

Katja Talvela

**LOHKOKETJUTEKNOLOGIAN HYÖDYNTÄMINEN
FINANSSIALALLA - HAJAUTETTU RAHOITUS**



JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Talvela, Katja

Lohkoketjuteknologian hyödyntäminen finanssialalla – Hajautettu rahoitus

Jyväskylä: Jyväskylän yliopisto, 2022, 35 s.

Tietojärjestelmätiede, kandidaatintutkielma

Ohjaaja: Halttunen, Veikko

Tutkielmassa tarkastellaan lohkoketjuteknologian hyödyntämistä finanssialalla sekä sen mahdollista potentiaalia muuttaa alan perustaa. Lohkoketjut ovat nykypäivän trendi, mutta niiden käyttö on vielä vähäistä verrattuna nähtyihin mahdollisuuksiin, minkä takia tällaisen tutkielman tekeminen onkin perusteltua. Tämän lisäksi motiivina tutkielman tekemiseen toimii kirjoittajan oma kiinnostus tutustua aiheeseen syvemmin. Tutkielma on toteutettu kirjallisuuskatsauksena ja siinä perehdytään erityisesti siihen, kuinka lohkoketjuilla voitaisiin tehostaa finanssialan toimintaa, millaisia hyötyjä käyttöönotto on mukanaan alalle tuonut sekä millaisissa prosesseissa sitä voitaisiin vielä tulevaisuudessa tehokkaammin hyödyntää. Kontrastina koettuihin hyötyihin pohditaan myös syitä, miksi lohkoketjuteknologian käyttöönotto ja hyödyntäminen on haastavaa finanssialalla sekä millaisia rajoituksia siihen nykypäivänä vielä liittyy. Tutkimustuloksina esitetään finanssialalla todistettuja lohkoketjujen käyttökohteita muun muassa erilaisien älysopimuksia käyttävien hajautettujen finanssiapplikaatioiden muodossa. Lopussa eritellään myös oikeudellisia, kaupallisia ja teknologisia haasteita, joita tutkimuksista on ilmennyt.

Asiasanat: DeFi, Finanssiala, Hajautettu rahoitus, Lohkoketjuteknologia, Älysopimus

ABSTRACT

Talvela, Katja

Utilizing Blockchain Technology in Finance – Decentralized Finance

Jyväskylä: University of Jyväskylä, 2022, 35 pp.

Information Systems Science, Bachelor's Thesis

Supervisor: Halttunen, Veikko

The thesis examines the use of blockchain technology in finance and its potential to change the foundation of the industry. Blockchains are a trend today, but their use is still limited compared to the opportunities seen, which is why such a thesis is justified. In addition, motivation for writing this thesis is the author's own interest in exploring the subject in more depth. The thesis has been carried out as a literature review and it focuses on how blockchains are used to improve the efficiency of the financial sector, and the processes in which they could be utilized more effectively in the future. In contrast to the perceived benefits, the paper also considers the reasons why the implementation of blockchain technology in the financial sector is challenging and the limitations that still exist today. The results of the research will present proven applications of blockchain in the financial sector, including various distributed financial applications using smart contracts. Finally presenting the legal, commercial, and technological challenges that have emerged from the research.

Keywords: Blockchain, DeFi, Decentralized Finance, Finance, Smart Contracts

KUVIOT

KUVIO 1	Lohkoketjun rakenne	12
KUVIO 2	DeFi-sovelluksien rakenne julkisissa lohkoketjuissa	21

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

KUVIOT

1	JOHDANTO.....	6
2	LOHKOKETJUTEKNOLOGIA	9
	2.1 Toimintaperiaate.....	9
	2.2 Rakenne.....	11
	2.3 Konsensusmekanismi.....	12
	2.4 Lohkoketjujen hyödyt	13
3	FINANSSIALA	15
	3.1 Nykyaikainen rajoitusjärjestelmä.....	15
	3.2 Finanssialan prosessit.....	17
4	HAJAUTETTU RAHOITUS.....	18
	4.1 DeFi-sovellukset.....	19
	4.2 Ethereum.....	21
	4.3 Älysopimus.....	22
5	MAHDOLLISUUDET JA HAASTEET	23
	5.1 Mahdollisuudet finanssialalla.....	24
	5.1.1 Hajautetut finanssiapplikaatiot.....	25
	5.1.2 Arvonsiirto	26
	5.1.3 Kustannukset	26
	5.1.4 Varainhankinta ja sijoittaminen	27
	5.2 Käyttöä rajoittavat tekijät	27
	5.2.1 Oikeudelliset ja sääntelyyn liittyvät rajoitteet.....	28
	5.2.2 Kaupalliset rajoitteet	28
	5.2.3 Tekniset rajoitteet	29
6	YHTEENVETO JA POHDINTA	31
	LÄHTEET	33

1 JOHDANTO

Tässä tutkielmassa tarkastellaan lohkoketjujen hyödyntämistä finanssialalla ja niiden potentiaalia suorittaa alan prosesseja tehokkaammin. Lohkoketjuteknologia on nykyään noussut suureksi trendiksi ja sen mahdollisuuksiin uskotaan vahvasti monellakin alalla. Teknologian potentiaalista huolimatta näyttöjä sen hyödyntämisestä on todistetusti melko vähän verrattuna sen uskottuihin mahdollisuuksiin (Tilooby, 2018). Sen vuoksi tällaisen tutkimuksen tekeminen on varsin perusteltua ja tämän kirjallisuuskatsauksen myötä ymmärrystä aiheesta kokonaisuudessaan olisi tarkoitus pystyä hahmottamaan selkeämmin.

Lohkoketjut nousivat monien tietoisuuteen kryptovaluutta Bitcoinin myötä vuonna 2009, jonka jälkeen kiinnostus tätä teknologiaa kohtaan on kasvanut nousujohteisesti (Yli-Huumo, Ko, Choi, Park & Smolander, 2016). Kasvaneen kiinnostuksen sekä teknologian uutuuden vuoksi onkin alettu perehtymään lisää, mihin kaikkeen kyseistä teknologiaa voitaisiin hyödyntää kryptovaluuttojen lisäksi. Satoshi Nakamoton (2009) kirjoittama artikkeli "Bitcoin: A Peer-to-Peer Electronic Cash System" on lohkoketjujen tutkimuksen saralla noussut ikoniseksi artikkeliksi. Tämänkin tutkielman usea lähde on viitannut artikkeliin, jossa Nakamoto esittelee ja perustelee teknologiaa Bitcoinin takana. Ennen kyseisen artikkelin ja Bitcoinin julkistusta lohkoketjut eivät olleet juurikaan kiinnostava teknologia huolimatta siitä, että niiden historia osittain ulottuu paljon kauemmas.

Vaikka lohkoketjujen mahdollisuuksia uskotaan olevan monella eri alalla, nähdään finanssialan toimijat kuitenkin sen avainkäyttäjiksi (Nofer, Gomper, Hinz & Dirk, 2017). Finanssiala ja etenkin rahoitusmarkkinat mielletään usein todella laajoiksi ja monimutkaisiksi markkinoiksi, joiden toimiminen vaatii useita välikäsiä. Finanssiala sisältää paljon ongelmallisia kohtia, joiden myötä esimerkiksi kustannukset niin asiakkaiden kuin yritystenkin näkökulmasta ovat melko suuret. Prosessien jäykkyyden ja monivaiheisuuden vuoksi ne ovat alttiita myöhästymisille sekä vaativat monimutkaista paperityötä, joka työläyden lisäksi on erittäin haavoittuvaista myös rikoksille (Tapscott & Tapscott, 2017). Näihin alan epäkohtiin on alettu etsimään potentiaalisia ratkaisuja lohkoketjuteknologiaan nojautuen. Tutkimuksen myötä on löydetty uusia hajautettuja

malleja toteuttaa erilaisia prosesseja finanssialalla tehokkaammin, luotettavammin ja yksityisemmin. Finanssiala vaatii laajan skaalan erilaisia toimijoita ja prosesseja toteutuakseen. Apua lohkoketjujen käytöstä voitaisiin saada esimerkiksi myynti- ja ostoprosessien erilaisiin sopimuksiin liittyen. Näissä pystyttäisiin hyödyntämään lohkoketjuteknologiaa soveltaen sitä esimerkiksi toimeksiantojen automatisoinnissa. Lohkoketjujen avulla voidaan poistaa prosesseista välikäsiä ja tämän myötä saada niistä tehokkaita sekä turvallisia, ilman vaaraa lisääntyneestä rikollisuudesta. Tässä tutkielmassa tutustutaan näihin keinoihin ja niiden tuomiin vaikutuksiin finanssialalla.

Rahoitusmarkkinat ja etenkin pankkisektori ovat kokeneet luottamuspu-
laa erilaisten talouskriisien ja uudenlaisten rikosten myötä viime vuosikymmeninä. Näiden seurauksena, kun luottamus keskitettyihin toimijoihin on ollut koetuksella, ihailu keskittämättömiä järjestelmiä kohtaan on kasvanut. Varman (2019) tekemän tutkimusartikkelin mukaan lohkoketjuteknologian avulla voidaan luoda luottamusta ja turvaa eri prosessien ympärille, sillä kyseinen teknologia on läpinäkyvä ja avoin sen kaikille käyttäjäosapuolille. Lohkoketjujen sanotaan olevan avoimia ja muuttumattomia jaettuina digitaalisia tilikirjoja, joiden muutoshistoria on sen kaikkien käyttäjien tarkasteltavissa. Lohkoketjujen identifiointi yksilöllisillä tunnisteilla tekee teknologiasta myös peukaloinnin kestävä. Näitä uniikkeja tunnisteita kutsutaan tiivisteiksi ja niiden toimiminen perustuu päällekkäisyyteen edellisten lohkojen mukaan, mistä tuleekin teknologian nimeen sana "ketju". (Varma, 2019.)

Yhtenä käytännön esimerkkinä lohkoketjujen hyödyntämisestä voidaan mainita älysopimukset, joiden käyttö on alkanut viime vuosina lisääntymään ja niiden tehokkuutta on alettu osata hyödyntää monenlaisissa tilanteissa. Näiden avulla pystytään muun muassa alentamaan neuvotteluihin käytettäviä resursseja sekä automatisoimaan prosesseja, jotka tekevät sopimuksista kustannustehokkaita. Toki älysopimusten solmiminen periaatteessa onnistuu myös ilman lohkoketjuteknologiaa, mutta sen tärkein siitä saavutettava hyöty, tehokkuuden rinnalla, onkin lohkoketjujen tuoma luottamus sopimusten oikeellisuuteen ja muuttumattomuuteen.

Tutkielman tutkimusongelma jakautuu kahteen kysymykseen: 1. Kuinka lohkoketjuja voidaan hyödyntää finanssialan eri prosesseissa? ja 2. Mitä mahdollisuuksia ja haasteita on lohkoketjun käyttöönottoon liittyen havaittu? Tutkielma on toteutettu kirjallisuuskatsauksena ja aineiston hankinnassa on hyödynnetty erityisesti muun muassa palveluita Google Scholar ja JYKDOK. Läheteitä on etsitty myös suoraan tietojärjestelmätieteen saralla merkittäviksi lehdiksi arvioituista "Information Systems Journal" sekä "Journal of Information Technology" -lehdistä. Lähteiden laadun arvioinnissa on ollut käytössä Julkaisufoorumin julkaisukanavahaku, jonka mukaan lähteet on pyritty valitsemaan mahdollisimman korkealaatuisiksi asteikolla 1–3. Lähteissä, joita ei kyseisestä hakupalvelusta ole löytynyt, on arvioitu kriittisesti asiasisällön lisäksi muun muassa kirjoittajaa sekä julkaisupaikkaa.

Seuraavaksi kuvataan lyhyesti tutkielman kulku ja rakenne. Tutkielman luvussa 2 perehdytään lohkoketjuteknologiaan ja sen toimintaperiaatteeseen.

Tämän ohessa sivutaan myös hieman lohkoketjuihin liitettyjä yleisiä hyötyjä. Kolmannessa luvussa määritellään finanssiala tutkielman kannalta sekä eritellään sen prosesseja. Neljännessä luvussa käydään läpi keinoja ja tilanteita, missä lohkoketjuteknologiaa käytetään. Näiden yhteydessä tutustutaan lohkoketjujen mahdollistamaan uudenlaiseen rahoitusmuotoon eli hajautettuun rahoitukseen. Lopuksi luvussa 5 perehdytään enemmän lohkoketjujen nähtyyn potentiaaliin tulevaisuudessa sekä käydään läpi millaisia hyötyjä ja haasteita on lohkoketjujen käyttöönotossa huomattu.

2 LOHKOKETJUTEKNOLOGIA

Finanssialalla lohkoketjujen avainkomponenteiksi luokitellaan muun muassa älysopimuksia hyödyntävät sovellukset, rahaliikennettä ja transaktiologiikkaa määrittelevät sopimukset sekä lohkoketjualustat, jotka tarjoavat edellä mainituille toimintaympäristön. Yksi lohkoketjujen suurimmista eroista tavallisiin tietokantoihin on niiden jaettu perusta. Ideana on, ettei kukaan omista niitä eikä niillä ole mitään keskitettyä hallitsevaa toimijaa. Tällainen pohja lisää läpinäkyvyyttä teknologian ympärille ja tämän myötä luottamus toiminnan oikeellisuuteen kasvaa. Lohkoketjuja on julkisia ja yksityisiä eli niiden avoimuuteen pystytään myös vaikuttamaan, vaikka yleisesti ottaen niitä pidetäänkin kaikille avoimina. (Varma, 2019.)

Tässä luvussa perehdytään tarkemmin lohkoketjuteknologian toimintaperiaatteeseen sekä sen käytön tuomiin hyötyihin. Luvussa käydään läpi teknologian rakenne lohkoketjujen taustalla sekä perehdytään eri toiminnallisuuksiin, jotka luovat hyötyjä teknologian ympärille. Edellä mainittuihin alustaratkaisuihin palataan luvussa 4, kun tarkastellaan niitä finanssiapplikaatioiden näkökulmasta.

2.1 Toimintaperiaate

Lohkoketjujen peruseriaate nimensä mukaan on, että tapahtumat muodostavat lohkoja ja näistä lohkoista muodostuu ketju, kun lohkot kasautuvat päällekkäin kronologisesti. Lohko voi tarkoittaa esimerkiksi kryptovaluuttaa vaihdettaessa kirjaa transaktioista eli valuutan omistuksen muutoksista. Jokainen tällainen transaktio kirjautuu lohkoketjuun linkitetysti toisiinsa yksilöityjen tiivisteiden avulla. Näistä tapahtumista muodostuu kaikille lohkoketjua varmantaville osapuolille avoin tilikirja. (Treleaven, Brown & Yang, 2017.)

Transaktiot ovat kirjauksia kahden tai useamman osapuolen kesken tapahtuneesta vaihdoksesta. Yleisesti ottaen vaihdos voi liittyä mihin tahansa palveluun tai hyödykkeeseen, mutta finanssialalla lohkoketjuista puhuttaessa ne

yleensä ovat yhteydessä omaisuuseriin jossakin muodossa. Vaikka lohkojen sanotaan useimmiten olevan kirjauksia tämän tyylistä transaktioista, voivat ne kuitenkin koostua muustakin datasta esimerkiksi älysovimuksien yhteydessä ohjelmoiduista funktioista. (Chakravarty & Sarkar, 2020 s. 137–138.)

Verrattuna perinteisiin tietokantoihin lohkoketjujen toimintaperiaate perustuu niiden jaettavuuteen ja hajautettuun rakenteeseen. Lohkoketjuteknologiaan pohjautuvissa palveluissa käyttäjistä puhutaan solmuina (engl. node). Vielä tarkemmin sanottuna solmuilla tarkoitetaan käyttäjän laitetta, esimerkiksi tietokonetta, eli päätettä, jolla verkkoon ja muihin käyttäjiin ollaan yhteydessä (Chakravarty & Sarkar, 2020, s.140). Solmujen tehtävä on varmentaa tapahtumia lohkoketjussa sen lisäksi, että ne osallistuvat transaktioiden myötä tapahtumien muodostumiseen. Tällaiseen varmentamiseen perustuu lähdekoodin avoimuus ja lohkoketjujen läpinäkyvyys, kun jokainen solmu saa tarkasteltavakseen kopion tilikirjasta. Jokaisella lohkoketjun solmulla on tämän myötä pääsy tarkastelemaan koko tietokantaa ja versiohistoriaa, jos näitä ei tietoturvan vuoksi ole rajoitettu pääsyoikeuksilla. Kukaan ei kuitenkaan itsenäisesti pysty hallitsemaan tai omistamaan lohkoketjujen sisältämää dataa tai tietoa, vaan muutokset ja lisäykset lohkoketjuun vaativat hyväksynnän lohkoketjun muilta käyttäjiltä toteutuakseen. (Amesar, Mali, Nerkar, Nitnaware & Prashant, 2020.)

Edellä mainitut päätteet eli solmut toimivat vertaisverkoissa (engl. peer-to-peer network), joilla ei ole keskusasiaa vaan ne rakentuvat kaikista verkon komponenteista yhteisesti. Yleisesti tunnettu esimerkki hahmottamaan tämän tyylistä verkkoa on erilaiset tiedostojen jakamiseen tarkoitettut järjestelmät vaikkapa pilvipalvelut, jotka synkronoituvat reaaliaikaisesti. Näissä data tallentuu verkon kaikille asemille eli lohkoketjujen yhteydessä puhuttaessa solmuille. (Chakravarty & Sarkar, 2020, s.134: Amesar ym., 2020.) Luvussa 2.3 käydään läpi lohkoketjujen konsensusmekanismia, jossa palataan solmujen suorittamaan varmennukseen ja sen synnyttämään yhteisymmärrykseen eli konsensukseen.

Lohkoketjut voidaan jaotella esimerkiksi kaikille avoimiksi, yhteisöjen käyttöön tai yksityisiksi. Tämän mahdollistavat erilaiset alustarakaisut, joita lohkoketjuteknologiapohjaisille sovelluksille on käytettävissä. Riippuen alustasta, jota lohkoketjun toteutukseen käytetään, voidaan niihin lisätä rajoituksia tai oikeuksia, jotka dataa voivat tarkastella tai keillä on oikeus lisätä lohkoja ketjuun. Julkisista eli ”luvattomista” (engl. permissionless) lohkoketjuista ensimmäinen ja tunnetuin on kryptovaluutta Bitcoin. Tällaisiin lohkoketjuihin voi liittyä yksinkertaisesti kuka tahansa liittämällä tietokoneensa hajautettuun vertaisverkkoon, lataamalla lohkoketjupohjaisen applikaation sekä aloittamalla transaktioiden käsittelyn. Esimerkkinä tässä tutkielmassa perehdytään tarkemmin julkiseen alustaan Ethereumiin, mikä on älysovimuksiin perustuva alusta lohkoketjuapplikaatioille. Tähän palataan tarkemmin luvussa 4.2. Luvalisissa eli yksityisissä (engl. permissioned) lohkoketjuissa taas liittymiseen tarvitaan hyväksyntä verkon nykyisiltä käyttäjiltä. Tämän tyyllisiä yksityisiä lohkoketjuja käyttävät yleensä organisaatiot, jotka haluavat hyödyntää jaettua kirjaa tapahtumista organisaation sisällä. (Perwej, Perwej & Haq, 2019.)

Lohkoketjuissa jokainen lohko on solmittu toisiinsa linkitettyinä edeltäviin tapahtumiin. Erilaisia laskennallisia algoritmeja ja lähestymistapoja käytetään varmistamaan, että tallennettu data tietokantaan on pysyvä, kronologisesti järjestetty ja saatavilla kaikille muille verkossa toimiville. Tämän mahdollistavat digitaalinen allekirjoitus ja yksilöityjen tiivisteiden taustalla toimiva algoritmi. Nämä muodostavat yhdessä lohkoketjujen kryptografian (Perwej ym., 2019). Näihin tutustutaan tarkemmin seuraavassa luvussa, kun käydään läpi lohkoketjujen rakennetta ja tunnistettavien tiivisteiden muodostumista.

2.2 Rakenne

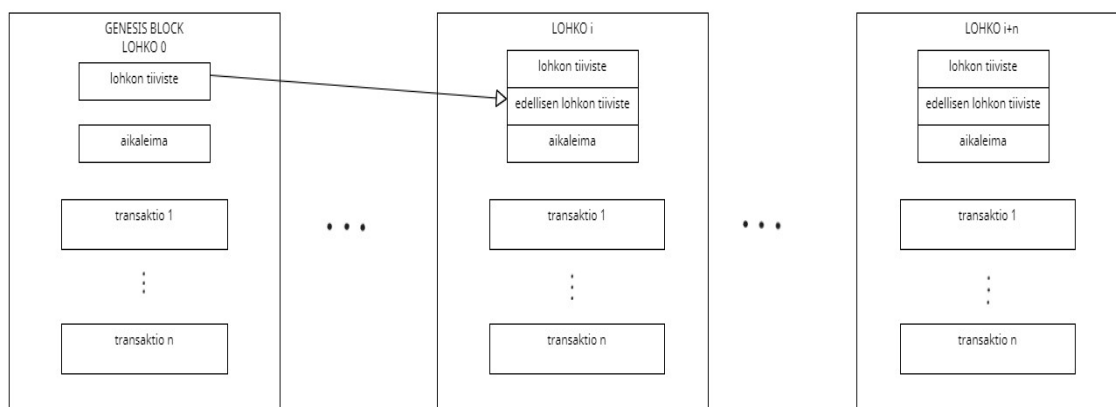
Kuten edellä mainittu, lohkoketjujen muuttumattomuus varmistetaan yksilöllimällä jokainen lohko uniikilla tiivisteellä (engl. hash) algoritmien avulla. Varman (2019) mukaan yksilöity tiiviste on luotu lohkojen tunnistamiseksi ja varmentamiseksi, jotta lohkojen sisältöä ei pystytä muuttamaan ilman jokaisen lohkon muuttamista ja uusien tiivisteiden muodostumista. Tällä käytännössä kuitenkin tarkoitetaan, että transaktiota on lähes mahdotonta muokata tai poistaa sen jälkeen, kun se on lohkoketjuun lisätty eli, kun tapahtuma on toteutunut (Chakravarty & Sarkar, 2020, s.139).

Erilaisien kirjaimista ja numeroista muodostuvien tiivisteiden toteutuksessa hyödynnetään algoritmeja. Yhdysvaltain kansallinen turvallisuusvirasto NSA on suunnitellut kryptografisia tiivistefunktioita, joista yksi yleisesti lohkoketjujen käytössä oleva on muun muassa SHA-256. Se on käytännössä 64 merkin eli numeron ja kirjaimen muodostama yksilöllinen merkkijono. Algoritmit luovat täsmälleen saman tiivisteeseen, jos data lohkoissa on täsmälleen sama kuin vertailtavassa yksilössä. Jos datassa taas muutetaan yhtäkään bittiä, saadaan täysin uusi tiiviste. Tämän myötä tiivisteet pysyvät lohkojen kesken yksilöllisinä, eikä samaa tiivistettä ole mahdollista olla olemassa ilman identtistä lohkoa. Lohkoketjuun lisätyn lohkon tiiviste on myös seuraavan lohkon lähtötieto ja tämän avulla lohkot ketjutetaan toisiinsa. (Perwej ym., 2019.)

Kirjassaan Chakravarty ja Sarkar (2020) tarkastelee algoritmeihin perustuvaa tunnistautumista esimerkin avulla, missä sopimuksen allekirjoittamiseen vaaditaan PKI eli "Public Key Infrastructure" -mekanismi. Tämän tarkoitus on olla ohittamaton tunnistautumisen avain ja vain kyseisellä avaimella voi päästä käsiksi salattuun dataan (Chakravarty & Sarkar, 2020, s. 132–133). Tällainen lohkoketjupohjainen varmentaminen perustuu digitaalisia allekirjoituksia hyödyntäviin avainmekanismeihin, joihin kuuluu kahdenlaisia avaimia, julkisia ja yksityisiä (engl. public and private key)(Amesar ym., 2020). Esimerkiksi Bitcoinin salausmekanismi koostuu tällaisista avaimista, joista julkista avainta käytetään osoittamaan henkilön Bitcoin-lompakko ja yksityisellä avaimella taas todennetaan käyttäjä (Yli-Huumo ym., 2016).

Kuten edellä käytiin läpi, lohkoketjun muodostavat lohkot sisältävät dataa esimerkiksi transaktioita tai älykkään sopimuksen suorittamaa koodia. Lisäksi lohkon lisätään edellä mainitut tiivisteet eli lohkon oma tiiviste sekä myös

edellisen lohkon tiiviste, jotta pystytään tarkastelemaan vaikkapa viimeisimmästä versiosta tehtyjä muutoksia. Kun tiivisteet tämän ansiosta linkittyvät toisiinsa lohkojen välillä, syntyy Merkle-juuri, jota käytetään nimenomaan havainnoimaan lohkojen järjestystä ja helpottamaan lohkojen tarkastelua. Lohkoketjujen ensimmäistä lohkoa kutsutaan englanniksi "Genesis Block", jota siis ei pystytä sitomaan mihinkään aikaisempaan lohkoon. Tässä tapauksessa lohko sisältää vain oman tiivisteensä ja Merkle-juuri alkaa kerääntymään vasta seuraavien lohkojen myötä. Edellisten lisäksi lohkoihin merkataan aina aikaleima, joka mahdollistaa ketjujen muodostumisen tapahtumien mukaan kronologisesti eli aikajärjestyksessä. (Amesar ym., 2020.) Alla oleva kuvio 1 on luotu kuvaamaan tätä lohkojen rakennetta.



KUVIO 1 Lohkoketjujen rakenne (Nofer ym., 2017)

2.3 Konsensusmekanismi

Lohkoketjujen varmentamista kaikkien osapuolten kesken, sekä tämän muodostamaa yhteisymmärrystä, kutsutaan konsensukseksi. Sen periaate on varmentaa tapahtumien aitous ja oikeellisuus, sekä poistaa joukosta sellaiset toimijat, jotka eivät noudata yhteisiä toimintatapoja. Konsensus auttaa lohkoketjua toimimaan ilman keskitettyä toimijaa, vaikka jokin verkon jäsen olisikin hetkelisesti toimimaton (Perweij ym., 2019). Lohkoketjun hajautetussa vertaisverkossa toimimisen tulee olla yleisten protokollien mukaista jokaiselta solmulta, mikä pystytään varmentamaan konsensuksen keinoin (Zhang, Wang & Wu, 2020). Lohkoketjua ei pystytä muokkaamaan tai poistamaan sen jälkeen, kun solmut ovat hyväksyneet tiedot. Tämän takia lohkoketjuissa datan sanotaan olevan eheää ja lohkoketjut ovat tunnettuja turvallisuudestaan ja läpinäkyvyydestään (Yli-Huumo ym., 2016). Tällaista varmentamista varten on kehitetty erilaisia konsensusmekanismeja, joista tässä tutkielmassa käydään läpi nykyään yleisimmin käytetyt proof-of-work- ja proof-of-stake- mekanismit. Näille ei suomen kielessä ole vakiintuneita käsitteitä, joten tässä tutkielmassa käytetään englanninkielisiä nimityksiä. Näiden kahden mekanismin ero piilee niiden varmenta-

mislogiikassa ja seuraavaksi tutkielmassa perehdytään niiden toimintaan tarkemmin.

Proof-of-work-mekanismi perustuu työntodentamiseen, mitä kryptovaluuttojen yhteydessä kutsutaan louhimiseksi (engl. mining) (Treleven ym., 2017). Louhinnassa solmuja niin sanotusti palkitaan tapahtumien varmentamisesta ja palkkio tällöin voi olla vaikkapa oikeus kryptovaluutan vaihtamiseen. Tässä ideana siis on varmentaa transaktiot ja muu toiminta vaatimalla käyttäjiltä kohtalainen määrä laskentatehoa saavuttaakseen oikeuden tiettyyn resurssiin. Tämän tyylinen työntodentaminen on käytössä muun muassa Bitcoinissa. (Yli-Huumo ym., 2016.) Laskenta louhinnan takana perustuu tutkielmassa aikaisemmin esiteltyjen tiivisteiden muodostukseen, jonka avulla solmut tapahtumia varmentavat. Laskennan ideana on saavuttaa mahdollisimman pieni kohdeluku, mistä uuden lohkon tiiviste muodostuu.

Uuden lohkon luomista ja liittämistä lohkoketjuun yritetään pitää mahdollisimman tasaisena verkon vakauden ja tietoturvan takia (Buterin, 2015). Proof-of-work-mekanismi on yleisesti todettu toimivaksi ja tasa-arvoiseksi varmentamisen tavaksi. Se on kuitenkin saanut kritiikkiä suuresta energiakulutuksestaan vaatiessaan solmuilta paljon laskentatehoa. Tätä ei yhteiskunnallisesti ole katsottu kovin hyväksyttäväksi etenkin ilmastonmuutoksen näkökulmasta (Perwej ym., 2019). Proof-of-work on siis hyvin energiakuluttava tapa, jonka vuoksi on alettu kehittämään uusia keinoja toteuttaa konsensusta.

Proof-of-work-mekanismin rinnalle on noussut nykyään proof-of-stake-mekanismi. Siinä todentaminen tapahtuu sijoitettuun pääomaan perustuen edellä kuvatun proof-of-work-mekanismin laskentatehon sijaan. Tässä siis täytyy olla kyseisen lohkoketjun valuuttaa, jolla taataan tapahtuman aitous ja toiminta protokollan mukaisesti. Oma pääoma lohkoketjussa myös on suoraan yhteydessä oikeuteen liittää lohkoja ketjuun (Gaži, Kiayias & Zindros, 2019). Proof-of-stake-mekanismi on energiatehokkaampi ja huomattavasti vähemmän verkkoa ruuhkauttava keino toteuttaa konsensusta, sillä varmentamiseen ei tarvita niin paljoa resursseja solmuilta. Muun muassa myöhemmin tutkielmassa esiteltävä alustaratkaisu, Ethereum, on siirtymässä vaiheeseen, jossa aletaan käyttämään proof-of-stakea-mekanismia proof-of-work-mekanismiin sijasta.

2.4 Lohkoketjujen hyödyt

Lohkoketjujen on nähty tuovan paljon hyötyä monenlaisissa tehtävissä erilaisilla aloilla. Tässä tutkielmassa kuitenkin perehdytään erityisesti finanssisalaan, jolla hyötyjä on jo nähty paljon, mutta odotuksetkin ovat vielä suuret. Lohkoketjuista monelle ensimmäisenä nousee mieleen vain kryptovaluutat. Näiden synty ja olemassaolo perustuu täysin lohkoketjuihin sekä niiden suosion vuoksi teknologiaa on alettu tarkastella paremmin. Kuitenkin useat mahdollisuudet ja positiiviset vaikutukset ovat vielä monille tuntemattomia, jonka vuoksi tämän kaltainen tarkastelu on perusteltua.

Lohkoketjuteknologian avulla uskotaan pystyvän nopeuttamaan ja tehostamaan finanssialan toimintaa sekä lisäämään luottamusta niin julkisella kuin yksityisellä sektorilla (Treleaven ym., 2017). Suurin lohkoketjujen tarjoama mahdollisuus rahoituslalla nähdään olevan prosessien automatisointi älysovimuksien avulla. Tämä yksinkertaistaa prosessien läpivientiä useiden välikäsien tippuessa pois sekä sen myötä vähentää käsittelyjen kuluja. Kun toimeksiannot pystytään automatisoimaan täysin, nopeutuu myös eri prosessien edistyminen. Ihmiset tosin vielä nykyäänkin ovat usein skeptisiä eri teknologioihin luottamisessa, mikä varmasti myös osaltaan on vaikuttanut lohkoketjun kaltaisen, teknologisesti haastavan, teknologian toteutuksessa.

Luottamusta lohkoketjuteknologian käytössä luo sen muuttumattomuus, minimaalinen vastapuolenriski sekä mahdollisuus vahvaan yksityisyyden suojaan julkisen avaimen salauksen myötä. Toiminta lohkoketjuissa on erittäin läpinäkyvää, sillä kaikki data ja transaktiot ovat julkisesti tarkasteltavissa erityisesti, kun puhutaan julkisista lohkoketjuista. Hyötyjen näkökulmasta vaikutukset ovat kauaskantoisia, sillä luottamus on finanssialalla yleisesti tärkeässä avainasemassa. Yksilön näkökulmasta on varsin tärkeää, esimerkiksi rahoitusta tarvitsevalle, että palvelut ovat luotettavia, niin institutionaalisesti kuin teknologisesti. Organisaatioiden kannalta ja yhteiskunnallisesti tarkasteltaessa voidaan todeta finanssialan tarvitsevan yksilöiden luottamusta toimiakseen.

Lohkoketjut perustuvat vahvasti tietotekniseen logiikkaan ja pohjimmiltaan ne ovat suunniteltu toimimaan ohjelmoitujen funktioiden mukaisesti. Tämä helpottaa algoritmien hyödyntämistä apuna lohkoketjuissa, joka taas palvelee ja mahdollistaa teknologisesti automatisaation. Algoritmien ja automatisoinnin vuoksi voidaan asettaa rajaehtoja laukaisemaan toimeksiantoja, jolloin niitä ei tarvitse manuaalisesti toteuttaa. Tällä pystytään vähentämään käsittelyyn käytettyjen resurssien määrää huomattavasti. Lohkoketjut mahdollistavat myös ketterämmät arvoketjut, nopeammat tuotekehitykset ja nopeamman integraation muun muassa pilviteknologiaan sekä esineiden internetiin (Amesar ym., 2020). Esineiden internetin, pilviteknologian sekä lohkoketjuteknologian on yhdessä uskottu tulevaisuudessa mahdollistavan monien palveluiden toimivan täysin automaatiolla ilman ihmisten manuaalista puuttumista prosesseihin. Tutkimuksen mukaan tehokkuutta lisäävät lohkoketjuissa myös muun muassa integraatiotarpeiden ja epäsymmetrisen informaation väheneminen, tehokkaampi päätöksenteko sekä hajautetun tietokannan tuoma luotettavuus ja viansietokyky. (Dumay, Garanina & Ranta, 2021).

3 FINANSSIALA

Finanssiala koostuu monenlaisista toimijoista ja organisaatioista, joita yhdistää jollain tapaa rahan käsitteleminen. Näihin lukeutuvat muun muassa pankit sekä vakuutus- ja rahoitusyhtiöt, jotka toimivat yhteiskunnassa nykypäivänä keskitettyinä toimijoina. Finanssialalla on tärkeä rooli nyky-yhteiskunnan toimimisessa, jotta talous pystyy vastaamaan nykyisiä tarpeita (Harwick & Caton, 2020). Aikaisemmin kansallisten valuuttojen arvo oli sidottua jalometalleihin, mutta nykyään arvo perustuu luottamukseen maan taloutta, hallitusta ja keskuspankia kohtaan (Chen & Bellavitis, 2019). Tähän luottamukseen perustuu koko nykyaikainen rahatalous. Tästä syystä luottamus arvon säilyvyyteen on varsin tärkeää, jotta finanssiala toimii niin kuin kuuluukin.

Ymmärtääksemme paremmin lohkoketjuteknologian tuomat koetut hyödyt, tulee ensin tutustua hieman alan perustaan. Rahoituksia ja omistuksia koskevien tietokokonaisuuksien tallentaminen ja niistä sopiminen muodostavat rahoitusmarkkinoiden toiminnan perusytimen. Nykyiset menetelmät ovat erittäin monimutkaisia, arkkitehtuuriltaan hajanaisia ja kärsivät yhteisten standardien puutteesta. Tämä aiheuttaa jatkuvan tarpeen yhteensovittaa dataa massiivisten järjestelmien kanssa. Alalla tapahtuu myös paljon päällekkäisiä prosesseja, mikä johtaa korkeisiin kustannuksiin ja pitkittyneisiin tehtäviin kuluviin aikoihin. (Perwej ym., 2019.)

Tässä luvussa tutustutaan finanssialaan ja nykyaikaiseen rahoitusjärjestelmään sekä käydään läpi erilaisten toimijoiden prosesseja. Tämän myötä on tarkoitus pystytää muodostamaan viitekehys lohkoketjujen tuoman muutoksen tarkastelemiseksi.

3.1 Nykyaikainen rajoitusjärjestelmä

Finanssiala ja etenkin nykyaikainen rahoitusjärjestelmä on varsin tehoton ja haavoittuvainen rikoksille. Järjestelmää kutsutaan jopa antiikkiseksi sen uudistustarpeen vuoksi. Tämän lisäksi finanssiala toteutuu erittäin keskitetysti, mikä

hidastaa ja monimutkaistaa sen toimintaa. Keskitetty toiminta on myös riskialttiimpaa järjestelmien vioille ja ulkopuolisille riskitekkijöille, muun muassa hakkerien hyökkäyksille. (Tapscott & Tapscott, 2017.) Finanssialan keskeisiksi toimijoiksi yleisesti lasketaan pankit ja rahoituslaitokset, vakuutus- ja sijoitusyhtiöt, luotonantajat sekä muut yksittäiset instituutiot, jotka rahoituspalveluita tarjoavat. Kaikkien näiden toimijoiden prosessit sisältävät paljon protokollia ja muun muassa salassapitovelvollisuutta, mitkä ovat tuoneet omat vaikeutensa siirtää dataa yleisesti ottaen kaikille avoimiin lohkoketjuihin. Rahoitusjärjestelmän tehtävä finanssialalla on vastata rahoituksen kanavoinnista säästäjiltä sitä tarvitseville (Suomen Pankki, 2022).

Nykyisessä rahoitusjärjestelmässä keskitetyt toimijat omaavat markkinoilla yleisen luottamuksen, jonka vuoksi niiden uskottavuutta ei juurikaan epäillä potentiaalisten asiakkaiden toimesta. Tätä luottamusta on kuitenkin aika ajoin horjuttanut muun muassa erilaiset talouskriisit. Esimerkiksi vuoden 2008 finanssikriisi on nähty muistutuksena rahoitusalan riskillisyydestä liittyen keskitettyihin toimijoihin. Vastaavia kriisejä pyritään yhteiskunnassa maailmanlaajuisestikin ehkäisemään monin erilaisin raha- ja talouspoliittisin keinoin, mutta lohkoketjujen myötä voitaisiin pienentää keskitettyjä asemia, mikä puolestaan saisi markkinat toimimaan läpinäkyvämmin.

Finanssialan avaintoimijoiksi voidaan määritellä esimerkiksi pörssissä tapahtuvia kauppvoja takaava keskusvastapuoli, erilaisia selvityksiä hoitavat arvopaperikeskukset, maailmanlaajuisesta rahansiirrosta vastaava SWIFT (engl. the Society for Worldwide Interbank Financial Telecommunication) sekä vastaava Euroopan sisäisestä rahansiirrosta huolehtiva SEPA (Single Euro Payments Area), keskuspankit sekä erilaisia muita pankkitoimintaa harjoittavia yksiköitä, esimerkiksi säilytyspalveluita tai sijoituspalveluita tarjoavat yritykset. Näiden toimijoiden prosesseihin nähdään potentiaalisesti lohkoketjuteknologian tarjoavan houkuttelevampi vaihtoehtoinen tapa organisoida nykyaikainen rahoitus. (Johnson, Dandapani & Sharokhi, 2020; Varma, 2019)

Visa, PayPal ja edellä mainittu SWIFT ovat kansainvälisiä keskitettyjä maksuverkkoja, jotka helpottavat verkkokauppaa, mutta toisaalta perivät suhteellisen korkeita maksuja palveluistaan (Chen & Bellavitis, 2019). Jos tällaiset toimijat pystyisivät hyödyntämään lohkoketjuteknologiaa prosessiensa läpiviennissä, voisivat vaikutukset olla merkityksellisiä niin näiden yritysten kuin heidän asiakkaidensakin näkökulmasta. Vaikka nykyiset transaktioiden selvitys- ja toimitusmenetelmät ovatkin huomattavasti kehittyneet aiemmista sukupolvista, ovat ne edelleen kalliita ja niihin liittyy monia täsmäytys- ja vastapuo- liriskejä. Lisäksi moniin rahoitustuotteisiin liittyy korkeita transaktiokustannuksia ja rahoitusmarkkinoille osallistuminenkin on varsin epätasaista vielä monissa osissa maailmaa. (Casey, Crane, Gensler, Johnson & Narula, 2018).

3.2 Finanssialan prosessit

Edellisessä luvussa eriteltyjen toimijoiden prosessit ovat keskenään hyvin erilaisia, jonka vuoksi finanssialan tarkastelu käsitteenä onkin haastavaa laajuutensa vuoksi. Seuraavaksi kuitenkin esitellään toimijoiden pääasiallinen rooli ja toiminta yhteiskunnassa, jotta tutkimustulosten tarkastelu helpottuu.

Pankkien tehtävä on vastata arvon säilytyksestä ja siirrosta asiakkaidensa vaatimilla tavoilla. Kansainvälinen rahansiirto on erittäin keskitettyä vain tietyille suurille toimijoille, jotka vastaavat omien alueidensa toiminnasta. Näiden lisäksi jokaisella maalla on oma hallitseva pankkinsa, keskuspankki, jonka tehtävä on vastata muun muassa pankkien vakaavaraisuudesta. Suomessa vastaavassa asemassa toimii Suomen Pankki, jonka tehtävänä on vastata ja ohjata kaikkien Suomessa toimivien liikepankkien toimintaa. Liikepankkien tärkeimmiksi tehtäviksi taas lukeutuva transaktioiden suorittaminen, tiliotot ja -panot asiakkaiden toiveiden mukaisesti sekä säilytyspalvelu luotettavasti.

Rahoitusmarkkinoiden tehtävä on yhdistää rahoitusta tarvitsevat ja tarjoavat osapuolet. Yleensä ne jaetaan kahteen osaan eli raha- ja pääomamarkkinoihin sijoituksen tai rahoitustarpeen keston mukaan. Rahamarkkinoilla käydään kauppaa alle vuoden mittaisista sijoituksista ja pääomamarkkinoilla taas yli vuoden. Näihin yleensä osallistuvat esimerkiksi rahoituslaitokset, pörssit sekä sijoitusyhtiöt. Nämä toimivat apuna löytämään sopivat osapuolet keskenään sekä toteuttamaan käytännössä rahoitukset. Rahoitusmarkkinoilla käydään kauppaa finanssialan instrumenteista, joita ovat esimerkiksi erilaiset osakkeet, velkakirjat tai johdannaiset. Näiden markkinoiden kauppapaikkoina yleisesti toimivat erilaiset pörssit tai instrumentteja myyvät rahoituslaitokset. (Knüpfer & Puttonen, 2018).

Vakuutuslaitosten tavoitteena on turvata yritysten ja yksityisten henkilöiden omaisuus ja luoda sosiaaliturvaa. Yksilön näkökulmasta tarkoituksena on pystyä minimoimaan omaa elämää uhkaavat riskit sekä näiden mahdollisesti aiheuttama taloudellinen tappio. Vakuutuslaitokset keräävät asiakkailtaan pieniä maksuja, joilla kollektiivisesti pystytään takaamaan varojen riittävyys vahinkojen sattuessa. (Finanssiala, 2022).

4 HAJAUTETTU RAHOITUS

Tutkimuksen mukaan lohkoketjuteknologian uskotaan tarjoavan mahdollisuuksia finanssialalle niin kustannusten kuin tuottojenkin näkökulmasta. Tuottojen osalta nähdään mahdollisuutena uudet liiketoimintamallit ja tuotteet sekä nykyisiltä että uudenlaisilta yrityksiltä. Lohkoketjuun perustuvat uudet alustat mahdollistavat esimerkiksi uudenlaisen pääoman hankkimisprosessin sekä kaikkien muiden myöhempien vaiheiden optimoinnin. Kustannusten osalta potentiaalia syntyy koko lisäarvoketjussa rahoitusalan näkökulmasta, kun optimoinnin myötä pystytään vaikuttamaan arvoketjun muodostumiseen. (Ame-sar ym., 2020.)

Koska lohkoketjut toimivat hajautetusti, on finanssialallakin alettu puhua hajautetusta rahoituksesta. Rahaa, osakkeita, joukkovelkakirjoja, arvopapereita, tositteita, sopimuksia ja lähes kaikenlaista omaisuutta voidaan siirtää ja säilyttää turvallisesti ja yksityisesti vertaisverkon avulla. Tällaisissa prosesseissa luottamusta luo lohkoketjujen verkosto, konsensus, salaus ja älykäs koodi (Tapscott & Tapscott, 2017). Tällä hetkellä käytössä olevien lohkoketjupohjaisten ratkaisujen taustalla toimii pääasiassa ajatus muuttaa perinteisiä prosesseja hajautempaan muotoon. Muutoksen myötä halutaan pystyä saavuttamaan lohkoketjujen mahdollistamat hyödyt, jotta voidaan tuottaa ratkaisujen kautta lisäarvoa.

Tässä luvussa tutustutaan uusiin lohkoketjun mahdollistamiin sovelluksiin sekä perehdytään uuteen rahoituksen muotoon eli hajautettuun rahoitukseen, joka toimii täysin lohkoketjupohjausten alustojen päällä. Tämän yhteydessä käydään läpi esimerkin myötä malli julkisesta alustasta, jonka päällä suurin osa tämänhetkisistä finanssiapplikaatioista toimii. Lopuksi tutustutaan vielä älysopimukseen, jotka toimivat osana hajautettua rahoitusta ja mahdollistavat automaation sen sisällä.

4.1 DeFi-sovellukset

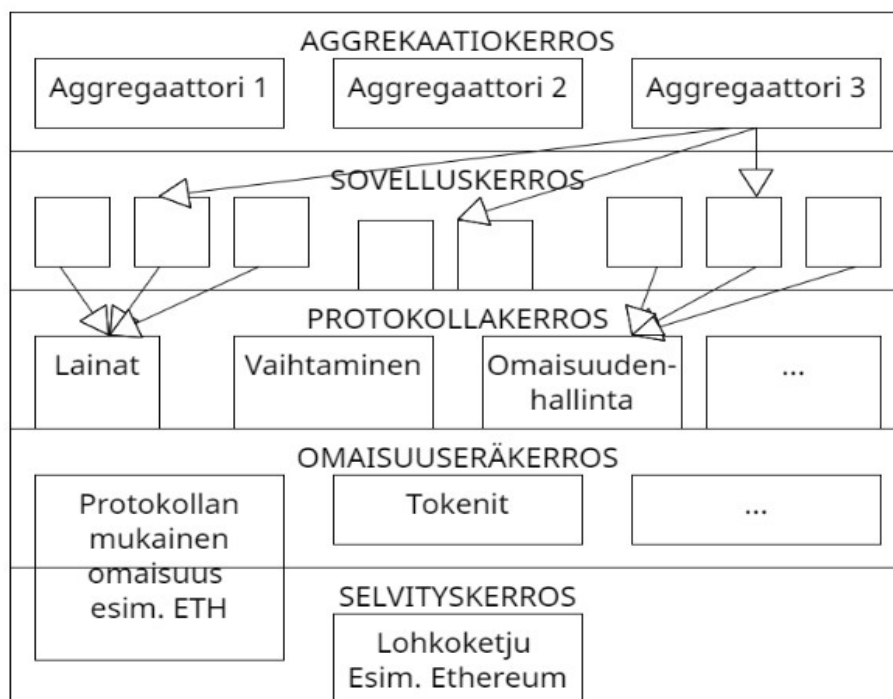
Tässä tutkielmassa kerrotusta hajautetusta rahoituksesta puhutaan usein DeFi:nä, joka tulee englannin kielen termistä "Decentralized Finance". DeFi on finanssiteknologian eli FinTechin muoto, jonka taustalla toimivat vahvasti lohkoketjut. Tälle, kuten monelle muullekaan rahoituksen termille ei löydy suomenkielistä, yleisesti hyväksyttyä vastinetta, joten monesti kuullaan puhuttavan vain lyhenteestä DeFi. Tässä tutkielmassa käytetään termiä DeFi-sovellukset, jolla viitataan siis hajautetun rahoituksen finanssiapplikaatioihin. Schärin (2021) mukaan DeFi-sovellukset ovat hajautettuja finanssiapplikaatioita, jotka toimivat älysopimusten avulla yleensä julkisen lohkoketjualustan päällä. Käytännössä tällaiset älysopimukset pystytään toteutumaan ilman keskitettyä toimijaa, sillä niiden toiminta perustuu ohjelmoituun koodiin. DeFi-sovellusten tarkoituksena on älysopimusten avulla tuottaa protokollia, joiden avulla nykyisiä rahoituspalveluja pystyttäisiin tuottamaan avoimesti, läpinäkyvästi ja yhteensopivasti. Tällaiset applikaatiot tarjoavat globaalin markkinapaikan finanssialalla toimijoille ilman vastapuolen riskiä, vaikka toista osapuolta ei tunnetaakaan. Alustana DeFi-sovelluksille voidaan käyttää julkista lohkoketjua, josta esimerkkinä käydään seuraavassa luvussa tällä hetkellä tunnetuin ja käytetyin vertaisverkossa toimiva alusta Ethereum. (Jensen, Wachter & Ross, 2021; Schär, 2021).

Prosessit ovat nykyisessä rahoitusjärjestelmässä hitaita ja vaativat paljon manuaalista työskentelyä toteutuakseen. Ne vaativat myös edellä mainitusti kolmannen osapuolen eli esimerkiksi pankin tai rahoituslaitoksen varmistamaan tapahtumien aitous ja tunnistamaan molemmat osapuolet. Näiden välikäsien aiheuttamiin kustannuksiin ja jäykkyyteen on alettu lohkoketjujen myötä keksimään ratkaisua. Tämä potentiaalinen ratkaisu eli DeFi-sovellukset toimivat älysopimusten perusteella, jotka taas toteutuvat korkean tason ohjelmointikielellä koodattujen funktioiden mukaisesti. Tällaiset sopimukset sijaitsevat lohkoketjujen myötä hajautetussa verkossa eli ne ovat teknologiansa tavoin läpinäkyviä ja tilannekohtaisia sekä todentuvat yleisen konsensuksen mukaisesti. (Jensen ym., 2021) Älysopimukseen perehdytään vielä tarkemmin lisää alaluvussa 4.3.

Chenin ja Bellavitisin (2019) mukaan finanssialalla lohkoketjuteknologia voi mahdollistaa hajautetumpia, innovatiivisempia, yhteensopivampia, rajattomampia ja avoimempia rahoituspalveluja, joiden avulla palveluiden saataavuus helpottuu ja pystytään luomaan alustaa uusille yrittäjille ja innovaatioille. Tällaisilla nykyaikaisilla hajautetuilla rahoitussovelluksilla pystytään tarjoamaan erilaisia rahoituspalveluita kaupankäynnin, luotonannon, sijoitusten, omaisuudenhoidon ja vakuutuspalveluiden tueksi (Jensen ym., 2021). Esimerkiksi hajautetussa pörssissä voidaan ostaa Yhdysvaltain dollariin sidottua valuuttaa, jota kutsutaan stablecoiniksi. Stablecoinien myötä lainausalustalla käydään kauppaa instrumenteista, jotta voidaan ansaita korkoa (Schär, 2021). Stablecoineilla pyritään poistamaan kryptovaluuttojen epävakautta, kun niiden arvo on sidottuna fiat-valuuttoihin eli valtion liikkeelle laskemiin kysyntään ja

tarjontaan perustuviin valuuttoihin. Näistä tunnetuimpina mainittakoon euro ja Yhdysvaltain dollari (Chen & Bellavitis, 2019).

Kuviossa 2 esitellään DeFi-sovellusten rakennetta julkisissa lohkoketjuissa. Tässä kohtaa täytyy mainita, että eri tarkoituksiin luodut sovellukset ovat rakenteeltaan hyvin erilaisia. Kuviota tarkasteltaessa täytyy siis muistaa sen yleispätevyys ja yksinkertaistettu luonne. Tarkoituksena on havainnollistaa, kuinka data hajautetuissa finanssiapplikaatioissa rakentuu ja käyttäytyy yleisesti ajatellen. DeFi-sovellukset rakentuvat viidestä kerroksesta. Pohjimmaisena on "selvityskerros", jolla tarkoitetaan alustaa, jonka päällä lohkoketju toimii. Toisena kerroksena on "omaisuuseräkerros", joka koostuu kaikista omaisuus-eristä, joita lasketaan liikkeelle lohkoketjun sisällä. Yleensä näitä kutsutaan lohkoketjuissa tokeneiksi. Kolmas kerros on "protokollakerros", joka tarjoaa standardit tietyille käyttötapauksille esimerkiksi hajautetuille pörsseille, velkemarkkinoille tai lohkoketjussa tapahtuvalle omaisuudenhallinnalle. Nämä yleensä käytännössä toteutuvat älysovimuksilla. Neljäs eli sovelluskerros sisältää käyttäjälähtöisesti luotuja sovelluksia, jotka ovat vuorovaikutuksessa älysovimuksiin ja protokoliin. Päälimmäinen eli "aggregaatiokerros" on sovelluskerroksen laajennus. Aggregaattorit luovat käyttäjäkeskeisiä alustoja, jotka yhdistävät useita sovelluksia ja protokollia. Ne tarjoavat yleensä työkaluja palveluiden vertailemiseen ja arvioimiseen sekä antavat käyttäjille mahdollisuuden suorittaa muutoin monimutkaisia tehtäviä yhdistämällä useita protokollia samanaikaisesti. Täten aggregaattorit yhdistävät asiaankuuluvaa tietoa selkeällä ja ytimekkäällä tavalla. (Schär, 2021).



KUVIO 2 DeFi-sovelluksien rakenne julkisissa lohkoketjuissa. (Jensen ym., 2021; Schär, 2021)

4.2 Ethereum

Ethereum on Bitcoinin tapainen julkinen lohkoketju, joka on luotu palvelemaan erilaisia transaktioita mahdollistavia applikaatioita rahoitusjärjestelmässä älysopimuksien avulla. Ethereumkin perustuu avoimeen lähdekoodiin ja on muuttumaton tilikirja, mihin transaktioita ja arvonsiirtoja talletetaan. Ethereumin on kehittänyt vuonna 2015 yhdessä monien muiden tiedeyhteisön jäsenten kanssa Vitalik Buterin, jonka ideana oli kehittää arvonsäilytystä ja -siirtoa helpottava alusta huomatessaan virtuaalivaluuttojen myötä potentiaalin tällaiselle kehitykselle. (Buterin, 2016).

Edellä käydyt DeFi-sovellukset toimivat siis Ethereumin kaltaisten lohkoketjupohjaisten alustojen päällä. Tällaisten alustojen lähtökohtainen tarkoitus on tarjota sovelluksille toimintaympäristö, joka toteuttaa älysopimuksia ja mahdollistaa DeFi-sovellusten toimimisen. Ethereum on kehitetty palvelemaan sovelluksia, jotka edellyttävät tokenisointia eli käytännössä omaisuserien tai muiden resurssien jakamista ja kaupankäyntiä. Tokenisointi vaatii ennen toteutumistaan kansallisen valuutan muuttamista lohkoketjuissa käytettyihin kryptovaluuttoihin. Tästä johtuen Ethereum-lohkoketjussa on käytössä oma valuutansa eli kryptovaluutta ETH, jolla arvoa siirretään kaikissa sen päällä olevissa sovelluksissa (Hewa, Ylianttila & Liyanage, 2021).

Hewanin, Ylianttilan ja Liyanagen (2021) tutkimuksen mukaan vertailtaessa vuoden 2020 älysopimuksille käytössä olevia lohkoketjualustoja, Ethereum on käytetyin ja suosituin alusta finanssipalveluissa sekä arvonsiirrossa. Ethereumilla onkin Schärin (2021) mukaan sen hetken suurin älysopimusala markkinakapasiteetiltaan saatavilla olevien sovellusten ja kehitysaktiivisuuden suhteen. Vuonna 2019 jopa 87-prosenttia DeFi-sovelluksista on käyttänyt alustanaan Ethereumia, jonka vuoksi on perusteltua väittää Ethereumin omaavan tämänhetkisten hajautettujen finanssiapplikaatioiden markkinaylivoi-
ma.

4.3 Älysopimus

Aikaisemmin tutkielmassa mainitut älysopimukset perustuvat lohkoketjuteknologiaan. Tällaiset sopimukset poikkeavat elektronisista sopimuksista luotettavuudellaan. Kun sopimuksen sitomisessa on osallisena lohkoketjuteknologia ja algoritmit, pystytään sopimuksen oikeellisuus todistamaan paljon paremmin. Tällaiset sopimukset eivät salli väärennöksiä tunnistautumisen vuoksi, joka mahdollistaa sopimuksien pätevyyden. Älysopimukseen on koodattu jokin lo-
giikka tai funktio, jonka perustella sopimus toteuttaa itsensä, kun raja-arvot täyttyvät. Ne perustuvat täysin ohjelmistokoodiin sekä laskennalliseen infrastruktuuriin. (Hewa ym., 2021).

Koodit älysopimuksissa ovat lohkoketjujen tapaan muuttumattomia, jolloin ennalta määritellyjä toimeksiantoja ei pystytä muuttamaan tai perumaan. Näis-
säkin vastapuoliriski on siis minimoitu, eikä välikätkä prosessissa tarvita. Hewa, Ylianttila ja Linyanage (2021) esittelevät älysopimuksien avaintoiminnoiksi kolmannen osapuolen puuttumisen, väärentämättömyyden, läpinäkyvyyden, automaation sekä paikkansapitävyyden. Näiden kaikkien voidaan sanoa olevan myös pelkästään lohkoketjujen hyötyjä, joka korostaakin älysopimusten riippu-
vuutta lohkoketjuteknologiaan saavuttaakseen kyseiset hyödyt. Älysopimuk-
sien yhteydessä täytyy luottaa koodin oikeellisuuteen ja toimivuuteen. Tällais-
ten sopimusten kuten myös yleisesti lohkoketjujen koodi on kaikkien tarkastel-
tavissa ja sen muuttaminen on lähes mahdotonta. Tämä luo älysopimuksistakin
läpinäkyviä kaikkien osapuolet kesken ja niiden riskit liittyvätkin pääasiassa
vain koodin toimimiseen.

5 MAHDOLLISUUDET JA HAASTEET

Kuten todettu, vielä toistaiseksi on nähty melko vähän konkreettista näyttöä lohkoketjujen edistyneestä käytöstä finanssialan eri osa-alueilla. Bitcoinin julkistuksen jälkeen on nähty vain muutamia lohkoketjusovelluksia, joidenka vähäisyyttä Varma (2019) perustelee tutkimusartikkelissaan muun muassa oikeudellisilla ja kaupallisilla esteillä. Pääasiallinen käyttö lohkoketjuilla on vieläkin ollut kryptovaluuttojen hajautettu maksualusta (Bossler & Kroenung, 2022). Lohkoketjujen haasteissa nähdään myös paljon teknisiä rajoitteita, jotka vaativat vielä paljon kehitystyötä.

Lohkoketjut voisivat mullistaa useita finanssialan monimutkaisia toimintoja, joita edellä käsiteltiin. Prosessien uudellinen tehokkuus voisi parantaa toimijoiden mainetta ja asiakkaiden yksityisyyttä, mahdollistaa arvon siirtäminen aikaisempaa yksinkertaisemmin sekä tehokkaammin muun muassa maksujen ja rahaliikenteen osalta. Myös arvon varastointi, luotonanto ja -otto sekä arvolla käytävä kappo ovat toimintoja, joihin lohkoketjuilla voisi olla lähtemätön vaikutus. Vakuutukset ja riskinhallinta sekä tilintarkastus- ja verotustoiminnot ovat osaltaan nähty mahdollisina lohkoketjujen hyödyntäjinä, vaikka varsinaisesti eivät osallistukaan arvon siirtämiseen. Näiden prosesseissa hyöty voidaan saavuttaa älysovimuksien käytön yhteydessä muodostuneesta automatisaatiosta ja lohkoketjujen tarkistettavuuden mukana tuomasta luotettavuudesta.

Bossler ja Kroenung (2022) tutkimusartikkelissaan käsittelevät lohkoketjuteknologian ympärille kasvanutta kiinnostusta ja tarkastelevat lohkoketjuteknologiaa rahoitusosalalle muutoksia aiheuttavana teknologiana. Artikkelissa esitellään lohkoketjujen tutkimuksen tämänhetkistä tilannetta ja siitä nousee esille kaksi merkittävää muutosta lohkoketju-tutkimuksen saralla. Ensinäkin lisääntyneiden tutkimusten ja kasvaneen kiinnostuksen myötä lohkoketjut ovat muuttuneet yleishyödylliseksi aiheeksi tiedeyhteisöjen keskuudesta. Se on noussut tärkeäksi tietojärjestelmätieteen tutkimusaiheeksi. Tutkimuksesta käy ilmi, että sana "blockchain" eli lohkoketju on tutkimuksissa ollut vuonna 2022 paljon käytetympi avainsana kuin "distributed ledger" eli hajautettu tilikirja, vaikka tutkimukset lohkoketjujen osalta usein jäivätkin melko pinnallisiksi. Tästä voidaan päätellä lohkoketjujen ympärillä olevan vielä tiedeyhteisössäkin

yliarvostusta, kun sanaa halutaan käyttää sen trendinomaisen luonteen vuoksi. Toisena tutkimustuloksena Bossler ja Kroenung (2022) esittelevät kiinnostuksen yleisesti lohkoketjuteknologiaa kohtaan ylittäneen kryptovaluutat, jotka pitkään olivat huomattavasti taustateknologiaansa yleisempiä tutkimuksissa. Koska lohkoketju ja kryptovaluutta ovat ”hypetettyjä” aiheita, tutkijoilla on tapana sisällyttää ne eri aiheita käsitteleviin artikkeleihin, jotta lukijakunnan kiinnostus heräisi, vaikka aiheen painopiste olisikin toisaalla. (Bossler & Kroenung, 2022).

Tässä luvussa tutustutaan vielä syvemmin tulevaisuuden mahdollisuuksiin ja haasteisiin, mitä lohkoketjujen uskotaan kohtaavan. Ensiksi käydään läpi uskottua potentiaalia ja erilaisia käyttökohteita, joihin nykyisen tutkimuksen mukaan lohkoketjuilla voisi olla ratkaisuja. Toisessa alaluvussa taas perehdytään vielä tarkemmin erilaisiin rajoittaviin tekijöihin ja haasteisiin, jotka tulisi vielä ratkaista ennen kuin lohkoketjuja voitaisiin edistyneesti hyödyntää kaikilla sen potentiaalisilla osa-alueilla finanssialan näkökulmasta.

5.1 Mahdollisuudet finanssialalla

Lohkoketjujen aiheuttamaa muutosta on spekuloitu jopa paradigmaattisena muutoksena, missä keskiössä ovat hajauttaminen ja välittäjäpalveluiden poistaminen (Chen & Bellavitis, 2019). Paradigmalla tieteessä tarkoitetaan yleisesti valloilla olevaa suuntausta tai ajattelutapaa, joka on tiedeyhteisön kesken hyväksytty perustuen tehtyihin tutkimuksiin. Tästä päätellen lohkoketjujen ajatellaan siis pystyvän muuttamaan radikaalisti nykyisiä ajatuksia ja suuntauksia finanssialan toteutuksesta. Tällainen perusteltu spekulatio tuntuu melko vakuuttavalta, etenkin tilanteessa, jossa aletaan käytännössä nähdä merkittäviä edistysaskeleita lohkoketjupohjaisten ratkaisujen käytöstä.

Tutkimuksessaan Dumay ym. (2021) keskittyvät lohkoketjujen käyttöön tilintarkastuksessa ja laskentatoimessa. Finanssialan näkökulmasta tällä nähdään vaikutuksia erityisesti ulkoisten sidosryhmien kannalta esimerkiksi kilpailukykyyn parantamisessa. Tämän koetaan voivan myös synnyttää luottamusta markkinaosapuolten välillä. Tutkimustuloksena kuvataan suurta kasvua lohkoketjuihin ja tilintarkastukseen liittyvien tutkimusten määrässä. Tällä on nähty olevan myös vaikutuksia sidosryhmien mielipiteeseen yrityksestä. Laskentatoimen ja tilintarkastuksen näkökulmasta lohkoketjuja käyttävien organisaatioiden on lähes mahdotonta esittää yrityksen taloudellista tilannetta kuvaavia lukuja tai arvoja niin sanotusti kaunistellusti. Nykyaikaisessa esityksessä tällaista esitystapaa käytetään, jotta saadaan luvut näyttämään paremmilta tai huonommilla mitä ne oikeasti ovat, millä taas voidaan vaikuttaa lukuja tarkastelevan tahon mielipiteeseen. Lohkoketjuja hyödyntäessä kuka tahansa voisi milloin tahansa koota yrityksen liiketoimet vaikkapa tuloslaskelman ja taseen muotoon, eikä heidän tarvitsisi enää luottaa yrityksen laatimiin neljännesvuosittaisiin tilinpäätöksiin. Esimerkiksi, jos sijoittaja on kiinnostunut sijoittamaan johonkin yritykseen tai organisaatioon, pystyisi hän saamaan reaaliaikaisesti oikeat ja luotetta-

vat tunnusluvut yrityksen taloudellisesta tilanteesta. (Dumay ym., 2021; Yu ym., 2018)

Finanssialaan vahvasti kuuluvat varainhankinnanprosessit eli sijoittajien ja rahoitusta tarvitsevien välinen yhteys. Yleisesti rahoitusmarkkinat määritellään näiden kahden toimijan väliseksi. Kuitenkin nykyään vielä varainhankinnassa vaaditaan välikäsi muun muassa pankki tai pörssi, joka hoitaa arvonsiirrot ja säilytykset käytännössä. Hajautetuilla malleilla voitaisiin esimerkiksi pörssissä tapahtuvan kaupan tapaista rahoitusinstrumenttien vaihtoa toteuttaa ilman kolmatta osapuolta luotettavasti. Lohkoketjuilla on hajautuksen myötä nähty potentiaalia myös tällä saralla. Lohkoketjujen tuoman finanssialan kehityksen myötä lisääntyisivät mahdolliset tavat hankkia rahoitusta tai sijoittajan näkökulmasta saada voittoa rahoilleen. Seuraavissa alaluvuissa perehdytään DeFi-sovellusten tuomiin mahdollisuuksiin sekä tarkastellaan lohkoketjujen vaikutuksia arvonsiirroissa ja kustannusten muodostumisessa.

5.1.1 Hajautetut finanssiapplikaatiot

Julkisissa alustaratkaisuisissa sovellusten kehittäminen ja testaus on helppoa kenelle tahansa, koska kehittäjinä voivat toimia verkon solmut eli he eivät tarvitse lupaa tehdäkseen sovellukseen muutoksia tai kokeillakseen uusia sovelluksia (Chen & Bellavitis, 2019). Toimivuuden parantamisella Chenin ja Bellavitisin (2019) artikkelissa tarkoitetaan saumattomampaa toimimista eri rahoituslaitosten kesken. Perinteinen finanssiala toimii ikään kuin siiloissa, mikä lisää jäykkyyttä prosessien kesken. Teknologian saralla siilot tarkoittavat putkilomaista toimintaa. Tällä tarkoitetaan eri toimintojen tapahtuvan erillään toisistaan, jolloin palvelutkaan eivät ole yhteensopivia toistensa kanssa. Tällaisissa tapauksissa pääoman ja arvon siirtyminen siilojen välillä voi olla kallista ja hankalaa.

Aikaisemmin mainittu Ethereum on ollut vuoden 2019 tutkimuksen mukaan hallitseva alusta julkisille DeFi-sovelluksille. Jopa 87 prosenttia sovelluksista on toiminut Ethereumin päällä, jossa kaikki nämä palvelut ovat olleet yhteensopivia. Yhtenä haasteena lohkoketjujen yhteensopivuudessa on nähty eri alustoilla toimivat sovellukset, jotka eivät pysty keskustelemaan keskenään. Tähän ongelmaan on tällä hetkellä olemassa kaksi vaihtoehtoista ratkaisua. Ensimmäisenä vaihtoehtona on esitelty yhden hallitsevan alustan, kuten Ethereumin, toimiminen alustana kaikille sovelluksille. Tämän avulla voitaisiin rakentaa täydellinen yhteensopivuus, mutta ongelmaksi tässä kuitenkin koituu se, ettei lohkoketjut teknisesti ole vielä valmiita palvelemaan kaikkia prosesseja, joilla on eri tarpeita. Tämän takia yhteensopivuuden kasvattaminen eri lohkoketjujen välillä on nähty parempana ratkaisuna, mutta se voi kuitenkin osoittautua teknisesti erittäin haastavaksi saavuttaa. (Chen & Bellavitis, 2019).

5.1.2 Arvonsiirto

Tilooby (2018) artikkelissaan esittelee Zhaon, Fanin ja Yanin (2016) sekä Mougayarin (2016) ajatuksia ja ennustuksia lohkoketjuteknologian muutosvaikutuksista. He kokevat maailmanlaajuisten luotettavien transaktioiden mahdollistamisen olevan samansuuntainen kuin internetin paradigmaattinen vaikutus tiedon saatavuuteen. Zhao, Fan ja Yan (2016) tarkentavat edelleen, että lohkoketjuteknologiasta syntyvä hajautettu luottamus lieventää transaktioiden kustannuksia, jotka johtuvat keskittämiseen liittyvistä ei-teknisistä asioista, kuten asiakkaan tunnistamisesta tai transaktion täsmäyksestä. Näistä syistä on perusteltua väittää lohkoketjujen mahdollistavan kustannustehokkaat maailmanlaajuiset rahansiirrot täysin uudenlaisin keinoin. (Mougayar, 2016; Tilooby, 2018; Zhao ym., 2016)

Luvussa 3 mainitun SWIFT:n tehtävänä on vastata nykypäivän maailmanlaajuisten pankkien välisestä maksuverkostosta. SWIFT on näyttänyt omalla toiminnallaan jo merkittäviä edistysaskeleita digitalisoituneempaan ja hajautempaan toimintaan. Instituutio on muun muassa aloittanut pilottihankkeen hajautettujen tilikirjojen myötä, jonka tarkoituksena on tilien virtaviivaisempi täsmäytys, jotta voitaisiin poistaa rajanylittävien maksujen viivästyksiä ja tarjota avoimempaa maksujen hinnoittelua ja seurantaa (Casey ym., 2018). Tutkimuksen mukaan lohkoketjujen mahdollistamien kryptovaluuttojen avulla maailmanlaajuiset rahansiirrot voitaisiin nopeuttaa nykyisestä muutaman päivän kestosta alle tuntiin, ellei jopa muutamiin sekunteihin (Johnson ym., 2020).

Myös käteistransaktioista saataisiin lohkoketjujen avulla tehtyä reaaliaikaisia, kun prosessista voitaisiin poistaa aikaa vieviä selvitystöitä. Lohkoketjupohjaisessa alustassa transaktiot tapahtuvat välittömästi toimeksiannon tapahtuessa esimerkiksi omaisuuserän tai sopimuksen omistusoikeuden siirrosta. Kun käyttäjät pystyvät hyödyntämään samaa, kaikille avointa alustaa kaupankäynnissä, lohkoketjut edistävät prosessien läpivientä (Perwej ym., 2019). Näin voitaisiin vähentää huomattavasti viiveitä ja virheitä prosessissa sekä lisätä luottamusta ilman kolmannen osapuolen liittymistä tapahtumaan.

5.1.3 Kustannukset

Prosessien automatisointi älysopimusten avulla on nähty auttavan vähentämään hallinnollisia menettelyjä ja tämän myötä syntyneitä kustannuksia (Perwej ym., 2019). Vaikka transaktioiden hintoja voitaisiin tämän johdosta alentaa, ei maksuja voida kokonaan poistaa. Kustannukset vaihtelevat verkon sekä sen tukkoisuuden mukaan, sillä verkon ruuhkautuminen nostaa hintoja sekä vaatii enemmän energiaa toteutuakseen. Myös transaktioiden kompleksisuudella on vaikutusta hinnanmuodostuksessa.

Thakor (2020) esittelee lohkoketjujen hyödyntämisen pankkialalla mahdollistavan alhaisemmat etsintäkustannukset liiketoimien osapuolten yhteensovittamisesta, mahdollisuuden saavuttaa mittakaavaetuja suurten tietojen keräämisessä ja käytössä, halvemmän ja turvallisemman tiedonsiirron. Näiden

lisäksi pystyttäisiin vähentämään todentamiseen vaadittavia resursseja, joista kustannuksia syntyy. (Thakor, 2020).

5.1.4 Varainhankinta ja sijoittaminen

Initial Coin Offerin eli ICO on uudenlainen tapa saada rahoitusta esimerkiksi projektille. Se on listautumisannin eli initial public offering (IPO) tapainen, mutta hajautettu muoto tästä. Listautumisannissa yritys tuo ensimmäistä kertaa osakkeensa julkisesti esimerkiksi pörssiin myyntiin, jolloin yritys voi kerätä itselleen rahoitusta (Johnson ym., 2020, s. 762). ICO:ssa ideana on tokenien muodossa hankkia rahoitusta julkisessa lohkoketjussa tarjoamalla uutta kryptovaluuttaa vastineeksi rahoitukselle. Tokeneita siis myydään rahoittajille ja niihin voi arvon lisäksi olla sidottuna esimerkiksi luontaisia hyötyjä hankkeen tuotteisiin tai alustoihin liittyen. Hyötypuolena on nähty näiden vähentävän kitkaa varainhankinnassa, mikä helpottaa pääoman saamista ja edistää täten innovointia ja yrittäjyyttä. (Heiskanen, 2017.)

Lohkoketjujen avulla on voitu mahdollistaa myös hajautettuja pörssejä, joissa omaisuuseriä pystytään vaihtamaan julkisten lohkoketjualustojen päällä. Näillä pyritään jäljittelemään perinteisiä pörssejä, jotka toimivat keskitetysti. Tällaisten alustojen avulla on haluttu helpottaa rahoitussopimusten toteuttamista ja laatimista, poistaa toimitusketjujen monimutkaisuus sekä automatisoida omaisuudenhallinta (Jensen ym., 2021).

5.2 Käyttöä rajoittavat tekijät

Rahoitus on olennainen osa rahataloutta ja yleisesti talouden toimintaa, joka tekee finanssialasta yhteiskunnallisesti merkittävän tekijän. Infrastruktuuritasolla kryptovaluutat voisivat hoitaa rahoituksen tehtäviä paremmin kuin nykyiset kansalliset valuutat, mutta kuitenkin niiden vuorovaikutussuhteiden riittämättömyyden vuoksi ne eivät ole valmiita korvaamaan perinteistä rahoitusta kokonaan (Harwick & Caton, 2020). Kryptovaluutoissa arvo perustuu luottamukseen teknologiaa kohtaan, jonka saavuttaminen yhteiskunnallisella tasolla on vielä varsin haastavaa. Luottamus on tärkeässä roolissa finanssialalla, mutta teknologioiden on vielä nykypäivänäkin vaikea voittaa sitä puolelleen. Bitcoinin rajallisen onnistumisen myötä on alettu kehittämään kryptovaluuttoja, joita voidaan siirtää ja säilyttää rajattomasti ilman keskusyksikön osallistumista. (Chen & Bellavitis, 2019).

Varman (2019) mukaan haasteet lohkoketjujen käyttöönottoon liittyen finanssialalla ovatkin ensisijaisesti juridisia, sääntelyyn liittyviä, institutionaalisia tai kaupallisia, mutta teknisiäkin rajoitteitakin löytyy ja kehitykselle on vielä hurjasti tilaa. Oikeudellisten ja kaupallisten esteiden ylittäminen voi kestää useita vuosia. Keskitetyt rahoituksen välittäjät voisivat käyttää tätä aikaikkunaa rakentaakseen uudelleen menetetyt luottamuksensa ja torjuakseen lohkoketju-

jen myötä koetun uhkan tällaisia toimijoita kohtaan. Nähtäväksi jää kuitenkin, onnistuvatko he rakentamaan uudelleen luottamuksen, vai mistä syystä uusi teknologia koetaan niin uhkaavana ja epäihailtuna.

5.2.1 Oikeudelliset ja sääntelyyn liittyvät rajoitteet

Lohkoketjuteknologisten ratkaisujen ympärillä on vielä paljon epäselvyyksiä liittyen sääntelyyn ja oikeudellisiin seikkoihin. Casey ym. (2018) esittelevät tutkimuksessaan sidosryhmien huolia liittyen pseudoanonymiyteen erityisesti sääntelyiden ja lainvalvonnan näkökulmasta. Lohkoketjut mielletään turvallisiksi ja manipuloinnattomiksi, mutta niidenkin sisällä kuitenkin nähdään potentiaalisia uhkia. Bossler ja Kroenung (2022) nostavat esille kysymyksen lohkoketjupohjaisten järjestelmien käyttöönotosta erilaisissa käyttötarkoituksissa. He korostavat muun muassa kuinka järjestelmät tulisivat toteuttaa, jotta ne palvelevat esimerkiksi henkilötietojen käsittelyä koskevia säännöksiä sekä yksityisyydensuojaa. Toisekseen on vielä ratkaisematta, kuinka väärinkäytöksistä tulisi rangaista, jos sellaisia ilmenee.

Dumay ym. (2021) tuovat ilmi myös verotukseen liittyvät sääntelyt. Tokeineiden ja muunlaisten kryptovaluuttojen suhteen tulisi selvittää oikeudelliset ja verotuspolitiikkaa koskevat epäselvyydet, jotta niistä saataisiin arvokkaita ja vakaita pääomamarkkinoilla toimivia varoja. Tällaisia ongelmia ratkaistaessa tulee kiinnittää huomiota myös uudenlaisten markkinoiden globaaliuteen, joka lisää ratkaistavuuteen omat haasteensa. Koska jokaisella maalla on oma lainsäädäntönsä ja verotuspolitiikkansa, joita valvotaan tarkasti, tulisi ratkaisunkin olla kaikkia palveleva ja huomioonottava.

5.2.2 Kaupalliset rajoitteet

Kaupallisiin haasteisiin voidaan luokitella muun muassa sidosryhmien hyväksyntä ja päätös käyttöönottaa uusi lohkoketjuihin perustuva järjestelmä tai sovellus. Yksilötasolla tunteet ja henkilökohtaiset päätökset vaikuttavat voimakkaasti päätöksiin ja asenteisiin teknologioita kohtaan. On varsin tervettä tarkastella uusia teknologioita skeptisesti, jos ei täysin tunne tai ymmärrä niiden toimintaa. Lohkoketjupohjaiset ratkaisut ovat kuitenkin teknologialtaan todella kompleksisia ja monilla saattaa olla puutteita tällaisten ymmärryksessä. Kuitenkin organisaatiotasolla yleensä halutaan pysyä aallon harjalla viimeisimpien teknologioiden suhteen, jotta kilpailukyky säilyy mahdollisimman hyvänä. Tässä siis kannustimina toimivat muun muassa sidosryhmien sitouttaminen ja tavoitteiden yhteensovittaminen, jotta yksilöiden mahdolliset vastustavat mielipiteet saadaan käännettyä hyväksymään uuden teknologian käyttöönotto.

Toisena kaupallisena haasteena nähdään transaktiokustannukset. Aikaisemmin tutkielmassa esitetty kustannusten aleneminen pitää kyllä paikkansa, mutta kustannukset ovat siitä huolimatta kiistely aihe. Erityisesti kustannuksiin vaikuttavat ei-teknisten kustannusten väheneminen, mutta kuitenkin uusien teknologioiden käyttö ja erityisesti käyttöönotto ei ole ilmaista. Kustannuksia aiheuttaa Bosslerin ja Kroenungin (2022) mukaan kolmenlaiset tekijät: perus-

tamis- ja käyttöönottokustannukset, käyttömaksut sekä koordinointi- ja lieventämiskustannukset. Perustamis- ja käyttöönottokustannukset koostuvat järjestelmän käyttöönottoon liittyvistä kustannuksista. Käyttökustannukset nähdään taas hieman kiistellympänä aiheena, sillä osittain niitä alentavat automatiikka lohkoketjujen takana, jonka ansiosta resursseja tarvitaan toteutukseen vähemmän. Toisesta näkökulmasta taas kustannuksia voi lisätä uudenlaiset palvelut tai operaatiot sekä kilpailu, mitä ei keskitettyjen toimijoiden lomassa ole oikeastaan juurikaan ollut. Koordinointi- ja lieventämiskustannuksiin taas lasketaan kustannukset, joita aiheutuu, jos jotakin prosessissa menee pieleen. Tällaiset tapaukset ovat todella harvassa, mutta tutkimuksen mukaan näiden sattuessa myös taloudelliset tappiot voivat olla huomattavasti suurempia verrattuna keskitettyihin järjestelmiin. (Bossler & Kroenung, 2022).

5.2.3 Tekniset rajoitteet

Lohkoketjujen käytön volyymin kasvattamista varten on ratkaistava vielä lukuisia teknisiäkin haasteita liittyen suorituskykyyn, skaalautuvuuteen, yksityisyyden suojaan, turvallisuuteen, implementaatioon ja hallintoon (Casey ym., 2018). DeFi-sovellusten käyttäjien näkökulmasta riskit liittyvät pääasiassa ohjelmistojen toimivuuteen ja sovellusten turvallisuuteen. Vaikka teknologia itsessään onkin läpinäkyvä ja turvallinen, on sitä käyttävissä sovelluksissa omat riskinsä näiden suhteen. Jensenin, Wachterin ja Rossin (2021) mukaan lohkoketjujen muuttumattoman luonteen vuoksi riski omaisuuserien menetykseen liittyy useimmiten älysovimuksien koodausvirheisiin tai järjestelmäriskeihin. Myös petoksien vuoksi DeFi tarvitsee vielä kehitystä toimimassaan ympäristössä, jotta voidaan taata vastuulliseen innovointiin kannustava järjestelmä, josta pystytään karsimaan pois petolliset toimijat. Koska prosesseissa ei ole mukana keskustoimijaa niin kuin perinteisesti, ei kiistanalaisissa tilanteissa välttämättä ole ketään kenen puoleen kääntyä. Tämän takia voidaan myös ajautua tilanteisiin, ettei olla varmoja kenellä vastuuvollisuus on ongelmien ilmaantuessa. (Chen & Bellavitis, 2019).

Yli-Huumo ym. (2016) tutkimuksessaan erittelevät Swanin (2015) esittämiä lohkoketjujen kehityskohteita liittyen niiden haasteisiin ja rajoituksiin. Ensimmäinen näistä on lohkoketjujen transaktioiden läpivientikyky, joka vuonna 2016 on ollut 7 transaktiota sekunnissa. Tässä vertauskohtana on käytetty Visaa, joka tuolloin on kyennyt perinteisin keinoin käsittelemään jopa 2000 transaktiota sekunnissa. Myös viive on nähty lohkoketjujen haasteena, sillä nykyiset vertaisverkot ovat erittäin tukkoisia, mikä hidastaa osaltaan myös prosessien tai transaktioiden läpivientä. (Swan, 2015; Yli-Huumo ym., 2016.)

Skaalautuvuudessa on tutkimuksen mukaan vielä ratkaistavia kohtia, jotta lohkoketjujen käyttö voitaisiin tulevaisuudessa nähdä mahdollisena erilaisissa finanssialan tarpeissa (Yli-Huumo ym., 2016). Tästä esimerkkinä rahansierrot pankkien kesken nähdään suurena mahdollisuutena saada transaktiokulut alas, jos vertaisverkko saadaan kestäväksi ja käsittelemään ruuhkautumista paremmin. Se vaatii kuitenkin suurta teknologisen toteutuksen edistystä ja tapaa estää verkon ruuhkautuminen. Aikaisemmin tutkielmassa on käyty läpi lohkoketju-

jen proof-of-work- ja proof-of-stake- konsensusmekanismeja, joista jälkimmäisen keksiminen on jokseenkin nähty edistävän ongelman ratkaisua. Bossler ja Kroenung (2022) myös tutkimuksessaan korostavat skaalautuvuuden tarvetta ja nostavat esille muun muassa käytössä olevat hybridijärjestelmät, joissa osa prosesseista tapahtuu lohkoketjuja hyödyntäen, mutta kuitenkin suuri osa dataa tallennetaan vielä perinteisiin tietokantoihin. Tällaisilla ratkaisuilla voitaisiin poistaa volyyymiin liittyviä skaalautuvuuden haasteita, mutta kuitenkin niiden ei koeta olevan yksiselitteinen ratkaisu varsinaiseen ongelmaan.

6 YHTEENVETO JA POHDINTA

Tässä kandidaatintutkielmassa käytiin läpi, kuinka lohkoketjuja hyödynnetään finanssialalla ja mitä rajoittavia sekä mahdollistavia tekijöitä sen käyttöön liittyy. Tutkimuksesta nousi esille, että lohkoketjuteknologian ympärillä on vielä paljon spekulatiivista kannatusta. Tällä hetkellä sen koetaan olevan uusien teknologioiden leviämistä kuvaavan Gartnerin-hypekäyrän huipun jälkeisessä laskusuhdanteessa. Aluksi Bitcoinin julkistuksen myötä lohkoketjut nousivat nopeasti käyrän huipulle, mutta kun näytöt teknologian edistyneestä käytöstä jäivät vähäisiksi, laski sen yliarvostettu kannatuskin. (Kietzmann & Archer-Brown, 2019). Potentiaalia lohkoketjuteknologian mahdollistaman hajautetun rahoituksen ympärillä nähdään paljon, mutta se sisältää myös vielä huomattavia epäkohtia. Näistä haasteista huolimatta yrittäjät ja innovaattorit ovat halukkaita kehittämään ja toteuttamaan uusia liiketoimintamalleja hajautetusti kehittyäkseen teknologian mukana.

Tutkimuksen myötä voidaan sanoa, että pääasiallinen lohkoketjujen käyttö finanssialalla on vielä tällä hetkellä arvonsiirrossa kryptovaluuttojen muodossa. Suurimpana potentiaalisena käyttökohteena voidaan todeta olevan älysovimuksiin perustuvat prosessit, joita pystyttäisiin rajaheitojen avulla toteuttamaan ilman kolmatta osapuolta. Tällaista automatisointia voisivat hyödyntää lähes kaikki finanssialan toimijat, mutta edelleen sen suurin vaikutus nähdään olevan arvonsiirtoon jollain tapaa liittyvissä prosesseissa. Merkittäviä vaikutuksia arvonsiirtoon käytettävien resurssien alentamisessa nähdään, jos lohkoketjuteknologian avulla voitaisiin toteuttaa globaaleja kansallisia rajoja ylittäviä arvonsiirtoja. Nämä maksut ovat nykyisen finanssialan mukaisesti tänä päivänä keskitettyjä prosesseja tietyille instituutioille, jonka vuoksi ne ovat jäykkiä sekä kalliita toteuttaa. Lohkoketjuteknologian mahdollistamat DeFi-sovellukset ja keskittämättömät järjestelmät nähdään potentiaalisena ratkaisuna alentamaan kustannuksia ja arvonsiirtoon käytettyä aikaa. Tämän myötä lohkoketjuteknologian arkkitehtuuri voisi luoda muuttumattoman, läpinäkyvän ja erittäin universaalin rahoitusjärjestelmän tulevaisuudessa, joka mahdollistaisi reaaliaikaiset prosessit finanssialalla ja poistaisi täten alan jäykkyyttä.

Tutkielman tulosten valossa lohkoketjujen nähdään mahdollistavan muutoksia alan perustassa, kunhan otetaan ensin vielä edistysaskeleita rajoitteiden suunnalla. Suurimpina ongelmina voidaan todeta olevan volyymin kasvattamiseen vaikuttavat tekniset seikat, koska finanssiala halutaan pitää toimivana sen kaikille osapuolille. Toistaiseksi lohkoketjujen toimintaympäristö eli vertaisverkot eivät pysty palvelemaan tarvittavan suuta volyyimia ilman ruuhkautumisen aiheuttamia ongelmia. Toisena tärkeänä kehityskohteena ovat rajoitteet liittyen sääntelyyn ja oikeudellisiin seikkoihin, kun prosessien täytyy noudattaa tarkkoja protokollia. Tässäkin haasteena nähdään globaalin rahoitusjärjestelmän tuomat haasteet, kun täytyisi pystyä yhteensovittamaan kaikkien käyttäjäosapuolien vaatimukset, jotta lohkoketjujen tuomat hyödyt pystyttäisiin optimoimaan.

Vaikka lohkoketjujen käyttöönottoon vaikuttavista tekijöistä on olemassa joitakin alustavia arvioita, lisätutkimus tämän suuntaisesta toiminnasta on perusteltua. Tutkimuksen saralla on vielä varsin epäselvää millaisella aikajanalla kehitystä olisi mahdollista realistisesti saavuttaa. Finanssialalla käytettävien lohkoketjujen tutkimukset jäivät vielä nykyisinkin melko spekulatiivisiksi ja jokseenkin pintapuolisiksi. Tästä syystä on perusteltua sanoa, että tällä saralla tarvittaisiin syvempää ja rajoitteisiin keskittyntä tutkimusta, jotta kaikki lohkoketjujen ympärillä nähty potentiaali pystyttäisiin käytännössä toteuttamaan.

Lisätutkimuksissa tulisi keskittyä lohkoketjujen skaalautuvuuden ongelmaan, joka nähdään teknisestä näkökulmasta finanssialalla käytön suurimpana haasteena. Tämän lisäksi tulisi kehittää tehokkaampia järjestelmiä ja protokollia sekä sen myötä osoittaa, miten skaalautuvuusongelmia pystyttäisiin lieventämään käytännössä. Jatkotutkimuksessa voisi lisäksi keskittyä siihen, millaisia kompromisseja skaalautuvuuden ja turvallisuuden välillä on olemassa, jotta ratkaisuihin saataisiin optimaalisia prosessien näkökulmasta. Tämän ohella on tärkeää ottaa huomioon miten suurempi skaalautuvuus ja volyymi vaikuttavat lohkoketjuteknologian käyttöönottoon. Skaalautuvuuden ja volyymin näkökulmasta voisi olla olennaista myös tarkastella, miksi siilojen poistuminen alalla olisi erityisen tärkeää vai voisiko ratkaisu sittenkin olla esimerkiksi useat eri lohkoketjut, joissa säilytettäisiin erilaisia tietoja? Tulevaisuudessa tutkimuksen saralla olisi hyvä perehtyä myös, mitkä ovat onnistuneen kustannusten vähentämisen reunaehdot. Tämän myötä pystyttäisiin selvittämään milloin lohkoketjuja olisi kannattavaa ottaa käyttöön hyötyjen ja kustannusten näkökulmasta.

LÄHTEET

- Amesar, Y., Nerkar, Y., Mali, N., Nitnaware, A., & Prashant, Y. (2020). *Decentralized Banking Application using Block chain Technology*. International Journal of Scientific Research in Engineering and Management. 4 (9).
- Bossler, L. F., & Kroenung, J. (2022). *Exploring the Current State of Research on Blockchain and Cryptocurrency - Analyzing Enablers, Inhibitors, and Indeterminate Factors*. Association for Information Systems. Wirtschaftsinformatik 2022 Proceedings. 4.
- Buterin, V. (2016). *Ethereum: Platform Review: Opportunities and Challenges for Private and Consortium Blockchains*. 45.
- Casey, M., Crane, J., Gensler, G., Johnson, S., & Narula, N. (2018). *The impact of blockchain technology on finance: A catalyst for change*. ICMB International Center for Monetary and Banking Studies.
- Chakravarty, S., & Sarkar, P. (2020). *An Introduction to Algorithmic Finance, Algorithmic Trading and Blockchain*. Emerald Publishing Limited.
- Chen, Y., & Bellavitis, C. (2019). *Blockchain disruption and decentralized finance: The rise of decentralized business models*. Journal of Business Venturing Insights. 13 (e00151). <https://doi.org/10.1016/j.jbvi.2019.e00151>
- Dumay, J., Garanina, T., & Ranta, M. (2021). *Blockchain in accounting research: Current trends and emerging topics*. Accounting, Auditing & Accountability Journal. 35 (7). <https://doi.org/10.1108/AAAJ-10-2020-4991>
- Gaži, P., Kiayias, A., & Zindros, D. (2019). *Proof-of-Stake Sidechains*. IEEE Symposium on Security and Privacy (SP), 139–156. <https://doi.org/10.1109/SP.2019.00040>
- Harwick, C., & Caton, J. (2020). *What's Holding Back Blockchain Finance? On the Possibility of Decentralized Autonomous Finance*. The Quarterly Review of Economics and Finance. 84 (420-429). <https://doi.org/10.1016/j.qref.2020.09.006>
- Heiskanen, H. (22.11.2017). *Kryptovaluutat ja ICO (Initial Coin Offering) sijoituskohteina, onko kyse kuplasta?*. Finanssisivonta. <https://www.finanssisivonta.fi/tiedotteet-ja-julkaisut/blogit/2017/kryptovaluutat-ja-ico-initial-coin-offering-sijoituskohteina-onko-kyse-kuplasta/>
- Hewa, T., Ylianttila, M., & Liyanage, M. (2021). *Survey on blockchain based smart contracts: Applications, opportunities and challenges*. Journal of Network and Computer Applications. 177 (102857). <https://doi.org/10.1016/j.jnca.2020.102857>

- Jensen, J., Wachter, V., & Ross, O. (2021). *An Introduction to Decentralized Finance (DeFi)*. *Complex Systems Informatics and Modeling Quarterly*, 26 (46-54). <https://doi.org/10.7250/csimq.2021-26.03>
- Johnson, D., Dandapani, K., & Sharokhi, M. (Eds.). (2020). *Blockchain Applications in Finance*. Emerald Publishing Limited. <http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=6423594>
- Kietzmann, J., & Archer-Brown, C. (2019). *From hype to reality: Blockchain grows up*. *Business Horizons*, 62 (3). <https://doi.org/10.1016/j.bushor.2019.01.001>
- Knüpfer, S., & Puttonen, V. (2018). *Moderni rahoitus (10. painos)*. Alma.
- Mougayar, W., & Buterin, V. (2016). *The business blockchain: Promise, practice, and application of the next Internet technology (1st edition)*. John Wiley & Sons, Inc.
- Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Cryptography Mailing list at <https://metzdowd.com>.
- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). *Blockchain*. *Business & Information Systems Engineering*, 59 (3), 183–187. <https://doi.org/10.1007/s12599-017-0467-3>
- Perwej, Dr. A., Perwej, Dr. Y., & Haq, K. (2019). *Blockchain and its Influence on Market*. *International Journal of Computer Science Trends and Technology* 7 (5), 82-91. <https://doi.org/10.33144/23478578/IJCST-V7I5P10>
- Schär, F. (2021). *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*. *Federal Reserve Bank of St. Louis Review*, 103 (2), 153-74. <https://doi.org/10.20955/r.103.153-74>
- Suomen Pankki. (2022). *Rahoitusjärjestelmä*. <https://www.suomenpankki.fi/fi/rahoitusvakaus/rahoitusjarjestelma-lyhyesti/>
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy (1st edition)*. O'Reilly Media.
- Tapscott, A., & Tapscott, D. (2017). *How Blockchain Is Changing Finance*. Harvard Business Review.
- Thakor, A. V. (2020). *Fintech and banking: What do we know?* *Journal of Financial Intermediation*, 41 (100833). <https://doi.org/10.1016/j.jfi.2019.100833>
- Tiloooby, A. (2018). *The Impact of Blockchain Technology on Financial Transactions*. 162. Dissertation, Georgia State University.
- Treleaven, P., Brown, R., & Yang, D. (2017). *Blockchain Technology in Finance*. *Computer*, 50 (9), 14–17. <https://doi.org/10.1109/MC.2017.3571047>

- Varma, J. (2019). *Blockchain in Finance*. Vikalpa. The Journal for Decision Makers. 44 (1). 1-11. <https://doi.org/10.1177/0256090919839897>
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). *Where Is Current Research on Blockchain Technology? – A Systematic Review*. PLOS ONE. 11 (10). e0163477. <https://doi.org/10.1371/journal.pone.0163477>
- Yu, T., Lin, Z., & Tang, Q. (2018). *Blockchain: The Introduction and Its Application in Financial Accounting*. Journal of Corporate Accounting & Finance. 29 (4). 37-47. <https://doi.org/10.1002/jcaf.22365>
- Zhang, C., Wu, C., & Wang, X. (2020). *Overview of Blockchain Consensus Mechanism*. Proceedings of the 2020 2nd International Conference on Big Data Engineering, 7-12. <https://doi.org/10.1145/3404512.3404522>
- Zhao, J. L., Fan, S., & Yan, J. (2016). *Overview of business innovations and research opportunities in blockchain and introduction to the special issue*. Financial Innovation, 2 (28). <https://doi.org/10.1186/s40854-016-0049-2>