



Chainlink: oraakkeli-verkosto kaupankäynnissä

Andreas Achte

OPINNÄYTETYÖ
Syyskuu 2024

Tietojenkäsittely, Tamk
Ohjelmistotuotanto

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Ohjelmistotuotanto

ACHTE, ANDREAS:
Chainlink: oraakkeliverkosto kaupankäynnissä

Opinnäytetyö 28 sivua, joista liitteitä 0 sivua
Syyskuu 2024

Opinnäytetyön aihe valikoitui mielenkiinnosta lohkoketjuteknologiaan. Lohkoketjuteknologiat ovat yleistyneet viime vuosina kaupankäynnissä. Opinnäytetyön tavoitteena oli analysoida Chainlink -nimistä oraakkeliverkostoa. Tarkoituksena oli tarkastella miten Chainlink auttaa ja tukee kaupankäyntiä lohkoketjupohjaisissa alustoissa. Tarkoituksena oli myös analysoida Chainlinkin teknologiaa ja lohkoketjuteknologiaa syvällisemmin sekä muodostaa yleinen käsitys lohkoketjuteknologioista ja Chainlinkin käytännön sovelluksista.

Aiheen tutkimisessa tehtiin kirjallisuuskatsaus. Tiedonhaussa käytettiin alan kirjallisuutta sekä esimerkiksi Chainlinkin teknistä dokumentaatiota ja artikkeleita internetissä. Katsottiin myös julkista lohkoketjudataa internetin välityksellä. Materiaalia analysoitiin ja tutkittiin.

Havaittiin, että Chainlink on tärkeä protokolla monenlaisissa lohkoketjupohjaisissa sovelluksissa internetissä. Sovellukset liittyvät mm. kaupankäyntiin, valuuttojen vaihdantaan ja rahoituspalveluihin. Chainlinkin oraakkeliverkostolla on tärkeä rooli esimerkiksi lohkoketjupohjaisten hajautettujen rahoituspalvelujen tiedonlähteenä.

Asiasanat: lohkoketjut, virtuaalivaluutta, kauppa, verkostot, kirjanpitojärjestelmä

ABSTRACT

Tampere University of Applied Sciences
Degree programme in Information Sciences
Software production

ACHTE, ANDREAS:
Chainlink: Oracle Network in Trade

Bachelor's thesis 28 pages, appendices 0 pages
September 2024

The objective of this thesis was to analyze the Chainlink oracle network in trading. The purpose was to collect information about blockchain networks in general and analyze the networks from a technological perspective.

Information and data was collected from books, online articles and Chainlink's official documentation. The information was studied and analyzed. The theoretical section explores Blockchain technology and Chainlink's technology in detail.

The information suggests that Chainlink has an important role in the blockchain ecosystem. Chainlink provides accurate and reliable data to many blockchain networks. These networks can then provide new ways to trade or use financial services, for example.

The research indicates that these distributed ledger systems can provide new ways to store data about money and economic value. In the current monetary system, data is centralized, hidden and controlled. In the distributed ledger system, economic data is distributed and open. The technology is there to potentially alter the current financial system.

Key words: blockchains, cryptocurrency, trade, networks, ledger

SISÄLLYS

1	JOHDANTO	5
2	Lohkoketju ja älykkäät sopimukset	7
	2.1 Virtuaalivaluutta ja lohkoketjuverkostot	7
	2.2 Bitcoin: ensimmäinen laajassa käytössä oleva lohkoketjuverkosto	7
	2.3 Älysopimukset	10
	2.4 Oraakkeliongelma	10
3	Johdatus Chainlinkiin	12
	3.1 Historia ja kehitys	12
	3.2 Yleiskatsaus Chainlink verkostoon	12
	3.3 Chainlinkin tärkeimmät komponentit	13
4	Chainlinkin tekninen arkkitehtuuri	16
	4.1 Solmun funktiot	16
	4.2 Dataturvallisuusmekanismi ja validaatio	16
5	Chainlink: käyttötapaukset kaupankäynnissä	17
	5.1 DeFi: hajautetut finanssitulokset	17
	5.2 Tokenization: oikean elämän omistuksien tokenisointi	19
6	Chainlink 2.0: kehitys ja edistyneemmät mekanismit	21
	6.1 Oraakkeliriski	21
	6.2 Tietoturvallisuusmekanismi	22
	6.3 Sillat ja CCIP	22
7	Tekninen analyysi: Aave-protokollan Chainlink –integraatio	24
	7.1 Historia ja konteksti	24
	7.2 Toiminta	24
8	Pohdinta	27
	LÄHTEET	28

1 JOHDANTO

Vuonna 2021 julkaistussa World economic forumin raportissa: “Digital Assets, Distributed Ledger Technology, and the Future of Capital Markets” käsitellään hajautettua kirjanpitojärjestelmää. Lohkoketjuteknologia on yksi tällainen hajautettu kirjanpitojärjestelmä. Lohkoketjuteknologiat ovat yleistyneet käytössä viime vuosina enemmän ja enemmän. Ensimmäinen isompi käyttöön otettu lohkoketju-sovellus oli Bitcoin, joka julkaistiin vuonna 2009. Bitcoin on kuin iso tilikirja, ja sen yksiköitä voidaan lähettää ja vaihtaa ympäri maapalloa suhteellisen nopeasti, ilman välikäsiä. Bitcoinin jälkeen on luotu paljon muitakin lohkoketjutekniikkaan perustuvia verkostoja, jotka tarjoavat monenlaisia toiminnallisuuksia.

Lohkoketjuteknologiat ovat mahdollistaneet monipuolisten hajautettujen sovellusten luomisen. Nämä hajautetut sovellukset ja alustat voivat mahdollistaa kaupankäyntiä hieman erilaisilla säännöillä ja mahdollisuuksilla kuin mihin Fiat-rahajärjestelmässä on totuttu.

Chainlink on erilaisia lohkoketju –verkostoja palveleva oraakkeliverkosto. Chainlinkin käyttökohteet ovat moninaiset, ja se varmistaa monen isomman lohkoketjuverkoston sekä applikaation toimintaa tarjoamalla luotettavaa, tietoturvallista ja ajankohtaista tietoa. Chainlink mahdollistaa myös esimerkiksi kommunikaatiota ja kaupankäyntiä eri lohkoketjujen välillä. Näin se voi auttaa kaupankäynnissä.

Tämän opinnäytetyön tavoite on analysoida Chainlinkiä ja sen käyttötapauksia. Samalla tarkoituksena on lisätä ymmärrystämme mm. hajautetuista kirjanpitojärjestelmistä ja lohkoketjuteknologiasta laajemminkin. Jotta voimme ymmärtää Chainlinkin teknologiaa, on mielestäni tärkeä ymmärtää myös hieman perusasioita lohkoketjuverkostoista muutenkin. Aihe on laaja, mutta keskityn tässä opinnäytetyössä lähinnä teknologiaan ja siihen, miten verkostoissa käsitellään tietoa. Käsittelen myös muutamia muita kryptovaluuttoihin liittyviä verkostoja, koska Chainlink toimii yhteistyössä muiden verkostojen kanssa, mahdollistaen siten uudenlaisia tapoja siirtää taloudellista arvoa ja käydä kauppaa.

Taloudellisessa kontekstissa ja mittakaavassa Chainlink on varsin pieni verkosto verrattuna esimerkiksi Bitcoiniin. Tällä hetkellä se on markkina-arvolla mitattuna 13. Suurin kryptovaluutta. Chainlinkin osuus kaikista kryptovaluutoista noin 8 miljardin markkina-arvolla on vain noin 0.3% (Coinmarketcap, a) Tämä kertoo kuitenkin hieman siitä, että Chainlinkin LINK-tokeneilla on tällä hetkellä joku taloudellinen arvo, ja niitä saa myytyä. Token tarkoittaa verkoston vaihdantayksikköä. LINK –tokeneita voidaan siis siirrellä, lähetellä ja omistaa. Tämä tapahtuu käytämällä kryptolompakkoa.

2 Lohkoketju ja älykkäät sopimukset

2.1 Virtuaalivaluutta ja lohkoketjuverkostot

Kryptovaluutalla tarkoitetaan yleensä lohkoketjupohjaista valuuttaa. Käyttäjä voi omistaa valuuttaa ja siirrellä sitä. Lohkoketju siis tunnistaa uniikin käyttäjän, ja pystyy yleensä varmistamaan omistajuussuhteen. Näin on esimerkiksi Bitcoinin tapauksessa. Käyttäjä voi omistaa Bitcoineja käyttämällä kryptolompakkoa. (Laurence, 2023)

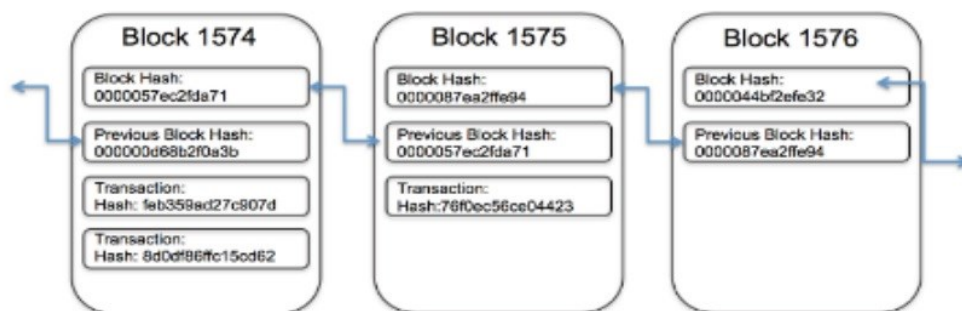
Bitcoin on ensimmäinen laajaan käyttöön levinnyt sovellus lohkoketjusta ja se on myös markkina-arvoltaan suurin kryptovaluutta edelleen keväällä 2025. Riippuen ajoista ja lähteistä, on Bitcoin-dominanssi ollut vuoden 2017 jälkeen noin 40% - 70% välillä. (Coinmarketcap, b) Tämä luku kuvaa, kuinka suuri osa kryptovaluuttojen kaikesta markkina-arvosta on jakautunut Bitcoinin ja muihin kryptovaluuttoihin.

Bitcoinin jälkeen on siis kehitetty monia muita lohkoketjuverkostoja. Esimerkiksi 2015 käyttöön otettu Ethereum –verkosto on aika isoon rooliin ja käyttöön nousut uusi lohkoketjuteknologia. Ethereumin markkina-arvo on keväällä 2025 noin 192 miljardia (Coinmarketcap, c). Tämä on noin 12% Bitcoinin markkina-arvosta samalla ajan hetkellä. Ekosysteemi kryptovaluuttojen ympärillä on kehittynyt nopeasti, ja tämä näkyy myös monien kryptovaluuttojen markkina-arvossa eli siinä arvossa, millä kolikon saa todennäköisesti myytyä.

2.2 Bitcoin: ensimmäinen laajassa käytössä oleva lohkoketjuverkosto

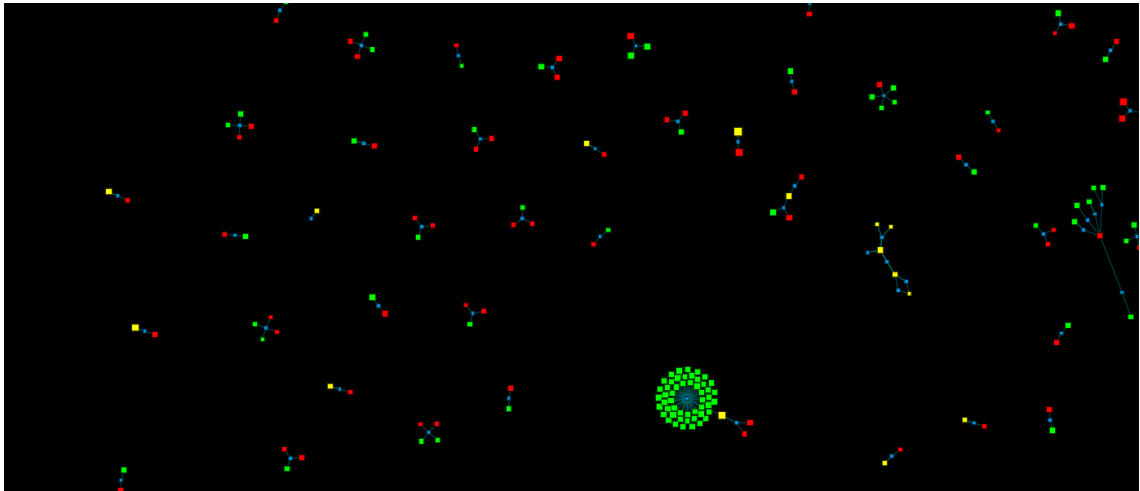
Lohkoketju on tietorakenne, jonka avulla tietoa voidaan tallentaa niin sanottuihin lohkoihin. Jokainen lohko sisältää dataa transaktioista, oman uniikin tiivisteen sekä viitteen ketjun edelliseen lohkoon. Tämän viitteen salaamiseen käytetään esimerkiksi Hash –funktioita (Bitcoinissa Sha 256 – algoritmi.) Salaustekniikat tekevät lohkojen välisestä linkistä tietoturvallisen. Lohkojen järjestys on lukittu ikään kuin ketjuksi. Näitä lohkoja on ketjussa peräkkäin käytännössä rajattomasti,

ja niitä kirjoitetaan koko ajan lisää. Näin lohkot muodostavat siis ketjumaisen rakenteen. Olennaista lohkokossa on, että siihen saadaan kirjoitettua tiedot: omistaja X on siirtänyt Bitcoinin yksiköitä omistajalle Z. Nämä transaktiot julkaistaan ja ne ovat kaikille nähtävissä koko ajan. Käyttäjät identifioidaan verkostossa lompakon uniikeilla avaimilla, eikä esimerkiksi virallisella nimellä. Kuviossa yksi on kuvattuna lohkoketjun yksittäisiä lohkoja. Lohko sisältää aina vähintään viitteen edelliseen ja seuraavaan lohkoon. Lisäksi lohkokossa voi olla transaktioon liittyvää tietoa. (Laurence, 2023)



Kuvio 1: Lohkoketju (Gupta, 2018)

Esimerkiksi Bitcoinin lohkoketjua ei ole tallennettu mihinkään yksittäiseen palvelimeen vaan sitä ylläpidetään vertaisverkkona. Käytännössä ketjun ylläpidosta vastaavat solmut. Solmuja on erilaisia: täyssolmut tallentavat koko Bitcoinin lohkoketjun historioineen. Kun uusi transaktio hyväksytään louhijisolmujen toimesta, tallennetaan se täyssolmujen Bitcoinin ketjuun. (Laurence, 2023) Jokainen täysnoodi ylläpitää siis tietoa koko lohkoketjusta, reaaliajassa päivittyen. Esimerkiksi Bitcoinin lohkoketju on tallennettu vuonna 2023 noin 13000 täyssolmulle ympäri maapalloa, mutta luvut vaihtelevat riippuen lähteistä. Kuviossa kaksi näkyy visuaalinen representaatio Bitcoinin verkostosta. Kuviossa eri väriset pisteet kuvaavat uusia transaktiota. Nämä transaktiot lisätään ketjuun varmistuksen jälkeen. (Laurence, 2023, BitcoinMagazinePro)



Kuvio 2: Bitcoin -verkoston visuaalinen representaatio. (Blockchain visualisation)

Kun Bitcoin –verkostossa tehdään transaktio, osallistuvat verkoston louhijasolmut transaktion vahvistamiseen. Transaktiota suoritettaessa varmistetaan, että omistajalla todella on omistuksessaan Bitcoinit, joita yritetään siirtää. Tämä tarkistusprosessi sisältää matemaattista laskentaa ja se vaatii laskentatehoa tietokoneelta. Näiden matemaattisten operaatioiden suorituksesta palkintona solmu voi saada pienen määrän Bitcoinia. Tätä kutsutaan louhinnaksi. Louhintaa siis samalla ylläpitää verkostoa ja sen tietoturva. (Laurence, 2023)

Lohkoketjut ovat mahdollisia konsensusprotokollien ansiosta – sääntöjärjestelmien, jotka määrittelevät, millaiset lohkot voivat liittyä ketjuun ja siten liittyä osaksi verkoston “totuutta”. Nämä protokollat on suunniteltu vastustamaan haitallista manipulaatiota tiettyyn turvarajaan asti. Keskeisenä periaatteena on työtodistus (Proof of Work, PoW) -konsensusmekanismi, joka perustuu laskennallisesti ja energialtaan intensiiviseen kryptograafisten laskutoimitusten suorittamiseen uusien lohkojen valinnassa. Tämä on toteutettu vielä niin, että louhijasolmut kilpailevat siitä, mikä solmu saa transaktion varmistettua nopeimmin. Nopeudesta palkitaan, jolloin solmujen ylläpitäjillä on taloudelliset kannustimet lisätä resursseja laskentaan (laskentatehoa), mikä johtaa myös parempaan tietoturvaan. (Harvey, Ramachandran, Santoro, 2021)

Lohkoketjussa tieto on siis avointa ja suhteellisen luotettavaa sekä todennäköisesti pysyvää. Tämä mahdollistaa uudenlaisia sovelluksia. Esimerkiksi rahan

vaihdossa, verkkokaupoissa, vakuutuslalla, kiinteistökaupoissa, palkan maksussa tai äänestyksessä lohkoketju voisi tuoda tulevaisuudessa tehokkaita ja luotettavia internetin välityksellä toimivia sovelluksia. (Laurence, 2023)

2.3 Älysopimukset

Älykkäät sopimukset ovat lohkoketjussa toimivia sopimuksia, jotka toteuttavat niihin ohjelmoitua toiminnallisuutta. Sopimuksen ehdot voidaan kirjoittaa ja tallentaa lohkoketjuun ohjelmakoodina (esimerkiksi Solidity-kieli). Näin lohkoketju voi esimerkiksi suorittaa automaattisesti halutun sopimuksen tiettyjen ehtojen täyttyessä. Tämä voi lisätä läpinäkyvyyttä ja reaaliaikaisuutta transaktioissa ja ihmisten välisessä kaupankäynnissä ja vaihtokaupassa. (Ethereum, a)

Älysopimuksien hyötyjä ovat siis automaatio, läpinäkyvyys, turvallisuus ja tehokkuus. Älysopimukset toimivat lohkoketjussa, jolloin niiden toiminta on avointa ja kaikille näkyvää, pois lukien yksityiset tiedot. Älysopimukset ovat yleensä turvallisia, koska koodia ei voida muuttaa lohkoketjun hajautetun luonteen takia. Tehokkaita ne voisivat olla koska ne poistavat kaupankäynnistä ja sopimuksen teosta välikäsiä. Ne voivat myös vähentää virheitä, koska kaikki tapahtuu automaattisesti ja tarkasti ennalta määritettyjen ehtojen mukaan. (Laurence, 2023)

Älysopimukset voisivat tuoda nykyiseen kaupankäyntijärjestelmään parannuksia. Nykyään monet kaupankäyntiin liittyvät asiat vaativat pankin tai muun vastaavan tahon palveluja. Olennaista on luottamuksen käsite. Hajautettu verkosto toteuttaa luottamuksen ennalta määritellyillä säännöillä. Voimme todennäköisesti luottaa, että rahat siirtyvät eteenpäin verkostossa, ja emme tarvitse tähän pankkia tai jotain muuta yksittäistä tahoa. (Laurence, 2023)

2.4 Oraakkeliongelma

Älykkäiden sopimusten keskeisenä rajoituksena on niiden kyvyttömyys hankkia luotettavaa reaaliaikaista tietoa lohkoketjunsä ulkopuolelta. Tämä rajoitus, joka

tunnetaan oraakkeliongelmana, johtuu lohkoketjujen suljetusta arkkitehtuurista, joka estää suoran vuorovaikutuksen ulkoisten datalähteiden kanssa. Jotkut ensimmäiset ratkaisut tähän ongelmaan käyttivät yksittäisiä keskitettyjä oraakkeleita, mikä loi haavoittuvuuksia manipulaatiolle ja yksittäisen epäonnistumispiirteen. (Harvey, Ramachandran, Santoro, 2021)

Oraakkelin tarjoaman tiedon tulisi siis olla luotettavaa, reaaliaikaista sekä tietoturvallista, jotta älysopimus pystyy toimimaan tietoturvallisesti ja luotettavasti. On helppo kuvitella huijauksia, joissa älysopimukselle lähetetään väärää tietoa, esimerkiksi hintatietoa, jolloin hyökkääjä pystyy hankkimaan taloudellista etua manipuloimalla hintaa ja sen jälkeen suorittamalla vaihtokauppoja itselle edulliseen hintaan. Chainlinkin oraakkeliverkosto on kehitetty ratkaisemaan mm. näitä ongelmia. (Ethereum, b)

3 Johdatus Chainlinkiin

Chainlink on hajautettu oraakkeliverkosto, joka mahdollistaa lohkoketjun älysopimusten tiedon saannin ulkopuolisista lähteistä.

3.1 Historia ja kehitys

Chainlinkin taustalla on Smartcontracts.com -niminen yritys, jonka perusti vuonna 2014 Sergey Nazarov. Vuonna 2017 Chainlink järjesti joukkorahoituksen, jota kutsutaan ICO:ksi. Tässä ICO:ssa Chainlink keräsi itselleen 32 miljoonan dollarin rahoituksen. Vuonna 2019 Chainlink aloitti toimintansa Ethereumin verkoston kanssa yhteistyössä. "Vuonna 2020 Chainlink koki merkittävää kasvua arvonnousun ja yhteisön käyttöönoton suhteen, kun monet hajautetun rahoituksen (DeFi) palvelut alkoivat integroida Chainlinkin oraakkelipalveluita käyttöönsä." (Coinmotion)

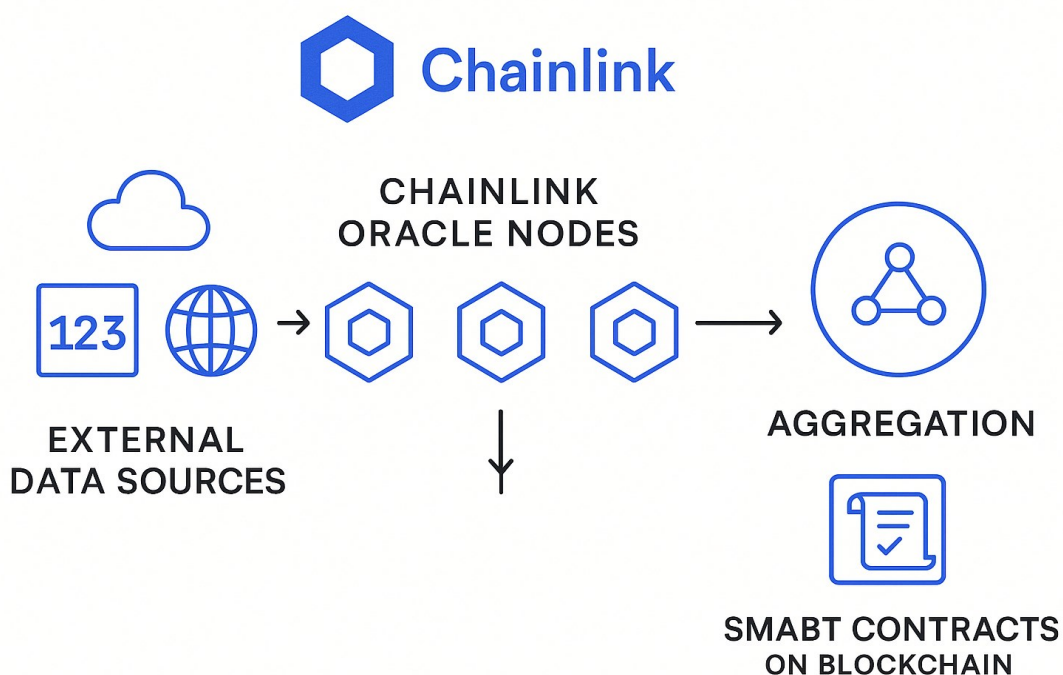
Chainlinkin kehitystä on jatkettu aktiivisesti tämän jälkeen ja tämä näkyy myös Chainlinkin tokenin LINK:in hinnassa: se on ollut yksi parhaiten suoriutuvista kryptovaluutoista hinnan ja markkina-arvon suhteen. (Coinmotion)

Kehitys on jatkunut mm. CCIP –protokollan julkaisuna 2023. Sen lisäksi Chainlink on pyrkinyt lisäämään verkoston integraatiota ja käyttöä monien erilaisten rahoitusalan toimijoiden kanssa. (Northcrypto) Chainlink on kaikista oraakkeliverkostoista yleisin ainakin markkina-arvolla mitattuna keväällä 2025. (Coinmarketcap, c)

3.2 Yleiskatsaus Chainlink verkostoon

Chainlink on hajautettu oraakkeliverkosto, jonka tarkoitus on tarjota lohkoketjun älykkäille sopimuksille luotettavaa ulkopuolista dataa. Toimintaperiaatteena on, että oraakkelit keräävät dataa monista eri verkon lähteistä, arvioiden dataa samalla. Älysopimuksen tiedon pyyntöön kerätään myös aina dataa monesta eri oraakkelista, jotta tieto on luotettavaa ja virhemarginaali vähenee. Näin ei myöskään tarvitse täysin luottaa minkään yksittäisen oraakkelin vastaukseen. Kun

tieto on kerätty monen eri oraakkelin kautta, laskee Chainlink lopullisen vastauksen, jonka tavoitteena on olla luotettava. Tässä laskennassa Chainlink voi myös käyttää monimutkaisempia parametreja, kuten mainejärjestelmää. Chainlink pitää yllä erilaisia hintoja ja tietoja jatkuvasti päivittyen. Kuviossa kolme nähdään visuaalinen representaatio Chainlinkin perustoiminnasta. Ja sen yhteyksistä tiedon lähteisiin ja älysovimuksiin. Aggregation tarkoittaa tiedon koostamista ja jäsentelyä. (Coinmotion)



Kuvio 3: Tekoälyn tuottama visuaalinen kuvaus Chainlinkin verkoston toiminnasta ja yhteyksistä muihin toimijoihin. (Perplexity AI)

3.3 Chainlinkin tärkeimmät komponentit

Chainlink voidaan jakaa erilaisiin osiin eli teknologisiin komponentteihin. Oraakkelilla tarkoitetaan yhtä tiedonlähdettä verkostolle. Yksittäinen oraakkeli on käytännössä esimerkiksi yhdellä palvelimella ajettava ohjelma. Oraakkelin tehtävä on hakea tietoa julkisista lähteistä, kuten erilaiset julkiset tietolähteet, pankkien sivut, pörssien sivut, jne. Sitten oraakkeli lähettää tietoa koko oraakkeliverkostolle, mahdollisesti myös arvioiden tiedon oikeellisuutta. (Ethereum, b)

Solmuoperaattorit ovat käyttäjiä, jotka ajavat oraakkeleita omilla palvelimillaan, eli tarjoavat verkostolle laskentatehon. Solmuoperaattorit toimivat kuin palvelimena, mahdollistaen oraakkeli-verkoston toiminnan. Operaattorit voivat saada palkkioksi LINK –tokenia. Verkostoa ylläpidetään hajautetusti ympäri maailmaa. Näin verkoston ylläpidolle on olemassa taloudellinen kannustin. Käytännössä Chainlink siis tarjoaa ohjelman logiikan ja säännöt, jotka asennetaan sitten omalle tietokoneelle ajettavaksi. Näin periaatteessa kuka tahansa voi toimia “palvelimena” ja julkisena oraakkeli-ylläpitäjänä, tarjoten oraakkeli-verkostolle dataa. Erilaisia tiedonlähteitä voivat olla mm. Erilaiset pörssit, pankkien tiedot, yms. (Chainlink, a)

Oraakkeli-verkosto on monen oraakkeliin muodostama verkosto. Kun oraakkeleista muodostetaan verkosto, saadaan monipuolisempaa ja luotettavampaa dataa. Kun tietoa kerätään monelta oraakkeliilta, laskee oraakkeli-verkosto tiedosta koosteen. Verkosto ylläpitää siis jatkuvasti ajankohtaista tietoa, jota tietoa tarvitsevat käyttäjät voivat kutsua suoraan älysovimuksissaan. Internetissä on julkisesti nähtävissä ajankohtainen verkoston ylläpitämä tieto. Siellä voi tarkastella myös esimerkiksi oraakkeliin erilaisia vastauksia, joista verkosto koostaa jonkun keskiarvon. (Chainlink, b)

Link –token on Chainlinkin vaihdettava yksikkö. Link –token on ERC677- standardia noudattava token, jota voidaan siirrellä lompakosta toiseen. Link –tokenissa erityistä onkin logiikka, miten sitä luodaan lisää. Tokeneita on rajattu määrä, ja tokeneita luodaan lisää aina silloin, kun oraakkeliit osallistuvat Chainlinkin verkoston ylläpitoon. Verkoston ylläpitäjillä on siis taloudellisia kannustimia ylläpitää verkostoa ja lisätä resursseja sen käyttöön. Tavoitteena tällaisessa logiikassa on ollut tehdä verkostosta tietoturvallinen ja hyökkäyksiä vastustava. LINK –tokenilla voidaan käydä kauppaa: sitä voidaan myydä ja sitä voidaan myös vaihtaa. (Chainlink, c) Tällaisilla säännöillä ja logiikalla Chainlinkin verkoston luojat ovat pyrkinet ohjaamaan verkostoa luotettavaan ja tietoturvalliseen toimintaan. Mitä enemmän verkostossa on hyviä toimijoita, sitä vaikeampi on manipuloida verkoston tietoa. (Chainlink, c)

Mainejärjestelmällä tarkoitetaan että verkosto määrittää kullekin solmuoperaattorille maineen perustuen mainepisteisiin. Mainejärjestelmän avulla varmistetaan tiedon luotettavuutta. Jos operaattori on tarjonnut luotettavaa tietoa, sen mainepisteet kasvavat. Näin kyseisen operaattorin vastaukset saavat suuremman painoarvon tulevaisuudessa. Tämäkin tehostaa verkoston toimintaa ja luotettavuutta. (Chainlink, b)

4 Chainlinkin tekninen arkkitehtuuri

4.1 Solmun funktiot

Jokainen yksittäinen solmu verkostossa toteuttaa muutamia tärkeitä funktioita. Yksi funktio on tiedon haku eri lähteistä. Tämä funktio voi suorittaa esimerkiksi API-kutsuja internetin välityksellä erilaisiin julkisiin tiedonlähteisiin. Toinen funktio on tiedon käsittelyä varten. Kun tietoa on haettu internetistä monesta lähteestä, suorittaa solmu operaattori tiedon käsittelyä ja koostaa saadusta tiedosta jonkun vastauksen. Kolmas funktio on tiedon lähetys. Hajautetussa oraakkeli-verkostossa tämä tieto lähetetään verkoston aggregaatio –sopimukselle, joka koostaa vastauksen monista eri oraakkeleista. (Chainlink, b)

4.2 Datan aggregaatio ja validaatio

Oraakkeli-verkosto kerää tiedon hajautetusti monelta operaattorilta, jotka ajavat oraakkeleita. Verkostossa suoritetaan aggregointifunktioita, jotka käsittelevät saatua tietoa, muodostaen tiedosta koosteen tai keskiarvon. Parametrit, jota käytetään datan validaatiossa ja aggregaatioissa voivat vaihdella ja Chainlinkin kehittäjillä on valta myös muuttaa näitä parametreja. (Chainlink, b)

Chainlinkin mainejärjestelmä on keskeinen osa tiedon validointiprosessia. Chainlink laskee operaattoreille mainepisteitä perustuen ”huonojen” vastausten määrään ja vastausten laatuun. Nämä mainepisteet vaikuttavat solmujen antamien tietojen painoarvoon tiedon käsittelyssä. Tällainen mainejärjestelmä todennäköisesti lisää kannustimia tuottaa operaattoreilla hyvää tietoa. (Chainlink, b)

5 Chainlink: käyttötapaukset kaupankäynnissä

Hajautetun rahoituksen palvelut tarkoittavat uudenlaisia lohkoketjupohjaisia rahoituspalveluja. Näillä palveluilla voi olla hyötyjä verrattuna perinteisiin pankkien säänneltyihin palveluihin. Käytännössä tarkoitetaan siis esimerkiksi rahan, pääoman ja omaisuuden siirtoa, vaihdantaa ja lainaamista. (Harvey, Ramachandran, Santoro, 2021)

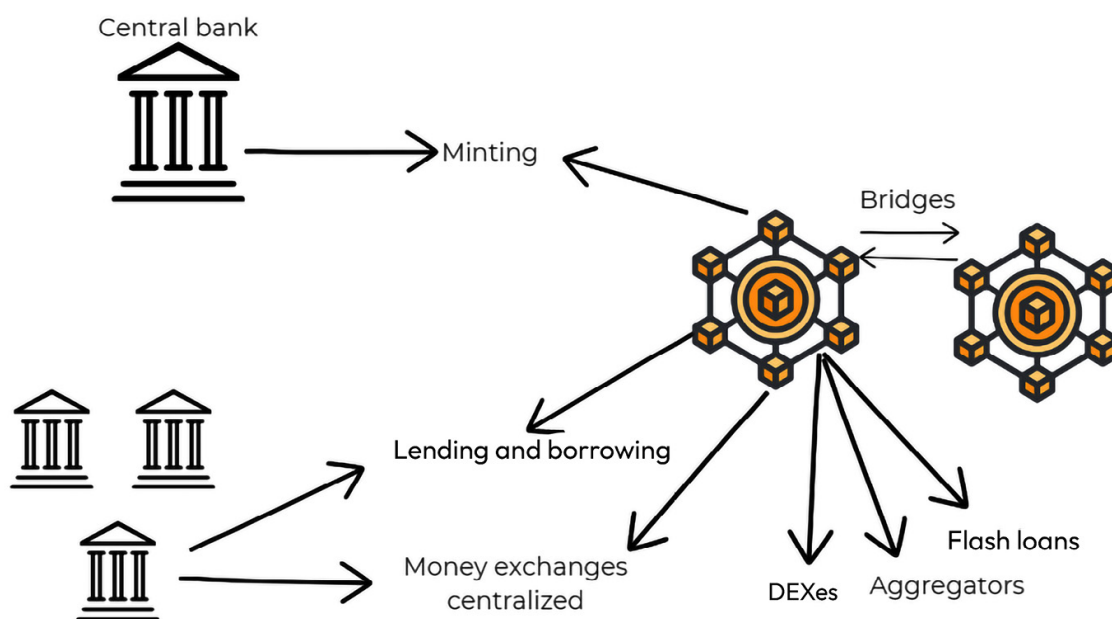
5.1 DeFi: hajautetut finanssituotteet

Defi –lyhenne tulee sanoista decentralized finance. Käyttäjälle hajautetun rahoituksen palvelu voi tarjota esimerkiksi lainauspalveluita: lainaa voi ottaa sekä omaa pääomaa voi antaa lainaksi korkoa vastaan. Lisäksi kryptovaluuttojen panostaminen korkoa vastaan voi olla mahdollista, sekä passiivisen tulon saaminen antamalla omaa kryptovaluuttaa pantiksi palvelulle. (Harvey, Ramachandran, Santoro, 2021)

Hajautetun rahoituksen sovellukset voivat olla kasvava alue tulevaisuudessa. Ne tuovat perinteisiin pankkien pyörittämään rahoitusalaan uusia sovelluksia ja palveluja. Hajautetun rahoituksen sovellukset voivat mahdollisesti tarjota rahoitusta kevyemmin, joustavammin, halvemmin ja tehokkaammin kuin esimerkiksi pankkiala. Hajautetun rahoituksen sovellukset voisivat mahdollisesti auttaa esimerkiksi pienempiä yrityksiä saamaan rahoitusta helpommin, tasavertaisemmin ja tehokkaammin. (Harvey, Ramachandran, Santoro, 2021)

Chainlinkillä on olennainen rooli hajautetun rahoituksen sovelluksissa. Rahoitus-toiminnassa on tärkeää, että älysopimuksien saama data on koko ajan ajankoh-taista. Juuri tähän ongelmaan Chainlinkin oraakkeli-verkosto tuo yhden ratkaisun. Esimerkiksi valuutan vaihto tai lainasopimuksen ylläpito tarvitsevat molemmat reaaliaikaista dataa eri valuutoiden hinnoista ja arvoista. Oraakkeli-verkosto tekee todennäköisesti hajautetun rahoituksen sovellusten toiminnasta luotettavampaa, tietoturvalisempaa sekä myös tehokkaampaa. (Harvey, Ramachandran, Santoro, 2021)

Käytännössä hajautetun rahoituksen sovellukset toimivat eri lohkoketjuissa. Käyttäjä tarvitsee aluksi yleensä jotain kryptovaluuttaa käyttäkseen näitä palveluja. Verrattuna perinteisiin finanssipalveluihin, hajautetun rahoituksen palvelut voivat tarjota käyttäjille hienostuneita ja edistyneitä rahoituspalveluja avoimesti, tasavertaisesti, läpinäkyvästi ja ehkä myös tehokkaammin, koska älysopimukset toimivat meklarin tai pankkiirin roolissa ja kaikki tapahtuu automatisoidusti. (Areco, 2023) Kuviossa 5 on kuvattuna yhteyksiä pankkien, keskuspankin ja lohkoketjun välillä. Rahaa voidaan siirtää esimerkiksi euroista ja dollareista lohkoketjuun. Lohkoketju mahdollistaa sitten mm. siltoja ja erilaisia sovelluksia, koska se toimii eri säännöillä kuin pankki. Chainlinkin rooli tässä yhteyksien verkossa on varmistaa luottamus yhteyksien välillä. Arvon siirto tai vaihdanta ei onnistuisi, jos emme voisi luottaa, että on tarjolla tasavertaista ja luotettavaa tietoa.



Kuvio 5: Perinteiset pankit ja keskuspankit ovat yhteydessä lohkoketjuun: arvoa voidaan siirtää Fiat- rahasta lohkoketjuun ja takaisin. (Areco, 2023)

Huomioitavaa on myös, että hajautetun rahoituksen tuotteet ovat uusi alue, ja niiden käyttöön liittyy myös riskejä. Näistä isoimmat ovat varmaan lailliset riskit sekä protokollien toimintaan liittyvät riskit. Laillisella riskillä tarkoitetaan esimerkiksi, että noudattavatko lainanotto -älysopimukset jotain virallisia sopimuksia ja

säännöksiä? Tämä on myös varmaankin hieman epäselvää ja uutta aluetta, mutta pahimmassa tapauksessa joku palvelu voitaisiin esimerkiksi sulkea valtion tai muun institutionaalisen toimijan toimesta, johtaen jopa käyttäjien arvon menetykseen. Toinen riski on tekninen ja teknologinen. Mitä jos koodissa on virheitä, ja rahoja katoaa ns. "bittiavaruuteen"? (Damsker, 2024)

5.2 Tokenization: oikean elämän omistuksien tokenisointi

Nimensä mukaisesti tokenization termillä tarkoitetaan oikean elämän omaisuuden siirtämistä lohkoketjuun. Siirrettävä arvokas omaisuus voi olla esimerkiksi fyysistä kultaa, yrityksen osakkeita tai jopa kiinteistöjä. Tokenisaatio toimii siten, että fyysinen omaisuus pantataan esimerkiksi holviin tai tilille tai lukitaan fyysisesti. Tähän voidaan käyttää Chainlinkin mukaan jotain kolmansiä osapuolia verifioimaan pantin arvo ja määrä. (Chainlink, d)

Kun omaisuus on pantattu oikeassa maailmassa ja verifioitu, luodaan lohkoketjuun valuuttaa fyysistä omaisuutta vastaava määrä. Tämän jälkeen voidaan alkaa käymään kauppaa tokenilla lohkoketjussa ja lohkoketjujen välillä. Sen jälkeen tokenilla on mahdollista tehdä samoja asioita kuin muilla kryptovaluutoilla, kuten pantata se korkoa vastaan, ottaa lainaa tokenia vastaan, jne. (Chainlink, d)

Chainlink voi toimia tässä kohtaa välikätenä ja tiedon varmistajana. Oikean elämän omaisuuksissa prosessi on myös erilainen riippuen omaisuuden tyypistä. On helppo kuvitella, että esimerkiksi S&P500 indeksin osakkeen omistaminen ja panttaaminen pystytään verifioimaan digitaalisesti. Tätä toteuttava palvelu on esimerkiksi backed. Backed käyttää Chainlinkin "Proof of Reserve" -protokollaa verifioimaan oikean elämän omaisuuden määrää ja arvo. Proof of reserven tarkoitus on pyrkiä varmistamaan oraakkeleiden avulla, että pantattu arvo vastaa tokenin arvoa lohkoketjussa. (Backed)

Käyttäjä ostaa backed -sivulta valitsemaansa omaisuutta kuvaavaa tokenia. Esimerkiksi S&P500 -indeksin omistusta representoivaa tokenia. Heti ostotapahtuman tapahduttua Backed ostaa pörssimeklarilta/palvelusta ostettua tokenia vas-

taavaa indeksiä tai osaketta. Tämän jälkeen käyttäjälle luodaan tätä uutta tokenia, esim. BSPC ja ostetut oikean maailman osakkeet lukitaan backed –yrityksen tilille suhteessa 1:1. Backed toimii kuin holvina, joka säilyttää digitaalisen representaation S&P500 –indeksin osakkeesta. Ulkopuolinen The Network Firm saa lukuoikeuden backed –palvelun tileille, josta varmistetaan osakkeen osto. Tätä valvontaa suoritetaan koko ajan niin, että varmistetaan lohkoketjussa olevan tokenin vastaavuus holvin sisältöön 100%. Chainlinkin oraakkeli-verkostolle lähetetään tiedot The Network firmistä. Chainlink alkaa monitoroimaan sitä, että tilillä on koko ajan oikea määrä osakkeita, perustuen The Network Firmiltä saamiin tietoihin. (Major, 2025)

Tämän jälkeen Chainlinkin oraakkelit osallistuvat myös hinnan oikeellisuuden ylläpitoon jatkuvasti päivittyen. Chainlinkin oraakkeli-verkosto pitää siis yllä hintatietoa esimerkiksi S&P500 -indeksistä. Kun tokenit on luotu, käyttäjä omistaa ne ja pystyy sitten vaihtelemaan niitä vapaasti eri lohkoketjujen välillä. Käyttäjä saattaa myös päättää vain omistaa näitä tokeneita, koska niiden arvohan nousee jos indeksit nousevat ja päinvastoin. Näiden tokeneiden vaihdanta –arvon pitäisi siis teoriassa koko ajan seurata pantatun oikean elämän omaisuuden arvoa.

6 Chainlink 2.0: kehitys ja edistyneemmät mekanismit

Chainlink on ottanut strategiakseen ratkaista tietoturvallisuuden ja lohkoketjujen välisen yhteyden parantamisen ongelmia. Chainlink olisi oman visionsa mukaan iso verkosto, joka yhdistää perinteistä rahoitusalaan, kuten pankkeja ja valtiollisia toimijoita uudempiin lohkoketjupohjaisiin markkinoihin. (Chainlink, e)

6.1 Oraakkeliriski

Koska oraakkeleilla on niin tärkeä rooli lohkoketjupohjaisissa sovelluksissa (kuten DeFi), sisältyy niiden käyttöön myös riskejä. “Oracles represent significant risks to the systems they help support. If an oracle's cost of corruption is ever less than an attacker's potential profit from corruption, the oracle is extremely vulnerable to attack.” (Harvey, Ramachandran, Santoro, 2021). Tämä tarkoittaa, että jos hyökkääjällä on mahdollisuus tehdä taloudellista voittoa hyökkäämällä ja manipuloimalla oraakkeleita, niin sitä tullaan todennäköisesti hyödyntämään. Oraakkeliverkoston toiminta täytyy siis suunnitella erittäin tietoturvalliseksi, jos halutaan suojautua hyökkäyksiltä.

Chainlink on “API-oraakkeli”, tämä tarkoittaa, että lohkoketjun on käytännössä vain luotettava siihen, että tieto mitä Chainlinkistä saadaan, on oikeaa ja luotettavaa. Toki älysovimukseen voidaan varmaankin ohjelmoida joitain tietoturva ja riskin käsittely mekanismeja sisäänkin. Chainlink kuitenkin hoitaa tiedon käsittelyn ja laskennan erillisenä, omana toimijana. Tähän sisältyy manipulaation riski. Hyökkääjä voisi iskeä juuri oraakkeliverkoston tavoitteena saada taloudellista etua manipuloimalla esimerkiksi hintatietoa. Tätä riskiä kutsutaan oraakkeliriskiksi. (Harvey, Ramachandran, Santoro, 2021)

“Front-running” tarkoittaa, että joku toimija tai botti voi hyötyä tiedossa olevasta tulevasta hintamuutoksesta. Näin on Chainlinkin historiassa tapahtunutkin monesti. Hajautettujen finanssipalveluiden (DeFi) maailmassa huijaukset ja manipulaatiot ovat olleet yleisiä tapahtumia. (Harvey, Ramachandran, Santoro, 2021)

6.2 Tietoturvallisuusmekanismit

Chainlink 2.0 -strategiassaan (2021) Chainlink on määritellyt uusia strategioita ja kehityskohtia myös tietoturvallisuuden alueella. Tavoitteena on luoda panttaus - systeemi. Käytännössä tämä tarkoittaa, että verkoston ylläpitäjät sekä Link-tokenin omistajat voivat panostaa omia Link -tokeneitaan pantiksi, samalla lisäten verkoston luotettavuutta. Panttaamisessa tokenit lukitaan, ja kun ne haluaa takaisin käyttöön, on usein määritelty joku aika, esimerkiksi 28 päivää, ennen kuin ne saa takaisin käyttöön. (Gemini, 2023)

Solmuoperaattorin ylläpitäjä voi saada panostukselleen korkoa. Tämä edellyttää, että solmuoperaattorin ylläpitäjä varmistaa, että palvelin toimii koko ajan luotettavasti ja tehokkaasti. Näin siis koko verkostoa ohjataan tietoturvallisempaan toimintaan taloudellisen kannustimen avulla. Jos jonkin operaattorin toiminnassa havaitaan toistuvasti virheellistä tietoa, tai se on paljon pois päältä, voidaan solmua rangaista "slashing" -mekanismilla. Slashing tarkoittaa, että pantattuja Link-tokeneita otetaan käyttäjältä pois rangaistuksena epäonnistuneesta tai väärästä toiminnasta. (Exponential, 2024)

6.3 Sillat ja CCIP

Kryptovaluuttojen maailmassa taloudellinen arvo on jakautunut moniin eri lohkoketjuihin. Ongelmana on ollut eri lohkoketjujen välinen kommunikaatio ja taloudellisen arvon vaihtaminen ja siirto lohkoketjujen välillä. (Phantom) Ennen tämä on tehty esimerkiksi lähettämällä kolikoita omasta lompakosta kryptopörssiin, jossa tehdään vaihto, jonka jälkeen toiset kolikot sitten lähetetään takaisin omaan lompakkoon. Tässä prosessissa käyttäjä voi menettää paljonkin taloudellisesta arvostaan, riippuen lähetyskuluista, kaasumaksuista ja vaihdantakuluista pörssissä. (Phantom) Kun käyttäjä haluaa vaihdella valuuttoja toisiin ja jopa ketjuista toisiin lohkoketjuihin, voidaan hyödyntää myös siltoja. Siltojen avulla taloudellista arvoa voidaan siirtää lohkoketjusta toiseen, käyttämättä jotain kolmannen osapuolen pörssiä. (Phantom)

Sillat on mahdollistettu käyttäjälle esimerkiksi “Lock and mint”, “Burn and mint” tekniikoiden ja likviditeettialtaiden avulla. Lock and mint tarkoittaa, että kun arvoa siirretään lohkoketjusta toiseen, tapahtuu lähtöketjussa tokenien lukkiutuminen, ja käyttäjä saa tavoiteketjussaan vastaavan määrän “paketoituja” tai “synteettisiä” kolikoita. (Across) Prosessin palauttaminen toiseen suuntaan vapauttaa alkupe- räiset tokenit. Burn and mint tarkoittaa, että lähtöketjussa “poltetaan” eli tuhotaan tietty määrä tokeneita, ja vastaava määrä (yleensä mitattuna tokenien myyntiar- volla sillä hetkellä) tokenia luodaan toisessa lohkoketjussa. (Chainlink, e)

CCIP –protokollan keskeinen periaate on, että se toimii hajautettuna verkostona. Sillan yhteydessä toimii myös erillinen riskin hallinta verkosto, joka monitoroi sil- lan toimintaa. Chainlinkin CCIP –protokolla on yhteensopiva Ethereum ERC-20 standardin kanssa. Tämä tarkoittaa, että se on yhteensopiva monien Ethereum pohjaisten lohkoketjujen ja sovellusten kanssa. Samalla Chainlink on julkaissut oman standardinsa: CCT –standard. CCIP –verkostoon liittyvien lohkoketjujen täytyy täyttää tietyt ehdot jotta se toimii yhdessä tässä Chainlink –pohjaisessa vaihdantaverkostossa, ja voidaan liittää siihen. (Chainlink, e)

Tässä yhteydessä on mielestäni hyvä muistaa, että CCIP –protokolla kilpailee tavallaan myös Kryptopörssien kanssa käyttäjistä. Perinteisesti valuuttoja on pys- tytty vaihtamaan käyttämällä pörssijä (esim. Binance tai Coinbase). Tämä saat- taan olla yksittäiselle käyttäjälle edelleen helpoin vaihtoehto. Chainlinkin kehittämä CCIP –protokolla onkin suunnattu enemmän kehittäjille, jotka haluavat kehittää uudenlaisia sovelluksia, rakentaen vanhan teknologian “päälle”. Tämä protokolla voi mahdollistaa joitain ihan uusia käyttötapauksia mitä emme vielä ole nähneet. Toisaalta käyttäjälle on myös nyt jo käytössä joitain CCIP:tä tukevia applikaati- oita, joissa voidaan vaihtaa joitain kolikoita toisiin, esimerkiksi transporter -si- vusto. Käytännössä nämä sillat ovat siis jo toiminnassa. (Chainlink, e; Transpor- ter)

7 Tekninen analyysi: Aave-protokollan Chainlink –integraatio

7.1 Historia ja konteksti

Aave protokolla on esimerkki hajautetun rahoituksen palvelusta. Aave on julkaistu toimintaan vuonna 2020. Aaveen julkaisun jälkeen Chainlinkillä on ollut merkittävä rooli Aaveen toiminnassa. Aave tukee monia eri lohkoketjuja. Suurimpia valuuttoja 7.4.2025 Aaveen digitaalisissa holveissa ovat mm. ETH, USDT (Tether), WBTC (paketoitu bitcoin) ja USDC (Usd coin) Aaveen keskeisimmät palvelut ovat lainan myöntäminen ja laina valuutan tarjoaminen korkoa vastaan. (Harvey, Ramachandran, Santoro, 2021)

Aave protokolla on yksi suosituimmista ja suurimmista DeFi –protokollista, jos mitataan käyttöä esimerkiksi lukitun taloudellisen arvon määrällä. Aaveen oman sivun mukaan 1.4.2025 Aave –protokollan verkostoon on lukittuna noin 27 miljardin dollarin arvosta likvideettiä. Tämä likvideetti on jakautunut mm. Ethereumiin ja muihin lohkoketjupohjaisiin verkostoihin joita Aave tukee. (Harvey, Ramachandran, Santoro, 2021, Aave)

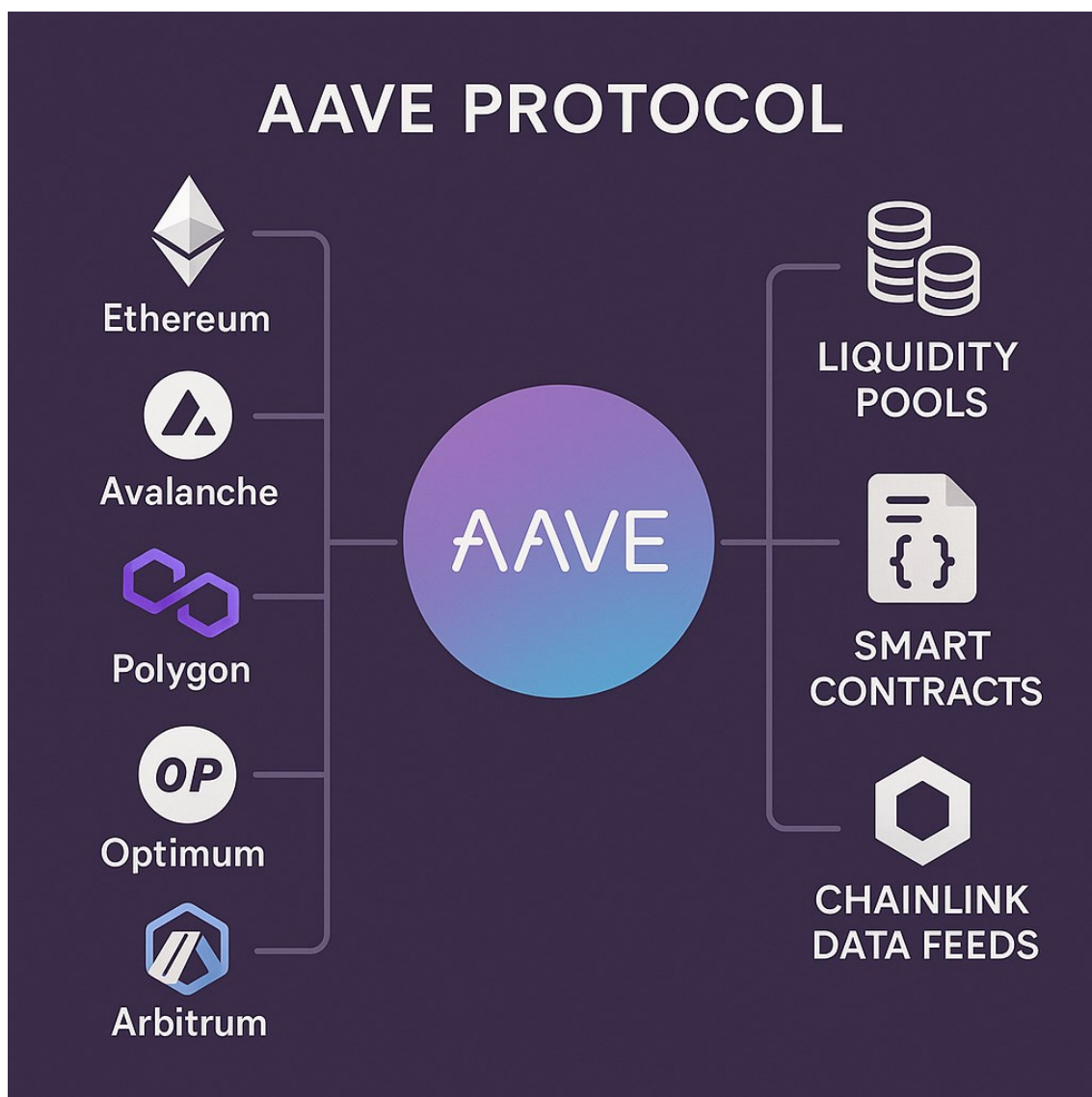
7.2 Toiminta

Aaveen toiminta perustuu siihen, että käyttäjät lukitsevat omistamiaan kryptovaluuttoja Aaveen ylläpitämiin älysopimuksiin, saaden palkinnoksi jotain korkoa panostukselleen. Näitä lukittuja tokeneita voidaan sitten lainata eteenpäin toisille käyttäjille. Näin Aave ylläpitää likvideettialtaita. Monesti lainan ehdot ja korot määräytyvät likvideettialtaan parametrien (kysynnän ja tarjonnan) mukaan. Esimerkiksi jos jostain tokenista on pulaa, voi sitä panttaamalla saada parempaa korkoa. (Aave)

Chainlinkin hintasyötteet toimivat Aaveen tärkeimpänä datan lähteenä. Chainlinkin tarjoaman luotettavan tiedon avulla pyritään turvaamaan Aaveen toiminta luotettavana ja tietoturvallisena. Käytännössä Aaveen älysopimukset hakevat tietoa jatkuvasti Chainlinkin verkostolta. Riskinä Aaveen toiminnalle olisi esimerkiksi hintojen manipulaatio ja näin taloudellinen hyväksikäyttö. Chainlinkin tavoitteena

on estää tämä hintojen manipulaatio ja varmistaa, että Aave toimii luotettavasti ja tietoturvallisesti. (Etherscan –sivusto)

Aave käyttää myös hyödykseen edellisessä kappaleessa käsittelemiämme siltoja. Tämä mahdollistaa käyttäjälle esimerkiksi yhden tokenin panttaamisen ja jonkun toisen tokenin lainaamisen toisessa lohkoketjussa. Aave suorittaa kaiken logiikan käyttäjän puolesta taustalla älysopimuksien avulla. Näin Chainlink on hyvin läheisesti mukana koko Aaveen toiminnassa. CCIP- teknologian myötä Aave on julkaissut myös oman tokeninsa, GHO. Kuviossa kymmenen näemme tekoälyn luoman visuaalisen kuvauksen Aave –protokollan toiminnasta ja yhteyksistä. Vasemmalla näkyvät lohkoketjut ovat kaikki Aaveen tukemia. Oikealla kuviossa näkyvät keskeiset osat koko Aave –protokollan toiminnassa: likviditeettialtaat, älysopimukset ja Chainlinkin luotettavat datasyötteet. Lopputuloksena käyttäjälle mahdollistuvat joustavat rahoituspalvelut Aaveen applikaation kautta. (Chainlink, f)



Kuvio 10: Tekoälyn luoma visuaalinen kuvaus Aaveen toiminnasta Lohkoketjuissa. (ChatGPT, 2025)

8 Pohdinta

Chainlinkin teknologian ytimessä on sen kyky tuoda lohkoketjun älykkäille sopimuksille ulkopuolista, luotettavaa dataa. Tämä tiedon luotettavuus on mahdollistanut uudenlaisia sovelluksia. Chainlink eliminoi siis virheitä lohkoketjujen toiminnasta ja kommunikaatiosta. Ennen Chainlinkin kehitystä yksi lohkoketjujen toiminnan epävarmuus olivat yksittäiset virhetiedot. Chainlinkin oraakkeliverkoston hajautettu luonne ratkaisee tuon ongelman, tehden älysopimusten datasta luotettavaa.

Hajautus ja tietoturvallisuus ovat mielestäni muutenkin monen lohkoketjun toiminnan kantavana periaatteena. Chainlink toteuttaa näitä periaatteita myös lohkoketjulle saatavan ulkopuolisen datan osalta. Tämä voi tehdä lohkoketjujen toiminnasta luotettavampaa. Periaatteena usein lohkoketjuissa on pidetty, että meidän ei tarvitsisi luottaa yksittäiseen instituutioon tai keskusvaltaan, vaan luottamus hajautetaan verkostolle. Säännöt voitaisiin luoda ehkä alunperin sellaisiksi, että verkosto tukee ja mahdollistaa luotettavaa kaupankäyntiä.

Mielestäni Chainlink vaikuttaa verkostolta, joka ainakin tukee jo olemassa olevien ja toimivien lohkoketjujen toimintaa. Vaikka teknisesti lohkoketjut ovat kyllä mielenkiintoinen järjestelmä, se ei mielestäni automaattisesti tarkoita sitä, että se olisi jotenkin parempi kuin nykyinen kaupankäyntijärjestelmä.

Luulen, että hajautetun kirjanpidon järjestelmät ovat sellaisia, joita voidaan kyllä hyödyntää ja tullaankin hyödyntämään joissain käyttötapauksissa. Tällä hetkellä näyttää siltä, että lohkoketjuverkostot muodostavat monimutkaisen järjestelmän, jossa liikkuu rahaa. Ajan myötä varmaan nousevat sellaiset teknologiat suosioon, jotka voivat oikeasti hyödyttää ihmisiä.

LÄHTEET

Aave price oracle. N.d. Etherscan.io. Live-sivu oraakkelista. Lohkoketju. Viitattu 2.5.2025

<https://etherscan.io/address/0xa50ba011c48153de246e5192c8f9258a2ba79ca9>

Aave. N.d. Aave governance. Äänestys. Viitattu 02.05.2025

<https://app.aave.com/governance/v3/proposal/?proposalId=120>

Across. 14.01.2025. The Complete Guide to Crypto Bridges: Moving Assets Across Chains Made Simple. Viitattu 2.5.2025

<https://across.to/blog/complete-guide-to-crypto-bridges>

Areco, G.C. 2023. Data Science for Web3: A Comprehensive Guide to Decoding Blockchain Data with Data Analysis Basics and Machine Learning Cases. Packt Publishing, Limited

Backed. N.d. Proof of reserves. Verkkosivu. Viitattu 02.05.2025

<https://defi.backed.fi/proof-of-reserves>

Bitcoin Magazine Pro. 3.9.2024. Complete Guide to Bitcoin Nodes and How They Work. Viitattu 08.04.2025

<https://www.bitcoinmagazinepro.com/blog/complete-guide-to-bitcoin-nodes-and-how-they-work/>

Chainlink, a. n.d. Operator. Chainlink Docs. Viitattu 02.05.2025

<https://docs.chain.link/chainlink-nodes/contracts/operator>

Chainlink, b. n.d. What Is a Blockchain Oracle? Viitattu 02.05.2025.

<https://chain.link/education/blockchain-oracles>

Chainlink, c. n.d. LINK Token Contracts. Chainlink DevHub. Viitattu 02.05.2025

<https://docs.chain.link/resources/link-token-contracts>

Chainlink, d. 5.9.2024 Asset Tokenization: What It Is and How It Works. Chainlink Education. Viitattu 02.05.2025

<https://chain.link/education/asset-tokenization>

Chainlink, e. n.d. Cross-Chain Token (CCT) standard. Chainlink DevHub. Viitattu 02.05.2025

<https://docs.chain.link/ccip/concepts/cross-chain-tokens>

Chainlink, f. 17.6.2023. Chainlink CCIP Launches on Mainnet With DeFi Leaders Synthetix and Aave as Early Adopters. Prnewswire. Viitattu 2.5.2025

<https://www.prnewswire.com/news-releases/chainlink-ccip-launches-on-mainnet-with-defi-leaders-synthetix-and-aave-as-early-adopters-301878092.html>

ChatGpt. Dall-E. 2025. Kuva generoitu 2.5.2025. (

[Chatgpt.com](https://chatgpt.com)

Coinmarketcap a. n.d. Today's Cryptocurrency Prices by Market Cap. Viitattu 08.04.2025

<https://coinmarketcap.com/>

Coinmarketcap b. n.d. Bitcoin Dominance. Coinmarketcap. Viitattu 08.04.2025

<https://coinmarketcap.com/charts/bitcoin-dominance/>

Coinmarketcap c. n.d. Today's Cryptocurrency Prices by Market Cap. Viitattu 08.04.2025

<https://coinmarketcap.com/>

Coinmotion. 23.01.2023. Chainlink (LINK) - opas sijoittamiseen. Coinmotion. Viitattu 23.05.2024.

<https://coinmotion.com/fi/chainlink-link-aloittelijan-opas/>

Damsker, A. 2024. Understanding DeFi. O' Reilly.

Ethereum, a. n.d. Introduction to smart contracts. Ethereum Docs. Viitattu 06.06.2024

<https://ethereum.org/en/developers/docs/smart-contracts/>

Ethereum, b. n.d. Oracles. Ethereum docs. Viitattu 8.4.2025

<https://ethereum.org/fi/developers/docs/oracles/>

Exponential.fi. 06.06.2024. What is Chainlink staking? Exponential.fi. Artikkel. Viitattu 27.03.2025

<https://exponential.fi/blog/what-is-chainlink-staking>

Gemini. 2023. Chainlink 2.0: Advanced Decentralized Oracle Networks. Cryptopedia, Gemini. Artikkel. Viitattu 25.03.2025

<https://www.gemini.com/cryptopedia/chainlink-staking-link-crypto-chainlink-smart-contracts-update>

Github. N.d. Blockchain visualisation. Viitattu 09.04.2025

<https://dailyblockchain.github.io/>

Gupta, M. 2018. Blockchain for Dummies, 2nd edition. E-kirja. John Wiley & Sons.

Harvey, R. Campbell, Ashwin Ramachandran, Joey Santoro 2021. DeFi and the Future of finance. E-kirja. Wiley.

Laurence, T. 2023. Blockchain for dummies. E-kirja. O' Reilly.

Major, J. 2025 Backed integrates Chainlink Proof of Reserves to strengthen transparency in tokenized assets. FinBold. 27.9.2023. Viitattu 10.4.2025.

<https://finbold.com/backed-integrates-chainlink-proof-of-reserves-to-strengthen-transparency-in-tokenized-assets/>

Northcrypto. N.d. Mikä on Chainlink? Viitattu 24.03.2025

<https://www.northcrypto.com/fi/learn/about/chainlink>

Perplexity Ai. Tuotettu 2.5.2025. Kuvio. Generoitu sanoilla: “generate a visual simple representation of data flow model of chainlink”

<https://www.perplexity.ai/>

Phantom. N.d. What is a crypto bridge?. Viitattu 26.03.2025

<https://phantom.com/learn/crypto-101/crypto-bridge>

World economic forum. I.c. Boston consulting group. 2021. Digital Assets, Distributed Ledger Technology, and the Future of Capital Markets. World economic Forum. Raportti. Viitattu 07.04.2025

<https://www.weforum.org/publications/digital-assets-distributed-ledger-technology-and-the-future-of-capital-markets/>