Teemu Kupiainen

# ÄLYSOPIMUSTEN JA LOHKOKETJUJEN SOVELTAMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

# TIIVISTELMÄ

Kupiainen, Teemu
Älysopimusten ja lohkoketjujen soveltaminen
Jyväskylä: Jyväskylän yliopisto, 2023, 35 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Taipalus, Toni

Lohkoketjuteknologia on saanut paljon huomiota viime vuosina johtuen sen lupaamasta mahdollisuudesta hajautettuun sekä turvalliseen toimintaan eri liiketoiminnan aloilla tai sovellettuna kryptovaluutoiksi. Älysopimukset mahdollistavat perinteisten sopimusten ohjelmoinnin ja automaation ennennäkemättömällä tavalla, mutta samaan aikaan varsinaisia todellisen maailman käyttötapauksia lohkoketjuille tai älysopimuksille on ilmestynyt verrattain vähän, jos kyseessä on paradigmaa siirtävä teknologia. Kirjallisuuskatsauksessa selvitettiin millä tavalla lohkoketjuja sekä älysopimuksia on onnistuttu soveltamaan reaalimaailmassa ja onko tällä tavalla kyetty tehostamaan tai parantamaan jo olemassa olevia prosesseja. Tutkielma toteutettiin kuvailevana kirjallisuuskatsauksena tarkoituksena vastata seuraaviin kysymyksiin: mitä älysopimussovelluksia on olemassa rahakejärjestelmien eli kryptovaluuttojen lisäksi ja miten älysopimuksia voidaan käyttää suljetun lohkoketjuympäristön kuten Ethereumin ulkopuolella. Tutkielmassa saatiin selville, että lohkoketjusovelluksia varsinkin toimitusketjujen hallinnalle oli jo olemassa sekä tämä näyttää olevan yksi lupaavimmista käyttökohteista teknologialle. Suurimmat esteet löytyivät eri lohkoketjujen yhteentoimivuuden, standardoinnin puutteen sekä tiedon siirron osalta. Tiedonsiirtoa luotettavasti ulkomaailmasta lohkoketjuille voidaan pitää suurimpana näistä esteistä. Ennen kuin oraakkeliongelmalle on hyvä ratkaisu, älysopimusten hyödyntäminen reaalimaailmassa on vähintäänkin vaikeaa. Tulokset osoittivat, että älysopimukset ja lohkoketjut teknologiana mahdollistavat liiketoiminnan tehostamista automaatiolla sekä avoimempaa kanssakäymistä eri sidosryhmien välillä. Luottamuspohjaisten järjestelmien korvaaminen älysopimusten luottamuksettomuudella, joka taataan kryptografisesti, mahdollisesti vähentäisi liiketoiminnan kitkaa.

Asiasanat: lohkoketju, älysopimus, kryptovaluutta, lohkoketjusovellus, oraakkeliongelma

# ABSTRACT

Kupiainen, Teemu
Smart contract and blockchain applications
Jyväskylä: University of Jyväskylä, 2023, 35 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Taipalus, Toni

Blockchain technology has garnered significant attention in recent years due to its potential for enabling decentralized and secure operations across various business sectors and in the context of cryptocurrencies. Although smart contracts can facilitate the programming and automation of traditional contracts in innovative ways, there have been relatively few real-world use cases for blockchains or smart contracts. This bachelor's thesis conducts a literature review to investigate how blockchains and smart contracts have been successfully applied in real-world settings and whether they have streamlined or improved existing processes. The thesis was carried out as a general literature review with the aim of answering the following questions: what smart contract applications exist in addition to monetary systems, i.e., cryptocurrencies, and how can smart contracts be used outside of a closed blockchain environment like Ethereum. The study found that there were already blockchain applications, especially for supply chain management, and this seems to be one of the most promising uses for the technology. The biggest obstacles were found in the interoperability of different blockchains, the lack of standardization, and the transfer of information. Reliable data transfer from the outside world to blockchains can be considered the biggest of these obstacles, and until a good solution is found for the oracle problem, it will be at least difficult to utilize smart contracts in the real world. The results showed that smart contracts and blockchain technology enable the streamlining of business through automation and more open interaction between different stakeholders. Replacing trust-based systems with trustlessness, which is guaranteed cryptographically, could potentially reduce friction in business.

Keywords: blockchain, smart contract, cryptocurrency, blockchain applications, oracle problem

# KUVIOT

# SISÄLLYS

# 1 JOHDANTO

Lohkoketjuteknologia on uudehko teknologia-ala, jota potentiaalistaan huolimatta ei ole sovellettu paljoa reaalimaailmassa. Syitä voi olla useita kuten uusissa teknologioissa ylipäätään: käyttötarkoitusten kohdentaminen, standardointi tai lainsäädännölliset rajoitteet.

Alkuperäinen Bitcoinin tekninen raportti ei vielä mainitse älysopimuksia tai niiden käyttöä lohkoketjukontekstissa, vaikka älysopimukset teoria- sekä toteutustasolla ovat vanhempia kuin Bitcoin ja Bitcoin itsekin pystyy matalan tason skriptikieleen, mutta ei todellisiin älysopimuksiin. Ainoastaan pseudonyymistään tunnetun Satoshi Nakamoton alkuperäinen tarkoitus Bitcoinille oli hajautettu elektroninen rahasysteemi, joka mahdollistaa vertaisverkossa tapahtuvat siirrot, mikä eliminoi välikädet (Nakamoto, 2008). Älysopimuksia ei tässä vaiheessa vielä suunniteltu, vaan tarkoitus oli vain luoda kryptografisesti varmennettu ja turvallinen tapa siirtää arvoa.

Buterinin esittämiä potentiaalisia käyttötarkoituksia älysopimuksille ovat rahakejärjestelmät, rahoitusjohdannaiset, identiteetti- ja luottamusjärjestelmät, digitaalisen informaation hajautettu hallinta, hajautettu autonominen organisaatio ja jatkokehitykseen erilaiset vakuutukset sekä hajautetut tietosyötteet (Buterin, 2014a). Useat näistä vaativat nyky-ymmärryksemme mukaan toimivaa tiedon siirtoa lohkoketjun ulkopuolelta, jotta voimme välttää erilaiset häiriötilat ja väärinkäytökset. Tätä Buterin ei vielä osannut ennakoida vuonna 2014. Lohkoketjuinfrastruktuurin kehittyessä on tullut ilmi useita tapauksia, joissa väärää dataa voidaan käyttää hyödyksi esimerkiksi hajautetussa rahoituksessa protokollan manipulaatioon ja rahallisen hyödyn tavoitteluun. Caldarelli ja Ellul (2021) tuovat esiin useita hyviä esimerkkejä älysopimuksien väärinkäytöstä kuten sybil-hyökkäykset, sisäpiirikauppa ja salamalainojen hyväksikäyttö hintamanipulaatioon. Yleensä näissä tapauksissa ongelmana on ollut joko tiedon saaminen luotettavasti älysopimukselle tai älysopimuksen huonosta suunnittelusta johtuvia heikkouksia on käytetty hyväksi. Koko protokollaa on voitu manipuloida hyökkääjän eduksi tai käyttäjien varojen varastamiseksi.

Älysopimuksia voidaan käyttää tietenkin myös kryptovaluuttojen tai erilaisten rahakejärjestelmien kehittämiseen ja julkaisemiseen, mitkä ovat tällä hetkellä niiden suosituimpia käyttökohteita. Ethereumin luottamuksettomuus ja hajautettu luonne on ideaali ympäristö älysopimusten käyttämiselle (Buterin, 2014a). Ethereum on saavuttanut nykyisen asemansa suurimpana älysopimuksia mahdollistavien lohkoketjujen joukossa ainakin osittain verkostoefektin sekä sen edelläkävijäaseman takia. Kilpailijoita kuten Solana, Cardano, Avalanche tai Hyperledger on ilmaantunut lohkoketjuekosysteemin kypsyessä, mikä on johtanut useiden yhteentoimivuusprotokollien kehittämiseen. Jos lohkoketjuja halutaan käyttää oman suljetun ekosysteeminsä ulkopuolella, on yhteentoimivuus välttämätöntä.

Belchior, Vasconcelos, Guerreiro sekä Correia (2022) tutkivat tätä ja määrittelivät yhteentoimivuuden lohkoketjun kyvyksi vaihtaa tietoa ja hyödykkeitä saumattomasti ilman kolmansien osapuolien apua. Esimerkkeinä näistä yhteentoimivuusprotokollista ovat atomivaihdot eli älysopimuksia hyödyntävät kahden eri lohkoketjun väliset vaihdot kahden osapuolen välillä. Tämän lisäksi sivuketjut eli päälohkoketjun rinnalla toimivat ylimääräiset lohkoketjut, lohkoketjujen ylittävät sillat ja erilaiset yhteentoimivuusalustat kuten Polkadot sekä Cosmos ovat yhteentoimivuusprotokollia. Tutkimuspaperin mukaan lohkoketjujen yhteentoimivuutta on vaikeuttanut standardisoinnin puute, lohkoketjujen välisen kommunikaation monimutkaisuus sekä tarve luottamuksettomille ja turvallisille mekanismeille hyödykkeiden vaihtoon eri lohkoketjujen välillä (Belchior ym., 2022).

Yksi syy, miksi älysopimuksia, lohkoketjuja ja niiden sovellutuksia tulisi tutkia lisää on automaation yleistyminen. Älysopimuksilla on mahdollista automatisoida perinteisiä luottamukseen perustuvia sopimuksia ja täten vähentää mahdollisia välikäsiä, mikä voisi johtaa liiketoiminnassa tapahtuvan kitkan vähenemiseen. Liiketoimintaprosessit ovat hyvin pitkälle optimoituja ja tehokkaita, älysopimuksilla voitaisiin saada kiristettyä lisää tehokkuutta. Tämä yleensä johtaa kustannusten alenemiseen. Lohkoketjuteknologia on potentiaaliltaan samaan aikaan perustavaa laatua oleva teknologia, mutta sillä on myös mahdollisuus muuttaa tämänhetkistä liiketoimintaympäristöä rakentamalla valmiiden toimintaprosessien päälle, syrjäyttäen ne tehottomampina. Rahoituksen osalta tätä on tutkittu arvopaperimarkkinoilla, vakuutuksissa ja ulkomaankaupan rahoituksessa. Osa näistä on yltänyt teoriatasolta käytäntöön, mutta ongelmia on esiintynyt kannattavuuden ja monimutkaisuuden osalta (Wang, Ouyang, Yuan, Ni, Han ja Wang, 2019).

Kandidaatintutkielma on toteutettu kirjallisuuskatsauksena, jonka päällimmäisenä tarkoituksena on selvittää lohkoketjujen ja älysopimusten soveltamista sekä niiden potentiaalia rahakejärjestelmien eli kryptovaluuttojen suljetun ekosysteemin ulkopuolella. Samalla on tarkoitus kartoittaa mahdollisia esiin tulevia ongelmia tai hidasteita lohkoketjuteknologian laajemmalle käyttöönotolle. Tutkielmassa pyritään vastaamaan kahteen päätutkimuskysymykseen ja yhteen lisäkysymykseen, koska kyseinen ongelma on niin tärkeä koko lohkoketjuteknologian käytettävyyden kannalta:

- Mitä älysopimussovelluksia on olemassa rahakejärjestelmien eli kryptovaluuttojen lisäksi?
- Miten älysopimuksia voidaan käyttää suljetun lohkoketjuympäristön kuten Ethereumin ulkopuolella, hyödyntäen reaalimaailman dataa?
    - Mikä on oraakkeliongelma?

Kandidaatintutkielma on toteutettu Salmisen (2011) esittämänä kuvailevana kirjallisuuskatsauksena, joka on yleiskatsaus ilman tiukkoja ja tarkkoja sääntöjä materiaalista. Tällä tavalla tutkittava ilmiö pystytään kuvaamaan laaja-alaisesti sekä luokittelemaan tutkittavan ilmiön ominaisuuksia (Salminen, 2011). Kuvaileva kirjallisuuskatsaus valikoitui tutkielmalle parhaaksi koska lohkoketjuihin ja älysopimuksiin liittyvä vertaisarvioitu tieteellinen kirjallisuus on vielä suhteellisen vähäistä ja hajanaista, vaikka lohkoketjut teknologiana eivät ole enää uusimpia ilmiöitä. Kuvaileva kirjallisuuskatsaus antoi enemmän vapautta lähteiden valinnassa ja tämä helpotti itse tutkimuksen tekemistä merkittävästi.

# 2 LOHKOKETJUJEN JA ÄLYSOPIMUSTEN TERMISTÖÄ

Lohkoketjuihin sekä älysopimuksiin liittyy paljon termistöä, jota ei välttämättä käytetä tämän kontekstin ulkopuolella. Tästä syystä on sopivaa tutustua termistöön tarkemmin ennen kuin siirrytään varsinaisiin sisältökappaleisiin. Luvussa käydään lyhyesti läpi tutkielmassa käytetyt termit ja niiden määritelmät tukeutuen lähdekirjallisuuteen.

## 2.1 Lohkoketju

Lohkoketjulla tarkoitetaan Nakamoton (2008) kuvailemaa hajautettua tietokantaa, joka tallentaa kaikki verkossa tapahtuneet transaktiot. Jokaisella lohkolla on aikaleima ja kryptografinen tiiviste edellisestä lohkosta mikä muodostaa muuttumattoman tallenteen kaikista transaktioista. Itse lohkoketjua ylläpitää hajautettu verkosto solmuja tai noodeja, jotka tarkastavat transaktioita ja lisäävät uusia lohkoja ketjuun käyttäen konsensusmekanismia, joka perustuu työntodisteeseen tai varantotodisteeseen. Työntodisteessa ratkaistaan monimutkaista matemaattista laskentaa. Integriteetin ja riittävän hajautuksen saavuttamiseksi toisistaan riippumattomia solmuja tulisi olla mahdollisimman monta. Hajauttamalla solmukohdat ja käyttämällä työntodistetta konsensusmekanismi on tehty vaikeaksi yhdelle henkilölle tai ryhmälle manipuloida tai ottaa verkosto haltuun, tällä tavalla järjestelmää on vaikea, ellei mahdoton sensuroida tai hyökätä vastaan. Varantotodiste (Proof of Stake) on toinen konsensusmekanismi, jota käytetään lohkoketjuissa varmistamaan turvallinen ja luotettava tapa lisätä uusia lohkoja ketjuun (Nguyen, Hoang, Nguyen, Niyato, Nguyen, Dutkiewicz, 2019). Varantotodisteessa lohkojen lisäämiseen ja vahvistamiseen ei tarvita laskentatehoa toisin kuin työntodisteessa. Varantodisteeseen perustuvissa lohkoketjuissa osallistujat, joita kutsutaan validointipalvelimiksi tai validaattoreiksi asettavat panoksena tietyn määrän kryptovaluuttaa (Nguyen ym., 2019).

## 2.2 Älysopimus ja rahake

Älysopimusta terminä on käyttänyt Nick Szabo jo vuonna 1996 blogikirjoituksessaan "Smart Contracts: Building Blocks for Digital Markets". Kirjoituksessa Szabo ehdottaa, että älykkäillä sopimuksilla monet perinteiset sopimuskohdat voidaan sisällyttää laitteistoihin ja ohjelmistoihin tavalla, että sopimuksen rikkominen olisi kalliimpaa kuin noudattaminen (Szabo, 1996). Älysopimuksella tarkoitetaan tapahtumavetoista ohjelmoitavaa sopimusta tai tietokone-ohjelmaa, joka toteutetaan ja valvotaan kaikkien osallistujien toimesta vertaisverkossa (Hu ym., 2021). Ethereumin käynnistys vuonna 2015 mahdollisti ensimmäisen kerran älysopimusten käytön Turing-täydellisessä lohkoketjussa eli älysopimuksia voi ohjelmoida tekemään samanlaista laskentaa kuin muutkin tietokoneohjelmat (Buterin, 2014a).

Kryptovaluutta on Chohanin (2017) mukaan digitaalinen omaisuus, joka on suunniteltu toimimaan vaihdon välineenä ja perustuu kryptografialla turvattuun transaktiovirtaan ja lisäyksiköiden luontiin. Rahake (token) on käytännössä kryptovaluutta, jota lisäksi käytetään johonkin lohkoketjulla tapahtuvaan toimintaan kuten hallinnointiin tai älysopimusinteraktioihin.

## 2.3 Oraakkeli ja luottamuksettomuus

Caldarellin (2020) määritelmän mukaan oraakkeli voi olla mikä tahansa asia tai keino, jolla ulkoista tietoa voidaan tuoda lohkoketjulle älysopimusten käytettäväksi ja esimerkkeinä tästä ovat sovellukset, anturit, ihmiset ja tekoäly. Oraakkeliongelmalla tarkoitetaan haastetta saada luotettavaa ja turvallista tietoa lohkoketjuympäristöön ja älysopimuksille (Ezzat, Saleh, Abdel-Hamid, 2022). Älysopimukset ovat luonteeltaan anteeksiantamattomia väärän tiedon suhteen koska älysopimukset eivät itsestään kykene varmistamaan tiedon oikeellisuutta. Väärän tiedon syöttäminen älysopimukselle voi johtaa käyttäjälle huonoihin lopputuloksiin kuten rahan menettämiseen.

Luottamuksettomuus lohkoketjukontekstissa on tavallisesti tarkoittanut perinteisen toiminnan luottamukseen perustuvien tapahtumien korvaamista älysopimuksilla tai lohkoketjulla, joissa luottamus taataan kryptografisen prosessin avulla ja täten osapuolten välinen luottamus voidaan eliminoida prosessista. De Filippi, Mannan ja Reijers (2020) artikkelissaan määrittelevät lohkoketjua luottamuksettoman teknologian sijaan luottamuskoneeksi, jolla luottamus taataan. Luottamuksettomuus -sanan käyttö ei ole täysin johdonmukaista lohkoketjukirjallisuudessa, mutta sitä kuitenkin esiintyy paljon joten se on hyvä määritellä.

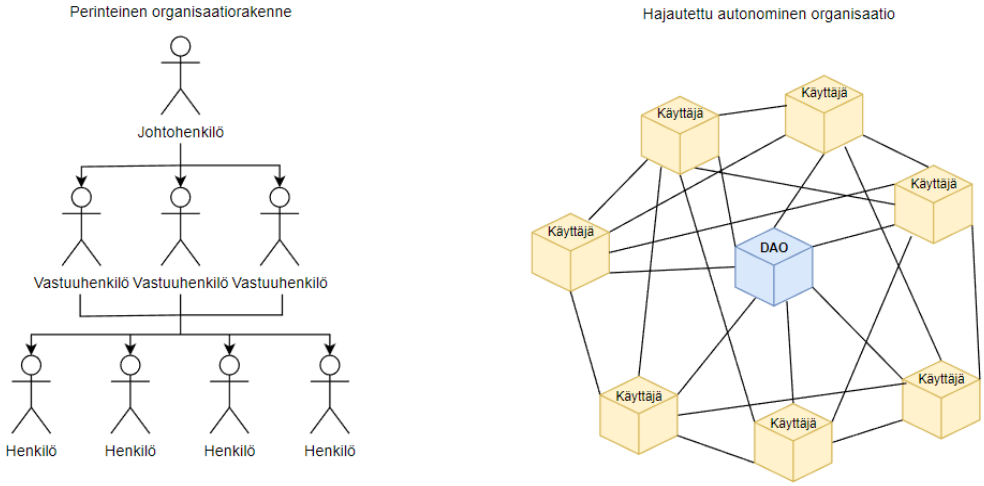
# 3 LOHKOKETJUSOVELLUKSET

Tässä luvussa tarkastellaan erilaisia älysopimuksia hyödyntäviä lohkoketjusovellutuksia. Tutkielman kohteeksi on rajattu sovellutukset, jotka eivät ole pelkkiä rahakejärjestelmiä tai kryptovaluuttoja eli sovelluksella on oltava joku muukin funktio kuin hyödykkeen varastointi ja siirtäminen lohkoketjua hyväksikäyttäen. Hyviä vaihtoehtoja ovat täten rahoitusjohdannaiset, identiteetti- ja luottamusjärjestelmät, digitaalisen informaation hajautettu hallinta, hajautettu autonominen organisaatio, erilaiset vakuutukset, toimitusketjujen hallinta sekä lohkoketjujen hyödyntäminen terveydenhuollossa.

## 3.1 Hajautettu autonominen organisaatio

Decentralized Autonomous Organization (DAO) eli hajautettu autonominen organisaatio on Buterinin (2014) kuvailema älysopimuksilla kirjoitettujen sääntöjen varassa toimiva entiteetti, jota ei kontrolloi mikään yksittäinen auktoriteetti tai taho. Sen sijaan sen jäsenet osallistuvat organisaation toimintaan ja kontrolloivat organisaatiota äänestämällä hajautetun hallintoprosessin avulla (Buterin, 2014b). Buterin on sitä mieltä, että DAO-malli voisi mullistaa perinteisiä organisaatioita tekemällä päätöksenteosta avoimempaa, demokraattisempaa sekä tehokkaampaa resurssien kannalta (Buterin, 2014b). Samalla Buterin kuitenkin tiedostaa, että hajautetut autonomiset organisaatiot ovat heikkoja esimerkiksi kolluusiohyökkäyksille ja muulle manipulaatiolle. Hajautetun autonomisen organisaation piirteisiin kuuluu, että ei ole keskitettyä hallintorakennetta, osallistujat ovat periaatteessa yhdenvertaisia, hallintoprosessiin kuuluu jollain tapaa äänestäminen sekä organisaatio hyödyntää älysopimuksia prosessien toteuttamisvaiheessa. Wang, Ding, Li, Yuan, Ouyang ja Wang (2019) myöntävät, että hajautetulla autonomisella organisaatiolla ei ole yhtä selkeää määritelmää, mutta itse määrittelevät sen sillä tavalla, että DAO on lohkoketjulla toimiva organisaatio, joka toimii itsestään

ilman keskitettyä hallintoa tai johtamishierarkiaa. Tämän lisäksi organisaation kaikki hallinta- sekä operatiiviset säännöt ovat kirjattu lohkoketjuun älysopimusten avulla. Kuviossa 1. havainnollistetaan yksinkertaisen perinteisen organisaation ja hajautetun autonomisen organisaation eroja.
Perinteinen organisaatiorakenne on tavallisesti hyvin hierarkkinen, jossa on




KUVIO 1 Esimerkki perinteisestä organisaatiosta ja hajautetusta autonomisesta organisaatiosta

selvät auktoriteetti- ja johtohahmot, jotka käyttävät valtaa parhaalla näkemällään tavalla ja täten ohjaavat organisaatiota käyttäen hyväksi jotain etukäteen määriteltyä strategiaa. Hajautetut autonomiset organisaatiot eivät tavallisesti noudata tällaista rakennetta, vaan kaikkeen päätöksentekoon tarvitaan jäsenien äänestys ennen kuin mitään muutoksia tehdään (Altaleb & Zoltan, 2022). Altaleb ja Zoltan (2022) kuvailevat miten ääntenlaskenta sekä äänestystuloksen implementaatio tapahtuu ilman kolmansia osapuolia. Äänestäminen tapahtuu usein jotakin rahaketta omistamalla, jolla todistetaan käyttäjän osallistuminen hajautetun organisaation toimintaan ja usein mitä enemmän omistat rahaketta, sitä enemmän äänestysvoimaa käyttäjällä on (Chao ym., 2022). Ethereumin suosion kasvettua kaasumaksut, joilla älysopimuksia toteutetaan, ovat kasvaneet huomattavasti ja älysopimusinteraktiot ovat muuttuneet alkuvaiheiden halvoista, muutaman dollarin interaktioista jopa satoihin dollareihin riippuen älysopimuksen monimutkaisuudesta ja Ethereum-verkon ruuhkasta. Tämä tietenkin luonnollisesti sulkee pois tavalliset käyttäjät hajautettujen organisaatioiden toiminnasta ja vain kryptovaluuttojen varhaiset omaksujat tai jo entuudestaan rikkaat käyttäjät pääsevät oikeasti osallistumaan päätöksentekoon, mikä puolestaan on vastoin demokraattista ja avointa periaatetta.

Hajautetun autonomisen organisaation ideaali suorasta demokratiasta voi silti usein olla toteutettavissa vain ideatasolla, sillä usein päätöksenteko monen eri sidosryhmän, joilla saattaa olla erilaisia tavoitteita tai näkemyksiä tulevaisuudesta, on vähintäänkin haastavaa. Tämä on erityisesti haastavaa, jos

on kyse rahallisista kannustimista. Samanlainen lopputulos huomattiin hajautetuissa organisaatioissa, jossa eri sidosryhmien mahdollisuudet vaikuttaa hallinnointiin, on johtanut eturistiriitoihin ja tehottomampaan päätöksentekoon kuin perinteinen organisaatio olisi mahdollisesti kyennyt (Altaleb & Zoltan, 2022).

### 3.1.1 DAO-hakkerointi ja sen jälkiseuraamukset

Lohkoketjujen muuttamattomuus on osoittautunut myös ongelmalliseksi hajautettujen autonomisten organisaatioiden osalta. Aivan ensimmäinen Ethereumilla toteutettu DAO nimeltään "The DAO" joutui kesäkuussa 2016 hakkerin tai hakkereiden kohteeksi ja DAO:sta siirrettiin 3,5 miljoonaa etheriä arvoltaan noin 50 miljoonaa Yhdysvaltain dollaria toiseen hajautettuun organisaatioon nimeltä childDAO. Teknisesti tarkasteltuna älysopimus toimi kuten se oli ohjelmoitu toimimaan ja hyökkääjä vain käytti hyväkseen haavoittuvuutta älysopimuksessa eli on kiistanalaista voiko tapahtumaa pitää todellisena hakkerointina koska lohkoketjuun ei tunkeuduttu eikä sitä todentavia tietokoneita otettu haltuun (Morrison, Mazey, Wingreen, 2020).

Älysopimuksen suunnitteluvaiheen inhimillisen virheen takia käyttäjät olivat menettäneet miljoonia ja vastaavaa ei olisi tapahtunut perinteisessä pankkimaailmassa, koska pankeilla ja tarvittaessa SWIFT:illä on paljon enemmän kontrollia rahaliikenteestä kuin lohkoketjulla toimivalla organisaatiolla. DAO:n sijoittajat sekä Ethereum Foundation lopulta päätyivät käyttämään hyväksi radikaalia ratkaisua, jossa lohkoketju jaetaan vanhaan lohkoketjuun ja uuteen lohkoketjuun, tälle toimenpiteelle käytetään termiä "hard fork" – vanha lohkoketju ei ole siis enää yhteensopiva uuden kanssa (Morrison ym., 2020). Käyttäjät ja Ethereum Foundation siis siirtyivät sellaiseen versioon Ethereum-lohkoketjusta, jossa hyökkäystä ei ollut tapahtunut ollenkaan ja varat palautuivat käyttäjille (Morrison ym., 2020). Osa Ethereum-verkon käyttäjistä eivät hyväksyneet lohkoketjun perusidean vastaista toimenpidettä, jossa lohkoketjun muuttumattomuutta ja "koodi on laki" -periaatetta sivuutettiin näin pahasti ja täten Ethereum-lohkoketju jakautui kahteen lohkoketjuun; Ethereumiin ja Ethereum Classiciin – Ethereum Classicissa DAO-hyökkäyksen lopputulos on siis eri ja hyökkääjä piti varat, vaikka niiden arvo oli paljon vähemmän kuin alkuperäinen 50-60 miljoonaa Yhdysvaltain dollaria (Morrison ym., 2020).

Lohkoketjun jakaminen älysopimuksen nollaamiseksi on vastoin koko hajautetun autonomisen organisaation perusideaa, missä koodin tulisi olla lakia ja älysopimusten tulisi toteuttaa käyttäjien syötteitä. Tapauksen jälkeen voitiin kyseenalaistaa koko hajautetun organisaation sekä lohkoketjun perusideaa. Muuttumattomuus onkin muuttumattomuutta vain silloin kun tarpeeksi moni käyttäjä on samaa mieltä. Toisaalta kyseinen toimenpide saattoi pelastaa vielä silloin nuoren Ethereumin tulevaisuuden ja sen vakiintumisen yleisimmäksi älysopimusalustaksi.

Vaikeaksi tilanteen tekee myös hajautettujen autonomisten organisaatioiden laillinen asema – oikeassa maailmassa jos varastat toiselta osapuolelta yksipuolista sopimusta hyväksikäyttäen 50 miljoonaa dollaria,

joudut oikeuteen ja todennäköisesti sinut todetaan syylliseksi. DAO:n tilanteessa, jos noudatetaan algoritmista auktoriteettia eli DAO:n älysopimukseen oli kirjoitettu mahdollisuus käyttäjille käyttää sopimusta tällä tavalla ei käyttäjä "lain" mukaan tehnyt mitään väärää vaan kyse on lähinnä epäeettisyydestä. Tässä onkin mielenkiintoisia risteymäkohtia lohkoketjumaailman ja oikean maailman kanssa, koska jos kyseinen käyttäjä olisi tunnistettu, häntä olisi todennäköisesti voitu haastaa oikeuteen riippuen käyttäjän kotimaasta. Saman epäkohdan huomasivat myös Wang ja muut (2019) kun he luettelivat hajautetun autonomisen organisaation implementaation ja käytön vaikeuksia. Näistä kolme tärkeintä nostoa olivat turvallisuus, epäselvä laillinen status ja tekniset rajoitukset (Wang ym., 2019).

### 3.1.2 Erilaisia hajautettuja autonomisia organisaatioita

Kivikkoisesta alkutaipaleesta huolimatta lohkoketjuteknologian kypsyminen on johtanut monenlaisten organisaatioiden syntymiseen. Suurin osa näistä ovat yhteisöjä, jotka osallistuvat jonkinlaiseen lohkoketjuihin liittyvään sijoitustoimintaan, lohkoketjuprojektien rahalliseen tukemiseen tai hajautettuun rahoitukseen. Tässä alaluvussa tutustumme tarkemmin muutamaan organisaatioon ja niiden toimintaan.

Hajautetun rahoituksen esimerkki hajautetusta autonomisesta organisaatiosta on Ethereumilla toimiva MakerDAO, joka aloitti toimintansa vuonna 2017. Arroyo, El Faqir ja Hassan (2020) tutkimusartikkelissaan esittelevät MakerDAO:n yhteisönä, joka hallinnoi Maker Protokollaa, minkä he nimeävät yhdeksi suurimmista hajautetuista sovelluksista (DApp). Maker Protokolla määrittelee vakaavaluutakseen Dai-nimisen valuutan, joka on hajautettu, puolueeton, panttitaattu kryptovaluutta, mikä on sidottu Yhdysvaltain dollariin 1:1 suhteessa (Maker Foundation, 2020). Dai-valuuttaa ei ole suoraan taattu Yhdysvaltain dollareilla, vaan se taataan muilla omaisuuksilla, joita Ethereum-lohkoketju mahdollistaa. Alkuperäisessä Makerin julkaisussa tämä oli vain ether, mutta 2019 alkaen muitakin mahdollisia kryptovaluuttoja voidaan käyttää panttina (Kjaer, di Angelo, Salzer, 2021). Kjaerin, di Angelon ja Salzin (2021) kuvailemat holvit ovat yksi tärkeimmistä osista Makerin ekosysteemiä. Holvit toimivat periaatteella, jossa Dai-valuuttaa lainaavat osapuolet lukitsevat itse päätettävissä olevan määrän valuuttaa vakuudeksi ja saavat vastineeksi tietyn määrän Dai:ta – pantin määrään päättää Makerin hajautettu hallintojärjestelmä. Etherin tapauksessa vakuussuhde on 150 % eli vakuudeksi annetun etherin pitää olla arvoltaan ainakin 1,5 kertaa enemmän kuin saatu Dai (Kjaer, di Angelo, Salzer, 2021). Käyttäjä tämän jälkeen voi käyttää saamaan valuuttaa haluamallaan tavalla, mutta jos annetun pantin arvo laskee liian paljon voi hänen lainapositionsa joutua likvidoiduksi. Tämä on varsinkin kryptovaluutoissa suhteellisen yleinen riski johtuen markkinoiden volatiliteetista. Tällä hetkellä, toisin kuin perinteisessä pankkijärjestelmässä, jossa vähimmäisvarantojärjestelmä mahdollistaa pankille yleensä vähintään 1:10 -vivun tai enemmän, Maker ei ainakaan mahdollista alipantattuja positioita

käyttäjilleen eikä lainanantajan tarvitse luottaa lainaajan lupauksiin likviditeetistä.

Uniswap on automatisoitu markkinatakaajaprotokolla, joka mahdollistaa hajautetun kaupankäynnin eri käyttäjien välillä (Adams, Zinsmeister, Salem, Keefer, Robinson, 2021). Automatisoitu markkinatakaaminen on Hansonin (2003) mukaan logaritmista pisteytystä käyttävä tapa, joka kannustaa osallistujia raportoimaan oikein uskomuksensa eri tapahtumien todennäköisyydestä. Hanson (2003) väittää, että perinteiset markkinatakaamisen menetelmät käyttävät lineaarisia pisteytyssääntöjä, mikä johtaa kiinteään maksuun oikeasta hinta-arvioinnista, mutta tämän tavan käyttäminen voi johtaa markkinamanipulointiin ja epätarkkaan hinnoitteluun (Hanson, 2003).

Uniswap DAO on hajautettu autonominen organisaatio, joka hallinnoi Uniswap-protokollaa. Tämän kyseisen organisaation muodostavat Uniswap-tiimi, sijoittajat ja ylipäätään kaikki, jotka pitävät hallussaan UNI-rahaketta. Käyttäjät voivat tehdä esityksiä siitä, miten protokollaa tulisi kehittää tai mitä uusia ominaisuuksia tulisi jatkokehittää. (Uniswap, 2020) Tämän hallintotavan mahdollinen ongelma tietenkin tavallisen käyttäjän osalta on se, että esityksen aloittaminen vaatii paljon pääomaa tai tukea muilta käyttäjiltä, mutta Uniswap on luonut käyttäjilleen avoimen foorumin, jossa he voivat keskustella esityksistä ja täten argumentoida niiden puolesta tai vastaan.

## 3.2 Toimitusketjujen hallinta

Lohkoketjuteknologiakeskustelussa usein tulee esiin toimitusketjujen hallinta mahdollisena käyttötarkoituksena. Lohkoketjua hyödyntämällä voitaisiin implementoida liiketoiminnan eri osapuolien tarkastelulle avoin ja muuttumaton jatkumo jokaisesta tapahtumasta raaka-aineista valmiiseen tuotteeseen. Tällä tavalla voitaisiin vähentää petoksia sekä epävarmuutta ja täten lisätä luottamusta eri tavarantoimittajien, valmistajien, jakelijoiden sekä kuluttajien välillä. Jäljitettävyyden helpottaminen on yksi selkeimmistä käyttötarkoituksista lohkoketjuille toimitusketjujen hallinnassa. Lohkoketjua ja kestävyyttä tutkiessaan Lund, Jaccheri, Li, Cico ja Bai (2019) tulivat johtopäätökseen, että vaikka toimitusketjujen hallinnan osalta lohkoketjuteknologia on lupaavaa, standardisoinnin puute tekee perinteisistä järjestelmistä siirtymisestä kallista ja riskialtista. Tämän lisäksi ei ole hyvää keinoa ratkaista tuotteiden fyysisen peukaloinnin estämistä.

Risso, Ganga, Filho, de-Santa Eulalia, Chikhi ja Mosconi (2023) kirjallisuuskatsauksessaan tulivat samanlaisiin johtopäätöksiin, jossa lohkoketjuteknologian avulla voidaan parantaa toimitusketjuhallinnan avoimuutta, jäljitettävyyttä sekä turvallisuutta. Heidän mukaansa suurimmat käyttöönoton ongelmat ovat teknisiä, organisatorisia sekä lainsäädännöllisiä. Tekniset ongelmat olivat pääsääntöisesti teknologian monimutkaisuus sekä yhteentoimivuusongelmat eri lohkoketjujärjestelmien välillä. Organisatoriset ongelmat heidän mukaansa olivat tarve yhteistyölle ja luottamukselle

toimitusketjun eri osapuolien kanssa sekä muutosvastaisuus. Lainsäädännölliset ongelmat olivat selkeän lainsäädäntökehyksen sekä standardien puute lohkoketjuille. (Risso ym., 2023)

Sunmola ja Burgess (2022) ehdottavat "transparency by design" -lähestymistapaa, jossa lohkoketjuihin pohjautuvat toimitusketjut varmistavat liiketoimien rehellisyyden ja vähentävät virheiden mahdollisuutta. Tämän lisäksi lohkoketjuintegraatio vihreiden sijoitusstrategioiden voi olla ajamassa eteenpäin kestävien toimitusketjukäytäntöjen kasvattamalla rehellisyyttä liiketoimissa ja varmistamalla, että eri osapuolia kohdellaan yhdenvertaisesti (Li, Ma, Shi ja Zhu, 2022). Lohkoketjun hyödyntämistä hiilijalanjäljen analysointiin ovat tutkineet Shakhbulatov, Arora, Dong ja Rojas-Cessa (2019) ruoan toimitusketjun kontekstissa. He tuovat esiin lisääntyvät huolet ruoantuotannon sekä siirtämisen ympäristövaikutuksista ja esittelevät avoimen sekä jäljitettävissä olevan seurantajärjestelmän ruokatoimitusketjujen hiilidioksidipäästöille. Lohkoketjujärjestelmä mahdollistaa reaaliaikaisen seurannan tuotteiden hiilijalanjäljelle, mikä tuo eri sidosryhmille lisää informaatiota tehdä päätöksiä ja ottaa käyttöön kestävämpiä liiketoimintakeinoja (Shakhbulatov ym., 2019). Esitelty järjestelmä mahdollistaa tiedon avoimen säilömisen ja myöhemmän tarkastelun samalla kuitenkin säilyttäen tarvittaessa osapuolten yksityisyyden, täten kuluttajat tai muut toimitusketjuun osallistuvat kykenevät tekemään paremmin informoituja päätöksiä.

Smartsupply on Sun, Wangin ja Kimin (2018) esittelemä toimitusketjujärjestelmä, jossa yhdistyy liiketoimintojen varmentaminen, tiedonhaku sekä vikasietoisuus tietokantahakuja tehdessä. Heidän mukaansa tällä Ethereum-pohjaisella järjestelmällä voisi havaita väärennöksiä ja samalla hyötyä muuttumattomuudesta ja sen tuomista hyödyistä kirjanpidollisissa toimenpiteissä (Su ym., 2018). Tämänlaisen järjestelmän luonnollinen ongelma on tiedon oikeellisuuden varmistettavuus, sillä oletettavasti suurin osa syötetystä tiedosta tulee vain yhdestä lähteestä, mikä on heikoin linkki hajautuksen osalta.

Arunmozhi, Venkatesh, Arisian, Shi ja Sreedharan (2022) esittelevät autonomisten ajoneuvojen tuotantoketjulle älysopimussovelluskehikon, jolla voidaan tehostaa toimitusketjun hallintaa. Erilaisia älysopimuksia hyödyntäen automatisoidaan ja valvotaan autonomisten ajoneuvojen tuotantovaiheissa. Arunmozhi ja muut esittävät, että näitä käyttämällä voitaisiin tehostaa tuottavuutta, prosessien tehokkuutta, parempaa energiankäyttöä sekä kustannusten hallintaa (Arunmozhi ym., 2022). Viitekehys sisältää keinoja älykkäiden tekniikkojen implementointiin ja testaamiseen ajoneuvojen kokoamisessa, prosessiautomaatiossa, suunnittelutavoissa sekä datalähtöisessä päätöksenteossa. Dataa, jota saadaan eri operaatiovaiheista, mallinnetaan käyttäen siihen soveltuvia koneoppimismalleja, tutkimus esittelee myös uuden MI-indikaattorin tukemaan arvonmuodostusta. Indikaattori auttaa ennustavan analytiikan tulosten seulomisessa. Viitekehystä ja älysopimussovelluksia ajoneuvotuotannon eri vaiheissa testattiin Singaporessa sijaitsevassa yrityksessä, joka tuottaa autonomisia ajoneuvoja Singaporeen ja Kaakkois-Aasian alueelle.

Konseptia testatessa huomattiin 12,48 % vähennys energiahukassa sekä 11,58 % vähennys piilokustannuksissa (Arunmozhi ym., 2022).

Ruoantuotannon toimitusketjuissa lohkoketjun hyödyntäminen on suosittu aihe, sillä ruokahävikin vähentäminen ja ruoan alkuperän varmentaminen olisivat arvokkaita sekä loppuasiakkaille, että eri tuotantoketjun sidosryhmille. Tyypillinen maatalouden tuotantoketju sisältää monta eri sidosryhmää mukaan lukien tuottajat, jalostajat, sertifiointivirastot, vaihtajat, jakelijat, jälleenmyyjät ja lopulta loppukäyttäjät (Cao, Yi, Wan, Hu, Li, Wang, 2022). Heidän tutkimuksessaan identifioidaan kolme tärkeää riskitekijää maatalouden tuotantoketjuissa, joista yksi on rahoitusriski eli rahoittajat voivat kärsiä moraalikadon tai epärehellisen käytöksen tuottamia ongelmia. Toinen riskitekijä on vastapuoliriski eli mahdollisuus, että eri sopimusten vastapuolet eivät täytäkään sopimuksen ehtoja, esimerkiksi maanviljelijälle ei maksetakaan luvattua määrää sadostaan. Kolmas ja viimeinen esiintuotu haaste on kuluttajien luottamuksen puute, mikä johtuu siitä, että kuluttajat eivät kykene varmentamaan myyjän väitteitä tuotteiden laadusta, turvallisuudesta tai kestävyydestä. (Cao ym., 2022) Lohkoketjua voidaan ainakin teoriatasolla hyödyntää jokaiseen näistä ongelmista. Moraalikato vähenee, jos hyvin tehty älysopimus toteuttaa transaktiot eikä rahoittajien tarvitse huolehtia varojensa väärinkäytöksistä. Oikein tehty ja käytetty älysopimus poistaa lähes kokonaan vastapuoliriskin, koska molempien osapuolien mahdollisuus olla noudattamatta sopimusta vähenee huomattavasti, jos sopimus on automatisoitu ja noudattaa sille annettuja reunaehtoja. Lohkoketjun avoimuuden ja muuttumattomuuden takia loppukäyttäjän on myös helppo seurata tuotteidensa alkuperää ja varmistaa, onko myyjän väitteet tuotteesta todenmukaisia, joten luottamusongelmaa ei enää synny ja huonot tekijät karsiutuisivat markkinoilta pois. Mallintaessaan kuluttajakäyttäytymistä Liu, Hua, Kang, Cheng ja Xu (2022) huomasivat, että käyttäjän riskinsieto vaikutti siihen, että kannattaako yrityksen hyödyntää lohkoketjua. Jos kuluttaja oli huolissaan ruoan turvallisuudesta, lohkoketjun hyödyntäminen olisi yleensä tuottanut paremman lopputuloksen kuluttajien sekä tuottajien osalta (Liu ym., 2022).

Perinteisesti ruoantuotannon kestävyysstandardit ovat perustuneet vapaaehtoisuuteen ja kansalaisjärjestöjen toimintaan, mutta Köhler, Bager ja Pizzol (2022) tutkivat lohkoketjuteknologian tehostamien kestävyysstandardien ja vapaaehtoisten kestävyysstandardien synergiaa ja päätyivät lopputulokseen, että suurimmassa osassa tapauksista näitä voitaisiin käyttää yhdessä samaan aikaan. On kehitetty lohkoketjuratkaisuja, joissa sen sijaan, että asiakas näkisi jonkun sertifiointimerkinnän kuten FAIRTRADE, he voisivat skannata QR-koodin. Koodista voisi lukea muuttumattomaan lohkoketjuun kirjatut tiedot tuotteesta ja sen eri vaiheista alkuperämaasta loppukäyttäjälle. Köhler ja muut tosin myöntävät, että näiden mahdollisten synergioiden todentaminen pitkällä aikavälillä on vielä vaikeaa koska monet lohkoketjupohjaiset kestävyysstandardit ovat vielä aikaisessa kehitysvaiheessa. (Köhler ym., 2022) Hun, Huangin ja Qinin (2022) tutkimuksen mukaan lohkoketjuun perustuvan jäljitettävyyssertifikaattimallin ja verkkokauppamallin käyttöönotto pystyy

lisäämään koko tuotantoketjun kokonaistuottoa sekä maanviljelystuotteiden lisäarvoa. Tämän lisäksi molemmat mallit lisäisivät kuluttajaylijäämää, millä voisi olla orgaaniselle maanviljelylle kokonaisuudessaan kasvattava vaikutus (Hu ym., 2022).

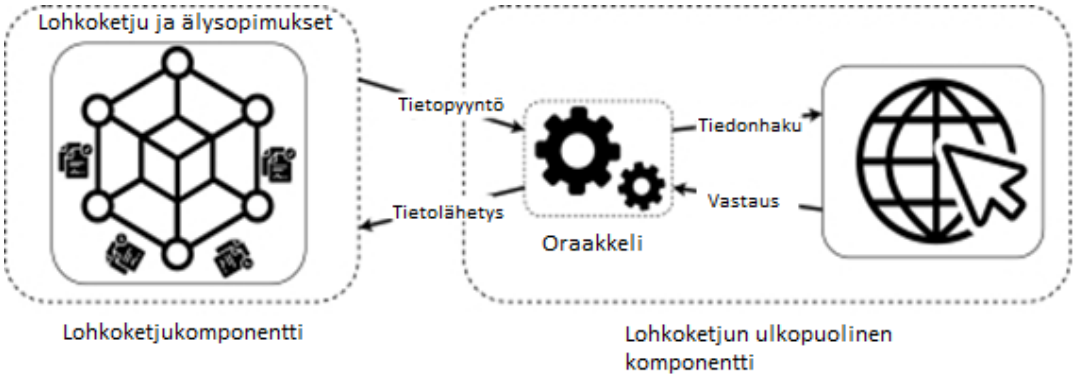
Toimitusketjujen hallintaan liittyvällä lohkoketju- ja älysopimusteknologialla näyttäisi tämän hetken kirjallisuuden mukaan olevan eniten käyttöä, joka ulottuu lohkoketjujen omien sisäisten ekosysteemien ulkopuolelle ja voivat täten tehostaa myös oikean maailman liiketoiminnan prosesseja.

# 4 ÄLYSOPIMUKSET JA LOHKOKETJUN ULKOPUOLINEN DATA

Yksi suurimmista, ellei suurin ongelma lohkoketjusovellusten ja älysopimusten käyttöönotossa ja yleismaailmallisessa hyödyntämisessä on luotettavan tiedon syöttäminen älysopimuksille. Tätä ongelmaa kutsutaan yleisesti oraakkeliongelmaksi, millä tarkoitetaan oikean maailman tiedon käyttämisen haasteita turvallisella ja luotettavalla tavalla. Lohkoketjut ovat luonnostaan deterministisiä, hajautettuja järjestelmiä, jotka perustuvat konsensusmekanismeihin varmistaakseen tiedon rehellisyyden ja estääkseen peukaloinnin. Kontrastina tälle, oikean maailman tieto on usein ristiriidassa lohkoketjun deterministisyyden kanssa, sillä sitä voidaan saada monesta eri lähteestä vaihtelevalla oikeellisuudella ja epätarkkuuksilla tai pahimmassa tapauksessa manipulaatiolla.

Oraakkeliongelman keskiö on se, että lohkoketjut eivät voi vastaanottaa tai varmentaa oikean maailman tietoa suoraan, koska näin tekeminen vaarantaisi turvallisuuden, avoimuuden ja eheyden, jonka luottamuksettomuus tarjoaa. Tätä varten tarvitaan luotettava välikäsi, jota kutsutaan oraakkeliksi, yhdistämään lohkoketju ulkoiseen tietolähteeseen. Lohkoketjuoraakkelit, joita voidaan kutsua myös tietosyötteiksi ovat yhdistelmiä älysopimuksista, jotka toimivat käytännössä ohjelmointirajapintana, jolla pystyy palvelemaan tietopyyntöjä muilta älysopimuksilta (Pasdar, Lee, Dong, 2023). Oraakkelit ovat vastuussa oikean maailman datan hakemisesta, sen prosessoimisesta ja toimittamisesta älysopimuksille ja lohkoketjuverkostoille. Oraakkeleja voidaan tietysti käyttää myös lohkoketjuympäristön sisällä, esimerkiksi monen erillään olevan lohkoketjun tiedon aggregointiin. Oraakkeleihin tukeutuminen esittelee uudenlaisia ongelmia varsinkin hajautuksen puutteen ja tietoturvaheikkouksien osalta, sillä niistä tulee helposti yksittäisiä vikakohtia tai kohteita toimijoille, jotka haluaisivat käyttää hyväksi tai manipuloida dataa, jota syötetään lohkoketjulle. Tämän jatko-ongelman ratkaisuksi on ehdotettu ja muodostunut hajautetun oraakkeliverkoston (Decentralized Oracle Network tai DON) käyttäminen (Ellis, Juels, Nazarov, 2017). Hajautetussa oraakkeliverkostossa oraakkeleita on useita, jotka kaikki ilmoittavat oman tietolähteensä ja nämä

kasataan konsensuskokonaisuudeksi. Kuviossa 2. on pelkistetty malli, joka kuvaa oraakkelin toimintaa, missä yhdistetään lohkoketju ulkoiseen informaatioon. Kuviossa oraakkeli kuvataan kokonaan lohkoketjun ulkopuolelle, mutta yleensä oraakkelit sijoittuvat näiden välimaastoon. Oraakkelit ovat sekä lohkoketjun komponentteja, että lohkoketjun ulkopuolen komponentteja.



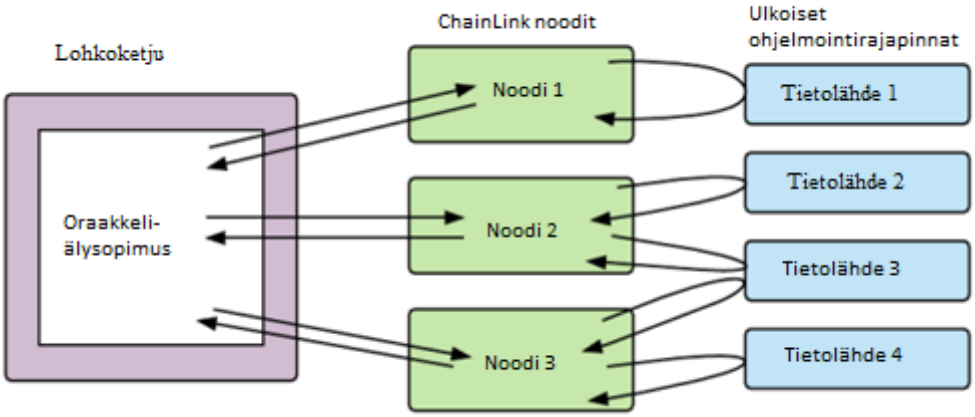

KUVIO 2 Yksinkertaistettu malli oraakkelin toiminnasta (Pasdar, Lee, Dong, 2023)

Oraakkelilähteet voidaan Pasdar, Lee ja Dong (2023) mukaan jakaa sovellusoraakkeleihin, missä tieto tulee verkossa olevista lähteistä esimerkiksi joltain palvelimelta. Laitteisto-oraakkeleihin, joissa tieto tulee fyysisestä maailmasta esimerkiksi antureilta ja viimeiseksi inhimillisiin oraakkeleihin eli ihmisen täytyy varmentaa tiedon aitous ja sen kääntyminen älysopimuksille (Pasdar ym., 2023). Viimeisessä kahdessa vaihtoehdossa ongelmana on se, että voiko jokainen sidosryhmä luottaa tietoon, joka tulee käytännössä vain yhdestä lähteestä. Riippuen älysopimuksen monimutkaisuudesta tai siitä rahallisesta arvosta, mitä älysopimus käsittelee, pitää tehdä päätös tarvitaanko enemmän hajautusta vai riittääkö pelkkä yksi anturitieto tai yhden ihmisen syöte. Tässä luvussa tarkastellaan tarkemmin erilaisia oraakkeliratkaisuja ja luotettavan tiedon tuomista turvallisesti lohkoketjun ulkopuolelta älysopimuksille, jotta niitä voidaan mahdollisesti hyödyntää oman ekosysteeminsä ulkopuolellakin.

## 4.1 Chainlink

Uudenlaisten teknologioiden ominaisuuksien kuvailu nojaa paljon kyseisten teknologioiden teknisiin raportteihin. Älysopimukset luovat uudenlaisia luottamusrakenteita sidosryhmien välille, koska ne itsenäisesti tarkistavat ja toteuttavat sopimuksen ehdot, mikä varmistaa niiden koskemattomuuden ulkoiselta tai sisäiseltä asiattomalta käsittelyltä (Ellis ym., 2017). Ellisin, Juelsin ja Nazarovin (2017) mukaan tämä uudenlainen luottamusmalli kuitenkin esittelee yhdistettävyyden teknisenä ongelmana, yhdistettävyys tässä kontekstissa

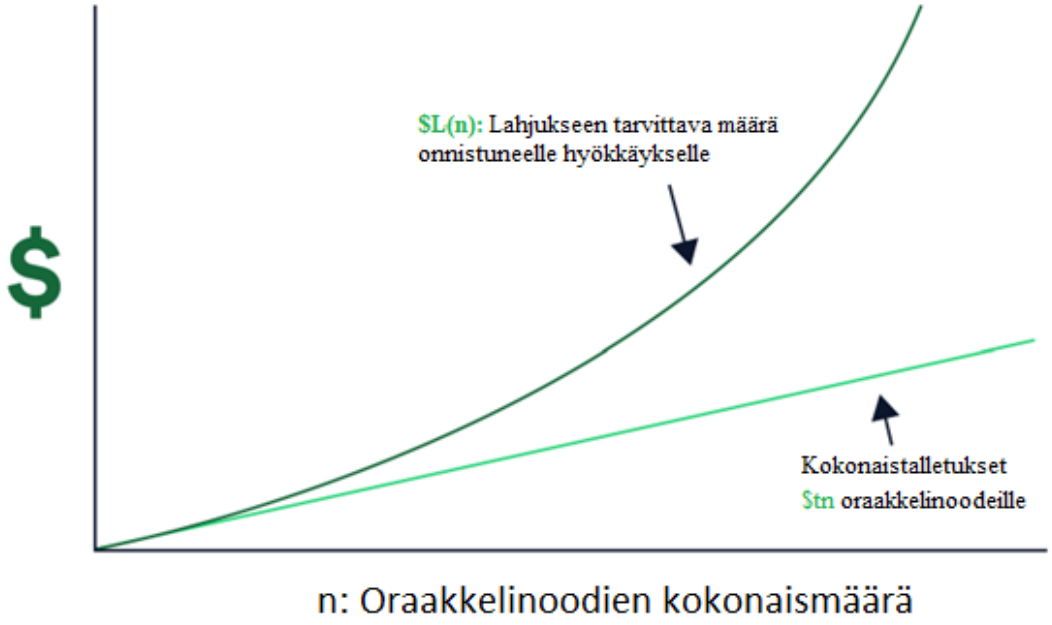
tarkoittaa älysopimusten kykyä vastaanottaa oikean maailman tietoa – heidän näkemyksensä mukaan älysopimusten on pakko muuttua ulkoisesti tietoisiksi, jos niiden halutaan korvaavan tämän hetken digitaaliset sopimukset. Tähän ratkaisuksi esitellään Chainlink, mikä on hajautettu oraakkeliverkosto (Decentralized Oracle Network tai DON), minkä hajauttaminen tapahtuu tiedon keräämisellä useasta eri lähteestä, jolloin yksi väärässä oleva lähde ei vielä aiheuta ongelmia älysopimukselle. Tämän lisäksi aivan kuten oraakkelien lähteitä voidaan lisätä, itse oraakkelisolmujen määrää voidaan lisätä, kuviossa 3. on Chainlinkin teknisen raportin kuvailu tästä esitellystä ratkaisusta.




KUVIO 3 Oraakkeliälysopimus yhdistettynä Chainlink-solmuihin, jotka saavat tietoa ulkoisista ohjelmointirajapinnoista (Ellis, Juels, Nazarov, 2017).

Heissin, Eberhardtin ja Tain (2019) määritelmän mukaan Chainlinkin tapa rakentaa oraakkeleita kuuluu äänestyspohjaiseen tiedon siirtämiseen lohkoketjulle. Äänestyspohjaisessa tiedon siirtämisessä totuudenmukaisen tiedon välittämistä motivoi yleensä jonkinlainen taloudellinen kannustin, tämän lisäksi väärän tiedon välittämistä voidaan rankaista esimerkiksi menettämällä sopimuksia tai sakottamalla (Heiss ym., 2019). Chainlinkillä on oma natiivi rahake nimeltä LINK, jota käytetään oraakkeliverkoston palveluihin. Jokainen verkostossa tapahtuva tietopyyntö maksetaan LINK-rahakkeilla. LINK-rahaketta on olemassa miljardi kappaletta yhteensä, mutta ERC-677-rahakkeet ovat tarvittaessa jaollisia 18:nteen desimaaliin asti, jos yhden kokonaisen LINKin arvo olisi liian korkea sen käyttötarkoitukseen tiedon välittämisessä. Chainlinkin teknisessä raportissa on myös kuvailtu rahakkeiden panttaaminen oraakkelisolmuille, joka kannustaisi solmuoperaattoreita antamaan totuudenmukaista tietoa sillä uhalla, että väärästä tiedosta voisi menettää osan pantista leikkausmekanismilla (Breidenbach ym., 2021). Yksinkertaistettuna oraakkelien välittäessä oikeaa ja totuudenmukaista tietoa, saavat ne palkkioina LINKiä ja mahdollisissa virhetilanteissa tai väärää tietoa välittäessä oraakkelioperaattori voisi menettää osan pantatuista LINKeistään sakon muodossa. Datalähteiden aggregointi varmistaa, että on peliteoriaoptimia välittää oikeaa tietoa ja saada siitä korvausta kuin yrittää välittää väärää tietoa ja

saada siitä sakkoa tai menettää sopimus. Vaikka solmu tai noodi antaisi väärää tietoa, ei mahdollisesta manipulaatioyrityksestä voisi hyötyä rahallisesti, koska tämän yksittäisen solmun väärin ilmoitettu data ei vaikuta muiden solmujen konsensukseen riittävästi. Kuvio 4. havainnollistaa miten onnistuneeseen hyökkäykseen tarvitaan suurempi lahjusmäärä kuin oraakkelisolmuihin talletettu kumulatiivinen määrä on.




KUVIO 4 Super-lineaarisen panttauksen vaikutus lahjontahyökkäystapauksissa (Breidenbach ym., 2021)

Chainlink on saavuttanut käytetyimmän hajautetun oraakkeliverkoston aseman, koska se on helposti integroitavissa sekä historiallisesti luotettava oraakkeliratkaisu tarkalle ja kryptografisesti varmistetulle tiedolle (Goswami, Danish, Zhang, 2022). Huhtikuussa 2023 Chainlinkin osuus kaikesta hajautetun rahoituksen turvatusta arvosta (total value secured, TVS) oli 45,66 % eli noin 12,47 miljardia Yhdysvaltain dollaria – saman lähteen mukaan toiseksi suurin oraakkelituottaja oli 28,55 % kokonaisarvosta eli Chainlink on selkeästi suurin toimija kyseisessä ekosysteemissä (DefiLlama, 2023). Tämä näkyy myös tilastoissa, sillä Chainlinkin ekosysteemissä tapahtuneiden kaikkien transaktioiden arvo kumulatiivisesti vuonna 2022 oli 6,9 triljoonaa Yhdysvaltain dollaria. Transaktioiden varmistamisen lisäksi Chainlink on tuonut 5,8 miljardia datapistettä eri lohkoketjuille sekä käynnistänyt yli tuhat uutta oraakkeliverkostoa heidän oman raportointinsa mukaan (Nazarov, 2023). Tästä huolimatta, kaikkia Chainlinkin alkuperäisessä teknisessä raportissa esiteltyjä ominaisuuksia kuten maineeseen ja tilauksiin kohdennettuja älysopimuksia, joilla automaattisesti valittaisiin sopivimmat oraakkelit, ei ole vielä toteutettu

(Goswami ym., 2022). Vuoden 2022 lopulla julkaistiin ensimmäinen 0.1 versio Ethereumin hintasyötteen panttausominaisuudesta, jolla on tulevaisuudessa tarkoitus varmistaa taloudellisten kannustimien kautta, että kyseistä hintasyötettä raportoivat oraakkelisolmut eivät anna väärää tietoa tarkoituksellisesti tai vahingossa. Chainlinkin teknisen raportin mukaan panttaus (staking) on mekanismi, jolla rationaalisesti toimivat käyttäjät ohjautuisivat toimimaan rehellisesti omien taloudellisten intressiensä painostamana eikä epärehellinen toimija kykenisi lahjomaan muita käyttäjiä olemaan epärehellisiä koska tämän toiminnan kustannus olisi liian kallista verrattuna totuuden esittämiseen (Breidenbach ym., 2021).

Chainlinkin toimintatapaa, joka perustuu kannustimiin ja aggregaatiomalleihin on myös kritisoitu mahdollisten kustannus- ja skaalautuvuusongelmien takia (Taghavi, Bentahar, Otrok, Bakhtiyari, 2023). Tähän vastauksena on kehitetty lohkoketjun ulkopuolista raportointia (Off-Chain Reporting tai OCR), missä konsensusalgoritmi eri oraakkelisolmuille tapahtuu lohkoketjun ulkopuolella solmujen omassa vertaisverkossa. Tällä tavalla oraakkelit raportoivat samalla tavalla, mutta lohkoketjulla tapahtuvia transaktioita tulee vain yksi (Eskandari, Salehi, Gu, Clark, 2021). Yksinkertaistettu esimerkki tästä olisi usean postipaketin lähettäminen ja sen sijaan, että jokaisesta paketista maksetaan erikseen maksu, paketit paketoidaan yhteen suurempaan pakettiin ja siitä maksetaan yksi kertamaksu. Toisaalta lohkoketjulla transaktiosta ei välttämättä tarvitse maksaa enempää koska lähetettävän tavaran koko ei ole suoraan verrannollinen hintaan.

### 4.1.1 Arkkitehtuuri

Chainlinkin arkkitehtuuri on kehittynyt avoimeksi kehikoksi, jonka avulla voidaan käynnistää toisistaan riippumattomia oraakkeliverkostoja, oraakkeliverkostoilla voi olla erilaisia käyttökohteita tai palveluita mitä ne tarjoavat:

1. Tietosyötteet (Data feeds)
2. Todiste varannoista (Proof of Reserves)
3. Varmistettavissa oleva satunnaisfunktio (Verifiable Random Function) (Micali, Rabin, Vadhan, 1999)
4. Nollatietotodistus (Zero Knowledge Proof)

Tarkoitus on kehittää ekosysteemi, jossa palveluntarjoajat kykenevät erikoistumaan niihin palveluihin, mitkä ovat heille ominaisimpia – tällä tavalla toivotaan asiakkaiden kokonaiskustannusten olevan alempia kuin vaihtoehtoisessa mallissa, jossa jokainen solmu ja verkko tarjoavat kaikki mahdolliset palvelut (Breidenbach ym., 2021).

Chainlinkin perusarkkitehtuuri on jaettavissa lohkoketjulla tapahtuvaan arkkitehtuuriin sekä lohkoketjun ulkopuoliseen arkkitehtuuriin. Lohkoketjulla tapahtuva arkkitehtuuri rakentuu kolmen pääasiallisen älysopimuksen varaan:

- Mainesopimus, joka tarkkailee oraakkelipalvelutarjoajien suorituskykymittareita.
- Tilausten kohdentamiseen luotu älysopimus, joka ottaa vastaan palvelutasosopimuksen, muuttaa ne parametreiksi ja kerää tarjoukset oraakkelitarjoajilta minkä jälkeen se valitsee tarjoukset maineen perusteella ja viimeistelee oraakkelin palvelutasosopimuksen.
- Aggregaatiosopimus, joka kerää oraakkelitarjoajien vastaukset ja laskee konsensustuloksen Chainlink-kyselyyn ja palauttaa tämän kyselyn esittäjälle. Tämän lisäksi sopimus myös syöttää oraakkelitarjoajien mittaustilastoja mainesopimukselle.

Chainlinkin sopimukset ovat rakennettu modulaarisiksi, joten niitä voidaan muokata käyttäjien tarpeille sopivammiksi (Ellis ym., 2017).

Lohkoketjun ulkopuolista arkkitehtuuria on Chainlinkin ydin eli noodien sovellus, joka on vastuussa lohkoketjun kanssa liitännöistä, aikatauluttamisesta sekä työn tasapainottelusta erilaisten ulkoisten palvelujen kanssa. Ellis, Juels ja Nazarov (2017) kuvailevat noodien tekemää työtä toimeksiannoiksi, jotka ovat joukko erilaisia alitehtäviä, mitkä prosessoidaan tietynlaisessa putkessa. Ytimen lisäksi on kaikki ulkoiset adapterit, jos valmiiksi rakennettuja alitehtäviä ei ole toimeenannolle, voidaan rakentaa mukautettuja alitehtäviä mitä kutsutaan adaptereiksi. Ulkoiset adapterit rakennetaan minimaalisina REST-ohjelmointirajapintoina ja täten ohjelmia voidaan helposti implementoida millä tahansa ohjelmointikielellä. Alitehtävien eli adapterien skeemat ovat viimeinen osa ulkopuolista perusarkkitehtuuria, skeemoilla on tarkoitus varmistaa yhteentoimivuus adapterien välillä. (Ellis ym., 2017)

Sekä Chainlinkin uudistettu tekninen raportti (2021), että Zhaon, Kangin, Lin, Chun ja Wangin (2022) tutkimusartikkeli luotettavista hajautetun rahoituksen oraakkeliratkaisuista mainitsevat uudenlaiset hybridiälysopimukset, joissa laskentaa tapahtuu lohkoketjulla ja -ketjun ulkopuolella. Hajautetun oraakkeliverkoston logiikka tapahtuu itse kohdelohkoketjun ulkopuolella, mutta tieto kulkee kryptografisesti varmennetun ankkuriälysopimuksen läpi (Zhao ym., 2022). Tämän tarkoitus on vähentää lohkoketjulle asetettua kuormaa ja samalla alentaa tiedonhaun kustannuksia.

### 4.1.2 Chainlinkin palvelut

Hajautetun oraakkeliverkostoninfrastruktuurin kypsyminen on mahdollistanut monenlaisten eri palveluiden tarjoamista. Kaikki palvelut pohjimmiltaan perustuvat hajautetun oraakkeliverkoston toimintaan, mutta niitä on kehitetty tarkemmin vastaavaan erilaisia käyttäjien tarpeita. Tietosyötteet ovat yleensä ensimmäinen oraakkelien käyttökohde, joka tulee keskustelussa esiin. Ulkoisen datan syöttäminen lohkoketjulle sekä lohkoketjujen välisen datan syöttäminen älysopimuksille on hajautetun rahoituksen perustana (Li ym., 2020). Chainlinkin hintasyötteet tuovat peukaloimatonta dataa, kuten kryptovaluuttojen hintoja,

valuuttojen vaihtosuhteita tai kauppatavaroiden hintoja niitä tarvitseville käyttäjille.

Toinen heidän tarjoama palvelunsa on hajautetut oraakkeliverkostot, jossa on mahdollista luoda muokattavia oraakkeliverkostoja. Tämä antaa mahdollisuuden kehittäjien valita haluamansa oraakkelinoodit, tietolähteet ja konsensusmetodit spesifiin käyttötarkoitukseensa. Tällä tavalla voidaan käyttää monenlaisia sovelluksia hajautetun rahoituksen alustoista toimitusketjujen hallinnan järjestelmiin.

Varmistettavissa oleva satunnaisfunktio (verifiable random function tai VRF) on alun perin Micalin, Rabinin ja Vadhanin (1999) esittelemä konsepti, joka yhdistää pseudosatunnaisia funktioita ja digitaalisia allekirjoituksia. Tämänlainen funktio mahdollistaa satunnaisen tulosteen, joka voidaan julkisella tarkastelulla varmistaa todella satunnaiseksi. Tämänlaista satunnaisfunktiota voidaan käyttää esimerkiksi konsensuksen optimointiin ja paremman turvallisuuden takaamiseen (Wang ym., 2022). Chainlinkin oman teknisen raportin mukaan monet lohkoketjusovellukset tarvitsevat kyvyn varmentaa todellinen satunnaisuus, tästä esimerkkinä he tuovat esiin digitaaliset hallintatodistukset (non-fungible token eli NFT), erilaiset lohkoketjuilla toimivat pelit, jotka tarvitsevat satunnaisfunktioita sekä lottoarvonnat (Breidenbach ym., 2021). Satunnaisuuden varmistamista tällä logiikalla voitaisiin käyttää kaikessa toiminnassa, jossa on eri osapuolia ja ainakin toisen osapuolen tulee luottaa siihen, että pelin tai tapahtuman lopputulos todella on satunnainen eikä häntä voida huijata. Tässä palataan taas lohkoketjun peruskonseptiin, jossa on mahdollista vähentää käyttäjien välistä luottamuksen tarvetta ja silti säilyttää rehellisyys tai jopa vahvistaa sitä.

Nollatietotodistus (zero-knowledge proof) kuvattiin ensimmäisen kerran Goldwasserin, Micalin sekä Rackoffin (1985) tutkimuspaperissa kryptografisena protokollana, jolla voidaan todistaa toteamus antamatta lisätietoa itse toteamuksesta. Nollatietotodistuksen pääpiirteet kyseisen paperin mukaan ovat:

1. Täydellisyys eli jos väite on tosi, rehellinen todistaja voi aina vakuuttaa rehellisen tarkastajan protokollan todistemekanismin avulla.
2. Eheys eli väitteen ollessa epätosi, epärehellinen todistaja ei kykene todistamaan rehellistä tarkastajaa suuremmalla todennäköisyydellä kuin sattumalla.
3. Nollatieto eli jos väittämä on tosi, rehellinen tarkastaja ei opi uutta informaatiota väittämästä itsestään pois lukien sen, että väittämä on tosi. Väittämän todenpitävyys todistetaan simulaattorialgoritmilla, joka kykenee tuottamaan tulosteen todisteprotokollasta, joka on samanlainen kuin tuloste todistajan ja tarkastajan interaktiossa.

Simulaattorin kyky tuottaa tuloste tietämättä todistajan salaisuutta osoittaa, että varmistaja ei saa mitään ylimääräistä tietoa salaisuudesta protokollan aikana (Goldwasser ym., 1985).

Nollatietotodistusten käyttökohteet löytyvät tilanteista, joissa yksityisyys ja luottamuksellisuus korostuvat. Tällä tavalla voidaan todistaa laskennon virheettömyys sekä transaktion oikeellisuus paljastamatta taustatietoja tai yksityiskohtia. Lohkoketjukontekstissa nollatietosopimusten käyttäminen mahdollistaa datan luottamuksellisuuden perinteisesti julkiselle tarkastelulle avoimissa lohkoketjuympäristöissä (Harikrishnan & Lakshmy, 2019).

Chainlinkin kehitysputkessa on oma implementaatio nollatietotodistuksiin perustuvasta oraakkeliratkaisusta nimeltä DECO, joka laajentaa HTTPS/TLS-protokollia ja varmistaa, että tieto pysyy yksityisenä ja koskemattomana sen siirron aikana. Breidenbachin ja muiden (2021) mukaan tyypillisessä DECOn käyttötapauksessa käyttäjä tai yksittäinen noodi voi viedä dataa yksityisestä istunnosta verkkopalvelimelta kaikille noodeille hajautetussa oraakkeliverkostossa. Hyödyntäen nollatietotodistusta voidaan varmistaa usean oraakkelin avulla tiedon autenttisuus, vaikka tietolähde olisi alkuaan vain yhdestä noodista (Breidenbach ym., 2021). Käyttämällä nollatietotodistuksiin perustuvia älysopimuksia asiakkaat voivat itse valita mitä tietoa he haluavat kirjata mahdollisesti julkiselle lohkoketjulle silti säilyttäen hajautetun lohkoketjun hyödyt, kuten muuttumattomuuden, turvallisuuden ja luotettavuuden sidosryhmien välillä. Yritykset luonnollisesti eivät halua tuoda kilpailuetua vaarantavia asioita julki kaikkien nähtäväksi. Nollatietotodistukset mahdollistavat älysopimuksien rakentamisen tavalla, josta yritykset voivat silti hyötyä näissä tapauksissa.

## 4.2 Oraakkelien turvallisuus

Jos älysopimuksia on tarkoitus käyttää liiketoiminnassa, jossa käsitellään satoja miljoonia dollareita, on älysopimuksille syötettävän tiedon oltava turvattua. Lohkoketjuilla turvallisuus on sisäänrakennettua, kun hajautus on riittävää, mutta tiedon tuominen lohkoketjun ulkopuolelta on aina riski turvallisuudelle. Turvallisuusongelmia ovat esimerkiksi keskitetyt oraakkelit eli tiedonlähteenä on vain yksi oraakkeli, jota on helpompi manipuloida tai tehdä toimimattomaksi. Sybil-hyökkäyksessä väärinkäyttäjät luovat useita valheellisia oraakkelinoodeja vääristääkseen älysopimuksille syötettävää tietoa. Datamanipulaatiohyökkäyksissä yritetään vaikuttaa lohkoketjun ulkopuolisiin tietolähteisiin, kuten ohjelmoitaviin rajapintoihin tai tietokantoihin, mistä oraakkelit noutavat tietonsa tarkoituksenaan syöttää älysopimuksille vääränlaista tietoa.

Keskitettyjen oraakkelien aiheuttamiin ongelmiin kirjallisuuden mukaan yksinkertaisin ratkaisu on hajautettu oraakkeliverkosto, joka tuo tietoa useista lähteistä (Al-Breiki, Rehman, Salah, Svetinovic, 2020; Liu, Szalachowksi, Zhou, 2021). Jos tiedonlähteitä on tarpeeksi ja niiden käytettävyysaika on tarpeeksi korkea, voidaan toivoa, että saatu konsensus on tarpeeksi luotettava. Sybil-hyökkäyksien estäminen on helpointa, jos oraakkeleilla on rakennettu luottamusjärjestelmä tai oraakkeleihin on pantattuna rahallista arvoa, joka

kannustaa peliteoriallisesti toimimaan rehellisesti ja tarjoamaan tarkkaa tietoa. Panttaamalla jonkinlaisen rahakkeen oraakkelitarjoajat ovat valmiita menettämään arvoa, jos he raportoivat väärin (Breidenbach ym., 2021). Oraakkelien historialliseen suorituskykyyn perustuva luottamusjärjestelmä helpottaa myös oikeiden oraakkelien valintaa, kun etsitään tietolähteitä älysopimuksille. Vaikka oraakkelien tarve on uusi ilmiö, on joissain tapauksissa helpompaa hyödyntää jo olemassa olevia luottamussuhteita aikaisemmasta liiketoiminnasta, koska lohkoketju ei syntynyt tyhjiössä ja liiketoimintaa on harjoitettu ennen ja jälkeen lohkoketjuteknologian kehittämistä. Joissain tapauksessa oraakkelien valkolistaus on toimiva tapa varmistaa turvallisuus, varsinkin jos panttausta tai historiaan perustuvaa luottamusjärjestelmää ei ole olemassa.

Lohkoketjun ulkopuolisten lähteiden kuten rajapintojen tai tietokantojen datamanipulaatioon voi olla ratkaisuna luotettavat suoritusympäristöt (Trusted Execution Environment, TEE) kuten Intelin SGX. Jos oraakkeli toteutetaan suojatuilla ympäristöillä, tiedonkäsittely ja -siirto toteutuu turvallisesti ilman ulkopuolisten pääsyä järjestelmään. Tästä on tehty prototyyppi, jossa lohkoketjulle siirretään tietoa mikrokontrollerista rakennetusta luotettavasta suoritusympäristöstä, jolla voidaan varmentaa rokotteen koskemattomuus kuljetuksen aikana (Liu ym., 2022). Tällä tavalla ainakin sensoridataan perustuvien oraakkelien luotettavuus on paljon suurempi, jos käyttäjien ei tarvitse huolehtia tiedon koskemattomuudesta ennen kuin se saatetaan lohkoketjulle.

# 5 YHTEENVETO

Lohkoketjujen ja älysopimuksien kehittyminen teknologiana on mahdollistanut uudenlaisten palveluiden ja sovellusten käyttöönottoa. Lohkoketjuteknologian kehittyminen on luonut uuden paikoitellen kaoottisen toimintaympäristön, missä sääntelyn puute, globaali levinneisyys ja anonymiteetti mahdollistaa käyttäjien väärinkäytökset. Erilaiset huijaukset ovat todennäköisesti aiheuttaneet merkittävääkin mainehaittaa koko teknologialle. Vuonna 2023 kuitenkin teknologiaympäristö on paljon kehittyneempi kuin se oli Ethereumin julkaisun aikana, puhumattakaan Bitcoinista. Tällä hetkellä on toteutettu ja toteutetaan erilaisia älysopimuksia hyödyntäviä sovellutuksia, jotka eivät pelkästään ole huijauksia tai yksinkertaisia siirtoon tai varastointiin perustuvia rahakkeita. Ei voida vielä puhua minkäänlaisesta paradigmallisesta siirtymästä, mutta lohkoketjuteknologian tutkiminen on tärkeää ja ajankohtaista, koska kyseisen teknologian oikeanlaisella käytöllä on potentiaalia tehostaa liiketoimintaa ja samalla vähentää luottamuspohjaisten järjestelmien kitkaa.

Tämän kandidaatintutkielman tarkoitus oli selvittää lohkoketjujen ja älysopimusten sovellutuksia olemassa olevan tieteellisen kirjallisuuden avulla. Tutkielmassa pyrittiin vastaamaan kahteen tutkimuskysymykseen:

- Mitä älysopimussovelluksia on olemassa rahakejärjestelmien eli kryptovaluuttojen lisäksi?
- Miten älysopimuksia voidaan käyttää suljetun lohkoketjuympäristön kuten Ethereumin ulkopuolella, hyödyntäen reaalimaailman dataa?
    - Mikä on oraakkeliongelma?

Ulkopuolelle rajattiin sellaiset lohkoketjujen ja älysopimusten käyttötapaukset, joista yleisesti puhutaan kryptovaluuttoina eli rahakkeet. Jos rahakkeella ei ollut muuta käyttöä kuin ostaminen, myyminen tai varastointi, tätä ei tutkittu.

Tutkielma on kuvaileva kirjallisuuskatsaus, johtuen lohkoketjuihin liittyvän tieteellisen kirjallisuuden paikoittaisista puutteista. Lähteiden etsiminen tapahtui englanninkielisiä hakutermejä käyttämällä, tarkoituksena oli

rajata aiheelle olennaisimmat artikkelit. Hakutietokantoina toimivat pääosin IEEE Explore, ScienceDirect ja ACM Digital Library, mutta joitakin teknisiä ominaisuuksia tutkittaessa jouduttiin tukeutumaan myös teknisiin raportteihin tai valkopapereihin. Suurin osa lohkoketjuihin tai älysopimuksiin liittyvästä kirjallisuudesta on ilmestynyt vasta vuoden 2015 jälkeen, joten tutkimusaihe on suhteellisen uusi. Haastavinta oli löytää hyvää jatkumoa lähteistä, koska usein artikkelit kuvasivat jonkinlaista yksittäistä toteutustapaa tai ilmiötä. Tämä voidaan nähdä tutkielman rajoitteena, sillä hyvän tutkimusmateriaalin kerääminen ei ollut itsestäänselvyys. Teknologia on suhteellisen uusi, joten siitä ei ole kirjoitettu vielä paljoa laadukasta tutkimusmateriaalia. Tutkimusaiheen laajuus myös sulki pois useita älysopimusten käyttötarkoituksia, kun aihetta jouduttiin rajaamaan kirjallisuuden puitteissa.

Tutkielmassa selvisi, että lohkoketjut ja älysopimukset ovat todella riippuvaisia luotettavan ulkoisen tiedon saannista, jos niiden käyttökohteet ovat reaalimaailmalle suunnattuja. Voitaisiin jopa todeta, että oraakkeliongelman ratkaiseminen on yksi suurimmista haasteista lohkoketjujen yleisen ja laajan hyödyntämisen kannalta. Muitakin ongelmia on olemassa kuten korkeat siirtokustannukset, jos lohkoketju on korkeassa käytössä. Näitä skaalautuvuusongelmia varten on kehitetty ja kehitetään abstrahointitasoja, joilla kuormitusta voidaan lievittää pääketjulta. Lähdemateriaalia tutkiessa esiin nousi ainakin kolme potentiaalista sovellustyyppiä, missä lohkoketjuteknologiaa voidaan hyödyntää oikeassa maailmassa: hajautetut autonomiset organisaatiot, toimitusketjujen hallinta ja oraakkeliverkostot älysopimusten tukena. Toimitusketjujen avoimuuteen ja turvallisuuden lisäämiseen on olemassa jo lohkoketjutoteutuksia, jotka parantavat nykyisiä toimintatapoja. Oraakkeliverkostojen kehittyminen mahdollistaa uudenlaisten sovellusten ja palveluiden tuottamista.

Tutkielman tulokset osoittavat, että vaikka lohkoketjut ja älysopimukset ovat teknologioina vielä suhteellisen nuoria ja jatkokehitystä tarvitaan huomattavasti, käyttöpotentiaalia on reilusti myös reaalimaailmassa. Perinteisistä liiketoiminnan luottamusjärjestelmistä täysin siirtyminen luottamuksettomiin järjestelmiin, jossa ohjelmoitu sopimus on lakia vastaava, on kuitenkin vielä pitkällä tulevaisuudessa. Liiketoiminnan pidemmälle viety automatisointi itsestään toteutuvilla, älykkäillä sopimuksilla on jo nyt toteutettavissa. Turvallisuus on älysopimusten laajemmassa hyödyntämisessä yksi tärkeimmistä seikoista, joten olisi tärkeää tehdä jatkotutkimusta älysopimusten heikkouksista sekä niiden turvallisesta toteuttamisesta hyödyntäen ulkomaailman tietolähteitä. Pitkittäistutkimuksia älysopimusten sekä lohkoketjujen hyödyntämisessä teollisuudessa pitäisi tutkia enemmän, jotta voitaisiin nähdä, onko teknologialla edellytyksiä liiketoiminnan tehostamisessa. Olisi tärkeää myös tehdä laajempaa tutkimusta erilaisista automaatiomahdollisuuksista, jotka voisivat hyötyä älysopimuksista, mutta tässä tulisi muistaa ongelmanratkaisu hyödyntämällä sopivaa teknologiaa. Uuden teknologian pakottaminen kaikkiin mahdollisiin ongelmiin ei ole toimivaa, vaan lohkoketjua tai älysopimuksia tulisi soveltaa hyödyllisenä

työkaluna niissä tapauksissa mihin se parhaiten sopii eli automaatiossa, muuttumattomuuden varmistamisessa ja julkisen kirjanpidon käyttötarkoituksissa.

# LÄHTEET


Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2021). Uniswap v3 Core. https://uniswap.org/whitepaper-v3.pdf

Adjei-Arthur, B., Gao, J., Xia, Q., da Silva Tavares, E., Xia, H., Amofa, S., & Wang, Y. (2022). A blockchain-adaptive contractual approach for multi-contracting organizational entities. Future Generation Computer Systems, 132, 93–107. https://doi.org/10.1016/j.future.2022.02.003

Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. IEEE Access, 8, 85675–85685. https://doi.org/10.1109/ACCESS.2020.2992698

Altaleb, H., & Zoltan, R. (2022). Decentralized autonomous organizations review, importance, and applications. 2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES), 000121–000126. https://doi.org/10.1109/INES56734.2022.9922656

Antonio Risso, L., Miller Devós Ganga, G., Godinho Filho, M., Antonio de Santa-Eulalia, L., Chikhi, T., & Mosconi, E. (2023). Present and future perspectives of blockchain in supply chain management: A review of reviews and research agenda. Computers & Industrial Engineering, 109195. https://doi.org/10.1016/j.cie.2023.109195

Arunmozhi, M., Venkatesh, V. G., Arisian, S., Shi, Y., & Raja Sreedharan, V. (2022). Application of blockchain and smart contracts in autonomous vehicle supply chains: An experimental design. Transportation Research Part E: Logistics and Transportation Review, 165, 102864. https://doi.org/10.1016/j.tre.2022.102864

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

Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., Koushanfar, F., Miller, A., Magauran, B., Moroz, D., Nazarov, S., Topliceanu, A., Tramèr, F., & Zhang, F. (2021). Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks. https://research.chain.link/whitepaper-v2.pdf

Buterin, V. (2014a). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

Buterin, V. (2014b, toukokuuta 6). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide

Caldarelli, G., & Ellul, J. (2021). The Blockchain Oracle Problem in Decentralized Finance—A Multivocal Approach. Applied Sciences, 11(16), 7572. https://doi.org/10.3390/app11167572

Cao, Y., Yi, C., Wan, G., Hu, H., Li, Q., & Wang, S. (2022). An analysis on the role of blockchain-based platforms in agricultural supply chains. Transportation Research Part E: Logistics and Transportation Review, 163, 102731. https://doi.org/10.1016/j.tre.2022.102731

Chao, C.-H., Ting, I.-H., Tseng, Y.-J., Wang, B.-W., Wang, S.-H., Wang, Y.-Q., & Chen, M.-C. (2022). The Study of Decentralized Autonomous Organization (DAO)in Social Network. The 9th Multidisciplinary International Social Networks Conference, 59–65. https://doi.org/10.1145/3561278.3561293

Chohan, U. (2017). Cryptocurrencies: A Brief Thematic Review. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3024330

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society, 62, 101284. https://doi.org/10.1016/j.techsoc.2020.101284

DefiLlama. (2023, huhtikuuta 13). Total value secured all Oracles. https://defillama.com/oracles

El Faqir, Y., Arroyo, J., & Hassan, S. (2020). An overview of decentralized autonomous organizations on the blockchain. Proceedings of the 16th International Symposium on Open Collaboration, 1–8. https://doi.org/10.1145/3412569.3412579

Ellis, S., Juels, A., & Nazarov, S. (2017). Chainlink A Decentralized Oracle Network. https://research.chain.link/whitepaper-v1.pdf

Eskandari, S., Salehi, M., Gu, W. C., & Clark, J. (2021). SoK: Oracles from the ground truth to market manipulation. Proceedings of the 3rd ACM Conference on Advances in Financial Technologies, 127–141. https://doi.org/10.1145/3479722.3480994

Ezzat, S. K., Saleh, Y. N. M., & Abdel-Hamid, A. A. (2022). Blockchain Oracles: State-of-the-Art and Research Directions. IEEE Access, 10, 67551–67572. https://doi.org/10.1109/ACCESS.2022.3184726

Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC '85, 291–304. https://doi.org/10.1145/22145.22178

Goswami, S., Danish, S. M., & Zhang, K. (2022). Towards a middleware design for efficient blockchain oracles selection. 2022 Fourth International

Conference on Blockchain Computing and Applications (BCCA), 55–62. https://doi.org/10.1109/BCCA55292.2022.9922433

Hanson, R. (2003). LOGARITHMIC MARKETS CORING RULES FOR MODULAR COMBINATORIAL INFORMATION AGGREGATION. The Journal of Prediction Markets, 1(1), 3–15. https://doi.org/10.5750/jpm.v1i1.417

Harikrishnan, M., & Lakshmy, K. V. (2019). Secure Digital Service Payments using Zero Knowledge Proof in Distributed Network. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 307–312. https://doi.org/10.1109/ICACCS.2019.8728462

Heiss, J., Eberhardt, J., & Tai, S. (2019). From Oracles to Trustworthy Data On-Chaining Systems. 2019 IEEE International Conference on Blockchain (Blockchain), 496–503. https://doi.org/10.1109/Blockchain.2019.00075

Hu, B., Zhang, Z., Liu, J., Liu, Y., Yin, J., Lu, R., & Lin, X. (2021). A comprehensive survey on smart contract construction and execution: Paradigms, tools, and systems. Patterns, 2(2), 100179. https://doi.org/10.1016/j.patter.2020.100179

Hu, S., Huang, S., & Qin, X. (2022). Exploring blockchain-supported authentication based on online and offline business in organic agricultural supply chain. Computers & Industrial Engineering, 173, 108738. https://doi.org/10.1016/j.cie.2022.108738

Kjaer, M., di Angelo, M., & Salzer, G. (2021). Empirical Evaluation of MakerDAO's Resilience. 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 193–200. https://doi.org/10.1109/BRAINS52497.2021.9569811

Köhler, S., Bager, S., & Pizzol, M. (2022). Sustainability standards and blockchain in agro-food supply chains: Synergies and conflicts. Technological Forecasting and Social Change, 185, 122094. https://doi.org/10.1016/j.techfore.2022.122094

Li, K., Tang, Y., Chen, J., Yuan, Z., Xu, C., & Xu, J. (2020). Cost-Effective Data Feeds to Blockchains via Workload-Adaptive Data Replication. Proceedings of the 21st International Middleware Conference, 371–385. https://doi.org/10.1145/3423211.3425696

Li, Q., Ma, M., Shi, T., & Zhu, C. (2022). Green investment in a sustainable supply chain: The role of blockchain and fairness. Transportation Research Part E: Logistics and Transportation Review, 167, 102908. https://doi.org/10.1016/j.tre.2022.102908

Liu, B., Szalachowski, P., & Zhou, J. (2021). A First Look into DeFi Oracles. 2021 IEEE International Conference on Decentralized Applications and

Infrastructures (DAPPS), 39–48. https://doi.org/10.1109/DAPPS52256.2021.00010

Liu, C., Guo, H., Xu, M., Wang, S., Yu, D., Yu, J., & Cheng, X. (2022). Extending On-chain Trust to Off-chain—Trustworthy Blockchain Data Collection using Trusted Execution Environment (TEE). IEEE Transactions on Computers, 1–1. https://doi.org/10.1109/TC.2022.3148379

Lund, E. H., Jaccheri, L., Li, J., Cico, O., & Bai, X. (2019). Blockchain and Sustainability: A Systematic Mapping Study. 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 16–23. https://doi.org/10.1109/WETSEB.2019.00009

Maker Foundation. (2020). The Maker Protocol. https://makerdao.com/en/whitepaper/

Micali, S., Rabin, M., & Vadhan, S. (1999). Verifiable random functions. 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039), 120–130. https://doi.org/10.1109/SFFCS.1999.814584

Morrison, R., Mazey, N. C. H. L., & Wingreen, S. C. (2020). The DAO Controversy: The Case for a New Species of Corporate Governance? Frontiers in Blockchain, 3, 25. https://doi.org/10.3389/fbloc.2020.00025

Nazarov, S. (2023). The Chainlink Network in 2023. https://blog.chain.link/the-chainlink-network-in-2023/

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. IEEE Access, 7, 85727–85745. https://doi.org/10.1109/ACCESS.2019.2925010

Pasdar, A., Lee, Y. C., & Dong, Z. (2023). Connect API with Blockchain: A Survey on Blockchain Oracle Implementation. ACM Computing Surveys, 55(10), 1–39. https://doi.org/10.1145/3567582

Shakhbulatov, D., Arora, A., Dong, Z., & Rojas-Cessa, R. (2019). Blockchain Implementation for Analysis of Carbon Footprint across Food Supply Chain. 2019 IEEE International Conference on Blockchain (Blockchain), 546–551. https://doi.org/10.1109/Blockchain.2019.00079

Su, S., Wang, K., & Kim, H. S. (2018). Smartsupply: Smart Contract Based Validation for Supply Chain Blockchain. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 988–993. https://doi.org/10.1109/Cybermatics_2018.2018.00186

Sunmola, F., & Burgess, P. (2023). Transparency by Design for Blockchain-Based Supply Chains. Procedia Computer Science, 217, 1256–1265. https://doi.org/10.1016/j.procs.2022.12.324

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Uniswap. (2020). Community Governance Process. https://gov.uniswap.org/t/community-governance-process/7732

Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., & Wang, F.-Y. (2019). Decentralized Autonomous Organizations: Concept, Model, and Applications. IEEE Transactions on Computational Social Systems, 6(5), 870–878. https://doi.org/10.1109/TCSS.2019.2938190

Wang, Z., Zhu, M., Wang, Y., & Hei, X. (2022). Hyperledger Fabric Consensus Optimization Method Based on Endorsing Nodes. 2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology (ICCASIT), 65–68. https://doi.org/10.1109/ICCASIT55263.2022.9986575

Zhao, Y., Kang, X., Li, T., Chu, C.-K., & Wang, H. (2022). Toward Trustworthy DeFi Oracles: Past, Present, and Future. IEEE Access, 10, 60914–60928. https://doi.org/10.1109/ACCESS.2022.3179374