Tampereen yliopisto

Jani Mäkelä

PILVIPALVELUIDEN TUKI LOHKOKETJUILLE

Pro gradu-tutkielma

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Toukokuu 2022

TIIVISTELMÄ

Jani Mäkelä: Pilvipalveluiden tuki lohkoketjuille
Pro gradu -tutkielma, 60 sivua
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Toukokuu 2022

Lohkoketjuissa on kyse hajautetuista tietokannoista. Osa niiden tausta-ajatuksista kuten muuttumattomuus ja luotettavuus ovat yhä vahvoja, mutta kuitenkin esimerkiksi tavoite keskushallinnottomuudesta on murenemassa. Tähän on johtanut pilvipalvelujen tulo lohkoketjumarkkinaan Blockchain as a Service (BaaS) -palveluilla. BaaS helpottaa yritysten mukaantuloa lohkoketjuihin, mutta muuttaa lohkoketjuja ottamalla kolmannen osapuolen keskeiseen rooliin ja siirtää lohkoketjun pilveen keskitetylle toimijalle, jolloin lohkoketjuissa luovutaan sen alkuperäisestä hajauttamisen periaatteesta. Tässä tutkimuksessa on myös pyritty tuottamaan ymmärrystä siitä, että mihin lohkoketjut ja BaaS soveltuvat.

Tutkimuksessa esitetään lohkoketjujen skaalautuvuuden trilemma (*Buterin's Scalability Trilemma*), jossa selvitetään, että kaikissa lohkoketjuteknologioissa tulee tasapainotella desentralisaation, skaalautuvuuden ja tietoturvallisuuden suhteen. Lohkoketjujen skaalautuvuuden trilemman pohjalta tutkimuksessa arvioidaan minkälainen painotus Blockchain as a Service -lohkoketjussa on trilemman eri osa-alueista.

Tutkimuksen tavoite on vastata siihen, että minkälainen vaikutus lohkoketjujen pilvipalveluiden Blockchain as a Servicellä on lohkoketjuihin. Tutkimuksen tuloksissa vastattiin, että BaaS on vielä uusi teknologia ja sen vaikutusten arviointi on vielä hankalaa. On kuitenkin viitteitä, että se toisi yritystoimintaa ja lohkoketjuja lähemmäs toisiaan, jolloin ne voisivat päästä symbioosiin keskenään. Tästä voi seurata kehä, joka auttaa molempia kehittymään yhä kiihtyvässä tahdissa. Suurin haaste tässä on kuitenkin se, että se vaatii muutoksia asenteisiin ja ajatteluun niin liiketoiminnassa kuin lohkoketjuyhteisöissä.

Avainsanat: lohkoketjut, lohkoketju, Blockchain as a Service, BaaS, blockchain service, lohkoketjupalvelu, tilikirjatietokanta, tilikirjatietokannat, lohkoketjujen skaalautuvuuden trilemma, Buterin's Scalability Trilemma

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

1 Johdanto

Tietojenkäsittelyllä ja tiedon luotettavuuden tarpeella on pitkät juuret ihmisten historiassa. Jo renessanssin Italiassa huomattiin, että tiedon parempaan luotettavuuteen pystyttiin kahdenkertaisen kirjanpidon kautta. [Felin & Lakhani 2018] Tämä keksintö on siis elänyt jo yli puoli vuosituhatta, ja se kehittyy yhä sillä uusimpia tietojenkäsittelyä ja kirjanpitoa helpottavana ilmiönä ovat tulleet lohkoketjuteknologiat. Ne sisältävät tilikirjoja, joista selviää tarkkaan se, että mikä on kunkin tilin saldo ja kuinka paljon kyseisen tilin kautta on kulkenut dataa ja kenen kanssa. Niihin talletettu data on pysyvää ja läpinäkyvää, joten niiden sisältämällä datalla pyritään yhä parempaan luotettavuuteen.

Tässä tutkimuksessa pyrin vastaamaan, että mikä vaikutus pilvipalveluiden tarjoamalla Blockchain as a Service (*BaaS*) palvelulla on lohkoketjuihin. Vastausta aiheeseen on etsitty perehtymällä aihetta käsittelevään tutkimukseen. Jotta tähän kysymykseen pystytään vastaamaan, niin on syytä ymmärtää lohkoketjuja ja niiden taustaa. Tässä työssä iso osa onkin lohkoketjujen taustan ja käyttökohteiden selvittämistä.

Lohkoketjut toimivat vertaisverkossa, ja vertaisverkkoon liitettyjä laitteita kutsutaan noodeiksi. Kaikissa lohkoketjuratkaisuissa pyritään tasapainottelemaan desentralisaation, skaalautuvuuden ja tietoturvallisuuden suhteen, tätä kutsutaan lohkoketjujen skaalautuvuuden trilemmaksi (*Buterin's Scalability Trilemma*). Sillä on alkujaan pyritty tuomaan ilmi lohkoketjujen konsensusalgoritmien kehityksen haasteita. Esimerkiksi Bitcoinin käyttämä Proof of Work -algoritmi johtaa korkeaan sähkönkulutukseen ja transaktioiden tehottomuuteen, koska siinä desentralisaatio ja tietoturvallisuus on pyritty maksimoimaan. Bitcoinin alkuperäisenä tarkoituksena on ollut vähentää yritysten valtaa ja siirtää sitä yksilöille itselleen. Lohkoketjujen skaalautuvuuden trilemma on hyvä keino arvioida myös muita lohkoketjuihin liittyviä arkkitehtuureja, sillä nykyisin puhutaan usein siitä, että jokaiseen ratkaisuun tulisi löytää optimaalinen määrä desentralisaatiota, skaalautuvuutta ja tietoturvallisuutta.

Vaikka monissa yrityksissä on todettu, että lohkoketjujen käyttöönotto ja ylläpito on koettu hankalaksi niin ne ovat silti tuoneet kilpailua perinteisille tietokannoille. Tästä syystä pilvipalvelujentarjoajat ovat tuoneet oman Blockchain as a Service -nimisen ratkaisunsa markkinoille, joiden avulla yritykset pääsevät keskittymään itse business-logiikan kirjoittamiseen. Näissä pilvipalveluntarjoaja hoitaa lohkoketjun käyttöönottoon ja ylläpitoon liittyvät toiminnot. BaaS:ssa on kuitenkin erikoista se, että miten keskitetystä pilvestä voidaan toteuttaa hajautettu järjestelmä. Tämä tapahtuu siten, että pilveen asennetaan jokaiselle noodille oma virtuaalikoneensa, johon asiakas ottaa yhteyden lohkoketjua käytettäessä. Tähän on päädytty, koska monissa yrityksille suunnatuissa lohkoketjuissa korkeasta hajautuksen tasosta ei ole koettu saatavan merkittävää hyötyä ja noodien

ylläpitäminen pilvessä helpottaa koko lohkoketjuarkkitehtuurin ylläpitoon liittyviä toimenpiteitä. Näistä on kehittynyt myös uusi lohkoketjuun verrattava tietokantatyyppi tilikirjatietokannat, joiden avulla transaktioiden luotettavuuteen ja läpinäkyvyyteen on pyritty vastaamaan, mutta niissä on luovuttu hajautuksesta kokonaan.

Lohkoketjujen käyttöönottoa on hidastanut se, että yrityksissä tunnetaan paremmin lohkoketjujen heikkoudet kuin niiden tuomat mahdollisuudet. On siis tärkeää tuottaa tutkimusta aiheesta, jotta lohkoketjujen tuomia mahdollisuuksia saisi paremmin hyödynnettyä sille soveltuvissa käyttötarkoituksissa. Lohkoketjuista on vielä paljon esillä epäselvyyttä ja mediankin tuottama kuva niistä on kovin yksipuolinen, sillä se on yleensä keskittynyt yksittäisiin ilmiöihin itse teknologian sijasta.

Tämän johdantoluvun jälkeen tutkielman rakenne on seuraavanlainen. Luvussa kaksi selvitetään itse tutkimuksesta ja sen taustoista. Sen jälkeen luvussa kolme pyrin tekemään selonteon siitä, että mitä lohkoketjut oikein ovat, ja mitä ilmiöitä niihin liittyy. Luvussa neljä puolestaan käyn esimerkkien kautta läpi mihin lohkoketjut soveltuvat. Luvussa viisi esittelen lohkoketjujen skaalautuvuuden trilemman ja mitä ominaisuuksia niissä huomioidaan. Luvussa kuusi käydään läpi, että minkälaisia lohkoketjuja pilvipalveluissa on tarjolla, ja mitä hyötyjä ja haittoja seuraa siitä, että lohkoketju on pilvessä. Luvussa seitsemän arvioidaan, että miten BaaS vertautuu muihin lohkoketjuihin ja mitä vaikutuksia sillä on. Luvussa kahdeksan puolestaan kasaan johtopäätökset tästä tutkimuksesta, ja luvussa yhdeksän teen yhteenvedon.

2 Tutkimuksenteko ja tutkimusaihe

Tämän tutkimuksen tutkimustyyppi on laadullinen tutkimus. Lohkoketjuaiheisen tutkimuksen määrä on noussut viime vuosina eksponentiaalisesti, joten aiheen rajaaminen on nyt erityisesti tarpeen. Tästä syystä tutkimuskysymykseni on:

”Mikä vaikutus pilvipalveluiden Blockchain as a Service lohkoketjuilla on lohkoketjuihin?”

Itse pilvipalveluiden lohkoketjuista on tutkimusta vain vähän ja yleinen käsitys niiden hyödynnettävyydestä on vain harvoilla. Lohkoketjut tulisi nähdä vaihtoehtona perinteisien tietokantojen rinnalla. Pilvipalveluiden lohkoketjutarjonnalla ei ole arvoa, jos käyttäjät eivät tiedä mitä niillä voi saavuttaa. Sen vuoksi iso osa tästä työstä on lohkoketjujen taustoitusta.

Akateemisissa julkaisuissa on käynyt ilmi, että lohkoketjujen käyttöönottoa on hidastanut se, että yrityksillä on usein tietoisuus lohkoketjujen puutteista, mutta tietämättömyys niiden mahdollisuuksista [Lacity & Van Hoek 2021]. Lisäksi tulisi ymmärtää, että lohkoketjuja on erilaisia ja eri lohkoketjuja koskettavat erilaiset ongelmat. Myös lohkoketjut terminä usein yhdistetään ensimmäiseen lohkoketjuun eli Bitcoiniin. Tästä on kuitenkin vasta alkanut lohkoketjujen kehittyminen ja nykyisin niitä on useita erilaisia. Esittelenkin tässä työssä lohkoketjujen skaalautuvuuden trilemman kautta, että lohkoketjuissa tasapainotellaan skaalautuvuuden, desentralisaation eli hajautuksen ja tietoturvan suhteen. Erilainen tasapaino näiden suhteen aiheuttaa omanlaisensa ongelmansa lohkoketjuihin.

Tutkimuksessa tuodaan esille lohkoketjujen suurimmat puutteet lohkoketjujen skaalautuvuuden trilemman kautta. Tutkimuksesta käy ilmi, että miten trilemmaa ratkaistaan ja minkälaisia seuraavia kehitysharppauksia julkisiin lohkoketjuihin on tulossa. Selvitän myös, että julkisten lohkoketjujen ongelmat eivät kosketa samalla tavalla yksityisiä lohkoketjuja. Tämän vuoksi käsitykset lohkoketjujen puutteista eivät realisoidu yrityskäytössä. Pyrin tutkimuksessani myös tuomaan ilmi sen, että vaikka lohkoketjut muokkaisivat nykyisiä vallitsevia rakenteita ja haastaisivat liiketoimintamalleja niin jokaisella yrityksellä on mahdollisuus päästä kiinni lohkoketjujen tuomiin uusiin liiketoimintamalleihin pilvipalveluiden tarjoamien ratkaisujen kautta. Tuon tässä tutkimuksessa myös esimerkkien kautta ilmi minkälaisia mahdollisuuksia niin julkiset kuin yksityisetkin lohkoketjut ovat tähän mennessä tuoneet.

Ensisijaisina lähteinä olen käyttänyt vertaisarvioituja akateemisia artikkeleita. Tutkimusten lisäksi olen käyttänyt lohkoketjuaiheisia kirjoja, raportteja (*whitepaper*), uutisia, sekä lohkoketjujen kehittäjille tuotettua dokumentaatiota. Tutkimusalana lohkoketjut ovat vielä uusi, jossa on vaikea pysyä viimeisimpien trendien perässä, sillä lohkoketjut ja

niihin liittyvät ilmiöt kehittyvät erittäin nopeasti. Tämän vuoksi olen seurannut keskustelua lohkoketjuista erilaisissa podcasteissa. Olen hyödyntänyt näistä erityisesti sellaisten lohkoketjuasiantuntijoiden puheenvuoroja, jotka itse hyödyntävät lohkoketjuteknologiaa.

3 Taustaa lohkoketjuista

Lohkoketjuteknologialla tarkoitetaan tiedon talletukseen käytettävää teknologiaa, jossa lohkossa on viite aina aiemmin luotuun lohkoon muodostaen ketjun. Ketju on tallessa jokaisen lohkoketjun käyttäjän omalla koneella eli noodilla, joten se on hajautettuna ja toimii vertaisverkossa. Ketjuun talletetut lohkot talletetaan siten, että niihin ei voi tehdä muutoksia vaan ne ovat talletuksen jälkeen pysyviä osia ketjua. Yksi lohko sisältää lokikirjaa seurattavasta datasta. Tässä on ajatuksena, että kaikki lohkoketjun sisältämä data on saatavilla kaikilla sen käyttäjillä. Lohkoketjuilla voidaan tarkoittaa tätä tietorakennetta tai hajautettua teknologiaa, joka sisältää tämän tietorakenteen [Belchior *et al.* 2021]. Koska lohkoketju on teknologia, jonka avulla talletetaan tietoa se ei välttämättä juurikaan näy loppukäyttäjälle.

Lohkoketju terminä on kuitenkin syytä määritellä tarkemmin, sillä joissakin yhteyksissä ajatellaan, että lohkoketju on nimenomaan tilikirja, jossa dataa säilötään, ja lohkoketjuteknologia puolestaan on, kun tämä tilikirja on talletettuna vertaisverkkoon. Tilikirja on talletusmuoto, johon kirjataan aikajärjestyksessä se, että keneltä siirretään kenelle ja kuinka paljon. Käytän tässä tutkielmassa termiä lohkoketju viitaten vertaisverkossa toimivaan hajautettuun tietokantaan. Puolestaan keskitetysti toimivista lohkoketjuista puhun tilikirjatietokantoina.

Lohkoketjuja on useampia erilaisia, ja niiden kategorisoiminen erilaisten ominaisuuksien perusteella on hankalaa, koska niissä on suurta hajontaa. Eroavaisuuksia on esimerkiksi yhteensopivuuden ja arkkitehtuurin suhteen. [Belchior *et al.* 2021] On hyvä kuitenkin todeta, että jokseenkin vakiintunut kategorisoiminen on jaotella ne niiden hajautuksen perusteella. Tämä tapahtuu tunnistamalla se taho, joka päättää lohkoketjuteknologian kehityksestä. Vaihtoehtoja ovat loppukäyttäjä, konsortio ja kolmas osapuoli [Belchior *et al.* 2021]. Lohkoketjut ovat lähtöisin julkisista lohkoketjuista, joten niiden vaikutus näkyy myös yksityisissä ja konsortioiden lohkoketjuissa. Myös median antama kuva lohkoketjuista koskee myös pitkälti julkisia lohkoketjuja. Tässä työssä pyrinkin tuomaan esiin sitä, että se on kovin yksiulotteinen kuva siihen nähden, että lohkoketjuja on useita erilaisia.

Lohkoketjuteknologioiden taustalla näkyy selvästi useampi jo aiemmin keksitty teknologinen innovaatio ja periaate, jotka yhdistyvät lohkoketjussa. Esimerkiksi älysopimus, virtuaalivaluutat, hakkerietiikka, kryptatut tiivisteet, hajautus, NFT ja konsensusalgoritmit on keksitty jo ennen lohkoketjuja. [Belchior *et al.* 2021]

3.1 Ajatukset lohkoketjujen taustalla

Lohkoketjuteknologiat ovat iältään nyt toisella vuosikymmenellään, mutta ajatukset taustalla ovat vanhoja. Lohkoketjut on alun perin toteutettu hakkerietiikan periaatteiden mukaan, jotka sisältävät libertalistista ideologiaa. Siinä yksilöt ja yksilö nousee yhteiskunnan keskiöön ja valtiolle ja muille instituutioille tarjotaan mahdollisimman pieni rooli. Kyseessä on samat ideaalit kuin alkuvuosien hakkereilla eli libertalistinen yksilökeskeisyys ja yksilöiden välinen puolisosialistinen yhteistyö. Tämän lisäksi kannatetaan ajatusta vapaasta jakamisesta. Puolestaan hajauttaminen on 1900-luvun alun kybernetiikkaa. [Rantala 2018a]

Lohkoketjut ovat tulleet uutena teknologiana Bitcoinin myötä. Bitcoin oli ensimmäinen lohkoketjua hyödyntävä alusta. Sen uuden tyyppinen tiedon tallettamisen muoto ratkaisi sähköisiä tuotteita koskevan ongelman siitä, että alkuperäisen tuotteen varmentaminen oli lähes mahdotonta. Ennen lohkoketjua tuote siirrettiin uuteen kohteeseen kopioimalla kyseinen tuote uudessa kohteessa. Näin alkuperäinen tuote saattoi olla kahdessa paikassa samanaikaisesti. Tätä ongelmaa kutsutaan Double-spending-ongelmaksi. Perinteisesti finanssimaailmassa varmuus siitä, että kukaan ei voi käyttää samaa rahaa kahdesti vaati sen, että rahaliikennettä varten tarvittiin välimiehiä, jotka varmensivat transaktiot. Pseudonyymi Satoshi Nakamoto esitteli Bitcoinin julkaisuraportissa vuonna 2008, että miten teknologian avulla voidaan päästä eroon näistä välimiehistä luomalla uudenlainen teknologia. Bitcoinilla oli vastalause samaan aikaan päällä olevaan asuntomarkkinoiden lainakriisiin eli subprime-kriisiin, joka oli aiheutunut vastuuttomasti toimivista pankeista.

Lohkoketjuja kuvaavia ominaisuuksia ovat hajautus, tiedon avoin käytettävyys, kryptaus, muuttumattomuus ja läpinäkyvyys. Näiden ominaisuuksien avulla se vastaa teknologiana parempaan käyttäjien väliseen luottamukseen. Hajautus ja tiedon vapaa käytettävyys ovat keinoja, joiden avulla pyritään tiedon parempaan läpinäkyvyyteen. Puolestaan kryptaus on keino, jolla lohkoketjuissa voidaan varmistaa datan muuttumattomuutta.

Hajautus on oleellinen osa lohkoketjuja. Sen mahdollistaa vertaisverkko (*Peer to peer - P2P*), jonka ansioista lohkoketju voi toimia ilman keskitettyä tahoa. Hajautetuille käyttäjien väliselle ratkaisulle on tarvetta, koska niiden avulla voidaan varmistaa se, että suuryhtiöillä ja valtioilla ei ole viimeistä päätäntävaltaa siitä, mitä verkossa on näkyvillä. Tästä toisena esimerkkinä on sipuliverkko ns. Internetin pimeä puoli, jossa on vahvennettu salaus käyttäjästä. Vahvennettu käyttäjän salaaminen edistää tiedon vapautta ja tarjoaa yksityisyyden suojaa. [Harviainen & Tikkanen 2021] Lohkoketjujen teknologisessa toteutuksessa on noudatettu samoja periaatteita hajautetusta käyttäjien välisestä verkosta. Myös lohkoketjujen voi ajatella toteuttavan tiedon vapaata liikkumista, mutta ei kuitenkaan yhtä vahvaa yksityisyyden suojaa kuten sipuliverkko tarjoaa.

Ideologisista syistä tarjottu teknologia mahdollistaa rikollisen käyttäytymisen lieveilmiönä. Vuonna 2011 Silk Road oli ensimmäinen pimeän verkon markkinapaikka, jossa

käytiin vaihdantaa laittomilla tarvikkeilla. Silk Road ei ollut lohkoketjusovellus vaan toimi salatussa sipuliverkossa. Alustan kehittäneellä Ross Ulbrichtilla oli kuitenkin samat libertalistiset ajatukset keskushallinnottomuudesta ja yksilönvapaudesta kuin ensimmäisillä lohkoketjuilla. Silk Roadilla Bitcoin oli ensisijainen vaihdonväline ja mahdollisti verkkokaupan lainvalvojien ulottumattomissa. [Harviainen & Tikkanen 2021] Tämä on yksi syy, miksi lohkoketjut liitetään herkästi vieläkin laittomaan toimintaan. Lohkoketjujen keskushallinnottomuus ja yksilönvastuu näkyvät yhä julkisissa lohkoketjuissa esimerkiksi siinä, että niissä ei ole tahoa jolta käyttäjä voisi kysyä kadonneen salasanan palautusta.

Lohkoketjuihin talletettu data on muuttumatonta. Tämä johtaa siihen, että niiden käyttö hämärissä liiketoimissa ei ole järkevää. Tämä kun vielä yhdistetään siihen, että käyttäjät ovat pseudonyymejä niin kryptovaluutalla käyty laiton kauppa voi herkästi paljastua, kun osa pseudonyymeistä saadaan yhdistettyä todellisiin identiteetteihin. [Wichmann & Kurimo 2021] Pseudonyymit käyttäjät tarkoittavat sitä, että käyttäjillä on kryptattu merkkijono käyttäjätunnuksena. Vaikka käyttäjän nimeä ei saa selville suoraan lohkoketjusta niin kyseisen merkkijonon toiminta tapahtuu aina saman merkkijonon takaa. Tästä seuraa se, että mikäli pseudonyymi saadaan yhdistettyä käyttäjän henkilöllisyyteen, voidaan seurata, sitä keiden muiden pseudonyymien kanssa käyttäjä on suorittanut transaktioita. Lohkoketjujen muuttumattomuusperiaatteen nojalla transaktiot jäävät lohkoketjuun niin pitkäksi aikaa, kun lohkoketju on toiminnassa.

Lohkoketjujen muuttumattomuus tarkoittaa, että data, jota ne sisältävät ei voi muuttua jälkikäteen. Lohkoketjuun voidaan ainoastaan lisätä uusia osia eli se on Append-only tyyppinen tietorakenne. Tämä johtuu siitä, että lohkoketjut eivät tue tietokannoista tuttuja päivitä (*update*) tai poista (*delete*) operaatioita. Mikäli datassa huomataan virheellisyyttä, se tulee korjata uuteen lohkoon niin että myös muut noodit hyväksyvät sen. Virheelliset tapahtumat jäävät kuitenkin datan historiaan. Data ankkuroidaan muuttumattomaksi kryptauksen avulla. Jokaisen lohkon otsikossa eli header-osuudessa on lohkon sisältö SHA256-algoritmilla tiivisteeseen (*hash*) kryptattuna [Lin & Qiang 2018]. Mikäli lohkon yksikin merkki muuttuu, niin lohkon palauttama tiiviste muuttuu. Näin vertaisverkon muut käyttäjät saavat selville sen, että jokin osuus datasta on muuttunut ja oletuksena ne eivät hyväksy muutosta.

Myös lohkoketjun ensimmäinen lohko (*genesis-lohko*) on tehty muuttumattomaksi. Se yleensä sisältää konfiguraatioita, joita ei yleensä myöskään voida muuttaa jälkikäteen [Kilroy 2019]. Datan muuttumattomuuden kannalta suunnitteluvaiheessa tulee harkita, että mitä lohkoketjuun tallettaa ja miten varmistaa, että talletettava data pysyy laadukkaana. Muuttumattomuudesta johtuen myös henkilötietojen lisäämistä lohkoketjuun ei tulisi tehdä. Lohkoketjujen muutokset ovat kyllä todellisuudessa mahdollisia jälkikäteen,

mutta vaatii, että suurin osa vertaisverkosta hyväksyy ne. Jos niitä ei hyväksytä niin lohkoketjuun aiheutuu haarukoituminen eli rinnakkain jää kaksi lohkoketjua, joiden noodit jakaantuvat uuden ja vanhan välille. Muutoksia on hyvin vaikea saada voimaan julkisissa lohkoketjuissa, joissa on paljon toisistaan riippumattomia noodeja.

Julkiset lohkoketjut on tehty avoimen lähdekoodin periaatteella eli niiden koodi on vapaasti kaikkien tarkasteltavissa. Tämä tarkoittaa sitä, että niiden koodin voi myös halutessaan kopioita omiin tarkoituksiinsa. Tällä pyritään varmistamaan toiminnan läpinäkyvyyttä. Läpinäkyvyyttä pyritään lisäämään myös pitämällä kaikki lohkoketjussa suoritetut transaktiot julkisina. Julkisilla transaktioilla tarkoitetaan, että niistä näkyy mitkä pseudonyymit kyseiseen transaktion ovat suorittaneet ja kuinka suuria summia on siirretty. Yksityisissä lohkoketjuissa kuitenkin läpinäkyvyyttä voidaan kuitenkin rajata.

3.2 Lohkoketjuteknologiat

Lohkoketjut jaetaan tavallisesti avoimiin ja suljettuihin lohkoketjuihin sen perusteella, että voiko käyttäjä liittyä siihen noodiksi halutessaan. Suljetut lohkoketjut ovat rajatuille käyttäjille ja tiettyyn käyttötapaukseen. Ne ovat myös useimmin yrityskäytössä. Lohkoketju on datan säilöntään käytettävä teknologia, ja sen vuoksi loppukäyttäjälle voi jäädä hämärän peittoon, jos käytetty tietojärjestelmä käyttää lohkoketjua [Kilroy 2019]. Tästä johtuen avoimet lohkoketjut ovat enemmän esillä mediassa, ja median takia mielikuvat lohkoketjuista useimmin ovat muokkaantuneetkin juuri avoimien lohkoketjujen kautta. Tietoa lohkoketjujen käyttötarkoituksista ja mahdollisuuksista ei passiiviselle seuraajalle ole juurikaan saatavilla. Tällä hetkellä yrityksissä ei myöskään usein tunneta lohkoketjujen mahdollisuuksia omaan liiketoimintaan [Lacity & Van Hoek 2021]. Avoimissa ja suljetuissa lohkoketjuissa teknologiset ratkaisut vaikuttavat merkittävästi niiden suorituskykyyn, joten tämän tutkimuksen yksi päätarkoituksia on tuoda paremmin tietoisuuteen näiden eroja.

Lohkoketjuteknologioita on nykyisin useita erilaisia, joissa on pieniä eroavaisuuksia siitä, mitä ominaisuuksia niissä on ja minkälaisiin teknologisiin ratkaisuihin niissä on päädytty. Yhdistäviä tekijöitä niissä ovat kuitenkin läpinäkyvyys, hajautus, kryptaus, tiedon säilyttäminen transaktioista ja konsensusalgoritmi. Sen lisäksi nykyisin uudemmissa lohkoketjuissa yleensä lohkoketjuun on yhdistetty virtuaalikone, joka mahdollistaa sen, että lohkoketjuun voi kehittää logiikkaa eli älysopimuksia. Virtuaalikoneen ja älysopimusten ansioista lohkoketjuihin saadaan tehtyä sovelluskehitystä, jolloin niistä voidaan puhua lohkoketjualustoina. Tässä kohtaa on hyvä esitellä termi hajautetut applikaatiot (*Decentralized Application - DApp*), joita monissa lohkoketjuprojekteissa tehdään. Lohkoketjuteknologia mahdollistaa niiden käytön siten, että hajautetun sovelluksen data on talletettuna varmasti ja turvallisesti kaikissa sovellusta käytettävissä sijainneissa [Wichmann & Kurimo 2021].

Lohkoketjujen älysopimukset eivät tee mahdolliseksi mitään aikaisemmasta poikkeavaa, vaan ne helpottavat ja nopeuttavat sopimusten toimintaa [Rantala 2018a]. Tämä mahdollistaa sen, että lohkoketjun dataa voidaan hyödyntää useassa paikassa samaa lohkoketjua. Niiden kehittäminen vaatii kuitenkin erityistä tarkkuutta sillä ne eivät nimestään huolimatta ole kovinkaan älykkäitä. Ne eivät saa tietoa koodin ulkopuolelta, ja ne suoriutuvat aina niihin kirjoitetun koodin mukaan. Gavin Woodin mukaan kyseessä on tilakone, joka suorittaa transaktioita laskennallisten tilojen perusteella [Rantala 2018a]. Sen lisäksi, että ne ovat melko yksinkertaisia niin niiden muuttaminen jälkikäteen voi olla hankalaa, koska ne sijoitetaan lohkoketjuun ja lohkoketjut noudattavat muuttumattomuuden periaatetta.

Kaksi tunnetuinta avointa lohkoketjua ovat Bitcoin ja Ethereum. Bitcoin oli ensimmäinen lohkoketju, joka toi mukaan lohkoketjuteknologian. Ethereum puolestaan oli ensimmäinen lohkoketju, johon oli yhdistetty virtuaalikone, johon on toteutettu oma ohjelmointikieli Solidity. Ethereumin julkaisuraportin (*whitepaper*) julkaisi venäläiskanadalainen Vitalik Buterin vuonna 2014 ollessaan vain kaksikymmentävuotias. Nykyisin hän on ikonisessa asemassa lohkoketjupiireissä ja toimii yhä merkittävässä roolissa vaikuttaen Ethereum-lohkoketjun kehitykseen. Hän kuvailee Ethereumin raportissa, että Nick Szabo oli jo vuonna 2005 ehdottanut lohkoketjumaista tietokantaratkaisua maaomistajuuden säilömiseen, mutta vielä tuolloin käyttötapaukseen ei ollut tiedossa sopivaa teknologiaa [Buterin 2014]. Vastaavasta ajatuksesta hän loi Bitcoinin pohjalta luoda hajautetun järjestelmän, joka sisältää replikoituja tietokantoja, joka tunnetaan nykyisin Ethereum-lohkoketjuna.

Lohkoketjuja on nykyisin useita erilaisia, esimerkiksi sivulohkoketjut (*sidechain*), joita on rakennettu toisten lohkoketjujen päälle ”Layer2” teknologioina kuten Polygon-lohkoketju, joka on rakennettu Ethereumin päälle. Sen avulla pyritään rakentamaan skaalautuvampi lohkoketjualusta. Eri teknologioita vertailtaessa olisi hyvä tuntea niiden taustaa ja teknologiaa ja tiedostaa, että mihin ne soveltuvat parhaiten ja minkälaisia rajoitteita niillä on. Esimerkiksi Hyperledger Fabric on yrityskäyttöön suunniteltu suljettu lohkoketju, joka on toteutettu yhdessä monen teknologiayrityksen yhteistyössä.

Kaikissa lohkoketjuissa data tulee olla yhteisymmärryksessä eri noodien välillä. Tätä tehtävää lohkoketjussa hoitaa konsensusalgoritmi. Eri lohkoketjuissa on päädytty erilaisiin konsensusalgoritmeihin, ja sillä on paljon vaikutusta lohkoketjun skaalautuvuuteen, turvallisuuteen ja hajautuksen tasoon. Yleisimpiä konsensusalgoritmeja esitellään tarkemmin tässä työssä lohkoketjujen skaalautuvuuden trilemman yhteydessä.

Lohkoketjuista voidaan tunnistaa kolme erityyppistä objektia. Ne ovat käyttäjät, tuotteet ja transaktiot. Transaktio syntyy, kun käyttäjät siirtävät tuotteet toisilleen. [Kilroy 2019] Useimmin tuote on jokin kryptovaluutta, mutta se voi olla jotain muutakin. Ainoastaan sillä käyttäjällä, joka omistaa tuotteen on mahdollisuus vaihtaa tuotteen

omistajuutta toiselle käyttäjälle. Omistajuuden vaihto vaatii kuitenkin sen, että koko lohkoketju löytää konsensuksen siihen, että data lohkoketjun sisällä muuttuu. Näin lohkoketju pysyy jokaisessa solmussa yhdenmukaisena ja se hyödyntää konsensuksen ylläpitämiseksi konsensusalgoritmia, jolla se voi varmentaa muutosten validiuden.

Transaktiohistoriaa voidaan pitää tilikirjana ja yhdistämällä kaikkien käyttäjien tilit voidaan saada lohkoketjun maailmantila. Tuotteen omistajan vaihtuessa se talletetaan transaktio tilikirjaan. Siihen kerätään kaikki datan muutokset tietyltä aikaväliltä. Varsinkin monissa yksityisissä lohkoketjuissa on lohkoketjun rinnalla käytössä niin kutsuttu maailmantilatietokanta. Transaktiohistoriaa puolestaan talletetaan tilikirjaan eli lohkoketjuun. [Kilroy 2019]

3.3 Lohkoketjuihin liittyvät ilmiöt

Lohkoketjuihin liittyy monia ilmiöitä kuten mediassa näkyvät kryptovaluutat ja NFT:t. Niiden lisäksi ilmiöiksi luokittelen uudet organisoitumisen muodot, joihin liittyy yksityisten lohkoketjujen puolelta erityisesti konsortio hankkeet, ja julkisten lohkoketjujen puolelta Web 3.0 eli uusi hajautettu Internet, jossa suurille teknologia yrityksille keskittynyt valta siirtyisi käyttäjille.

Julkiset lohkoketjut sisältävät nykyisin pääasiassa kryptovaluuttaa tai rahakkeita (*token*), jotka ovat myös kryptovaluuttaa. NFT (*Non Fungible Token*) on kryptovaluutta, jonka avulla sisällytetään rahakkeena jokin objekti lohkoketjuun. Niiden avulla voidaan todistaa immateriaalioikeuksia. Taustalla on ajatus omistajuuden todentamisesta lohkoketjujen avulla. [Wichmann & Kurimo 2021] Puolestaan IoT (*Internet of things*) yhteydessä puhutaan termistä digitaalinen kaksonen (*digital twins*), joka on reaalimaailman viittaava digitalisoitu malli, joka täydentää datalla reaalimaailman tuotetta. [Felin & Lakhani 2018]. NFT voi olla myös, lohkoketjuun sisällytetyn digitaalisen kaksosen rahake.

Mediassa on erityisesti nostettu esiin viime aikoina julkisiin lohkoketjuihin yhdistettävä ilmiö, jossa ihmiset ostavat JPEG-kuvien immateriaalioikeuksia. Todellisuudessa oikeuksien omistaminen ei estä sitä, että kukaan ottaisi kuvasta kopion ja käyttäisi tätä lohkoketjun ulkopuolella esimerkiksi taustakuvana. Oikeuksien käyttäminen on relevanttia usein vasta siinä kohtaa, kun kuvia kaupallistetaan.

Vaikka NFT kuvien ostaminen ei vaikuttaisi rationaaliselta, niin sitä voidaan perustella perinteisen taiteen kautta. Esimerkkinä voidaan miettiä teosta Mona Lisa. Useat ihmiset haluavat mennä katsomaan sitä museoon, koska se on alkuperäinen taideteos, vaikka sitä esittävä kopio löytyisi selaimen hakukenttään teoksen nimen kirjoittamalla. Jos museossa olisi näkyvillä oikean näköinen kopio, niin se voisi herättää ihmisissä samat tunteet kuin alkuperäinen. Todellisuudessa arvo kyseiselle teokselle muodostuu ihmisten mielikuvissa sen tekovaiheista ja taiteilijasta samoin myös teoksen historiasta. [Rantala 2018b]

NFT mahdollistaa sen, että sähköiseen muotoon tehty taideteos pysyy alkuperäisen veroisena, vaikka siitä muuten saisi tehtyä kopioita. Sen avulla on mahdollista luoda arvoa digitaalisille tuotteille myös niiden omistajuushistorian perusteella. Myös itse taitelijat ovat pitäneet NFT kehitystä positiivisena, sillä niiden avulla voidaan toteuttaa rojaltijärjestelmä. [Rantala & Korhonen 2021]

Lohkoketjuteknologiaan voi sisällyttää myös monia muita asioita. Esimerkiksi ensimmäisiä tunnettuja käyttöönotettuja yksityisiä lohkoketjuja on Everledger, jossa timanttien immateriaalioikeuksia todennetaan lohkoketjun avulla ja jonka avulla pystytään seuraamaan näiden toimitusketjua [Felin & Lakhani 2018]. Ainakaan tällä hetkellä näistä ei kuitenkaan käytetä termiä NFT, vaikka se tekee käytännössä samaa sillä Everledger on oma lohkoketjunsa, jolle on oma käyttötapauksensa. Toinen omistajuuteen liittyvä käyttötapaus, johon olisi todellista kysyntää olisi lohkoketju maa-alueiden omistajuudesta erityisesti kehittyvissä maissa, sillä niiden avulla voidaan vähentää korruptiota ja muita epäselvyyksiä [Felin & Lakhani 2018].

Lohkoketjujen käyttöönoton yhteydessä tehdyt prosessien automatisoinnit tarkoittavat myös sitä, että automatisointi ei välttämättä itsessään liity lohkoketjuun vaan koko prosessin sähköistämiseen. [Felin & Lakhani 2018] On siis tärkeää tiedostaa, että vaikka tuotteet sisällytettäisiin lohkoketjuun niin sen sisältämä data ei välttämättä kuvaa maailman todellista kuvaa, jos lohkoketju ei saa tietoa reaalimaailmassa tapahtuvista muutoksista. Tämä ei poikkea mitenkään tavallisista tietojärjestelmistä, joten lohkoketjut ovat tässäkin mielessä aivan tavallinen datan talletukseen käytettävä tietojärjestelmä. Muodostamalla linkitys reaalimaailman tuotteen ja virtuaalisen tuotteen välille tarkoittaa sitä, että dataa tulee ylläpitää. Ylläpito onnistuu vain, jos tuotteen lohkoketjujärjestelmään on rakennettu riittävän hyvä prosessi datan ja reaalimaailman välille.

Toinen merkittävä lohkoketjuilmiö on hajautettu autonominen organisaatio (*Decentralized Automomous Organization - DAO*). Se on yleinen järjestäytymismuoto julkisissa lohkoketjuissa, jossa organisaatio tarjoaa palveluaan älysopimuksessa. DAO on virtuaalinen entiteetti, joka perustuu avoimeen lähdekoodiin [Buterin 2014]. DAO toimii aina sen älysopimuksen lähdekoodin mukaan. Sen toimintaa voidaan muuttaa, jos organisaation yhteisössä päätetään niin. DAO:ssa ei tavallisesti ole kuitenkaan työntekijöitä ja sen osakkaaksi pääsee useimmin ostamalla sille kuuluvaa virtuaalivaluuttaa. Omistamalla DAO:n virtuaalivaluuttaa voi osallistua DAO:n päätöksen tekoon tai päätäntävaltaa voi antaa muille haluamilleen tahoille. Tämä on kuitenkin määritetty älysopimukseen ja sieltä selviää myös, että kuinka paljon yhdellä osuudella on päätösvoimaa ja päätösvalta suhteessa omistetun valuutan määrään [Kulechov *et al*. 2021]. Voisi siis ajatella, että DAO:t ovat kuin osakeyhtiöitä lohkoketjujen sisällä ja niiden toimintaan voi osallistua omista-

jana. DAO:n valuuttaa usein myös usein ”steikataan” eli taataan, kun tehdään uusia ehdotuksia älysopimukseen, jolloin mahdollisista muutoksista johtuvista tappioista voidaan saada takuun määrän korvausta [Kulechov *et al*. 2021].

DAO-toimintaan liittyy sellainen termi kuin ICO (*Initial Coin Offering*), joka on yleinen DAO:n rahoitusmuoto. Niiden avulla DAO hakee joukkorahoitusta myymällä rahakkeita, jotka on tarkoitus sisällyttää DAO:n älysopimukseen. Näin ostajat voivat saada tulevaisuudessa hyödyn omistamistaan rahakkeista tai myydä niitä eteenpäin.

Hajautettujen organisaatioiden kautta on hyvä esitellä kolmas ilmiö eli hajautettu Internet. Käytössä on myös termit ”arvon Internet” ja lohkoketjupiireissä tästä puhutaan myös termillä Web 3.0. Se siirtäisi erityisesti talouden toiminnot algoritmien ja tekoälyn hallintaan, sen sijaan että jokin kolmas taho hallitsisi niitä [Johansson *et al.* 2019]. Sen ajatus on, että lohkoketjujen avulla voidaan toteuttaa Internet, joka toimisi täysin vertaisverkossa ilman keskitettyjä palvelimia. Sen taustalla on ajatus keskushallinnottomuudesta, jonka mahdollistaa lohkoketjut. Myös Lin ja Qiang [2018] mainitsevat, että lohkoketjuilla voisi olla potentiaalia korvata nykyiset kolmetoista juuripalvelinta, joka mahdollistaisi hajautetun Internetin. Web 3.0 lohkoketjuissa on haluttu eroon organisaatioista, jotka kaupallistavat käyttäjistä kerättyä dataa (eli kolmansista osapuolista). Myös organisaatioista, jotka toteuttavat alustan, jossa palvelun tarjonta ja kulutus tapahtuu alustan käyttäjien välillä. Eroon on haluttu myös valtioista, jotka eivät anna tiedon virrata vapaasti Internetissä. Hajautetussa alustassa tuottojen olisi tarkoitus mennä tasaisesti kaikille alustalla toimiville tahoille. [Wichmann & Kurimo 2021]

Neljäntenä ilmiönä nostan toisen organisoitumismuodon, joka liittyy lohkoketjuihin eli konsortiot. Verkostoituminen on yleinen suuntaus nykyisessä liiketoiminnassa, mutta se näkyy erityisesti lohkoketjuissa. Yksityisiä lohkoketjuja on hyvin kuvannut alusta asti yhteistyön parantaminen ja läpinäkyvyyden lisääminen. Tästä syystä sen ympärille on muodostunut useampia erilaisia konsortioita. Lohkoketjuista saatava hyöty on parhaillaan silloin kun jaetaan informaatiota ja pyritään kehittämään järjestelmä, joka palvelee kaikkia osapuolia. Lohkoketjuissa on kahdenlaisia konsortioita: liiketoimintaan ja teknologiaan keskittyviä konsortioita [Johansson *et al*. 2019]. Teknologiaan keskittyvät konsortiot keskittyvät lohkoketjuteknologian kehittämiseen. Puolestaan liiketoimintaan keskittyvissä konsortioissa on pääpaino itse liiketoiminnan kehittämisessä, jossa lohkoketju nähdään työkaluna. Lohkoketjujen avulla on mahdollista toteuttaa hajautettuja sovelluksia, jonka vuoksi ne sopivat hyvin yritysten väliseen yhteistyöhön. [Kilroy 2019].

Lohkoketjun on todettu olevan hyvä alusta, kun halutaan toimia konsortiossa tai muuten yhteistyössä. Lohkoketjujen avulla voidaan varmistaa, että kaikki sidosryhmät olisivat yhdenvertaisia yhteisessä tietojärjestelmässä. Se luo hyvän aihion yhteistyölle, sillä se

estää sen, että sidosryhmistä kukaan olisi hallitsevassa asemassa. Lohkoketjuissa käyttäjät toimivat omissa noodeissaan ja yrityslohkoketjuissa yritykset toimivat käyttäjinä, joten järjestelmä on hajautettu käyttäjien kesken.

Lohkoketjukonsortiosta hyvänä esimerkkinä on Hyperledger, joka tuottaa avoimen lähdekoodin työkaluja yksityisten lohkoketjujen kehitykseen [Song *et al.* 2021]. Se on siis itse teknologiaan keskittyvä konsortio. Se on heti alusta asti ollut usean suuren teknologian yhtiön konsortio, joista alkuperäisiä jäseniä ovat ainakin Linux Foundation ja IBM. Nykyisin siihen näiden lisäksi kuuluu kymmeniä toimijoita, joita ovat esimerkiksi Accenture, Siemens, Visa, JP Morgan, Huawei, Walmart ja Oracle [Hyperledger members].

Konsortiot ja yhteistyö vaatii toimiakseen uudenlaista ajattelua yritysten yhteistyöstä monelle yritykselle. Toisen etu ei ole aina toiselta pois, vaikka kilpailisikin samassa markkinassa. [Lacity & Van Hoek 2021] Kaikki arvon luonti ei ole myöskään pelkästään rahallisesti mitattavissa sillä informaation vaihdanta voi olla jopa arvokkaampaa monissa yhteyksissä niiden kanssa, jotka toimivat vastaavien asioiden kanssa päivittäin. [Azure whitepaper 2019]

3.4 Julkisten lohkoketjujen sääntely

Julkiset lohkoketjut on toteutettu ylikansallisesti noudattaen hakkerietiikkaa, joka pitää sisällään libertalistisen ajatuksen siitä, että ihminen itse ymmärtää parhaiten sen, että mikä tälle on parhaaksi. Itse teknologia on neutraali sen suhteen, että mihin lohkoketjua käytetään. Lohkoketjut eivät kuitenkaan vielä ole saatu sääntelyn piiriin, vaikka yksittäisissä maissa niihin olisikin tullut sääntelyä. [Lappalainen HS 2022] Käytännössä on käyttäjän vastuulla se, että tämä noudattaa omaa paikallista lainsäädäntöään. Tämä lähtökohta on käyttäjälle hankala. Vaikka itse teknologiaan voi luottaa niin muiden käyttäjien etiikasta ei voi olla täysin varma. Sama lähtökohta pätee myös tavallisessa liiketoiminnassa ja kaupankäynnissä, mutta tämän vuoksi yrityksille on säännelty vastuita tilinpäätösvelvollisuudesta vastuullisuusraportteihin. Myös lohkoketjuissa voisi olla tarve tämän tyyppiselle sääntelylle. Ongelma on kuitenkin siinä, että vaikka itse lohkoketjut ja älysopimukset voivat olla läpinäkyviä niin käyttäjät itsessään eivät ole muuta kuin sen suhteen, että mihin transaktioihin ne ovat osallistuneet. Esimerkiksi NFT-markkinan kanssa on huomattu, että niihin liittyy merkittävä määrä hämäriä transaktioita, joita voidaan epäillä rahanpesuksi. Toisaalta myös taidekauppa on lohkoketjujen ulkopuolella yleinen rahanpesun väylä eikä tähän tunnu löytyvän hyviä ratkaisuja. [Rantala & Korhonen 2021] Lohkoketjussa näitä tapauksia on kuitenkin helpompi todentaa jälkikäteen niiden muuttumattomuuden ansiosta.

Lohkoketjuja on yritetty hallita paikallisesti regulaation avulla. Tämä on kuitenkin hankalaa, koska avoimissa lohkoketjuissa toimiminen on ylikansallista. Esimerkiksi Wyoming on ensimmäinen USA:n osavaltio, joka on hyväksynyt lain mukaan DAO:n yhtiömuotona ensimmäinen heinäkuuta 2021. Viralliselta nimeltään yhtiömuoto on DAO LLC. Lakia hyväksyttäessä oli ajatus siitä, että regulaation selkeys toisi keskittymän DAO toiminnasta Wyomingiin. Laki on aiheuttanut kuitenkin paljon haasteita yhtiöille, jotka ovat rekisteröityneet Wyomingiin sillä rekisteröitymisen jälkeen yhtiöitä koskee käytännössä samat vastuut ja velvoitteet kuin osakeyhtiöillä on kyseisessä osavaltiossa. DAO:ssa ei kuitenkaan välttämättä ole selkeää vastuunkantajaa raporttien tekijästä. Johtuen uusista raportointivelvollisuuksista niin on todennäköistä, että monikaan organisaatio ei halua rekisteröityä Wyomingiin, vaikka se yhtiömuoto hyväksyttiin laissa. [Crank 2021]

Toinen merkittävä haaste lohkoketjuissa on liittynyt ICO:ihin, eli DAO-toimintaan liittyvään rahoitusmuotoon. Ne on nähty erityisen ongelmallisina niiden olemattoman regulaation takia. Vaikka yritys järjestäisi ICO-ulosannin, niin sillä ei välttämättä ole mitään kyvykkyyksiä toteuttaa ulosannin yhteydessä olevia tavoitteita. Tästä syystä taas yritysmaailmassa julkisten osakeyhtiöiden pörssiin listautuessa sijoittajien suojaksi toteutetaan yhtiön arvonmääritystä siitä mihin osakkeen listautumishinta perustuu. Tämän vuoksi esimerkiksi USA:ssa ICO on säännelty siten, että ICO tulee valmistella samalla tavalla kuin osakeyhtiön listautuminen. Tätä on kuitenkin kierretty tarjoamalla osakkuutta vastaavaa kryptovaluuttaa jollakin toisella nimellä kuin ICO. [Miettinen *et al*. 2022]

Sääntelyn ongelmiin ratkaisu olisi se, että ylikansallinen lohkoketjualustan mahdollistaja ottaisi vastuun regulaatiosta. Esimerkiksi Ethereum-lohkoketjussa kehitetään työkalua, jonka avulla voidaan toteuttaa näitä lainsäätäjille ongelmallisia teknologioita. Ethereumin on hankala vaikuttaa siihen, että mihin tämän kehittämiä työkaluja käytetään. Näkisin kuitenkin, että se pystyisi vastaamaan regulaation tarpeeseen tuomalla jotkin standardit, jonka perusteella käyttäjät saisivat arvion riskistä. Tähän keinoina voisivat olla esimerkiksi sertifikaatit kehittäjien osaamisesta ja yhteistyökumppaneista.

Puolestaan EU:n yleinen tietosuoja-asetus (*General Data Protection Regulation - GDPR*), joka rajoittaa henkilötietojen käsittelyä tietojärjestelmissä [Tietosuoja.fi], on aiheuttanut lohkoketjuille ongelmia. Erityisesti GDPR:n kohta: ”oikeus tulla unohdetuksi” on ongelmallinen lohkoketjujen tapauksessa, kun dataa ei voi poistaa tai muuttaa jälkikäteen tilikirjasta. [Belchior *et al*. 2021] Muuttumaton data mahdollistaa tarkan seurannan siitä mihin suuntiin transaktiot eri pseudonyymien välillä ovat siirtyneet. Pseudonyymien poistaminen tilikirjoilta jälkikäteen olisi ratkaisu, mutta siihen ei ole tukea lohkoketjuissa.

Regulaation avulla on myös pyritty estämään sitä, että kaiken tyyppisiä lohkoketjuja tietojärjestelmiin ei saa käyttää. Esimerkiksi USA:ssa monissa osavaltioissa on säädetty, että sovellusta ei saa käyttää julkisella puolella, jos se sisältää kryptovaluuttoja tai muita

vastaavia ominaisuuksia. Aina tietojärjestelmiä kehitettäessä on syytä tiedostaa mitä lainsäädännössä näistä sanotaan. [Kilroy 2019]

Toinen merkittävä lohkoketjujen kasvun estoon pyrkivä regulaatio on valtioiden kryptovaluuttojen omistamisen, käyttämisen ja louhimisen kielto [HS-Reuters 2021]. Intian lakiesitys oli todennäköisesti vastalause Diem-nimisen lohkoketjun julkaisuraportille, jonka tavoitteena oli tarjota 1,7 miljardille nykyisen ihmiselle pankkipalveluita, joilla niitä ei tällä hetkellä vielä ole. Näille valuutta sijaitsisi lohkoketjussa. Ongelmana on se, että valtiot, niiden keskuspankit ja niiden oma valuutta voisi menettää merkitystään, jos Diem olisi paljon käytössä kohdemaassa. Diem on konsortio, jonka suurin toimija on Meta (Facebook).

Kansallisesti regulaatiolla on aina vaikutusta. Tämä koskee myös lohkoketjuja varsinkin, jos sen organisaatiolla on paikallinen hallinto. Lohkoketjut olisi kuitenkin syytä saada ylikansallisen sääntelyn piiriin, jotta sääntely johtaisi oikeisiin toimenpiteisiin. Loppujen lopuksi lohkoketju on kuitenkin vain datan säilömiseen käytettävä teknologia, mutta niiden kansainvälisesti hajautetun luonteen vuoksi on vaikeaa todeta, että mitä lainsäädäntöä niiden tulisi noudattaa. Silti myös Suomessa olisi syytä kasvattaa resursseja alan seurantaan. Pelkkä paikallinen seuranta ja sääntely ei kuitenkaan riitä.

Lohkoketjujen ylikansallisuudesta kertoo myös se, että lohkoketjuilla on mahdollisuus toimia myös Venäjällä Ukrainaan kohdistuvan hyökkäyssodan aikana. Niitä voidaan käyttää Venäjällä hyvässä ja pahassa. Niiden avulla on esimerkiksi mahdollista kiertää Venäjän ylläpitämää sensuuria, mutta myös Lännen asettamia talouspakotteita.

4 Lohkoketjujen käyttökohteet

Lohkoketjuja tarvitaan silloin, kun halutaan tuottaa palvelu ilman kolmansia osapuolia. Tämä on alkuperäinen lohkoketjujen idea. Kyseessä ei ole välttämättä se suunta, jota tarvitaan toimivissa yhteiskunnissa, mutta sen avulla voidaan kiertää esimerkiksi sensuuria. Myös toimivissa yhteiskunnissa on kuitenkin hyvä olla myös vaihtoehtoja.

Lohkoketjuja tarvitaan myös silloin, kun halutaan antaa elektronisen tuotteen omistajuus asiakkaan käyttöön aidosti. Lohkoketju on sopiva teknologia tähän käyttötarkoitukseen sen kopioimattomuuden ja muuttumattomuuden takia. Lohkoketjujen avulla on mahdollista taata, että digitaalisessa tuotteessa on kyse juuri tietystä tuotteesta eikä vain sen kopio alkuperäisestä. Tämän mahdollistaa lokikirja, josta selviää tuotteen luontiaika ja omistajuuden vaihdokset. Lohkoketjun avulla tuote siirtyy asiakkaan lompakkoon, josta asiakas voi käyttää tuotetta. Virtuaalinen lompakko on useimmin lisäosana asiakkaan selaimessa. Virtuaalisen lompakon johdosta myös uudelleenmyyntioikeus siirtyy asiakkaalle.

Lohkoketjujen avulla voidaan rakentaa myös palveluita, joissa voidaan varmistua siitä, että palvelu maksaa juuri sen verran kuin tuotetta tulee käytettyä ja varmistua siitä, että rojaltit menevät halutuille tahoille. Käytännössä vastaavanlaista hinnoittelua kuin pilvipalveluilla eli ”pay-as-you-go” jossa hinta muodostuu käytön mukaan. Tämän tyyppisiä sovelluksia löytyy esimerkiksi musiikin striimauspalveluna. Tämä on mahdollista, koska lohkoketjujen avulla voidaan automatisoida rojaltimaksuja. Toinen esimerkki rojaltimaksujen automatisoinnista on Xbox Enterprise Blockchain Platform. Se on Microsoftin ja ”Big four” tilintarkastustoimisto Ernst & Youngin tekemä lohkoketjuhanke, jonka avulla transaktioiden ja rojaltimaksujen automatisoiminen onnistui. Automatisointiin käytetään älysopimuksia, joiden avulla on mahdollista parantaa maksujen käsittelynopeutta, jolloin maksujen käsittelynopeus parani viikoista tunteihin. [Felin & Lakhani 2018]

Lohkoketjut sopivat myös silloin kun asiakkaille halutaan toteuttaa yhteinen järjestelmä, jossa datan omistajuus on hajautettu kaikille osakkaille ja halutaan varmuus, että data on validia. Tästä johtuen se on konsortioille erittäin potentiaalinen alusta, kun halutaan toteuttaa hajautettuja sovelluksia. On hyvin mahdollista myös toteuttaa ainoastaan tietty osuus informaatioarkkitehtuurista lohkoketjun päälle. Toteutus on mahdollista liittää rajapintojen kautta muuhun infraan ja onkin enimmäkseen yrityksestä ja sen omista tietojärjestelmistä kiinni, miten se käyttäisi lohkoketjussa olevaa dataa.

Yritysten tulisi aktiivisesti koittaa löytää strategia, jonka avulla ne voisivat hyötyä lohkoketjuista. Felin ja Lakhani [2018] lähestyvät strategian luontia seuraavin kysymyksin. Yritysten tulisi aktiivisesti koittaa löytää strategia, jonka avulla ne voisivat hyötyä lohkoketjuista. Käyttökohteiden löytämiseen voi hakea vastauksia kysymyksiin, että ”*Miksi lohkoketju-sovellus tehdään*?”. Usein vastaukset ovat seuraavanlaisia: se auttaa seurantaan, se antaa varmistusta, se kokoaa dataa yhteen tai se tuottaa lokimerkintöjä. Sen

jälkeen, ”*Mitä arvoa näillä on*?”. Usein näihinkin löytyviä vastauksia ovat informaatio, vastuullisuus, saatavuus, omistajuus, maine ja luottamus, transaktiot itsessään, sopimukset ja päätösvalta. Viimeinen kysymys on, että ”*Kenelle arvoa luodaan*?”. Tähän usein puolestaan löytyy vastaus sidosryhmistä eli asiakkaille, työntekijöille, toimittajille, tuottajille, valvonnalle, hallinnolle vai jopa kansalaisille. Helpoimmin vastauksen löytää miettimällä ensin sidosryhmiä ja mahdollisia kehityskohteita organisaation ja sen sidosryhmien välille, mikäli jokin miksi kysymyksen vastauksista voisi auttaa tätä suhdetta niin lohkoketju voisi olla hyvä ratkaisu tähän. [Felin & Lakhani 2018].

Lohkoketjun käytön keskipiste ei ole sovelluksessa itsessään vaan se mahdollistaa olemassa olevien työvaiheiden jäljitettävyyttä ja läpinäkyvyyttä. Sen sijaan, että yrityksen miettisivät, että miten lohkoketjua voi käyttää tulisikin miettiä, että mitkä yrityksen yhteistyössä tapahtuvat prosessit kaipaisivat parannusta, ja miten lohkoketju voisi parantaa luottamusta ja tehokkuutta tällä osa-alueella. [Kilroy 2019]

Lohkoketjuja on hyödynnetty niin julkisella kuin yksityisellä puolella. Lohkoketjuissa on todettu, että ne ovat olleet hyödyllisiä toimitusketjuissa ja siinä, että immateriaalioikeuksista palkkiot menevät ensisijaisesti niiden tekijöille [Lacity & Van Hoek 2021]. Lohkoketjuja on hyödynnetty myös julkisella puolella, koska niiden avulla on mahdollista vähentää byrokratiaa ja korruptiota. Korruptiota se pystyy vähentämään tekemällä datasta paremmin paikkaansa pitävää ja vähentämällä dataan liittyvää hierarkiaa, jolloin datan läpinäkyvyyttä on mahdollista parantaa. [Kassen 2022] Luotettavampi data puolestaan on johtanut siihen, että voidaan rakentaa parempia tietojärjestelmiä, joiden avulla hallinnon automatisointi on mahdollista.

Perinteisten julkisen ja yksityisen puolen lisäksi älysopimukset ovat luoneet uudenlaista liiketoimintaa hajautettujen organisaatioiden ja hajautettujen sovellusten muodossa. Niitä hyödynnetään erityisesti finanssipalveluissa, joista puhutaan hajautettuina rahoituspalveluina, mutta myös pelialalla tai muissa vapaa-ajan sovelluksissa. Kyseessä on kuitenkin vain toiminnallisuus hajautetussa tietokannassa. Lohkoketjuissa ja älysopimuksissa on siis vain kehittäjien mielikuvitus rajana siinä mihin niitä halutaan käyttää. On kuitenkin syytä pohtia, että onko niistä saatavilla hyötyä, vaikka sen voisi toteuttaa.

Nykyiset yrityskäyttöön tehdyt lohkoketjut eivät juurikaan muokkaa nykyistä liiketoimintaa, mutta niiden avulla on onnistuttu vähentämään kitkaa ekosysteemin partnerien välillä. Yritysten välisiin lohkoketjuihin on tullut uusia kolmansia osapuolia kuten lohkoketjujentarjoajat, joten konsortiot eivät yleensä kehitä niitä täysin keskenään. Usein yrityskäyttöön tehdyt lohkoketjut toimivat suljetussa lohkoketjussa. Tarkoittaen sitä, että toimijoilla on tarkat roolit ja datan omistajuus. Saavutettu hyöty suljetusta lohkoketjusta on se, että se toimii nopeammin kuin avoin ja sitä voidaan hallita helpommin. [Lacity & Van Hoek 2021]

Onnistuneita käyttöönottoja yrityskäytön lohkoketjuissa on yhdistänyt liiketoimintalähtöinen yhteistyö käyttöönottajien kesken, jolloin on onnistuttu tarjoamaan koko ekosysteemiä hyödyttävä ratkaisu. Lohkoketjun avulla on pystytty luottamaan muuttumattomaan dataan, vaikka kaikkea dataa ei jaeta yhteistyökumppaneille. Esimerkiksi IBM:n Aaron Lieber TradeLenssin hallinnosta sanoo, että lohkoketjun datamäärät on pidetty pieninä, ja usein pelkkä tiiviste ollut riittävä. Tiivisteen perusteella voidaan hakea muu data ohjelmiin. TradeLens on tanskalaiselle Maersk rahtilaivayhtiölle toteutettu lohkoketjupohjainen sovellus, jonka avulla onnistuttiin parempaan ja halvempaan konttien seurantaan. Projekti digitalisoi toiminnan paperittomaksi ja vähensi hallinnointikuluja. [Lacity & Van Hoek 2021]

Muita sopivia käyttötarkoituksia on löydetty myös sotateollisuudesta, sillä myös sotilasvallat kuten Kiina, Venäjä ja Nato ovat ottaneet lohkoketjuteknologian käyttöön omissa tietojärjestelmissään. Lohkoketjun hajautettu rakenne pystyy turvaamaan myös poikkeusoloissa datan säilymisen, joten siinä on nähty korkea arvo sotateollisuudessa. [Kassen 2022]

Seuraavaksi tutustutaan esimerkkeihin lohkoketjujen mahdollisuuksista liiketoiminnassa. Ensimmäinen esimerkki on IBM Food Trust -lohkoketju, jota käytetään ruuan toimitusketjussa. Se on yksityinen lohkoketju, jota käytetään usein esimerkkinä myös monissa julkaistuissa tutkimuksissa. IBM Food Trust on esimerkki siitä, että perinteinen liiketoiminta ei lohkoketjun myötä muutu kovinkaan paljoa. Käytän tässä esimerkissä aiemmin esiteltyä Felinin ja Lakhanin [2018] mallia, jonka avulla yritykset voivat luoda omaa lohkoketjustrategiaansa. Toinen esimerkki puolestaan kertoo siitä, että minkälaista liiketoimintaa julkisiin lohkoketjuihin on syntynyt. Aave on merkittävä lohkoketjuihin hajautetun rahoitusalan toimija, joka haastaa perinteistä pankkitoimintaa. Nämä ovat hyvin erityyppisiä esimerkkejä, ja niiden avulla pystytään kuvaamaan miten merkittävästi erityyppisiä ratkaisuja julkiset ja yksityiset lohkoketjut tarjoavat.

4.1 Yritysten lohkoketjut ja IBM Food Trust

IBM Food Trust on erinomainen esimerkki siitä, miten lohkoketju vaikuttaa yritysten liiketoimintaan, ja miksi se on haluttu ottaa käyttöön. Se on ruuantoimitusketjuun käytettävä suljettu lohkoketju. Siinä on mukana omina noodeinaan Walmart ja Kroger, jotka ovat molemmat suuria yhdysvaltalaisia vähittäiskauppaketjuja. [Kilroy 2019] Kilpailijat eivät halunneet mukaan Wallmartin lohkoketjuun, vaikka Wallmartin toimitusketjun jäljitys olisi toiminut muissa vähittäiskaupoissa samalla tavalla. Tästä syystä lohkoketjukehittäjä IBM sai puolueettoman osapuolen tittelin itselleen. Puolestaan mukana toimivat yritykset muodostavat neuvoa antavana konsortion. [Lacity & Van Hoek 2021].

IBM Food Trustin käyttämä teknologia on IBM Blockchain Platform ja Hyperledger Fabric. Ne ovat suljettuja lohkoketjuteknologioita, joissa on rajattu näkyvyys datasta. Rajattu näkyvyys tarkoittaa sitä, että kilpailijat eivät näe kaikkea dataa toistensa transaktioista tai kenen kanssa nämä suorittavat transaktioita. Mikäli kuitenkin jossakin elintarvikkeiden erässä on jostakin syystä riski sairastua ruuan laadusta johtuviin sairauksiin IBM Food Trustin avulla molemmat pystyvät saamaan tiedon saman järjestelmän kautta. Ennen Foodtrustia näissä tapauksissa esimerkiksi mangoerien selvitykseen meni usein noin viikko, kun taas Foodtrustin kautta tieto on saatavilla alle kolmessa sekunnissa. [Kilroy 2019] Epäillyt huonot erät ovat myyntikiellossa selvitystyön ajan molemmilla kauppaketjuilla, kunnes huono erä löytyy ja saadaan lisättyä hävikkiin. Viikon selvityksessä usein myös osa hyvästä erästä saattaa joutua hävikkiin sen seisotuksen vuoksi.

Seuraavaksi vastataan Felinin ja Lakhanin [2018] aiemmin esitellyn mallin mukaisesti käyttäen IBM Food Trustia esimerkkinä. Miksi siis IBM Food Trust tehtiin? Haluttiin parantaa ruuan jäljitettävyyttä ja tehostaa prosesseja virheellisten erien löytämiseksi. Teknologialla siis helpotetaan laadun seurantaa. Mitä arvoa laadun seurannalla on? Se viestii yrityksen vastuullisuudesta ja ylläpitää mainetta. Sen lisäksi sillä on myös taloudellinen hyöty, kun prosessit tehostuvat. Entä kenelle tätä ruuan jäljitettävyyttä tehdään? Ensisijaisesti tulisi varmasti miettiä, että yritykselle itselleen, jotta toiminta tehostuu, mutta myös asiakkaille, jotta nämä eivät sairastu ja tästä ei aiheudu mainehaittaa. Toisaalta parempi järjestelmä helpottaa myös työntekijöitä ja viranomaisia, jotka valvovat elintarvikkeiden laatua.

4.2 Julkiset lohkoketjut ja Aave

Aaveesta ei vielä ole juurikaan tutkimusjulkaisuissa ollut puhetta, mutta esittelen sen hyödyntäen Aaveen perustajan Stani Kulechovin [2021] haastattelua Nordnetin #rahapodi-podcastissa ja Aaveen toiminnassa mukana olleen Martin Wichmanin [2021] haastattelua Lohkoketju-podcastissa. Protokollan historiasta on löytynyt lohkoketjuihin liittyvältä Youtube-kanavalta nimeltä Finematics. Aave on suomalaislähtöinen organisaatio, mutta toimii nykyisin Lontoosta. Se on tällä hetkellä arvossa mitattuna toisiksi suurin DeFi alusta. [Kulechov *et al*. 2021]

DeFi (*Decentralized Finance*), eli hajautettufinanssiala on lohkoketjujen päälle rakennettu toimiala, jossa pankkipalveluja tarjotaan älysopimusten kautta. Älysopimusten ja lohkoketjun avulla yksityishenkilöt toimivat lainanantajina pankkien sijaan ja näin ollen voivat itse määrittää mihin lainan hintaan tyytyvät. Tämä haastaa perinteisiä liiketoimintamalleja ja mahdollistaa uudenlaisen kilpailun pankkitoimialalle. DeFi toimii suoraan ylikansallisesti, joten lainanhakija ja lainanantaja voivat hyvin olla eri mantereilla.

Tämä on erittäin suuri ero verrattuna perinteiseen pankkisektoriin, jossa asiakkaat toimivat yleensä samassa valtiossa, jotta riskien määrittäminen onnistuu helpommin. [Wichman & Kurimo 2021]

Hajautetun finanssinalan toimija Aave on julkisissa lohkoketjuissa kuten Ethereumissa toimiva hajautettu organisaatio ja protokolla, joka toimii älysopimuksen avoimen lähdekoodin varassa [Kulechov *et al*. 2021]. Aave on perustettu alkujaan 2017 nimellä ETHLend, joka tarjosi lainapalveluja vertaisverkossa (*Peer to peer - P2P*) käyttäjien välille. Se oli alkujaan P2P-lainapalvelu älysopimuksen avulla, mutta siinä oli ongelmia, kun lainaajia ja lainanhakijoita oli eri määrä. P2P muutettiin myöhemmin käyttäjien ja älysopimuksien väliseksi (*Peer to contract - P2C*) protokollaksi, jolloin lainan saanti helpotti. P2C:ssä lainanantajat ”poolitetaan” eli yhdistetään yhdeksi lainanantajaksi, jolloin selvitään siitä, että ei tarvita suoraan yhtä lainanhakijaa yhtä lainanantajaa kohden. Muutoksen yhteydessä nimi muutettiin Aaveeksi. [Finematics 2021]

Aave haki kasvun yhteydessä kansainvälistä rahoitusta ICO:n avulla, antamalla ulos annin Aave-rahakkeista [Finematics 2021]. Aave-rahakkeita vaaditaan Aaveen DAO-toimintaan osallistumiseen. DAO-toimintaa ovat äänestäminen uusista muutoksista Aave-protokollaan Aaveen verkkosivuilla. Samoin uusia muutoksia ehdottavat joutuvat takaamaan rahakkeilla ehdottamiaan muutoksia, jotta saadaan vakuus älysopimuksessa, mikäli muutoksesta koituu tappioita. [Kulechov *et al*. 2021] Aave-rahakkeesta voi ajatella, että ne ovat käytännössä kuin osakkeita Aaveesta, sillä itse rahakkeilla on myös oma volatiliteettinsa erilaisissa kryptopörsseissä.

Kun Aaveen likviditeettiä kasvatetaan, niin sillä on enemmän lainattavaa rahaa tarjolla. [Kulechov *et al*. 2021] Aaveen likviditeetti on 2022 huhtikuussa 21,5 miljardia USA:n dollaria, kun likviditeetti käännetään kryptojen markkinahinnasta dollareihin [Aave.com 16.4.2022]. Aaveen likviditeettiä kasvatetaan kahdella tapaa. Ensimmäinen on, kun käyttäjät tarjoavat suoraan lainaa jossakin kryptovaluutassa. Toinen on ”steikkaaminen” eli takauksen tarjoaminen Aave-protokollalle, jolloin takaaja saa vakuutena Aave-rahakkeita. Lainan ja takauksen tarjoamisesta saa vuosittain tasaisen koron sinne sijoitetusta kryptovaluutasta.

Aaveen palveluihin pääsee käsiksi suoraan yhdistämällä oma kryptolompakkonsa Aaveeseen Aaveen verkkosivujen kautta. Käytännössä kirjautuminen tapahtuu avoimen lohkoketjun lompakolla, joka on selaimen lisäosa. [Wichman & Kurimo 2021] Lainan hakeminen Aaveessa onnistuu juuri verkkosivujen kautta. Usein takaukseksi vaaditaan suurempaa digitaalisen omaisuuden arvoa kuin Aaveen kautta tarjotaan asiakkaalle. Idea tässä on se, että takaus kattaa lainan, jos lainan ehtoja ei noudateta. Aave toimii siten, että se tarjoaa mahdollisuuden vaihtaa omia kryptovaluuttojaan toisiin kryptovaluuttoihin ilman välikäsiä [Kulechov *et al*. 2021]. Lainan avulla kryptovaluutoilla on helpompi

tehdä maksuja ilman, että maksun yhteydessä tulisi maksaa kryptovaluutan vaihdosta koituvaa pääomatuloveroa. Toinen syy on, että lainan hakija tarvitsee toista kryptovaluuttaa lyhytaikaisesti. Sitä voidaan tarvita esimerkiksi ”steikatakseen” eli taatakseen toisessa lohkoketjussa tai protokollassa. [Finematics 2021]

Aaveessa puolestaan vaaditaan merkittävä määrä takausta, jotta lainan haku onnistuu. Tällöin myös lainan riski on myös huomattavasti pienempi lainanantajalle. Riski siirtyy kuitenkin teknologian avulla pankilta yksityishenkilölle. Viimekädessä uudet teknologiat kuten Aave ovat täysin riippuvaisia siitä, että ovatko käyttäjät valmiita ottamaan käyttöön tämän tyyppisiä uusia innovaatioita.

5 Lohkoketjujen skaalautuvuuden trilemma

Trilemman avulla voidaan selittää mikä on ollut lohkoketjujen suurin este läpilyönnille suurelle yleisölle. Sen avulla voidaan myös selvittää, miksi jotkin lohkoketjut ovat tehottomia ja paljon energiaa vieviä. Skaalautuvuuden ongelmat ovat johtaneet siihen, että vaikka suuri yleisö haluaisi käyttää lohkoketjupohjaista arkkitehtuuria, niin teknologiana se ei olisi riittävän tehokas toimimaan, jos siinä olisi moninkertainen määrä käyttäjiä. Tästä on hyvänä esimerkkinä Bitcoin, joka toimii aiemminkin sijoitusinstrumenttina kuin maksuvälineenä. Bitcoinissa on hitaat ja kalliit transaktiot, joten se ei sovellu hyvin maksuvälineeksi pienissä ostoksissa.

Lohkoketjujen skaalautuvuuden trilemma (*Buterin's Scalability Trilemma*) [Altarawneh *et al.* 2020, Mogavero *et al.* 2021] on Ethereum-lohkoketjun perustajana tunnetun Vitalik Buterinin esiin tuoma lohkoketjujen skaalautuvuuteen liittyvä ongelma. Lohkoketjujen skaalautuvuuden trilemma on se, että jokaisessa lohkoketjujen konsensusalgoritmissa tasapainotellaan tietoturvallisuuden, skaalautuvuuden ja desentralisaation suhteen. Syy miksi tämä on haasteena lohkoketjuissa, on se, että jokaisen noodin pitää pysyä samassa tahdissa ja yhteisymmärryksessä eli konsensuksessa transaktioista muiden noodien kanssa [ETH-wiki].

Trilemmaa on yleinen aihe lohkoketjututkimuksissa ja siihen onkin löytynyt joitakin ratkaisuja. Näissä tutkimuksissa on usein todettu, että ongelman mallia tulisi jatkaa uusilla muuttujilla. Esimerkiksi Lin ja Qiang [2018] kirjoittavat trilemman muotoon, että lohkoketjuissa haaste on saada niistä samanaikaisesti tietoturvallisia, skaalautuvia ja läpinäkyviä. Mogavero ja muut [2021] kirjoittavat, että trilemmasta tulisi puhua aiemminkin quadliremmana, sillä se ei huomioi laskentatehoa. He myös nostavat esiin, että muissa tutkimuksissa neljänneksi muuttujaksi on ehdotettu sääntelyä, lohkoketjun geneerisyyttä, yksityisyyttä [Mogavero *et al.* 2021]. Kaikissa versiossa on kyse kuitenkin siitä, että kun lohkoketjusovelluksen konsensusalgoritmia toteutetaan niin jokin näistä muuttujista jää pullonkaulaksi. Syy sille miksi lohkoketjuissa skaalautuvuus on haasteena, on se, että tavallisen noodin laskentatehossa tulee yläraja vastaan ja kun konsensus- ja varmennusalgoritmeja tekee varmemmiksi niin ne usein muuttuvat myös laskentateholle raskaammiksi. Kun osa noodeista tippuu pois laskennasta niin myös lohkoketjun desentralisaatio laskee. Isossa osassa algoritmeista turvallisuus on riippuvainen siitä, että mitä enemmän lohkoketjussa on toisistaan riippumattomia käyttäjiä niin sitä todennäköisemmin suurin osa pyrkii toimimaan rehellisesti, jolloin tietoturva paranee.

Equilibrium-nimisen lohkoketjuja kehittävän yrityksen ja Coinmotion-nimisen krypto-pörssin perustaja Päivinen [2021] puhuu Lohkoketju-podcastin haastattelussa, että desentralisaation, turvallisuuden ja nopeuden välille tulisi löytää tasapaino, joka on kyseiseen sovelluskäyttöön oma optimaalinen määrä. Tähän vaikuttaa erityisesti lohkoketjun käyttötarkoitus ja sen käyttäjät, jolloin voidaan miettiä myös, että kuka transaktioita

validoi. Ei siis ole tarvetta pyrkiä samaan tasapainoon trilemman osa-alueissa esimerkiksi rahaliikenteessä ja pelien sisällä. Yhdistelmän saavuttaminen ollut haasteena lohkoketjujen alusta asti.

5.1 Desentralisaatio, skaalautuvuus ja turvallisuus

Lohkoketjujen skaalautuvuuden trilemman kolme osa-aluetta ovat siis desentralisaatio, skaalautuvuus ja turvallisuus. Desentralisaation avulla lohkoketjuissa pyritään puolueettomuuteen. Alkuperäisissä lohkoketjuissa se on viety äärimmilleen, mutta nykyisin on huomattu, että se hankaloittaa lohkoketjujen skaalautumista huomattavia määriä. Voidaan ajatella, että desentralisaation avulla on voitu demokratisoida päätöksentekoa, mutta nyt kun käyttäjäkunta on kasvanut niin suureksi, että jokaiseen muutokseen demokraattisen päätöksen saaminen sovelluskehityksessä hankaloittaa sitä. Tarve olisi nyt vastaava kuin länsimaisissa yhteiskunnissa käytössä olevassa edustuksellisessa demokratiassa, jonka ansiosta tavallisen kansalaisen ei tarvitse osallistua viikoittain kansanäänestyksiin uusista laeista vaan sen hoitaa edustaja, jonka kansa on sinne valinnut. Lohkoketjut alkavat olla siinä mittaluokassa, että suora demokratia ei ole paras ratkaisu vaan edustuksellinen voi olla parempi.

Buterin [2017] jakaa hajautuksen kolmeen osaan, jotka perustuvat arkkitehtuurin, päätäntävaltaan ja logiikkaan. Arkkitehtuurilla hän viittaa lähinnä fyysisiin laitteisiin. Laitteiston hajautuksella Buterin [2017] tarkoittaa, että lohkoketjujen tulisi tukea mahdollisimman paljon erilaisia laitteita eikä vaatimuksena lohkoketjun ylläpidosta tulisi olla tietynlainen supertietokone tai tietyn valmistajan prosessori tai esimerkiksi ASCII-tietokone. Päätäntävallalla Buterin [2017] viittaa päätöksenteon rakenteisiin, ja että päätöksien tulisi olla demokraattisia ja geologisesti hajautettuja. Tämä turvaisi lohkoketjua siltä, että sen päätöksenteossa mietittäisiin tarpeeksi erilaisia näkökulmia, ja että se olisi puolueetonta.

Loogisella hajautuksella puolestaan tarkoitetaan sitä, että, jos koko toiminnan jakaisi osiin niin voisiko toiminta jatkua samanlaisena ilman häiriöitä vai kaatuisiko se, kun jokin tietty osa poistuu. Looginen hajautus on Buterinin [2017] mukaan verrattavissa kieleen, sitä ei kukaan voi ottaa toiselta pois ja yhteinen kieli säilyy, vaikka vähän aikaa olisi ollut toisen kielisessä maassa, jossa muut eivät sitä ymmärrä. Tämän tyyppinen hajautus olisi Buterinin [2017] mielestä tavoiteltavaa kaikissa hajautetuissa sovelluksissa, sillä se ylläpitää sovelluksen resistenssiä muutoksille, vaikka esimerkiksi yhdessä maassa sovellus haluttaisiin sulkea pois markkinoilta kokonaan. [Buterin 2017] Hajautus tulisi siis ymmärtää laajempana kokonaisuutena, jota tulisi varjella kehittäjien mielissä myös tulevaisuudessa.

Lohkoketjujen skaalautuvuudella tarkoitetaan erityisesti transaktioiden määrää sekunneissa. Mitä enemmän käyttäjiä on, sitä suurempi määrä transaktioita sen tulee pystyä

käsittelemään. Kun lohkoketju transaktio lähetetään suoritettavaksi, siitä tulee ensin kandidaattitransaktio ennen kuin se hyväksytään lohkoketjuun. Kandidaattitransaktion hyväksyntä validoidaan ennen kuin sitä voidaan lisätä uuteen lohkoon. Myös, kun lohko luodaan, se tulee vielä validoida ennen kuin transaktio menee läpi. Tässä prosessissa menee useimmissa julkisissa lohkoketjuissa minuutteja.

Hankaluutta tähän prosessiin tuo se, että yhden lohkon koko on rajattu. Esimerkiksi Bitcoinin tapauksessa lohkon koko 1MB [Buterin & Fridman 2021]. Tämä aiheuttaa transaktiokaton, sille että kuinka monta transaktiota yhteen lohkoon mahtuu. Sen lisäksi validoinneissa tietoa siirretään lohkon luojalta sitä validoiville noodeille, jotka toimivat ympäri maailmaa, jolloin tiedonsiirroissa on viivettä (*latency*). Viivettä voisi pienentää rajaamalla lohkoketjua maantieteellisesti, mutta se heikentäisi desentralisaation tasoa.

Transaktioon liittyy siis useampia osapuolia. Nämä osapuolet ovat lohkon louhijat, validoijat ja käyttäjät. Lohkoketjussa yksi osapuoli voi olla näitä kaikkia samanaikaisesti, mutta niitä on myös erotettu toisistaan, jotta niiden käyttö ei vaatisi niin paljon laskentatehoa laitteilta. Erityisesti transaktioiden louhijoilla ja transaktioiden suorittajilla on vastakkaiset tavoitteet transaktioiden hinnan suhteen. Louhijat usein haluaisivat paremman korvauksen ylläpidostaan, kun taas käyttäjät mahdollisimman vähän käsittelykustannuksia. [Jiang *et al.* 2022]. Tämä on kuitenkin johtanut siihen, että transaktiokustannukset nousevat varsinkin ruuhkaisina aikoina ja suuremmalla validointipalkkiolla saa nopeammin transaktionsa läpi [Mogavero *et al.* 2021]. Ethereumissa transaktiot suoritetaan Ether-nimisellä krytpovaluutalla, mutta transaktioiden yhteydessä käytetään virtuaalivaluuttaa nimeltä Gas (*Kaasu*). Gas-transaktiot suoritetaan lohkoketjua ylläpitäville noodeille. Transaktiokatto aiheuttaa sen, että osa transaktioista jää suorittamatta, jolloin ne eivät tallennu. Tallentamatonta transaktiota tulee yrittää tallettaa uudelleen, ja varmemmin sen saa läpi, kun tarjoaa enemmän Kaasua ylläpitäjille [Fekete & Kiss 2021].

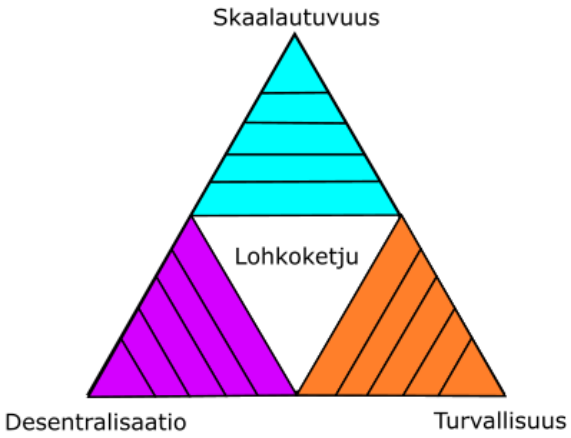
Lohkoketju algoritmeissa on alkujaan pyritty suuremmissa määrin ylläpitämään niiden turvallisuutta laskennallisin ja algoritmisin keinoin ilman kolmatta osapuolta. Kun lohkoketjuissa ei ole kolmatta osapuolta niin on ajateltu, että se ei ole aiheuttamassa niissä ennalta arvaamatonta riskiä yllättävällä käytöksellään. Toisaalta tällöin ei myöskään ole tahoa, joka voisi korjata virhetilanteet jälkikäteen. Lohkoketjujen turvallisuuteen on pyritty kryptauksessa käytettävillä avainpareilla, kaiken auditoitavuudella ja läpinäkyvyydellä.

Lohkoketjujen turvallisuuteen liittyviä uhkia, joihin lohkoketjujen algoritmeissa on pyritty vastaamaan ovat palvelunestohyökkäykset, Sybil-hyökkäys, Byzantine-toleranssi ja kaksinkertainen rahankäyttö. Sybil-hyökkäys, on tietojärjestelmissä tapahtuva hyökkäys, jossa hyökkääjä käyttää useampaa identiteettiä omaan tarkoitukseensa esimerkiksi äänestykseen [Bamakan *et al.* 2020]. Byzantine-toleranssi puolestaan tarkoittaa, että jär-

jestelmä kestäisi, vaikka osa noodeista huijaisi [Altarawneh *et al.* 2020]. Tavallisin huijausyritys on transaktioiden muuttaminen jälkikäteen, jossa pyrkimyksenä on huijata itselleen enemmän varoja. Tämän tyyppisiin hyökkäyksiin lohkoketjuissa on varauduttu antamalla päätäntävalta noodien laskentatehon enemmistön mukaan. Teoriassa oletetaan, että alle puolet laskentatehon noodeista olisi huijareita, joten huijauksista ei päästä konsensukseen. Laskentatehon enemmistön käyttäminen suunnannäyttäjänä ei kuitenkaan ole täysin aukoton, mutta mitä laajempi lohkoketjuverkostosta tulee sitä hankalammin huijausyritykset onnistuvat.

Yksi merkittävä turvallisuuteen liittyvä ominaisuus on se, että miten hyvin lohkoketju selviää, vaikka osa noodeista lopettaisi lohkoketjussa toimimisen tai se kohtaisi palvelunesto hyökkäyksen. Tähän auttaa se, että lohkoketjut ovat hajautettuja, jolloin vaikka hyökkäys tapahtuisi osaan noodeista, niin se ei kuitenkaan estäisi lohkoketjun käyttöä muissa noodeissa. Tässä tulee huomioida myös se, että miten hyvin lohkoketjusta poistuminen ja siihen palaaminen onnistuu. Altarawneh ja muut [2020] käyttävät tästä termiä Crash-toleranssi. Siihen vaikuttaa esimerkiksi, se että kuinka keskitettyä lohkojen louhinta on.

Aiemmista kryptovaluutoista erottava ominaisuus Bitcoinissa oli Double-spending-ongelman ratkaiseminen [Nakamoto 2008]. Virtuaalirahoja on ollut käytössä jo 1990-luvulta monissa virtuaaliympäristöissä kuten peleissä [Rantala 2018a]. Double-spending-ongelma oli ennen Bitcoinia digitaalisia valuuttoja vaivannut ongelma, jossa sama raha onnistuttiin käyttämään useampaan kertaan eri transaktioissa. Monissa lohkoketjuissa tämä on estetty niin, että yhden lohkon aikana sama raha ei voi siirtyä kuin yhdessä transaktiossa. Tähän se käyttää konsensusalgoritmeja, jossa muissa noodeissa transaktiot tarkistetaan ennen niiden hyväksyntää. Ongelman ratkaisemiseksi lohkoketjuissa ei ole käytössä datan poistoon ja päivitykseen liittyviä operaatioita vaan mahdolliset korjaukset tulee suorittaa uusina transaktioina. Tämä johtuu siitä, että tilikirjassa oleva data on muuttumatonta.



Kuva 1. Trilemman kolmion osa-alueet.

Kuvassa 1 on trilemman osa-alueet kuviona, jossa kaikki osa-alueet on maksimoitu. Kuvan mukainen painotus on optimaalinen lohkoketju, jossa trilemma on ratkaistu. Tutkielmassa käytetään vastaavaa kuviota myöhemmin antamaan suuntaa siitä, että miten eri osa-alueisiin on painotettu eri konsensusalgoritmeissa ja pilvipalveluiden tarjoamissa lohkoketjuissa.

5.2 Yleisimmät konsensusalgoritmit

Seuraavaksi käyn läpi lyhyesti kolme yleisintä konsensusalgoritmia ja miten ne painottavat trilemman osa-alueita. Konsensusalgoritmeja on siis useita erilaisia, mutta käytännössä kaikissa niistä joudutaan miettimään trilemman kaikkia kolmea muuttujaa. On siis monia erilaisia konsensusalgoritmeja ja niissä voidaan olla päädytty hieman erilaisiin ratkaisuihin. Eri konsensusalgoritmeissa noodeille voidaan tarjota myös hieman erilaisia rooleja.

Julkisissa lohkoketjuissa on yleisesti priorisoitu eniten tietoturvaa ja niiden skaalautuvuus on usein jäänyt vähemmälle huomioille [Lin & Qiang 2018]. Lohkoketjujen läpinäkyvyyteen on pyritty mahdollisimman hyvällä desentralisaatiolla ja transaktioiden varmennettavuudella. Tietoturvaan ja luotettavuuteen lohkoketjuissa on pyritty varmennusalgoritmeilla. Näiden tekijöiden yhdistelmästä usein skaalautuvuus on kärsinyt.

Suljetuissa lohkoketjuissa skaalautuvuuden ratkaisu on löytynyt jo sillä, että kuka tahansa ei saa liittyä lohkoketjuun. Näin lohkoketjun koko pysyy hallittavissa ja skaalautuvuus ei aiheuta niin suuria haasteita. Tarjoamalla lohkoketjua rajatulle käyttäjäkunnalle on epärehellisten käyttäjien riski pienempi, sillä lohkoketjuun osallistuminen vaatii sen, että ainakin osa käyttäjistä tuntevat toisensa. Luottamusta järjestelmään voidaan rakentaa käyttäjien välisen luottamuksen kautta. Tämä on johtanut siihen, että tietoturvaa varmentavia varmennus- ja peliteoreettisia-algoritmeja on kevennetty tai osasta niistä on luovuttu kokonaan. Usein myös hajautuksen tasossa voidaan joustaan yksityisissä lohkoketjuissa, jos sovelluskehitys on ulkoistettu, joten mitään trilemman osa-alueista ei tarvitse viedä äärimmilleen. Näin myös transaktionopeudet ja sähkönkulutus ovat aivan eri mittaluokassa kuin julkisissa lohkoketjuissa, kun turvallisuutta ylläpitävää laskentaa ei tarvitse suorittaa.

Suljetuissa lohkoketjuissa eli yksityisissä lohkoketjuissa on useimmin käytössä auktoriteettivarmennus (*Proof of Authority - PoA*) konsensusalgoritmina. Siinä uusien lohkojen luonti ja transaktioiden varmennus on keskitetty tietyille noodeille. Tämä konsensusalgoritmi tukee usein hyvin yrityskäyttöä. Siinä on hieman alhaisemmalla tasolla hajautus ja tietoturva, mutta ne usein ovat suorituskyvyltään parempia kuin avoimet lohkoketjut.

Alkuperäinen Nakamoton [2008] Bitcoinin mukana tuoma konsensusalgoritmi on työvarmennus (*Proof of Work - PoW*). Se on parhaiten tunnettu lohkoketjualgoritmi, joka

vaikuttaa merkittävästi Bitcoinin tavoin ihmisten käsityksiin lohkoketjuista. PoW-algoritmissa kaikki louhijat pyrkivät ratkaisemaan matemaattista arvoitusta tiivistefunktion avulla. Arvoituksen vaikeusastetta voidaan säätää vaadittavan tiivisteen pituutta säätämällä ja asettamalla siihen muita laskentaan liittyviä ehtoja. Kun ensimmäinen louhija saa tiivisteen ratkottua, se lähetetään muulle lohkoketjuverkostolle, jossa muut verkoston osat tarkistavat sen. Jos tarkistus menee läpi, niin siitä luodaan uusi lohko, joka sisältää tarvittavat parametrit seuraavan lohkon ratkaisemiseksi. [Bamakan *et al.* 2020] Uuden lohkon luoneelle noodille maksetaan korvaus uutena kryptovaluuttana ja sen vuoksi tätä kutsutaan louhinnaksi. Transaktioiden suorittajat maksavat myös usein jonkin osuuden transaktioiden vahvistuksesta niitä käsitteleville noodeille. Osassa lohkoketjuista louhivat ja ylläpitävät käyttäjät ovat erotettu toisistaan, toisissa puolestaan käyttäjät suorittavat molempia toimenpiteitä.

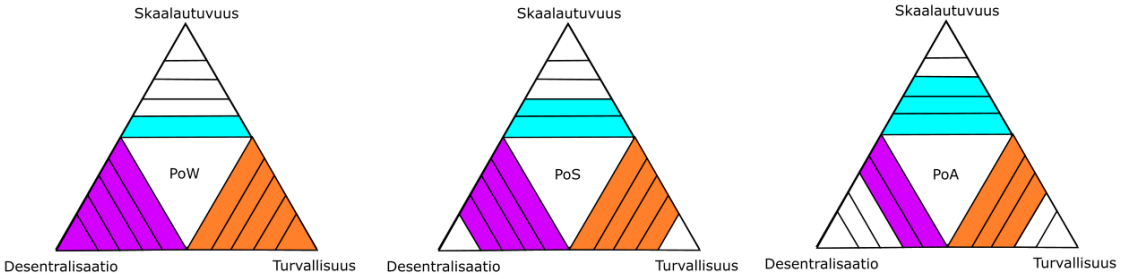
Työvarmennuksen kääntöpuolena on se, että se kuluttaa paljon energiaa ja sen transaktioiden käsittelynopeus on hidas. Se pystyy käsittelemään tyypillisesti alle 20 transaktiota sekunnissa [Lacity & Van Hoek 2021]. Se on erittäin hidas verrattuna esimerkiksi Visaan, joka pystyy käsittelemään jopa 20 000 transaktiota sekunnissa [Bamakan *et al.* 2020].

Bitcoin lohkoketjun ylläpitäminen kuluttaa erittäin paljon energiaa. Vuositasolla määrä on jopa enemmän kuin monella valtiolla. Louhijat usein ajattelevatkin maksavansa lohkoketjun tarvitsemasta sähköstä vaihtoehtoiskustannuksen, jolloin he saavat korvauksen kryptovaluuttana [Heinonen & Tikkanen 2021]. Tästä on seurannut se, että louhintaan on tullut suuria keskittymiä maihin, joissa on edullista sähköä saatavilla [Chow & Peck 2017]. Nykyisin se on myös johtanut siihen, että tavalliset noodien tietokoneet eivät pärjää louhinnassa keskittymille, joissa on käytössä louhintaan kehitettyjä ASCII-tietokoneita [Heinonen & Tikkanen 2021]. Keskittymien ja suuremman laskentatehon vaatimuksen takia desentralisaatio on laskenut, ja siitä on tullut ajan kuluessa yhä keskittyneempää [Lin & Qiang 2018, Mogavero *et al.* 2021].

Korkeaa energiatarvetta on myös perusteltu hyvänä asiana, koska suuri energiatarve tuo kannusteen kehittää parempia energiatuotannon muotoja ja antaa kannusteen myös yksityishenkilöille hyödyntää hukkaenergiaa. Tämä näkökulma nojaa vahvasti juuri libertalistiseen ajatteluun, jossa uskotaan PoW:n ylläpitävän korkeaa hajautuksen tasoa.

Osakkuusvarmennus (*Proof of Stake - PoS*) on nähty todennäköisenä korvaajana PoW:lle. Se vaatii vähemmän laskentatehoa ja siinä vältytään moninkertaiselta laskennalta. Siinä uuden lohkon louhija valitaan sattuman perusteella joukosta, jotka ovat listautuneet halukkaiksi louhimaan. Näin vältytään PoW-algoritmin kilpailusta aiheutuvasta turhasta louhimistyöstä, joten sen energiakulutus on merkittävästi vähäisempi. Kilpailun poistuessa on yhä silti mahdollista, että epärehellinen noodi saisi louhimisoikeuden itsel-

leen. Tämän takia tarkistuksiin menee kuitenkin vielä energiaa ja epärehellisyyden vältämiseksi listautuessa usein vaaditaan vakuus, joka on kryptovaluuttaa. Mikäli louhinnassa muodostuu tiiviste, jota ei hyväksytä muissa noodeissa menee osuus vakuudesta jokaisesta väärästä vastauksesta ja louhijaa voidaan vaihtaa. Tämän uskotaan peliteoreettisesti antavan riittävän kannusteen louhijoille toimimaan rehellisesti. Sen tietoturvallisuutta voidaan kuitenkin pitää alhaisempana kuin työvarmennuksen. Listautuminen yleensä myös maksaa merkittävän summan kryptovaluuttaa ja se voi aiheuttaa sen, että louhinta keskittyy tiettyjen toimijoiden välille. Tästä johtuen osakkuusvarmennus voi johtaa siihen, että rikkaat noodit rikastuvat, ja tavallisten noodien kynnys osallistua louhintaan laskee ajan myötä. Osakkuusvarmennus siis myös laskee desentralisaation tasoa. Osakkuusvarmennuksessa uuden lohkon luojalle palkintona on ainoastaan transaktiokustannukset [Bamakan *et al.* 2020].



Kuva 2. Eri algoritmit trilemman läpi tarkasteltuna.

Kuvasta 2 selviää suuntaa antavasti, että miten aiemmin käsitellyissä konsensusalgoritmeissa on painotettu eri osa-alueisiin. Kuvioita ei voi lukea absoluuttisesti sillä myös eri alustoihin toteutetuissa samannimisissä konsensusalgoritmeissa on vaihteluja. Esimerkiksi työvarmennuksessa on mahdollista joustaa turvallisuudesta useamman asteen verran, jotta skaalautuvuutta voidaan saada enemmän. Toinen huomioon otettava seikka on se, että vaikka skaalautuvuuden saisi käännettyä luvuiksi niin desentralisaation ja turvallisuuden arvioiminen ei ole keskeistä tässä työssä, joten sitä ei ole tehty. Voidaan todeta, että auktoriteettivarmennuksen turvallisuuden taso on alhaisempi kuin työvarmennuksen ja osakkuusvarmennuksen, koska auktoriteettivarmennuksessa turvallisuuden vaatimustaso on myös alhaisempi. Toinen syy miksi turvallisuus laskee, on se, että kun tietyillä noodeilla on enemmän valtaa järjestelmässä niin järjestelmässä on myös selkeämpiä kohteita, joihin suorittaa hyökkäyksiä. Työvarmennuksessa kilpailu uuden lohkon luonnista johtaa siihen että, sen turvallisuus on maksimoitu, mutta se vaatii kaikkein eniten laskenta tehoa. Kilpailu johtaa myös siihen, että suoritettavaa laskentaa menee hukkaan muissa noodeissa paitsi oikean ratkaisun löytäneessä noodissa. Osakkuusvarmennuksessa sen vaatima energiamäärä laskee, koska siinä luovutaan kilpailusta, mutta varmennus uudesta

lohkosta haetaan kuitenkin muilta noodeilta. Puolestaan auktoriteettivarmennuksessa varmennus on keskitettynä niille noodeille, jotka voivat myös lisätä uusia lohkoja, jolloin se vaatii vielä vähemmän laskentatehoa.

5.3 Skaalautuvuuden ratkaisut

Trilemmalle ei ole vielä löydetty konsensusalgoritmeissa yleisesti käytössä olevaa ratkaisua skaalautuvuuteen. Sitä on kuitenkin ratkottu lohkoketjuissa koskematta itse konsensusalgoritmiin. Seuraavaksi käyn lyhyesti eniten esillä olevat keinot vastata skaalautuvuuteen.

Skaalautuvuuden ja transaktioiden suorituskyky määrän nostamiseen yksinkertaisimpana ratkaisuna on ehdotettu lohkon koon kasvattamista, jotta yhteen lohkoon mahtuisi enemmän transaktioita kerralla. Lohkon kokoa kasvattamalla saa helpoimmin tehokkuutta lohkoketjuun, mutta tämä alentaa tietoturvaa. Hajautus on paras keino tietoturvaan lohkoketjuissa ja lohkoketju pyrkii maksimoimaan usein turvallisuutta eikä tehokkuutta. [Jiang *et al.* 2022] Sopivan koon löytäminen on kompromissi sillä isompi koko tarkoittaa, että louhijoiden on helpompi kirjoittaa uusia transaktioita, mutta pienemmästä on validoijien helpompi tarkistaa niitä [Buterin & Fridman 2021].

Lohkon pieni koko on myös todettu johtavan transaktioiden ruuhkautumiseen, jolloin lohkoketjun vaatima muistimäärä kasvaa, joten sitä ei voi nähdä pitkäaikaisena ratkaisuna [Päivinen *et al*. 2021]. Käsiteltävän datan määrän lisääminen johtaa herkästi siihen, että osa lohkoketjuverkoston koneista ei pysy vaadittavassa laskentatehossa perässä. Se johtaa herkästi keskitettyyn ratkaisuun, jossa vain erittäin tehokkaat tietokoneet pystyvät ylläpitämään lohkoketjua. [ETH-wiki] Näin myös riski haarukoitumiselle kasvaa vaadittavan muistimäärän kasvaessa [Lin & Qiang 2018].

Trilemman ratkaisuksi on nähty pääasiassa Layer2, jossa alkuperäisen lohkoketjun päälle rakennetaan uusi kerros lohkoketjuja, joista varmennettua dataa lähetetään lohkoketjuun. Tämän avulla saadaan alkuperäisen lohkoketjun transaktiomääriä pienennettyä. Layer2 siis vähentää alkuperäisen lohkoketjun desentralisaatiota, mutta näissä on huomioitu se, että lohkoketjuissa tulisi löytää optimaalinen määrä desentralisaatiota, turvallisuutta ja nopeutta.

Layer1 on siis alkuperäinen lohkoketju kuten Bitcoin tai Ethereum. Layer2 on puolestaan sovellus tai älysopimus, joka palautuu takaisin alkuperäiseen lohkoketjuun. Datan palautukseen tasojen välille on kehitetty niin kutsutut kuitit (*rollup*), jotka ovat kuitteja Layer2:lta Layer1:lle. [Päivinen *et al.* 2021] Layer2 tarve on perusteltu myös sillä, että se laskee transaktioiden hintaa, sillä Layer1-tasolla on maksimimäärä transaktioita, jotka mahtuvat yhteen lohkoon. Transaktioiden hinta nousee, koska transaktioiden houkuttelevuutta voidaan kilpailuttaa tarjoamalla korkeampaa kaasun hintaa. Näin transaktiokustannukset voivat kasvaa useisiin kymmeniin euroihin.

Käytännössä kuitit ovat on useamman käyttäjän lompakkoja, jonka sisällä käyttäjät saavat suoritettua keskenään transaktiot, ennen päälohkoketjuun siirtämistä [Lin & Qiang]. [Päivinen *et al*. 2021]. Yleisimmät kaksi tapaa palauttaa kuitit takaisin lohkoketjulle ovat optimistinen kuitti (*optimistic rollup*) ja tiedostomaton kuitti (*zero knowledge rollup*) [Päivinen *et al*. 2021]. Niitä pidetään tyypillisimpinä ja potentiaalisimpina skaalautuvuusratkaisuina lohkoketjuille. Haittapuolena useamman käyttäjän lompakoissa on se, että lohkoketjun läpinäkyvyys kärsii, kun osa transaktioista tapahtuu piilossa [Lin & Qiang 2018] samoin myös desentralisaatio. Tämän vuoksi useamman käyttäjän lompakkoihin tarvitaan valvontaa [Lin & Qiang 2018].

Tiedostomaton kuitti (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge - zkSNARK*) sisältää tiivistealgoritmin, jonka avulla voidaan todistaa, että data paikkaansa ilman, että itse data paljastetaan. Paikkaansa pitävyyttä arvioidaan historian ja nykyisen tilan perusteella [ETH-wiki]. Vahvistettu zkSNARK voidaan todentaa tiedostamattoman todisteen (*Zero-knowledge proof - ZKProof*) kautta. Tämän tyyppiset algoritmit ovat kehittyneet erittäin nopeasti sillä vielä kymmenen vuotta sitten nämä olivat vain lähinnä teorian tasolla ja ne vaativat yhä erittäin paljon laskentatehoa [Buterin & Fridman 2021].

Optimistisessa kuitissa oletetaan, että kuitti pitää paikkaansa, kunnes joku haastaa sen petostodisteella (*fraud proof*). Tarkoittaen siis sitä, että niitä tulee valvoa. Usein tämä tehdään automatisoidusti, mutta tarkistusta siis ei ole sisäänrakennettu kuitille. [Päivinen *et al*. 2021] Näiden varmennuksissa käytetään useimmin vakuuksia eli huijauksesta kiinni jäädessään joutuu korvaus velvolliseksi [Buterin & Fridman 2021]. Samoin petostodisteesta-haasteista joutuu tarjoamaan vakuuden, jotta niitä ei väärinkäytetä [Päivinen *et al*. 2021].

Salamaverkko (*Lightning network*) on Bitcoinin Layer2-sovellus, joka tuottaa kuitteja Bitcoinin Layer1-tasolle. Se on esimerkki tässä työssä Layer2-sovelluksesta, jota käytetään useamman käyttäjän lompakon kautta. Sen sisällä on mahdollista toteuttaa jopa yli miljoonia transaktioita sekunnissa. Salamaverkko on järjestelmä, joka toimii verkostossa useamman käyttäjän välillä lohkoketjun ulkopuolella. Lompakossa avataan kanava kahden käyttäjän välille. Kanavaan talletetaan valuuttaa sen verran kuin käyttäjien välillä on tarkoitus siirtää kryptovaluutta. Näin kanavaan sidottua kryptovaluuttaa voidaan siirtää niin monta kertaa kuin halutaan Layer2-sovelluksen sisällä. Käyttäjät maksavat transaktiomaksun ainoastaan liittyessään ja poistuessaan sovelluksesta. Jokaisen käyttäjän välille ei tarvita omaa kanavaa, mutta jokaisella käyttäjällä tulee olla kanava johonkin toiseen käyttäjään. Näin kaksi käyttäjää, joilla ei ole kanavaa auki voi käydä kauppa keskenään verkoston avulla siten, että siirrettävä määrä valuuttaa siirtyy useassa kanavassa aina seuraavalle käyttäjälle. Käytettyjä kanavia suojataan aikalukkojen avulla, joten kesken olevan transaktio ei voi jäädä matkalle väärälle käyttäjälle. Jos transaktio ei mene

perille asti niin tila palautetaan siihen, joka se oli ennen transaktion yritystä. Kun jossakin kohtaa halutaan siirtää varat pois kanavasta niin silloin lohkoketjulle annetaan kanavan nykyinen tila ja siirretään sen mukaan käyttäjien varat näiden omille tileille. Kanavat linkittyvät toisiinsa sipuliverkon tavoin. [Finematics 2019]

Ethereumissa pääasiallisena Layer1 skaalautumisen ratkaisuna on nähty lohkoketjun pirstaloiminen (*sharding*). Siinä jokaisen noodin ei tarvitsisi vahvistaa jokaista transaktioita koko lohkoketjusta, vaan sitä tehtäisiin vain tietyllä osalla koneista. Tämä laskee lohkoketjun turvallisuutta ja desentralisaatiota, mutta parantaa suorituskykyä. [ETH-wiki] Muutoksesta puhutaan nimellä Ethereum 2.0 ja se tulee tapahtumaan vanhan Ethereumin päälle parantaen Ethereumia Layer1-tasolla [Buterin & Fridman 2021]. Työvarmennus hankaloittaa pirstalointia, mutta osakkuusvarmennukseen siinä on saatavilla selkeä ratkaisu. [ETH-wiki] Tästä johtuen konsensusalgoritmiin Ethereum-lohkoketjussa on juuri nyt käynnissä muutos. Siinä pirstaloitu Ethereumin osa palauttaisi varmennetun kuitin oman pirstaleensa transaktioista Ethereumin muille pirstaleille. Tästä johtuen Ethereumiin tuleekin muodostumaan 64 rinnakkaista lohkoketjua, jotka ovat yhteydessä toisiinsa [Buterin & Fridman 2021].

Pirstaloinnin jaottelu olisi mahdollista tehdä maantieteellisesti, koska sen avulla on mahdollista laskea tietoliikenteen viiveestä johtuvaa tehottomuutta. Tästä aiheutuu kuitenkin uusia riskejä, kun käyttäjiä voidaan sulkea osuudesta pois pelkästään sijainnin perusteella. Se esimerkiksi synnyttäisi uusia tietoturvariskejä, ja samoin myös sääntely vaikuttaisi tiettyyn pirstaleeseen todennäköisemmin. [ETH-wiki] Pirstaloinnin on tarkoitus koskea ainoastaan dataa, jota lohkoketjussa on, jotta tietoturva ei laskisi. Pirstaloinnin myötä desentralisaatio laskee ja sitä myötä myös hieman tietoturva. [ETH-wiki].

Muita merkittäviä ratkaisuja, joista puhutaan lohkoketjujen skaalautumisen yhteydessä ovat sivuketjujen (*sidechain*) skaalautumisratkaisut. Niissä alkuperäinen lohkoketju kopioidaan ja otetaan muokattuna käyttöön. Tästä on esimerkkinä Polygon-niminen lohkoketju, joka on rakennettu Ethereumin päälle ja käyttää Ethereumin virtuaalikonetta älysopimuksissaan. Sivuketjut toimivat yleensä myös usean käyttäjän lompakon kautta Layer1 tasolla. Sivuketjut nähdään aiemminkin niin, että niiden avulla voidaan nostaa transaktioiden määrää, mutta ne eivät sinänsä ratkaise muita ongelmia kuin sen, että transaktioita saadaan sisään enemmän kerralla, mutta tästä voi aiheutua suorituskyvyn kanssa ongelmia. [Lin & Qiang 2018]

Esitellyt ratkaisut koskevat siis pääasiassa julkisia lohkoketjuja, joissa skaalautuvuus, tietoturva ja desentralisaatio asettavat omat haasteensa. Vaikka skaalautuvuuden trilemma on alun perin kehitetty lohkoketjujen konsensusalgoritmin arviointiin, on sitä nykyisin hyvä käyttää koko lohkoketjuarkkitehtuurin arviointiin. Itse konsensusalgoritmiin ei ole löydetty trilemmaan ratkaisua, mutta esimerkiksi Ethereum 2.0 on koko lohkoketjun arkkitehtuuria koskeva muutos, jonka uskotaan myös ratkaisevan skaalautuvuuden

trilemman. Eri ratkaisujen yhdistelmällä Layer1 ja Layer2 -tasoilla on oletettu, että Ethereum skaalautuisi järjestelmäksi, joka kestäisi ihmisten jokapäiväistä käyttöä ympäri maailman.

6 Pilvipalveluiden tarjoamat lohkoketjut

Pilvilaskennalla (*cloud computing*) tarkoitetaan informaatioteknologian resurssien kuten laskentatehon, tiedonvarastoinnin tai erilaisten sovellusten tarjoamista pilvipalvelualustan (*cloud service platform*) kautta asiakkaille Internetissä. Niiden hinnoittelu tapahtuu tavallisimmin käytön mukaan (*pay-as-you-go pricing*). Hyötynä siinä on erityisesti se, että se vapauttaa yrityksen investoimasta omiin palvelimiin. Näin vältytään myös niiden ylläpidosta. Hyötynä pilvipalveluissa on se, että yritykset saavat siirrettyä laitteiston ylläpitoon kuluvan osuuden kiinteistä kuluista muuttuviin kuluihin ja tämä tuo toimintaan joustavuutta. Toinen merkittävä hyöty siinä on se, että pilvilaskennan kautta yritys voi ostaa juuri sen verran laskentatehoa ja tilaa kuin se tarvitsee sekä voi skaalata sitä tarpeen mukaan. [AWS Whitepaper 2022] Yrityksen pitäessä huolta omista palvelemistaan palvelimen tehokkuus asettaa usein ylärajan siihen, miten tehokkaasti se pystyy käyttämään resurssejaan, mikä puolestaan voi aiheuttaa haasteita liiketoiminnan kasvaessa. Toisaalta varmuuden vuoksi ostettu liian suuri määrä laskentatehoa tarkoittaa, että yritys ei saa parasta irti omasta investoinnistaan, jos osa laskentatehosta jää käyttämättä. Pilvilaskennan voidaan siis nähdä tuottavan merkittäviä hyötyjä liiketoiminnalle sen mahdollistaman joustavuuden ansiosta.

Pilvilaskennan yleisimmät mallit ovat infrastruktuuri palveluna (*Infrastructure as a Service – IaaS*), alusta palveluna (*Platform as a Service - PaaS*) ja tietokoneohjelmisto palveluna (*Software as a Service - SaaS*). IaaS mallina tarkoittaa sitä, että palveluntarjoajalta käytännössä vuokrataan tai liisataan informaatioteknologia resursseja tai koneita, jolloin asiakasyrityksellä on mahdollisuus keskittyä omaan ydinosaamiseensa enemmän. Vuokratut osat voivat olla virtuaalisia tai fyysisiä mahdollistaen sen, että yrityksen toiminta pysyy ketteränä, jos tarve resursseille on vaihteleva. PaaS puolestaan tarkoittaa, että asiakas vuokraa palvelintilaa niin, että se saa keskitettyä oman palvelunsa palveluntarjoajan alustaan. SaaS puolestaan tarkoittaa loppukäyttäjän käyttämää tietokonesovellusta, jonka se saa käyttöönsä lisenssiä vastaan. SaaS on useimmiten yksi tietokoneohjelma, joka on keskitetty. Ajatuksena on, että kaikki asiakkaat käyttävät tätä samaa tietokoneohjelmaa, jolloin korjaus yhden asiakkaan löytämään ongelmaan korjaa ongelman samalla myös muilta asiakkailta. [AWS Whitepaper 2022]

Blockchain as a Service (*BaaS*) on pilvipalveluiden tarjoama tuote, jossa asiakkaalle tarjotaan lohkoketju, jota pilvipalveluntarjoaja ylläpitää. Blokchain as a Service keskittäytyy pilvipalvelun kautta palveluntarjoajalle, mutta lohkoketjuteknologia voi silti olla hajautettu siinä toimivien yritysten kesken. Tämä on kuitenkin vielä melko uusi teknologia ja BaaS on vielä hajanainen käsite. Sillä voidaan tarkoittaa alustan, joko Infrastructure as a Service, Platform as a Service tai Software as a Servicen tyyppistä lohkoketjupalvelua [Zheng *et al.* 2019]. BaaS-termin takaa löytyy erilaisia sovelluksia, ja sen vuoksi ne

on syytä esitellä. BaaS voi siis tarkoittaa lohkoketjua, joka toimii SaaS sovelluksen taustalla, jolloin palvelun maksajalle ei välttämättä ole edes selvillä käyttäkö tämä lohkoketjua vai ei [Karen 2019]. Silloin kyseessä on SaaS-tason BaaS. PaaS-tason BaaS oli ensimmäinen versio BaaS-arkkitehtuurista ja siitä puhutaan, kun lohkoketju tarjotaan keskitetysti pilven kautta asiakkaalle, ja toimitaan kolmantena osapuolena. BaaS, joka on IaaS voidaan ajatella olevan kyseessä, kun lohkoketju noodit siirretään myös pilveen, jolloin koko lohkoketjuihin liittyvä infrastruktuuri sijaitsee palveluntarjoajan pilvessä. [Song *et al*. 2021] IaaS-tason BaaS on pisimmälle viety keskityksessä ja siinä on pyritty helpottamaan lohkoketjujen kehitystä eniten. Noodien sijoittaminen pilveen on auttanut siinä, että jokainen noodi pysyy ajan tasalla viimeisimmästä lohkoketjun tilasta, sillä BaaS-palveluntarjoajat ovat huomanneet, että monet virhetilanteet ovat usein johtuneet siitä, että noodi ei ole ollut saanut viimeisintä tilaa, joka on konsensuksessa muiden käyttäjien kanssa. [Fekete & Kiss 2021] Tässä työssä BaaS:sta puhuttaessa puhutaan pääasiassa IaaS-tason sovelluksista. Se on nykyisin yleisimmin ymmärretty taso BaaS-lohkoketjuissa, sillä sen avulla voidaan tuottaa kokonaisvaltaisin palvelu asiakkaille.

Monet isot teknologiajätit ovat ottaneet BaaS:n tarjontaansa. BaaS:n avulla voidaan tarjota lohkoketju pilvipalvelussa yrityksille, joiden ydinosaaminen ei ole lohkoketjuteknologiassa. BaaS on kehitetty helpottamaan yritysten toimintaa, jotka haluaisivat ottaa lohkoketjun käyttöön, mutta kokevat teknologian itsenäisen käyttöönoton ja rakentamisen liian työlääksi. [Song *et al.* 2021] Yrityksen kuten IBM, Microsoft, Oracle ja AWS ovat perinteisesti olleet suurimpia tietokantojen tarjoajia. Nämä kaikki toimijat tarjoavat nykyisin pilvipalveluita ja lohkoketjuja. Kaikki nämä perinteisesti tietokantoja tarjoavat yritykset ovat ottaneet omaan tuoteportfolioonsa lohkoketjut. Siihen löytyy helposti vastaus tietokantojen ja lohkoketjujen samasta käyttötarkoituksesta eli datan säilyttämisestä.

6.1 Blockchain as a Service -arkkitehtuuri

BaaS on aina suljettu lohkoketju, jossa konsensusalgoritmina toimii Proof of Authority [Song *et al.* 2021]. Kaikissa lohkoketjuissa on yhteistä hajautus, replikoitu tilikirja, kryptografia ja konsensuksen hakeminen ennen kuin uusia tietueita lisätään lohkoketjuun. Lohkoketju on myös aina Append-only-tyyppinen ja se johtaa siihen, että sen vaatima muistimäärä kasvaa jatkuvasti ja tuottaa hukkaresursseja yhä enemmän ajan kuluessa. [Zheng *et al.* 2019] Append-only tarkoittaa siis sitä, että lohkoketjuun voi ainoastaan lisätä uusia tietueita. Datan ylikirjoittaminen tai poistaminen ei ole mahdollista. Mikäli lohkoketjussa halutaan päivittää tai poistaa vanhoja tietueita niin korjaus luodaan uutena transaktiona nykyiseen lohkoon. Uusia lohkoja muodostuu aina tietyin väliajoin, jolloin tilikirjan nykyiseen tilaan voidaan merkitä poistoja tai päivityksiä, mutta näitä muutoksia ei saada koskaan vietyä vanhoihin lohkoihin. Päivittämällä tilikirjan nykyistä tilaa tallen-

tuu se historiaan ja luo seuraavalle lohkolle datan lähtötilanteen. Tarvittaessa on mahdollista käydä tarkistamassa datan liike ja historia sen tilikirjasta. Datan muuttumattomuuden ansiosta sillä voidaan suojautua petolliselta toiminnalta ja datan tarkastettavuudella saadaan työntekijöitä toimimaan vastuullisemmin. Jo näiden kahden ominaisuuden avulla voidaan saada merkittäviä tehostuksia liiketoimintaan joissakin ympäristöissä [Wan *et al.* 2018].

BaaS-arkkitehtuuri toimii siis pilvessä, ja sitä käsitellään rajapintojen (*Application based interface - API*) kautta. Rajapintojen ansiosta kehittäjien vastuualueita on helppo rajata siten, että kaikkien ei tarvitse tuntea koko koodikantaa tai edes ohjelmointikieltä, jolla rajapinnan takana toimiva sovellus toimii. [Kilroy 2019] Tämä tehostaa projektien kehitystä huomattavasti ja mahdollistaa lohkoketjujen ulkoistamisen palvelun tarjoajille. [Song *et al.* 2021] BaaS helpottaa erityisesti lohkoketjun kehitystä ja käyttöönottoa, koska sen avulla voidaan vähentää teknistä päällekkäisyyttä järjestelmien välillä. Esimerkiksi rajapintojen takana on omat kutsut älysopimuksille ja lohkoketjuun liittymisille. [Zheng *et al.* 2019] Palvelurajapinnan kautta toimiminen mahdollistaa sen, että järjestelmä toimii samoin, kun siinä ei olisi lohkoketjuja. Näin ollen käyttöliittymän kehittäjälle tai loppukäyttäjälle lohkoketjun olemassaolo voi jäädä myös hämärän peittoon [Wan *et al.* 2018].

Pilvipalvelun avulla myös voidaan välttää lohkoketjun eritytymmistä omaksi teknologiseksi saarekseen. [Ma *et al.* 2020] Rajapintojen käyttö helpottaa lohkoketjujen integraatioita myös tietojärjestelmiin kuten yritysten vanhoihin (*legacy*) järjestelmiin. [Wan *et al.* 2018] Varsinkin siinä tapauksessa, jos yritys käyttää jo jotakin pilvipalvelua niin BaaS:n integrointi sen omiin järjestelmiin ei välttämättä vaadi edes suuria muutoksia omiin järjestelmiin tai toimintatapoihin [Kilroy 2019].

BaaS-arkkitehtuuriin liittyy myös vahvasti pilveen talletetut virtuaaliset kontit. Yleisimpiä virtuaalikonttien tarjoajia ovat Docker ja Kubernetes. Konttien ansiosta BaaS-ympäristössä, jokainen organisaatio ei tarvitse omaa laitetta, joka liitettäisiin noodiksi, sillä organisaatio voidaan liittää noodiksi pilvestä omassa Docker- tai Kybernetes-kontissaan [Song *et al.* 2021]. Dockerin ja Kubernetesin avulla lohkoketjujen muutoksien tekeminen helpottuu huomattavasti, kun muutokset voidaan viedä suoraan noodien omiin virtuaalisiinkontteihin [Zheng *et al.* 2019]. Kontit ovat erityisen hyödyllisiä kehittäessä, koska niiden avulla voi ajaa useampaa noodia samanaikaisesti yhdestä järjestelmästä [Kilroy 2019]. Nykyisin jo yli 60 % Ethereumin noodeista sijaitsee eri pilvipalveluiden tarjoajien keskitetyillä palvelimella. Näistäkin lähes puolet pelkästään AWS:n palvelimilla. Tieto perustuu ethernodes.org nimisen sivuston dataan, joka kerää tietoa noodien sijainnista niiden IP-osoitteen perusteella. [Canelis 2019]

Olennainen osa BaaS arkkitehtuuria ovat älysopimukset. Myös älysopimukset voidaan tallettaa omiin kontteihin ja niitä voidaan kutsua sovelluksessa eri vaiheissa. Hajautuksen kannalta on kuitenkin parempi, että älysopimukset talletetaan noodia vastaaviin

kontteihin. Tämä siksi, että älysopimuksen ajaminen onnistuu reaaliajassa, toisaalta tämän ajaminen voisi olla mahdollista myös keskitetysti pilvessä. Etuna siinä, että älysopimus ajetaan lokaalisti, olisi se, että voidaan olla varmoja siitä, että älysopimus on muuttumaton, ja tätä voidaan käyttää konsensuksen yhteydessä. [Ma et al. 2020]

Älysopimuksessa voidaan suorittaa testit aina uutta dataa tai noodeja lisätessä. Älysopimuksissa on syytä olla tarkkana, niiden tietoturvallisuuden kanssa ennen niiden käyttöönottoa, koska niiden muuttaminen jälkikäteen on hankalaa, ja bugeista johtuvat ongelmat voivat johtaa isoihin tappioihin. Tästä syystä testaukseen ja testien analysointiin on syytä panostaa erityisen paljon. [Zheng *et al.* 2019] BaaS soveltuu hyvin Edge-computing ja Cloud-computing alustoihin. Edge-computingissa laskenta tapahtuu lähempänä käyttöä, jolloin saadaan reaaliaikaisia tuloksia. Näin saadaan poistettua datansiirtymisestä johtuvat virheet. [Song *et al.* 2021] On siis käyttötapauksesta kiinni mihin kukin älysopimus kannattaa sijoittaa BaaS-arkkitehtuurissa.

6.2 Miksi siirtää lohkoketju pilveen?

Lohkoketjujen käyttöönotossa on huomattu, että aika menee enemmän teknologian opetteluun kuin itse business-logiikan kirjoittamiseen. Tehokkuuden kannalta olisi kuitenkin parempi, että jälkimmäiseen kuluisi suuriosa ajasta. Erityisesti haasteita kehitystiimeille on luonut kaikkien lohkoketjuun osallistuvien tahojen hallinta ja vikojen korjaus. Tähän on huomattu saatavan helpotusta, kun lohkoketju on lisätty pilvipalveluun. Pilvipalvelun avulla koko lohkoketjuekosysteemistä on saatu kattavampi, sillä sitä on pystytty täydentämään tavallisimmilla pilvipalveluiden ominaisuuksilla. [Zheng *et al.* 2019]

BaaS:ssa palveluntarjoajan tehtävänä on pystyttää lohkoketju ja hallinnoida siihen kuuluvia noodeja. Palveluntarjoaja pitää huolta myös siitä, että lohkoketju toimii riittävän nopeasti pilvipalvelussa, joten se vastaa palvelimen ylläpidon vaatimuksista. Näin asiakkaan ei tarvitse välittää lohkoketjun suorituskykyyn ja infrastruktuuriin liittyvistä ongelmista vaan palveluntarjoaja varmistaa, että resursseja ja kaistaa on varattu riittävästi. BaaS-palvelua käyttävät yritykset voivat siis keskittyä itse business-logiikkaan sen sijaan, että ne käyttäisivät energiaansa lohkoketjujen ylläpitoon. [Song *et al.* 2021] BaaS:ssa palveluntarjoajalle kuuluu, että se hoitaa myös lohkoketjun hallintaan liittyvät toimenpiteet kuten konsensuksen ylläpitämisen, hallinnoi haarukointia, validoi noodit, suorittaa transaktiot, hallinnoi varmuuskopioita ja synkronoi lohkoketjun ulkopuoliset ”off-chain” ja lohkoketjujen sisäiset ”on-chain” tapahtumat keskenään. Osan näistä tapahtumista se saa tehtyä lohkoketjulla itsellään [Zheng *et al.* 2019].

Lohkoketjuja käytettäessä palveluntarjoajan kautta luovutaan ainakin osittain tai kokonaan lohkoketjuteknologian hajauttamisperiaatteesta. Se tekemällä saadaan palvelun

tarjoajasta luotettu kolmas osapuoli, jolloin saadaan ratkaisu aiemmassa luvussa esiteltyyn trilemmaan. Näin lohkoketjuteknologiaan saadaan huomattava määrä lisää tehokkuutta niin, että sen turvallisuus säilyy.

Lohkoketjut kiinnostavat yrityksiä, koska niillä voidaan tarjota hajauttaminen, pysyvyys, anonymiteetti ja tarkastettavuus samanaikaisesti. [Wan *et al.* 2018] Blokchain as as Service on siis keino saada nämä lohkoketjujen tarjoamat hyödyt käyttöön helpommin. Lohkoketju itsessään ei kuitenkaan pitäisi olla sovelluksen kehityksessä keskiössä vaan sen avulla pitäisi tuoda työnkulkuun parempaa jäljitettävyyttä ja läpinäkyvyyttä. Sen sijaan, että yrityksen miettisivät, että miten ne voisivat hyödyntää lohkoketjuja, niiden tulisi miettiä, että mitkä yhteistyössä tehdyt prosessit voisivat kaivata parannusta, ja miten luottamuksen parannus voisi parantaa tehokkuutta. Lohkoketjuista on saavutettavissa hyötyä, kun työnkulku on moniosainen ja vaatii useita eri osapuolia. Toinen missä kohtaa lohkoketjut on nähty hyödyllisiksi, on kun on pyritty saamaan selville, liittyykö johonkin työvaiheeseen korruptiota tai muuta peukalointia. [Karen 2019]

Parhaillaan se mitä BaaS voisi tarjota olisi koko toimialan yhteinen tietojärjestelmä, joka helpottaa kaikkia toimialan yrityksiä. Kun ajatellaan, että toimialan yhteinen tietokanta voisi olla hyödyllinen, niin silloin alan yhteinen lohkoketju voisi olla ratkaisu siihen, että miten dataa säilytetään yhdessä. Nykyisin monilla aloilla käsitellään eri yrityksissä dataa eri järjestelmien kautta, jolloin datan yhteensopivuus järjestelmien välille voi vaatia paljon työtä. Samalla alalla voi olla monta erilaista järjestelmää, ja järjestelmien yhteensovittamisessa on useaan kertaan päällekkäistä työtä eri yritysten kesken. Yhteisellä lohkoketjulla selviäisi moninkertaisesta työstä, koska lohkoketju standardoisi datan muotoilua, kun integraatiot toteutettaisiin sen kautta. Sen avulla ei tarvitsisi myöskään miettiä, että kuka sen sisältämää dataa hallinnoi, koska kaikilla olisi lohkoketjun kautta oma roolinsa, ja tiedot voisi olla näkyvissä eri noodeissa ainoastaan käyttäjän suostuessa tähän. Lohkoketjun avulla voidaan vastata siihen, että jos vaihtoehtona olisi yhteinen tietokanta, niin siinä voi olla riski se, että dataa muokataan tai väärin käytetään, BaaS:n avulla se olisi kurissa.

Nykyisiä BaaS-arkkitehtuureja yhdistäviä tekijöitä ovat konsortiot ja pilvipalveluntarjoaja [Song *et al.* 2021]. Tämän perusteella voisi päätellä, että jo nyt useat konsortiot ovat nähneet lohkoketjuissa piilevää potentiaalia. Hyötyä on saatavilla erityisesti, kun yritykset haluavat toimia verkostona. Pilvipalveluntarjoaja voidaan tässä nähdä neutraalina ulkoisena toimijana, joka voi rakentaa yhteistä järjestelmää. Esimerkiksi IBM:n kehittämä IBM Food Trust lähti Walmartin aloitteesta, mutta toimittajat ja kilpailijat eivät halunneet, että tietojärjestelmä, jota toimitusketjussa käytetään, olisi Walmartin oma. Tästä syystä IBM:n katsottiin olevan sopivan neutraali osapuoli rakentamaan tämä BaaS-sovellus yhteiskäyttöön.

6.3 Tilikirjatietokannat

Lohkoketjuja tulisi lähestyä sitä kautta, että tunnistaisi missä prosesseissa olisi saatavilla hyötyä yhteistyöstä ja mitkä prosessin osat kaipaisivat parempaa jäljitettävyyttä ja läpinäkyvyyttä. Tähän ovat myös monet pilvipalveluidentarjoajat vastanneet sillä nykyisin uutena tietokantatyyppinä on tullut tilikirjatietokannat (*ledger database, LDB*). Tilikirjatietokantojen avulla pystytään vastaamaan teknologiana samoihin vahvuuksiin kuin lohkoketjuilla, kun puntaroidaan lohkoketjuteknologian valinnasta saatavia hyötyjä. Eli ovatko työvaiheet monen käyttäjän välisiä ja auttaako parempi läpinäkyvyys ja jäljitettävyys näissä prosesseissa. Tilikirjatietokannoilla pyritään nimenomaan vastaamaan prosessien läpinäkyvyyteen ja jäljitettävyyteen. Lohkoketjuteknologiassa on nähty potentiaalia käyttäjien ja sidosryhmien välisen luottamuksen parantamisessa ja nyt myös tilikirjatietokanta pyrkii vastaamaan lähes samoilla ominaisuuksilla markkinaan. Osa pilvipalveluiden tarjoajista myykin tilikirjatietokantoja suoraan vaihtoehtona BaaS-palvelulle. Hajautuksen puuttumisesta johtuen tilikirjatietokannassa ei tarvitsisi toimia yhteistyössä vaan riittää jo se, että on vastuussa raportoimaan sidosryhmille.

Tilikirjatietokannan voisi ajatella olevan BaaS-arkkitehtuurissa vastaavanlainen kuin usein käytössä olevaa tietokanta, jota käytetään kuvaamaan nykyistä lohkoketjun tilaa (*Worldstate database*), mutta itse hajautettua lohkoketjua ei ole. Tilikirjatietokantaan onkin liitetty lohkoketjujen muuttumattomuuden ja jäljitettävyyden periaatteita liittämällä niihin lohkoketjun tilikirja ja tarkistettavuus osuudet ankkuroivine tiivistefunktioineen.

Tilikirjatietokantojen tarvetta on perusteltu, sillä että monissa suljetuissa lohkoketjuissa on todettu, että hajautuksesta saatavalle hyödyille ei ole juurikaan käyttöä. Hajautusta puolestaan ei kannata tehdä, jos sitä ei käytetä sillä se tuo turhaa raskautta järjestelmään ja sen arkkitehtuuriin. Tilikirjatietokannat tarjoavat myös mahdollisuuden tehokkaampaan datan indeksointiin. [Yang *et al.* 2020] Hajautuksen puuttuminen on johtanut myös siihen, että niissä ei ole tarvetta konsensusalgoritmeille [Fekete & Kiss 2021]. Luopumalla hajautuksesta järjestelmästä saadaan nopeampi, tehokkaampi ja levytilaltaan pienempi.

AWS:n tilikirjatietokanta Amazon QLDB on julkaistu alkuvuodesta 2019 [AWS Release history 2022]. Se sisältää tietokannan lisäksi tilikirjan, joka sisältää nykyisen tilan ja historia datan kaikesta datasta. Dokumentissa sanotaan, että perinteisiä relaatiotietokantoja voidaan käyttää samassa tarkoituksessa käyttämällä auditointilokeja (*audit logs*), mutta niihin tämän toiminnallisuuden rakentaminen vie aikaa ja kehitysvaihe on herkkä ihmisen tekemille virheille. Ne eivät myöskään ole oletuksena täysin muuttumattomia. Tästä syystä tilikirjatietokanta on hyvä vaihtoehto perinteiselle tietokannalle. [AWS Whitepaper 2022]. On hyvin mahdollista, että tilikirjatietokannoista on tulossa uusi standardi aloille, joissa datan luotettavuudelle on erityisvaatimuksia.

Ensimmäinen BaaS-tarjoaja oli Azure, joka tarjosi kehitysalustan lohkoketjuille palvelullaan Ethereum Blockchain as a service (EBaaS) [Azure EBaaS 2015]. Tämä tapahtui jo loppuvuodesta 2015. Se kuitenkin luopui syyskuussa 2021 omasta BaaS-tarjonnastaan. Se ei kuitenkaan tarkoita, että se olisi lopettanut niiden tukemisen vaan itse lohkoketjuja ylläpidetään yhä Azuren päällä. Toiminta ulkoistettiin ConsenSys-nimisen organisaation Quorum-lohkoketjupalveluihin, jotka ovat yhä Azuren pilvessä. [Azure blockchain] Azure teki tällä toimella myös tilaa omille uusille lohkoketjuja vastaaville palveluilleen, sillä se on julkaisemassa oman tilikirjatietokantansa. Sen nimi on Azure database ledger, joka on vasta public preview -vaiheessa alkuvuodesta 2022 [Azure Documentation 2022].

Voisiko tulevaisuudessa siis tilikirjatietokannat korvata perinteisiä relaatiotietokantoja? Lohkoketjut ja tilikirjatietokannat nähdään usein parannuksena siihen, että ne parantavat datan läpinäkyvyyttä ja jäljitettävyyttä. Mikään ei estä sitä, että perinteisiä tietokantaja ei rakentaisi myös noudattaen näitä periaatteita. Tilikirjatietokannoissa jäljitettävyys ja muuttumattomuus ovat kuitenkin oletuksena, ja niistä saisi hyvän standardin niille aloille, joissa läpinäkyvyys ja jäljitettävyys on elintärkeää. Perinteisessä tietokannassa ei välttämättä saada samanlaista varmuutta siitä, että kukaan ei tee poistoja tai muuten korruptoi dataa ja tästä syystä tilikirjatietokanta voi olla hyvä vaihtoehto perinteisille tietokannoille. Tämän takia uusissa sovelluksissa tulisi vähintäänkin harkita tilikirjatietokantaa, mutta itse teknologiasta toiseen vaihtaminen ja migraatiotyö ei välttämättä ole järkevää.

6.4 Blockchain as a Servicen riskit ja ongelmat

Suurin BaaS:n aiheuttama riski on se, että palveluntarjoajaa on hankala vaihtaa jälkikäteen eli pilvipalvelun kautta joudutaan lukkiutumaan palveluntarjoajaan [Wan *et al.* 2018]. BaaS:n palvelumaksut myös voivat käydä kalliiksi [Kilroy 2019]. Palveluntarjoajan vaihtaminen on erityisen vaikeaa varsinkin siinä kohtaa, jos BaaS yhdistää useita eri toimijoita. Uuteen palveluun tulisi saada nykyisiä noodeja mukaan, jotta siinä voi saada saman verkostoitumishyödyn. Lohkoketjuteknologioiden tekeminen voi olla haasteellista, mutta vielä haasteellisempaa on usein saada eri yhtiöiden omat sidosryhmänsä saman järjestelmän ääreen [Azure whitepaper 2019]. Suurin haaste lohkoketjuissa ei ole teknologia itse vaan menestyksekäs yhteistyö ekosysteemin kumppaneiden kanssa. [Lacity & Van Hoek 2021]

BaaS:ssa kolmanteen osapuoleen täytyy pystyä luottamaan. Se ei saa ajaa yksittäisten noodien etuja vaan sen pitää pyrkiä lohkoketjussa yhteiseen hyvään [Zheng *et al.* 2019]. Koska suurin hyöty lohkoketjuissa saadaan, kun sitä käytetään muiden toimijoiden kanssa, niin lohkoketjun räätälöinti on usein haasteellista, vaikka monissa asiakasyrityksissä sille voisi olla tarvetta [Zheng *et al.* 2019]. Kolmannen osapuolen mukaan tulo tekee

sen, että kolmas osapuoli voi kokea, että jollakin asiakasyrityksistä on suurempaa neuvotteluvoimaa kuin toisella. Näin ollen tallaisen osapuolen toiveet saattavat mennä läpi niin, että se astuisi voimaan lohkoketjussa ja sitä kautta jokaisessa noodissa.

Luottamus kohdistuu BaaS:ssa usein johonkin tahoon tai auktoriteettiin. Se ei välttämättä ole samalla tasolla läpinäkyvyyden, tasa-arvoisuuden, reiluuden ja tarkastettavuuden kanssa kuin teknologia, johon kolmas osapuoli lohkoketjun tapauksessa olisi ulkoistettavissa. [Ma *et al.* 2020] Luottamuspula voi siis kohdistua kummalta puolen tahansa, jolloin yhteistyö hankaloituu. Ei voi kuitenkaan olettaa, etteikö itse teknologia voisi menettää myös asiakkaan luottamusta. Tällöin voi olla jopa parempi asia, että luottamusta koittaa palauttaa itse auktoriteetti, sillä menetettyä luottamusta on usein vaikea palauttaa.

Ongelmia on nähty myös lohkoketjujen noodien eri käyttäjien hallinnassa. Ongelmaksi on koettu varsinkin, kun koko organisaatio on toiminut yhden avainparin takaa. Erityisesti silloin, jos yhtiön avain on vuotanut organisaatiosta ulos. Tämän osa BaaS-lohkoketjuista hallitsee tarjoamalla jokaiselle organisaatiolle oman identiteettiketjunsa, jossa käyttäjille voidaan asettaa niiden tarvitsemia toiminnallisuuksiaan. [Zheng *et al.* 2019] Myös Kilroy [2019] kirjoittaa myös siitä, että lohkoketjuun ei tulisi sisällyttää useampaa yrityksen sisäistä tilamuutosta vaan ne hoidettaisiin päälohkoketjun ulkopuolella. Tähän ratkaisuina on nähty aliketjut tai vähintään omat identiteettiavaimet yrityksen eri toimijoille tai jokin muu sisäinen järjestelmä.

Tilikirjatietokannoissa on yleensä luovuttu lähes kokonaan hajautuksesta, mutta ne sisältävät silti datan muuttumattomuutta kuvaavia ominaisuuksia, joten niistä on myös puhuttu lohkoketjuina. Näen tämän ongelmallisena, koska osaa tilikirjatietokannoista myydään nimenomaan suoraan BaaS-palveluna. Tästä johtuen BaaS ja lohkoketju termeistä on tullut ongelmallisia. Niitä käytetään erilaisista sovelluksista, joissa pyritään vastaamaan datan jäljitettävyyteen käyttäen kryptaavia algoritmeja, jotta niiden data olisi pysyvää ja tarkistettavissa jälkikäteen. Molemmissa termeissä viitataan aina tiedon talletaviin teknologioihin, joihin tarjotaan ainoastaan datan haku ja uuden datan lisäys ominaisuudet.

Esimerkiksi Wan ja muut [2018] kirjoittavat artikkelissaan tiivistetyistä lohkoketjuista. Näissä BaaS-arkkitehtuureissa toiminnallisuus tapahtuu ”mustan laatikon” sisällä, eli piilossa käyttäjältä ja ehdottaakin BaaS-lohkoketjujen jakoa pilven natiivi lohkoketjuihin ja pilven tiivistettyihin lohkoketjuihin. Myös Son ja muut [2021] kirjoittavat, että esimerkiksi Tencentin TrustSQL on kuin tietokanta, jossa on lohkoketjumaisia toiminnallisuuksia. Piilossa tapahtuvat toiminnot syövät erityisesti jäljitettävyyden ja hajautuksen tasoa. Sen lisäksi ne tekevät selkeämmän eron asiakkaan ja palveluntarjoajan rooleihin [Wan *et al.* 2018]. On siis todennäköistä, että markkinoinnillisista syistä myös tilikirjatietokantoja on myyty lohkoketjuna ja BaaS-palveluina. Olisi kuitenkin parempi, jos

viestintä asiakkaille olisi selkeämpää kuten AWS ja Azuren tapauksessa, joissa nämä ehdottavat suoraan omia tilikirjatietokantojaan vaihtoehdoksi BaaS-palvelulleen. Perinteisesti lohkoketju on aina aiemmin ollut myös hajautettu, mutta nyt uudet tarjotut versiot ovat myös vahvasti keskitettyjä, joissa osa toiminnallisuuksista tapahtuu piilossa. Tutkimuksessa ja puheessa olisikin syytä erottaakin teknologian hajautuksen ja piilotettujen operaatioiden perusteella se onko kyse lohkoketjusta vai tilikirjatietokannoista. Tilikirjatietokanta tuo puolueettomaan osapuoleen luottamisen ja tästä riippuvuuden vieläkin korkeammalle tasolle. Niissä auditointilokit eivät myöskään yleensä ole tavallisille käyttäjille saatavilla, joka myös nostaa riippuvuuden tasoa [Fekete & Kiss 2021].

7 Blockchain as a Service ja lohkoketjut

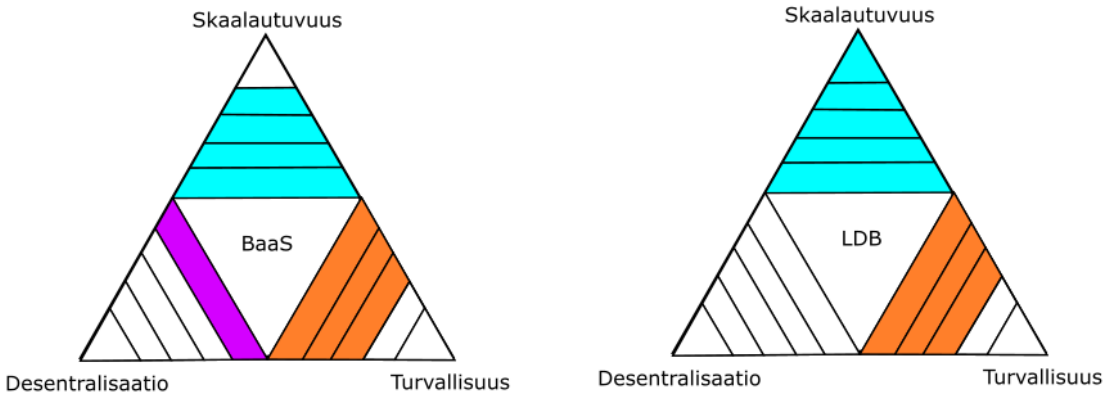
Yrityksissä on usein koettu, että lohkoketjuja on hankala ymmärtää. Sen lisäksi niiden käyttöönotto ja ylläpito on koettu vaikeiksi. BaaS madaltaa yritysten lohkoketjuihin mukaan tulemista auttamalla näissä haasteissa. Lohkoketjumarkkinassa on ollut käynnissä nopeuskilpailu siitä, että kuka ehtii ottamaan lohkoketjumarkkinan haltuunsa. Samanaikaisesti on tapahtunut pilvipalveluiden nousu hallitsevaksi tavaksi järjestää IT-infrastruktuuri. Pilvipalvelut ovat saaneet myös merkittävän osan nykyisistä yritysten lohkoketjuista, sillä niiden Blockchain as a Service (*BaaS*) on yrityksille helppo keino saada lohkoketjut käyttöön. BaaS voi myös olla houkuttelevampi vaihtoehto monelle asiakasyritykselle, jos ne käyttävät pilvipalveluita verrattuna siihen, että ne kehittäisivät kokonaan oman lohkoketjunsa. Asiakkaan näkökulmasta tämä voi johtaa siihen, että ne joutuvat lähes lukkiutumaan omaan pilvipalveluntarjoajaansa. Julkisista lohkoketjuista voittajana on tällä hetkellä Ethereum, joka on ensimmäinen lohkoketju, johon on voinut rakentaa omia sovelluksiaan. Sillä on kaikkein eniten käyttäjiä ja sen päälle on rakennettu useita muita lohkoketjuja ja linkityksiä muihin lohkoketjuihin. Myös monet BaaS-palvelut käyttävät sitä.

BaaS-palveluidentarjoajille avautuu tarjonnan kautta mahdollisuus päästä mukaan isompaan rooliin eri alojen liiketoiminnassa. Toisaalta tätä on tapahtunut paljon jo pelkästään tarjoamalla pilvipalveluita. Erona BaaS:ssa on kuitenkin se, että mikäli sen päälle saadaan rakennettua organisaatioiden verkosto, tulee palveluntarjoajan vaihtamisesta entistä vaikeampaa. Toisaalta ilman BaaS-palveluita, monella toimialalla ei osattaisi hakea lohkoketjuista saatavilla olevaa hyötyä. Lohkoketju ei ole vielä tällä hetkellä tuote, joka myisi itse itseään vaan asiakkaiden on ensin ymmärrettävä lohkoketjuja melko hyvin, että ne osaisivat hakea lohkoketjuista parannusta omiin prosesseihin.

Usein yritykset harkitsevat uuden teknologian käyttöönottoa sillä asenteella, että odotetaan ja katsotaan mitä teknologia tuo niille, jotka sen ottavat käyttöön. Tämä johtuu siitä, että usein pelätään uusien investointien olevan tappiollisia. Lohkoketjun tapauksessa odottaminen voi koitua kalliiksi, koska se voi vaikuttaa merkittävästi liiketoimintoihin. [Felin ja Lakhani 2019] Tämä johtuu siitä, että lohkoketjujen avulla on mahdollisuus muokata eri alojen sisäisiä voimasuhteita, varsinkin jos joku toimija pystyy luomaan lohkoketjuun verkoston, jossa se parantaa asemiaan markkinassa. Myös yhteistyössä toimiminen voi vaikuttaa yrityksen voimasuhteeseen markkinassa verrattuna siihen, että jättäytyisi yhteistyön ulkopuolelle.

7.1 Miten BaaS-lohkoketjut vertautuvat perinteisiin lohkoketjuihin?

Pilvipalveluiden lohkoketjuilla on saavutettavissa monissa tilanteissa yrityksille se hyöty mitä lohkoketjuilla on saavutettavissa. Niissä on onnistuttu löytämään skaalautuvuuden trilemmaan ratkaisuja, eikä niitä koske samalla julkisiin lohkoketjuihin yhdistetty kasvanut hiilijalanjälki heikon suorituskyvyn ohella. Pilvipalveluiden tarjoamissa ratkaisussa myös hankalaksi koettu käyttöönotto saadaan ulkoistettua. Kuvassa 3 on arvioitu lohkoketjujen ominaisuudet trilemman kautta. Niissä on siis luovuttu suuremmasta määrästä hajautusta, jotta niiden skaalautuvuutta on saatu parannettua. Todennäköisesti tarjottu ratkaisu on riittävän hyvä moniin käyttötapauksiin erilaisissa liiketoimissa. Varsinkin silloin, jos yritys käyttää jo nyt pilvipalveluiden tarjoamia palveluja niin kyseistä vaihtoehtoa on syytä harkita.



Kuva 3. BaaS ja Tilikirjatietokannat trilemman kautta tarkasteltuna.

Kuvasta 3 näkee, että BaaS luistaa hieman lohkoketjuteknologian muuttumattomuuden ja hajautuksen periaatteista, sillä siirtämällä lohkoketju keskitettyyn pilveen teknologian hajautuksen taso luonnollisesti laskee verrattuna siihen, että noodit sijaitsisivat asiakkaiden omilla laitteilla. Tämä tehdään juuri sen takia myös, että palveluntarjoajan on helpompi saattaa teknologiaan tehdyt muutokset voimaan asiakkaiden noodeihin, jolloin myös muuttumattomuudesta on joustettu. Puolestaan tilikirjatietokannoissa skaalautuvuuden haasteet on ratkaistu desentralisaatiosta luopumalla, tarjoamalla keskitetty järjestelmä.

Pilvipalveluiden BaaS-ratkaisut eivät ratkaise lohkoketjujen skaalautuvuuden trilemmaa sillä sen tarjoama ratkaisu vähentää lohkoketjujen hajautuksen tasoa. Niiden avulla lohkoketjujen painopiste tietoturvallisuudesta ja hajautuksesta siirtyykin skaalautuvuuteen ja tietoturvallisuuteen. Tietoturvallisuus kuitenkin laskee hajautuksen vähenemisen myötä sillä keskitetympi järjestelmä ei tuo niitä etuja tietoturvallisuuteen kuin hajautettu järjestelmä toisi. Keskitetty järjestelmä tuo hyökkääjälle takaisin mahdollisuuden iskeä keskitettyyn kohteeseen. Keskitetty kohde voi kuitenkin pyrkiä ennaltaehkäisemään sitä, että se ei joutuisi hyökkäyksen kohteeksi. Myös itse pilvipalvelun palvelunestohyökkäys

vaatisi valtavat määrät resursseja siihen, joka vaatisi hyvin koordinoitua suunnittelua, joten sitä eivät pienet toimijat pysty samalla tavalla tekemään kuin palvelunestohyökkäys onnistuisi yksittäiseen yritykseen, joka itse pitää huolta omista palvelimistaan. Pilvipalveluissa on yleensä myös panostettu tietoturvallisuuteen jo itse palveluntarjoajan tasolla eli sitä kautta myös tietoturvaa tulee katettua. Tästä syystä niiden ei välttämättä tarvitse suojautua palvelunestohyökkäykseen itse lohkoketjussa samoissa määrin. Toisaalta muut tietoturvallisuuteen liittyvät riskit voivat liittyä itse käyttäjiin eikä voida täysin poissulkea, että joku ylläpitävätoimija ei haluaisi tuottaa haittaa yritykselle, jolloin esimerkiksi sen Byzantine-toleranssi ei ole yhtä korkea kuin perinteisissä lohkoketjuissa.

Pilvipalvelulohkoketjujen skaalautuvuus paranee siinä mielessä, että se poistaa viiveen, joka kuluisi itse tiedonsiirrossa noodilta toiselle noodille sillä saman palvelimen sisällä useampi noodi tarkoittaa, että data liikkuu palvelimen sisällä. Tämä parantaa itsessään jo lohkoketjujen suorituskykyä. Toisaalta BaaS toimii myös suljetussa lohkoketjussa, jolloin sen käyttäjäkunta on myös rajattu. Tämä myös tarkoittaa, että sen ei välttämättä tarvitsisi edes kyetä vastaamaan samoissa määrin skaalautuvuuteen. BaaS-lohkoketjut yleensä käyttävät myös Proof of Authority -konsensusalgoritmia, ja se tuo mukanaan sen, että kaikkien noodien ei tarvitse suorittaa varmennusta siitä, että auktoriteetti ei toimisi lohkoketjun vastaisesti vaan useimmin näissä muut auktoriteetit suorittavat varmennusta. Myös tämä parantaa niiden suorituskykyä. Koska BaaS pystyy parempaan käsittelyaikaan niin sinne voidaan sisällyttää myös enemmissä määrin transaktioita, ja tästä syystä sen skaalautuvuus on merkittävä tekijä.

Analysoin taulukossa 1 kerättyjen tietojen perusteella suuntaa sille, miten yksittäinen muuttuja näyttäytyy Blockchain as a Service lohkoketjuissa verrattuna yleisimmin käytössä olevaan lohkoketjuun Ethereumiin yksittäisen noodin kannalta. Taulukon analysoitavat ominaisuudet ovat kategorisoitu seuraavasti lohkoketjumaiset perusominaisuudet, ylläpitoon liittyvät ominaisuudet, desentralisaatio, skaalautuvuus ja tietoturvallisuus. Ominaisuudet jaetaan vielä pienempiin osiin, jotta niiden arvioiminen onnistuu järkevästi. Lopputulos on kuitenkin riippuvainen siitä, että mitä ominaisuuksia tarkasteluun on haluttu ottaa mukaan, ja tästä johtuen myös painotus voisi muuttua, jos uusia muuttujia otettaisiin mukaan tarkasteluun. Pisteytyksessä on käytössä ainoastaan 0–2, joka on valittu ainoastaan sen takia että pisteytyksistä voidaan saada suuntaa antavia.

0 = poistettu, 1 = heikko, 2 = vahva

Analysoitava muuttuja	Blockchain as a Service	Julkinen Ethereum
Lohkoketjumaiset perusominaisuudet		
Teknologian läpinäkyvyys	2	2
Datan läpinäkyvyys	1	2
Datan muuttumattomuus	2	2
Lohkoketjumaisten perusominaisuuksien pisteytys	5 / 6	6 / 6
Lohkoketjujen ylläpitoon liittyvät ominaisuudet		
Lohkoketjun logiikan muutettavuuden helppous jälkikäteen	2	1
Teknologian liittäminen muuhun IT arkkitehtuuriin	2	1
Teknologian liittämisen helppous muihin lohkoketjuihin	1	1
Älysopimusten liittämisen helppous teknologiaan	2	2
Sääntelyn vaikutus	2	1
Käyttäjästä aiheutuvien virheiden korjauksien helppous	2	0
Lohkoketjujen ylläpidon helppouden pisteytys	11 / 12	6 / 12
Desentralisaatio		
Päätäntävallan hajautus	1	2
Arkkitehtuurin hajautus	0	2
Looginen hajautus	1	2
Desentralisaation pisteet	2 / 6	6 / 6
Skaalautuvuus		
Transaktiomääräinen suorituskyky	2	1
Transaktion käsittelynopeus	2	1
Transaktion matala hinta	2	1
Energiatehokkuus	2	1
Skaalautuvuuden pisteet	8 / 8	4 / 8
Tietoturvallisuus		
Byzantine-toleranssi	1	2
Kesto Sybil-hyökkäystä vastaan	2	2
Kesto palvelunestohyökkäystä vastaan	1	2
Crash-toleranssi	2	2
Double-spending vastustus	2	2
Tietoturvallisuuden pisteet	8 / 10	10 / 10

Taulukko 1. BaaS verrattuna Ethereum-lohkoketjuun.

BaaS:in kautta siis tehokkuuden lisäksi lohkoketjujen käyttökokemusta helpotetaan huomattavasti loppukäyttäjälle esimerkiksi kadonneen salasanan tapauksessa. BaaS-lohkoketjuilla pyritään myös helpottamaan lohkoketjun kehittäjien työtä tarjoamalla niihin ratkaisuja, esimerkiksi sillä, että muutokset lohkoketjuun saadaan vietyä noodeille virtuaalikoneen kautta. Lohkoketjumaisista ominaisuuksista BaaS ei saa täysiä pisteitä, koska niissä voidaan rajata käyttäjien datan näkyvyyttä siten, että noodi näkee vain sille kuuluvaa dataa. Taulukosta 1 saa mielenkiintoisen pisteytyksen, kun arviot lasketaan yhteen. Yhteispisteet esiteltynä seuraavaksi taulukossa 2.

Analysoitava muuttuja	Blockchain as a Service	Julkinen Ethereum
Taulukon 1 yhteispisteet	34 / 42	32 / 42
Taulukon 1 yhteispisteet ilman ylläpidon ominaisuuksia	23 / 30	26 / 30

Taulukko 2. Yhteispisteet BaaS verrattuna Ethereum-lohkoketjuun.

Mielenkiintoinen huomio Taulukon 2 pisteytyksestä on se, että vaikka tarkastelun kokonaispisteissä BaaS saa kaksi pistettä enemmän niin riisumalla niistä ylläpidon ominaisuudet niin Ethereum ohittaa BaaS:n kokonaispisteissä kolmella pisteellä. Tämä tarkoittaa, että ensimmäisessä taulukossa suurin painoarvo on lohkoketjujen ylläpidon ominaisuuksissa. Tämä painotus on otettu tarkasteluun, koska siinä nimenomaan on BaaS:n suurin arvo verrattuna muihin lohkoketjuihin, joten kyseisellä painotuksella BaaS pärjäisi hyvin myös verrattuna tavalliseen Proof of Authoritya käyttävään yksityiseen lohkoketjuun, joka voisi saada lähes samanlaiset pisteet ominaisuuksistaan, vaikka saisi paremman pisteytyksen arkkitehtuurin hajautuksesta. Muuttujia voi käyttää eri lohkoketjujen vertailuun, eikä olisi mieltä verrata näillä muuttujilla esimerkiksi tietokantoihin.

7.2 BaaS ja sen jatkokehitys

BaaS-palveluiden avulla yritykset saavat suhteellisen helposti lohkoketjut käyttöön, kun ne löytävät sopivia käyttötarkoituksia niihin omassa liiketoiminnassaan. Vaikka BaaS jäisi jossakin kohtaa vanhentuneeksi konventioksi lohkoketjujen kannalta niin käyttöönotetut järjestelmät tuskin ovat heti korvaantumassa kokonaan uusilla tietojärjestelmillä. BaaS:n rajapintaratkaisut ovat todennäköisesti siinä mielessä kestävä ratkaisu, että rajapintojen kautta BaaS-järjestelmät ovat yhdistettävissä uusiin järjestelmiin vielä pitkällä tulevaisuudessa, vaikka API-ratkaisu ei olisi alan standardi [Belchior *et al.* 2021]. Yritysten tulisi keskittyä teknologian haltuunotossa nykyhetkeen ja ne eivät saisi unohtaa nykyisiä järjestelmiään [Lacity & Van Hoek 2021]. Vaikka lohkoketju olisi yrityskäytössä niin se ei tarkoita, että sen tarvitsisi olla ainut tiedontalletukseen käytettävä teknologia vaan sinne voi hyvin tallettaa vain sen datan,

josta sinne on suurin hyöty. Talletetusta datasta on hyvä olla tallessa avain lohkoketjussa, jonka avulla löytäisi muista tietojärjestelmistä kyseistä avainta koskevan datan. Muut tietojärjestelmät voivat hyvin käyttää esimerkiksi relaatiotietokantaa, jolloin lohkoketjut olisivat vain yksi osa yrityksen IT-infrastruktuuria.

Lohkoketjujen yhteensovittaminen muihin järjestelmiin on rahakkeiden siirtämisen lisäksi myös esimerkiksi datan ja älysopimusten siirtämistä. Vaikka tässä onnistuttaisiin niin lohkoketjujen yhdistäminen muihin järjestelmiin kuten legacy-järjestelmiin tulee olemaan haastavaa. [Belchior *et al.* 2021] Tässä kuitenkin helpottaa nimenomaan rajapintaratkaisut, joita BaaS-ratkaisuihin on tehty.

Nykyisin julkisissa lohkoketjuissa kuitit (*rollup*) ovat vallitseva keino dataliikenteen sisään lukuun. On todennäköistä, että ne yleistyvät myös yksityisissä lohkoketjuissa. Jos yksityinen lohkoketju tukee rajapintoja ja halutaan jälkikäteen liittää julkiseen lohkoketjuun niin se tarkoittaa, että sille pitää tehdä liikenteen mahdollistava kuittilompakko, jonka avulla rajapintaliikennettä voidaan suorittaa. Yhdistäminen lohkoketjuteknologiaan vaatii todennäköisesti kehitystyötä myös yhdistettävän järjestelmän rajapintoihin, joista liitos halutaan tehdä. Tämä ei välttämättä ole yksinkertaista, mutta siihen varmasti löytyy keinoja.

On hyvä huomioida, että tällä hetkellä kuitteihin käytettävät työkalut ovat melko alkeellisia ja ne vaativat erikoisosaamista. Ne ovat lähempänä konekieliä ja siitä syystä niiden haltuun ottaminen on monille lohkoketjujen parissa toimiville työläämpää. [Päivinen *et al*. 2021] On todennäköistä, että ajan saatossa työkalut näiden käsittelyyn kehittyvät, jolloin niiden käyttäminen ja kehittäminen on helpompaa. Samoin myös niiden lukemiseen rajapintojen avulla tulee varmasti löytymään standardeja. Yritysten tulisi keskittyä nykyhetkeen, ja miettiä miten nykyisiä järjestelmiä saisi integroitua lohkoketjuihin. Siihen rajapinnat ovat keskeinen keino järjestelmien yhteensovittamiseksi, ja vasta myöhemmin todennäköisesti tulevat kuitteihin liittyvät ratkaisut.

Kuittien yhdistämisestä lohkoketjuun pitäisi saada pidemmällä aikavälillä palvelu, jossa asiakkaille tarjottaisiin valmis ratkaisu kuittiensa tekemiseen. Valmis SaaS-tyyppinen ratkaisu voisi olla toimiva, jos sen saisi helposti liitettyä erityyppisiin lohkoketjuihin. Tämä helpottaisi myös Aaveen kaltaisten uusien hajautettujen sovellusten syntymistä ja myös Web 3.0 ajatuksen hyödyntämistä perinteisessä liiketoiminnassa olevien yritysten toimesta. Kuittien avulla tietojärjestelmiä yhdisteleviä yrityksiä on alalla, mutta valmista palvelua ei taida olla.

Jos BaaS-lohkoketjut yleistyvät niin niistä voi hyvin tulla uuden tyyppinen tapa kehittää tietojärjestelmiä. Se tarjoaisi uuden tyyppisiä töitä varsinkin, jos yritykset näkisivät enemmän mitä lohkoketjujen avulla voisi saavuttaa. Kun tietojärjestelmien kehittäjät on perinteisesti jaettu perinteisten frontend- ja backend-kehittäjiin niin voisiko tähän rinnalle

nousta blockchain-kehittäjät. Toisaalta kyseessä on ennemminkin backend-teknologia, joten näille voi lohkoketjujen kautta tulla uusia teknologioita hallittavakseen. Hyvä huomioida, että esimerkiksi Solidity, jota Ethereum Virtual Machine käyttää on hyvin paljon JavaScriptin kaltainen ohjelmointikieli, ja sen kautta se on hyvin soveltunut myös frontend-kehittäjille. Sen kehitys on hieman samantapaista kuin käyttäen Node.js kirjastoa, jonka avulla JavaScriptiä on mahdollista käyttää vastaavasti backend-puolella.

Tulevaisuudessa samaan tarkoitukseen tehdyt lohkoketjut olisi hyvä saada toimimaan keskenään, jotta ei olisi montaa rinnakkaista järjestelmää. Tämä vaatiikin uusia konventioita [Lacity & Van Hoek 2021]. Mikäli pilvipalveluiden tarjoajille tulee lohkoketjujen keskittymiä niin ne voivat ratkoa yhteensovittamista. Vastaavaa työtä ollaan tekemässä samanaikaisesti julkisissa lohkoketjuissa. Julkisiin ja yksityisiin lohkoketjuihin on luotu jo joitakin ratkaisuja, mutta on oletettavissa, että nämä lohkoketjut ovat jossakin kohtaa myös keskenään paremmin yhteensopivia. Yhteen sopiessaan BaaS voisi olla Ethereum 2.0 pirstaleiden kaltainen lopputulos, jossa useampi lohkoketju lopulta yhdistyy isompaan päälohkoketjuun.

Nykyiset BaaS-alustat on usein rakennettu julkisten lohkoketjujen päälle, joka voidaan nähdä ongelmallisena, sillä dataa voi vuotaa sen kautta haitallisille toimijoille [Ma *et al*. 2020]. Kilroy [2019] nostaa esiin sen, että jos BaaS liitetään julkisiin lohkoketjuihin niin kannattaa ottaa selvää, mitä lainsäädäntö sanoo julkisten rahakkeiden käytöstä. Ainakin USA:ssa joidenkin osavaltioiden lainsäädäntö sanoo, että julkisissa hankkeissa ei haluta toimia sovellusten kanssa, joissa käytetään virtuaalivaluuttaa tai muita rahakkeita. Palveluntarjoajan kautta lohkoketju menettää myös autonomisen asemansa, sillä palveluntarjoajan tulee noudattaa paikallista sääntelyä. Julkiset lohkoketjut toimivat ylikansallisesti juuri sen keskittämättömän luonteensa vuoksi.

7.3 Mikä vaikutus BaaS-lohkoketjuilla on?

Lohkoketjut tuovat mukanaan liiketoiminnan tavanomaista digitalisoitumista, jossa toimintoja tehostetaan automatisaation avulla. Siihen ei itsessään tarvittaisi lohkoketjuja, vaan automatisaatiota tapahtuu teknologian kehittymisen myötä. Lohkoketjut ja BaaS tulisi nähdä vaihtoehtona, koska niiden avulla voidaan saavuttaa parempaa läpinäkyvyyttä. Niiden avulla esimerkiksi Walmart sai digitalisoitua omaa toimitusketjuaan otettuaan käyttöön IBM:n Food Trustin, joka käyttää IBM:n BaaS-palvelua.

Perinteisesti lohkoketjuja on leimannut voimakas vastakkainasettelu vallitsevien instituutioiden ja lohkoketjujen tuomien uusien organisoitumismahdollisuuksien välille. Nykyisistä instituutioista irtaantuminen vaatisi sen, että ihmiset yhdessä haluaisivat päästä niistä irti. Sen lisäksi vaadittaisiin jokin rakenne, joka estäisi organisaatioiden ja instituutioiden liittymisen lohkoketjuihin ja osallistumista esimerkiksi DAO-päätöksentekoon.

Suurin vaikutus, joka lohkoketjuilla potentiaalisesti on, liittyy toimialojen uudelleen organisoitumiseen. Lohkoketjujen avulla valtaa siirtyy käyttäjille itselleen enemmän. Samoin niiden avulla myös nykyiset toimijat voivat sementoida oman asemansa alan toimijana vielä tiukemmin. Todennäköisesti vaikutus organisaatioihin ja liiketoimintaan on vastaavanlainen kuin esimerkiksi sosiaalisenmedian vaikutus perinteiseen mediaan. Nykyisin sosiaalisessa mediassa jaetaan paljon perinteisten medioiden tuottamaa sisältöä, ja samoin perinteisillä medioilla on omia sosiaalisen median kanaviaan, joten ne ovat myös osa kyseistä sosiaalista mediaa. On todennäköistä, että jotkin organisaatiot tuovat omia palveluitaan myös julkisiin lohkoketjuihin. Näin ihanne käyttäjille täysin hajautetusta järjestelmästä sortuu.

Monet kehittäjät ja lohkoketjujen käyttäjät, jotka ovat olleet alalla jo pitkään kannattavat lohkoketjuja aatteellisista syistä eivätkä haluaisi joustaa perinteisestä hakkerietiikastaan. On selvää, että joustamattomuus desentralisaation suhteen on haitaksi lohkoketjujen kasvulle pitkässä juoksussa. Perinteiset lohkoketjuihin liitettävät aatteet tuskin nousevat hallitsevaksi aatteeksi suurelle yleisölle, jos maailma ei radikaalisti muutu lyhyessä ajassa.

BaaS-lohkoketjut ovat alkuperäistä Web 3.0 ajatusta vastaan sillä se antaa pilvipalveluille merkittävää valta-asemaa. Alkuperäinen Web 3.0 ajateltu keskitettyjen alustojen vallasta irtautumisesta vaikuttaa utopistiselta sillä teknologiana DAO ei ota kantaa siihen, että onko siihen osallistuva taho yritys vai yksityishenkilö. On todennäköistä, että alustat tulevat olemaan osa Web 3.0 arkkitehtuuria varsinkin, kun olemassa olevia yrityksiä liittyy siihen käyttäjinä.

Lohkoketjuista puhutaan, että se demokratisoisi teknologiaa. Tässä jää huomioimatta se, että kuka teknologiaa hallinnoi. Lohkoketjujen kehitystyö ja päivitykset usein syntyvät rajatuissa yhteisöissä, joissa käyttäjä ja kehittäjä eivät ole samanlaisessa asemassa. On siis tärkeä ymmärtää, kuka ohjelmistoa tarjoaa ja mihin sitä käytetään. BaaS selkeyttää tätä jakoa, sillä sen avulla teknologialle löydetään helpommin vastuunkantaja.

Digitalisaation ja kehityksen myötä ohjelmien käyttäminen ja käyttöönottaminen pitäisi onnistua myös helposti. Nyt vaikuttaisi siltä, että suurin osa myös Ethereumin noodeista on pilvipalveluiden palvelimilla. Tästä voisi päätellä, että sen käyttäjät ovat teknologisesti valveutuneita. Virtuaalikoneen ja lohkoketjunoodin pystyttäminen ei ole yleistä vielä tavallisten tietokoneen käyttäjien keskuudessa. Toisaalta Ethereumissa tavallisena käyttäjänä ei välttämättä tarvitse pystyttää noodia sillä Ethereumin käyttäminen onnistuu jo pelkästään lompakon asentamisella selaimeen. BaaS palvelun kautta puolestaan virtuaalikoneen asentaminen voidaan ulkoistaa palveluntarjoajalle, jolloin myös vähemmän teknologiasta ymmärtävät käyttäjät pääsevät mukaan noodeiksi.

Lohkoketju ei ole tällä hetkellä teknologia, jota ymmärretään kovinkaan hyvin teknologiaratkaisuja pohdittaessa. BaaS helpottaa lohkoketjujen ylläpitoa ja käyttöönottoa, ja

siitä syystä voisi kuvitella, että niiden avulla lohkoketjut voidaan nähdä useammassa yrityksessä helpommin tietokantojen rinnalla tai osana niitä. Monissa yrityksissä voidaan kuitenkin pitää tilikirjatietokantoja helpommin ymmärrettävä konseptina, sillä se on lähempänä perinteisiä tietokantoja. Tämä voisi olla myös syy sille miksi BaaS olisi vain välimalli lohkoketjuille kohti tilikirjatietokantoja. Tilikirjatietokantojen läpilyönti kuitenkin jättäisi historiankirjoihin merkinnän ajasta, jolloin lohkoketjuista olisi kehittynyt BaaS:n kautta tilikirjatietokantoja.

Jotta yritykset voivat saavuttaa tiukemman aseman omaan liiketoimintaansa lohkoketjujen avulla niiden on syytä olla ajoissa liikkeellä oman lohkoketjuteknologian ja yhteistyöverkostonsa kanssa. Todellinen haaste on usein saada eri yhtiöiden omat sidosryhmänsä saman järjestelmän ääreen ja tehdä kaikkia hyödyttävää yhteistyötä. Yhteisessä teknologiassa haaste on nimenomaan saada kaikki jäsenet saman teknologian ympärille.

7.4 Yritykset mukaan lohkoketjuihin BaaS:n avulla

Pilvipalveluiden ja Blockchain as a Servicen kautta lohkoketjut tulevat lähemmäs yrityksiä. Niissä on jo ennestäänkin yritystoimintaa, mutta se on enimmäkseen ollut DAO-tyyppisten startup-yritysten erityisalaa. Yritysten kautta lohkoketjuihin valuu enemmän resursseja ja käyttäjiä, jotka eivät välttämättä muuten olisi teknologiaan tulleet. Perinteiset isommat teknologia-alan toimijat olivat konsortiona jo pari vuotta sitten kyllä alalla. Silloin oli painopiste siinä, että miten lohkoketjuja tulisi kehittää, että niistä tulisi paremmin nykyisiä liiketoimintoja tukeva teknologia. Nyt konsortioiden painopiste on muuttunut siihen suuntaan, että ne voivat yhdessä kehittää uusia prosesseja ja liiketoimintaa lohkoketjujen ympärille.

DAO-toiminta kyllä kehittää lohkoketjuja, mutta kehittääkseen lohkoketjuja suuremmissa määrin niin resurssipula on myös johtanut siihen, että lohkoketjut kehittyvät hitaasti. Vaikka lohkoketju markkinaan on kanavoitunut suuret määrät rahaa kryptovaluuttasijoittamisbuumin myötä niin ne eivät kanavoidu tehokkaimmalla tavalla käyttäjien lompakoista lohkoketjuja kehittäviin organisaatioihin. Yritysten mukaantulo tekee sen, että alalla varat kasaantuvat tehokkaammin niihin toimintoihin, joista koetaan saatavan hyötyä.

Yksittäisten toimijoiden ajatus riippumattomasta teknologiasta alkaa olla tiensä päässä. Yritysten mukaan tulo mahdollistaa sen, että toiminnasta voidaan saada laajemmin ammattimaisempaa. Nykyisin moni lohkoketjuprojekti toimii sivuprojektina tai vapaaehtoisten voimavaroin. DAO:n ICO:t kyllä mahdollistavat rahoituksen hakemisen, jotta kokopäiväinen työskentely DAO:n parissa toimii niin silti perinteisten markkinoiden ja rahoitussektorin mukaan tulo tuo enemmän resursseja lohkoketjujen kehitykseen.

Vaikka aiemminkin yrityksillä olisi ollut mahdollisuus liittyä lohkoketjuihin älysopimusten kautta niin ainakin toistaiseksi vielä se vaatisi erityisiä ponnisteluja siihen, että

nykyinen järjestelmä tukisi lohkoketjuja. Siinä myöskin hyödyt ovat olleet melko pienet, sillä se pääasiassa mahdollistaisi sen, että lohkoketjuissa pystyisi maksamaan kryptovaluutoissa. Nyt BaaS:n myötä yrityksillä on aidosti mahdollisuus saada hyötyä lohkoketjuista. BaaS:n avulla on mahdollista tukea nykyisiä tietojärjestelmiä, eikä se juurikaan muuta yritysten vanhaa liiketoimintaa. BaaS-lohkoketjujen avulla yritykset voivat digitalisoida prosesseja ja poistaa tehottomuutta. BaaS:n ymmärtämisen myötä voi tulla ajatus siitä, että yritys voisi laajentaa IT-arkkitehtuuriaan kiinni myös muun tyyppisiin lohkoketjuihin.

8 Johtopäätökset

Tämän tutkimuksen tarkoituksena oli vastata kysymykseen *”Mikä vaikutus pilvipalveluiden Blockchain as a Service lohkoketjuilla on lohkoketjuihin?”*.

Blockchain as a Service on vielä uusi teknologia, joka ei ole vielä ehtinyt vaikuttaa paljoakaan lohkoketjuihin. BaaS kuitenkin tuo yritystoimintaa ja lohkoketjuja lähemmäs toisiaan siten, että ne voisivat molemmat auttaa toisiaan kehittymään. Tällä hetkellä BaaS on tuote, jota ei vielä välttämättä tunneta yrityksissä kunnolla. Vaaditaankin vielä kehitystyötä ja lisää tietämystä aiheesta, jotta BaaS voisi kasvaa merkittävämmäksi lohkoketjujen ja yritysten kannalta. Näkisin, että kääntöpiste olisi se, kun yritykset itse aktiivisesta hakeutuisivat käyttämään niitä. Tästä syystä moni arvio vaikutuksista on vielä spekulatiivista. Voi hyvin olla, että Blockchain as a Service on vain hetken tarjolla oleva palvelu, joka korvataan piankin tilikirjatietokannoilla. Se on ollut kuitenkin merkittävä etappi lohkoketjuille kohti tilikirjatietokantoja.

Yrityksille ei ole aiemmin ollut näin helppoa ottaa lohkoketjuja omaan käyttöönsä, mutta silti niiden käyttö on vähäistä. Jos Blockchain as a Service ei ole se lohkoketjuteknologia, joka tulee lyömään läpi perinteisessä liiketoiminnassa, niin voidaan todeta, että lohkoketjut eivät todennäköisesti koskaan pysty vastaamaan niiden ympärille kasattuihin odotuksiin. Jos koetaan, että niistä ei ole hyötyä nyt niin niistä tuskin koskaan saadaan ulosmitattua hyötyjä. Ainut tapa olisi myöhemmin se, että maailmassa nousisi libertaristinen maailmankuva hallitsevaksi ajattelumaailmaksi, mutta se ei vaikuta kovinkaan realistiselta. Tärkeintä juuri nyt olisi on saada teknologiasta päättävien ihmisten tietoisuuteen mahdollisuus BaaS-palveluista yrityksissä, joissa lohkoketjujen hyödyt ovat saavutettavissa.

Suljetut lohkoketjut soveltuisivat hyvin eri yritysten välisten tietojärjestelmien dataintegraatioihin, sillä sen avulla olisi mahdollista standardoida dataa. Blockchain as a Service tuo konkreettisesti yrityksille mahdollisuuden käyttää lohkoketjuja. Aiemmin se on vaatinut paljon osaamista ja ymmärrystä teknologiasta, mutta nyt osaaminen ja ymmärrys voidaan helposti ostaa kolmansilta osapuolilta. Kaikkein eniten lohkoketjuteknologioista on saatavilla hyötyä, kun tehdään yhteistyötä muiden toimijoiden kanssa, sillä niiden avulla pystytään tuottamaan läpinäkyvämpää ja luotettavampaa dataa tietojärjestelmiin. Kolmansien osapuolien avulla yritykset saavat ulosmitattua näitä lohkoketjuista saatavia hyötyjä.

Kolmannen osapuolen mukaantulo lohkoketjuihin puolestaan muuttaa lohkoketjujen skaalautuvuuden trilemman painotusta desentralisaatiosta ja tietoturvallisuuden maksimoinnista tasapainoisempaan tilaan. Tässä erityisesti desentralisaatiosta joustetaan vastaamaan parempaa skaalautuvuutta. Tämä puolestaan vaikuttaa myös siihen, että nämä lohkoketjut eivät ole niin paljon energiaa kuluttavia, sillä niissä moninkertaista laskentaa ja varmentamista ei tarvitse tehdä. Tämä johtaa siihen, että BaaS-lohkoketjuja ei tulisi

nähdä samalla tavalla ilmastonmuutosta kiihdyttävänä teknologiana, kuten nyt esimerkiksi Bitcoin on. BaaS siis pystyy vastaamaan lohkoketjujen suureen energiankulutukseen ja on paljon houkuttelevampi vaihtoehto monille yrityksille kuin julkisiin lohkoketjuihin liittyminen.

Blockchain as a Service tuo myös konkreettisesti esiin sen, että kolmas osapuoli ei ole vain pahasta lohkoketjussa. Tämä on juurtunut tausta-ajatus monissa lohkoketjuissa, mutta se estää lohkoketjujen nousemisen yleiskäyttöisemmäksi teknologiaksi. Lohkoketjujen avulla yritykset, jotka käyttävät sitä voivat toimia läpinäkyvämmin ja viestiä vastuullisuudesta sitä kautta.

Blockchain as a Servicen myötä myös lohkoketjujen sääntelyllä on suurempia vaikutuksia. Varsinkin julkisissa lohkoketjuissa on ajatus autonomisista lohkoketjuista, joita sääntely ei kosketa. Tämä johtuu myös alkuperäisistä ajatuksista, että lohkoketjuissa irtaudutaan kolmansista osapuolista. BaaS myötä BaaS-tarjoajasta tulee merkittävä kolmas osapuoli, jonka on pakko reagoida paikalliseen sääntelyyn.

Blockchain as a Service kiihdyttää lohkoketjujen kehitystä, sillä suurempi määrä toimijoita lohkoketjujen ympärillä tarkoittaa, että niiden kehitykseen siirretään enemmän resursseja. Yritykset, joilla on perinteistä liiketoimintaa voivat tehdä helpommin investointeja omiin lohkoketjuihin, joista voi olla hyötyä myös muissa lohkoketjuissa. Samalla perinteiset liiketoiminnan yritykset myös tuovat mukanaan rahoitusta, joka on perinteiseltä rahoitussektorilta. Näin ollen lohkoketjujen pariin tulee resursseja sekä työvoiman että rahoituksen puolelle. Tästä voi hyvin tulla kiertävä kehä, jolloin kasvu voi kiihdyttää alan kasvua ja kehitystä yhä enemmän. BaaS:n käyttö tekee lohkoketjuista helpommin ymmärrettäviä teknologioita, sillä käytettäessä lohkoketjuja yleensä ymmärrystä niistä tulee myös asiakasyrityksen työntekijöille, jolloin ymmärrys lohkoketjuista kasvaa uudelle käyttäjäkunnalle.

Yksi havainto pilvipalveluiden tarjontaa tutkiessa oli, että osassa niistä lohkoketjuteknologia ja lohkoketju on erotettu toisistaan termeinä. Näissä tapauksissa lohkoketjuteknologia on teknologia, joka tarjoaa lohkoketjun tilikirjan käyttäjilleen hajautettuna konsensusta ylläpitävänä sovelluksena. Vaikuttaa kuitenkin siltä, että lohkoketjua pidetään monissa tapauksissa pelkkänä tilikirjana, joka sisältää datan nykyisen tilanteen ja datahistorian, sekä funktion, jonka avulla voidaan auditoida datan muuttumattomuutta. Ehdotankin, että näistä hajauttamattomista lohkoketjuista, joissa osa toiminnoista tapahtuu piilossa, puhuttaisiin yleensäkin tilikirjatietokantoina, sillä yleisesti lohkoketjuteknologiasta puhuttaessa käytetään usein termiä lohkoketju.

Tilikirjatietokanta on siis uuden tyyppinen tietokanta, joka pyrkii tuomaan samoja vahvuuksia kuin lohkoketjut pystyvät tarjoamaan, mutta niissä on luovuttu hajautuksesta kokonaan ja näin ollen myöskään konsensusalgoritmeilla ei ole virkaa suoraan tietokan-

nassa. Niiden avulla pystytään saavuttamaan tavallisen tietokannan tavoin tehokasta tietojenkäsittelyä, sillä niissä datan indeksointi on helpommin hallittavissa kuin hajautetuissa järjestelmissä. Tilikirjatietokantojen avulla yksittäinen yritys voi pyrkiä saamaan lohkoketjujen hyötyjä läpinäkyvyyden ja auditoitavuuden suhteen itselleen ilman yhteistyössä toimimista pitäen tietojärjestelmän tehokkaana. Niissä data ja datanhistoria erotetaan toisistaan, ja datahistoria ankkuroidaan muuttumattomaksi lohkoketjujen lohkojen tavoin kryptauksella. Tilikirjatietokannoissa jokaisella käyttäjällä on oma pseudonyyminsä ja sen avulla on selvitettävissä, että kuka dataa on muokannut ja milloin.

9 Yhteenveto

Tutkimuksen tavoite oli vastata, että minkälainen vaikutus lohkoketjujen pilvipalveluiden Blockchain as a Servicellä on lohkoketjuihin. Jotta tutkimuskysymykseen voitiin vastata, tuotiin tutkimuksen alussa esiin, että minkälaisia ajatuksia lohkoketjujen taustalla on ja mitä lohkoketjut oikein ovat. Kysymykseen vastaaminen vaati myös selvityksen siitä, että mikä on pilvipalveluiden tarjoama lohkoketjupalvelu Blockchain as a Service. Tutkimuksessa tuotiin ilmi, että se muuttaa perinteisiä lohkoketjuja siirtämällä lohkoketjun pilveen keskitetylle toimijalle, ja että se sotii alkuperäistä lohkoketjujen ajatusta vastaan ottamalla lohkoketjuihin keskeiseen rooliin kolmannen osapuolen. Tutkimuskysymykseen laajempaan vastaamiseen esiteltiin lohkoketjujen skaalautuvuuden trilemman joka on teoria, skaalautuvuuden trilemman teoria, jonka mukaan kaikissa lohkoketjuteknologioissa tulee tasapainotella desentralisaation, skaalautuvuuden ja tietoturvallisuuden suhteen. Lohkoketjujen skaalautuvuuden trilemma auttaa itsessään ymmärtämään lohkoketjuja paremmin, mutta se on teoria, jonka pohjalta voi arvioida erilaisten lohkoketjuteknologioiden painotusta sen suhteen, että minkälainen tasapaino niihin on löydetty trilemman eri osa-alueista. Tutkimuksessa on sen lisäksi pyritty tuottamaan ymmärrystä siitä, että mihin lohkoketjut ja BaaS soveltuvat, sillä ilman käyttötarkoituksien ymmärrystä ei tämä tutkimuskaan pysty tuottamaan arvoa muille kuin alan asiantuntijoille.

Pilvipalveluiden tarjoamat Blockchain as a Service lohkoketjupalvelut ovat siis palveluja, joiden avulla yritykset pääsevät pienimmällä vaivalla itse kiinni suljettuihin lohkoketjuihin. Niiden hyötynä on se, että yritys saa ulkoistettua lohkoketjun kehittämisen ulkoiselle toimijalle, jolloin yhtiöt pääsevät keskittymään omaan ydinosaamiseensa uuden tietojärjestelmän suunnittelussa, ja saavat käyttöönsä lohkoketjujen tarjoamat hyödyt. Haittapuolena on puolestaan se, että palveluntarjoajaan joudutaan lukkiutumaan, sillä vaikka itse lohkoketjun siirtäminen toiselle palveluntarjoajalle on suuri haaste niin vielä suurempi haaste olisi saada kaikki muut konsortion jäsenet vakuuttuneeksi siitä, että palveluntarjoajaa kannattaa vaihtaa.

Julkisten ja suljettujen lohkoketjujen käyttökohteet ovat erityyppisiä. Useimmin julkisten lohkoketjujen käyttäminen liiketoiminnassa tarkoittaa, että julkisen lohkoketjun sisältämää kryptovaluuttaa käsitellään älysopimuksen kautta. Esimerkkinä tästä tutkimuksessa on esitelty hajautetun rahoitussektorin puolelta Aave, joka tuottaa finanssipalveluja älysopimuksen avulla. Suljetuissa lohkoketjuissa puolestaan usein luodaan toimijoille kokonaan oma lohkoketju, johon sisällytetään toimialalle oleellisia tuotteita, joissa luotettavampi tieto tuo arvoa itsessään. Näissä lohkoketjuissa osapuolet toimivat yhteistyössä vähintäänkin lohkoketjun kautta. Lohkoketjun avulla osapuolet voivat jakaa toisilleen kriittistä informaatiota nopeammin. Tästä esimerkkitapauksena tutkimuksessa käytettiin IBM Food Trust -lohkoketjua, jonka avulla ruuan toimitusketju digitalisoitiin lohkoket-

juun ja sen avulla ongelmatilanteissa on löydettävissä ne erät, joita ongelma koskee. Tietojärjestelmän avulla sen jäsenet voivat myös viestiä toisilleen, mikäli jokin erä olisi syytä saada pois myynnistä.

Tutkimuksessa vastattiin kysymykseen, että mikä vaikutus pilvipalveluiden Blockchain as a Service -lohkoketjuilla on lohkoketjuihin lyhykäisyydessään näin: BaaS on vielä uusi teknologia ja sen vaikutusten arviointi on vielä hankalaa. On kuitenkin viitteitä siitä, että se toisi yritystoimintaa ja lohkoketjuja lähemmäs toisiaan, jolloin ne voisivat päästä symbioosiin keskenään. Tästä voi seurata kehä, joka auttaa molempia kehittymään yhä kiihtyvässä tahdissa. Suurin haaste tässä on kuitenkin se, että se vaatii muutoksia asenteisiin ja ajatteluun niin liiketoiminnassa kuin lohkoketjuyhteisöissä.

Tätä tutkimusta voi hyvin hyödyntää kuka tahansa, joka haluaa ymmärtää lohkoketjuja. Tutkimuksen näkökulma on yritys- ja organisaatiolähtöinen, ja sen vuoksi se voi auttaa puntaroimaan lohkoketjujen käyttöönottoa organisaatioissa. Se voisi auttaa myös julkisten lohkoketjujen parissa toimivia kehittäjiä ymmärtämään yritysten mukaantulon vaikutuksen koko lohkoketjualalle. Tutkimus antaa lähtökohdan ymmärtää aihealuetta ja alan tutkimusta osallistuen aiheen akateemiseen keskusteluun. Uusia keskustelunavauksia tässä työssä ovat ainakin hajautetusta organisaatiosta Aaveesta ja tilikirjatietokannoista. Suomenkielisessä tutkimuksessa ja julkisessa keskustelussa ei ole vielä ollut juurikaan puhetta myöskään Blockchain as a Service -palveluista.

Lohkoketjut ovat jatkuvasti ja nopeasti kehittyvä aihe, johon parhaillaan kohdistuu paljon kehitys- ja tutkimustyötä. Tästä syystä käsitykset lohkoketjuista saattavat muuttua nopeastikin ja tässäkin tutkimuksessa esiin tuotuja asioita on syytä tarkastella uudestaan lähitulevaisuudessa. Lohkoketjuaiheisia jatkotutkimuskohteita löytyisi siis paljon. Voi hyvin olla, että tulevaisuudessa monella alalla on lähdetty mukaan lohkoketjuihin BaaS:n kautta tai voidaan todeta, että on parempi olla käyttämättä niitä. Olisi mielenkiintoista tietää syitä näiden päätösten taustalla, sillä nyt suurin este hyödyntämiselle on teknologian ymmärryksen ja käyttötarkoitusten puute, jolloin lohkoketjuihin investointi on vähäistä. Myös Ethereum 2.0 päivitys on tulossa lähiaikoina ja sen odotetaan vaikuttavan suuresti lohkoketjuihin. Päivityksen jälkeen olisi mielenkiintoista arvioida, että miten se vaikuttaa lohkoketjujen kehitykseen. Olisi myös mielenkiintoista saada selville, että tuoko se itsessään enemmän yritystoimintaa mukaan lohkoketjuihin tai kasvaako hajautettujen organisaatioiden määrä merkittävästi. On myös mielenkiintoista seurata, että mikä vaikutus BaaS-lohkoketjuilla on pidemmällä aikavälillä niin markkinaan kuin itse lohkoketjuihin.

10 Viiteluettelo

Altarawneh, Amani, Tom Herschberg, Sai Medury, Farah Kandah, and Anthony Skjellum. 2020. Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms. *2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE*.

AWS Whitepaper. 2022. Overview of Amazon Web Services: AWS Whitepaper. Julkaistu: 12.1.2022 Saatavilla: https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html. Katsottu: 18.3.2022.

AWS Release history. 2022. Release history for Amazon QLDB. Julkaistu: 11.4.2022 Julkaistu: https://docs.aws.amazon.com/qldb/latest/developerguide/document-history.html. Katsottu: 12.4.2022.

Azure Blockchain Saatavilla: https://azure.microsoft.com/en-us/solutions/blockchain/#overview. Katsottu: 22.4.2022.

Azure Documentation. 2022. Azure SQL Database ledger. Julkaistu: 18.2.2022 Saatavilla: https://docs.microsoft.com/en-us/azure/azure-sql/database/ledger-overview. Katsottu: 12.4.2022

Azure EBaaS 2015. Julkaistu: 9.11.2015. Saatavilla: https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/. Katsottu: 22.4.2022.

Azure Whitepaper. 2019. What are Blockchain-Enabled Digital Ecosystems Why they are Vital to Your Digital Transformation. Julkaistu: 29.4.2020 Saatavilla: https://azure.microsoft.com/en-us/resources/what-are-blockchain-enabled-digital-ecosystems/. Checked: 25.3.2022

Bamakan, Seyed Mojtaba Hosseini, Amirhossein Motavali, and Alireza Babaei Bondarti. 2020. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications* 154 113385.

Belchior, Rafael, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2021. A survey on blockchain interoperability Past, present, and future trends. *ACM Computing Surveys (CSUR*) 54(8) 1-41.

Buterin, Vitalik. 2014. Ethereum: A next-generation smart contract and decentralized application platform. *Ethereum Project White Paper*.

Buterin, Vitalik. 2017. The meaning of decentralization. *Medium.com*. Saatavilla: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Katsottu: 1.4.2022

Canelis, David. 2019. More than 60% of Ethereum nodes run in the cloud, mostly on Amazon Web Services Is this decentralization? *thenextweb* Julkaistu: 23.9.2019. Saatavilla: https://thenextweb.com/news/ethereum-nodes-cloud-services-amazon-web-services-blockchain-hosted-decentralization Katsottu 22.4.2022

Chow, Stefen, and Morgen E. Peck. 2017. The bitcoin mines of China. *IEEE Spectrum* 54(10) 46-53.

Crank, Joel. 2021. Wyoming DAO LLCs: Potential Pitfalls for the Novel Entity. *SSRN 3950916.*

Crosby, Michael, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation 2.6-10*: 71.

ETH.wiki. Sharding faq. *Ethereum.* Saatavilla: https://eth.wiki/sharding/Sharding-FAQs Katsottu: 31.3.2022.

Felin, Teppo, & Karim Lakhani. 2018. What problems will you solve with blockchain?. *MIT Sloan Management Review*.

Jiang, Shangrong, Yuze Li, Shouyang Wang, and Lin Zhao. 2022. Blockchain competition: The tradeoff between platform stability and efficiency. *European Journal of Operational Research* 296(3) 1084-1097.

Hyperledger Members. Saatavilla: https://www.hyperledger.org/about/members Katsottu: 14.4.2022

HS-Reuters. 2021. Intia on kieltämässä krypto-valuutat lailla, jopa omistaminen johtaisi sakkoihin. *Helsingin Sanomat.* Julkaistu: 16.3.2021. Saatavilla: https://www.hs.fi/talous/art-2000007863655.html. Luettu: 29.4.2022.

Johansson, Patrik Elias, Mikko Eerola, Antti Innanen, Juha Viitala, ja Mikko Alasaarela. 2019. Lohkoketju-Tiekartta päättäjille. *Alma Talent Oy*.

Kassen, Maxat. 2022. Blockchain and e-government innovation: Automation of public information processes. *Information Systems* 103 101862.

Kilroy, Karen. 2019. Blockchain as a Service - Understanding the Landscape and Potential Benefits. First edition. Sebastopol, CA: O'Reilly Media. Print.

Lacity, Mary, and Remko Van Hoek. 2021. What We've Learned So Far About Blockchain for Business. *MIT Sloan Management Review* 62(3), 48-54.

Lappalainen, Elina. 2022. Sota ja pakotteet nostivat kryptovaluuttojen sääntelyn uuteen rooliin. *Helsingin Sanomat*. Julkaistu: 14.3.2022. Saatavilla: https://www.hs.fi/visio/art-2000008670920.html?share=8a4810c9874e1ecc5b369a7462435b84. Luettu: 13.4.2022.

Lin, Fei, and Minqian Qiang. 2018. The challenges of existence, status, and value for improving blockchain. *IEEE Access* 7 7747-7758.

Fekete, Dénes László, and Attila Kiss. 2021. A Survey of Ledger Technology-Based Databases. *Future Internet* 13(8) 197.

Ma, Zhaofeng, Weizhe Zhao, Shoushan Luo, and Lingyun Wang. 2020. TrustedBaaS: blockchain-enabled distributed and higher-level trusted platform. *Computer Networks*, 183 107600.

Mogavero, Francesco, Ivan Visconti, Andrea Vitaletti, and Marco Zecchini. 2021. The Blockchain Quadrilemma: When Also Computational Effectiveness Matters. *2021 IEEE Symposium on Computers and Communications (ISCC). IEEE.*

Nakamoto, Satoshi 2008. A peer-to-peer electronic cash system. *Bitcoin*. Saatavilla: https://bitcoin.org/bitcoin.pdf. Katsottu: 18.3.2022.

Rantala, Juho. 2018a. Lohkoketjuteknologian yhteiskunta. Osa I: Bitcoinista Ethereumiin. *Niin & Näin.*

Rantala, Juho. 2018b. Lohkoketjuteknologian yhteiskunta. Osa II: Rajatut, desentralisoidut markkinat. *Niin & Näin.*

Rantala, Juho, & Outi Korhonen 2021. Lohkoketjuteknologian yhteiskunta. Osa III: Hajahuomioita uniikeista tokeneista. *Niin & Näin*.

Song, Jie, Pengyi Zhang, Mohammed Alkubati, Yubin Bao, and Ge Yu. 2021. Research advances on blockchain-as-a-service: Architectures, applications and challenges. *Digital Communications and Networks*.

Tietosuoja.fi Saatavilla: https://tietosuoja.fi/gdpr. Katsottu: 4.5.2022

Wan, Zhitao, Cai Minqiang, Yang Jinqing, and Lin Xianghua. 2018. A novel blockchain as a service paradigm. *International Conference on Blockchain.* 267-273. Springer, Cham.

Yang, Xinying, Yuan Zhang, Sheng Wang, Benquan Yu, Feifei Li, Yize Li, and Wenyuan Yan. 2020. LedgerDB: A centralized ledger database for universal audit and verification. *VLDB Endowment*, 13(12), 3138-3151.

Zheng, Weilin, Zibin Zheng, Xiangping Chen, Kemian Dai, Peishan Li, and Renfei Chen. 2019. Nutbaas: A blockchain-as-a-service platform. *Ieee Access*, 7, 134422-134433.

Podcastit ja videot:

Buterin, Vitalik & Lex Fridman. 2021. Vitalik Buterin: Ethereum 2.0 | Lex Fridman Podcast #188. *Lex Fridman Podcast*. Julkaistu: 4.6.2021. Saatavilla: https://www.youtube.com/watch?v=XW0QZmtbjvs. Katsottu: 16.4.2022.

Finematics. 2021. AAVE - The Road To $3 Billion - DEFI Explained. *Finematics*. Julkaistu: 20.1.2021. Saatavilla: https://www.youtube.com/watch?v=WwE3lUq51gQ. Katsottu: 16.4.2022.

Finematics. 2019. Lightning Network Explained. *Finematics*. Julkaistu: 17.4.2019. saatavilla: https://www.youtube.com/watch?v=9UIOeoBEjmw. Katsottu: 29.4.2022.

Harviainen, Tuomas, Henry Tikkanen. 2021. Internetin pimeä puoli | Tiedetrippi. *Tiedetrippi*. Yle. Julkaistu: 29.11.2021. Saatavilla: https://areena.yle.fi/audio/1-50953344. Katsottu: 16.4.2022.

Heinonen, Henri, Henry Tikkanen. 2021. Salaperäinen Satoshi Nakamoto – Bitcoinin tuntematon luoja | Tiedetrippi. *Tiedetrippi*. Yle. Julkaistu: 12.4.2021. Saatavilla: https://areena.yle.fi/audio/1-50760473. Katsottu: 29.4.2022.

Kulechov, Stani, Martin Paasi ja Miikka Luukkonen. 2021. Kryptovaluutta, uusi maailmanvaluutta? Vieraana Stani Kulechov | #rahapodi 230. *#rahapodi*. Nordnet. Julkaistu: 8.1.2021. Saatavilla: https://www.nordnet.fi/blogi/kryptovaluutta-uusi-maailmanvaluutta-vieraana-stani-kulechov-rahapodi-230/. Katsottu: 29.4.2022.

Miettinen, Sami, Martin Wichmann ja Leevi Leino. 2022. Digimarkka, rahajärjestelmät ja huoltovarmuus (Sami Miettinen & Martin Wichmann) | Puheenaihe 230. *Puheenaihe*. Puhemedia. Nauhoitettu 28.3.2022. Saatavilla: https://podtail.com/fi/podcast/-puheenaihe/digimarkka-rahajarjestelmat-ja-huoltovarmuus-sami-/. Katsottu: 29.4.2022.

Päivinen, Teemu, Martin Wichmann ja Rami Kurimo. 2021. Ethereum ja layer 2 -teknologiat (Teemu Päivinen) | Lohkoketju 2. *Lohkoketju*. Puhemedia. Nauhoitettu: 8.10.2021. Saatavilla: https://podtail.com/fi/podcast/lohkoketju-1/ethereum-ja-layer-2-teknologiat-teemu-paivinen-loh/. Katsottu: 16.4.2022.

Wichmann, Martin, Rami Kurimo. 2021. Ethereum, älysopimukset, DeFi ja NFT (Martin Wichmann) | Lohkoketju 1. *Lohkoketju*. Puhemedia. Nauhoitettu: 22.10.2021. Saatavilla: https://podtail.com/fi/podcast/lohkoketju-1/ethereum-alysopimukset-defi-ja-nft-martin-wichmann/. Katsottu: 16.4.2022.