Tampereen yliopisto

Niilo Koskinen

LOHKOKETJUTEKNOLOGIAAN PERUSTUVA RAHOITUS

Johtamisen ja talouden tiedekunta
Kandidaatintutkielma
Syyskuu 2022

TIIVISTELMÄ

Niilo Koskinen: Lohkoketjuteknologiaan perustuva rahoitus
Kandidaatintutkielma
Tampereen yliopisto
Kauppatieteiden kandidaatin tutkinto-ohjelma, taloustiede
Syyskuu 2022

Lohkoketjuteknologian on ennustettu mullistavan sähköisten palveluiden tarjoamisen. Tämä nouseva teknologia yhdistetään useimmiten rahoitusalaan, jossa lohkoketjuteknologiaa on toistaiseksi hyödynnetty eniten. Tässä tutkielmassa tutkitaan lohkoketjuihin pohjautuvia hajautettuja rahoituspalveluja sekä niiden taustalla toimivaa teknologiaa. Työn tavoitteena on luoda kirjallisuuskatsauksena yleiskuva hajautetusta rahoituksesta käsitellen sekä ilmiön etuja että heikkouksia pohjautuen aiempaan kirjallisuuteen.

Tutkielman alussa käsitellään yleisesti lohkoketjuteknologiaa sekä älysopimuksia hyödyntävän Ethereum-lohkoketjualustan toimintaa ennen siirtymistä hajautettujen rahoituspalveluiden tarkasteluun. Hajautettujen rahoituspalveluiden tarkastelu on jaettu kahteen osaan. Ensin käsitellään eri rahoituspalveluiden rakennetta ja toimintaa, jonka jälkeen siirrytään käsittelemään hajautettuihin rahoituspalveluihin liittyviä hyötyjä ja heikkouksia.

Kirjallisuudesta nousee esiin monia lohkoketjuteknologiaan pohjautuvien hajautettujen rahoituspalveluiden etuja perinteisiin rahoituspalveluihin nähden. Tutkimustuloksissa korostuu etenkin lohkoketjuteknologian mahdollistama läpinäkyvyys, tehokkuus sekä saatavuus. Kirjallisuuden perusteella hajautettu rahoitus mahdollistaa halvemmat transaktiot, läpinäkyvämmän toiminnan sekä rahoituspalvelut saatavuuden kaikille myös pankkipalveluja vailla oleville. Myös monia ongelmia sekä riskejä nousee kirjallisuudessa toistuvasti esiin. Suurimpina ongelmina aineiston perusteella pidetään lohkoketjualustojen heikkoa skaalautuvuutta, virheitä älysopimusten koodeissa sekä sääntelyyn liittyvää epävarmuutta. Tutkielman perusteella voidaan todeta, että hajautettu rahoitus ei vielä haasta perinteisiä rahoituspalveluja, mutta sen potentiaali on suuri ja nuori ala kehittyy kovaa vauhtia.

Avainsanat: lohkoketju, hajautettu rahoitus, kryptovaluutta, Bitcoin, Ethereum

Sisällysluettelo

1 JOHDANTO

Tämä kandidaatintutkielma käsittelee lohkoketjuteknologiaan perustuvia hajautettuja rahoituspalveluita. Työ toteutetaan laadullisena tutkimuksena hyödyntämällä olemassa olevaa kirjallisuutta lohkoketjuteknologiasta ja hajautetuista rahoituspalveluista. Työn tavoitteena on muodostaa kokonaiskuva hajautettujen rahoitussovellusten toiminnasta sekä niiden heikkouksista ja hyödyistä.

1.1 Tutkielman tausta

Lohkoketjuteknologian ja etenkin siihen yhdistettävien kryptovaluuttojen suosion kasvu on ollut suurta koko niiden noin kymmenen vuoden olemassaolon ajan. Kryptovaluuttoja omistivat pitkään vain niistä ja niiden teknologiasta todella kiinnostuneet ihmiset, jotka uskoivat lohkoketjuteknologian tulevaisuuteen. Viimeisten vuosien aikana kasvanut kryptovaluuttojen mediahuomion määrä ja kryptovaluuttojen nopeat arvonheilahtelut ovat houkutelleet paljon myös pikaisen rikastumisen toivossa eläviä ihmisiä ostamaan ja omistamaan kryptovaluuttoja, ja yhä useampi ihminen on vähintäänkin kuullut kryptovaluutoista jossakin yhteydessä.

Harva kuitenkaan todella ymmärtää kryptovaluuttojen takana olevan lohkoketjuteknologian toimintaa ja sen muita mahdollisia käyttökohteita valuuttojen lisäksi. Lohkoketjuteknologiasta mediassa käytävä keskustelu rajoittuu monesti vain kryptovaluuttojen tarkasteluun ja nekin nähdään usein ennemminkin riskisenä ja spekulatiivisena sijoituskohteena kuin mahdollisena fiat-rahan haastajana ja korvaajana.

Lohkoketjuteknologia poistaa tarpeen keskitetyille toimijoille valuuttojen lisäksi myös muista rahoituspalveluista. Näitä lohkoketjuteknologiaan perustuvia hajautettuja rahoituspalveluita kutsutaan nimellä DeFi, joka tulee englanninkielisistä sanoista ”decentralized finance” eli vapaasti suomennettuna hajautettu rahoitus. Kyse on kuitenkin hyvin tuoreesta vain muutaman vuoden vanhasta ilmiöstä, josta melko harva kryptovaluuttaalaa seuraamaton on edes kuullut.

1.2 Tutkielman tavoite

Tämän kandidaatintutkielman tavoitteena on muodostaa yleiskuva hajautetusta rahoituksesta ilmiönä pohjautuen aiempaan kirjallisuuteen aiheesta kirjallisuuskatsauksen muodossa. Tarkoituksena on saada vastaus tutkimuskysymykseen: Miten hajautetut rahoituspalvelut toimivat ja mitkä ovat niiden hyödyt ja heikkoudet? Tavoitteena on myös muodostaa kokonaiskuva hajautetun rahoituksen tilasta perinteisen keskitetyn finanssijärjestelmän haastajana.

Tavoitteena on tutkia ilmiötä kriittisesti ja löytää hajautettujen palveluiden hyötyjä kuin myös heikkouksia. Käsittelen lisäksi mahdollisia ratkaisuja hajautettujen rahoitussovellusten ongelmiin sekä alan tulevaisuuden näkymiä. Näen tarpeelliseksi käsitellä myös lohkoketjuteknologiaa yleisesti ilmiön kokonaisvaltaisen ymmärtämisen kannalta.

Aiheen uutuudesta johtuen sitä ei ole tutkittu vielä erityisen paljoa ja suomenkielistä kirjallisuutta aiheesta ei vielä ole. Ilmiön jatkuvan kehityksen takia koen tärkeäksi käyttää mahdollisimman tuoreita lähteitä työssäni.

Tutkimus rajataan käsittelemään erityisesti Ethereum-lohkoketjualustaa ja sen ekoympäristössä toimivia rahoitussovelluksia. Ethereum on toistaiseksi hallitseva lohkoketjualusta hajautetuille rahoitussovelluksille, joten käsittelyn rajaaminen koskemaan erityisesti sitä tuntui luonnolliselta valinnalta.

1.3 Hajautettu vai keskitetty

Tutkielmassa käytetään paljon termejä hajautettu ja keskitetty, joten koen tarpeelliseksi avata näiden eroavaisuuksia heti tutkielman aluksi. Tässä tutkielmassa näillä termeillä viitataan erilaisiin valtarakennemalleihin. Perinteisesti organisaatioissa, kuten rahoituspalvelua tarjoavassa yrityksessä, valta on keskitetty tietylle toimijalle, joka voi olla esimerkiksi rahoituspalvelua tarjoavan yrityksen johto. Tällaista valtarakennemallia kutsun tutkielmassa termillä keskitetty.

Termillä hajautettu viitataan taas rakenteisiin, jossa valta ei ole yksittäisellä taholla vaan nimensä mukaisesti hajautettu. Tässä tutkielmassa käsiteltävien rakenteiden hajautus on

toteutettu lohkoketjuteknologialla. Esimerkiksi kryptovaluuttojen kohdalla vallan hajautus on toteutettu lohkoketjuteknologialla, joka mahdollistaa, että millään taholla ei ole valtaa esimerkiksi luoda lisää kyseistä kryptovaluuttaa tai sulkea toimijoita palvelun ulkopuolelle.

1.4 Tutkielman rakenne

Tutkielmassa tarkastellaan hajautettua rahoitusta viiden pääluvun avulla. Ensimmäisessä luvussa esitellään tutkielman aihe ja tavoitteet. Toisessa luvussa siirrytään käsittelemään lohkoketjujen ja erityisesti Ethereum-lohkoketjualustan toimintaa. Tämän jälkeen käsitellään hajautetun rahoitusympäristön toimintaa ja erilaisten rahoituspalveluiden toteutustapoja hajautetussa ympäristössä. Tutkielman keskeisimmässä neljännessä luvussa käydään läpi hajautetun rahoituksen merkittävimpiä hyötyjä ja ongelmia kokonaiskuvan luomiseksi hajautetun rahoituksen nykytilasta. Lopuksi viimeisessä luvussa tehdään yhteenveto koko tutkimuksesta ja sen tuloksista.

2 LOHKOKETJUTEKNOLOGIA

Lohkoketjuteknologian juuret yltävät aina vuoteen 1991 asti, jolloin Stuart Habert ja Scott Stornetta julkaisivat artikkelin ”Kuinka merkitä digitaalisen asiakirjan aikaleima”. Tätä artikkelia voidaan pitää lohkoketjuteknologian teoreettisena perustana. Siinä Habert ja Stornetta esittävät, kuinka digitaalisen asiakirjan aikaleimaamisen voisi toteuttaa luotettavalla tavalla ilman väärentämisen mahdollisuutta. Ratkaisuksi esitetään hajautetun tietoketjun hyödyntämistä, jolloin luottamuksen tarve keskitettyyn toimijaan poistuu, kun luottamus on hajautettu palvelun käyttäjien kesken. (Haber & Stornetta, 1991.)

Laajempaa huomiota teknologia sai kuitenkin vasta vuonna 2008, kun Satoshi Nakamoto esitteli Bitcoinin idean julkaisemassaan dokumentissa. Hänen ideoimansa Bitcoin voidaan nähdä eräänlaisena vastareaktiona vuoden 2008 finanssikriisille, joka osoitti keskitetyn finanssijärjestelmän heikkoudet. Nakamoton Bitcoinin päätarkoitus olikin päästä eroon kolmansista osapuolista elektronisten maksujen välittäjinä. Hän halusi luoda elektronisen maksujärjestelmän, joka perustuu kryptografiseen suojaukseen luottamuksen sijasta. Nakamoton mukaan Bitcoin mahdollistaa suorat toimijoiden väliset transaktiot ilman tarvetta luotettavalle kolmannelle osapuolelle. (Nakamoto, 2008.)

2.1 Lohkoketjut

Lohkoketju on eräänlainen väärentämätön ja hajautettu digitaalinen tilikirja, joka mahdollistaa digitaalisten erien siirtämisen suoraan käyttäjältä käyttäjälle (Bamakan, Motavali & Bondarti, 2020). Lohkoketju koostuu tietoa sisältävistä lohkoista ja nämä lohkot ovat linkittyneet toisiinsa muodostaen ketjun. Jokaisessa lohkoketjun lohkossa on tieto transaktiosta tai muusta tapahtumasta sekä lisäksi tieto edellisestä lohkosta linkittyen näin osaksi ketjua. Identtiset kopiot tästä ketjusta jaetaan ympäri vertaisverkkoa. (Hirsh & Alman, 2019.) Lohkoketju voidaan siis nähdä yhtenä suurena tilikirjana, jossa yksi lohko sisältää tiedon yhdestä tai useammasta transaktiosta.

Lohkoketju toimii vertaisverkkona, jossa verkon yhtenä palvelimena voi toimia mikä tahansa verkkoon kytketty tietokone, johon on asennettu vaadittava sovellus. Tämä verkon toimija varmistaa, tallentaa ja monistaa tiedon, jonka se saa toiselta verkon toimijalta,

johon se on yhteydessä. (Lee, 2015). Verkkoa siis ylläpitää suuri määrä itsenäisiä tietokoneita ympäri maapalloa, jolloin järjestelmä on hajautettu eikä yhden keskitetyn toimijan hallinnassa.

2.2 Lohkoketjujen tyypit

On tärkeää ymmärtää, että lohkoketju terminä ei ole yksiselitteinen, koska lohkoketjuja on erityyppisiä, joiden toimintaa ohjaavat teknologiset ratkaisut eroavat toisistaan. Ensinnäkin lohkoketjut voidaan jakaa julkisuutensa perusteella julkisiin, yksityisiin ja konsortiolohkoketjuihin. Osallistumisen avoimuuden perusteella lohkoketjut voidaan jakaa myös luvanvaraisiin ja luvattomiin lohkoketjuihin.

Tunnetuimmat julkiset lohkoketjut ovat Bitcoin ja Ethereum. Julkinen lohkoketju on täysin hajautettu ja läpinäkyvä eikä sitä voi manipuloida kukaan yksittäinen taho. Yksityiset lohkoketjut taas ovat käytännössä keskitettyjä järjestelmiä, koska niitä hallinnoi yksi toimija. Tämä toimija voi muokata lohkoketjua ja säätää sen avoimuutta rajaamalla käyttäjiä pois. Yksityinen lohkoketju kuitenkin mahdollistaa nopeammat transaktiot kuin julkinen, koska sen uusien transaktioiden vahvistamisprosessi on kevyempi ja nopeampi julkiseen verrattuna (Jo ym., 2020). Yksi tunnetuimmista yksityisestä lohkoketjusta on Linuxin projekti Hyperledger Fabric. Se on tarkoitettu ympäristöksi, jossa yritykset voivat kehitellä ja rakentaa lohkoketjualustoja ja niihin liittyviä sovelluksia helposti ja turvallisesti (Hyperledger Foundation, 2022).

Konsortiolohkoketju on taas edellisten välimuoto. Sen hallinto koostuu useammasta eri organisaatiosta, jotka ovat usein saman alan toimijoita. Tällaisessa järjestelmässä valta on hajautettu useammalle eri organisaatiolle, ja muutokset lohkoketjun toimintaan vaativat yhteisymmärryksen organisaatioilta. (Bouraga, 2021.) Tämän tyyppisestä lohkoketjusta hyvä esimerkki on projekti nimeltä Corda, jonka tarkoitus on yhdistää rahoitusalan toimijoita samaan ekosysteemiin. Projektissa on mukana maailman suurimpia finanssialan toimijoita, kuten JP Morgan ja Goldman Sachs.

Jako luvanvaraisiin ja luvattomiin lohkoketjuihin tehdään lohkoketjuun osallistuvien rajaamisen perusteella. Valtaosa lohkoketjuista, kuten Bitcoin ja Ethereum, kuuluvat luvat-

tomiin lohkoketjuihin. Luvattomassa lohkoketjussa kuka tahansa voi suorittaa transaktioita ja myös osallistua uusien lohkojen vahvistamiseen. Luvanvarainen lohkoketju on taas lohkoketju, jossa tarvitaan lupa verkkoon osallistumiseen. Ainoastaan hyväksytyt toimijat voivat tarkastella verkon tietoja ja osallistua uusien tapahtumien validoimiseen. (Guadamuz, 2019.)

2.3 Konsensusalgoritmi

Hajautetussa tietojärjestelmässä suurena haasteena on yhteinen tiedonkäsittely. Uuden tiedon oikeellisuus täytyy varmistaa ennen kuin se voidaan lisätä osaksi lohkoketjua, jotta väärennetyt transaktiot eivät olisi mahdollisia. Verkossa tapahtuvat transaktiot jaetaan kaikkien verkon osallistujien kesken ja toimijat muodostavat yhteisymmärryksen siitä, miten tilikirja tulisi päivittää. (Johansson, Eerola, Innanen, Viitala & Alasaarela, 2019, 56) Tämä prosessi voidaan toteuttaa erilaisilla konsensusalgoritmeilla, joista yleisimmät ovat Proof of Work (PoW), Proof of Stake (PoS) ja Proof of Importance (PoI). Konsensusalgoritmi on protokolla, jolla uudet lohkot liitetään osaksi lohkoketjua (Morabito, 2017).

Kun on saavutettu yhteisymmärrys siitä, kuinka hajautettu tilikirja tulisi päivittää uusien transaktioiden osalta, suoritetaan nämä päivitykset ja kaikki osallistujat saavat identtisen kopion uudesta päivitetystä tilikirjasta. Tätä kryptografisesti eli salakirjoitustekniikkaa hyödyntäen salattua lohkoketjua ei voida muokata enää tietojen kirjaamisen jälkeen, mikä tekee sen manipuloinnista lähes mahdotonta. (Johansson ym., 2019, 57) Konsensusprosessin ansiosta lohkoketjuissa ei ole tarvetta keskitetylle toimijalle, vaan lohkoketjun päivittäminen tapahtuu käyttäjien yhteisen konsensuksen avulla.

Proof of Work on vanhin todistuspohjainen konsensusalgoritmi. Tätä algoritmia käyttävät esimerkiksi suurimmat kryptovaluutat Bitcoin ja Ethereum. Tässä konsensusprosessissa vertaisverkon toimijat käyttävät koneidensa laskentatehoa saadakseen oikeuden lisätä uusi lohko osaksi ketjua. (Nguyen & Kim, 2018.) Näitä verkon ylläpitäjiä kutsutaan louhijoiksi ja laskentatehon tarjoamista lohkoketjun ylläpitämiseksi kutsutaan louhinnaksi. Louhijat yrittävät ratkaista vaikeita matemaattisia pulmia ja oikein ratkaissut saa oikeuden lisätä uuden lohkon osaksi ketjua. Näin löydetään ”pätevin” toimija louhijoiden jou-

kosta. Louhijat saavat laskentatehon tarjoamisesta palkkioksi kyseisen lohkoketjun valuuttaa. Uuden tiedon lisäämiseksi lohkoihin ja lohkojen liittämiseksi osaksi ketjua tarvitaan siis louhijoita ja ilman näitä järjestelmä ei toimisi. (Johansson ym., 2019, 69)

Tämän algoritmin yhtenä heikkoutena on kuitenkin sen valtava energiankulutus. Kaikki louhijat käyttävät valtavasti sähköä koittaessaan ratkaista samaa matemaattista pulmaa. Esimerkiksi pelkästään Bitcoinin louhintaan käytettävä sähkönkulutus on Cambridgen Yliopiston laskurin (2022) mukaan noin 130 terawattituntia vuodessa. Tilastokeskuksen (2022) mukaan koko Suomen vuosittainen sähkönkulutus on noin 80 terawattituntia. Bitcoinin ylläpitäminen kuluttaa siis enemmän sähköä kuin koko Suomi. Osittain myös tästä syystä Ethereum on siirtymässä PoW-algoritmista Proof-of-Stake-algoritmiin.

PoS-algoritmi on PoW-algoritmia energiatehokkaampi, koska siinä valitaan yksi toimija suorittamaan vaadittu tehtävä. PoW algoritmiin pohjautuvassa järjestelmässä verkon ylläpitäjiä ei kutsuta louhijoiksi vaan vahvistajiksi. Toimijan todennäköisyys päästä lisäämään uusi lohko osaksi ketjua ei riipu laskentatehon määrästä vaan vahvistamistoimintaan talletetun valuutan määrästä. Tätä lukittua valuuttaosuutta kutsutaan ”stakeksi”. Mitä isompi osuus sitä suurempi mahdollisuus tulla valituksi. Tehtävän suorittaja saa onnistuneesta suorituksesta palkkioksi kyseisen lohkoketjun kryptovaluuttaa, mutta virheellisestä suorituksesta häneltä otetaan pois tallettamastaan osuudestaan suurempi määrä kuin mitä onnistuneesta suorituksesta olisi saanut. Tämä luo suorittajalle intressin suorittaa tehtävä kunnolla. (Hassani ym., 2019 s. 64–65.)

PoS-algoritmin toimintatapa perustuu ajatukseen, että mitä enemmän kyseisen lohkoketjun valuuttaa toimijalla on, sitä suurempi intressi sillä on ylläpitää järjestelmän turvallisuutta ja toimivuutta. Järjestelmässä tapahtuvat väärinkäytökset laskisivat nimittäin valuutan ja siten toimijan varallisuuden arvoa. (Bentov, 2016.) Toisaalta järjestelmää on kritisoitu siitä, että siinä ”rikkaat rikastuvat”, koska palkkiot päätyvät suuremmalla todennäköisyydellä enemmän valuuttaa jo ennestään omaaville.

Kolmas käytetyimmistä algoritmeista on Proof-of-Importance, jossa vahvistajat pisteytetään tärkeyden mukaan. Pisteet muodostuvat omistetun valuutan määrän sekä suoritettujen transaktioiden suuruuden ja määrän perusteella. (Hazari & Mahmoud, 2019.) Tämä algoritmi yrittää tarjota ratkaisun aikaisemmin mainitsemaani PoS-algoritmin ”rikkaat rikastuvat” ongelmaan.

2.4 Älysopimukset

Vaikka Bitcoin mahdollistikin hajautetun valuuttajärjestelmän, jossa rahaa voidaan siirtää käyttäjältä toiselle ilman keskitettyä toimijaa, ei sen järjestelmä mahdollista muita tärkeitä rahoituspalveluja. Pelkkä mahdollisuus rahan siirtämiseen ei ole riittävän monipuolinen rahoitusjärjestelmä perinteisten keskitettyjen rahoitusinstituutioiden korvaamiseksi. Älysopimukset tarjoavat tähän ratkaisun mahdollistamalla monimutkaistenkin rahoituspalveluiden muodostamisen lohkoketjuympäristössä. Älysopimuksiin perustuvaa lohkoketjua kutsutaankin monesti lohkoketju 2.0:ksi. Vuonna 2015 toimintansa aloittanut Ethereum oli ensimmäinen älysopimusten hyödyntämisen mahdollistanut lohkoketju.

Älysopimukset ovat lohkoketjuun talletettuja ohjelmia, joiden suorittaminen on automatisoitu. Älysopimuksiin on koodattu mitä tapahtuu, kun tietyt ehdot täyttyvät. (Schaer, 2021) Älysopimus voi tarvittaessa myös säilöä lohkoketjun valuuttaa, kuten Etheriä Ethereum-verkossa. Joustavuutensa ansiosta älysopimukset mahdollistavat monenlaiset rakennelmat, kuten uusien kryptovaluuttojen perustamisen helposti Ethereum alustan päälle. (Palladino, 2019.)

Yksi älysopimusten tärkeä ominaisuus on niiden muuttumattomuus. Kun älysopimus on liitetty lohkoketjun osaksi, ei sitä voida enää muuttaa. Tästä syystä älysopimuksille tehdään laajoja tarkastuksia ohjelmointivirheiden huomaamiseksi ennen niiden liittämistä lohkoketjuun. (Viglianisi, 2020.) Älysopimus ei voi myöskään olla riippuvainen mistään lohkoketjun ulkopuolisesta lähteestä, vaan Ethereum verkossa oleva älysopimus voi olla vuorovaikutuksessa vain toisen Ethereum verkossa toimivan älysopimuksen kanssa (Palladino, 2019).

DApp:it (Decentralized Application, suom. hajautettu sovellus) ovat hajautetun lohkoketjualustan päälle rakennettuja applikaatioita, joiden toiminta perustuu joukkoon älysopimuksia. Kuluttajat käyttävät näitä sovelluksia verkkosivun tai selaimen lisäosan kautta, jolla ei ole erillistä serveriä vaan se on yhteydessä suoraan lohkoketjun verkkoon. Teknisesti sovellukset toimivat niin, että sovellus lähettää käyttäjän puolesta transaktioita älysopimuksiin, jotka sitten tekevät niihin ohjelmoituja toimenpiteitä. (Palladino, 2019.) Nämä hajautetut sovellukset mahdollistavat esimerkiksi rahoituspalveluiden järjestämisen ilman keskitettyä toimijaa välikätenä.

DApp:it ovat token-pohjaisia eli niiden käyttäminen vaatii kyseisen sovelluksen käyttämän tokenin omistamista. Token voidaan nähdä sovelluksen sisäisenä vaihdonvälineenä. Tokenisointi on prosessi, jossa tiettyä arvoa luodaan edustamaan digitaalinen token. Yksi token on tämän tokenisoidun arvon laskentayksikkö. (Freni, Ferro & Moncada, 2020). Sovelluksessa maksettavat palkkiot maksetaan sovelluksen tokeneissa ja niiden kokonaismäärä kierrossa on ennalta määrätty sovellusta perustettaessa.

Kuluttajan kannalta sovellukset ovat yleensä suhteellisen helppokäyttöisiä, mutta vaativat kuitenkin jonkin verran perehtymistä käytettävän lohkoketjualustan ja sen valuutan (esimerkiksi Ethereum ja Ether) toimintaan. Sovelluksien käyttäminen nimittäin vaatii sovelluksen käyttämän valuutan tai tokenin omistamista. Käyttäjän näkökulmasta DAppien käyttö ei kuitenkaan eroa oikeastaan mitenkään perinteisten sovellusten käytöstä.

2.5 Ethereum

Olen jo aikaisemmin tekstissä sivunnut lohkoketjua nimeltä Ethereum. Se on käytetyin alusta erilaisille hajautetuille sovelluksille ja myös hajautetuista rahoitussovelluksista suurin osa on rakennettu Ethereumin päälle. Siksi käsittelemme nyt tarkemmin juuri Ethereum lohkoketjua ennen siirtymistä hajautettujen rahoitussovellusten käsittelyyn.

Ethereum on julkinen ja luvaton lohkoketju eli se on täysin hajautettu ja kuka tahansa voi osallistua sen verkon varmistamiseen. Sen käyttämä ohjelmointikieli on Solidity ja sen oma natiivi kryptovaluutta on Ether (ETH). (Solomon, 2019). Ether on kirjoittamishetkellä markkina-arvoltaan kryptovaluutoista toiseksi suurin heti Bitcoinin jälkeen. Ethereum käyttää toistaiseksi Proof of Work konsensusalgoritmia, mutta sen siirtymisprosessi kohti Ethereum 2.0 versiota on jo käynnissä. Suurin Ethereum 2.0:n mukanaan tuoma muutos on siirtyminen Proof of Stake algoritmin käyttämiseen konsensusprosessina. Uuden Ethereum 2.0:n tavoitteena on parempi skaalautuvuus ja pienemmät transaktiokustannukset. (Ethereum, 2022a.) Skaalautuvuudella tarkoitetaan lohkoketjun kykyä kasvattaa lohkoketjussa tapahtuvien transaktioiden volyymiä ilman toiminnan häiriintymistä.

Ethereum julkaistiin ja käynnistettiin vuonna 2015, mutta sen perustaja Vitalik Buterin oli kehitellyt sitä jo vuodesta 2013 lähtien. Ethereum mullisti lohkoketjujen käyttömah-

dollisuudet älysopimusten avulla. Se oli ensimmäinen älysopimuksia hyödyntävä lohkoketju. Sen päälle voi kuka tahansa vapaasti kehitellä uusia älysopimuksia ja niitä hyödyntäviä DAppeja. (Solomon, 2019). Selkeimmät käyttömahdollisuudet ovat rahoitusalalla, mutta myös sosiaaliseen mediaan ja videopeleihin liittyviä sovelluksia on kehitelty.

3 HAJAUTETTU RAHOITUS

DeFi, joka tulee englanninkielisistä sanoista ”decentralized finance”, on yksi puhutuimmista ilmiöistä kryptoalalla. DeFi eli vapaasti suomennettuna ”hajautettu rahoitus” viittaa vaihtoehtoiseen hajautettuun rahoitusinfrastruktuuriin, jonka päätarkoitus on päästä eroon vallan keskittymisestä keskitetyille toimijoille. DeFi on siis yleiskäsite kaikille lohkoketjuteknologian hajautukseen perustuville rahoituspalvelusovelluksille. Näiden sovellusten toiminta perustuu lohkoketjun sisältämiin älysopimuksiin eivätkä ne vaadi välittäjiä tai muita keskitettyjä instituutioita, kuten pankkeja (Schaer, 2021).

DeFi sovelluksista noin 70 % eli valtaosa on rakennettu Ethereum-lohkoketjualustan päälle (Ossinger, 2022). Ensimmäinen DeFi projekti nimeltään Maker käynnistettiin Ethereum-lohkoketjussa vuonna 2017. Ethereum on edelleen hallitseva alusta DeFi palveluille, mutta uusia kilpailevia alustoja on useita. DeFi projektien määrästä ei ole saatavilla tarkkaa ajankohtaista tietoa, mutta erilaisia projekteja on jo ainakin useampi sata (DeFi Pulse, 2022a).

Yhteenlaskettu DeFi projektien lukittu arvo on kirjoittamishetkellä noin 35 miljardia dollaria, mutta vuoden 2022 aikana arvo on käynyt parhaimmillaan 100 miljardissa dollarissa. Vielä kaksi vuotta sitten sama yhteenlaskettu arvo oli vain noin 10 miljardia dollaria. (DeFi Pulse, 2022b.) Projektien lukittu kokonaisarvo lasketaan projekteihin talletettujen kryptovarojen kokonaisarvona ja se sisältää kaikkiin DeFi protokollien toimintoihin talletetut varat (George, 2022). Kyseessä on siis varsin uusi, mutta kovaa vauhtia kasvava ala.

3.1 Järjestelmän rakenne

DeFi palveluiden toiminta perustuu lohkoketjussa oleviin älysopimuksiin. Älysopimuksiin on koodattu tieto toteutettavista tapahtumista, kun tietyt ehdot täyttyvät. Koodia säilytetään lohkoketjussa, joten se on kaikkien nähtävissä ja tutkittavissa. Älysopimukset voivat myös säilöä varoja ja toimia näin välittäjänä, jonka toimintaa ohjaava koodi määrää kenelle ja millä ehdoin varoja voidaan vapauttaa. Kaikki sopimusten sisältämät toi-

mintokutsut transaktioiden muodossa varmennetaan konsensusprosessin avulla, aivan kuten normaalitkin siirtotransaktiot. (Schaer, 2021.) Älysopimukset ovat siis hyvin joustavia ja läpinäkyviä, mikä mahdollistaa monipuolisten rahoituspalveluiden rakentamisen niitä hyödyntäen.

DeFi ekosysteemin rakenne on monikerroksinen, jossa jokaisella kerroksella on selkeä tehtävänsä. Rakennetta voidaan havainnollistaa jakamalla se esimerkiksi viiteen kerrokseen, joista alin on alustakerros. Alustana toimii jokin lohkoketju, joista käytetyin on Ethereum. Kaikki muu ekosysteemissä rakentuu tämän lohkoketjun päälle. Toista kerrosta kutsutaan varallisuuskerrokseksi. Se sisältää kaikki kyseiseen lohkoketjuun liikkeelle lasketut omaisuuserät. Osana lohkoketjua toimii aina vähintäänkin sen oma natiivi valuuttansa, kuten Ethereumilla Ether (ETH). Muita lohkoketjuun liikkeelle laskettuja varallisuuseriä kutsutaan tokeneiksi. (Schaer, 2021.)

Kolmas protokollakerros koostuu protokollista, jotka tarjoavat standardeja erilaisiin käyttötarkoituksiin, kuten johdannaisten tai velkamarkkinoiden toimintaan. Nämä protokollat koostuvat usein useista eri älysopimuksista ja niitä voi kuka tahansa hyödyntää sovelluksiensa rakentamiseen. Tästä päästäänkin seuraavaan sovelluskerrokseen. DAppit eli hajautetut sovellukset yhdistelevät protokollia muodostaen erilaisia rahoituspalveluita käyttäjille. Ylimpänä viidentenä kerroksen on vielä yhdistelmäkerros, joka on sovelluskerroksen laajennus. Se muodostuu käyttäjäkeskeisistä alustoista, jotka yhdistelevät useita sovelluksia ja protokollia. Nämä yhdistelypalvelut yleensä mahdollistavat esimerkiksi eri sovellusten vertailemisen tai monimutkaisempien tehtävien suorittamisen. (Schaer, 2021.)

DeFin rakennetta tarkasteltaessa on tärkeää ymmärtää, kuinka kerrokset rakentuvat toistensa päälle. Useat eri sovellukset käyttävät samoja protokollia ja siten myös samoja älysopimuksia. Samalla tavalla useat eri älysopimukset hyödyntävät samoja tokeneita. Tämän sisäistettyä on helppo nähdä rakenteeseen liittyvä heikkous. Ylemmät tasot ovat vain yhtä turvallisia kuin tasot niiden alapuolella (Schaer, 2021). Siispä virhe jonkin älysopimuksen koodissa vaarantaa kaikki sitä hyödyntävät protokollat ja näitä protokollia hyödyntävät sovellukset. Toisaalta ekosysteemin rakenne sisältää myös etunsa. Protokollien ja sovellusten saumattoman yhdistelemisen sekä päälle rakentamisen vapaus mahdollistavat nopeasti kehittyvät ja monimuotoiset hajautetut rahoituspalvelut.

3.2 Varojen säilytys

DeFi palveluissa pankkitiliä vastaa käyttäjän digitaalinen osoite, joka on verrattavissa pankkitilin numeroon. Osoitteeseen voidaan siirtää ja siellä voidaan säilyttää kryptovaluuttoja ja muita DeFi ympäristön sisältämiä varallisuuseriä, kuten tokeneita ja älysopimuksia. Jokaisella osoitteella on oma yksityinen avaimensa, joka on pitkä merkkijono. Tällä avaimella päästään hallitsemaan osoitteen sisältöä. Jokainen osoite toimii osana yhtä tiettyä lohkoketjua, joten siihen voidaan lähettää ja siellä voidaan säilyttää vain tietyn lohkoketjun sisältämiä digitaalisia varallisuuseriä. Digitaalisiksi lompakoiksi kutsutaan ohjelmistoja, joilla luodaan ja hallitaan näitä digitaalisia osoitteita. (Schueffel, 2021) Näitä varojen hallintaan tarkoitettuja ohjelmistosovelluksia on useita kilpailevia, kuten Coinbase ja ZenGo. Digitaalisella lompakolla hallitaan tiettyjä osoitteita ja niiden avaimia. Yhteen lompakkoon voidaan yhdistää useankin eri lohkoketjun osoitteita, mikä helpottaa kryptovarallisuuden hallintaa.

Yksinkertaisin tapa säilyttää avaimia ovat online-lompakot, joita tarjoavat esimerkiksi kryptovaluuttojen kauppapaikat, kuten suomalainen Northcrypto. Tällöin varojen turvallisuus on kauppapaikan tietoturvan varassa ja varat ovat alttiina kyberhyökkäyksille. Kryptovaluuttojen olemassaolon aikana kauppapaikkojen hyökkäyksiä on ollut useita ja hyökkäyksissä on onnistuttu varastamaan satojen miljoonien dollarien edestä kryptovaluuttoja (Crystal, 2021).

Käyttäjä voi säilyttää osoitteita ja niiden avaimia myös fyysisesti, esim. paperille kirjoitettuna. Tällaista säilytystapaa kutsutaan paperilompakoksi. Kylmälompakoksi taas kutsutaan avainten säilyttämistä muistitikulla tai ulkoisella kovalevyllä, jolloin ne eivät ole yhteydessä internettiin ja täten immuuneja tietoturvahyökkäyksille. (Jan, 2018.) Kyseisiä säilytystapoja pidetään online-lompakoita turvallisempina tietoturvan kannalta, mutta ne sisältävät omat riskinsä, koska osoite ja sen avain ovat ainoa keino päästä osoitteen varoihin käsiksi. Siispä paperin tai muistitikun kadottua osoitteen sisältöön ei voi enää päästä käsiksi. Esimerkiksi kaikista tähän mennessä louhituista Bitcoineista arvioidaan kadonneen kierrosta jopa viidesosa eli noin 3 miljoonaa Bitcoinia (Kuhn, 2021). Näiden markkina-arvo tänä päivänä olisi noin 60 miljardia dollaria.

3.3 Tokenit

Ethereum lohkoketju mahdollistaa oman natiivivaluuttansa Etherin lisäksi muiden varallisuuserien lisäämisen hajautettuun tilikirjaan. Näitä muita varallisuuseriä kutsutaan tokeneiksi ja uusien varallisuuserien luomisprosessia tokenisoinniksi. Tokenien ideana on tehdä transaktioista tehokkaampia, sillä niitä voidaan siirtää käyttäjältä toiselle sekunneissa. Niitä voidaan säilöä myös älysopimuksissa, mikä on hyödyllinen ominaisuus monien rahoitussovellusten kannalta. (Schaer, 2021.) Token voidaan luoda edustamaan mitä tahansa arvoa, mikä mahdollistaa esimerkiksi johdannaisten luomisen.

Ethereumissa uudet tokenit luodaan suurimmaksi osaksi käyttäen ERC-20 standardia, joka on eräänlainen malli uusille tokeneille. Näitä tokeneita voi hyödyntää Ethereum ekosysteemissä mikä tahansa älysopimus tai sovellus. (Schaer, 2021.) Ethereum kehitti ERC-20 standardin vuonna 2015 ja se määrittää tietyt ehdot ja säännöt tokeneille Ethereum ekosysteemissä. ERC-20 mahdollistaa kehittäjille uusien tokeneiden luomisen Ethereumiin mahdollisimman pienellä vaivalla ja takaa tokeneiden turvallisuuden.

Tärkein tokenien mahdollistama asia on stablecoin, josta käytetään myös suomenkielistä termiä vakaavaluutta. Kryptovaluutat ovat tunnetusti arvoltaan melko epävakaita, mikä tekee niiden käyttämisestä rahoituspalveluissa hankalaa. Siksi Ethereumiin rakennetuissa hajautetuissa rahoituspalveluissa käytetään monesti mieluummin vakaavaluutta-tokeneita kuin natiivivaluuttaa Etheriä. Vakaavaluutat ovat tokeneita, joiden arvo on sidottu yleensä dollariin (Catalini, de Gortari & Shah, 2021). Niiden arvon pitäisi siis pysyä vakaana ja ovat täten kätevämpi vaihtoehto perinteisille kryptovaluutoille rahoituspalveluissa.

Vakaavaluutat voidaan toteuttaa monella eri tapaa ja ne vaihtelevat keskitetyistä hajautettuihin malleihin. Suurin osa vakaavaluutoista perustuu keskitettyyn malliin, kuten vanhin ja markkina-arvoltaan suurin Tether (USDT). Keskitetyssä mallissa vakaavaluutta on täysin taattu todellisilla dollareilla (dollariin sidotun vakaavaluutan tapauksessa). Tällöin tarvitaan keskitetty rahoitusinstituutio, jolla on säilössä jokaista liikkeelle laskettua vakaavaluutan yksikköä kohden yksi dollari tai sijoitusinstrumentteja, jotka ovat vaihdettavissa dollareihin. (Catalini, de Gortari & Shah, 2021.) Tällöin joudutaan luopumaan täydellisestä hajautuksesta, koska joudutaan luottamaan keskitettyyn toimijaan valuutan takaajana. Siispä hajautettuja rahoitussovelluksia, jotka hyödyntävät keskitettyyn malliin perustuvia vakaavaluuttoja, ei voida todellisuudessa pitää täysin hajautettuina.

Vakaavaluutta voidaan kuitenkin toteuttaa myös täysin hajautetulla mallilla, kuten Dai. Dai on Ethereumissa toimiva dollariin sidottu vakaavaluutta, jota voi laskea lisää liikkeelle kuka tahansa, jolla on lukittuna älysopimuksiin vakuudeksi riittävästi muita kryptovaluuttoja, kuten Etheriä. Vakuuksia täytyy olla yli 100 % arvon heilahtelujen turvaksi. Tätä mallia pidetään kuitenkin riskialttiimpana kuin keskitettyä mallia, koska kryptovaluuttojen äkillinen suuri arvonaleneminen voisi johtaa alivakuutettuihin älysopimuksiin. (Catalini, de Gortari & Shah, 2021.)

Toinen tapa toteuttaa hajautettu vakaavaluutta on algoritmimalli. Siinä vakaavaluutta ei ole taattu fiat-rahalla eikä lohkoketjuun lukituilla kryptovaroilla vaan vakaus perustuu algoritmeihin. Yleensä tämän tyyppiset valuutat muodostuvat kahdesta eri tokenista, vakaavaluutasta ja sijoitustokenista. Automaattiset algoritmit sitten säätelevät näiden välistä suhdetta kierrossa kysynnän mukaan pitäen vakaavaluutan arvon lukittuna esimerkiksi yhteen dollariin. Tällaista mallia ei kuitenkaan pidetä luotettavana vakauden mahdollistajana pitkällä aikajänteellä monien siihen sisältyvien riskien takia. (Catalini, de Gortari & Shah, 2021.)

Viiden suurimman kryptovaluutan joukkoon kuuluneen Terra Lunan ja siihen linkittyvän UST:n romahdus kesken tämän tutkielman kirjoittamisen osoitti algoritmimalliin sisältyvät riskit. Algoritmimallilla toteutetun vakaavaluutta UST:n ja sen sisarvaluutta Lunan arvot romahtivat muutamassa päivässä vain murto-osiin aikaisemmasta toukokuussa 2022. UST:n arvo laski dollarista muutamaan senttiin ja Lunan arvo 80 eurosta sentteihin. Romahdukseen johti vakaavaluutan kiinnityksen menettäminen ja sitä seurannut markkinoiden paniikki. Kiinnityksen menettämiseen taas johti äkillinen sijoittajien varojen kotiuttaminen inflaatiouutisten myötä ja osaltaan myös tekniset ongelmat Terra-verkon ruuhkautuessa. (Eklund, 2022.)

Vakaavaluutat ja muut valuuttatokenit eivät ole kuitenkaan ainoa käyttökohde tokeneille. Esimerkiksi hallintotokeneiden avulla voidaan jakaa hajautettujen organisaatioiden hallinto-oikeuksia. Token voi edustaa myös esimerkiksi osaketta tai velkakirjaa ja niin sanotut synteettiset tokenit voivat seurata jonkin todellisen maailman omaisuuserän arvoa. (Schaer, 2021.) Tokeneiden käyttömahdollisuudet ovat varsin laajat ja mahdollistavat monenlaisten rahoituspalveluiden kehittämisen joustavuutensa ansiosta.

Myös mediassa viime aikoina paljon esillä ollut NFT (non fungible token, suom. korvaamaton token) on eräänlainen token. Toisin kuin normaalit tokenit, useimmat NFT:t on muodostettu käyttäen ERC-721 tai ERC-1155 standardeja, koska jokaista NFT:tä on aina olemassa vain tasan yksi uniikki kappaleensa. NFT voi edustaa periaatteessa mitä tahansa uniikkia digitaalista tai fyysistä omaisuuserää. Jokaisella NFT:llä on oma digitaalinen tunnisteensa ja niitä on mahdoton väärentää tai kopioida. Käytännössä NFT on siis digitaalinen omistusoikeuden kirjaus, joka voidaan sitten myydä eteenpäin ja täten siirtää omistusoikeus toiselle. NFT voi edustaa esimerkiksi fyysistä asuntoa tai digitaalista kuvaa. (Ethereum, 2022b.)

3.4 Kolikkoanti (Initial Coin Offering, ICO)

Kolikkoanti on hajautettu joukkorahoituksen muoto, jolla lohkoketjuprojektien kehittäjät keräävät rahoitusta uuden kryptovaluutan tai dAppin perustamiseen. Kolikkoanti voidaan nähdä kryptomaailman vastineena perinteisen rahoitusalan listautumisannille. Kolikkoannissa lohkoketjuprojekti kerää rahoitusta myymällä projektinsa tokeneita. Käytännössä sijoittaja lähettää Etheriä tai muuta ennalta määrättyä lohkoketjun kryptovaluuttaa älysopimukseen, joka sitten lähettää takaisin sijoittajan lompakkoon projektin tokeneita.

Token voi edustaa projektin ”osaketta”, jolloin sen arvo heijastaa projektin arvoa. Toisaalta token voi olla myös valuuttatoken, mikäli projektissa on kyse uuden valuutan luomisesta. Kolmas mahdollinen tokentyyppi on hyötytoken, joka antaa omistajalleen pääsyn projektin palveluun tai tuotteeseen. (Masiak, C., Block, Masiak, T., Neuenkirch & Pielen, 2019.) Sijoittajalle voidaan jakaa kolikkoannin yhteydessä myös aikaisemmin mainittuja hallintotokeneita, joilla voidaan hajauttaa projektin hallinto-oikeuksia. Tokenit voivat siis edustaa lähestulkoon mitä tahansa, millä voisi olla jotain arvoa sijoittajan kannalta (Wiśniewska, 2018).

Kolikkoanneista on monenlaisia hyötyjä. Ne mahdollistavat projektin kehittäjien palkitsemisen ilman operatiivisen hallinnan antamista heille. Mahdolliset projektin luoman palvelun tulevat asiakkaat voivat rahoittaa palvelun luomista siinä toivossa, että palvelun ja siten myös tokenin arvo kasvaisi tulevaisuudessa. Monet kolikkoannit ovatkin tuottaneet valtavia tuottoja sijoittajille, mutta kolikkoantien joukossa on ollut myös monia huijauksia.

Ehkä suurin eroavaisuus kolikkoannin ja perinteisen listautumisannin välillä on kolikkoannin sääntelyn puuttuminen. Sääntelyn ja valvonnan puuttumisen vuoksi kolikkoannit ovat hyvin paljon riskisempiä kuin perinteiset listautumisannit. Kolikkoannissa jaetut tokenit ovat kuitenkin joustavuutensa ansiosta monipuolisempia kirjoltaan kuin perinteisen listautumisannin osakkeet ja velkakirjat. (Wiśniewska, 2018.)

3.5 Pörssialustat ja johdannaiset

Perinteiset rahoituspalvelut kuten pörssi, lainaaminen, johdannaiset ja sijoitusrahastot on jo onnistuttu toteuttamaan lohkoketjussa hajautettuina ilman tarvetta keskitetyille toimijoille. Tarkastellaan nyt näiden palveluiden toimintaa tarkemmin. Käsitellään ensin pörssejä. Suurin osa kryptovaluuttojen vaihdannasta tapahtuu keskitetyissä pörssipalveluissa, kuten Binancessa ja Coinbasessa. Keskitettyjen pörssipalveluiden tapauksessa käyttäjä joutuu luopumaan vaihdettavien varojen suorasta omistuksesta ja luottamaan keskitettyyn toimijaan, koska pörssiä käyttääkseen hänen täytyy tallettaa varansa pörssipalveluun. (Schaer, 2021.)

Täysin hajautettuja kryptovaluuttapörssejä on kuitenkin olemassa, kuten Ethereumissa toimiva Uniswap. Se toimii alustana satojen eri Ethereum pohjaisten tokeneiden vaihdannalle. (Chohan, 2021) Hajautetuissa pörsseissä vaihdot toteutuvat automaattisesti älysopimusten avulla. Transaktio toteutuu siis molempien vaihdon osapuolten kannalta samaan aikaan automaattisesti, jolloin vastapuoleen liittyvä riski poistuu. (Schaer, 2021.)

Hajautetut pörssit eivät voi ottaa vastuuta toimijoiden henkilöllisyydestä toisin kuin säädellyt keskitetyt pörssialustat. Hajautettuja pörssejä ei voida myöskään pitää vastuussa käyttäjien kokemista tappioista toisin kuin julkisen vallan sääntelyn alaisia keskitettyjä toimijoita. (Chohan, 2021.) Mahdollisesti myös näistä syistä suurin osa kryptovaluuttojen vaihdannasta tapahtuu edelleen keskitetyillä pörssialustoilla.

Hajautetussa rahoitusjärjestelmässä johdannaisia vastaa johdannaistokenit, joiden arvo seuraa toisen varallisuuserän tai minkä tahansa havaittavan muuttujan kehitystä. Tämän toteuttamiseen käytetään niin kutsuttuja keskitettyjä hintaoraakkeleita, jotka välittävät lohkoketjuun tietoa seurattavista kohteista. Hintaoraakkeleiden takia johdannaiset ovat osittain riippuvaisia keskitetyistä toimijoista eivätkä näin ollen todellisuudessa ole täysin

hajautettuja. Johdannaistokenit voidaan vielä jakaa omaisuus- ja tapahtumapohjaisiin. Omaisuuspohjaiset seuraavat jonkin varallisuuserän kehitystä, kun taas tapahtumapohjaiset tokenit seuraavat jotakin havaittavaa muuttujaa, jolla on määriteltävissä oleva joukko mahdollisia lopputulemia.

3.6 Lainauspalvelut

Lainauspalvelut ovat tärkeä osa rahoitusjärjestelmää. Hajautetussa rahoitusympäristössä on olemassa paljon erilaisia lainausalustoja. Hajautetuilla lainausalustoilla osapuolten ei tarvitse tunnistautua, mikä tekee niistä hyvin erilaisia verrattuna perinteisiin lainauspalveluihin, jotka perustuvat pitkälti pankin ja asiakkaan väliseen asiakassuhteeseen ja luottamukseen. Hajautetuissa palveluissa kuka tahansa voi osallistua toimintaan ottamalla lainaa tai tarjoamalla varojaan lainausprotokollan likviditeettipooliin ansaitakseen korkoa. (Schaer, 2021.)

Hajautettujen lainausalustojen lainojen ehdot, kuten korko ja maturiteetti määritellään älysopimuksen avulla. Lainausalustoja on oikeastaan kolmea eri tyyppiä. Aikaisemmin mainitsemani Dai on esimerkki vakuudellisten velkapositioiden mahdollistajasta. Käyttäjä tallettaa Etheriä älysopimukseen vakuudeksi ja saa vastineeksi tietyn määrän Dai tokeneita. Dai lainapositioissa vakuusaste on tällä hetkellä 150 % eli käyttäjän tulee tallettaa vakuudeksi 1,5 kertainen määrä varallisuutta Dai tokeneiden vakuudeksi. Position sulkemiseksi käyttäjän täytyy lähettää loput takaisinmaksamattomat Dai tokenit ja kertynyt korko älysopimukseen, joka sitten vapauttaa vakuudet käyttäjälle. Mikäli käyttäjä ei pysty maksamaan lainaansa takaisin tai vakuusaste tippuu alle 150 % rajan, älysopimus alkaa realisoimaan vakuuksia. Vaikka järjestelmä on lähes täysin hajautettu, se on kuitenkin johdannaistokeneiden tavoin riippuvainen hintaoraakkeleista. (Schaer, 2021.)

Uusien tokeneiden luomisen sijaan on mahdollista lainata myös jo olemassa olevia kryptovaroja toisilta käyttäjiltä. Tätä kutsutaan vakuudelliseksi velkamarkkinaksi, jossa samalla tavalla kuin Dain tapauksessa lainan täysi vakuus lukitaan älysopimukseen. Lainaajien ja lainanottajien yhteen saattaminen voidaan toteuttaa useammalla tavalla. Yksinkertaisin on peer-to-peer pohjainen malli, jossa lainaaja lainaa varansa suoraan tietylle lainanottajalle. Tällöin lainaaja alkaa saamaan korkoa vasta kun sopiva lainanottaja on

löytynyt ja maturiteetista ja kiinteästä korosta on sovittu. (Schaer, 2021.) Tämä on kuitenkin kömpelö ja tehoton malli, jonka takia valtaosa velkamarkkinatoiminnasta tapahtuu likviditeettipooleja hyödyntävillä alustoilla.

Älysopimuksiin pohjautuva likviditeettipooli koostuu kaikista lainaajien sinne tallettamista varoista. Lainaaja alkaa ansaitsemaan korkoa saman tien tallettamisen jälkeen. Pooliin voi tallettaa ja sieltä voi lainata vain sen hyväksymiä kryptovaluuttoja. Tietyn valuutan tai tokenin korko määräytyy poolissa sen kysynnän ja tarjonnan perusteella ja lainanottaja voi valita lainaushetkellä ottaako vaihtuvan vai kiinteän koron lainalleen. Lainaajalle maksetaan kiinteää korkoa, jonka suuruuteen vaikuttaa kysynnän ja tarjonnan lisäksi myös talletusaika eli kuinka pitkäksi ajaksi varat lukitaan pooliin.

Perinteiset pankit voivat säädellä lainan korkoja asiakkaan maksukäyttäytymisen perusteella. Mitä luotettavampi asiakas on aikaisemmin ollut, sitä pienempi riski tarjota tälle lainaa. Myös hajautetussa rahoituksessa tämä olisi ainakin teknisesti mahdollista. Tietyn osoitteen voidaan olettaa kuuluvan yhdelle henkilölle, jolloin kaikki sen osoitteen transaktiot historian saatossa voidaan olettaa olevan saman henkilön tekemiä. Kaikki transaktiohistoria on kaikkien vapaasti saatavilla, joten transaktiohistorian perusteella älysopimuksen on mahdollista tehdä päätelmiä käyttäjän luotettavuudesta. Toisaalta käyttäjillä saattaa olla useita osoitteita, joiden yhdistämistä samaan henkilöön ei voida tehdä hajautetussa lohkoketjuympäristössä.

Flash lainat ovat lohkoketjuteknologian mahdollistama vakuudeton laina, joka maksetaan saman tien pois. Lainaaminen ja takaisinmaksu tapahtuu kahdessa peräkkäisessä lohkoketjun lohkossa. Lainan kesto on siis vain sekunteja tai minuutteja. Flash lainojen maine on hieman kyseenalainen, sillä ne mahdollistavat hintamanipuloinnin. (Chohan, 2021.) Toisaalta ne nähdään myös tehokkaana työkaluna arbitraasien hyödyntämisessä ja portfolioiden uudelleenjärjestelyssä (Schaer, 2021).

4 HAJAUTETUN RAHOITUKSEN HYÖDYT JA HEIKKOUDET

4.1 Luottamus ja läpinäkyvyys

DeFissä käytetään kryptovaluuttoja, joita asiakas voi säilyttää omassa turvatussa digitaalisessa lompakossaan. Siispä käyttäjä voi itse hallita varojaan ilman, että kenelläkään muulla on niihin pääsyä. Keskitetyssä mallissa sen sijaan kuluttajan täytyy säilyttää varojaan pankissa. Tällöin kuluttajan täytyy luottaa, että pankki pitää varat turvassa ja että pankki on kyvykäs maksamaan asiakkaan varat ulos pankista tämän niin halutessa. Tämä on historian saatossa johtanut talouskriisien yhteydessä pankkiriiseihin, kun ihmiset ovat luottamuksen katoamisen myötä nostaneet suuret määrät talletuksia ulos pankeista ja pankit ovat ajautuneet maksukyvyttömyyteen. Hajautetussa rahoitusjärjestelmässä vastaavaa riskiä ei ole.

DeFi sovellukset ovat myös täysin läpinäkyviä sillä niiden toimintaa ohjaavien älysopimusten lähdekoodi on kaikkien tarkasteltavissa. Myös koko lohkoketjun transaktiohistoria on vapaata dataa, jota voidaan hyödyntää hajautetuissa sovelluksissa. Mahdollisten talouskriisien sattuessa tutkijoiden on helpompi tutkia, mikä on mennyt pieleen, kun kaikki data on vapaasti saatavilla. (Schaer, 2021.) Keskitetyssä järjestelmässä pääkirjanpidot joudutaan piilottamaan vain tiettyjen tahojen saataville.

Toisaalta läpinäkyvyyttä voidaan kritisoida siitä, että suurimmalla osalla ihmisistä ei ole tietotaitoa tutkia ja ymmärtää sovelluksia ohjaavaa koodia. Se ei kuitenkaan kumoa sitä tosiasiaa, että sovellusten toimintamalli on kaikkien saatavilla toisin kuin keskitetyssä järjestelmässä, jossa omia kehitelmiä suojellaan mahdollisimman hyvin kopiointia peläten.

Lohkoketjun ulkopuolinen data saadaan sovelluksien käyttöön nk. ”oraakkelien” välityksellä. Vaikka oraakkeliverkostot ottavat monesti datansa laajasta valikoimasta tiedonvälityspalveluita, tuovat ne sovelluksiin keskitettyjä riippuvaisuuksia. (Schaer, 2021.) Ulkoisen datan hyödyntämisen myötä monien hajautettujen rahoitussovellusten uskottavuus täysin hajautettuina heikkenee. Ulkoista dataa kuitenkin tarvitaan etenkin johdannaistokeneiden tapauksessa, koska niiden tehtävä on seurata jonkin toisen kohteen arvoa.

4.2 Saatavuus

Yksi DeFin vahvuuksista perinteiseen rahoitusjärjestelmään verrattuna liittyy sen saatavuuteen. DeFi:ssä protokollia ja niitä hyödyntäviä hajautettuja sovelluksia voi käyttää kuka tahansa, jolla on pääsy internetiin. DeFi sovellukset eivät vaadi tunnistautumista, mikä mahdollistaa rahoituspalvelut miljardeille ihmisille, jotka edelleen ovat vailla pankkipalveluja (Schueffel, 2021). Tästä syystä etenkin alkuvaiheessa DeFin suurimpana käyttökohteena nähdään monesti pankkipalveluja käyttävien ihmisten sijaan kehitysmaiden suuret ihmisjoukot, joilla ei ylipäänsä ole pääsyä pankkipalveluihin.

DeFi mahdollistaa rahoituspalvelut esimerkiksi ihmisille, joilla ei ole sosiaaliturvanumeroa tai henkilöllisyystodistusta, koska tunnistautumista ei tarvitse tehdä. Toisaalta kuluttajan on ensin hankittava kryptovaluuttoja käyttääkseen hajautettuja rahoituspalveluja, ja keskitetyt kryptovaluuttojen välityspalvelut vaativat ainakin jonkin tasoisen tunnistautumisen.

4.3 Tehokkuus ja skaalautuvuus

Kolmansien osapuolten puuttuminen hajautetuista rahoituspalveluista mahdollistaa tehokkaammat palvelut. Hajautetuissa palveluissa älysopimukset korvaavat perinteisten välittäjien roolin, jolloin transaktiot toteutuvat automaattisesti ja vastapuoleen liittyvä luottoriski katoaa. Tämä luottamuksen tarpeen väheneminen johtaa myös sääntelyn tarpeen vähenemiseen, mikä myös osaltaan laskee transaktiokustannuksia ja tekee palveluista tehokkaampia. (Schaer, 2021.) DeFi ratkaisuissa luottamuksen tarve on korvattu automatisoidulla hajautetulla lohkoketjulla, mutta toisaalta käyttäjän on luotettava teknologiaan, johon hajautus ja palveluiden toiminta perustuvat. Tähän teknologiaan kytkeytyvät vahvasti myös DeFin monet ongelmat.

Lohkoketjuteknologian mahdollistama hajautus ja turvallisuus tulee usein skaalautuvuuden kustannuksella. Skaalautuvuudella tarkoitetaan lohkoketjun kykyä kasvattaa lohkoketjussa tapahtuvien transaktioiden volyymiä ilman toiminnan häiriintymistä. Yksi suurimmista kryptovaluuttojen kohtaamasta kritiikistä liittyykin juuri niiden valtavaan sähkönkulutukseen, ruuhkautumiseen ja huonoon skaalautuvuuteen. Ethereumin ja muiden

lohkoketjujen louhintaan vaadittavat valtava sähkönkulutus on ollut kritiikin kohteena etenkin sen negatiivisten ympäristövaikutusten takia.

Ruuhkien aikaan nousevat transaktiokustannukset ja transaktioiden vahvistamisajat haittaavat DeFi käyttäjiä ja suosivat varakkaampia käyttäjiä, joilla on mahdollisuus suorittaa suuria transaktioita (Schaer, 2021). Transaktiokustannuksen suuruuteen ei vaikuta transaktion suuruus, joten suhteelliset kulut ovat sitä pienemmät mitä suuremmasta transaktiosta on kyse.

Ethereumin käyttämän PoW konsensusalgoritmin raskaudesta johtuen sen skaalautuvuus on melko rajattu. Siispä Ethereumissa toimivien rahoitussovellusten käytön laajeneminen yleiseen käyttöön maailmassa ei olisi edes mahdollista tällä hetkellä. Ethereum on kuitenkin siirtymässä nk. Ethereum 2.0 versioon, jonka suurin eroavaisuus vanhaan on konsensusalgoritmin vaihtuminen PoW-algoritmista huomattavasti kevyempään PoS-algoritmiin. Ethereum 2.0 transformaation tärkein tarkoitus onkin tehdä Ethereumista paremmin skaalautuva sekä laskea transaktiokustannuksia ruuhkautumisen vähenemisen myötä.

4.4 Yhteensopivuus ja avoimuus

Saman lohkoketjualustan älysopimukset, protokollat ja sovellukset ovat keskenään täysin yhteensopivia, jolloin tiedon ja varojen siirtäminen niiden välillä on vaivatonta. Tämä yhdistettynä älysopimusten lähdekoodin avoimuuteen mahdollistaa protokollien ja sovellusten vapaan yhdistelyn ja kehittämisen kenen tahansa toimesta. Tämän ennen näkemättömän joustavuuden ja yhteensopivuuden ansiosta hajautetut rahoituspalvelut voivat kehittyä ja laajentua perinteisiä rahoituspalveluja nopeammin. Hajautettu lohkoketjuympäristö mahdollistaa myös täysin uudenlaisten rahoituspalveluiden kehittämisen. Toisaalta lähdekoodin avoimuus tuo mukanaan myös ongelmia kilpailun kannalta.

Chohan (2021) pohtii artikkelissaan, että millä avoimen lähdekoodin markkinoilla kilpaillaan, kun kuka tahansa voi kopioida kehitetyn sovelluksen koodin. Chohan näkee kilpailutekijöinä volyymin ja markkinoinnin, mutta ongelmana on varojen siirtely kilpailevien alustojen välillä ilman todellisen kilpailua arbitraasi- ja manipulointiliikkeinä. Hän mainitsee tässä yhteydessä myös DeFi maailmassa valitettavan yleiset Ponzi-huijaukset,

joissa huijari voi luoda huijausprojektilleen tekaistua volyymia houkutellakseen sijoittajia. DeFi ympäristössä tapahtuviin huijauksiin liittyy vahvasti myös sääntelyn ja valvonnan puute sekä projektien suunnittelijoiden anonymiteetti. (Chohan, 2021)

Yhteensopivuus toteutuu kuitenkin vain saman lohkoketjun sisällä, eikä eri lohkoketjujen välistä yhteensopivuusongelmaa ole vielä ratkaistu (Michalikova & Poliakova, 2021). Michalikova ja Poliakova näkevät yhden dominoivan alustan mahdollisena ratkaisuna tähän ongelmaan, kun valtaosa sovelluksista toimisivat samassa lohkoketjussa. Toistaiseksi Ethereum on toiminut tällaisena dominoivana alustana ja edelleen selkeä enemmistö hajautetuista sovelluksista on rakennettu juuri Ethereum-lohkoketjuun. Nähtäväksi jää onnistuuko Ethereum säilyttämään valta-asemansa kilpailun kiristyessä vai hajautuuko DeFi selkeämmin eri alustoille.

4.5 Tekniset riskit

Älysopimusten toiminta pohjautuu koodiin, jossa voi tietysti esiintyä virheitä. Älysopimuksia hyödyntävien protokollien ja näitä hyödyntävien sovellusten tekninen sidonnaisuus nähdään riskinä juuri mahdollisten koodissa esiintyvien virheiden takia. Virheet koodissa voivat mahdollisesti johtaa kaikkien älysopimusta hyödyntävien protokollien ja edelleen näitä hyödyntävien sovellusten vaarantumiseen. Haavoittuvuudet älysopimuksessa voivat johtaa kaikkien sitä hyödyntävien sovellusten toimintahäiriöihin tai altistaa ne hyökkäyksille, jolloin älysopimuksiin talletetut varat ovat vaarassa (Schaer, 2021). Hajautetun rahoituksen kerroksittainen rakenne sovellusten keskinäisin sidonnaisuuksine sisältää siis hyötyjensä lisäksi myös riskin koko järjestelmän kattaviin häiriöihin.

4.6 Hallinnolliset ongelmat

Lohkoketjuun kehitettyjen protokollien ja sovellusten hallinnoimiseen liittyy monia ongelmia. Moniin sovelluksiin ja protokolliin on sisällytetty järjestelmänvalvojan avain, joka on yleensä kyseisen projektin kehittäneen ryhmän hallussa. Avaimella pystytään tarvittaessa päivittämään sovellusta ohjaavien älysopimusten toimintaa tai hätätapauksissa

sulkemaan koko sovelluksen toiminta. (Schaer, 2021.) Ilman tämän tyyppisiä avaimia sovelluksia ei pystyisi jälkikäteen kehittämään tai korjaamaan niissä ilmenneitä vikoja.

Avainten olemassaolo itsessään kuitenkin osittain kumoaa hajautuksen, koska avaimen ansiosta valta sovelluksen hallinnoimiseen on tiettyjen henkilöiden hallussa. Avaimet myös heikentävät sovellusten turvallisuutta, koska avainten joutuessa rikollisten käsiin vaarantuvat sovelluksessa olevat varat. Toisaalta sovelluksen kehittäjilläkin voi olla taloudellisia intressejä käyttää avaimen tuomaa valtaa väärin eivätkä kehittäjien henkilöllisyydet monesti ole edes tiedossa. Käyttäjien on siis avaimia hyödyntävien sovellusten tapauksessa monesti luotettava rajalliseen määrään tuntemattomiin ihmisiin, mikä on täysi vastakohta hajautettujen rahoituspalveluiden tärkeimmälle ominaisuudelle eli vallan hajauttamiselle.

Riskien pienentämiseksi on kehitelty aikalukko, joka määrittelee tietyn vähimmäisajan implementoidun muutoksen toteutumiselle, jonka aikana tehty muutos voidaan vielä peruuttaa. Monesti käytetään myös ”multisig” mallia, joka vaatiii useamman avaimen omistajan hyväksynnän toteutettavalle muutokselle. (Schaer, 2021.) Näin yksittäinen henkilö ei pysty käyttämään valtaansa väärin ja vilpilliset muutokset ehditään huomaamaan ja peruuttamaan aikalukon aikana.

Jotkin projektit hyödyntävät vaihtoehtoisesti hallintotokeneita, jolloin muutoksista päätetään äänestysperiaatteella hallintotokeneiden omistusosuuksien mukaisesti. Kuitenkin myös hallintotokeneiden tapauksessa valta kasautuu usein pienelle ryhmälle ihmisiä. Vaikka aluksi joukkorahoituksen yhteydessä hallintotokenit jakautuisivatkin melko tasaisesti, kasaantuvat ne yleensä lopulta pienelle ryhmälle. (Schaer, 2021.)

4.7 Sääntely

Kryptovaluuttojen ja niitä käyttävien hajautettujen rahoituspalveluiden sääntelystä on käyty keskustelua koko niiden olemassaolon ajan. Toistaiseksi mitään globaaleja säännöksiä ei kryptovaluuttoihin liittyen ole asetettu, vaan sääntely on pitkälti kansallista ja vaihtelee maittain aina kryptovaluuttatransaktioiden kieltämisestä sääntelyn puuttumiseen kokonaan. Tämä sääntelyn vähäisyys on houkutellut hajautetun rahoituksen piiriin paljon rikollista toimintaa, kuten rahanpesua ja terrorismin rahoitusta. (Salami, 2021.)

Sääntelyn vähäisyys on myös osaltaan mahdollistanut perinteisiä rahoitusmarkkinoita pienemmät transaktiokustannukset hajautetun rahoituksen piirissä (Schaer, 2021).

Hajautettujen rahoituspalveluiden ei tarvitse täyttää AML (anti-money laundering, suom. rahanpesun esto) ja KYC (know your customer, suom. tunne asiakkaasi) vaatimuksia, joita kaikkien keskitettyjen rahoitusinstituutioiden on noudatettava (Salami, 2021). Hajautettuja rahoituspalveluita voi yleensä käyttää kuka tahansa ilman minkään näköistä tunnistautumista, mikä tekee rikollisesta toiminnasta paljon helpompaa verrattuna perinteisiin rahoituspalveluihin. Tähän mennessä toteutetut kryptovaluuttoihin kohdistuvat säännökset liittyvät monesti juuri AML ja KYC vaatimuksiin. Esimerkiksi EU:n alueella tuli voimaan direktiivi tammikuussa 2020, joka vaatii kaikkien keskitettyjen kryptopörssien ja lompakkotarjoajien täyttämään AML ja KYC vaatimukset eli niiden tulee tunnistaa jokainen asiakas sekä vahtia ja estää rahanpesua palveluissaan (Salami, 2021).

Edellä mainittu sääntely liittyy lähinnä keskitettyihin toimijoihin DeFi-järjestelmässä. Hyvin hajautettuihin protokolliin ja niitä hyödyntäviin sovelluksiin esimerkiksi KYC vaatimusten lisääminen jälkikäteen olisi hyvin vaikeaa, koska hallinnolliset oikeudet voivat olla hajautettu hallintotokeneilla suurelle joukolle ihmisiä, jotka kaikki eivät välttämättä kannata KYC vaatimusten implementoimista palveluun (Salami, 2021).

Vastuullisten tahojen määrittely on erityisen vaikeaa hajautetun rahoituksen tapauksessa. Ketä voidaan pitää vastuullisena, jos palvelu toimii täysin itsenäisesti toteutuvien koodiin perustuvien älysopimusten avulla, joita kukaan ei pääse muokkaamaan tai edes sulkemaan? Muutamia tapauksia on tullut ilmi, joissa käyttäjät ovat menettäneet varansa älysopimuksen koodissa olleen virheen takia (Salami, 2020). Pitäisikö tällaisessa tapauksessa pitää vastuullisena älysopimuksen koodin kirjottanutta vai onko vastuu käyttäjällä? Käyttäjällä on ollut saatavilla koko älysopimusta ohjaava koodi, jonka hän olisi voinut itsekin tarkastaa, mutta toisaalta suurimmalla osalla ei ole edes osaamista lukea koodia, saati aikaa tarkastaa sitä. Älysopimusten ja hajautettujen sovellusten kehittäjätkin ovat monesti anonyymejä, joten myöskään heidän tunnistamisensa ei välttämättä onnistuisi.

Älysopimusten ja niitä hyödyntävien hajautettujen sovellusten kontrolloimattomuus on myös suuri haaste sääntelyn ja valvonnan kannalta. Salami (2020) pohtii artikkelissaan, että jos säätelijä ei pysty tarvittaessa edes sulkemaan sovellusta ohjaavaa koodia, niin herää kysymys kuinka tehokasta sääntely voi todellisuudessa olla. Huijausten ja muun

rikollisen toiminnan suuri määrä hajautetun rahoituksen piirissä osoittaa, että sääntelyä todella tarvitaan, mutta sen toteutus on edelleen suuri kysymysmerkki.

4.8 Käytännöllisyys

Tehokkuudesta ja saatavuudesta huolimatta hajautettu rahoitus ei ole kuluttajan kannalta välttämättä kovin käytännöllistä. Kuluttajan on ensin vaihdettava fiat-valuuttaansa kryptovaluuttoihin keskitetyn kryptovälittäjän kautta. Kun kuluttaja haluaa ostaa jotakin kryptovaroillaan, esimerkiksi ottamallaan lainalla, tulee hänen todennäköisesti vaihtaa kryptovaransa takaisin fiat-rahaksi, koska kryptovaluutat eivät vielä toistaiseksi ole yleisesti hyväksytty maksuväline.

Kryptovaluuttojen hyväksyminen maksuvaluuttana on kuitenkin yleistymään päin ja esimerkiksi monissa verkkokaupoissa on jo mahdollista maksaa kryptovaluutoilla. El Salvador teki ensimmäisenä maana maailmassa päätöksen ottaa bitcoin viralliseksi maksuvälineeksi, mutta todellisuudessa virallisesta asemasta huolimatta bitcoineilla ei pysty maksamaan juuri missään El Salvadorissakaan (Yle, 2022).

5 YHTEENVETO

5.1 Yhteenveto ja johtopäätökset

Tämän tutkielman tavoitteena oli tutkia, kuinka hajautetut rahoituspalvelut toimivat sekä mitä hyötyjä ja ongelmia niihin liittyy. Tarkastelu rajattiin koskemaan Ethereum-alustaa sen vahvasta asemasta johtuen. Työ toteutettiin kirjallisuuskatsauksena hyödyntäen mahdollisimman tuoreita lähteitä aiheesta.

Automatisointi on ollut jo vuosikymmeniä rahoitusalalla kasvamaan päin. Monet prosessit, kuten luottotarkastukset ja arvopaperikauppa, ovat jo täysin automatisoituja. FinTech on uusi finanssialan aalto, jolla tarkoitetaan finanssiteknologiaa, jonka avulla saadaan tuotettua tehokkaampia rahoituspalveluita asiakkaille matalammilla transaktiokustannuksilla. Nämä teknologiset ratkaisut liittyvät monesti juuri automatisointiin ja välikäsien minimoimiseen. FinTech ei ole kuitenkaan syrjäyttänyt perinteisiä finanssitoimijoita eikä ole onnistunut poistamaan välikäsiä kokonaan palveluista (Chen & Bellavitis, 2020). Lohkoketjuteknologiaan pohjautuva hajautettu rahoitus (DeFi) mahdollisti rahoituspalveluiden järjestämisen täysin ilman välikäsiä. Vaikka hajautetut rahoituspalvelut eivät toimi perinteisillä rahoitusmarkkinoilla, voidaan ne silti nähdä osana FinTech ilmiötä tai sen jatkumona, jossa automatisaatio on viety äärimmilleen.

Lohkoketjuteknologia on hyvin oleellinen käsite, kun puhutaan hajautetusta rahoituksesta. Lohkoketjut voidaan jakaa ominaisuuksiensa mukaan erityyppisiin lohkoketjuihin, kuten julkisiin ja yksisiin. Tekniset ominaisuudet määräävät lohkoketjun ja sen päälle rakennettujen hajautettujen rahoitussovellusten mahdollisen hajautuksen tason. Ethereum on julkinen ja täysin hajautettu lohkoketju, jonka päälle on mahdollista rakentaa täysin hajautettuja rahoitussovelluksia. Kuitenkin monet Ethereumissa toimivat rahoitussovellukset pitävät sisällään myös keskitettyjä osia, kuten oraakkeleita, joiden avulla sovellukseen saadaan tietoa lohkoketjuympäristön ulkopuolelta. Myös rajapinnalla hajautetun rahoituksen ja perinteisen keskitetyn rahoitusjärjestelmän välillä toimii keskitettyjä toimijoita, joita tarvitaan, kun fiat-rahalla ostetaan kryptovaluuttoja tai kryptovaluutoilla fiat-rahaa.

Sovelluksen käyttämä hallintoratkaisu vaikuttaa paljon sovelluksen todelliseen hajautuksen tasoon. Vaihtoehdoista ehkä parhaan hajautuksen mahdollistaa hallintotokenit, joiden avulla hallintovalta saadaan ainakin teoriassa hajautettua suurelle joukolle toimijoita. Täydellinen hajautus olisi käytännössä mahdollista vain jättämällä sovelluksen muuttamismahdollisuudet täysin pois, mutta se ei ole järkevää esimerkiksi koodiin mahdollisesti jääneiden virheiden tai lohkoketjualustan muutosten takia.

Kirjallisuuden perusteella hajautetun rahoituksen keskeisimmiksi hyödyiksi nousivat läpinäkyvyys, tehokkuus, yhteensopivuus sekä saatavuus. Hajautettu rahoitus mahdollistaa entistä halvemmat transaktiot, läpinäkyvämmän toiminnan ja pankkipalvelut kaikille maailman ihmisille ilman tunnistautumista. Samassa lohkoketjussa toimivien hajautettujen rahoitussovellusten yhteensopivuus ja avoimuus mahdollistavat ennennäkemättömän joustavan ja avoimen rahoitussuunnittelun sekä laajenevat mahdollisuudet rahoituspalveluiden kehittämiseen (Schaer, 2021).

Kirjallisuudessa toistuivat myös monet hajautettuun rahoitukseen liittyvät ongelmat ja riskit. Suurimpina teknisinä ongelmina pidettiin heikkoa skaalautuvuutta ja lohkoketjun ruuhkautumista. Myös mahdolliset tahalliset tai tahattomat virheet älysopimusten koodissa ovat ongelma, johon kaivataan ratkaisua. Protokollien ja sovellusten hallintoon liittyviin ongelmiin on jo kehitelty muutamia ratkaisumalleja, mutta edelleen hallinto-oikeuksiinkin liittyy suurta epävarmuutta.

Sääntelyyn liittyvä epävarmuus on mahdollisesti jopa suurin heikkous hajautetulle rahoitukselle. Sääntelyn puuttuminen lisää rikollista toimintaa, kuten huijauksia ja rahanpesua hajautetun rahoituksen piirissä. Sääntelyä ja valvontaa kaivattaisiin lisää, mutta sen toteutukseen liittyy monia ratkaisemattomia ongelmia.

Kokonaisuudessaan tutkielman perusteella voidaan todeta, että hajautettu rahoitus ei vielä haasta perinteisiä finanssipalveluita monien ratkaisemattomien ongelmien, kuten sääntelyyn liittyvän epävarmuuden takia. Myös tekniset riskit ja käytännöllisyyteen liittyvät ongelmat kertovat, ettei hajautettu rahoitus ole vielä valmis korvaamaan keskitettyjä rahoitusinstituutioita. Moniin teknisiin ongelmiin, kuten skaalautuvuuteen on kuitenkin jo kehitteillä ratkaisuja. Toistaiseksi hajautetuista rahoituspalveluista on todellista hyötyä lähinnä köyhissä maissa asuville, joilla ei ole pääsyä perinteisiin pankkipalveluihin.

Voidaan kuitenkin todeta, että hajautetun rahoituksen potentiaali on suuri ja ala kehittyy valtavalla vauhdilla eteenpäin. Kehitys on vielä hyvin varhaisessa vaiheessa, mutta näen, että hajautettu rahoitus voi tulevaisuudessa haastaa perinteisiä finanssipalveluita. Keskuspankkien kilpajuoksu digitaalisen keskuspankkirahan kehittämiseksi kertoo siitä, että keskitetytkin finanssitoimijat ymmärtävät hajautetun rahoituksen potentiaalin ja haluavat vastata kilpailuun (Scharnowski, 2022).

5.2 Rajoitteet ja jatkotutkimusmahdollisuudet

Tutkimusta tarkasteltaessa on tärkeää huomioida, että tutkimuskohteena oli koko hajautetun rahoituksen ilmiö, joten näinkin lyhyessä tutkielmassa ei kovin syvälle aiheeseen päästä. Aihetta voisi lähestyä tarkemmin rajatusta näkökulmasta esimerkiksi keskittyen pelkästään hajautettuun rahoitukseen liittyvän sääntelyn nykytilaan ja tulevaisuuden odotuksiin.

Hajautettu rahoitus ilmiönä on hyvin tuore ja jatkuvassa muutoksessa, joten kaikki tutkielmassa käsitellyt asiat eivät välttämättä ole täysin ajan tasalla ja ovat voineet jo muuttua. Monet tutkielmassa käsiteltävät asiat todennäköisesti muuttuvat merkittävästikin lähitulevaisuudessa, mutta tutkielman tavoitteena olikin kuvat juuri tämän hetken näkemyksiä ilmiöstä ja sen tilanteesta. Aihetta voisi mahdollisesti tutkia myöhemmin samasta näkökulmasta ja arvioida, miten ilmiö on kehittynyt ajan kuluessa.

Kryptovaluutat ovat jälleen osoittaneet taipumuksensa nopeisiin muutoksiin jatkuvasti kehittävänä alana, sillä vain hieman ennen tämän tutkielman julkaisua Ethereum otti seuraavan askeleensa kohti Ethereum 2.0 versiota. Ethereum siirtyi 15. syyskuuta käyttämään kevyempää proof-of-stake konsensusalgoritmia proof-of-work algoritmin sijasta. Siirtyminen vaikuttaa ainakin toistaiseksi onnistuneen ilman ongelmia. Uudistuksen myötä Ethereumin louhinta tuli päätökseensä, jonka ansiosta Ethereumin sähkönkulutus tippui vain murto-osaan aikaisemmasta. Päivitystä pidetään yleisesti historian merkittävimpänä uudistuksena kryptovaluuttakentällä.

LÄHDELUETTELO

Bamakan, S.M.H., Motavali, A., & Bondarti, A.B. (2020). A survey of blockchain consensus algorithms performance evaluation. Expert Systems With Applications, 154. https://doi.org/10.1016/j.eswa.2020.113385

Bentov, Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies Without Proof of Work. FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, FC 2016, 9604, 142–157. https://doi.org/10.1007/978-3-662-53357-4_10

Bouraga, S. (2021). A taxonomy of blockchain consensus protocols: A survey and classification framework. Expert Systems with Applications, 168, 114384–. https://doi.org/10.1016/j.eswa.2020.114384

Cambridge Centre for Alternative Finance. (2022). Cambridge Bitcoin Electricity Consumption Index. [Viitattu 28.08.2022] https://ccaf.io/cbeci/index

Catalini, C., de Gortari, A. & Shah, N. (2021). Some Simple Economics of Stablecoins. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3985699

Chen, Y. & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e151. https://doi.org/10.1016/j.jbvi.2019.e00151

Chohan, U.W. (2021). Decentralized Finance (DeFi): An Emergent Alternative Financial Architecture. Critical Blockchain Research Initiative (CBRI) Working Papers. http://dx.doi.org/10.2139/ssrn.3791921

Crystal. (2021). The 10 Biggest Crypto Exchange Hacks In History. [Viitattu 28.08.2022] https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/

DeFi Pulse. (2022a). The DeFi List [Viitattu 28.08.2022] https://www.defipulse.com/defi-list

DeFi Pulse. (2022b). DeFi Pulse [Viitattu 28.08.2022] https://www.defipulse.com/

Eklund, J. (2022). Tuhannet sijoittajat menettivät rahansa – Miten Terran Luna ja UST romahtivat? [Viitattu 28.08.2022] https://coinmotion.com/fi/terran-luna-ja-ust-romahtivat/

Ethereum. (2022a) Upgrades. [Viitattu 28.08.2022] https://ethereum.org/en/upgrades/

Ethereum. (2022b) Non-fungible tokens (NFT) [Viitattu 28.08.2022] https://ethereum.org/en/nft/

Frajtova Michalikova, K. & Poliakova, A. (2021). Decentralized finance. SHS Web of Conferences, 129, 3008. https://doi.org/10.1051/shsconf/202112903008

Freni, Ferro, E., & Moncada, R. (2020). Tokenization and Blockchain Tokens Classification: a morphological framework. 2020 IEEE Symposium on Computers and Communications (ISCC), 2020-, 1–6. https://doi.org/10.1109/ISCC50000.2020.9219709

George, B. (2022). Why TVL Matters in DeFi: Total Value Locked Explained. [Viitattu 28.08.2022] https://www.coindesk.com/learn/why-tvl-matters-in-defi-total-value-locked-explained/

Guadamuz, A. (2019). All watched over by machines of loving grace: A critical look at smart contracts. The Computer Law and Security Report, 35(6), 105338–. https://doi.org/10.1016/j.clsr.2019.105338

Haber, S. & Stornetta, W.S. (1991) How to time-stamp a digital document. J. Cryptology 3, 99–111. https://doi.org/10.1007/BF00196791

Hassani, Huang, X., & Silva, E. S. (2019). Fusing Big Data, Blockchain and Cryptocurrency: Their Individual and Combined Importance in the Digital Economy. Springer International Publishing AG. https://doi.org/10.1007/978-3-030-31391-3

Hazari, & Mahmoud, Q. H. (2019). Comparative evaluation of consensus mechanisms in cryptocurrencies. Internet Technology Letters, 2(3), e100–. https://doi.org/10.1002/itl2.100

Hirsh, S. & Alman, S. (2019). Blockchain. American Library Association.

Hyperledger Foundation. (2022). Hyperledger Fabric [Viitattu 28.08.2022] https://www.hyperledger.org/use/fabric

Jan, H. (2018). Näin pidät bitcoinisi turvassa! Opas kryptolompakkojen maailmaan. [Viitattu 28.08.2022] https://coinweb.fi/nain-pidat-bitcoinisi-turvassa/

Jo, Hu, K., Yu, R., Sun, L., Conti, M., & Du, Q. (2020). Private Blockchain in Industrial IoT. IEEE Network, 34(5), 76–77. https://doi.org/10.1109/MNET.2020.9199796

Johansson, P., Eerola, M., Innanen, A., Viitala, J., & Alasaarela, M. (2019). Lohkoketju: tiekartta päättäjille. Alma Talent Oy.

Kuhn, D. (2021). Bitcoin’s Lost Coins Are Worth the Price. [Viitattu 28.08.2022] https://www.coindesk.com/tech/2021/12/08/bitcoins-lost-coins-are-worth-the-price/

Lee, D. (2015). Handbook of digital currency : bitcoin, innovation, financial instruments, and big data. Academic Press.

Masiak, C., Block, J. H., Masiak, T., Neuenkirch, M. & Pielen, K. N. (2019). Initial coin offerings (ICOs): market cycles and relationship with bitcoin and ether. Small Business Economics, 55(4), 1113–1130. https://doi.org/10.1007/s11187-019-00176-3

Morabito, V. (2017) Business Innovation Through Blockchain. Springer International Publishing

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

Nguyen, & Kim, K. (2018). A survey about consensus algorithms used in Blockchain. Journal of Information Processing Systems, 14(1), 101–128. https://doi.org/10.3745/JIPS.01.0024

Ossinger, J. (2022). Ethereum's Dominance in DeFi Is 'Far From Given,' JPMorgan Says. [Viitattu 28.08.2022] https://www.bloomberg.com/news/articles/2022-01-06/ethereum-s-dominance-in-defi-is-far-from-given-jpmorgan-says

Palladino. (2019). Ethereum for Web Developers Learn to Build Web Applications on top of the Ethereum Blockchain (1st ed. 2019.). Apress. https://doi.org/10.1007/978-1-4842-5278-9

Salami, I. (2020). Decentralised Finance: The Case for a Holistic Approach to Regulating the Crypto Industry. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3733647

Salami, I. (2021). Challenges and approaches to regulating decentralized finance. AJIL Unbound, 115, 425–429. https://doi.org/10.1017/aju.2021.66

Schaer, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Review - Federal Reserve Bank of St. Louis, 103(2), 153–174. https://doi.org/10.20955/r.103.153-74

Scharnowski. (2022). Central bank speeches and digital currency competition. Finance Research Letters, 49, 103072–. https://doi.org/10.1016/j.frl.2022.103072

Schueffel, P. (2021). DeFi: Decentralized Finance - An Introduction and Overview. Journal of Innovation Management, 9(3). https://doi.org/10.24840/2183-0606_009.003_0001

Solomon, M. (2019). Ethereum (1st edition). John Wiley and Sons.

Tilastokeskus. (2022). Suomi lukuina – Energia. [Viitattu 28.08.2022] https://www.stat.fi/tup/suoluk/suoluk_energia.html

Viglianisi, Ceccato, M., & Tonella, P. (2020). A federated society of bots for smart contract testing. The Journal of Systems and Software, 168, 110647–. https://doi.org/10.1016/j.jss.2020.110647

Wiśniewska, A. (2018). THE INITIAL COIN OFFERING – CHALLENGES AND OPPORTUNITIES. Copernican Journal of Finance & Accounting, 7(2), 99–110. https://doi.org/10.12775/CJFA.2018.011

Yle. (2022). "Kuin nettikasinoa valtion rahoilla" – El Salvadorin bitcoin-kokeilu on ollut vaarallinen pannukakku [Viitattu 28.08.2022] https://yle.fi/uutiset/3-12273060