuviin hyökkäyksiin. Lisäksi voidaan implementoida tarpeen mukaan salausmenetelmiä, joilla turvataan transaktioiden ja niiden datan salaaminen ulkopuolisilta. Skaalautuvuus on ongelmana myös konsortiolohkoketjuissa varsinkin ketjun koon kasvaessa sekä suuremmilla käyttäjämäärillä. Täysin turvallista ja lohkoketjun periaatetta noudattavaa skaalausmenetelmää ei ole tällä hetkellä saatavilla, joten mikäli skaalautuvuus on tärkeä ominaisuus, ei lohkoketju ole välttämättä mielekkäin ratkaisu yritysjärjestelmän kannalta. Konsortiolohkoketjujen käyttö on siis hyvin tapauskohtaista, joskaan ei täysin poissuljettava vaihtoehto, sillä tällaisessa toteutuksessa käyttäjille ei

aseteta verkon solmuja lukuun ottamatta rooleja, joilla voitaisiin valvoa ketjun käyttöoikeuksia.

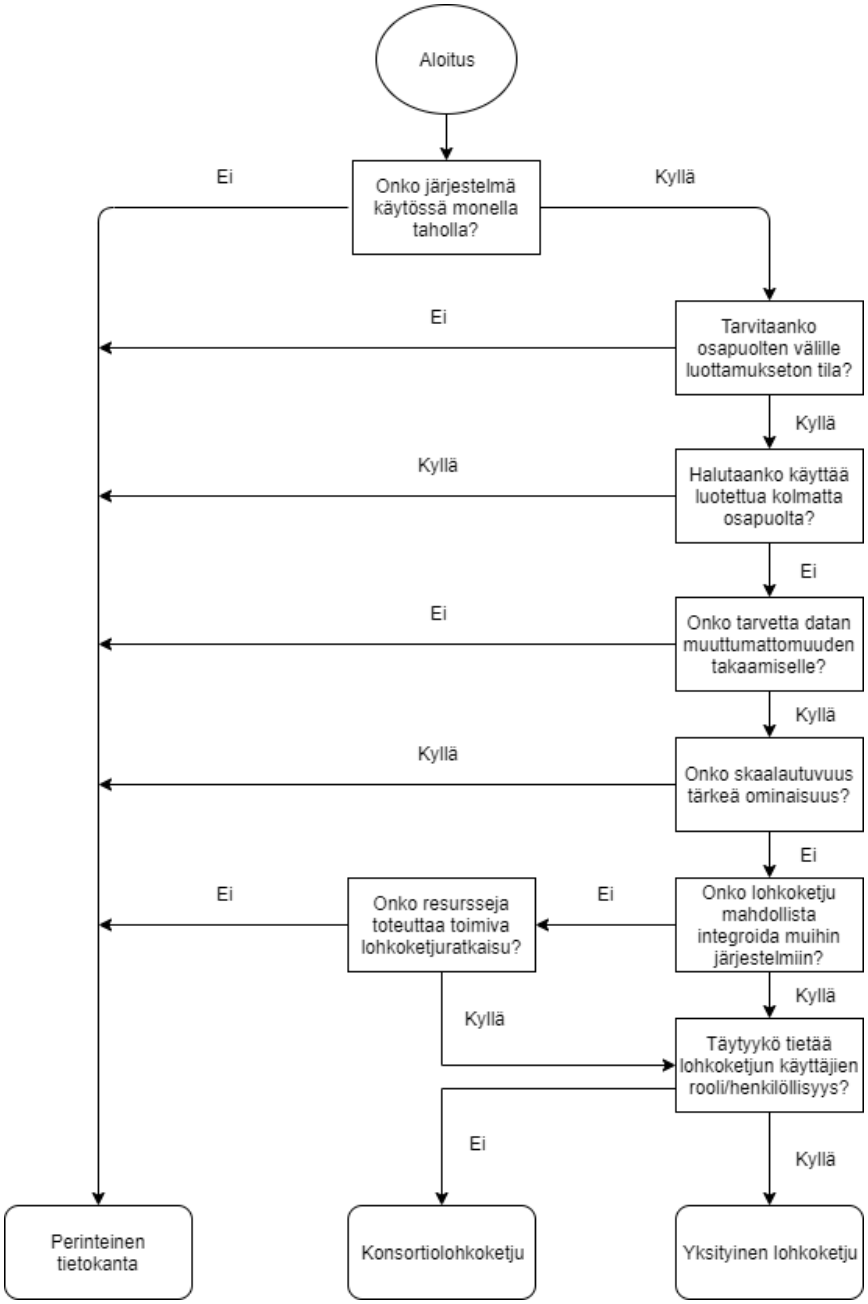
Yksityistä lohkoketjua hallitsee vain yksi taho, jolla on valtuudet asettaa käyttäjille rooleja ja oikeuksia. Ketjun operaatiot ovat vain tietyn käyttäjäryhmän saatavilla, jolloin sivutetaan pitkälti muissa lohkoketjutyypeissä esiintyvät turvallisuusongelmat ja datan salaukseen liittyvät kysymykset. Lohkoketjun skaalautuvuus pitkällä aikavälillä on muiden lohkoketjutyyppien tavoin ongelma myös yksityisissä ketjuissa ja se on otettava huomioon yritysapplikaatioiden kehityksessä. Yksityiset lohkoketjut ovat yritysten kannalta pääosin mielekkäimpiä vaihtoehtoja, sillä tarjolla on jo valmiita ratkaisuja, jotka voidaan implementoida yrityksen toimintaan. Lisäksi yksityisten lohkoketjujen antama päätösvalta ketjun käyttäjistä ja ketjun ominaisuuksien määrittely tekee niistä houkuttelevimman vaihtoehdon perinteiseen tietokantaan pohjautuvien järjestelmien rinnalle.

4.2 Päätöspuumalli

Chowdhury ym. (2018) tutkimuksessa on esitelty päätöspuu, joka kuvaa lohkoketjusovelluksen käyttöönottoon liittyvää loogista päättelyä. Malli ottaa huomioon lohkoketjua hallitsevien tahojen määrän, joka määrittää jo lähtökohtaisesti sitä seuraavien kysymysten relevanttiuden. Mikäli järjestelmää käyttää vain yksi taho, on lohkoketjua turha käyttää, sillä osapuolten välistä luottamuspulaa ei ole. Tutkimuksessa esitellyn mallin mukaan lohkoketjulle on tarve, mikäli osapuolten välillä on luottamusvaje, kolmatta osapuolta ei haluta käyttää, datan muuttumattomuus ei ole tärkeää ja skaalautuvuus ei ole tärkeä ominaisuus. Tämän jälkeen malli jakaa lohkoketjut joko julkisiin tai yksityisiin lohkoketjuihin julkisen verifioinnin tarpeen perusteella. Lopuksi ketjujen toiminta jaetaan tietovarastointimenetelmiin datan kestävyyden perusteella tiedon varastoimiseen lohkoketjussa ja varastoimiseen ketjun ulkopuolelle. Tässä luvussa esitellään tämän tutkielman perusteella koottu malli, joka käyttää pohjana edellä mainittua päätöspuuta.

Koottu malli esittää samat alkukysymykset kuin pohjana toimineen päätöspuun alkuvaihe, sillä ne ovat erittäin relevantteja päätökseen implementoida lohkoketjupohjainen ratkaisu yrityksen toimintaan. Mikäli uudella järjestelmällä ei ole useampi kuin yksi taho, joka käyttää järjestelmää, siirrytään suoraan perinteiseen tietokantaan. Tämän jälkeen selvitetään useamman kuin yhden osapuolen luottamusvaje, halukkuus käyttää luotettua kolmatta osapuolta ja tarve datan muuttumattomuudelle, jonka yhteydessä tulisi selvittää myös lakitekniset seikat datan säilömiselle, ja tarve järjestelmän skaalautuvuudelle. Näiden kysymysten jälkeen luotu päätöspuu eroaa pohjana käytetystä mallista. Koska Crowdhuryn ym. malli ei ota huomioon mahdollisia muita integroitavia järjestelmiä, ja koska ne ovat tämän tutkielman perusteella osa yritysimplementaatiota koskevia kysymyksiä, seuraava vaihe on selvittää mahdollisuus implementoida lohkoketjuratkaisu tarvittaessa yrityksen muihin järjestelmiin. Mi-

käli vanhat järjestelmät eivät ole yhteensopivia lohkoketjun kanssa, selvitetään, onko resursseja kehittää toimiva ratkaisu, joka korvaa yhteensopimattomat järjestelmät tai on yhteensopiva muiden järjestelmien kanssa. Resurssien puuttuessa joudutaan siirtymään perinteiseen tietokantaan. Mikäli lohkoketjuratkaisu on mahdollista toteuttaa, jaetaan ratkaisu yksityisiin ja konsortiolohkoketjuihin. Julkiset lohkoketjut on jätetty päätöspuusta pois, sillä ne todettiin epäkäytännöllisiksi aiemmassa pohdinnassa. Lopullinen jako tapahtuu selvittämällä roolien ja oikeuksien tarve lohkoketjussa. Jos käyttäjien henkilöllisyyden tai roolin tietämistä ei vaadita, siirrytään konsortiolohkoketjuun ja muussa tapauksessa valitaan yksityinen lohkoketju. Koko päätöspuu näkyy kuviosta 1.



KUVIO 1 Päätöspuu lohkoketjujen käytön perustelulle

5 YHTEENVETO

Tutkielmassa käytiin aluksi läpi lohkoketjujen toiminta sekä siihen liittyvää yleistä, tosin melko teknistä, käsitteistöä ottamalla esimerkiksi Bitcoin-alusta. Tämän jälkeen käytiin lyhyesti läpi älysopimusten toiminta ottamalla esimerkiksi Ethereum-alustan älysopimukset, jotta tutkielman seuraavissa vaiheissa tarkasteltava applikaatioiden rakentamisen käsittely olisi mielekästä. Seuraavaksi vertailtiin lohkoketjun toimintaa perinteisiin tietokantoihin. Vertailussa todettiin lohkoketjuilla olevan perinteisistä tietokannoista poikkeavia ominaisuuksia, kuten datan muuttumattomuus, läpinäkyvyys, luottamuksettomuus sekä eriävät turvallisuusriskit, jotka tekevät lohkoketjuratkaisujen käyttötapauksista spesifisempiä. Seuraavassa luvussa tarkasteltiin lohkoketjuratkaisujen ongelmia tutkielmassa esitellyn kolmijakoisen mallin pohjalta. Lohkoketjut jaettiin julkisiin, konsortio- ja yksityisiin lohkoketjuihin ja tarkasteltiin millaisia vaikutuksia turvallisuuskysymyksillä ja skaalautuvuusongelmilla on eri tyyppisiin ratkaisuihin yrityksen näkökulmasta. Turvallisuuskysymyksistä tarkasteltiin lohkoketjujen fragmentaatiota, joka mahdollistaa laskentatehon väärinkäyttöä hyödyntävät hyökkäykset, sekä lohkoketjujen anonymiteettiä koskevat ongelmat, kuten transaktioiden ja niiden sisältämän datan salauksen puute. Tutkielmassa todettiin, että nämä ongelmat ovat suurimpia julkisissa lohkoketjuissa. Skaalautuvuuden todettiin olevan ongelma kaikissa lohkoketjutyypeissä. Turvallisuus- ja skaalautuvuusongelmien lisäksi luvussa käsiteltiin myös lohkoketjupohjaisen ratkaisun kustannusrakennetta vertaamalla sitä perinteisen tietojärjestelmän käyttöönottoon. Vertailu tehtiin, koska löydetyssä tutkimustiedossa ei käsitelty suoraan ja kattavasti lohkoketjuratkaisun implementoinnin kustannuksia. Vertailussa todettiin, että kustannuksia syntyy ketjun tyypin mukaan ohjelmistolisensseistä, laitteistosta, ylläpidosta sekä käyttöönottoon liittyvistä kustannuksista, kuten integroinnista muihin järjestelmiin, käyttäjien kouluttamisesta ja konsultaatiosta. Tämän jälkeen pohdittiin tutkielmassa aikaisemmin esiintyneiden pointtien pohjalta, mitkä kolmijakoisen mallin tyypit soveltuvat yritysjärjestelmiin parhaiten. Pohdinnan tuloksena todettiin, että julkiset lohkoketjut eivät ole yritysten kannalta mielekkäitä ja konsortio- ja yksityisille lohkoketjuille löytyy käyttötapauksia yrityssovelluksista kuitenkin niin,

että konsortiolohkoketjujen käyttötapaukset ovat hyvin rajattuja. Lopuksi esiteltiin tätä ja aikaisempaa tutkimusta yhdistelevä päätöspuumalli, jolla selvitetään, onko lohkoketjuratkaisun käytölle perusteita.

Tutkielman suurimmaksi haasteeksi osoittautui aihetta kattavasti käsittelevän lähdemateriaalin löytäminen. Suurin osa lähdemateriaalinen tieteellisistä julkaisuista noudatti pitkälti samaa kaavaa, jossa esiteltiin lohkoketjujen historia Bitcoinin nousun myötä, käytiin lyhyesti läpi lohkoketjujen toiminta ja esiteltiin julkaisun mukainen teoria enemmän tai vähemmän kattavasti. Monissa tutkimuksissa käytiin myös läpi lohkoketjuratkaisujen käyttökohteita useimmiten melko optimistiseen sävyyn. Tämän tutkielman perusteella kootun päätöspuumallin pohjalta osa näiden tutkimusten esittämistä käyttökohteista voitaisiin hylätä esimerkiksi useamman luottamusvajetta kärsivän osapuolen puutteen ja skaalautuvuuden tärkeyden perusteella. Osa potentiaalisesta lähdemateriaalista jouduttiin hylkäämään puutteellisen kirjoitusasun ja kieliopin perusteella. Varsinkin lohkoketjujen turvallisuusongelmia kattavasti käsittelevän tutkimuksen löytäminen osoittautui erittäin haasteelliseksi, sillä suurin osa löydetystä lähdemateriaalista käsitteli ongelmia erittäin pintapuolisesti. Myöskään lohkoketjuratkaisun implementoinnin todellisista kustannuksista ei tässä tutkielmassa suoritettujen hakujen perusteella löytynyt tutkimustietoa, joten tutkielmassa oli sovellettava perinteisten järjestelmien käyttöönoton kustannuksiin liittyvää tutkimusta johtopäätösten vetämiseksi.

Tämä tutkielma pyrki vastaamaan kahteen tutkimuskysymykseen, jotka olivat seuraavat.

- Mitkä tekijät vaikuttavat lohkoketjuteknologioiden käyttöönottoon yrityksissä?
- Milloin lohkoketjuun pohjautuvan ratkaisun käyttö on perusteltua?

Tutkielman perusteella voidaan sanoa, että käyttöönottoon vaikuttavia tekijöitä ovat erityisesti lohkoketjun ominaisuudet, kuten skaalautuvuus, tarvittavat turvallisuusominaisuudet datan salaukseen ja mahdollisiin hyökkäyksiin liittyen sekä resurssit toteuttaa toimiva lohkoketjuratkaisu ja todellinen tarve sen käyttöönotolle. Tarve voidaan perustella päätöspuumallissa esitellyn polun avulla. Lohkoketjujen käyttöönotto on perusteltua, mikäli esitellyn päätöspuumallin mukaan päästään kysymykseen ”*Täytyykö tietää lohkoketjun käyttäjien rooli/henkilöllisyys?*”. Jatkotutkimukselle löydettiin tutkielman aikana aiheita pääasiassa lohkoketjuja koskevien turvallisuuskysymysten ja lohkoketjujen käyttöönoton kustannusrakenteen osalta. Turvallisuuskysymyksiä on aikaisemmassa tutkimuksessa käsitelty melko suppeasti ja esimerkiksi olemassa olevien toteutusten implementoimista turvallisuusmenetelmistä tai tiettyihin ongelmakohtiin perehtyvistä aiheista saisi helposti jatkotutkimukselle aiheita. Käyttöönoton kustannusrakenteesta saisi myös tutkimusaiheita esimerkiksi eri palveluntarjoajien ratkaisuihin perehtymällä tai mahdollisia reaalimaailman käyttöönottoja tarkastelemalla.

LÄHTEET

Zhang, R., Xue, R., Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys.* 52(3), Artikkeli 51. Haettu osoitteesta https://dl.acm.org/citation.cfm?id=3316481

CoinMarketCap. (30.9.2019). Listaus kryptovaluutoista. Haettu osoitteesta https://coinmarketcap.com/

Wessling, F., Ehmke, C., Hesenius, M., Gruhn, V. (2018) How Much Blockchain Do You Need. *IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*. 44-47. Haettu osoitteesta https://ieeexplore.ieee.org/document/8445058

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, F-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems.* Julkaistu ennakkoon verkossa. https://ieeexplore.ieee.org/document/8643084

Sadhya, V., Sadhya, H. (2018) Barriers to Adoption of Blockchain Technology. *Americas Conference on Information Systems, 24(3).* Haettu osoitteesta https://aisel.aisnet.org/amcis2018/AdoptionDiff/Presentations/20/

Ledger. (17.11.2019). A brief history on Bitcoin & Cryptocurrencies. Haettu osoitteesta https://www.ledger.com/academy/crypto/a-brief-history-on-bitcoin-cryptocurrencies/

Bitcoin. (17.11.2019). Bitcoin: A Peer-to-Peer Electronic Cash System. Haettu osoitteesta https://bitcoin.org/bitcoin.pdf

Chowdhury, M., Colman, A., Kabir, M., Han, J., Sarda, P. (2018) Blockchain Versus Database: A Critical Analysis. *IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).* Haettu osoitteesta https://ieeexplore.ieee.org/document/8456055

Balaskas, A., Franqueira, V. (2018) Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).* Haettu osoitteesta https://ieeexplore.ieee.org/document/8560672

Chauhan, A., Malviya, O., Verma, M., Mor, T. (2018) Blockchain and Scalability. *2018 IEEE International Conference on Software Quality, Reliability and*

Security Companion. Haettu osoitteesta https://ieeexplore.ieee.org/document/8431962

Worley, C., Skjellum, A., (2018) Blockchain Tradeoffs and Challenges for Current and Emerging Applications: Generalization, Fragmentation, Sidechains, and Scalability. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. Haettu osoitteesta https://ieeexplore.ieee.org/document/8726513

Davenport, A., Shetty, S., Liang, X. (2018) Attack Surface Analysis of Permissioned Blockchain Platforms for Smart Cities. *2018 IEEE International Smart Cities Conference (ISC2)*. Haettu osoitteesta https://ieeexplore.ieee.org/document/8656983

Yuan, Y., Wang, F-Y. (2018) Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 48*(9). Haettu osoitteesta https://ieeexplore.ieee.org/document/8419306

Bitnodes. (21.11.2019) Global Bitcoin Nodes Distribution. Haettu osoitteesta https://bitnodes.earn.com/

Etherscan (21.11.2019) Ethereum Node Tracker. Haettu osoitteesta https://etherscan.io/nodetracker

Nemnodes (21.11.2019) NEM nodes. Haettu osoitteesta https://nemnodes.org/

Gervais, A., Karame, G., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S. (2016) On the Security and Performance of Proof of Work Blockchains. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Haettu osoitteesta https://dl.acm.org/citation.cfm?id=2978341

Li, W., Sforzin, A., Fedorov, S., Karame, G. (2017) Towards Scalable and Private Industrial Blockchains. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. Haettu osoitteesta https://dl.acm.org/citation.cfm?id=3055531

Nikitović, M., Mahmutović, A.(2019) Hidden costs of ERP Implementation. *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Haettu osoitteesta https://ieeexplore.ieee.org/document/8756754

Marsalek, A., Kollmann, C., Zefferer, T., Teufl, P. (2019) Unleashing the Full Potential of Blockchain Technology for Security-Sensitive Business Applications. *2019 IEEE International Conference on Blockchain and*

Cryptocurrency (ICBC). Haettu osoitteesta https://ieeexplore.ieee.org/document/8751444

IBM (1.12.2019) Pricing for IBM Blockchain Platform for IBM Cloud. Haettu osoitteesta https://cloud.ibm.com/docs/services/blockchain?topic=blockchain-ibp-saas-pricing

Bahri, L., Girdzijauskas, S. (2018) When Trust Saves Energy: A Reference Framework for Proof of Trust (PoT) Blockchains. *WWW '18 Companion Proceedings of the The Web Conference 2018*. Haettu osoitteesta https://dl.acm.org/citation.cfm?id=3191553

Mohanta, B., Panda, S., Jena, D. (2018) An Overview of Smart Contract and Use Cases in Blockchain Technology. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. Haettu osoitteesta https://ieeexplore.ieee.org/document/8494045