Satu Kauppinen

LOHKOKETJUTEKNOLOGIAPOHJAISET ÄLYKKÄÄT SOPIMUKSET FINANSSIALALLA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Kauppinen, Satu
Lohkoketjuteknologiapohjaiset älykkäät sopimukset finanssialalla
Jyväskylä: Jyväskylän yliopisto, 2022, 27 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Lampi, Anna

Lohkoketjuteknologia on verrattain uusi teknologia. Tämä tutkimus tehtiin kuvailevana kirjallisuuskatsauksena ja pyrki selvittämään, miten lohkoketjuteknologiaa hyödynnetään tällä hetkellä finanssialalla, ja millaisia mahdollisuuksia ne tuovat sekä millaisia haasteita älykkäisiin sopimuksiin liittyy. Lohkoketjuteknologiapohjaiset älykkäät sopimukset ovat nekin kohtuullisen uusia ja kehitysvaiheessa. Jotta älykkäistä sopimuksista saataisiin kaikki hyöty irti, ne vaativat vielä paljon tutkimista ja kehittämistä huonojen ominaisuuksien poistamiseksi ja ratkaisemiseksi. Älykkäät sopimukset ovat nyt jo käytössä monilla aloilla, sillä ne mahdollistavat luotettavan tavan tehdä sopimuksia.

Lohkoketjuteknologiaa sovelletaan jo laajalti finanssialalla esimerkiksi pankeissa sekä alustoina kryptovaluutoille ja älykkäille sopimuksille. Lohkoketjuteknologiaan pohjautuvia älykkäitä sopimuksia voidaan hyödyntää finanssialalla monissa toiminnoissa, esimerkiksi asuntokaupoissa. Lohkoketjuteknologiapohjaiset älykkäät sopimukset tuovat monia etuja finanssialalle, kuten kustannusten pienenemisen sekä luottamuksen lisääntymisen osapuolten välille. Lohkoketjuteknologian ansiosta kaikki tiedot tallentuvat muuttumattomana ja luotettavasti ilman kolmannen osapuolen tarvetta. Kaikista tapahtumista jää peruuttamaton jälki, joten huijaamisen mahdollisuus on pystytty poistamaan.

Tulevaisuuden näkymät ovat lupaavat, mikäli lohkoketjuteknologian ongelmat saadaan ratkaistua. Lohkoketjuteknologian suurimpia ongelmia ovat huono skaalautuvuus, turvallisuus, oikeudelliset kysymykset, muuttumattomuus sekä konsensusmekanismit.

Lohkoketjuteknologiapohjaisilla älykkäillä sopimuksilla on paljon potentiaalia tulevaisuudessa finanssialalla, mikäli lohkoketjuteknologian ongelmat saadaan poistettua tai tilalle saadaan kehitettyä sopivampi teknologia.

Asiasanat: Lohkoketju, lohkoketjuteknologia, älykäs sopimus, finanssiala

ABSTRACT

Kauppinen, Satu
Blockchain based smart contracts in the financial sector
Jyväskylä: University of Jyväskylä, 2022, 27 pp.
Information systems, bachelor's thesis
Supervisor(s): Lampi, Anna

Blockchain technology is a relatively new technology. This research was done as a descriptive literature review and aimeds to find out how blockchain technology is currently being used in the financial sector, and what kind of opportunities they bring and what kind of challenges are associated with smart contracts. Smart contracts based on blockchain technology are also fairly new and in the development phase. In order to get the most out of smart contracts, they still require a lot of research and development to remove and solve bad features. Smart contracts are already in use in many fields, as they enable a reliable way to make contracts.

Blockchain technology is already widely used in the financial sector, for example in banks and as platforms for cryptocurrencies and smart contracts. Smart contracts based on blockchain technology can be used in many functions in the financial sector, for example in housing transactions. Smart contracts based on blockchain technology bring many benefits to the financial sector, such as reducing costs and increasing trust between the parties. Thanks to blockchain technology, all data is stored unchanged and reliably without the need for a third party. All events leave an irreversible trace, so the possibility of cheating has been eliminated.

The prospects for the future are promising, if the problems of blockchain technology can be solved. The biggest problems with blockchain technology are poor scalability, security, legal issues, immutability and consensus mechanisms. Smart contracts based on blockchain technology have a lot of potential in the future in the financial sector, if the problems of blockchain technology can be eliminated or a more suitable technology can be developed instead.

Keywords: blockchain, blockchain technology, smart contract, finance sector

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tässä tutkielmassa käydään läpi lohkoteknologiapohjaisia älykkäitä sopimuksia, niiden toimintaa ja mahdollisuuksia tulevaisuudessa. Aiheeksi on rajattu älykkäiden sopimusten tarkastelu finanssialalla.

Lohkoketjuteknologia on tapa, jolla voidaan yhdistää vanhoja, jo olemassa olevia teknologioita toisiinsa, kuten esimerkiksi kryptografiaa, salausta sekä vertaisverkkoja (Nakamoto, 2008). Lohkoketjut ovat hajautettuja, jaettuja ja läpinäkyviä tietokantoja. Lohkoketjuteknologia antaa pohjan luotettaville älysopimuksille. Älykkäät sopimukset vievät lohkoketjut vielä pidemmälle, sillä ne antavat mahdollisuuden luoda koodia sisälle lohkoketjuun. (Haque, Hasan & Zihad, 2021.)

Lohkoketjuteknologiapohjaisia älykkäitä sopimuksia on jo paljon käytössä. Pankeissa lohkoketjuteknologiapohjaisia älykkäitä sopimuksia voidaan hyödyntää esimerkiksi asuntokaupoissa, lainojen myöntämisessä, maksujen automatisoinnissa, raportoinneissa, apuna tietokantojen ylläpidossa sekä arvopaperikaupassa. Vakuutusyhtiöt käyttävät älykkäitä sopimuksia tehostamaan vakuutuskorvausten käsittelyprosessia. (Desplebin, Lux & Petit, 2021.)

Älykkäiden sopimusten ansiosta yleisiä sopimuksien ongelmia pystytään automatisoimaan ja ratkaisemaan ilman luottamuksellista kolmatta osapuolta. Lohkoketjuteknologiaa ja sen sovelluksia on jo käytössä, mutta laajempi käyttöönotto vaatii itse teknologian tutkimista ja sitä kautta sen haasteiden ja riskien poistamista tai ratkaisemista. (Shaik ym., 2020.)

Tutkimuksen pyrkimyksenä on selvittää, miten lohkoketjuteknologiapohjaisia älykkäitä sopimuksia on mahdollista hyödyntää ja soveltaa, sekä millaisia haasteita lohkoketjuteknologiapohjaisiin älykkäisiin sopimuksiin liittyy. Tarkoituksena on kertoa lohkoketjuista ja kuvata lohkoketjuteknologian sovelluksia finanssialalla sekä miten älykkäät sopimukset toimivat ja millaisia mahdollisuuksia ja riskejä ne tuovat. Pyrin saavuttamaan tutkimuksen tavoitteet vastaamalla kolmeen seuraavaan tutkimuskysymykseen:

- Miten lohkoketjuteknologiaa sovelletaan finanssialalla?

- Miten älysopimuksia voi soveltaa ja mitkä ovat niiden mahdollisuudet finanssialalla?
- Millaisia haasteita sekä riskejä älykkäisiin sopimuksiin liittyy?

Ensimmäisen tutkimuskysymyksen tavoitteena on selvittää, miten lohkoketjuteknologiaa hyödynnetään tällä hetkellä finanssialalla. Toisen tutkimuskysymyksen tavoite on saada selville, millaiset tulevaisuuden näkymät lohkoketjuteknologiapohjaisilla älykkäillä sopimuksilla on. Aihe on rajattu finanssialan älykkäisiin sopimuksiin, jotta tutkielmasta ei tule liian laaja, sillä älykkäitä sopimuksia hyödynnetään monilla eri aloilla. Kolmannen tutkimuskysymyksen tavoite on selvittää haasteita ja riskejä lohkoketjuteknologiapohjaisten älykkäiden sopimusten käyttöönottoon ja hyödyntämiseen liittyen. Tarkoitus on keskittyä älykkäiden sopimusten teknologian ongelmiin, esimerkiksi mitkä tekijät vaikeuttavat tai hidastavat teknologian käyttöönottoa ja näin ollen hidastavat älykkäiden sopimusten yleistymistä. Tutkimuksessani en keskity teknologian tarkasteluun ja tutkimiseen kovin syvällisesti, jottei tutkimuksesta tulisi liian tekninen tai vaikeaselkoinen. Tutkimukseni tavoitteena on selvittää lohkoketjuteknologiapohjaisten älykkäiden sopimusten mahdollisuuksia sekä haasteita finanssialalla.

Tutkimus on toteutettu kuvailevana kirjallisuuskatsauksena. Salmisen (2011) määrittelemänä kuvailevassa kirjallisuuskatsauksessa tutkimuskysymykset voivat olla väljiä, hyödynnetyt aineistot voivat olla laajoja, eikä aineiston valintaa rajata tiukasti. Pyrkimyksenä tutkielmassani on ollut etsiä mahdollisimman monipuolisesti erilaista tutkimustietoa sekä mahdollisimman tuoreita tutkimuksia, jotta tutkimus olisi mahdollisimman ajankohtainen ja sisältäisi tuoretta ja todenmukaista tietoa. Tutkimuksen lähteistä suurin osa on julkaistu vuosina 2018–2022. Tutkimuksia lohkoketjuteknologiaan ja älykkäisiin sopimuksiin liittyen löytyy tällä hetkellä kattavasti ja riittävästi, jotta koin tutkielmani onnistuvan. Tutkimusten hakemisen aloitin hakusanoilla, kuten lohkoketjuteknologia, finanssiala, älykkäät sopimukset, blockchain technology, blockchain in finance, smart contracts. Lähteitä hain Google Scholarin kautta sekä erikseen lehdestä IET eli ”Institution of Engineering and Technology”.

Tutkimuksia löytyi useita. Valitsin syvempään tarkasteluun tutkimuksia otsikoiden ja vuosilukujen mukaan 60 kappaletta. Niistä valikoin tiivistelmien ja sisältöjen perusteella sopivimmat, joihin syvennyin enemmän. Jäljelle jäi 22 tutkimuslähdettä, joita hyödynsin tutkielmassani. Tutkimuksen edetessä hain lähteitä vielä muutaman lisää, sillä syvennyttyäni tutkimusaiheeseen muovasin ensimmäistä tutkimuskysymystäni.

1.1 Käsitteet

Finanssiala kattaa esimerkiksi erilaisia pankkipalveluita, vakuutuksiin liittyviä asioita sekä sijoittamisen palveluita. Kehittynyt teknologia mahdollistaa finanssialan eri toiminnot. (Tapscott & Tapscott, 2017.)

Lohkoketju on lohkoketjuteknologian osa, joka koostuu monista peräkkäisistä tietolohkoista. Uusia lohkoja ketjuun muodostavat solmut eli koneet, jotka toimivat hajautetussa vertaisverkossa. Jokainen uusi lohko tallentaa viimeisimmät tapahtumatiedot ja muutokset. Lohkoketjut ovat hajautettuja, jaettuja ja läpinäkyviä tietokantoja. Lohkoketjuista muodostuvaa teknologiaa kutsutaan lohkoketjuteknologiaksi. (Nakamoto, 2008.)

Älykkäät sopimukset ovat hajautetuissa verkoissa toimivia ohjelmia. Ohjelman solmut tallentavat tiedot lohkoketjujen muodossa. Lisäksi on olemassa älykkäitä sopimuksia, jotka eivät perustu lohkoketjuteknologiaan. Lohkoketjuteknologiapohjaiset älykkäät sopimukset poistavat tarpeen luotettavalle kolmannelle osapuolelle, jonka yleensä normaalien opimusten tekeminen vaatii. Sopimukset ja tapahtumat voidaan suorittaa suoraan osapuolten välillä luottamuksellisesti. Sopimuksien jokainen vaihe tallentuu muuttumattomana tietona osaksi lohkoketjua. (Deng, Cheng, Zhao, Gao & Yin, 2020.)

”Proof-of-stake” on yksi konsensusprotokollista eli tiedon siirron varmistustavoista. Verkon siirrot varmistetaan asettamalla panos. Lohkoketjun varmistaja valikoituu sattumanvaraisesti, jolloin suuremman panoksen laittanut pääsee todennäköisimmin varmistamaan uuden lohkon. (Ahmad, Alabduljabbar, Saad, Nyang, Kim & Mohaisen, 2021.)

”Peer-to-Peer” muodostuu joukosta tietokoneita, jossa kaksi tai useampi koneista on linkitetty yhteen. Ne jakavat resursseja ilman erillistä palvelintietokonetta. Linkitetyillä koneilla on samat luvat ja vastuut tietojen käsittelemisessä. Verkon koneet voivat toimia palvelimina, mutta myös asiakaskoneina. (Li, Barenji & Huang, 2018.)

2 LOHKOKETJUTEKNOLOGIA FINANSSIALALLA

Jotta älykkäitä sopimuksia voidaan ymmärtää, on käytävä läpi, miten lohkoketjuteknologia toimii. Seuraavissa alaluvuissa perehdytään lohkoketjuteknologian taustaan, toimintaan sekä sovelluksiin finanssialalla.

2.1 Lohkoketjuteknologian tausta ja toiminta

Vuonna 2008 Satoshi Nakamoto teki julkaisun elektronisesta käteisestä. Julkaisun nimi on ”Bitcoin: A Peer to Peer Electronic Cash System”. Nakamoton julkaisema paperi sisältää nykyäänkin monien kryptovaluuttojen noudattaman suunnitelman. Bitcoin on ensimmäinen lukuisista nykyhetkeen mennessä kehitellyistä lohkoketjusovelluksista. (Nakamoto, 2008.)

Ennen Bitcoinia on ollut useita sähköisiä käteisrahajärjestelmiä, mutta yksikään niistä ei ole saavuttanut laajaa käyttöastetta. Lohkoketjun käyttö on mahdollistanut Bitcoinin toteuttamisen hajautetusti. Bitcoinin ensisijainen hyöty on mahdollistaa käyttäjien väliset suorat tapahtumat ilman tarvetta luotettavalle kolmannelle osapuolelle. Käyttämällä lohkoketjua ja konsensuspohjaista ylläpitoa, on pystytty luomaan itsevalvontamekanismi, joka varmistaa lohkoketjuun lisättävän vain kelvolliset tapahtumat ja lohkot. Bitcoinissa lohkoketju antaa käyttäjälle mahdollisuuden olla pseudonyymi eli käyttäjä on anonyymi, mutta tilitunnus ei ole. Kaikki tapahtumat ovat myös julkisesti näkyvissä. Koska Bitcoin on pseudonyymi, oli kehitettävä mekanismeja luottamuksen lisäämiseksi, sillä käyttäjiä ei ole helppo tunnistaa. Ennen lohkoketjuteknologian hyödyntämistä tämä luottamus saavutettiin tyypillisesti välittäjien kautta, joihin kaikki osapuolet pystyivät luottamaan. (Sapra & Dhaliwal, 2019.)

Lohkoketjuteknologia on tapa, jolla voidaan yhdistää vanhoja, jo olemassa olevia teknologioita toisiinsa, kuten esimerkiksi kryptografiaa, salausta sekä vertaisverkkoja (Nakamoto, 2008). Lohkoketjut ovat hajautettuja, jaettuja ja läpinäkyviä tietokantoja, joissa jokaisella lohkoketjun osapuolella on pääsy koko tietokantaan sekä koko tietokannan historiaan. Tietoja ei valvo vain jokin

yksittäinen osapuoli, vaan jokainen voi tarkistaa kumppaniensa kirjanpidot suoraan ilman välittäjää. (Mohanta, Jena, Panda & Sobhanayak, 2019.)

Lohkoketjuteknologiassa viestiminen tapahtuu suoraan vertaisryhmien välillä, eikä keskussolmun kautta. Solmut tallentavat ja välittävät tietonsa kaikille muille solmuille. Jokainen tapahtuma näkyy kaikille, joilla on pääsy järjestelmään. Tietueet ovat peruuttamattomia eli kun tietokanta on kerran vastaanottanut tiedon tapahtumista, ketjuja ei voi muuttaa. Pysyvän tallennuksen takaamiseksi lohkoketjuteknologia käyttää algoritmeja. Se tarkoittaa, että lohkoketjujen tapahtumat käyttävät laskennallista logiikkaa. Käyttäjät voivat itse määrittää eri algoritmeja ja sääntöjä, joiden mukaan omat lohkoketjutapahtumat toimivat. (Ciotta, Marinello, Asprone, Botta & Manfredi, 2021.)

Lohkoketjut ovat vikoja kestäviä. Muutaman solmun epäonnistuessa tai irrotessa verkosta, jäljellä olevat solmut kykenevät jatkamaan toimintaansa, sillä kaikilla solmuilla on kopiot kaikista tiedoista. (Nakamoto, 2008.)

Lohkoketjujen yksi eduista on niin sanottu Bysantin vikasietoisuus. Lohkoketjut pystyvät toimimaan muutaman solmun ollessa viallisia. Bysantin vikasietoisuus kuitenkin yrittää käsitellä ja korjata solmuja, jotka eivät toimi tai toimivat vain osittain. Hakkerointien ja kyberhyökkäysten lisääntyessä Bysantin vikasietoisuus on hyödyllinen ominaisuus. Vaikka rikollisjoukot saattavat tyytyä rahan varastamiseen, terroristiryhmien ja kansallisvaltioiden vastustajat saattavat yrittää aiheuttaa katastrofaalisia vahinkoja korruptoimalla tai tuhoamalla tietoja. Lohkoketjuteknologia tarjoaa vahvan suojan tällaisia hyökkäyksiä vastaan, koska data replikoidaan useissa eri tietokoneverkoissa toimivissa solmuissa ja lohkoketjuista löytyy eheystarkastukset. (Böhmecke-Schwafert ym., 2022.)

Lohkoketjun tiedot tallennetaan kryptografisesti salattuina paloina, joista käytetään nimitystä lohko. Seuraava lohko sisältää tietoja edellisestä lohkosta ja näin ollen lohkot muodostavat ketjun. Uusia lohkoja ketjuun muodostavat solmut eli koneet, jotka toimivat hajautetussa vertaisverkossa. Jokainen uusi lohko tallentaa viimeisimmät tapahtumatiedot ja muutokset. Tieto tallentuu kaikkiin lohkoihin samanaikaisesti. (Ciotta ym., 2021.)

Lohkoketjun muodostuminen noudattaa aina tiettyä logiikkaa. Uutta ketjua muodostaessa ensin tulee tapahtumapyyntö, eli halutaan jokin toiminto tai informaatio tallennettua. Tapahtumapyyntö menee kaikille vertaisverkossa oleville solmuille. Sen jälkeen solmujen tulee vahvistaa pyyntö sekä sen sisältämät tiedot. Edellä mainitut sekä muut aiemmat tapahtumat yhdistetään lohkoksi. Tämän jälkeen uusi lohko lisätään osaksi ketjua. Lohko ja kaikki sen sisältämä informaatio tulee osaksi muuttumatonta lohkoketjua. (Böhmecke-Schwafert ym., 2022.)

2.2 Yksityiset ja julkiset lohkoketjut

Lohkoketjut voidaan jakaa yksityisiin ja julkisiin lohkoketjuihin. Julkisia lohkoketjuja voi lukea kuka vain, ja kuka tahansa voi lähettää transaktioita, jotka lisätään lohkoketjuun niiden ollessa päteviä. Lisäksi kuka vain voi osallistua konsensusprosessiin. Julkiset lohkoketjut on suojattu kryptotalouden avulla.

Kryptotaloudessa salaustekninen todentaminen ja taloudelliset kannustimet on yhdistetty eri mekanismeilla, esimerkiksi käyttämällä varantodistetta. Mekanismit määrittävät, kuinka paljon joku kykenee vaikuttamaan konsensusprosessiin, mikä on verrannollinen taloudellisten resurssien sitouttamiseen. Tällaiset lohkoketjut mielletään yleensä täysin hajautetuiksi. (Mohanta ym., 2019.)

Julkisten lohkoketjujen avulla voidaan käyttäjiä suojata kehittäjiltä. Kehittäjät eivät voi tehdä tiettyjä toimintoja. Kehittäjä joutuu siis luopumaan osasta oikeuksistaan, joka voi tuoda luotettavuutta osapuolien välille. Tilanteessa, jossa kehittäjä joutuu painostetuksi, hän voi vedota oikeuksien puutteellisuuteen. (Nakamoto, 2008.)

Yksityisissä lohkoketjuissa kirjoitusoikeudet ovat keskitetysti yhdellä organisaatiolla. Yksityiset lohkoketjut mahdollistavat korkean tason yksityisyyden. Lukuoikeuksia voidaan rajoittaa tai ne voivat olla julkisia. Esimerkiksi jotkin yrityksen sisäiset asiat kuten tietokantojen hallinta ja auditointi voivat olla tarpeettomia julkiseksi luettavaksi. Yritys, joka ylläpitää yksityisiä lohkoketjuja, voi muuttaa niiden sääntöjä ja perua transaktioita. Yksityisten lohkoketjujen transaktiot ovat edullisempia kuin julkisten lohkoketjujen. Yksityisissä lohkoketjuissa vain muutama tehokas solmu varmistaa transaktiot. Solmut ovat liittyneitä toisiinsa hyvin ja virheiden korjaaminen manuaalisesti on nopeaa. Tämä mahdollistaa konsensusalgoritmien käytön, jotka muodostavat toimituksien lopullisuudet hyvin lohkoajoin. (Nakamoto, 2008.)

TAULUKKO 1. Yksityisten ja julkisten lohkoketjujen eroavaisuudet.

YKSITYISET	JULKISET
Nopea	Hidas
Rajoitettu jäseniä	Avoin jokaiselle
Luotettu	Luottamus vapaa
Hallittu ylläpito	Julkinen omistaminen
Skaalautuu hyvin	Skaalautuu heikosti

2.3 Lohkoketjuteknologian soveltaminen finanssialalla

Lohkoketjua hyödynnetään finanssialalla jo jonkin verran. Tällä hetkellä lohkoketjuja hyödynnetään muun muassa datan analysoimiseen sekä prosessoimiseen. Finanssialalla on jatkuvasti kehitteillä uusia formaatteja ja palvelumalleja, jotta laatu ja tehokkuus säilyisi ja kehittyy. Lohkoketjuteknologia voi auttaa esimerkiksi asiakkaiden luottoehtojen tunnistamisessa ja rajojen ylittävien maksujen tehostamisessa. (Zhang, Xie, Zheng, Xue, Zheng & Xu, 2020.)

Osalla finanssialan palveluntarjoajista odotukset ovat hyvinkin korkealla lohkoketjuteknologian suhteen. Lohkoketjujen odotetaan tuovan suuria etuja nykyiseen pankkijärjestelmään, yhteiskuntaan sekä yksittäisille kuluttajille. (Böhmecke-Schwafert ym., 2022.)

Xu ym. (2019) uskovat tutkimuksessaan, että lohkoketjuteknologia kykenee ominaisuuksiensa ansiosta saavuttamaan laajoja sovelluksia rahoitusalalla esimerkiksi pankkitoiminnassa, pääomamarkkinoilla sekä internet-rahoituksessa.

Isot finanssialan toimijat sijoittavat teknologiaan, jotta he voivat tehdä enemmän vähemmällä eli käyttämällä vähemmän rahaa sekä aikaa isompiin tuloksiin. Tätä kautta toiminta tehostuu. Lohkoketjujen nähdään olevan avain kustannustehokkaaseen toimintaan. Lohkoketjutesimerkiksi mahdollistavat yrityksen koosta riippumatta mahdollisuuden rahan keräämiseen ”peer-to-peerin” avulla maailmanlaajuisesti. (Tapscott, 2017.)

Siinä missä lohkoketjuteknologia on muuttanut finanssialan käytänteitä, finanssiala on myös tuonut muutoksia lohkoketjuteollisuuteen. Lohkoketjujen tulee kehittyä ja muuttua kysynnän mukana. (Tapscott, 2017.)

Lohkoketjuteknologiaa ei ole tutkittu juuri ollenkaan rahoituksen toimitusketjujen valossa. Täten on vaikea arvioida teknologian potentiaalia kaikilla finanssialan osa-alueilla. Rahoituksen toimitusketjut ja niissä lohkoketjujen hyödyntäminen antavat oivan tutkimusmahdollisuuden tulevaisuuden tutkijoille. (Ali, Ally & Dwivedi, 2020.)

2.4 Lohkoketjuteknologian haasteet ja riskit

Lohkoketjuteknologia on vielä kehitysvaiheessa oleva teknologia ja tarvitsee paljon tutkimuksia, jotta puutokset ja ongelmat voidaan ratkaista ja lohkoketjuteknologia ottaa laajemmin käyttöön finanssialalla. Vaikka lohkoketjuteknologia on joiltain osilta turvallisuutta lisäävä teknologia, se ei kykene poistamaan jo olemassa olevia kyberturvallisuusriskejä. Kyberturvallisuusriskien ehkäisemiseksi tarvitaan tarkkaan harkittua riskienhallintaa sekä jatkuvaa seurantaa. Moniin kyberturvallisuusriskeihin saattaa liittyä hyvinkin pieniä tekijöitä ja virheitä, joita voi käydä kenelle vain. Siitä syystä kyberturvallisuusosaaminen on tarpeen. Hakkerit opettelevat jatkuvasti enemmän lohkoketjuista ja niiden haavoittuvuuksista, joten heistä tulee yhä taitavampia ja he ovat yhä suurempi, jatkuva riski. Kyberturvallisuusstandardit ja -ohjeet ovat iso ja tärkeä osa lohkoketjuteknologiaa, jotta voimme turvata järjestelmiä. (Sapra & Dhaliwal, 2019.)

Lohkoketjujen on todistettava pystyvänsä skaalautuvuuteen, nopeuteen ja turvallisuuteen. Jotta nämä tavoitteet voidaan saavuttaa, on hajautettujen konsensusalgoritmien tutkiminen tärkeää. Tällä hetkellä ei ole löydetty vielä ratkaisua, jossa kaikki kolme edellä mainittua ominaisuutta täyttyisi ilman kompromissien tekemistä. Kehityksen alkuvaiheessa lohkoketjuteknologian varhaiset hyödyntäjät kohtaavat haasteita, kuten sopivan konsensusmekanismin ja järjestelmäarkkitehtuurin valinnan, sillä heillä ei ole pitkän aikavälin kuvaa eri ratkaisuiden hyödyistä ja haitoista. (Andoni, Robu, Flynn, Abram, Geach, Jenkins & Peacock, 2019.)

Lohkoketjuteknologian kehityskustannukset ovat tällä hetkellä korkeat. Tiedon siirto onnistuu todella alhaisilla kustannuksilla, mutta tietojen

todentamisesta aiheutuu korkeita laitteisto- ja energiakustannuksia. Todentamisen kustannukset nousevat, kun lisäkustannuksia syntyy tietojen tallentamisesta laajeneviin kirjanpitoihin. (Sapra & Dhaliwal, 2019.)

Lohkoketjuteknologian käyttöönottoa finanssialalla osaltaan hidastaa standardoinnin ja joustavuuden puute. Erilaisia standardeja tulisi kehittää, jotta teknologiaratkaisuiden välinen yhteentoimivuus olisi mahdollista. Käyttöönottoa saattaa myös hidastaa Bitcoinin alkuajoista kumpuava huono maine ja sen yhteys laittomaan toimintaan. (Andoni ym., 2019.)

3 LOHKOKETJUTEKNOLOGIAPOHJAISET ÄLYKKÄÄT SOPIMUKSET FINANSSIALALLA

Lohkoketjuteknologiapohjaisia älykkäitä sopimuksia löytyy jo paljon. Älykkäiden sovellusten ymmärrys vaatii itse teknologian, mutta myös älykkäiden sopimusten piirteiden ymmärrystä. (Ciotta ym., 2021.) Seuraavissa alaluvuissa käydään läpi älykkäiden sopimusten historiaa, älykkäiden sopimusten toimintaa, haasteita sekä tulevaisuuden mahdollisuuksia.

3.1 Älykkäiden sopimusten historia

Älykkäiden sopimusten historia alkaa jo noin 1990-luvulta, kun tietokoneinsinööri Wei Dai kehitti anonyymin lainaohjelman periaatteita. Anonyymiin lainaohjelmaan sisältyy lunastettavia joukkovelkakirjoja sekä kertasummaveroja. (Hu, Liyanage, Mansoor, Thilakarathna, Jourjon & Seneviratne, 2018.)

Vuonna 1997 Nick Zabo nosti esille salausmekanismien hyödyntämisen älykkäissä sopimuksissa. Salausmekanismien avulla lohkoketjujen turvallisuutta voisi parantaa. Siitä lähtien salausmekanismit ovat turvanneet älykkäiden sopimusten tapahtumia julkisissa verkoissa. Nykyään lohkoketjuteknologian ollessa kovassa kehitysvaiheessa, älykkäiden sopimusten luominen ja käyttäminen on yleistynyt. Salausten ansiosta älykkäät sopimukset voidaan lähettää suoraan osapuolten kesken luottamuksellisesti ilman kolmannen osapuolen osallistumista. (Hu ym., 2018.)

Vuonna 2009 onnistuttiin luomaan koko historian ensimmäinen lohkoketjuteknologiapohjainen älykäs sopimus. Älykäs sopimus sisälsi yksinkertaisia ja ennalta määritettyjä komentoja. (Hu ym., 2018.) Yksinkertaiset sopimusmuodot, esimerkiksi Bitcoin-tapahtumat, ovat määriteltyinä niin sanottuun Bitcoin-skriptiin (Lavene & Coen, 2021).

Vuonna 2013 NXT eli avoimen lähdekoodin kryptovaluutta- ja maksuverkosto tarjosi yleiseen käyttöön joukon älykkäitä sopimusmalleja. NXT

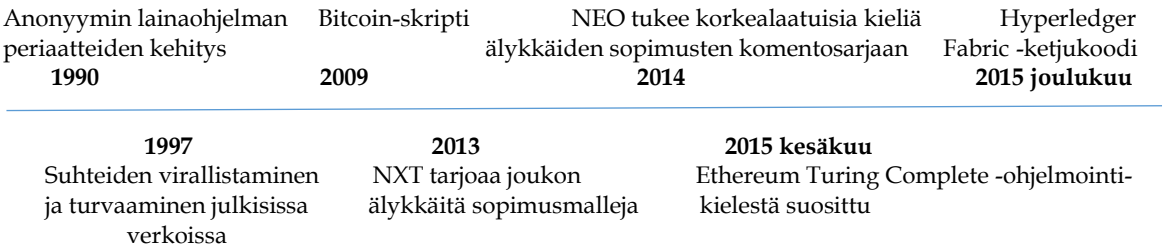
suunniteltiin tarjoamaan erityisesti joustavia alustoja sovellusten ja rahoituspalveluiden rakentamiseen.

Hong Fei ja Erik Zhang perustivat vuonna 2014 NEO:n. NEO on avoimen lähdekoodin lohkoketjujen sovellusalusta. NEO alkoi vuonna 2014 tukemaan korkealaatuisia ohjelmistokieliä älykkäiden sopimusten komentosarjassa. (Hu ym., 2018.)

Vuonna 2015 Etherium Turing Complete -ohjelmointikielestä tuli suosittu. Vuonna 2015 myös suunniteltiin ”Hyperledger Fabric -ketjukoodi” konsortioille. Hyperledger Fabric mahdollistaa älykkäiden sopimusten kirjoittamisen useilla korkean tason ohjelmointikielellä. (Hu ym., 2018.) ”Chaincode” eli ketjukoodi on ohjelma, joka suorittaa annetun toiminnon. Ketjukoodi voidaan luokitella älykkääksi sopimukseksi. (Salimitari, Chatterjee & Fallah, 2020.)

Hu ym. (2019) ovat kuvanneet artikkelissaan älykkäiden sopimusten historian aikajanalla. Diagrammi kuvastaa älykkäiden sopimusten kehittymistä vuodesta 1990 vuoteen 2015.

KUVIO 1. Aikajana. Mukailtu Hu ym. (2019, s. 2) älysopimusten historia.



3.2 Mitä älykkäät sopimukset ovat

Älykkäät sopimukset vievät lohkoketjut pidemmälle, sillä ne antavat mahdollisuuden luoda koodia sisälle lohkoketjuun (Haque ym., 2021). Älykkäät sopimukset eroavat perinteisistä paperisopimuksista siten, että älykkäät sopimukset automatisoivat sopimusmenettelyt, minimoivat osapuolten välisen vuorovaikutuksen ja pienentävät hallintokuluja. Lohkoketjujen ja älykkäiden sopimusten suuresta hypetyksestä huolimatta tekniikka on vasta aluillaan. (Deng ym., 2020.)

Älykäs sopimus on kahden tai useamman osapuolen yhteinen sopimus. Se pystyy tallentamaan tietoja, käsittelemään syötteitä ja kirjoittamaan ulostuloja ennakkoon määritettyjen toimintojen ansiosta. (Khan, Loukil, Ghedira-Guegan, Benkhelifa & Bani-Hani, 2021.)

Älykkäät sopimukset ovat hajautetuissa verkoissa toimivia ohjelmia. Ohjelman solmut tallentavat tiedot lohkoketjujen muodossa. Älykkäisiin sopimuksiin kohdistuu nykyisin paljon mielenkiintoa, sillä niiden avulla voidaan hallita ja siirtää huomattavan suuren arvon omaavaa omaisuutta. Yleisin

siirtomuoto on kryptovaluutat, kuten esimerkiksi Bitcoin, jotka ovat hajautettuja sovelluksia. Muita esimerkkejä hajautetuista sovelluksista ovat henkilöllisyyden vahvistus ja elintarvikeketjujen sekä energiamarkkinoiden hallinta. (Lavene & Coen, 2021.)

Vuonna 2003 oikeustieteen tohtori Szabo ehdotti termiä älykäs sopimus. Hänen määritelmänsä mukaan älykäs sopimus on joukko digitaalisessa muodossa määriteltyjä sitoumuksia. Yleisesti ottaen älykäs sopimus on sopimus, joka voidaan toteuttaa automaattisesti tiettyjen ehtojen täyttyessä tietokonejärjestelmässä. Lohkoketjuissa tehtävät älykkäät sopimukset varmistavat prosessien avoimuuden ja läpinäkyvyyden sekä estävät prosessin peukaloimisen. Lohkoketjuteknologiapohjaisilla älykkäillä sopimuksilla pystytään välttämään keskitettyjen instituutioiden vaikutus, jolloin ne pystyvät toimimaan tehokkaasti. Lohkoketjuteknologian ansiosta älykkäillä sopimuksilla on monia etuja, kuten hajauttaminen ja prosessien jäljittäminen. Älykkäät sopimukset voidaan lukea lohkoketjuteknologian ominaisuuksiksi. (Liu, Xu, Li, Zhao, Jiang, Yao & Chen, 2021.)

Lohkoketjuteknologiapohjaisiin älykkäisiin sopimuksiin sisältyy erilaisia tallennusmekanismeja sekä tapahtumien käsittelyä. Tapahtumia hyväksytään, käsitellään ja tallennetaan lohkoketjussa. Tapahtumat sisältävät pääasiassa lähetettävät tiedot sekä tapahtuman kuvauksen. Kun tapahtumatiedot ovat siirtyneet älykkääseen sopimukseen, resurssin tila päivittyy sopimusresurssikokoelmassa. Tämän jälkeen edellä mainitut tapahtumat laukaisevat automaattisesti älykkään sopimuksen tekemään tila-arviota. Jos yhden tai useamman toiminnon ehdot täyttyvät, sopimustoiminnot suoritetaan automaattisesti ennalta asetettujen tietojen mukaisesti. Älykkään sopimusjärjestelmän ydin on tapahtuma ja sen kanssa solmittu älykäs sopimus. Älykäs sopimus on loppujen lopuksi vain järjestelmä, joka koostuu tapahtumakäsittelymoduulista ja tilakoneesta. Älykäs sopimus ei itse luo älykästä sopimusta, eikä voi muokata sitä. Älykäs sopimus on olemassa digitaalisten ehtojen suorittamista varten oikeilla ehdoilla. (Liu ym., 2021.)

Älykkäät sopimukset ovat saaneet tärkeän roolin monilla eri aloilla. Älykäs sopimus nimenä voi antaa olettaa niiden olevan helppoja luoda, mutta sopimuksien sopimussääntöjen luominen sekä älykkäiden sopimusten kehittäminen on itseasiassa työlästä. Älykkäiden sopimusten koodaaminen vaatii liiketaloustietämystä, koodaustaitoja ja vahvaa teknistä osaamista. Osaamisen on pysyttävä ajantasalla uusien, nopeasti kehittyvien ja muuttuvien kielten ja lohkoketjualustojen takia. (Hamdaqa, Met & Qasse, 2022.)

Tehtävään sopimukseen voi määrittää rakentajatoiminnon, mikä mahdollistaa älykkään sopimuksen luomisen. Älykkäässä sopimuksessa voidaan määrittää itsetuhotoiminto. Älykkään sopimuksen omistaja kykenee näin ollen tuhoamaan tehdyn sopimuksen toiminnon avulla. Muut osapuolet eivät kykene sopimusta tuhoamaan. (Khan ym., 2021.)

Laillisen sopimuksen muuntamisessa älykkääksi sopimukseksi on tärkeää, että kummallakin osapuolella on selkeät oikeudet, velvollisuudet ja kiellot sopimuksessa määriteltyjen lausekkeiden puitteissa. Älykkäässä sopimuksessa

voidaan määrittää myös seuraamuksia kielletyn toimenpiteen suorittamisesta tai tiettyjen velvoitteiden laiminlyönnistä. (Khan ym., 2021.)

Älykkäiden sopimusten, jotka pohjautuvat lohkoketjuteknologiaan, tutkimiseen on havaittu kiinnostuksen nousua viime aikoina. Tutkimusten myötä älykkäitä sopimuksia on mahdollista hyödyntää aiempaa enemmän finanssialan lisäksi esimerkiksi terveydenhuollossa, älykaupungeissa, esineiden internetissä, pilvipalveluissa ja monessa muussakin. (Solaiman, Wike & Sfyrakis, 2021.)

Viime vuosien aikana on ehdotettu älykkäitä sopimuskieliä hajautettujen sovellusten määrittelemiseen. Eri kielillä tulisi olla erinomaiset turvatakuudet, jotta on mahdollista ohjelmoinnin kautta tehdä suuriakin pääoman siirtoja. Älykkäissä sopimuksissa on esiintynyt pieniä virheitä, joiden seurauksena viime vuosien aikana on menetetty rahaa jopa useita miljoonia dollareita. (Lavene & Coen, 2021.)

3.3 Älykkäiden sopimuksien lohkoketjualustat

Älykkäitä sopimuksia kehitetään ja otetaan käyttöön eri lohkoketjuteknologia-alustoilla. Monet alustoista tarjoavat ainutlaatuisia ominaisuuksia älykkäiden sopimusten kehittämiseen, mukaan lukien sopimusohjelmointikielet, sopimuskoodin suorittamisen ja suojaustasot. Osa alustoista tukee korkean tason ohjelmointikieliä älykkäiden sopimusten kehittämiseksi. (Akram, Malik, Singh, Anita & Tanwar, 2020.)

Bitcoin on yksi monista lohkoketjualustoista. Alustaa voidaan käyttää kryptovaluuttAliatransaktioiden käsittelemiseen. Bitcoin-alustalla on hyvin rajallinen laskentakyky. Alusta käyttää pinopohjaista tavukoodiskriptikieltä. Bitcoin-skriptikielillä älykkäiden sopimusten luominen on hyvin rajallista, sekä on vaikea saada tehtyä kattavaa lopputulosta. Bitcoiniin tulisi tehdä vielä suuria muutoksia, jotta Bitcoin-lohkoketjussa voitaisiin tehdä älykkäitä sopimuksia. (Khan ym., 2021.)

NXT on avoimen lähdekoodin lohkoketjualusta. Se perustuu täysin proof-of-stake -konsensusprotokollaan, joka sisältää tällä hetkellä valikoiman voimassa olevia älykkäitä sopimuksia. NXT ei ole Turing-täydellinen. Tämä tarkoittaa, että vain jo olemassa olevia sopimusmalleja voidaan käyttää. Uutta henkilökohtaista älykästä sopimusta ei voida ottaa käyttöön. (Khan ym., 2021.)

Ensimmäinen lohkoketjualusta älykkäiden sopimusten kehittämiseen on ollut Ethereum. Alusta tukee edistyneitä ja älykkäitä sopimuksia Turing-täydellisen virtuaalikoneen avulla, jota kutsutaan Ethereum-virtuaalikoneeksi (EVM). EVM on älykkäiden sopimusten ajonaikainen ympäristö, jossa jokainen Ethereum-verkon solmu suorittaa EVM-toteutuksen ja suorittaa siten samat ohjeet. Solidity on yksi korkean tason ohjelmointikielistä. Sitä käytetään älykkäiden sopimusten kirjoittamiseen, jolloin sopimuskoodi käännetään EVM-tavukoodiin ja näin pystytään ottamaan käyttöön lohkoketjussa . Ethereum on tämän hetkisistä alustoista suosituimpien joukossa älykkäiden sopimusten

kehitysalustana. Ethereum-alustaa voidaan käyttää hajautettujen sovellusten suunnitteluun useilla eri aloilla. (Khan ym., 2021.)

Bitcoin ja Etheraum ovat julkisia lohkoketjuja. Hyperledger Fabric sen sijaan on sallittu vain joukolle liiketoiminnan organisaatioita. Liittyminen lohkoketjuun on mahdollista vain jäsenpalveluntarjoajan kautta. Verkko rakennetaan vertaisryhmistä, jotka ovat organisaatioiden omistamia ja lahjoittamia. Hypeledger Fabric on IBM :n kehittelemä avoimen lähdekoodin yritystason hajautettu pääkirjateknologia-alusta. Alusta tukee älykkäitä sopimuksia. Alustan modulaarinen arkkitehtuuri mahdollistaa erilaisia yrityskäyttötapauksia plug and play -komponenttien avulla. (Khan ym., 2021.)

3.4 Finanssialalla käytettävien älykkäiden sopimusten haasteet ja riskit

Lohkoketjuteknologiapohjaisia älykkäitä sopimuksia tarkasteltaessa niiden riskit voidaan jakaa viiteen pääryhmään, jotka ovat turvallisuus, oikeudelliset kysymykset, muuttumattomuus, konsensusmekanismit sekä skaalautuvuus. Yksi suurimmista lohkoketjuteknologiaan liittyvistä huolista on sen turvallisuus. Monet haavoittuvuudet johtuvat teknologian kirjoituskielistä. Älykkäiden sopimusten semanttiset haavoittuvuudet voidaan luokitella tapahtumien tilausriippuvuuteen, aikaleimariippuvuuteen, väärin käsiteltyihin poikkeuksiin ja puhelupinon syvyyteen. (Uriarte, Zhou, Kritikos, Shi, Zhao & De Nicola, 2021.)

Jo olemassa olevien älykkäiden sopimuskielten parantamista ja uusien kehittämistä tulisi tulevaisuudessa tarkastella huolellisesti. Lohkoketjuihin kohdistuvat hyökkäykset vaihtelevat tyyleiltään ja kehittyvät ajan myötä. Käyttäjän on erittäin tärkeä ymmärtää tiettyjen lohkoketjuteknologiapohjaisten alustojen mekanismit ja haavoittuvuudet ennen niiden käyttöä. Esimerkiksi julkisten älykkäiden sopimusten pseudonyymi ei aina takaa ketjujen yksityisyyttä tai linkittämistä. Tähän on käyttäjän osattava varautua ja suhtautua oikein. (Uriarte ym., 2021.)

Yksi tapa yksityisyyden suojaamiseen on integroida ylimääräinen tietosuojakomponentti. Samankaltaisia ideoita ja tekniikoita hyödynnetään älykkäissä sopimuksissa. Ne mahdollistavat älykkäiden sopimusten käyttäjien ketjun yksityisyyden sekä sopimusturvallisuuden. Kaksi käyttäjää voi suorittaa toimintoja älykkäillä sopimuksilla ilman, että paljastavat todellisia tietoja. Huono puoli salausalgoritmien käyttämisessä on se, että ne tuovat usein ylimääräisiä kustannuksia järjestelmille. Tulevaisuuden kehitys kohdistuu yksityisyyden säilyttämistekniikoiden ratkaisuihin. Vaikka älykkäiden sopimusten toteuttamista säätelevät hyvin koodatut ohjelmistot, älykkäisiin sopimuksiin syötetty data on ulkopuolisten tahojen hallinnassa, joten niihin ei aivan täysin voi luottaa. (Deng ym., 2020.)

Kehittyvässä yhteiskunnassa lakiasiat saattavat tulla joissain tilanteissa ongelmaksi. Joissakin tilanteissa ketjun ulkopuolisiin luottaminen on

kyseenalaistettu, eteen saattaa tulla muuttumattomuusongelmia tai konsensusmekanismiin liittyvä ongelma. (Uriarte ym., 2020.)

Älykkäät sopimukset vaativat usein tietojen vastaanottamista resursseista, jotka eivät ole itse lohkoketjussa. Silloin käytetään oraakkeleita hakemaan ketjun ulkopuolelta tietoa ja laittamaan ne lohkoketjuun määriteltyinä aikoina. Oraakkelit ovat ohjelmistoja, joiden tehtävänä on muuttaa oikean maailman tiedot lohkoketjuille sopivaksi. Olemassa olevat oraakkelit on testattu kattavasti, mutta niissä voi esiintyä silti vikoja ja ne voivat aiheuttaa vikakohtia. Oraakkelin vika voi koskea esimerkiksi tilanteita, joissa se ei kykene antamaan tarvittavia tietoja, luovuttaa eteenpäin virheellistä tietoa tai lopettaa toimintansa. Älykkäiden sopimusten kehittämisessä on otettava huomioon vikojen mahdollisuus ennen kuin älykkäiden sopimusten käyttö voi yleistyä. (Hu, Zhuang, Lin, Zhang, Kan & Cao, 2021.)

Älykkäiden sopimusten oikeudelliset kysymykset ovat monien älykkäiden sopimusten haasteiden ratkaisu. Esimerkiksi Euroopan yleisessä tietosuoja-asetuksessa määrätään, että kansalaisilla on oikeus tulla unohdetuksi. Tämä on ristiriidassa älykkäiden sopimusten kohdalla niiden muuttumattoman luonteen vuoksi. Eri mailla on omat lakinsa, jonka seurauksena on vaikeaa varmistaa, noudatetaanko kaikkia säädöksiä. (Khan ym., 2021.)

Konsensusmekanismit johtavat lohkoketjujen turvallisuutta, skaalautuvuutta ja hajauttamisen ylläpitämistä lohkoketjuverkoissa samanaikaisesti. Erilaisia konsensusalgoritmeja on olemassa jo useita, kuten esimerkiksi Proof-of-Work, joka mahdollistaa suojauksen lohkoketjuissa, mutta samalla tuhlaa resursseja. Monet organisaatiot siirtyvätkin vanhemmista konsensusmekanismeista uudempiin, jotka lupaavat halvempia maksuja transaktioista ja alhaisempia energiakustannuksia lohkoketjuprosesseista. Tulevaisuuden tutkimuksissa käytetään uudempia konsensusmekanismeja, jotta niitä pystytään testaamaan ja kehittämään. (Ahmad ym., 2021.)

Älykkäiden sopimusten yksi tärkeistä ominaisuuksista on muuttumattomuus. Kun älykäs sopimus on otettu käyttöön, eivät eri osapuolet voi muuttaa koodia. Muuttumattomuuden huono puoli ilmenee, jos koodiin tulee virheitä. Virheitä ei pystytä korjaamaan, koska muuttumattomuus ominaisuutena estää muokkauksen. Älykkäiden sopimusten muokkaamiselle ei ole yksinkertaista tapaa, mikäli olosuhteet muuttuvat. Muutoksia voi tapahtua esimerkiksi laissa, tai osapuolten välillä on sovittu älykkään sopimuksen muokkaamisesta. Tästä johtuen asiantuntijat suorittavat laajoja ja mahdollisesti myös kalliita älysopimuksien tarkasteluja ennen niiden käyttöönottoa lohkoketjussa. Näin pyritään ratkaisemaan muuttumattomuusongelma. Toinen älysopimuksien luonteeseen vaikuttava tekijä on sen peruuttamattomuus. Lohkoketjun solmut saatetaan hakkeroida tai niitä voidaan käyttää väärin, jolloin väärä tai ei-toivottu tieto kirjautuu lohkoketjuihin muuttumattomalla tavalla. Peruuttamattomuus ominaisuutena osoittautuu siis edun lisäksi myös heikkoudeksi. (Khan ym., 2021.)

Skaalautuvuus on monesti kohkoketjujen suurimpia ongelmia. Esimerkiksi Visa käsittelee jopa 24 000 tapahtumaa sekunnissa, mutta Ethereum-lohkoketju

kykenee tarkistamaan vain 14 tapahtumaa sekunnissa, mikä on huomattava ero. Skaalautuvuusongelma voi johtaa verkon ruuhkautumiseen, liiketoimien palkkioiden nousuun sekä liiketoimien vahvistamiseen tarvittavan ajan pidentymiseen. Jotta skaalautuvuus-ongelmaan saadaan ratkaisu, täytyy sitä tutkia laajalti. Tutkimukset keskittyvät transaktioiden määrän lisäämiseen sekunnissa älykkäiden sopimusalustojen avulla. Tapahtumien todentaminen riippuu kuitenkin älykkäiden sopimusalustojen käyttämästä konsensusmekanismista. Skaalautuvuus riippuu siis toisinsanoen konsensusmekanismeista. (Khan ym., 2021.)

3.5 Älykkäiden sopimusten tulevaisuuden mahdollisuudet finanssialalla

Lohkoketjuteknologiapohjaisia älykkäitä sopimuksia hyödynnetään jo paljon eri aloilla. Pankeissa lohkoketjuteknologiapohjaisia älykkäitä sopimuksia voidaan hyödyntää esimerkiksi asuntokaupoissa, lainojen myöntämisessä, maksujen automatisoinnissa, raportoinneissa, apuna tietokantojen ylläpidossa sekä arvopaperikaupassa. Vakuutusyhtiöt käyttävät älykkäitä sopimuksia tehostamaan vakuutuskorvausten käsittelyprosessia. Älykkäiden sopimusten avulla yleisiä ongelmia voidaan automatisoida ja ratkaista ilman luottamuksellista kolmatta osapuolta. (Böhmecke-Schwafert, Wehinger & Teigland, 2022.)

Älykkäiden sopimusten tulevaisuudessa nähdään kaksi selkeää trendiä. Kerros 2 -protokolla näyttäisi ratkaisevan lohkoketjujen skaalautuvuusongelman. Kerros 1 -termiä käytetään kuvaamaan taustalla olevaa päälohkoketjun arkkitehtuuria. Kerros 2 on peittävä verkko,Ciott joka sijaitsee taustalla olevan lohkoketjun päällä. Terminä kerros 2 viittaa itseasiassa useampaan eri ratkaisuun, jotka rakennetaan olemassa olevan lohkoketjujärjestelmän päälle. Kerros 2 -protokollien tehtäviä ovat kryptovaluuttaverkkojen transaktionopeuden ongelmat sekä skaalautuvuusongelmat. Esimerkkejä kerros 2 -protokollan ratkaisuista ovat Bitcoin Lightning Netwok ja Ethereum Plasma. Lightning Network on ohjelmistoratkaisu julkisten lohkoketjujen ja kryptovaluuttojen yhteentoimivuuden skaalaamiseen. Sen tavoitteena on kustannuksien vähentäminen ja pienten tapahtumien siirtäminen kryptografisesti suojattuun ketjun ulkopuoliseen ympäristöön. Silloin vain suuret tapahtumat täytyy sovittaa resurssirajoitteiseen lohkoketjuun. Ethereum Plasma on sarja älykkäitä sopimuksia, jotka mahdollistavat monia lohkoketjuja juurilohkon sisällä. Lohkoketju myös valvoo plasmaketjujen tilaa. Kaiken laskennan toteuttaja maailmanlaajuisesti on juuriketju. Petostilanteissa ja todisteiden ilmaantuessa, juuriketju lasketaan ja petoksesta rangaistaan. Usean plasma-lohkoketjun on mahdollista toimia rinnakkain liiketoimintalogiikkansa ja älykkäiden sopimusehtojen kanssa. Kerros 2 -protokollan ansiosta voidaan siis suurin osa pääketjun suorittamasta työstä siirtää toiselle kerrokselle. Pääketju tarjoaa turvan. Toisen kerroksen protokollilla on antaa parempia ratkaisuja

skaalautuvuusongelmaan ja korkeamman suorituskyvyn saavuttamiseen, jotta tulevaisuudessa pystyttäisiin suorittamaan satoja ja jopa tuhansia tapahtumia sekunnissa. (Khan ym., 2021.)

Älykkäillä sopimuksilla on muitakin etuja kuin vain lohkoketjuteknologian edut. Termi kattaa sopimuksen koko digitaalisen elinkaaren neuvotteluista sopimusvelvotteiden täyttämisen valvontaan ja todentamiseen. Tällä hetkellä on jo mahdollista käyttää älykkäitä sopimuksia myös ilman lohkoketjuteknologiaa. Sitä kautta älykkäiden sopimuksien teknologiaan liittyvät ongelmat, kuten muuttumattomuusongelma sekä lohkoketjujen peruuttamattomuus, mahdollisesti ratkeaisivat. Huippuluokan sopimushallintaratkaisuissa on jokaisen osapuolen todistettava henkilöllisyytensä ja todettava pääsynsä tietoihin luottamuksen perustan varmistamiseksi. Tämän lisäksi kaikki sopimukseen liittyvät asiakirjat on tallennettu versiosuojatulla tavalla salatussa muodossa Euroopassa kehitetylle ja toimivalle pilvipohjaiselle alustalle. Näin voidaan varmistaa jokaisen tapahtuman läpinäkyvyys ja jäljitettävyys, niiden toimet ja vastuuhenkilöiden nimeäminen. Fabasoft Contracts on yksi esimerkki maailmalla esiintyvistä uusimmista sopimustenhallintaratkaisuista. Se on käyttövalmis pilvipohjainen ohjelmisto, joka kykenee tukemaan käyttäjiä koko sopimuksen elinkaaren ajan. Tuki ulottuu yritysten välisestä sopimusten valmistelusta tarkastelujen tehokkaaseen käsittelyyn ja hyväksymisprosesseista versioturvalliseen sopimusarkistointiin. Fabasoft Contracts mahdollistaa sopimusoikeuksien ja velvollisuuksien mallintamisen. Ne voidaan todentaa automaattisesti ja panna täytäntöön. Sopimushallintaratkaisulla on muutosturvallinen sopimushallinta, joka tarjoaa monia etuja, esimerkiksi hyvän jäljitettävyyden. (Khan ym., 2021.)

Lohkoketjuteknologiapohjaisia älykkäitä sopimuksia ja sen sovelluksia on jo käytössä finanssialalla, mutta laajempi käyttöönotto vaatii itse teknologian tutkimista laajalti lisää. Teknologian tuomia haasteita ja riskejä finanssialalla tulee tutkia enemmän, jotta ongelmat voidaan pyrkiä ratkaisemaan tai poistamaan. (Akram ym., 2020.)

4 YHTEENVETO JA POHDINTA

Lohkoketjuteknologia on vielä verrattain uusi teknologia, vaikka sen juuret voidaan jäljittää jo 1980-luvulle. Lohkoketjuteknologia on nopeassa kehityksen vaiheessa. Lohkoketjuja hyödynnetään jo monilla aloilla, mutta jotta käyttöä voidaan laajentaa, tarvitaan vielä paljon kehitys- ja tutkimustyötä.

Lohkoketjuja hyödynnetään muun muassa älykkäissä sopimuksissa. Lohkoketjut ovat hajautettuja, jaettuja ja läpinäkyviä tietokantoja. Lohkoketjuissa tiedot ja tapahtumat tallentuvat lohkoketjuteknologiaa käytettäessä. Teknologia poistaa sopimuksia tehdessä tarpeen kolmannelle luotettavalle osapuolelle. Osapuolet voivat tehdä keskenään luotettavasti sopimuksen. Kaikista tapahtumista jää peruuttamaton ja luotettava jälki lohkoketjuun, jolloin huijauksen mahdollisuus on pystytty poistamaan.

Älykkäiden sopimusten lohkoketjuteknologia tuo mukanaan myös huonoja puolia. Skaalautuvuus on tällä hetkellä huono, joten tapahtumien suorittaminen on hidasta. Muuttumattomuus lohkoketjuissa tuo luotettavuutta, mutta myös haasteita ongelmatilanteita kohdatessa. Lait eivät ole pysyneet lohkoketjuteknologian kehityksen perässä, sillä lakimuutokset vievät aikaa. Tällä hetkellä lait tuovat rajoituksia lohkoketjuteknologian hyödyntämiseen.

Lohkoketjuteknologia on hieman ongelmallinen teknologia älykkäille sopimuksille tällä hetkellä. Tulevaisuudessa onkin kaavailtu älykkäitä sopimuksia ilman lohkoketjuteknologiaa. Toteutuksia siitä löytyy jo, mutta vähän. Älykkäillä sopimuksilla näyttäisi olevan hyvä tulevaisuus, jos teknologian ongelmat saadaan ratkaistua.

Kerros 2 -protokollan avulla saadaan ratkaistua skaalautuvuus-ongelmia ja koko ajan kehitteillä on uusia menetelmiä, jotta teknologian ongelmat saataisiin ratkaistua. Tulevaisuus näyttää miten lohkoketjuteknologia oikeasti kehittyy ja kuinka älykkäitä sopimuksia sovelletaan.

Tutkimuksessa löysin vastaukset esittämiini tutkimuskysymyksiin. Vaikka lähteiden valinnassa noudatin tiettyä kaavaa, on mahdollista, että jotkin olennaiset ja tärkeät lähteet ovat jääneet huomaamatta.

TAULUKKO 2. Tutkimuskysymykset ja vastaukset tiivistettynä.

1. Miten lohkoketjuteknologiaa sovelletaan finanssialalla?	Lohkoketjuteknologiaa sovelletaan paljon esimerkiksi pankeissa sekä alustoina kryptovaluutoille ja älykkäille sopimuksille.
2. Miten älysopimuksia voi soveltaa ja mitkä ovat niiden mahdollisuudet finanssialalla?	Voi soveltaa monipuolisesti esimerkiksi pankeissa ja asuntokaupoissa. Tulevaisuuden näkymät hyvät, etenkin jos taustalla toimivan teknologian tilalla pystyttäisiin käyttämään jotain toista.
3. Millaisia haasteita sekä riskejä älykkäisiin sopimuksiin liittyy?	Tällä hetkellä haasteet johtuvat pääosin lohkoketjuteknologian ongelmista, joita ovat skaalautuvuus, turvallisuus, oikeudelliset kysymykset, muuttumattomuus sekä konsensusmekanismit.

Ensimmäisen tutkimuskysymyksen tavoitteena oli selvittää lohkoketjuteknologian tämän hetkistä roolia finanssialalla. Finanssialalla lohkoketjuteknologia nähdään hyödyllisenä, mutta sen virheisiin kaivataan ratkaisuja. Finanssialalla lohkoketjuteknologiaa käytetään paljon älykkäiden sopimusten muodossa. Lohkoketjuteknologian varaan on luotu monet kryptovaluutta-alustat. Ethereum oli ensimmäinen lohkoketjuteknologiaan perustuva alusta älykkäille sopimuksille.

Toinen tutkimuskysymykseni käsitteli älykkäiden sopimusten soveltamista ja tulevaisuuden mahdollisuuksia. Älykkäitä sopimuksia sovelletaan nyt jo monissa eri toiminnoissa ja eri aloilla. Esimerkiksi pankit hyödyntävät lohkoketjuteknologiapohjaisia älykkäitä sopimuksia asuntokaupoissa, lainojen myöntämisessä, maksujen automatisoinnissa, raportoinneissa, apuna tietokantojen ylläpidossa sekä arvopaperikaupassa. Vakuutusyhtiöt käyttävät älykkäitä sopimuksia tehostamaan vakuutuskorvausten käsittelyprosessia.

Älykkäiden sopimusten tulevaisuudessa tunnistetaan kaksi trendiä. Toinen liittyy kerros 2 -protokollaan ja toinen älykkäiden sopimusten toteuttamiseen ilman lohkoketjuteknologiaa, jollei ratkaisuja lohkoketjuteknologian ongelmiin löydetä. Kerros 2 -protokollan avulla pystyttäisiin mahdollisesti ratkaisemaan yksi lohkoketjuteknologian suurimmista ongelmista eli skaalautuvuus. Skaalautuvuusongelman ratketessa lohkoketjuteknologiapohjaisia älykkäitä sopimuksia voitaisiin hyödyntää ja ottaa käyttöön laajemmin. Kuten tutkimuksessa on käynyt ilmi, lohkoketjuteknologialla on monia haasteita, jotka tulisi vielä ratkaista. Mikäli älykkäät sopimukset pystyttäisiin toteuttamaan muulla teknologialla, lohkoketjuteknologian tuomat haasteet jäisivät taakse. Täytyy kuitenkin ymmärtää, että moitteetonta teknologiaa on vaikea luoda. Vaihtoehtoisten teknologioiden käyttäminen voi tuoda myös ongelmia, mutta erilaisia tai jopa samoja.

Kolmannen tutkimuskysymykseni avulla halusin selvittää lohkoketjuteknologiapohjaisten älykkäiden sopimusten suurimmat haasteet ja riskit. Ongelmakohdat löytyvät tällä hetkellä pääasiassa älykkäiden sopimusten käyttämästä teknologiasta. Lohkoketjuteknologian ongelmia tunnistetaan viisi erilaista: skaalautuvuus, turvallisuus, oikeudelliset kysymykset, muuttumattomuus sekä konsensusmekanismit. Nämä ongelmat tulisi ratkaista, jotta lohkoketjuteknologian käyttöä älykkäiden sopimusten toteuttamiseen voidaan jatkaa. Jollei teknologian ongelmia saada ratkaistua, voidaan lohkoketjuteknologia mahdollisesti korvata toisella teknologialla. Lohkoketjuteknologian korvaaminen onkin toinen tulevaisuuden trendeistä älykkäitä sopimuksia tarkastellessa.

Lohkoketjuteknologiapohjaisilla älykkäillä sopimuksilla on potentiaalinen tulevaisuus, mutta se vaatii vielä paljon tutkimustyötä sekä ongelmien ratkaisemista. Lohkoketjuteknologiapohjaiset älykkäät sopimukset mahdollistavat paljon erilaista tutkimustyötä tulevaisuudessa. Tulevaisuuden tutkimukset voivat keskittyä paljolti sovellusmahdollisuuksiin, lohkoketjuteknologian ongelmakohtiin sekä löytämään vaihtoehtoista teknologiaa lohkoketjuteknologialle. Lohkoketjujen hyödyntämistä rahoituksen toimitusketjuissa ei ole tutkittu juuri lainkaan. Se on siis alue, jota tulisi tutkia tulevaisuudessa ja jota varmasti halutaan tutkia. Aihe on sen verran laaja, että näkisin mahdollisena tehdä pro gradu -tutkielman lohkoketjuteknologiapohjaisista älykkäistä sopimuksista.

LÄHTEET

Ahmad, A., Alabduljabbar, A., Saad, M., Nyang, D., Kim, J., & Mohaisen, D. (2021). Empirically comparing the performance of blockchain's consensus algorithms. *IET Blockchain*, *1*(1), 56-64.

Akram, S. V., Malik, P. K., Singh, R., Anita, G., & Tanwar, S. (2020). Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy*, *3*(5), e109.

Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management*, *54*, 102199.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and sustainable energy reviews*, *100*, 143-174.

Böhmecke-Schwafert, M., Wehinger, M., & Teigland, R. (2022). Blockchain for the circular economy: Theorizing blockchain's role in the transition to a circular economy through an empirical investigation. *Business Strategy and the Environment*.

Ciotta, V., Mariniello, G., Asprone, D., Botta, A., & Manfredi, G. (2021). Integration of blockchains and smart contracts into construction information flows: Proof-of-concept. *Automation in Construction*, *132*, 103925.

Deng, S., Cheng, G., Zhao, H., Gao, H., & Yin, J. (2020). Incentive-driven computation offloading in blockchain-enabled E-commerce. *ACM Transactions on Internet Technology (TOIT)*, *21*(1), 1-19.

Desplebin, O., Lux, G., & Petit, N. (2021). To be or not to be: blockchain and the future of accounting and auditing. *Accounting Perspectives*, *20*(4), 743-769.

Hamdaqa, M., Met, L. A. P., & Qasse, I. (2022). iContractML 2.0: A domain-specific language for modeling and deploying smart contracts onto multiple blockchain platforms. *Information and Software Technology*, *144*, 106762.

Haque, B., Hasan, R., & Zihad, O. M. (2021). SmartOil: Blockchain and smart contract-based oil supply chain management. *IET Blockchain*, *1*(2-4), 95-104.

Hu, X., Zhuang, Y., Lin, S. W., Zhang, F., Kan, S., & Cao, Z. (2021). A security type verifier for smart contracts. *Computers & Security*, *108*, 102343.

Hu, Y., Liyanage, M., Mansoor, A., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2018). Blockchain-based smart contracts-applications and challenges. *arXiv preprint arXiv:1810.04699*.

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications*, *14*(5), 2901-2925.

Laneve, C., & Coen, C. S. (2021). Analysis of smart contracts balances. *Blockchain: Research and Applications*, *2*(3), 100020.

Li, Z., Barenji, A. V., & Huang, G. Q. (2018). Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robotics and computer-integrated manufacturing*, *54*, 133-144.

Liu, J., Xu, Z., Li, R., Zhao, H., Jiang, H., Yao, J., ... & Chen, S. (2021). Applying blockchain for primary financial market: A survey. *IET Blockchain*, *1*(2-4), 65-81.

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things*, *8*, 100107.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Salimitari, M., Chatterjee, M., & Fallah, Y. P. (2020). A survey on consensus methods in blockchain for resource-constrained IoT networks. *Internet of Things*, *11*, 100212.

Salminen, A. (2011). Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan Yliopisto.

Sapra, R., & Dhaliwal, P. (2022, August). Applications of Blockchain Technology: A Review. In *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing* (pp. 63-66).

Solaiman, E., Wike, T., & Sfyrakis, I. (2021). Implementation and evaluation of smart contracts using a hybrid on-and off-blockchain architecture. *Concurrency and computation: practice and experience*, *33*(1), e5811.

Tapscott, A., & Tapscott, D. (2017). How blockchain is changing finance. *Harvard Business Review*, *1*(9), 2-5.

Uriarte, R. B., Zhou, H., Kritikos, K., Shi, Z., Zhao, Z., & De Nicola, R. (2021). Distributed service-level agreement management with smart contracts and blockchain. *Concurrency and Computation: Practice and Experience*, *33*(14), e5800.

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, *5*(1), 1-14.

Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X., & Xu, X. (2020). The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science*, *37*(4), 691-698.