LOHKOKETJUTEKNOLOGIAN VAIKUTUS PANKKISEKTORILLA

Mahdollisuudet, hyödyt, riskit ja tulevaisuuden näkymät

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

kevät 2022

Tomi Mutka

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus Tiivistelmä
Tekijä Tomi Mutka Vuosi 2022

Työn nimi Lohkoketjuteknologian vaikutus pankkisektorilla
Mahdollisuudet, hyödyt, riskit ja tulevaisuuden näkymät

Ohjaajat Lasse Seppänen

Tämän opinnäytetyön tarkoituksena oli luoda kattava kokonaiskuva lohkoketjuteknologian perusteista sekä käsitellä laajasti ja monipuolisesti kyseisen teknologian vaikutuksia pankkisektorin eri osa-alueilla.

Opinnäytetyö on tutkimuksellinen ja opinnäytetyön tietopohjassa on hyödynnetty avoimia lähteitä. Opinnäytetyön tietopohja koostuu neljästä osasta. Ensimmäisessä osassa opinnäytetyössä kuvataan pankkisektoria lyhyesti ja perustasoisesti. Opinnäytetyön toisessa osassa käsitellään laajasti lohkoketjuteknologian perusteita, lohkoketjuteknologiaan liittyviä komponentteja sekä tekijöitä eri näkökulmista. Kolmannessa osassa arvioidaan lohkoketjuteknologian tämänhetkistä vaikutusta pankkisektorilla sekä arvioidaan lohkoketjuteknologian hyötyjä sekä riskejä pankkisektorille. Opinnäytetyön neljännessä osassa arvioidaan lohkoketjuteknologian tulevaisuutta pankkisektorilla.

Opinnäytetyön johtopäätöksenä voidaan todeta, että lohkoketjuteknologia mahdollistaa pankkisektorille täysin uusia innovaatioita mm. prosessien automatisoinnin, rahaliikenteen, tiedon rekisteröinnin sekä läpinäkyvyyden saralla nykyistä kustannustehokkaammin. Toisaalta lohkoketjuteknologiaan liittyvät riskit ovat merkittäviä eikä nykyinen sääntely tai lainsäädäntö ole vielä riittävän ajantasaista kyseisen teknologian massiiviseen käyttöönottoon turvallisesti.

Avainsanat Lohkoketjuteknologia, pankkisektori, teknologian käyttöönotto

Sivut 78 sivua ja liitteitä 1 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology — Abstract
Author Tomi Mutka — Year 2022
Subject The impact of blockchain technology on the banking sector
Opportunities, benefits, risks and outlooks
Supervisors Lasse Seppänen

The goal of this thesis was to gain an overall understanding on the basics of blockchain technology and to survey the effects of blockchain technology on the banking sector from various perspectives. This thesis is not commissioned by any party.

This thesis is a research based on open-source material and the theoretical part consists of four parts. The first part describes the banking sector shortly on a general basis. The second part of this thesis surveys thoroughly the basics of blockchain and its relating components. The third part evaluates the current influence, benefits and risks of blockchain technology on the banking sector. The fourth part of this thesis assesses the future of blockchain technology on the banking sector.

As a conclusion of this thesis, based on open-source material, it can be stated that blockchain technology will enable totally new innovations on the banking sector, such as process automation, monetary-transactions, data storage and transparency on a cost-effective way. At the same time, blockchain technology-related risks are significant and the legislation and regulations are currently not up to date for a safe mass-adoption of the technology.

Keywords Blockchain technology, banking sector, adoption of technology

Pages 78 pages and appendices 1 pages

Sanasto

Algoritmi	Ohjelma tai käsky, joka sisältää sarjan toimintoja siten, että ne ratkaisevat tietyn ongelman tai toteuttavat tietyn toiminnon.
AML (Anti-Money Laundering)	Rahanpesun estäminen
Avoin lähdekoodi	Tietokoneohjelman kehitysmenetelmä, jossa käyttäjä voi omien tarpeidensa mukaisesti muokata ohjelman lähdekoodia. Avoimen lähdekoodin ohjelmaa saa käyttää, muokata, kopioida ja levittää vapaasti sekä alkuperäisessä että muokatussa muodossa.
Big Data	Digitaalisessa muodossa olevat suuret, monipuoliset ja nopealla vauhdilla kasvavat tietovarannot.
Bitcoin	Tunnettu lohkoketjujärjestelmä, jolla kirjataan virtuaalivaluutoiksi kutsuttuja virtuaalisia arvomerkintöjä.
CBDC (Central Bank Digital Currency)	Keskuspankin liikkeelle laskema digitaalinen valuutta
CFT (Combating the Financing of Terrorism)	Terrorismin rahoittamisen estäminen
Clearing-prosessi	Clearing-prosessilla tarkoitetaan transaktion täsmäyttämistä siten, että transaktio on toteutunut täysimääräisesti kaikkien transaktion osapuolten näkökulmasta. Clearing-prosessia hyödynnetään esimerkiksi varojen siirroissa pankista toiseen tai sijoitusinstrumentteihin liittyvissä kauppatransaktioissa.
DAO (Distributed Autonomous Organization)	Hajautettu autonominen yhteisö/organisaatio, jossa päätöksenteko perustuu koodiin tai yhteisön jäsenten äänestykseen lohkoketjua hyödyntämällä.
DApps (Decentralized Applications)	Lohkoketjuverkossa toimiva hajautettu digitaalinen sovellus.

DeFi (Decentralized Finance)	Lohkoketjussa toimiva hajautettu rahoituspalvelu, joka mahdollistaa rahoituspalveluiden toteutumisen suoraan kahden tahon välillä ilman keskitettyä kolmatta osapuolta.
DEX (Decentralized Exchange)	Lohkoketjussa toimiva hajautettu vaihtoalusta, jossa kaksi tahoa voi vapaasti vaihtaa kryptovaluuttoja toisiin kryptovaluuttoihin ilman kolmannen keskitettyä kolmatta osapuolta. Tunnetuimpia DEX:ejä ovat mm. Uniswap ja Sushiswap.
Digitaalinen vaihtoalusta (Exchange)	Digitaalinen markkinapaikka, jossa voidaan suorittaa fiat-valuuttojen ja kryptovaluuttojen välisiä osto- ja myyntitoimeksiantoja sekä kryptovaluuttojen vaihtoja toisiin kryptovaluuttoihin. Tunnetuimpia digitaalisia vaihtoalustoja eli kryptovaluuttapörssejä ovat mm. Binance, Coinbase ja Kraken.
DL (Distributed Ledger)	Hajautettu tilikirja. Tietokanta, joka on jatkuvasti päivitettynä ja kaikkien tilikirjan osapuolten (noodien) saatavilla. Kaikki noodit voivat lisätä tietoa tilikirjaan ja lisätty tieto päivittyy automaattisesti näkyväksi kaikille noodeille.
DLT (Distributed Ledger Technologies)	Hajautetun tilikirjan teknologiat tarkoittaa lohkoketjuteknologian ylätason käsitettä, joka perustuu hajautettuun tilikirjaan.
Ethereum	Yksi tunnetuimmista julkisista lohkoketjuista. Ethereumin lohkoketjussa voidaan toteuttaa P2P-maksutapahtumia, luoda älysopimuksia sekä dApps:eja.
FATF (Financial Action Task Force)	Taloudellisen yhteistyö- ja kehitysjärjestö OECD:n alaisuudessa toimiva hallitusten välinen toimintaryhmä, jonka tehtävänä on luoda toimintamalleja ja säädöksiä estämään rahanpesua, terrorismia ja joukkotuhoaseiden rahoitusta sekä leviämistä.

Fiat-valuutat	Vaihdannan väline, jolla ei hyödykkeenä ole käyttöarvoa, mutta jonka arvo perustuu hallinnon luomiin säännöksiin tai lakeihin. Perinteisiä valtioiden liikkeelle laskemia valuuttoja kuten dollaria ja euroa luonnehditaan fiat-valuutoiksi.
FinTech (Financial Technology)	Finanssiteknologia on useimmiten tietotekniikkaan keskittynyttä teknologiaa, jota käytetään pankki-, rahoitus-, vakuutus- ja sijoituspalveluiden tuottamiseen.
G20	19 rikkaimmasta maasta ja Euroopan unionin edustuksesta koostuva ryhmä, jonka tarkoituksena on toimia yhteistyö- ja neuvontafoorumina kansainvälisistä rahoitusjärjestelmää koskevissa asioissa.
Hawala	Eräänlainen rekisteröimätön ja sääntelemätön rahansiirtojärjestelmä tai epävirallinen arvonsiirtojärjestelmä, jonka kautta jäsenet lähettävät rahaa. Järjestelmää käytetään rahan siirtämiseen erityisesti niille alueille, joissa pankkipalveluiden saatavuus on heikompaa.
Hajautettu tilikirja (Ledger)	Tapahtumarekisteri, johon lohkoketjussa suoritetut transaktiot tallennetaan. Noodit (nodes) ylläpitävät erillään omaa kopiotaan hajautetusta tilikirjasta ja tekevät siihen itsenäisesti päivityksiä konsensusalgoritmin mukaisesti.
IMF (International Monetary Fund)	Kansainvälinen valuuttarahasto
ICO (Initial Coin Offering)	Kolikkoanti. Kryptovaluutta-alalla toimivien yhtiöiden listautumisantia muistuttava joukkorahoitusmuoto, jossa yhtiö kerää rahoitusta uutta kryptovaluuttaa, applikaatiota tai palvelua varten ja rahoittaja saa vastineeksi tokeneita eli uuden liikkeeseen laskettavan kryptovaluutan yksiköitä.

IPO (Initial Public Offering)	Listautumisanti. Listaamaton yhtiö hakee osakkeidensa listaamista pörssiin julkisen kaupankäynnin kohteeksi, tarkoituksenaan saada yhtiölle kasvurahoitusta, tunnettuutta, kasvattaa markkina-arvoa tai saada osakkeille likviditeettiä.
Konsensusalgoritmi	Mekanismi, jolla konsensus saavutetaan. Algoritmi mahdollistaa uusien transaktioiden merkitsemiseen tilikirjaan sekä noodien resurssien jaon siten, ettei yksittäisen toimijan luotettavuudella ole merkitystä.
Konsensusprotokolla	Tilikirjaan suoritettavien uusien merkintöjen tekeminen vaatii konsensusalgoritmin mukaisesti noodien yhteisymmärryksen eli matemaattisilla menetelmillä muodostuvan konsensuksen. Tilikirja päivitetään konsensuksen muodostumisen jälkeen.
Konsortio	Kahden tai useamman organisaation yhteenliittymä, jossa tavoitteena on yhteenliittymän osapuolten edun ajaminen.
Kryptografia	Salausmenetelmä, jolla pyritään estämään kolmannen osapuolen pääsy salattuihin tietoihin.
Kryptovaluutta	Kryptografisesti suojattu digitaalisessa muodossa oleva valuutta.
KYC (Know Your Customer)	Asiakkaan tuntemistiedot ja asiakkaan tuntemiseen liittyvät velvoitteet. KYC-velvoitteet perustuvat yleensä kansalliseen tai kansainväliseen sääntelyyn ja niiden tavoitteena on AML-/CFT-toiminnan estäminen.
Ledger	Tilikirja.
Lohkoketju (Blockchain)	Hajautettu tietokanta, joka prosessoi ja tallentaa kronologisesti tietoa ketjutettuun ja muuttamattomaan, hajautettujen tietokoneiden verkkoon.
Noodi (Node)	Tietokone jonkin verkon osana. DLT:n yhteydessä noodi on DLT:n toimintaan osallistuva tietokone.

	Noodit ylläpitävät kopioita lohkoketjun datasta ja voivat myös prosessoida transaktioita. Lohkoketjuun tallennettua informaatioita ei voida tuhota tai menettää tuhoamatta jokaista verkkoon sidottua täyttä noodia.
Oraakkeli	Kolmannen osapuolen tarjoama lohkoketjun ulkopuolinen tietolähde.
P2P (Peer to Peer)	Hajautettu alusta, jolla kaksi tahoa on vuorovaikutuksessa toisiinsa ilman välissä toimivaa kolmannen osapuolen palveluntarjoajaa.
PKI (Public Key Infrastructure)	Julkisen avaimen salaus. Kokoelma toimintamalleja datan salaamiseksi hyödyntämällä yksityistä ja julkista avainta.
Proof of Stake (PoS)	Yksi lohkoketjuteknologiassa hyödynnettävä konsensusalgoritmin muoto.
Proof of Work (PoW)	Yksi lohkoketjuteknologiassa hyödynnettävä konsensusalgoritmin muoto.
Rahoituspalvelut	Pääsääntöisesti pankkien ja muiden rahoituslaitosten rahoituksen välityksen ja sitä palvelevan toiminnan lukuun ottamatta vakuutus- ja eläkepalveluja.
Single point of failure	Yksi vikapiste. Järjestelmän osa, joka kaatuessaan kaataa koko järjestelmän toiminnan.
Security-token	Digitaalisessa muodossa oleva arvoa sisältävän varallisuusmuodon osa. Esimerkiksi kiinteistö, auto tai osake voidaan pilkkoa osiin ja jokaisen osan arvo on kiinnitetty yksittäiseen security-tokeniin.
Stablecoin	Yksityisen tahon liikkeelle laskema digitaalinen valuutta, jonka arvo on sidottu johonkin varallisuuteen tai vaihtoehtoisesti matemaattiseen algoritmiin.
Syndikoitu luotto	Useamman rahoittajan yhteisesti myöntämä luotto.

Tekoäly (Artificial Intelligence, AI)	Koneen kyky käyttää perinteisesti ihmisen älyyn liitettyjä taitoja kuten päättelyä, oppimista, suunnittelemista tai luomista.
Token	Lohkoketjuun kytketty digitaalisessa muodossa oleva omaisuus, jonka arvo on sidottu tokeniin.
Trade Finance	Yrityksille tarjottuja rahoituspalveluratkaisuihin liittyviä tuotteita, joita hyödynnetään erilaisissa kaupallisissa transaktioissa. Esimerkkejä näistä ovat mm. pankkitakaukset eli remburssit ja dokumenttimaksut.
Virtuaalivaluutta	Digitaalisessa muodossa oleva arvon vastine. Virtuaalivaluutat kattavat mm. kryptovaluutat sekä yksityisten yritysten liikkeelle laskemat tokenit.
Virtuaalivaluuttalompakko	Julkisen avaimen salaukseen (PKI) perustuva, lohkoketjuihin yhteydessä oleva tietokoneohjelma, joka mahdollistaa virtuaalivaluutoiden lähettämisen ja vastaanottamisen sekä tilin hallinnoinnin.
Älysopimus	Digitaalinen tietokoneohjelma, joka on koodimuotoinen, suoritetaan lohkoketjuverkossa ja voi toteuttaa sisäisestä logiikastaan riippuen erilaisia lopputulemia.

Sisällys

Kuvat

Liitteet

1 Johdanto

Lohkoketjuteknologian tällä hetkellä herättämää kiinnostusta on verrattu jopa internetin alkuaikoihin, missä varsinainen tekninen ymmärrys oli useissa tapauksissa vielä alkeellisella tasolla, mutta into hyödyntää uutta teknologiaa vaikutti lähes rajattomalta. Lohkoketjuteknologian saaman suuren mediahuomion myötä keskustelussa on kieltämättä havaittavissa samoja piirteitä. Lohkoketjuteknologian poikkeuksellisen nopea kehitys, virtuaalivaluuttojen suosion räjähdysmäinen kasvu sekä lohkoketjuteknologian mahdollistamat lukuisat käyttötapaukset ja hyödyt ovat kasvattaneet teknologiasta globaalisti laajalti kiinnostavan niin yksityishenkilöille, julkiselle sektorille kuin myös liike-elämään. Nopea kehitys on myös pakottanut edellä mainittuja tahoja sekä kansallisia ja kansainvälisiä päättäjiä pohtimaan lohkoketjuteknologian mahdollisuuksia, hyötyjä, riskejä sekä haittoja nyt ja tulevaisuudessa.

Lohkoketjuteknologian mahdollistama maksamisen kehittyminen, virtuaalivaluutat sekä entistä nopeampi datan siirto turvallisesti, kustannustehokkaasti ja hajautetusti tekevät aiheesta erityisen ajankohtaisen pankkisektorilla. Maksamisen muutos ja virtuaalivaluutat pakottavat pankkisektoria tarkastelemaan kriittisesti omaa teknistä nykytilaansa ja samalla varautumaan uusiin, tuntemattomiin ja tulevaisuudessa arvaamattomiin riskeihin esimerkiksi teknologisesti tai pankkisääntelyn puitteissa pakollisen talousrikostorjunnan näkökulmasta.

Tämän opinnäytetyön aiheena on selittää lohkoketjuteknologian perusperiaatteita sekä kuvata pankkisektorin nykytilaa vuonna 2022 lohkoketjuteknologian näkökulmasta. Lisäksi tämä opinnäytetyö kuvaa lohkoketjuteknologian vaikutuksia pankkisektorille nyt ja tulevaisuudessa, huomioiden kyseisen teknologian mukanaan tuomia mahdollisuuksia, hyötyjä ja riskejä. Tätä opinnäytetyötä lukiessa on hyvä muistaa, että opinnäytetyö käsittelee pankkisektoria globaalisti. Suomalaista pankkisektoria voidaan pitää globaalilla mittapuulla monelta osin edelläkävijänä sekä teknisin että laadullisin mittarein mitattuna. Tästä johtuen lohkoketjuteknologian merkitys suomalaiselle pankkisektorille ei ole suoraan vertailukelpoinen suhteessa maihin, jossa esimerkiksi datan puutteellinen laatu,

henkilötietojen luotettavuus, erittäin korkeat maksupalveluiden hinnat tai jopa korruptio ovat ajankohtaisia ongelmia.

Opinnäytetyön tutkimuskysymykset ovat:

- Miten lohkoketjuteknologia toimii?
- Mitä vaikutuksia lohkoketjuteknologialla on pankkisektorille?
- Mitä hyötyjä lohkoketjuteknologialla voidaan saavuttaa pankkisektorilla?
- Mitä riskejä lohkoketjuteknologian hyödyntämiseen pankkisektorilla liittyy?

Tämän opinnäytetyön tavoitteena vastata tutkimuskysymyksiin ja luoda kattava ajankohtainen kuvaus lohkoketjuteknologian vaikutuksista pankkisektorille useista eri näkökulmista.

2 Pankkisektori

Finanssisektori on talousjärjestelmän osa, joka muodostuu yritys- ja yksityisille asiakkaille talouspalveluja tarjoavista yhtiöistä ja instituutioista. Finanssisektori kattaa laajan kirjon toimialoja mukaan lukien pankkiliiketoiminta, investointiyhtiöt, vakuutusyhtiöt sekä kiinteistönvälitysyhtiöt. (Kenton, 2021)

Pankkisektori käsitetään yhdeksi finanssisektorin osaksi ja sen ensisijainen tarkoitus tallettajien varojen hallinnointi sekä lainananto yksityisille tahoille sekä liiketoiminnoille. Pankit myös toimivat maksunvälittäjinä mahdollistaen monitahoisen päivittäisen rahaliikenteen. Pankit on jaoteltu keskuspankkeihin, vähittäispankkeihin sekä investointipankkeihin. Pankkien merkittävästä taloudellisesta roolista johtuen pankkien liiallisia riskejä aiheuttavaa toimintaa on pyritty estämään lainsäädännöllä maailmanlaajuisesti. (Hall, 2021)

Keskuspankkien tehtävänä on valtion rahapolitiikan määrittely ja toteuttaminen, rahan liikkeelle laskeminen sekä luotonannon valvonta. Keskuspankit voivat myös lainata varoja instituutioille tai jopa valtioille ja ne määrittelevät luottojen korkotasoja. (Segal, 2020)

Niin kutsuttujen vähittäispankkien tehtävänä on talletusten hallinnointi, rahan lainaaminen, maksujenvälitys, rahoitusvekseleiden ja shekkien tarjoaminen sekä esineiden ja asiakirjojen turvasäilytys. Näiden palvelujen lisäksi vähittäispankit voivat tarjota vakuutuspalveluja, sijoitusneuvontaa, korttimaksupalveluita ja muita finanssipalveluita yksityis- tai yritysasiakkaille. (Beattie, 2021)

Investointipankkien tehtävänä on toimia järjestelevänä välikätenä suurissa ja kompleksisissa finanssitoimissa kuten pörssilistautumisissa, fuusioissa tai taloudellisena neuvonantajana suurille finanssi-instituutioille kuten eläkeyhtiöille. (Hargrave, 2020)

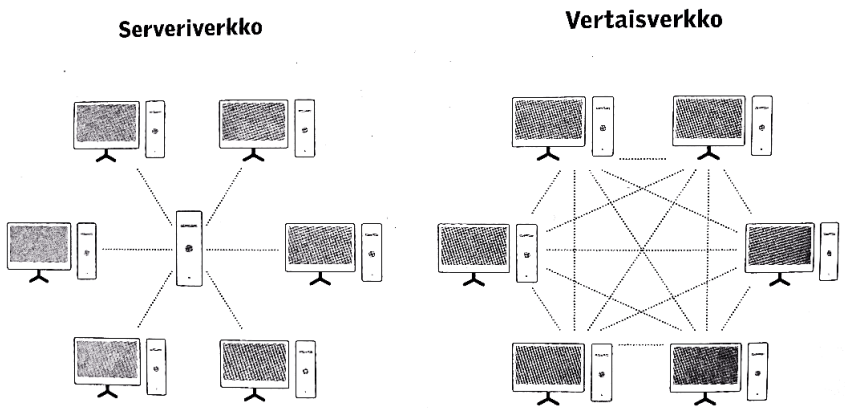
3 Lohkoketjuteknologia

Lohkoketjuteknologia voidaan määritellä yleistasolla hajautetuksi tietokannaksi, joka prosessoi ja tallentaa kronologisesti tietoa ketjutettuun ja muuttamattomaan, hajautettujen tietokoneiden verkkoon. Juuri hajautetun toiminnan merkitys lohkoketjuteknologiassa on olennaisin erottava tekijä perinteisiin datarakenteisiin nähden. Lohkoketjuteknologia perustuu keskitetysti kontrolloidun hallinnan sijaan lukuisten tietokoneiden muodostamasta tasa-arvoisesta vertaisverkosta, jossa tieto varmennetaan konsensusprotokollan avulla lohkoiksi kutsutuiksi, ennalta määrätyn kokoisiksi datapaketeiksi. Lohkoketjuteknologian keskeisiä teknologioita ovat muun muassa P2P-vertaisverkot, kryptografiset salausmenetelmät sekä konsensusalgoritmit. (Honkanen, 2017, p. 8; IBM, n.d.; Johansson et al., 2019, p. 56; Murray et al., 2019, p. 6; Natarajan et al., 2017, p. VII)

3.1 P2P-vertaisverkot

P2P- (Peer-to-Peer) eli vertaisverkoilla tarkoitetaan jaettua sovellusarkkitehtuuria, jossa tehtävät tai työtaakka jakaantuvat tasaisesti verkon osallistujien kesken. Vertaisverkossa osallistujat (noodit) sekä hyödyntävät verkkoa että tuovat siihen laskennallisia resursseja (prosessorin laskentateho, levytila tai kaista) ilman keskuspalvelimen tai muun keskitetyn tahon koordinointia (Kuva 1). (Johansson et al., 2019, pp. 60–61)

Kuva 1 Keskitetyn serveriverkon ja hajautetun vertaisverkon ero (Johansson et al., 2019, p. 60)

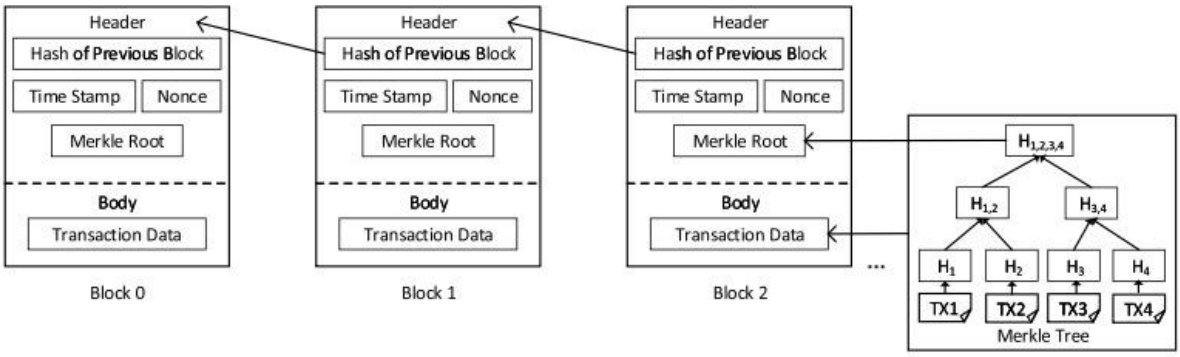


3.2 Lohkon rakenne

Yksittäisen lohkon voi kuvitella esimerkiksi kuutioksi, johon mahtuu vain määrätty määrä tietomerkintöjä. Lohkon täyttyessä siihen lisätty data varmennetaan oikeaksi ja lisätään ketjuun aiemmin lisätyistä tietomerkinnöistä täyttyneiden lohkojen jatkoksi. Lohkoketjun lohkoon talletettavat tietomerkinnät eli hyötykuorma voivat olla esimerkiksi virtuaalivaluuttojen varojensiirtomerkintöjä tai muita omaisuuslajien transaktioita, ohjeita, käskyjä (esim. arvopapereiden osto- tai myyntitarjouksia), omistus- tai tekijänoikeuksien muutoksia tai vaikka toimintalogiikkaansa toteuttavia älysopimuksia. (Honkanen, 2017, p. 8; Johansson et al., 2019, pp. 28, 30)

Yksittäinen lohko koostuu header- ja body-osasta. Body sisältää kaiken yksittäiseen lohkoon lisätyn hyötykuorman. Header koostuu edellisen lohkon hajautustiivisteestä (hash), aikaleimasta (timestamp), lohkon uniikista satunnaisnumerosta (nonce) sekä Merkle Root-nimisestä tiivisteestä, joka koostaa matemaattisella algoritmilla body-osaan talletetut transaktiot. Konsensusprotokollat vertaavat Merkle Root-tiivisteitä toisiinsa lohkoon lisätyn hyötykuorman verifioimiseksi. (Liang, 2020, pp. 122–123)

Kuva 2 Lohkon rakenne (Liang, 2020, p. 123)

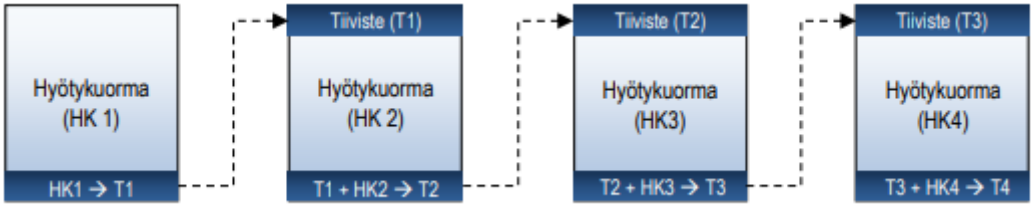


Lohkoketjuteknologiassa vanhoja tietomerkintöjä ei poisteta lainkaan, vaan kaikki kirjaukset merkitään tietokantaan uusina kirjauksina. Tätä kutsutaan append only -rakenteeksi. Juuri muuttumattomuus mahdollistaa lohkoketjun hyödyntämisen turvallisena tietokantana, sillä edes tietoja lohkoketjuun tallentanut käyttäjä ei pysty muuttamaan tai poistamaan kertaalleen säilöttyjä tietoja. (Honkanen, 2017, p. 8; Mattila et al., 2019, pp. 30–31)

3.3 Hajautustiiviste

Hajautustiivistettä voidaan kuvailla aikaleimalla varustetuksi ja kryptografisesti suojatuksi digitaaliseksi allekirjoitukseksi, joka muodostuu lohkoketjun hajautettujen osapuolten varmistettua lohkon sisällön. Hajautustiivisteen tarkoituksena on todentaa lohkoihin tallennetun tiedon muuttumattomuus. Yhden lohkon sisällön muuttaminen jälkikäteen missä tahansa lohkoketjun kohdassa vaikuttaisi kyseisen lohkon hajautustiivisteeseen, ja sitä kautta jokaiseen sitä seuraavan lohkon hajautustiivisteeseen (Kuva 2, Kuva 3). (Honkanen, 2017, p. 8; Mattila et al., 2019, pp. 30–31; Murray et al., 2019, p. 6; Natarajan et al., 2017, pp. VII, 8–9)

Kuva 3 Lohkoketjutietorakenteen muodostuminen ja hajautustiivisteen käyttö (Mattila et al., 2019, p. 30)



3.4 Kryptografiset menetelmät ja PKI

Kryptografialla viitataan yleisesti salausprotokollien rakentamiseen sekä analysointiin, millä estetään viestien luvaton lukeminen kolmansien osapuolten toimesta. Nykypäivän kryptografia linkittyy monitahoisesti mm. matematiikkaan, fysiikkaan, tietojenkäsittelytieteisiin, viestintätieteisiin sekä sähkötekniikkaan. Sen avulla pyritään varmistamaan datan turvallinen, kiistämätön, luotettava sekä eheä käsittely erilaisissa verkkoympäristöissä ja sovelluksissa. (Johansson et al., 2019, pp. 57–58)

Julkisen avaimen salaus (Public Key Infrastucture) on datan salaukseen käytetty kokoelma toimintamalleja, jotka perustuvat digitaalisten todistusten luomiseen, jakamiseen, käyttöön, tallentamiseen, hallinnointiin, sekä julkisen avaimen salaamiseen. Digitaalisen todistuksen tarkoituksena on minkä tahansa tahon, kuten esimerkiksi henkilön, tietokoneen, ohjelmistokokonaisuuden identiteetin todentaminen. Julkisen avaimen salaus perustuu

julkisesta ja yksityisestä avaimesta koostuvaan kahden avaimen järjestelmään siten, että yhtä julkista avainta kohden on kytkettynä yksi yksityinen avain. Julkinen avain on nimensä mukaisesti julkinen, mutta yksityinen avain on omistajalleen henkilökohtainen, sillä se saattaa pitää sisällään pääsyn henkilökohtaiseen omaisuuteen tai tietoon. (Johansson et al., 2019, pp. 58–60)

PKI-teknologiaa ja kryptografisia menetelmiä hyödynnetään erityisesti lohkoketjuteknologiassa, sillä lohkoketjuissa ihmisiin ja organisaatioihin kohdistettu luottamus on korvattu matemaattisesti. Lohkoketjun jokainen tietomerkintä on PKI-teknologiaa hyödyntämällä toimeenpanijansa digitaalisesti allekirjoittama, jokainen tietomerkintä on kiinnitetty edeltävään lohkoon hajautustiivisteen avulla ja tietomerkinnät on tallennettu tilikirjaan konsensusalgoritmin avulla. (Johansson et al., 2019, pp. 130–132)

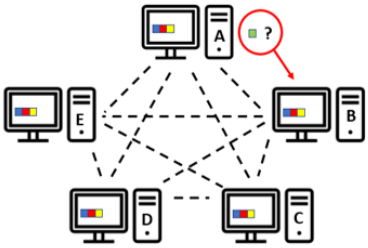
Esimerkiksi kryptovaluuttalompakot ovat julkisia ja avoimesti tarkasteltavissa, mutta lompakoille talletettuja varoja voidaan hallinnoida ainoastaan yksityisellä avaimella. Julkisessa lohkoketjussa voidaan esimerkiksi tarkastella vapaasti kahden eri kryptovaluuttalompakon välisiä varojen siirtoja. Ilman yksityistä avainta, kyseisten lompakoiden omistajia tai varojen alkuperää ja käyttötarkoitusta ei kuitenkaan voida todentaa. (Binance, 2019)

3.5 Konsensusprotokolla

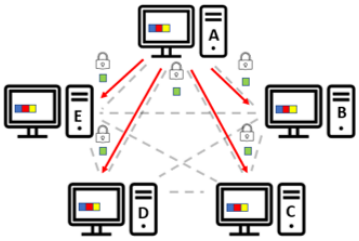
Lohkoketjuteknologian hajautettu perusta edellyttää lohkoketjun käyttäjien saavuttavan konsensuksen lohkoon lisätyn uuden hyötykuorman todenmukaisuudesta. Konsensusmekanismi perustuu ennalta määrättyyn matemaattiseen algoritmiin, joka vaihtelee konsensusprotokollasta, lohkoketjun tyypistä ja käyttötarkoituksesta riippuen. Periaatteessa kuka tahansa lohkoketjun käyttäjä voi ehdottaa uuden hyötykuorman lisäämistä lohkoon (pois lukien luvanvaraiset lohkoketjut, joissa tietoa saavat lisätä vain määrätyt käyttäjät). Hyötykuorman lisäämisen jälkeen konsensusprotokollasta riippuen määrätty määrä noodeja todentaa algoritmin perusteella lohkoon lisätyn hyötykuorman todenmukaisuuden, jonka jälkeen hyötykuormaa sisältävä lohko todetaan validiksi ja se lisätään osaksi lohkoketjua. Lohkoketjuverkossa lisätty ja validoitu hyötykuorma on tilikirjassa kaikkien noodien nähtävillä (Kuva 4). Tämän jälkeen aletaan muodostamaan

jälleen uutta lohkoa. (Honkanen, 2017, pp. 8–9; Johansson et al., 2019, p. 62; Natarajan et al., 2017, pp. 1–9)

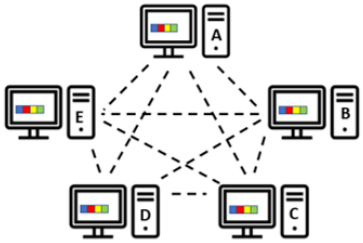
Kuva 4 Uuden lohkon muodostuminen lohkoketjuun



1. Lohkoketjuverkon noodi A ehdottaa hyötykuorman lisäämistä lohkoon siten, että hyötykuorma muodostaa uuden lohkon.



2. Uuden lohkon hyötykuormasta muodostuva Merkle Root-tiiviste jaetaan lohkoketjun noodeille (B-E) tarkistettavaksi.



3. Kaikki noodit todentavat lohkon todenmukaisuuden konsensusprotokollan mukaisesti eli validoivat lohkon. Sen jälkeen noodit päivittävät lisätyn hyötykuorman omaan hajautettuun tilikirjaansa (ledger).

Konsensusmekanismin merkitys korostuu tilanteissa, joissa useampi käyttäjä pyrkii lisäämään lohkoketjuun toisiinsa nähden ristiriitaista tietoa. Konsensusprotokolla varmentaa tällöin tiedon oikeellisuuden. Lohkoketjun väärentämättömyys estää esimerkiksi saman arvonmitan kaksoiskäytön, missä alkuperäinen arvo siirrettäisiin samanaikaisesti kahteen eri paikkaan. Kaksoiskäyttö kuitenkin vaatisi merkittävän suuria resursseja ja halua uuden haaran luomiseksi lohkoketjuun. Näin ollen kaksoiskäytön mahdollisuutta voidaan pitää lähinnä teoreettisena. Konsensusprotokollista tunnetuimpina voidaan pitää Proof of Work -protokollaa sekä riittäviin panoksiin perustuvaa Proof of Stake -protokollaa. (Honkanen, 2017, pp. 8–9; Natarajan et al., 2017, p. 6)

3.5.1 Proof of Work

Proof of Work -protokolla perustuu tietokoneella ratkaistavien matemaattisten yhtälöiden ratkaisemiseen eli louhintaan. Matemaattisen yhtälön ratkettua lohkoketjuun lisätään uusi, varmennettu lohko. Lohkon lisäämisestä louhijalle muodostuu louhintapalkkio. On kuitenkin huomionarvoista, että Proof of Work -protokollassa matemaattiset yhtälöt vaikeutuvat lohkoketjun pidentyessä ja tästä syystä louhiminen vaatii merkittävää koneellista laskentatehoa. Suurissa lohkoketjuissa PoW-protokollan etuna on valtava laskentatehon tarve, jonka takia halukkuus lohkoketjun tulvittamiselle tai muulle hyökkäykselle vähäistä. Pienempien PoW-lohkoketjuprojektien kohdalla hyökkäys on kuitenkin helpommin toteutettavissa. PoW-protokollan yksi tunnistettu heikkous on louhinnasta aiheutuva korkea energian kulutus. (Bitcoinkeskus.com, 2020; Lorne & Cawrey, 2020, pp. 43–44; Murray et al., 2019, pp. 19–20)

3.5.2 Proof of Stake

Proof of Stake -protokolla on suunniteltu parannelluksi versioksi Proof of Work -protokollasta. PoW-protokollasta eroten PoS-protokollassa ketjuun lisättäviä lohkoja ei varmenneta louhimalla vaan kryptovaluuttaa omistavat osapuolet steikkaavat (staking) kryptovaluuttaomistuksiaan eli toisin sanoen lukitsevat omistuksensa lohkoketjun käyttöön. Steikkauksesta palkitaan suhteessa steikattuun kryptovaluuttojen määrään. Omistuksiaan riittävän suuren määrän steikkaavat tahot toimivat validaattoreina. PoS-protokollassa konsensus muodostuu joko lukuisten steikkauskriteerien perusteella tietyille validaattoreille, jotka varmentavat lohkon oikeellisuuden, tai vaihtoehtoisesti satunnaisesti valituille steikkaajille. PoS-protokollan merkittävimmät hyödyt ovat PoS-lohkoketjun turvallisuus sekä merkittävästi PoW-protokollaa vähäisempi energiankulutus. Vastaavasti PoS-protokollan heikkouksia ovat validaattorivastuun jakautuminen keskitetymmin kyseessä olevasta lohkoketjusta enemmän kryptovaluuttaa omistaneille henkilöille. PoW-protokollassa hajautuneisuus on siis PoS-protokollaa korkeammalla tasolla. (Bitcoinkeskus.com, 2020; Lorne & Cawrey, 2020, pp. 51–54)

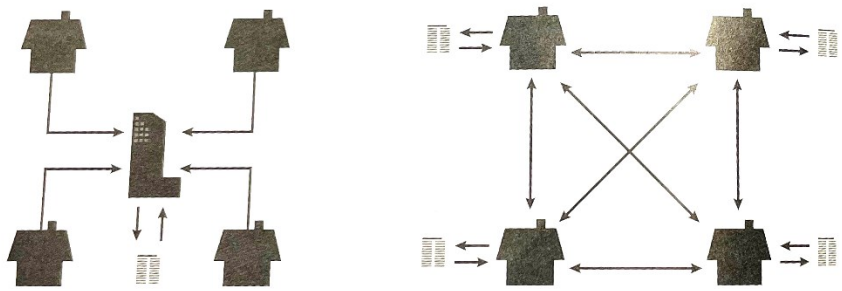
3.5.3 Muita konsensusprotokollia

Muita konsensusprotokollia ovat mm. Delegated Proof of Stake (DPoS), Liquid Proof of Stake (LPoS), Proof of History, Proof of Storage ja Practical Byzantine Fault Tolerance (pBFT). Konsensusmekanismien eroavaisuudet näkyvät monilla eri tavoilla kuten validoinnin hajautuneisuudessa, validaattoriksi pääsemisen rajoitteissa sekä lukuisissa teknisissä ominaisuuksissa, jotka heijastuvat suoraan lohkoketjun nopeuteen ja hajautuneisuuteen. (Bitcoinkeskus.com, 2020; Lorne & Cawrey, 2020, pp. 53–54)

3.6 Tilikirja

Kaikki lohkoketjuun tallennetut ja konsensusprotokollalla vahvistetut tietomerkinnät muodostavat kokonaisuutena hajautetun tilikirjan (ledger), jota voidaan tarkistaa reaaliaikaisesti vertaisverkon eri osapuolten toimesta. Lohkoketjuun tallennetut tietomerkinnät sisältävät aina aikaleiman, mikä mahdollistaa hyötykuorman jälkikäteisen tarkastelun tilikirjassa (Kuva 5). (Honkanen, 2017, p. 8; Johansson et al., 2019, p. 56; Liang, 2020, p. 122)

Kuva 5 Keskitetyn tilikirjan ja hajautetun tilikirjan ero (Johansson et al., 2019, p. 56)



3.7 Erilaiset lohkoketjut

Lohkoketjualustat voidaan jakaa karkeasti kolmeen alakategoriaan: julkiset, yksityiset ja niin kutsutut konsortio-lohkoketjut (Kuva 6). Julkisille ja yksityisille lohkoketjuille on yhteistä niiden perustuminen hajautettuun vertaisverkkoon ja molemmat lohkoketjun muodot

ylläpitävät konsensusprotokollan avulla tilikirjaa, joka on lähtökohtaisesti muuttamaton. (Harju, 2020; Honkanen, 2017, p. 9; Johansson et al., 2019, p. 75)

3.7.1 Julkiset lohkoketjut

Julkisia lohkoketjuja (public blockchain) ovat esimerkiksi Bitcoin- ja Ethereum -nimiset hajautetut lohkoketjut, joihin kuka tahansa voi liittyä ja joita kuka tahansa voi halutessaan hyödyntää. Julkisten lohkoketjujen huonoja puolia ovat vähäinen tai olematon yksityisyys, heikko turvallisuus sekä mahdollisesti merkittävä koneellisen laskentatehon tarve. (Harju, 2020; Honkanen, 2017, p. 9; IBM, n.d.)

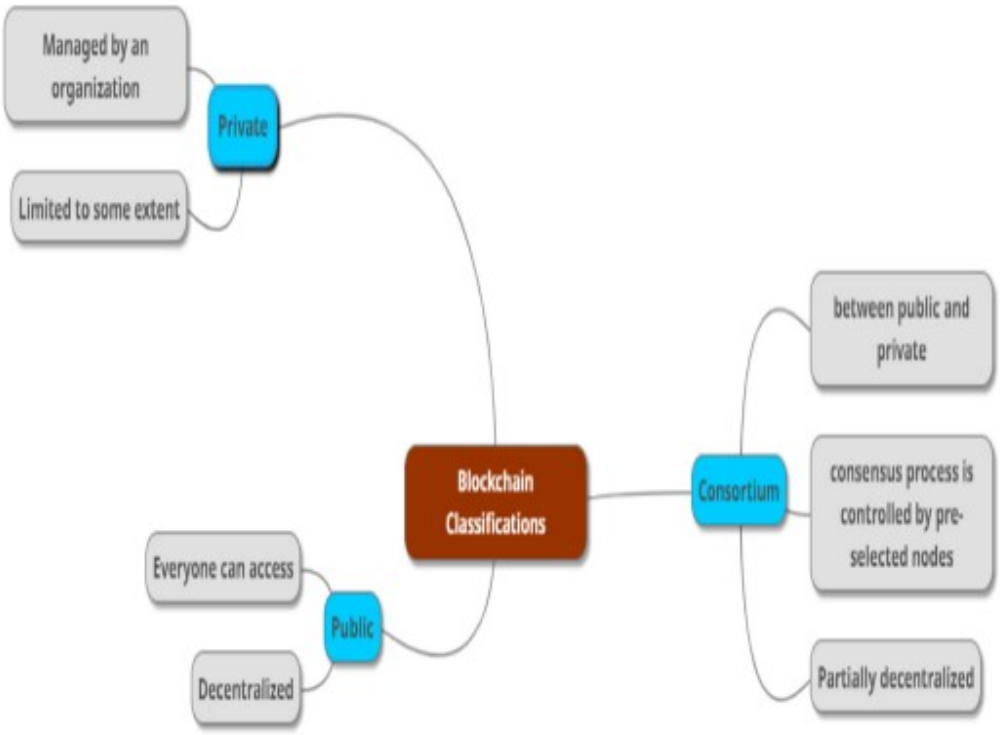
3.7.2 Yksityiset lohkoketjut

Yksityiset lohkoketjut (private blockchain) ovat julkisten lohkoketjujen kaltaisia, mutta ne on suunniteltu vain määrättyjen osapuolten keskitettyä käyttöä varten. Yksityistä lohkoketjua voidaan hyödyntää organisaation sisäisessä käytössä esimerkiksi auditoinneissa, uuden teknologian testauksessa tai useita järjestelmiä käsittävien transaktiokokonaisuuksien rakentamisessa lohkoketjualustalle. Alkuoletuksellisesti yksityiseen lohkoketjuun osallistuvat osapuolet luottavat toisiinsa. Organisaatio hallinnoi itse yksityistä lohkoketjua, määrittää yksityiseen lohkoketjuun osallistuvat tahot, toteuttaa konsensusprotokollaa ja ylläpitää jaettua tilikirjaa. (Harju, 2020; Honkanen, 2017, p. 9; IBM, n.d.)

3.7.3 Konsortio-lohkoketjut

Määriteltyjen yritysten yhteiset konsortiolohkoketjut ovat ulkopuolisilta tahoilta suljettuja lohkoketjuratkaisuja. Näin ollen konsortiolohkoketjut ovat ikään kuin julkisten ja yksityisten lohkoketjujen välimaastossa. Lohkoketjun ylläpito voidaan jakaa useiden tahojen kesken ja lohkoketjun käyttöoikeudet ja konsensusprotokolla voidaan yhdessä määritellä ja rajata ennalta. (Gomathi et al., 2021, p. 3; Harju, 2020; IBM, n.d.)

Kuva 6 Lohkoketjujen jaottelu. (Gomathi et al., 2021, p. 2)



3.7.4 Avoimet vs. luvanvaraiset lohkoketjut

Lohkoketjussa voidaan myös käyttää jakoa avoimiin ja luvanvaraisiin lohkoketjuihin. Avoimissa lohkoketjuverkoissa kuka tahansa voi olla osallisena, lohkoketjun hallinto ja ylläpito on hajautettu ja lohkoketjuun osallistuneet käyttäjät säilyvät anonyymeinä, eikä heidän tarvitse tuntea toisiaan. Lohkoketjun tilikirja on avoin ja läpinäkyvä kaikille lohkoketjuun osallisille. Vastaavasti avointen lohkoketjujen datan prosessoinnissa saattaa esiintyä hitautta ja avoimen lohkoketjun omistajan puuttuminen aiheuttaa tiettyjä juridisia haasteita. (Natarajan et al., 2017, pp. 11–12)

Luvanvaraiset lohkoketjut ovat tyypillisesti ainakin osin ulkoisesti hallinnoituja tai kontrolloituja ja vain ennalta valitut tahot voivat olla osallisia lohkoketjuverkossa. Osallisten identiteetin varmentaminen on tyypillisesti luvanvaraista lohkoketjua hallinnovan tahon tehtävä. Luvanvaraiseen lohkoketjuverkkoon osallistuvien tahojen keskinäinen luottamus on luvanvaraisuudesta johtuen avoimia lohkoketjuja korkeammalla tasolla ja tilikirjojen avoimuus ja läpinäkyvyys saattavat vaihdella eri tasoilla. Luvanvaraisuus mahdollistaa

nopeamman datan prosessoinnin ja juridisesta näkökulmasta luvanvaraisen lohkoketjun hallinto on selkeää. (Natarajan et al., 2017, pp. 11–12)

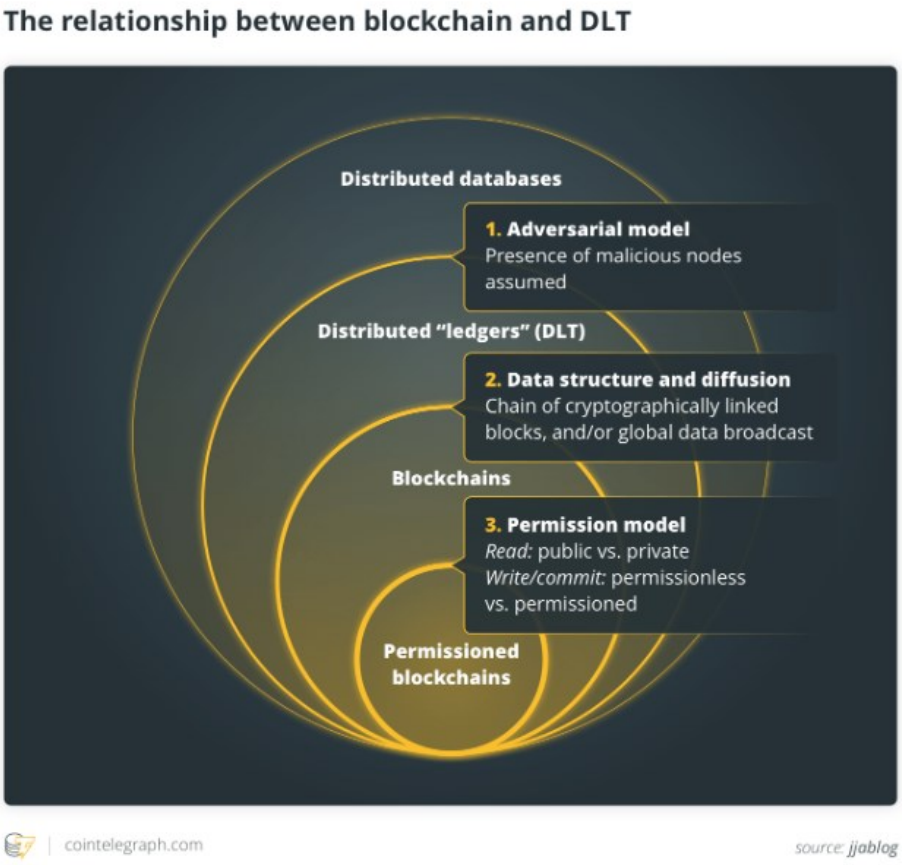
3.8 Lohkoketjuteknologia ja DLT

Lohkoketjun ja hajautetun tilikirjan (Distributed Ledger, DL) käsitteissä on eroja, vaikka niistä usein puhutaan samassa yhteydessä. Lohkoketjuteknologiaan ja hajautettuun tilikirjateknologiaan (Distributed Ledger Technology, DLT) liittyvä terminologia ei ole vielä saanut universaalia määrittelyä vaan kehittyy edelleen. (Natarajan et al., 2017, p. 2)

DLT on hajautettu tietokanta, jota hallinnoi usea käyttäjä. Lohkoketju on yksi DLT:n muoto, jossa hyödynnetään hajautustiivistettä (Kuva 7). Hajautustiivisteen avulla lohkoketju kerää tallennetut tapahtumat kronologisesti järjestettynä lohkoihin, jotka on kytketty toisiinsa. Hajautettu tilikirja taas tallentaa dataa toimijoiden kesken jaettuun tietokantaan. (Harju, 2020; Mattila et al., 2019, pp. 38–39; Natarajan et al., 2017, p. VII; R3, n.d.)

Kaikki hajautetut tilikirjat eivät siis hyödynnä lohkoketjuteknologiaa ja hajautetun tilikirjan määritelmää voidaan pitää laajempana ja vapaammin määriteltynä. Hajautetut tilikirjat eivät välttämättä sisällä kryptovaluuttoja, jotka taas lohkoketjuteknologiassa ovat usein olennaisia kannustinrakenteen luomiseen. Tyypillisesti erottavana tekijänä toimii myös lähdekoodin avoimuus, joka on lohkoketjuissa tyypillisesti avoin, kun vastaavasti hajautetuissa tilikirjoissa lähdekoodi on yleensä yksityisomisteinen. Vastaavasti lohkoketjuteknologialla ja hajautetulla tilikirjateknologialla yhteistä on tilikirjan hajautettu luonne, konsensusmekanismi sekä kryptografinen mekanismi. (Mattila et al., 2019, pp. 38–39; Natarajan et al., 2017, p. VII; R3, n.d.)

Kuva 7 Lohkoketjuteknologian ja DLT:n ero (Chandler, 2019)



3.9 Kryptovaluutat

Kryptovaluutat ovat lohkoketjujärjestelmiin sidottuja ja kryptografiseen tekniikkaan perustuvia digitaalisia varoja. (Natarajan et al., 2017, p. 3; Steinmetz et al., 2021, p. 1)

Lohkoketjujärjestelmillä voi olla lukuisia erilaisia käyttötarkoituksia ja niihin sidottujen kryptovaluuttojen tarkoituksena on sitouttaa varojen omistajia kyseisen lohkoketjujärjestelmän taloudelliseen tukemiseen. Juridisesta näkökulmasta ne toimivat arvonsäilyttäjinä, vaihdannan välineinä tai jossain tapauksissa arvopapereiden kaltaisena varallisuutena. (Steinmetz et al., 2021, pp. 1–2)

Financial Stability Boardin (FBS) määritelmän mukaan kryptovaluuttoihin lukeutuvat digitaaliset vaihtoalustat (exchanges) ja muut digitaaliset tokenit, kuten security-tokenit, varallisuussidonnaiset tokenit sekä käyttö-tokenit. Financial Action Task Force (FATF) mukaan virtuaalinen varallisuus määritellään seuraavasti: digitaalinen arvonmäärittäjä, jota voidaan

digitaalisesti vaihtaa, siirtää, käyttää maksuvälineenä tai hyödyntää investoinneissa. (Coelho et al., 2021, p. 3)

Sosioekonomisesta näkökulmasta kryptovaluutat ovat monialainen ilmiö. Samanaikaisesti kryptovaluutat mahdollistavat lainvastaisia toimia kuten rahanpesua, terrorismin rahoittamista ja veronkiertoa, kun taas toisaalta kryptovaluuttoihin pohjautuvalla teknologialla on potentiaalia radikaaliin positiiviseen muutokseen sosiaalisessa ja taloudellisessa kanssakäymisessä. (Steinmetz et al., 2021, p. 1)

3.9.1 Bitcoin

Bitcoin on tunnetuin lohkoketjuteknologiaan perustuva sovellus. Sen perusajatuksena oli Bitcoin-nimisten digitaalisten kryptovaluuttojen siirtäminen, säilyttäminen ja vastaanottaminen kahden osapuolen välillä turvallisesti. Olennaista Bitcoinissa on sen hajautettu luonne, joka mahdollistaa varojen siirrot ja säilytyksen ilman kolmannen osapuolen maksunvälittäjää. (Mattila et al., 2019, p. 57; Natarajan et al., 2017, p. 3)

3.9.2 Tokenit ja virtuaalivaluuttojen hankkiminen

Kryptovaluutoissa on merkittäviä eroja teknisen toteutuksen, arkkitehtuurin, hallinnon ja yleisemmin käyttötarkoituksen näkökulmasta. Lohkoketjujärjestelmiin sidottujen digitaalisten varojen lisäksi niin kutsuttuja tokeneita luonnehditaan kryptovaluutoiksi. Teknisesti tokenit ovat sidottuja lohkoketjuun ja voivat olla olemassa digitaalisen valuutan lomassa. Uusia tokeneita voidaan luoda helposti uusien kryptovaluuttaprojektien rahoittamiseksi ja tokenit muuttuvat tätä kautta spekulatiivisiksi varoiksi kyseiseen projektiin. Tätä ilmiötä kutsutaan ICO:ksi (Initial Coin Offering). (Steinmetz et al., 2021, pp. 1–2)

ICO:ssa kerätyt varat käytetään pääosin lohkoketjuprojektien luomiseen, kehittämiseen ja ylläpitoon. ICO:n päätarkoituksena on nopea varojen kerääminen. Vastaavasti ICO:jen suurimpia ongelmia ovat turvallisuus, regulaatio sekä liiallinen rahoitus. (Rangwala, 2017)

Virtuaalivaluuttaa voi hankkia myös ostamalla virtuaalivaluuttaa välittäviltä yrityksiltä. Käytännössä tämä tarkoittaa pankkitilillä olevan rahan vaihtamista digitaaliseksi valuutaksi. Virtuaalivaluuttaa varten tarvitset lohkoketjuun perustetun virtuaalivaluuttalompakon ja sinne perustetun tilin. Rahan siirrot virtuaalivaluutan välittäjältä virtuaalilompakkoon on yksi vahvistettu tapahtuma lohkoketjussa. (Harju, 2020)

3.9.3 Security tokenit

Security tokenilla tarkoitetaan arvopaperidipolia eli jonkun varallisuusluokan pilkkomista lohkoketjussa sijaitsevaksi digitaaliseksi arvopaperiksi. Security tokenien liikkeellelaskua kutsutaan STO:ksi (Security Token Offering). STO perustuu ICO:n tavoin tokenisaatioon eli määrätyn ominaisuuden kytkemistä lohkoketjussa sijaitsevaan digitaaliseen tokeniin. STO eroaa kuitenkin ICO:sta siten, että STO:n omistuksen taustalla on jokin oikea varallisuusmuoto, arvopaperi tai niiden osa. Arvopaperidipolien kautta olemassa olevaa omaisuutta voidaan pilkkoa helpommin siirreltäviin ja pienempiin eriin. Tällä hetkellä arvopaperidipolien käyttökohteet ovat pitkälti listaamattomia osakkeita ja Asiakastieto, Nordea, OP, Privanet ja Tieto ovatkin syksystä 2018 kehittäneet listaamattomien osakkeiden osakashallinnan ja osakevaihdon digitalisointia. Tulevaisuudessa arvopaperidipolien mahdollisuudet saattavat kuitenkin laajentua esimerkiksi urheiluseurojen, elokuvien, musiikkikappaleiden tai kiinteistöjen omistuksiin. Teoriassa minkä tahansa omaisuuden tokenisointi on mahdollista. (Johansson et al., 2019, pp. 118–119)

3.9.4 CBDC - Keskuspankkien digitaaliset valuutat

Keskuspankkien digitaaliset valuutat, CBDC:t (Central Bank Digital Currency) ovat yksinkertaisesti määriteltynä valtiollisten keskuspankkien luomaa perinteisen fiat-valuutan kaltaista valuuttaa digitaalisessa muodossa. Osa CBDC-sovellutuksista perustuu lohkoketjuun tai muihin DLT-ratkaisuihin ja osa saattaa suurella todennäköisyydellä perustua vain keskitettyyn tilikirjaan. Lohkoketjuun perustuvat keskuspankkien digitaaliset valuutat käyttävät tokenia fiat-valuutan digitaalisen version edustajana. CBDC:t kuitenkin eroavat merkittävästi kryptovaluutoista, koska CBDC:t ovat valtion liikkeelle laskemia ja ylläpitämiä, kun taas esimerkiksi Bitcoinin kaltaiset kryptovaluutat ovat ”rajattomia” eivätkä minkään

keskitetyn tahon tai valtion liikkeelle laskemia. CBDC:tä voi toki siirtää valtiollisten rajojen yli, mutta Bitcoinin tapauksessa valtiollisia rajoja ei periaatteessa ole olemassa. (Binance, 2021)

3.9.5 Stablecoinit

Niin kutsutut stablecoinit ovat digitaalisia tokeneita, joiden arvoa vastaava summa on katettu talletetuilla fiat-valuutoilla tai hyödykkeillä. Vaihtoehtoisesti stablecoinit voidaan sitoa varallisuuden sijaan tuettuun ja hajautettuun algoritmiin. Stablecoinien tavoitteena on vakaa arvonsäilyttäminen suhteessa siihen sidottuun varallisuuteen tai niiden johdannaisiin. (FATF, 2020, p. 6; FSB, 2019, p. 6)

Vaikka stablecoinit periaatteessa muistuttavatkin fiat-valuuttaa korvaavina digitaalisina tokeneina keskuspankkien digitaalisia valuuttoja, eroavat ne CBDC:istä merkittävästi. Stablecoinit ovat tyypillisesti yksityisen tahon liikkeelle laskemia ja sidottuja edellä mainitusti johonkin varallisuuteen tai algoritmiin. CBDC:t taas ovat valtiollisen keskuspankin liikkeelle laskemia fiat-valuutan vertaista valuuttaa digitaalisessa muodossa. (Binance, 2021)

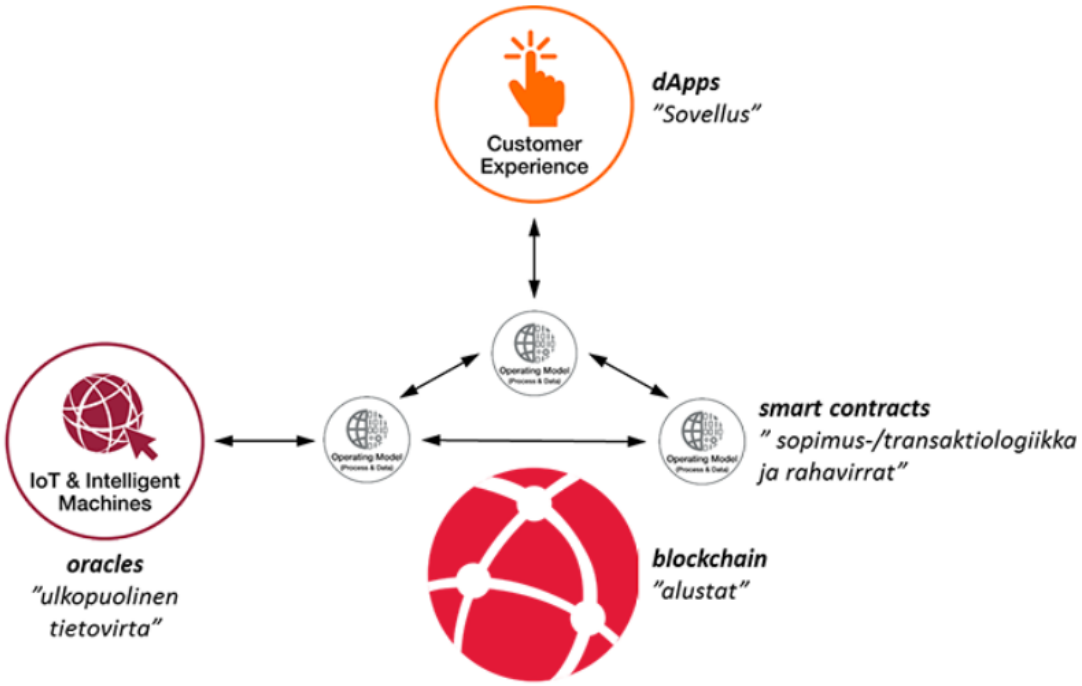
3.9.6 Kryptovaluuttalompakko

Kryptovaluuttalompakko on digitaalinen työkalu, joka on yhteydessä yhteen tai useampaan lohkoketjuun. Kryptovaluuttalompakko ei kirjaimellisesti säilö virtuaalivaluuttaa vaan lompakko muodostaa tarvittavan informaation lohkoketjulle, jonka perusteella voidaan todeta, että kyseisten virtuaalivaluuttojen omistajuus on merkitty kyseessä olevalle kryptovaluuttalompakolle. Kryptovaluuttalompakolla on identifioivasta numerosarjasta muodostettu osoite, joka perustuu yksityisen ja julkisen avaimen infrastruktuuriin. Tämä osoite määrittää tarkan ”sijainnin” lohkoketjussa, jonne virtuaalivaluutat voidaan siirtää. Virtuaalivaluutat eivät siis todellisuudessa koskaan ”poistu” lohkoketjusta. Jotta varojen lähettäminen kryptovaluuttalompakkoon onnistuu, tulee varojen lähettäjän tietää varojen vastaanottajan kryptovaluuttalompakon julkinen avain (Public Key). Yksityinen avain (Private Key) mahdollistaa kryptovaluuttalompakon käytön ja tästä syystä avainta ei tule luovuttaa kenenkään muun käyttöön. (Binance, 2019)

3.10 Lohkoketjun komponentit

Lohkoketjuteknologiassa avainkomponentteja ovat älysopimukset (Smart Contracts), hajautetut sovellukset (dApps) sekä oraakkelit (Oracles) (Kuva 8). Kyseiset komponentit ovat verrattavissa perinteiseen sovelluskehitykseen, joissa jokaisella komponentilla on osansa kokonaisuuden rakentamisessa. Älysopimukset ovat ohjelmoituja sopimuksia, jotka määrittelevät transaktiologiikkaa ja esimerkiksi rahan liikkeitä. Hajautetut sovellukset ovat sovelluksia, jotka on rakennettu älysopimusten ympärille ja oraakkelit ovat lohkoketjun ulkopuolisia tietolähteitä. (Harju, 2020)

Kuva 8 Lohkoketjun avainkomponentit (Harju, 2020)



3.10.1 Älysopimukset

Älysopimukset ovat ohjelmointikielellä koodimuodossa ohjelmoituja digitaalisia tietokoneohjelmia, joista suoritetaan ja säilytetään hajautetusti lohkoketjuverkossa, ja jotka voivat toteuttaa erilaisia ohjelmoituun logiikkaan perustuvia lopputulemia. Älysopimukset ovat autonomisia ja itsesuoriutuvia sopimuksia kahden tai useamman osapuolen välillä. Niiden toimeenpano ei siis ole riippuvainen kolmannen osapuolen toimijasta. (Mattila et al., 2019, pp. 40–41; Murray et al., 2019, p. 8; Wang et al., 2020, p. 813)

Teoriassa mikä tahansa tietokoneelle suoritettava toimenpide voidaan suorittaa älysopimuksella. Lohkoketjun tilikirjaan tallennettu transaktio tai tieto antaa älysopimukselle tarvittavan triggerin, jonka perusteella älysopimus toteuttaa siihen ohjelmoidut toimenpiteet. Tämän jälkeen älysopimuksen toteuttamat transaktiot tallentuvat jälleen lohkoketjun tilikirjaan. (Natarajan et al., 2017, p. 29)

Toisin sanoen älysopimuksia hyödyntämällä määrätyt osapuolet voivat lukita tiettyjä, älysopimuksen hallinnoitavaksi määriteltyjä varallisuuseriä toimimaan ennalta määrätyllä tavalla tulevaisuudessa. (Mattila et al., 2019, p. 24)

Älysopimusten hyödyntämismahdollisuudet ovat merkittävät ja ne voivat mahdollistaa normaalin sopimusoikeuden puitteissa tehtyjä sopimuksia turvallisempia sopimusten toimeenpanoja. Älysopimukset mahdollistavat varojen ja varallisuuden siirtelyn sekä maksamisen automatisoinnin, ja tästä syystä älysopimuksia voidaan tulevaisuudessa hyödyntää esimerkiksi johdannaismarkkinoilla, yrityskaupoissa ja fuusioissa sekä varojen ja varallisuuden siirroissa. Ne myös mahdollistavat neuvotteluun, varmennuksiin ja sopimusten toimenpanoon liittyviä kustannussäästöjä. (Natarajan et al., 2017, p. 29; Wang et al., 2020, p. 813)

Internetiin yhdistettyjen laitteiden jatkuvasti lisääntyvä määrä kasvattaa myös älysopimusten sovellutusmahdollisuuksia. (Murray et al., 2019, pp. 8–9)

Käytännön esimerkkinä tällaisesta sovellutuksesta voitaisiin pitää esimerkiksi ajoneuvon liittämistä älysopimukseen siten, että tietullit, pysäköinti- ja vakuutusmaksut toteutuvat automaattisesti kuljettajan käytön mukaan. Koodille rakentuvina ohjelmina älysopimukset eivät kuitenkaan aina täytä juridisen sopimuksen tunnusmerkkejä. (Kinnunen et al., 2017, pp. 14, 16; Mattila et al., 2019, pp. 40–41)

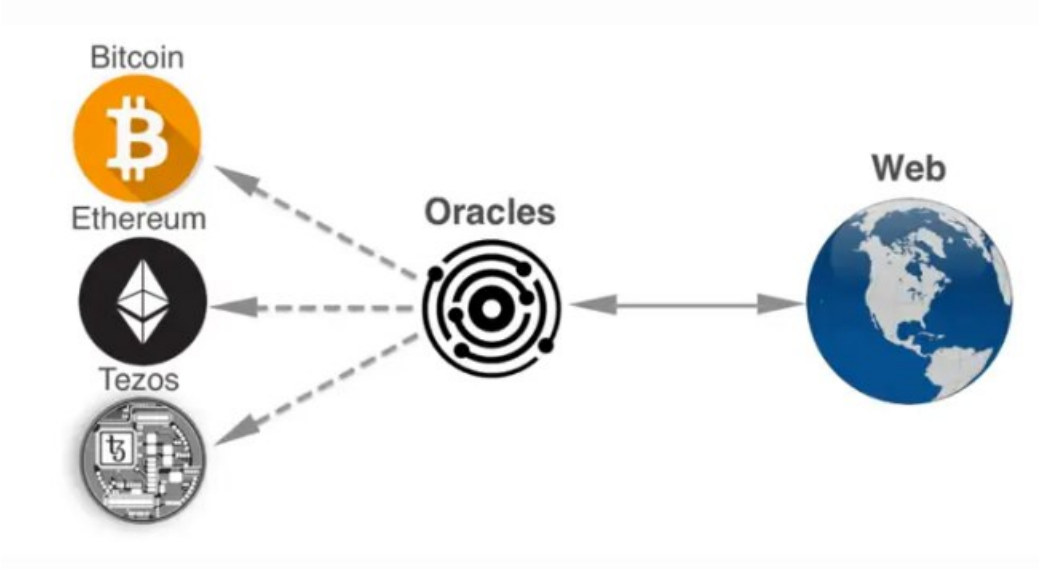
3.10.2 Oraakkelit

Älysopimukset eivät ole riippuvaisia kolmannen osapuolen toimijasta, vaan älysopimukset nojaavat luotettuihin datalähteisiin eli niin kutsuttuihin oraakkeleihin, jotka välittävät ennalta ohjelmoidulla ja algoritmeja hyödyntävällä tavalla ulkoista dataa lohkoketjuun

turvallisesti. Esimerkkejä oraakkeli -datalähteistä voivat olla esimerkiksi itsenäiset sensorit (esim. sade- tai lämpömittarit), online-syötteet (esim. osakekurssien muutokset, urheilukilpailujen tulokset) ja ihmisten tekemät päätökset (esim. Korkeimman oikeuden päätökset, kauppasopimukset) (Kuva 9). (Murray et al., 2019, pp. 8–9)

Oraakkelit siis tarjoavat lohkoketjuille ulkoista dataa, jota lohkoketjuun ei itsessään ole järkevää kerätä tai lohkoketju ei kykene todentamaan kyseistä dataa oikeaksi. Oraakkeleilla on siis merkittävä osuus komponenttina lohkoketjualustassa. (Harju, 2020)

Kuva 9 Oraakkelin toiminta (Lorne & Cawrey, 2020, p. 160)



3.10.3 Hajautetut sovellukset

Hajautetut sovellukset (Decentralized Applications, dApps) ovat älysopimuksilla toimivia lohkoketjuun sidottuja sovelluksia. Tyypillisesti hajautettujen sovellusten arkkitehtuuri on suunniteltu siten että taustaohjelmatoiminnot (backend) on rakennettu älysopimusten ympärille ja kevyt käyttöliittymä (frontend) on vuorovaikutuksessa taustaohjelmatoimintojen kanssa. Tämän tyyppiset sovellukset tekevät lohkoketjusta ohjelmoitavamman ja käytettävämmän. (Lorne & Cawrey, 2020, p. 90)

Hajautettujen sovellusten tärkein ominaisuus on muuttamattomuus, mikä tarkoittaa, ettei kukaan keskitetty toimija kykene muuttamaan hajautetun sovelluksen koodia lohkoketjuun julkaisun jälkeen. Useissa keskitetyissä sovelluksissa keskitetty osapuoli voi esimerkiksi

päättää mitä käyttäjät voivat ja eivät voi nähdä. Tästä syystä hajautettujen sovellusten käyttötarpeisiin törmätään ensisijaisesti siellä, missä keskitettyihin järjestelmiin on muodostunut pullonkauloja keskitetyn kolmannen osapuolen subjektiivisesta päätöksenteosta johtuen. Toinen merkittävä ominaisuus hajautetuissa sovelluksissa on, että ne mahdollistavat tehokkaat ja turvalliset varojen siirrot lohkoketjun avulla. (Lorne & Cawrey, 2020, pp. 90–91)

Hajautetuissa sovelluksissa on lukuisia haasteita, joita voi ilmetä sovellusten käyttöönotossa, asiakkaan käyttökokemuksessa, nopeudessa ja skaalautuvuudessa. Kyseisiä ongelmia on ilmennyt kaikilla lohkoketjualustoilla. Lohkoketjuun liitetyn datan muuttamattomuus tekee virheiden päivittämisen haastavaksi. (Lorne & Cawrey, 2020, pp. 90–91)

Hajautetut sovellukset ovat vielä verrattain uusia alustoja, joissa parhaat kehitys- ja hyödyntämistavat vaativat vielä opettelua. Hajautettuja sovelluksia ei vielä hyödynnetä kovinkaan laajamittaisesti ja tällä hetkellä olemassa olevista hajautetuista sovelluksista osa vaikuttaa rikollisilta. Useat niistä liittyvä pelaamiseen, vedonlyöntiin ja hajautettuihin markkina-alustoihin. (Lorne & Cawrey, 2020, pp. 90–91)

3.11 Nollatietotodistus

“Zero-Knowledge Proof” eli nollatietotodistus on kryptografinen menetelmä, jonka avulla yksi taho pystyy todistamaan valitun tiedon toiselle taholle paljastamatta kuitenkaan varsinaista tiedon sisältöä, ja paljastamatta kolmannelle osapuolelle edes tietävänsä valittua tietoa. Nollatietotodistuksia voidaan hyödyntää esimerkiksi transaktioiden aitouden ja paikkansapitävyyden todistamiseen siten, ettei tieto transaktioiden osapuolista tai muista yksityiskohdista paljastu. Nollatietotodistuksia voitaisiin teoriassa hyödyntää esimerkiksi verotuksessa, jolloin pelkkä nollatietotodistus todentaisi verottajalle, että verot tietyistä verotuksen alaisista transaktioista on maksettu asianmukaisesti. (Mattila et al., 2019, p. 25)

Nollatietotodistusten hyödyntäminen tehostaa merkittävästi monien järjestelmien yksityisyyttä sekä turvallisuutta. Vastaavasti se aiheuttaa lisäkustannuksia prosessointitehoon sekä tallennustilaan. Toinen huono puoli on, että nollatietotodistukset edellyttävät kahta osapuolta (todistaja ja varmentaja) kommunikoimaan keskinäisesti.

Lohkoketjuteknologiassa edellä mainitut heikkoudet ovat erityisen merkityksellisiä seuraavista syistä:

- Lohkoketjun louhijat tai validoijat ylläpitävät kopiota koko lohkoketjun reaaliaikaisesta tilikirjasta, joka kasvaa nopeasti hyvin suureksi lohkoketjun käytön lisääntyessä ja skaalautuessa. Nollatietotodistuksista johtuva datamäärän lisääntyminen kasvattaa tätä ongelmaa entisestään
- Lohkoketjuverkossa transaktion lähettäjä haluaa todistaa transaktion aitouden ja lohkoketjun louhijat tai validoijat todentavat transaktion aitouden. Ongelmaksi muodostuu, että normaalisti transaktion suorittajan ei tarvitse kommunikoida suoraan kaikkien transaktion aitouden todentajien (louhijat tai validoijat) kanssa vaan ainoastaan merkitä transaktio lohkoketjuun, jonka jälkeen transaktio validoidaan. Nollatietotodistus taas edellyttää nimenomaan keskinäistä kommunikaatiota. (Lorne & Cawrey, 2020, pp. 184–185)

Jotta nollatietotodistukset voitaisiin ottaa aktiiviseen käyttöön lohkoketjuissa tulisi sen mahdollistaa sekä parempi skaalautuvuus että tilanne, jossa noodit kykenevät vahvistamaan nollatietotodistuksen ilman suoraa keskinäistä kommunikointia. Toistaiseksi nollatietotodistuksia hyödynnetään erityisesti suljetuissa lohkoketjuissa, kuten yritysten omissa lohkoketjuissa, jotka eivät edellytä louhintaa. (Lorne & Cawrey, 2020, pp. 184–185)

3.12 DAO

Hajautettu autonominen organisaatio (Decentralized Autonomous Organization, DAO) esiteltiin alun perin Ethereum-nimisessä lohkoketjussa entistä pidemmälle viedyn hajauttamisen tavoittelun seurauksena. DAO:n ajatuksena oli korvata keskitettyjen toimijoiden hallinto älysopimuksilla. Samalla tavoin kuin ICO-konsepti korvaa keskitettyjen toimijoiden roolia julkisessa osakeannissa (Initial Public Offering, IPO), DAO:t hyödyntävät kryptovaluuttojen varainkeruuprojekteja luodakseen hajautetun hallinnollisen järjestelmän, jossa ICO:ihin sijoittaneille muodostuu äänestysoikeus päätöksentekoon siinä suhteessa paljonko ovat sijoittaneet kyseessä olevaan projektiin ICO:ssa. (Lorne & Cawrey, 2020, p. 87)

Konsepti asetettiin todelliseen testiin, kun The DAO -niminen projekti käynnistettiin Ethereum-ekosysteemissä huhtikuussa 2016. The DAO oli älysopimuksiin perustuva ICO-projekti, joka oli suunniteltu toimimaan autonomisesti. Päätökset perustuivat projektin ICO:ssa tokeneita omistavien henkilöiden äänestämiin päätöksiin. Projekti keräsi yhteensä yli 154 miljoonan dollarin varallisuuden yli 11 000 sijoittajalta. (Lorne & Cawrey, 2020, p. 87)

3.13 Lohkoketjuteknologian hyödyntäminen käytännössä

Lohkoketjuteknologian keskeisiä elementtejä ovat hajautettu arkkitehtuuri, vahva salaus ja konsensusmekanismi. Näin ollen lohkoketjuteknologia soveltuu toimintaan, joka edellyttää luottamusta tai missä tiedon epäsymmetria on suurta ja tiedon tulee olla varmennettavissa. Lisäksi kyseinen teknologia soveltuu toimintaan, jossa käsitellään tapahtumia tai jossa on paljon eri osapuolten välisiä integraatioita. Lohkoketjuteknologiaa hyödyntämällä yritykset, yhteisöt, yksilöt ja jopa valtiot voivat nopeuttaa ja tehostaa toimintaansa, samalla luottamusta lisäten. Toimintaa tehostavat esimerkiksi vähentyneet integraatiotarpeet, viansietokyky, informaation epäsymmetrian väheneminen sekä hajautetun arkkitehtuurin mukanaan tuoma luotettavuus. Luottamusta taas lisäävät mahdollisuus vahvaan yksityisyyden suojaan, luottamus muuttumattomaan menneisyyteen sekä luottamus toisen osapuolen aitouteen. (Harju, 2020; Natarajan et al., 2017, p. 5)

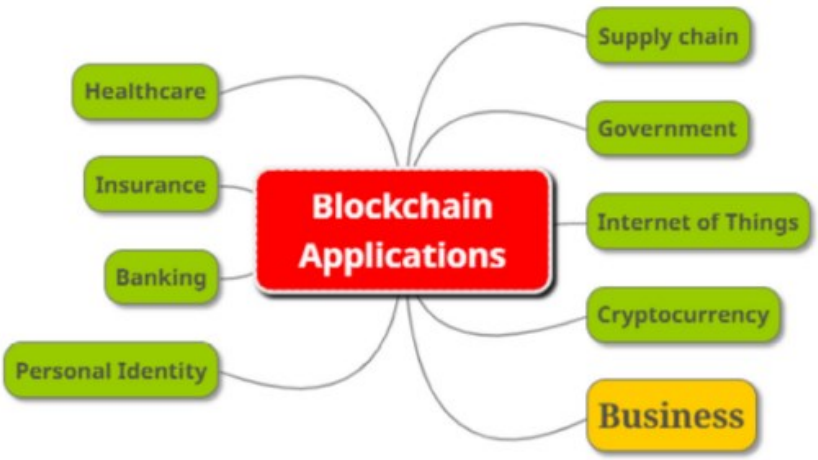
Liiketoiminta on vahvasti sitoutunutta informaatioon. Mitä nopeammin informaatio on saatavilla ja mitä tarkempaa se on, sitä parempi. Lohkoketju mahdollistaa reaaliaikaisen, jaetun ja täysin läpinäkyvän informaation, joka on tallennettu muuttamattomaan tilikirjaan lohkoketjusta riippuen kaikkien tai määriteltyjen osapuolten saataville. (IBM, n.d.)

Käytännössä lohkoketjuteknologiaa voidaan hyödyntää esimerkiksi terveydenhuollossa, vakuutusalalla, toimitusketjuissa, pankkialalla, asioiden internetissä (Internet of Things), hallinnoissa, ihmisten henkilöllisyyksissä, kryptovaluutoissa sekä muilla liiketoiminnan aloilla. Lohkoketjuteknologia voidaan hyödyntää esimerkiksi vakuutusalalla tehostamassa vakuutuskorvausten käsittelyä ja päätöksentekoa tai yritysten toimitusketjuissa varmentamassa tuotteiden alkuperää tai valmistuselinkaarta (Kuva 10). Liiketoimintoihin voidaan lohkoketjuteknologian avulla lisätä turvallisempia, kontrolloidumpia ja luotettavia prosesseja. (Gomathi et al., 2021, pp. 3–6)

Lohkoketjuun tallennetun tiedon muuttamattomuus mahdollistaa julkiset rekisterit, jotka ovat saatavilla kaikkialla samanaikaisesti. Väärentämättömyyttä ja mahdollisuutta varmentaa rekisteriin tallennetun tiedon aitous on hyödynnetty jo nyt esimerkiksi oppilaitosten tutkintotodistuksissa. Mahdollisuuksia nähdään tulevaisuudessa myös esimerkiksi terveydenhuollon asiakasrekisterien ylläpidossa sekä kiinteistö- ja maarekistereissä. Erityisesti lohkoketjuteknologian on arvioitu hyödyttävän yli kahta miljardia kehittyvien maiden asukasta, joilla ei ole virallista henkilöllisyyttä tai pankkitiliä. Jo pelkästään rahansiirtojen välitysmaksujen merkittävän laskun arvioidaan kasvattavan köyhimpien alueiden taloudellista hyvinvointia merkittävästi. (Honkanen, 2017, pp. 11–15)

Yksi potentiaalinen käyttökohde voisi myös olla yritysten lainmukaisuus- eli compliance-toiminnoissa. Esimerkiksi yritysten kirjanpito voitaisiin mahdollisesti tulevaisuudessa tallentaa lohkoketjuun, jolloin se olisi muuttamattomana suojassa väärinkäytöksiltä ja manipuloinnilta. Ajatus korruptoitumattomasta tietokannasta on herättänyt kansainvälistä kiinnostusta viranomaistahoissa ja pankkisektorilla sekä politiikassa. (Johansson et al., 2019, p. 31)

Kuva 10 Lohkoketjuteknologian hyödyntämismahdollisuudet (Gomathi et al., 2021, p. 5)



4 Lohkoketjuteknologia pankkisektorilla

Nykyisellä niin kutsutun ”Big Datan” aikakaudella pankit käyvät läpi laajamittaista digitaalista muutosta mahdollistaakseen paremman ja nopeamman digitaalisten palveluiden asiakaskokemuksen. Isoissa pankeissa tilikirjat ovat muuttuneet niin monimutkaisiksi, että pankin realistisen markkina-arvon määrittely on nykyisen kirjanpidon pohjalta haastavaa. Finanssi- ja pankkisektori onkin siirtymässä kohti avoimempia pankkitoimintoja, joissa maksimoidaan datan jakamisen hyödyt ja syvempi yhteistyö eri finanssialan toimijoiden välillä. (Johansson et al., 2019, p. 24; Wang et al., 2020, p. 813)

Finanssialan toimijat ovat tietokantojen suurkuluttajia ja ne tekevätkin tällä hetkellä merkittäviä investointeja luvanvaraisten lohkoketjujen tutkimiseen mahdollistaakseen kustannussäästöjä, nopeampia rajat ylittäviä rahan siirtoja, nopeampia yhteistyöpankkien välisiä maksuja ja clearingprosesseja, syndikoituja luottoja sekä trade finance -palveluita. (Natarajan et al., 2017, p. 13)

Lohkoketjusovelluksia kehitetään myös osakkeiden ja johdannaisten kaltaisten arvo-osuuksien kaupan tehostamiseksi ja luotettavuuden lisäämiseksi. Lohkoketjuteknologia mahdollistaa prosessien automatisoinnin kautta kustannussäästöihin esimerkiksi sopimusten ja rekisterien ylläpidossa. Esimerkiksi Bank of America on rekisteröinyt 35 lohkoketjuteknologiaan liittyvää patenttia viime vuosien aikana. (Chang et al., 2020, p. 5; Honkanen, 2017, p. 12)

Useita erilaisia konsortioita ja yhteisöjä on perustettu edistämään lohkoketjuteknologian käyttöönottoa sekä tutkimaan lohkoketjuteknologialle tarpeellista sääntelyä. Euroopan komissio on maininnut pyrkivänsä tutkimaan ja edistämään DLT- ja lohkoketjuteknologiaan perustuvia, maarajat ylittäviä palveluja mm. arvonlisäveron raportoinnin, tullauksen, yritysrekisterien, ympäristö-, talous- ja yritysraportoinnin, terveydenhuollon, verotuksen ja tullauksen osa-alueilla jo vuonna 2017. Myös YK ja Euroopan taloudellisen yhteistyöjärjestön (European Economic Co-operation, OECD) ovat määritelleet työryhmiä luomaan suosituksia ja raportteja lohkoketjujen käytöstä. Samoja toimia on toteutettu myös kansallisesti. (Laikari et al., 2018, p. 8; Mattila et al., 2019, p. 54)

Esimerkiksi edellä mainittuihin osa-alueisiin liittyvä raportoinnin muutos ja ajankohtaisen tiedon parempi saatavuus tulevat näkymään pankkisektorilla asiakaslähtöisempänä palveluna, korkeampana turvallisuutena sekä pankkien että asiakkaiden näkökulmista, väärinkäytösten ja rahanpesuriskin vähenemisenä ja yleisemmin entistä nopeampina prosesseina. (Natarajan et al., 2017, pp. 15–16, 21–23)

4.1 Yrityksille ja pankeille suunnatut DLT- ja lohkoketjualustat

Avoimen lohkoketjun vapaa käyttö ja lohkoketjun käyttäjän haasteellinen tunnistaminen ovat ristiriidassa finanssialan tämänhetkisten liiketoimintakäytäntöjen kanssa, jotka edellyttävät liiketoimien yksityisyyden säilyttämistä. Vastauksena tähän haasteeseen maailman finanssilaitokset ovat perustaneet yhteistyössä R3:n kanssa Corda-nimisen alustan DLT-järjestelmien kehittämiseen. Cordan jäseniä oli vuonna 2019 yhteensä yli 200 ja pohjoismaisista pankeista muun muassa OP, Nordea sekä Danske Bank ovat mukana R3-konsortiossa. Vastaavasti suurpankki JP Morgan on kehittänyt Quorum-nimisen luvanvaraisen DLT-alustan, jolla pyritään vastaamaan lohkoketjun yritysmaailman tarpeisiin; yksityisyyteen, nopeuteen ja suorituskykyyn. Muita pankkisektorilla toimivia konsortiolohkoketjuja Cordan ja Quorumin lisäksi ovat mm. Hyperledger ja Ethereum Enterprise Alliance. (Honkanen, 2017, p. 11; Johansson et al., 2019, pp. 140–142; Mattila et al., 2019, pp. 59–60; Natarajan et al., 2017, p. 13)

Vastaavia lohkoketjuteknologian hyödyntämiseen perustettuja yhteenliittymiä on perustettu mm. oikeudelliselle toimialalle (Global Legal Blockchain Consortium, GLBC) sekä vakuutusalalle (Blockchain Insurance Industry Initiative, B3i). Linux-säätiön ja IBM:n yhteistyössä kehittelemää Hyperledger-yhteistyöprojektia hyödynnetään sekä teknologia-, finanssi- että jakeluketjuyritysten toimesta. Hyperledgerin jäseniä ovat mm. Deutsche Bank, Baidu, American Express, Intel, SAP, Wells Fargo, Accenture, SWIFT, Fujitsu ja Cisco. (Johansson et al., 2019, pp. 140–144)

4.2 Keskuspankkien digitaaliset valuutat pankkisektorilla

Keskuspankkien kiinnostus digitaalisiin valuuttoihin on uutta ja herännyt vasta keskuspankkien huomattua digitaalisten valuuttojen mahdollistavan välineen tulevaisuuden

maksujen muokkaamiseen. Bank for International Setlementin (BIS) mukaan keskuspankkien digitaaliset valuutat eivät niinkään ole reaktio kryptovaluuttoihin ja yksityisen sektorin stablecoin-ehdotuksiin vaan ennemmin keskuspankkien teknologiavetoinen yritys ratkaista lukuisia julkisen politiikan tavoitteita kerralla. (CipherTrace, 2021, p. 63)

Keskuspankkien digitaaliset valuutat mahdollistavat valtavan määrän uusia teknisiä innovaatioita sekä hyötyjä pankkien tehokkuuden parantamisessa ja riskinhallinnan kehittämisessä. CBDC:t kehittyvät aiempia rahainnovaatioita nopeammin, kun uudet ketterät FinTech-toimijat ovat laajentaneet kilpailua markkinoilla. (Velissarios, 2021b, 2021a)

Suurin osa (jopa 86%) keskuspankeista on tällä hetkellä syvällisessä CBDC:n tutkimis- ja implementointivaiheessa. Tokenisoitu CBDC edustaa keskuspankkirahan kolmatta muotoa, joka jäljittelee seteleiden ominaisuuksia digitaalisessa muodossa. CBDC:ssä on sisäänrakennettuja ominaisuuksia, joiden avulla varat voivat vaihtaa omistajuutta todennettavasti ja ilman verkkoyhteyttä. (Auer & Böhme, 2021, p. 4; Velissarios, 2021b)

Yli 46 keskuspankkia on julkaissut suunnitelmansa tai prototyypin CBDC:stä ja 2 kuluttajakäytössä hyödynnettävää CBDC:tä on jo otettu käyttöön. Käyttöön otetut CBDC:t on toteutettu Bank of Bahamas:in ja Eastern Caribbean Central Bank:in toimesta. Useita CBDC-prototyyppejä on rakennettu yrityskäyttöön suunniteltujen DLT-alustojen kuten Cordan, Hyperledgerin tai Quorumin ympärille. (Auer & Böhme, 2021, pp. 4, 14)

Citigroupin toimitusjohtaja Michael Corbat ilmoitti joulukuussa 2020, että Citigroup työskentelee lukuisten hallintojen kanssa ympäri maailmaa keskuspankkien omien digitaalisten valuuttojen luomiseksi. Vaikka kyseessä olevia keskuspankkeja ei erikseen nimetty, todettiin julkaisussa, että yhteistyö liittyi sekä kehitykseen että kaupallistamiseen. Citigroupin lisäksi myös Visa ja Mastercard ovat julkaisseet omat CBDC-ohjelmansa. Corbatin mukaan CBDC:t ovat tulevaisuuden rahan väistämätön kehityssuunta. (CipherTrace, 2021, pp. 66–67)

4.3 FinTech

FinTech on lyhennetty “finanssiteknologia” -termistä (Financial Technology) ja sitä voidaan pitää nimensä mukaisesti finanssialan ja teknologian yhteenliittymänä. FinTech kiinnittää huomiota kahden merkittävän trendin vuoksi. Ensimmäinen trendi on Big Datan, koneoppimisen, tekoälyn sekä teknologisen kaupallistamisen mahdollistama kehitys. Toisena trendinä voidaan pitää faktaa, että yhä useammat uudet finanssialan ulkopuoliset yritykset ovat sijoittaneet finanssialan palveluihin. Yhtenä FinTech:in ulottuvuutena voidaan pitää perinteisiä finanssialan toimijoita, kuten esimerkiksi Morgan Stanley ja Goldman Sachs, jotka hyödyntävät big dataa ja muita uusia teknologioita muuttaakseen ja parantaakseen palveluitaan. Toisena ulottuvuutena voidaan pitää teknologia-alan yrityksiä, jotka pyrkivät hyödyntämään omia teknologioitaan finanssialan palveluiden kehittämiseksi. Tällaisina toimijoina voidaan pitää esimerkiksi Googlea, Applea ja Tencentiä, joiden alkuperäinen ajatus ei ollut toiminta rahoitustapahtumien parissa, vaan se on ollut seurausta asiakkaiden tarpeisiin vastaamisesta. (Chang et al., 2020, pp. 1–2; Feyen et al., 2021, p. V)

FinTech-alalla on kolme pääsuuntausta; mobiilimaksaminen, älysopimukset ja P2P-lainaaminen (Peer-to-Peer, vertaislainat) sekä lohkoketju. Yhteisiä tekijöitä FinTech-alalle ovat välitön yhteys, reaaliaikainen data, luotto-ratingit sekä päivitykset. FinTech-alan erityinen kiinnostus lohkoketjuteknologiaan johtuu pitkälti sen ominaisuuksista, jotka mahdollistavat nopeamman luottamuksen rakentamisen sekä sen potentiaaliin muuttaa finanssialan rakenteita. Lohkoketjuteknologian maturiteetti ei kuitenkaan ole vielä riittävällä tasolla, vaan siinä on ilmennyt turvallisuuteen, skaalautuvuuteen, viiveisiin ja yksityisyyteen liittyviä haasteita. (Chang et al., 2020, pp. 1–2)

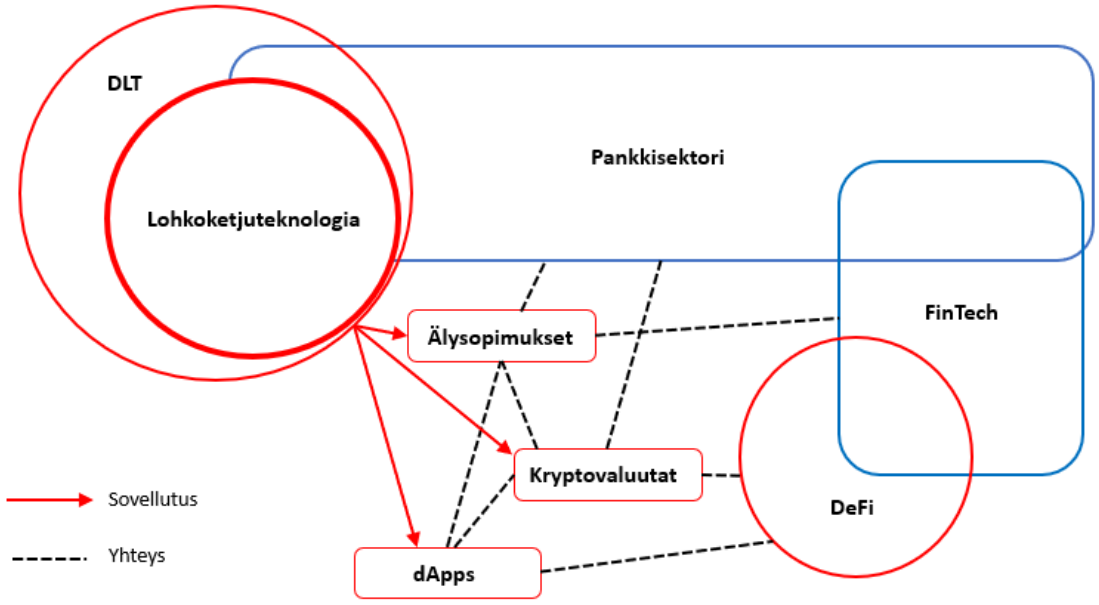
4.4 Keskitetyt vs. hajautetut talousjärjestelmät ja DeFi

Keskitetyssä talousjärjestelmässä finanssialan toimijat ovat keskeisiä osapuolia taloudellisten transaktioiden välityksessä ja hallinnoinnissa. Keskeisinä osapuolina finanssialan toimijat voivat kuitenkin kehittyä dominoiviksi tahoiksi, mikä voi aiheuttaa suhteettomia markkinaosuuksia ja sitä kautta taloudellisia hyötyjä. Hajautetussa talousjärjestelmässä vastavuoroisesti taloudellisia transaktioita hallinnoidaan hajautetussa vertaisverkossa keskitettyjen toimijoiden sijaan. Keskitettyjen toimijoiden roolia pienentämällä voidaan

pienentää transaktiokustannuksia ja luoda verkostovaikutusta ilman niin kutsuttuja keskitetyn tahon monopoliaseman mahdollistamia kustannuksia. (Chen & Bellavitis, 2020, p. 2)

Perinteisillä rahoituspalveluilla on ollut tyypillistä siiloutua ja keskittyä ylläpitämään omia kirjanpitojaan, joissa finanssipalvelut eivät ole yhteentoimivia toisten finanssipalveluiden kanssa. Tämän seurauksena pääomien ja varallisuuden siirtely siilosta toiseen voi muodostua kalliiksi ja hankalaksi. Vaihtoehtoisesti julkiseen lohkoketjuun rakennetut, hajautetut rahoituspalvelut (Decentralized Finance, DeFi) voisivat lisätä yhteentoimivuutta eri palveluiden välillä (Kuva 11). (Chen & Bellavitis, 2020, p. 3)

Kuva 11 FinTechin ja DeFin yhteydet pankkisektoriin ja lohkoketjuteknologian eri sovellutuksiin



4.5 Lohkoketjuteknologian mukanaan tuomat kuluerät

Kaikkien nykyisten finanssialan infrastruktuuriin liittyvien IT-järjestelmien, operatiivisten toimintojen ja institutionaalisten rakenteiden muuttaminen DLT-pohjaiseen infrastruktuuriin tulee aiheuttamaan finanssialalle kokonaisuudessaan merkittäviä kustannuksia. Kyseiseen siirtymään liittyy kustannusten lisäksi myös lukuisia muita riskejä. Näistä kustannuksista johtuen useat alan toimijat uskovat, että DLT-pohjaisia sovelluksia tullaan ensisijaisesti

hyödyntämään ”trade finance”- ja ”syndikoidut luotot”-tyyppisillä osa-alueilla, joissa ei ole tehty merkittäviä investointeja prosessien automatisointiin. (Natarajan et al., 2017, p. IX)

DLT-tietojärjestelmäkustannukset eivät itsessään merkittävästi eroa tavanomaisten digitalisaation tietojärjestelmähankkeiden kustannuksiin nähden niiltä osin, mistä järjestelmien perustamis- ja käyttökustannukset normaalisti muodostuvat. DLT-mallille tyypillisemmissä konsortiopohjaisissa yhteishankkeissa järjestelmien perustamis- ja suunnittelukustannukset jakaantuvat yleensä eri toimijoiden kesken, mikä eroaa perinteisemmistä tietojärjestelmähankkeista. (Mattila et al., 2019, p. 76)

Yhtenä merkittävimpänä lohkoketjuteknologiaan liittyvänä, uusia kustannuksia aiheuttavana tekijänä voidaan pitää älysopimuksia. Älysopimuksista aiheutuvat kustannukset voidaan jaotella kolmeen osaan; mukautumiskustannukset, oraakkelikustannukset sekä turvallisuuskustannukset. (Murray et al., 2019, p. 16)

Mukautumiskustannuksilla tarkoitetaan älysopimusten hyödyntämistä edellyttävän osaamisen puuttumista, joka saattaa aiheuttaa yrityksille uusia kustannuksia esimerkiksi ulkoistettujen älysopimuspalveluiden kautta. Oraakkelikustannuksilla viitataan niin kutsuttuun oraakkeliongelmaan, eli kolmansien osapuolien tietolähteiden virheellisyyteen, mikä aiheuttaa älysopimusten virheellisiä toimeksiantoja ja sitä kautta mahdollisia ylimääräisiä kustannuksia. Turvallisuuteen liittyvillä kustannuksilla viitataan erilaisiin lohkoketjuun kohdistuviin hyökkäyksiin, joilta suojautuminen ja varautuminen mahdollisesti lisää kustannuksia. (Murray et al., 2019, pp. 16–21)

Älysopimuksiin voi liittyä lohkoketjusta riippuen myös järjestelmän sisäisiä energiakustannuksia. Esimerkiksi Ethereum-järjestelmää käytettäessä energiakustannukset aiheutuvat lähtökohtaisesti älysopimuksen suorittaneelle taholle Ethereumin omina gas-virtuaalivaluuttayksikköinä. (Mattila et al., 2019, pp. 79–80)

Gas-virtuaalivaluuttayksiköiden tarkoituksena on varmistaa, ettei Ethereum-verkkoon luoda niin kutsuttuja loputtomasti silmukoilla itseään toistavia älysopimuksia (infinite loop) vaan älysopimukset lakkaavat toimimasta viimeistään käyttäjän gas-yksiköiden loputtua. (Lorne & Cawrey, 2020, p. 86)

4.6 Juridiset vaikutukset

Lohkoketjuteknologian sovellusten lainopillinen tila näyttäytyy ainakin toistaiseksi useiden oikeusalojen ja oikeuskysymysten näkökulmista varsin epäselvänä. Toistaiseksi lohkoketjuteknologiaa koskeva sääntely on koskettanut lähinnä rikos- ja vero-oikeudellisiin näkökulmiin, ja keskittyen niissäkin vain yksittäisiin ongelmiin. Vastaavasti työ-, sopimus- ja tietosuojalainsäädäntö on toistaiseksi jäänyt vähemmälle huomiolle. (Mattila et al., 2019, p. 14)

Älysopimusten osalta lainsäädäntö on edelleen odottavassa tilassa, eikä sopimuslainsäädäntö tällä hetkellä suojele älysopimusten hyödyntäjiä. Tuoreimmatkin lainsäädäntöön liittyvät julkaisut pyrkivät edelleen arvioimaan ja määrittelemään älysopimuksia sopimuslainsäädännön näkökulmaista. Lainsäädännön näkökulmasta älysopimukset nähdään teoriassa tehokkuutta lisäävänä ja kustannuksia laskevana mahdollisuutena, jotka voivat lisäksi tuoda hyötyjä datan ja kuluttajan suojan näkökulmista. Vastaavasti älysopimuksia pidetään ongelmallisina useista syistä; älysopimukset pitää kääntää ohjelmointikielelle, älysopimuksen jälkikäteinen muokkaaminen ei onnistu lohkoketjuun lisäämisen jälkeen ja älysopimukset eivät välttämättä noudata kaikkia sopimuslainsäädännön sääntöjä. Edelleen kehitysvaiheessa oleva lainsäädäntö voi aiheuttaa älysopimusten osalta ristiriitatilanteita siitä, kuka on vastuussa älysopimuksen mahdollisesti virheellisestä ohjelmoinnista ja minkä maan sopimuslainsäädäntöä älysopimuksessa kansainvälisissä tilanteissa sovelletaan.
(Eenmaa-Dimitrieva & Schmidt-Kessen, 2019, pp. 74–76, 86)

4.7 Ympäristövaikutukset

Lohkoketjuteknologiassa erityisesti Proof of Work -konsensusmekanismiin perustuvissa lohkoketjuissa konsensuksen muodostamiseen vaadittava prosessointiteho edellyttää merkittävää sähkönkulutusta ja sitä kautta kustannuksia. (Mattila et al., 2019, pp. 15, 79)

Bitcoinin louhintaan käytetty globaali kokonaisenergiankulutus on jo kasvanut massiivisiin mittoihin. Digiconomistin arvion mukaan Bitcoinin vuositason energiankulutus (tämän opinnäytetyön kirjoitushetkellä) on arviolta 175,7 terawattituntia, mikä vastaa n. 150% koko

Alankomaiden vuosittaisesta energiankulutuksesta ja 4,1% koko Yhdysvaltojen vuosittaisesta energiankulutuksesta. (Digiconomist, n.d.)

Saman tahon arvion mukaan yhden Bitcoin-transaktion energiankulutuksella voitaisiin toteuttaa 1,193,374 Visa-transaktiota ja yhden Bitcoin-transaktion aiheuttamalla hiilijalanjäljellä suorittaa 1,867,303 Visa-transaktiota. Uudemmat Proof of Stake -konsensusmekanismit ovat huomattavasti Proof of Work -protokollaa energiatehokkaampia ja sitä kautta ekologisempia. (Lorne & Cawrey, 2020, p. 52)

5 Lohkoketjuteknologian hyödyt pankkisektorilla

Lohkoketjuteknologiaa voidaan pitää poikkeuksellisen potentiaalisena ja käytännöllisenä ekosysteeminä pankki- ja investointisektorilla ja kyseisiä hyötyjä on todennettu useissa alaan liittyvissä raporteissa, blogeissa ja konferensseissa. (Garg et al., 2021, p. 2)

Oikeassa kontekstissa lohkoketjuteknologialla voi olla merkittäviä hyötyjä keskitettyihin tietokantoihin nähden. Lohkoketjuteknologian suurimmat potentiaaliset hyödyt ovat:

- hajautus ja kolmannen osapuolen tarpeen poistaminen
- parempi läpinäkyvyys ja helpompi tarkastettavuus
- automaatio ja ohjelmoitavuus
- muuttamattomuus ja todennettavuus
- hyödyt nopeudessa ja tehokkuudessa
- kustannusten pieneneminen
- kyberturvallisuuden paraneminen (Natarajan et al., 2017, p. 15)

Hajauttamisella ja kolmannen osapuolen tarpeen poistamisella tarkoitetaan, että lohkoketju mahdollistaa suorat kahden osapuolen väliset digitaalisten varojen siirrot sekä hajautetun tiedon säilömisen. Lohkoketju ei edellytä kolmatta osapuolta tai keskitettyä toimijaa, joka ylläpitää lohkoketjua. Tämä voi näkyä matalampina kuluina, parempana skaalautuvuutena sekä nopeutena. (Natarajan et al., 2017, p. 15)

Paremmalla läpinäkyvyydellä ja helpommalla tarkastettavuudella viitataan siihen, että jokaisella lohkoketjun osapuolella on täysi mahdollisuus tarkastella lohkoketjuun lisättyä tietoa. Tiedon lisäykset lohkoketjuun voidaan suorittaa ainoastaan saavuttamalla konsensus, joka jakaa tiedon lohkoketjun osapuolille samanaikaisesti. Tämä yhdistettynä keskitetyn toimijan roolin rajoittamiseen tai puuttumiseen mahdollistavat väärinkäytösten vähenemisen ja (transaktioiden) täsmäytyskustannusten alenemisen. (Natarajan et al., 2017, p. 15)

Automaatiolla ja ohjelmoitavuudella tarkoitetaan, että lohkoketju mahdollistaa ennalta sovittujen ehtojen täyttyessä suoritettavien automatisoitujen toimien ohjelmoinnin. Käytännössä tällä viitataan niin kutsuttuihin älysopimuksiin. Automaattinen laskun

maksutoimeksianto toimituksen vastaanoton yhteydessä on yksi esimerkki älysopimuksesta. Muuttamattomuudella ja todennettavuudella taas viitataan hajautustiivisteen varmentamaan oikeelliseen ja muuttamattomaan tietoon. (Mattila et al., 2019, p. 30; Natarajan et al., 2017, p. 15)

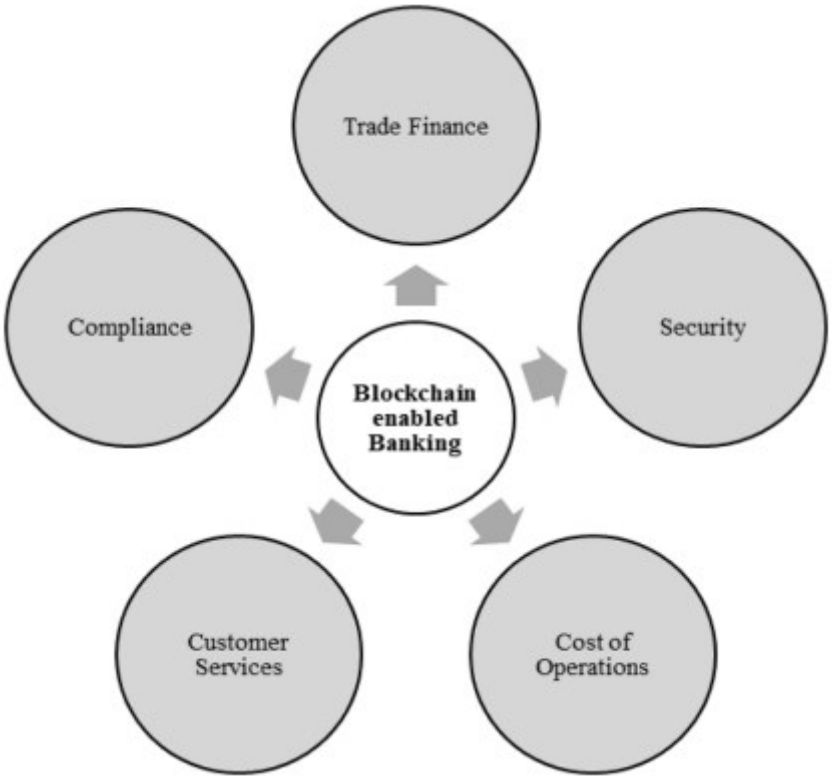
Nopeudessa ja tehokkuudessa saavutetuilla hyödyillä tarkoitetaan lohkoketjussa kolmansien osapuolten merkityksen vähenemisestä tai poistamisesta aiheutuvia tehokkuusetuja sekä prosessien automatisointia. Esimerkiksi trade finance -palveluissa on arvioitu saavutettavan lohkoketjuratkaisua hyödyntämällä luottolupaus asiakkaalle 24 tunnissa aiemman 5–10 päivän sijaan. (FSB, 2019, p. 17; Natarajan et al., 2017, p. 15)

Kustannusten vähenemisellä tarkoitetaan, että kaikki lohkoketjussa jaettu tieto on varmennettua lohkoketjun osapuolten kesken. Tämä mahdollistaa erilaisten tiedon täsmäyttämiseen liittyvien toimien vähentämisen sekä väärinkäytösten hillitsemisen. (FSB, 2019, p. 17; Natarajan et al., 2017, p. 15)

Kyberturvallisuuteen liittyvillä hyödyillä viitataan hajautuksen mukanaan tuomaan lisääntyneeseen turvallisuuteen verrattuna keskitettyihin tietokantoihin. (Natarajan et al., 2017, p. 15) Tällä hetkellä pääosa käytössä olevista tietokoneverkoistamme perustuu keskitettyyn tietoverkkoarkkitehtuuriin (Kuva 1). Ne tarjoavat hyvää suorituskykyä ja niiden rakentaminen on helppoa, mutta samaan aikaan keskitetty data muodostaa riskin kaiken servereille tallennetun datan menettämiselle. Järjestelmässä on tällöin niin kutsuttu Single point of attack eli yksittäinen hyökkäyspiste. Tämä tarkoittaa, että keskuspalvelimen kaatuessa koko järjestelmä voi vaarantua. Lohkoketjussa tätä riskiä on hajautettu jakamalla kaikki servereillä oleva tieto kaikille vertaisverkon toimijoille (Kuva 1). (Johansson et al., 2019, pp. 35–36)

Pankkisektorilla edellä mainitut tekijät näyttäytyvät potentiaalisesti lisääntyneenä turvallisuutena ja laadukkaampina compliance-toimintoina (erityisesti asiakkaan tuntemisen-, rahanpesun estämisen- ja terrorismin rahoittamisen estämisen toiminnot), mahdollisesti tehokkaampina trade finance -palveluina, kustannustehokkuutena sekä laadukkaampana asiakaspalveluna (Kuva 11). (Garg et al., 2021, pp. 5–6)

Kuva 12 Lohkoketjuteknologian hyödyt pankkisektorilla (Garg et al., 2021, p. 6)



5.1 Pankkipalveluiden mahdollistaminen kaikille

Maailmanpankki arvioi vuonna 2017, että maailmassa oli arviolta 1,7 miljardia ihmistä ilman pääsyä yleisiin pankkipalveluihin tai vailla omaa pankkitiliä. Useimmiten syynä on kehittyvien maiden puutteellinen infrastruktuuri, jonka vuoksi kyseisten maiden kansalaisilla on puutteelliset mahdollisuudet tunnistautumiseen ja varallisuuden omistamiseen. Luotettavan identifioinnin puuttuessa henkilön omistukset ja luottohistoria eivät ole aina riittävissä määrin todennettavissa ja sitä kautta pankkipalvelut eivät välttämättä ole tasapuolisesti kaikkien saatavilla. Nämä ovat konkreettisia esteitä köyhyydestä ja yleisestä kurjuudesta pois pääsemiseksi. (Johansson et al., 2019, pp. 46–47)

Lohkoketjuteknologian ympärille kehitetyt nopeat ja matalan kustannustason vertaislainapalvelut pienille lainoille sekä kustannustehokkaat varojen siirrot ovat jo nyt mahdollistaneet kehittyvissä maissa uusia mahdollisuuksia lainamarkkinoille pääsyyn sekä liiketoimintojen perustamiseen. Nämä tekijät voivat mahdollistaa nykyistä useammalle pääsyn pankkipalveluiden piiriin ja sitä kautta globaalissakin mittakaavassa positiivisemman arvon luonnin kehän. Valtiotasoisen infrastruktuurin näkökulmasta lohkoketjuteknologia

yhdistettynä biometristen tunnisteiden ympärille kehitettyihin identiteettijärjestelmiin voisivat osaltaan mahdollistaa ihmisten tehokkaamman tunnistamisen ja sitä kautta tehokkaamman pääsyn pankkipalveluiden piiriin. (Johansson et al., 2019, pp. 46–47)

5.2 Rahanpesun ja terrorismin rahoittamisen estäminen

Pankkisektori työllistää merkittävästi kolmansia osapuolia suuren transaktiomäärän monitorointiin ja hallinnointiin. Pankkisektori on kuormittunut tiedon varmentamiseen sekä lakisääteisiin tai sääntelyyn perustuvien tarkistusten prosesseista. Lohkoketjuteknologia voi muuttaa tätä tilannetta poistamalla kaksinkertaisen työn asiakkaan tuntemisen (Know Your Customer, KYC) sekä rahanpesun estämisen (Anti Money Laundering, AML) toimissa. Rahanpesun estämisessä lohkoketjuteknologia voi hyödyntää tekoälyn (Artificial Intelligence, AI) sekä koneoppimisen (Machine Learning, ML) toiminnallisuuksia tunnistaakseen ja estääkseen laittomia transaktioita. Lohkoketjuun perustuva tekoäly sekä koneoppiminen voivat merkittävästi seuloa dataa havaitakseen merkkejä laittomista toimista. Nämä työkalut voivat auttaa lohkoketjua monitoroimaan transaktioita entistä tehokkaammin ja mikäli työkalut havaitsevat epäilyttäviä transaktioita, ne voidaan jättää odottamaan tarkempaa tutkintaa. (Garg et al., 2021, pp. 5–6)

5.3 Lohkoketjuteknologiaan perustuvat sovellutukset

Kaksi suurinta trendiä lohkoketjuteknologiaan perustuvien sovellutusten kehityksessä ovat kaupalliset FinTech-startupit sekä samalle alalle muodostuvat konsortiot. FinTech-startupit kehittävät digitaalisia sovellutuksia lukuisiin eri käyttötarkoituksiin hyödyntämällä julkisia lohkoketjuja ja konsortiot tutkivat ja kehittävät yksityisissä, luvanvaraisissa lohkoketjuissa omalle toimialalleen spesifejä yritysratkaisuja. (Natarajan et al., 2017, p. 21)

FinTech-yrityksillä tarkoitetaan uudempia ja usein myös pienempiä finanssialan teknologian palveluihin erikoistuneita yrityksiä. (Feyen et al., 2021, p. V)

Lohkoketjuteknologiaan liittyvä konsortiotrendi näkyy erityisesti pankkisektorilla. R3-konsortiolohkoketjuun kuului jo vuonna 2017 yli 100 jäsentä ja vuonna 2019 yli 200 jäsentä, mukaan lukien pankkeja, säänteleviä tahoja sekä kauppaliittoja. Syksyllä 2018 Enterprise

Ethereum Alliance:n (EEA) jäseniksi oli liittynyt yli 500 tahoa. (Johansson et al., 2019, pp. 142–143; Natarajan et al., 2017, p. 21)

Finanssisektorilla lohkoketjuteknologiaan perustuvia sovellutuksia kehitetään mm. seuraavilla osa-alueilla: raha ja maksuliikenne, finanssipalvelut (pois lukien maksuliikenne), omistajuusrekisterit, finanssialan palveluntarjoajien sisäiset järjestelmät. Raha ja maksuliikenteessä kehitetään mm. digitaalisia valuuttoja, maksunvälitystä sekä maksun varmentamista, kansainvälisiä maksuja, valuutanvaihtoa sekä mikromaksuja. Ei-maksuliikenteeseen liittyvissä finanssipalveluissa kehitetään mm. ratkaisuja pääoma-, johdannais- ja lainamarkkinoille, rahoituspalveluihin (esim. ICO:t), irtaimen omaisuuden rekistereihin, syndikoituihin luottoihin sekä vakuutusmarkkinoille esimerkiksi vakuutuskorvausten automatisointiin. Omistajuusrekistereissä kehitetään sovellutuksia mm. maa- ja omaisuusrekistereihin (Kuva 12). (Natarajan et al., 2017, p. 22)

Finanssisektorin ulkopuolella lohkoketjuteknologiaan perustuvissa sovellutuksissa nähdään potentiaalia mm. henkilöllisyyden todentamisessa, toimitusketjuissa, maataloudessa, hallinnossa, terveydenhuollossa sekä humanitaarisessa avussa. Edellä mainituista sovellutuksista erityisesti kansainväliset maksut, digitaaliset henkilöllisyysjärjestelmät, varallisuusrekisterit sekä digitaaliset valuutat voivat mahdollistaa heikommassa asemassa olevalle väestölle merkittävästi paremman taloudellisen saatavuuden sekä osallisuuden. (Natarajan et al., 2017, p. 23)

Kuva 13 Katsaus mahdollisiin lohkoketjuteknologian sovellutuksiin finanssisektorilla ja muilla sektoreilla (Natarajan et al., 2017, p. 22)

Overview of Potential DLT Applications (at varying stages of development)	
Financial Sector Applications	
Money & Payments	• Digital currencies • Payment authorization, clearance & settlement • International remittances and cross-border payments (alternative to correspondent banking) • Foreign exchange • Micropayments
Financial Services & Infrastructure (beyond payments)	• Capital markets: digital issuance, trading & settlements of securities • Commodities trading • Notarization services (e.g. for mortgages) • Collateral registries • Movable asset registries • Syndicated loans • Crowdfunding (as initial coin offerings) • Insurance (in combination with smart contracts) for automating insurance payouts and validation of occurrence of insured event
Collateral registries and ownership registers	• Land registries, property titles & other collateral registries
Internal systems of financial service providers	• Replacing internal ledgers maintained by large, multinational financial service providers that record information across different departments, subsidiaries, or geographies
DLT-based applications in other sectors	
Identity	• Digital identity platforms[22] • Storing personal records: birth, marriage & death certificates
Trade & Commerce	• Supply chain management (management of inventory and disputes) • Product provenance & authenticity (e.g. artworks, pharmaceuticals, diamonds) • Trade finance • Post-trade processing • Rewards & loyalty programs • Invoice management • Intellectual property registration • Internet of Things
Agriculture	• Financial services in the agricultural sector like insurance, crop finance and warehouse receipts • Provenance of cash crops • Safety net programs related to delivery of seeds, fertilizers and other agricultural inputs
Governance	• E-voting systems • E-Residence • Government record-keeping, e.g. criminal records • Reducing fraud and error in government payments • Reducing tax fraud • Protection of critical infrastructure against cyberattacks
Healthcare	• Electronic medical records
Humanitarian & Aid	• Tracking delivery & distribution of food, vaccinations, medications, etc. • Tracking distribution and expenditure of aid money

5.3.1 Älysopimukset operatiivisessa liiketoiminnassa

Yksi liiketoiminnan kustannusten aiheuttaja on epätäydellisestä informaatioista johtuva tarve operatiivisten toimintojen monitorointiin. Päälliköillä on osakkeenomistajiin ja jopa

johtajiin nähden informatiivinen etulyöntiasema yhtiön liiketoimintaan. Tästä huolimatta päälliköt saattavat antaa yhtiön osakkeenomistajille tai heidän edustajilleen eli hallitukselle vääristyneen, jopa yltiöpositiivisen näkemyksen yhtiön liiketoiminnasta. Kokonaisen olemassa olevan organisaation muuttaminen toimimaan täysin älysopimusten pohjalta on sekä epäkäytännöllistä että mahdotonta. On kuitenkin useita osa-alueita, missä lohkoketjuteknologia mahdollistaa selkeitä hyötyjä operatiivisen päivittäisliiketoiminnan monitorointiin. Yhtiön omistajien ja johtajien seuratessa yhtiön päivittäisliiketoimintaa, vältetään informaation epäsymmetria, mahdollisesti virheellinen kuva liiketoiminnasta tai vallitsevista olosuhteista. Älysopimukset voivat samassa yhteydessä poistaa tarpeen mahdollisille kolmannen osapuolten sisäisille tarkastajille tai analyytikoille. (Murray et al., 2019, pp. 26–27)

Älysopimusten hyödyntäminen yhtiön operatiivisen toiminnan monitoroinnissa mahdollistaisi useita etuja sekä osakkeenomistajien että myös päälliköiden päätöksenteon näkökulmasta. Esimerkiksi toimitusketjussa reaaliaikainen toimitusketjusta saatava data voisi ilmoittaa kansainvälisestä salmonellatartuntariskin kasvusta, jonka perusteella älysopimus voisi tehdä reaaliaikaisen päätöksen tuotannon keskeyttämisestä. Näin ollen tämä mahdollistaisi päällikkötasolla tarkemman ja nopeamman päätöksenteon arvaamattomissa tilanteissa. Tämän seurauksena taas vältettäisiin virheellisistä päätöksistä johtuvat tappiot yhtiön osakkeenomistajille. (Murray et al., 2019, p. 28)

5.3.2 Lohkoketju tuotteen alkuperän varmentajana

Toimitusketjuissa lohkoketjuun on mahdollista lisätä (asiakkaille saatavilla olevaa) tietoa tuotteesta, kuten sen tuotantoon käytetty energiamäärä tai hiilijalanjälki. Myös luomu- tai Fair Trade -tuotteen sertifioiminen on tällä tavoin mahdollista. Asiakaskokemuksen parantumisen lisäksi lohkoketjuun talletettua tietoa toimitusketjusta voidaan hyödyntää kustannussäästöinä, kun kolmannen osapuolen tahoja ei enää tarvita todentamaan tuotteelle tiettyjä ominaisuuksia tai määritelmiä (kuten edellä mainitut luomu ja Fair Trade). (Murray et al., 2019, p. 28)

5.3.3 Kryptovaluutat henkilöstön kustannusten avoimuuden kasvattajana

Jokainen kryptovaluutalla suoritettu transaktio tallentuu lohkoketjuun ja tätä voitaisiin hyödyntää myös johdon kustannusten läpinäkyvyyden lisäämisessä. Johdon kustannuksia valvotaan useissa yhtiöissä sisäisesti jo nyt, eikä tähän välttämättä tarvita lohkoketjuteknologiaa. Lohkoketjuteknologia kuitenkin mahdollistaisi nykyistä paremman läpinäkyvyyden sekä mahdollisuuden kustannusten tarkasteluun myös yhtiön ulkopuolisille pääomistajille. Tämä läpinäkyvyys heijastuisi myös yhtiön ulkopuolisiin sidosryhmiin kuten institutionaalisiin sijoittajiin, yksityisiin sijoittajiin tai toimittajiin. (Murray et al., 2019, p. 31)

5.3.4 Älysopimusten hyödyntäminen työsuoritusten palkitsemisessa

Mikäli tietyt työtehtävät ovat objektiivisesti mitattavissa, ne ovat myös lähtökohtaisesti koodattavissa älysopimukseen. Tämä mahdollistaisi erityisesti ”entry level” -tasoisissa työtehtävissä työn suoriutumisen pilkkomisen yksittäisiin työtehtäviin ja määrittämään korvauksen kyseisissä tehtävissä suoriutumisen perusteella. Vastaavasti johtotehtävissä työtehtävät koostuvat vaikeammin mitattavissa olevista työtehtävistä, jolloin myös niiden koodattavuus älysopimukseen on haasteellisempaa. (Murray et al., 2019, p. 32)

5.4 Yhteentoimivuus

Yhteentoimivuuden (interoperability) tavoitteena on mahdollistaa sujuva informaation jakaminen, helpompi älysopimusten suorittaminen sekä käyttäjäystävällinen kokemus kahden eri lohkoketjun välillä. Yhteentoimivuutta pidetään yhtenä merkittävänä vaikuttajana tietyn lohkoketjun suurempaan käyttöönottoon. (Lorne & Cawrey, 2020, p. 247)

6 Riskit

Lohkoketju- ja DLT-teknologia kehittyvät kovaa vauhtia, mikä voi aiheuttaa uusia haasteita ja riskejä ratkaistavaksi. Useimmiten mainitut teknologiset-, juridiset- sekä sääntelyyn perustuvat ongelmat liittyvät skaalautuvuuteen, yhteensovittamiseen, operatiiviseen turvallisuuteen ja kyberturvallisuuteen, henkilöllisyyden varmentamiseen, datan suojaan, liiketoimintakiistoihin sekä lakien ja sääntelyn kehittämiseen teknologisen kehityksen mukana. Tämä voi näkyä merkittävinä muutoksina finanssisektorin toimijoiden rooleissa ja vastuunjaossa. (Natarajan et al., 2017, p. IX)

6.1 Muuttumattomuus ja konsensusprotokollan heikkous

Lohkoketjuteknologiaa kuvataan ajoittain ”muuttumattomaksi” tai ”lopulliseksi”, koska lohkoketjuun lisättyä tietoa ei voida konsensusmekanismien vuoksi enää jälkikäteisesti muokata. Tämä voi antaa käsityksen, että lohkoketju on oikeellisesta tiedosta koostuva turvallinen ja luotettava tietovarasto. On kuitenkin hyvä muistaa, että lohkoketjun konsensuksen muodostuminen on viime kädessä sosiaalista, eikä algoritmista, sillä lohkoketjujärjestelmässä protokollassa määritetyt säännöt ovat viime kädessä hajautetun lohkoketjuverkon käyttäjien päätäntävallassa. Periaatteessa lohkoketjuverkon käyttäjille ei ole estettä konsensussääntöjen muuttamiselle tai lohkoketjutietokannan muokkaamiselle halutulla tavalla. (Mattila et al., 2019, p. 42)

6.2 Lohkoketjuteknologiaan kohdistuvat hyökkäykset

Vaikka lohkoketjuteknologiaa voidaan pitää lähtökohtaisesti suhteellisen turvallisena, siihen liittyy kaikkien teknologioiden tavoin riski joutua hyökkäyksen kohteeksi. Esimerkkejä potentiaalisista hyökkäyksistä ovat esimerkiksi niin kutsuttu valtaosan hyökkäys (51% attack), itsekäs louhinta (selfish mining) sekä erilaiset palvelunestohyökkäykset. (Liang, 2020, p. 127)

Yksi tunnetuimmista lohkoketjuun kohdistuneista hyökkäyksistä on niin kutsuttu ”The DAO”-case. Kyseisessä tapauksessa The DAO -projekti hakkeroitiin Ethereum-lohkoketjuverkon koodista löytyneen yksittäisen haavoittuvuuden kautta ja projektin rahoituksesta varastettiin

yhteensä noin 50 miljoonan dollarin arvosta varoja. (Malhotra et al., 2021, pp. 11–12; Mattila et al., 2019, p. 45; Natarajan et al., 2017, p. 31)

6.2.1 51 % -attack

Lohkoketjuun lisätään hyötykuormaa, joka varmennetaan konsensusprotokollan avulla. Konsensuksen muodostuttua siihen osallistuneet tahot päivittävät ja tallentavat hajautettuun tietokantaan lisätyn hyötykuorman samanaikaisesti. Kärjistetysti, verkoston validoijien tallennettua lisätty hyötykuorma lohkoketjuun, kyseinen lohko sinetöidään, lisätään lohkoketjuun ja jatkossa dataa lisätään jälleen uuteen lohkoon. Yksi olennainen turvallisuusriski lohkoketjuteknologiassa on niin kutsuttu 51 % -hyökkäys (51 % -attack). Hyökkäyksellä viitataan tapahtumaan, jossa väärinkäytökseen pyrkivä taho tai tahot onnistuvat ottamaan hallintaansa 51% tai suuremman osan konsensusta validoivista noodeista ja ohjaavat konsensusprotokollaa peruuttamaan transaktioita tai luomaan virheellisiä transaktioita. Kyseistä toimintamallia ei käytännössä voida toteuttaa laajoissa hajautetuissa lohkoketjuverkostoissa vaan riski on teoreettisempi, mutta yksittäisestä noodista tai vähäisistä noodeista koostuvissa lohkoketjuverkoissa riski on merkittävämpi. (Gomathi et al., 2021, p. 8; Murray et al., 2019, p. 20)

Tähän riskiin liittyen yhdeksi yritysten tulevaisuuden kustannukseksi saattavat myös muodostua lohkoketjun turvallisuudesta vastaavat palvelut, jotka seuraavat reaaliaikaisesti lohkoketjun keskittyneisyyttä. Ne voivat tarpeen vaatiessa käyttää omaa koneiden laskentatehoa keskittyneisyyden hallitsemiseksi. (Murray et al., 2019, p. 20)

6.2.2 P2P-vertaisverkkoon kohdistuvat palvelunestohyökkäykset

Vertaisverkkoon kohdistuvissa palvelunestohyökkäyksissä pyritään aiheuttamaan vertaisverkkoon virhetilanteita joko yksittäisenä noodina tai useiden noodien kautta. Eclipse attack -nimisessä hyökkäyksessä pyritään yksittäisenä noodina validoimaan virheellisiä transaktioita ja aiheuttamaan sitä kautta virheellisiä merkintöjä lohkoihin ja sitä kautta koko lohkoketjuun. Sybil attack -nimisessä hyökkäyksessä tavoitteena on tulvittaa koko vertaisverkkojärjestelmää lukuisten noodien kautta luomalla lukuisia virheellisiä kahdensuuntaisia transaktioita ja lopulta estää lohkoketjun lohkojen luontia ja sitä kautta

hidastaa lohkoketjun toimintaa. Laajan mittakaavan Sybil attack voi johtaa 51 % -hyökkäykseen. Lohkoketjuteknologian ulkopuolinen esimerkki Sybil attack:ista voisi olla esimerkiksi yhden henkilön luomat lukuisat sosiaalisen median tilit, joita käytetään vääriin tarkoituksiin. (Binance, 2018; Gomathi et al., 2021, p. 7)

6.2.3 Selfish mining

Niin kutsutussa itsekkäässä louhinnassa pahantahtoiset noodit pyrkivät pidättämään Proof of Work -konsensusprotokollassa louhimaansa ja validoimaansa lohkoa siten, että onnistuu saamaan etulyöntiaseman myös seuraavan lohkon validoimiseen. Tämä taas mahdollistaa kyseiselle pahantahtoiselle noodille muita suuremmat louhintapalkkiot. Tätä ongelmaa on esiintynyt mm. Bitcoin-verkossa. Suuremmassa kuvassa Selfish mining -toiminta on kuitenkin kannattamatonta, sillä kyseisen tyyppisen häiriöt saattavat vaikuttaa laskevasti itsekkään louhinnan kohteena olevan kryptovaluutan hintaan, jolloin toiminta ei välttämättä ole enää kannattavaa louhinnan korkeiden sähkökustannusten vuoksi. (Binance, 2020; Liang, 2020, p. 127)

6.3 Lohkoketjuteknologian käyttöönoton riskit

Kuten minkä tahansa uuden järjestelmän käyttöönottoon, myös lohkoketjuteknologian käyttöönottoon liittyy riskejä. Yritysten näkökulmasta on tunnistettu kolme merkittävää strategista riskiä, liiketoiminnalliset riskit, juridiset riskit sekä teknologiset riskit. (Malhotra et al., 2021, pp. 2–3)

6.3.1 Liiketoiminnalliset riskit

Lohkoketjuteknologian käyttöönotto vaikuttaa yhtiöiden sisäisiin toimintamalleihin ja muutos vaikuttaa toissijaisesti myös yhtiön henkilöstöön. Havaitut epäkohdat aiheuttavat usein sisäistä vastustusta, erityisesti henkilöille, jotka pelkäävät lohkoketjuteknologian syrjäyttävän heidät työtehtävistään. Lohkoketjuteknologian käyttöönotto myös pakottaa yhtiötä luomaan uusia prosesseja sekä suunnittelemaan malleja potentiaalisten ongelmien havaitsemiseksi ihmisten suorittamissa työvaiheissa. Esimerkiksi niissä tilanteissa, missä tiettyä dataa on käsitelty henkilökohtaisesti, on datasta saatettu havaita poikkeamia, joihin

on pystytty reagoimaan spontaanisti. Tämän kaltaisten poikkeamien havaitsemisen väheneminen voi vaikuttaa laskevasti esimerkiksi asiakastyytyväisyyteen. (Malhotra et al., 2021, pp. 7–8)

Lohkoketjuteknologian käyttöönotto voi myös aiheuttaa nykyisten liiketoimintamallien korvaavana teknologiana tiettyjä keskittymishäiriöitä. Liike-elämässä on käytännön esimerkkejä tilanteista, joissa lohkoketjuteknologian käyttöönotto on saanut liikaa huomiota suhteessa yhtiön ydinliiketoimintaan, mikä on heikentänyt ydinliiketoiminnan suoriutumista. Saman aihepiirin riskinä voidaan myös pitää kilpailevien yhtiöiden kilpajuoksua lohkoketjuteknologian suunnittelussa sekä käyttöönotossa. (Malhotra et al., 2021, p. 8)

Yhtenä liiketoiminnallisena riskinä voidaan pitää lohkoketjuteknologian hyödyntämättä jättämistä suhteessa kilpailijoihin. Kuvitellaan esimerkiksi yhtiö, joka on automatisoinut älysopimuksilla laskujensa maksun 3 päivässä kilpailijan 30–60 päivään verrattuna. On todennäköistä, että edellä mainitulla esimerkillä on merkitystä esimerkiksi tavarantoimittajille. (Malhotra et al., 2021, p. 8)

Liiketoiminnallisena riskinä voidaan myös pitää strategista ja rakenteellista joustamattomuutta, sillä lohkoketjuteknologia sekä erityisesti älysopimukset edellyttävät ennalta ohjelmoituja sääntöjä. Ennalta ohjelmoidut älysopimukset eivät aina pysty mukautumaan liiketoiminnan muutoksiin, mikä saattaa hidastaa toimintamallien muutoksia ja yleisesti yhtiön strategista joustavuutta. (Malhotra et al., 2021, p. 9)

6.3.2 Juridiset riskit

Lohkoketjuteknologiaan perustuvat hajautetut alustat hämärtävät yksittäisen tahon vastuuta ja tästä syystä väärinkäytöstilanteissa voi olla vaikea syyttää yksittäistä tahoa. Oikeustoimielimet voivat kuitenkin mahdollisesti nähdä lohkoketjuprojektit tai niihin liittyvät ekosysteemit yhteisyrityksien kaltaisina, joissa kaikkia osapuolia voidaan pitää osallisina projektien kehitykseen ja käyttöönottoon. (Malhotra et al., 2021, p. 10)

Lohkoketjuteknologiaan perustuvien sovellutusten kehittyessä globaaleiksi ekosysteemeiksi myös juridiset hankaluudet nousevat esiin. Hajautuksesta johtuen rajat ylittävien kiistojen

ratkaisumallit tulevat tarpeellisiksi. Esimerkiksi älysopimusten osalta, sopimusten täytäntöönpanot sekä riitojen ratkaisut edellyttävät ennakkoharkintaa. Tässä piilee kuitenkin myös vaara, että eri maiden lait ovat näissä tilanteissa keskenään ristiriidassa tai niitä joudutaan soveltamaan yhtäaikaisesti. Datan ollessa lohkoketjusovellutusten keskeinen osa, datan sijaintiin voi kohdistua erilaisia juridisia vaatimuksia eri alueilla. (Malhotra et al., 2021, p. 10)

6.3.3 Teknologiset riskit

Usean tahon yhteistyö lohkoketjun käytössä voi myös lisätä turvallisuusriskiä. Lohkoketju toimii julkisten ja yksityisten avaimien yhdistelmillä, jotka mahdollistavat pääsyt hajautettuun lohkoketjuverkkoon. Julkisten ja yksityisten avainten lukumäärän kasvaessa, erityisesti useilla aloilla toimivissa lohkoketjuekosysteemeissä, myös potentiaalisten haavoittuvuuksien määrä lisääntyy. (Malhotra et al., 2021, p. 12)

Mikäli yritykset alkavat ottamaan käyttöönsä useita eri lohkoketjualustoja, yritykset saattavat kohdata yhteensovitettavuuteen liittyviä riskejä. Yhteensovitettavuuden riskit johtuvat siitä, etteivät yksittäiset lohkoketjualustat pysty tarjoamaan ratkaisuja kaikkiin yritystarpeisiin ja tästä johtuen yritykset saattavat alkaa hyödyntämään samanaikaisesti useita eri lohkoketjualustoja. Standardoinnin toistaiseksi puuttuessa yritykset saattavat joutua investoimaan vedonlyönnin tavoin samanaikaisesti lukuisiin eri lohkoketjualustoihin. Tämä voi aiheuttaa riskin niin sanotusti väärän alustan veikkaamisesta. (Malhotra et al., 2021, p. 12)

Lohkoketjuteknologian luvataan skaalautuvan helposti. Todellisuudessa eri alojen välisiä massiivisia ekosysteemeitä ei kuitenkaan olla vielä testattu täydessä mittakaavassa ja tästä syystä on mahdollista, että suuren mittaluokan skaalautuvuudessa voi ilmetä tuntemattomia haasteita. Tällä hetkellä lohkoketjuteknologian toimintojen ja virheiden kompleksiset haasteet lepäävät lahjakkaan ja hyvin pienen asiantuntijajoukon harteilla. Teknologia ei ole vielä saavuttanut yleisemmän universaalin osaamisen tasoa edes lahjakkaimpien ohjelmoijien ja kehittäjien joukossa. Lohkoketjuteknologian standardien kehittyessä ja lohkoketjuteknologian kasvun tasaantuessa, myös skaalautuvuushaasteet saattavat alkaa konkretisoitua. (Malhotra et al., 2021, pp. 12–13)

6.4 Hajauttamisen riskit pankkisektorilla

Useat eri finanssialan palveluntarjoajat ottavat mukaan uusia teknologioita, jotka mahdollistaisivat rahoitusjärjestelmien hajauttamisen. Rahoitusjärjestelmien hajauttamisella viitataan perinteisesti rahoituspalvelujen tarjoamisessa mukana olevien välittäjien tai keskitettyjen prosessien roolien pienentämiseen, poistamiseen tai jossain tapauksissa vähintään riskin hajauttamiseen perinteisiltä välittäjiltä. Tällä uskotaan saavutettavan merkittäviä taloudellisia vaikutuksia, mahdollisia hyötyjä taloudelliseen stabiliteettiin, laajempaa kilpailua, monimuotoisempi rahoitusjärjestelmä ja lisäksi hajauttamisen uskotaan vähentävän tiettyjen olemassa olevien tahojen systeemistä tärkeyttä. (FSB, 2019, p. 1)

6.4.1 Vaikutus taloudelliseen stabiliteettiin

Hajautetut teknologiat voivat periaatteessa aiheuttaa riskejä taloudelliseen stabiliteettiin, mutta ne riippuvat siitä, missä määrin hajautettuun teknologiaan perustuvia innovaatioita tullaan tulevaisuudessa ottamaan käyttöön. Riskit saattavat liittyä keskittämisen uusiin haasteisiin, prosykslisyyteen, älysopimus-liitännäisiin vastuuseen liittyviin haasteisiin, talousjärjestelmien haasteiden ratkaisemiseen ja palauttamiseen liittyviin haasteisiin ja muihin juridisiin sekä operatiivisiin haasteisiin. (FSB, 2019, pp. 1, 6–7)

Keskittämisen uusien haasteiden riskillä tarkoitetaan, että esimerkiksi DLT-järjestelmien omistajuus, lähdekoodin hallinnointi ja kehitys ovat keskitetysti pienen ihmisryhmän (esimerkiksi ohjelmistokehittäjät) vastuulla. Prosyklisyydellä viitataan esimerkiksi hajautukseen perustuviin P2P-lainapalveluihin, joiden tarjoamista luotoista voi aiheutua nykyisiä finanssialan toimijoita suurempia ja rajumpia tuottovaihteluita, erityisesti tilanteissa, joissa lainapäätökset on automatisoitu. Talousjärjestelmien haasteiden ratkaisemiseen ja palauttamiseen liittyvillä haasteilla tarkoitetaan, että nykyiset talousjärjestelmät luottavat keskitettyyn tiedon taltiointiin ja siihen, että kaikki markkinoiden toimijat ovat tunnistettuja ja niiden sijainti on tiedossa.
Muilla operatiivisilla ja juridisilla haasteilla tarkoitetaan, että erityisesti avoimissa järjestelmissä, joissa saattaa olla mukana anonyymejä käyttäjiä, saattaa esiintyä tarkoituksellista konsensusmekanismin häirintää esimerkiksi tarkoituksellisella virheellisten transaktioiden vahvistamisella. (FSB, 2019, pp. 1, 6–7)

6.4.2 Rahoitusalan sääntelyyn ja hallintoon liittyvät haasteet

Rahoitusjärjestelmien hajauttaminen voi aiheuttaa haasteita finanssialan sääntelystä ja valvonnasta vastaaville tahoille – erityisesti niille, joiden fokus on keskitetyissä finanssialan toimijoissa (esimerkiksi perinteisissä pankeissa). Hajautetumpi rahoitusjärjestelmä voi vahvistaa toimintoperusteisen sääntelyn tärkeyttä erityisesti niissä rahoituspalveluissa, joita on vaikea yhdistää tiettyyn tahoon tai lainkäyttöalueeseen. Sääntelystä ja valvonnasta vastaavien tahojen saattaa olla tarpeellista lisätä keskustelua teknologiasektorin kanssa pystyäkseen välttämään hajautettuihin teknologioihin liittyviä odottamattomia hankaluuksia. (FSB, 2019, p. 1)

6.4.3 Hajautettujen rahoituspalveluiden riskit

Hajautetuilla rahoituspalveluilla (Decentralized Finance, DeFi) tarkoitetaan lohkoketjuteknologiaan perustuvia, finanssipalvelut mahdollistavia hajautettuja applikaatioita eli dApps:eja. Esimerkiksi keskitetyissä finanssipalveluissa tarvitaan pankkia tai vastaavaa keskitettyä tahoa, joka suostuu mahdollisesti hyväksytyn lainahakemuksen jälkeen määrättyjen lainaehtojen puitteissa lainaamaan varoja. Tämän lainan hinnaksi aiheutuu korko- ja muita kustannuksia. DeFi-palvelussa voidaan itse määrittää tarvittavat lainavarat ja itselle sopivat lainaehdot, ja palvelu etsii tahon, joka on ilmoittanut halukkuudestaan lainata varoja kyseisten ehtojen nojalla. Jos nämä ehdot ovat kummankin tahon hyväksymiä, lainasuhde muodostuu suoraan kahden tahon välisenä ilman kolmatta osapuolta. DeFi ei tarkoita, etteikö lainalla voisi olla korko- tai muita kustannuksia vaan että lainan saamiselle muodostuu enemmän mahdollisuuksia, kun lainan myöntäjä voi olla missä päin maailmaa tahansa. (Sharma, 2022)

Hajautetut rahoituspalvelut eivät ole vielä saavuttaneet täyttä potentiaaliaan väärinkäytöksiin, volatiliteettiin, käytettävyyteen ja sääntelyyn liittyvistä haasteista johtuen. Ensinnäkin hajautetut rahoituspalvelut voivat olla testaamattomien innovaatioiden lisääntyessä alttiina väärinkäytöksille. Toisekseen hajautetut rahoituspalvelut rakentavat toistaiseksi tyypillisesti palveluitaan volatiilien kryptovaluuttojen ympärille, mikä haittaa palveluiden vakautta ja käyttöönottoa. Tätä ongelmaa on kuitenkin pyritty ratkaisemaan stablecoineilla, joiden arvo on usein sidoksissa fiat-valuuttoihin. Kolmanneksi, hajautetuilla

rahoituspalveluilla on ollut tapana seurata teknologista kehitystä markkinoiden tarpeen sijaan. Tämän seurauksena useat projektit ovat keskittyneet käytettävyyden ja käyttäjäystävällisyyden sijaan teknologiseen edistyneisyyteen. Neljänneksi, hajautetut rahoituspalvelut tulevat kohtaamaan huomattavaa sääntelyn ja valvonnan epävarmuutta, mikä voi vaikuttaa yrittäjyyteen ja innovaatioihin. (Chen & Bellavitis, 2020, p. 6)

Vaikka hajauksen lähtökohtana onkin avoimuus, voi äärimmäinen avoimuus myös vaarantaa yksityisyyden. Kun rahoitustapahtumat säilötään julkiseen lohkoketjuun, ne ovat vapaasti nähtävissä, mikä voi mahdollistaa yksityisyyden vaarantumisen. Käyttäjän yksityisyyden suojaamiseksi jotkin julkiset lohkoketjut (esim. Monero ja Zcash) hyödyntävät kehittynyttä kryptografiaa käyttäjän identiteetin sekä rahoitustapahtuman yksityiskohtien piilottamiseksi, vaikka ne säilyvätkin edelleen julkisessa lohkoketjussa. Vastaavasti käyttäjän yksityisyyden lisääntyminen edellisen kaltaisissa tapauksissa vähentää läpinäkyvyyttä ja lisää lisättävän tiedon prosessointikustannuksia. (Chen & Bellavitis, 2020, p. 6)

Hajautettujen rahoituspalveluiden ollessa vain vähän tai ei lainkaan suhteessa keskitettyihin tahoihin, voi väärinkäytöstapauksissa olla epäselvää, ketä tulee pitää vastuullisena hajautettujen rahoituspalveluiden ekosysteemissä. Haastavissa tai kiistanalaisissa tilanteissa ei välttämättä myöskään ole keskitettyä tahoa, johon nojata. Ongelmien ilmaantuessa kukaan keskitetty taho ei voi tehdä toimenpiteitä varojen jäädyttämiseksi, ongelmien korjaamiseksi ja liiketoimien palauttamiseksi takaisin normaaliin. Ilman kunnollista vastuullisuutta, hajautetut rahoituspalvelut voivat kohdata merkittäviä rajoitteita. (Chen & Bellavitis, 2020, p. 6)

Hajautetut rahoituspalvelut nojaavat ensisijaisesti koodattuihin sääntöihin ihmisen arvostelukyvyn sijaan. Kustannusten, epävarmuuden ja subjektiivisuuden vähenemisen näkökulmista koodattuihin sääntöihin nojaaminen voi olla etu, mutta samalla se voi olla merkittävä rajoite, sillä se ei välttämättä pysty myöskään hyödyntämään ihmisten subjektiivisen arvostelukyvyn hyötyjä. Jos näitä rajoitteita ei huomioida kunnolla, lohkoketjuun perustuvat hajautetut rahoituspalvelut eivät välttämättä saavuta koko potentiaaliaan. (Chen & Bellavitis, 2020, p. 7)

6.5 FinTech-riskit

Kustannussäästöistä, lisääntyneestä tehokkuudesta ja uudesta datasta sekä saatavilla olevasta tietokoneellisesta tehosta huolimatta FinTech on edelleen alttiina samoille riskeille, joita rahoitusalalla perinteisesti on. Luotto-, likviditeetti-, markkina- sekä operatiiviset riskit voivat vähentyä tai niitä voidaan siirtää, mutta niitä ei voida poistaa kokonaan. Useimmilla markkinoilla digitaaliset rahoituspalvelut eivät ole vielä saavuttaneet systeemisen riskin tasoa, mutta tilanne voi muuttua FinTech:in sekä suurten teknologiayhtiöiden rahoituspalveluiden kasvaessa ja vastaavanlaisten teknologioiden käyttöasteen lisääntyessä perinteisten pankkien toimesta. P2P-lainaaminen saavutti Kiinassa merkittävän tason ennen vuonna 2017 alkanutta tehostettua sääntelyä. Tämä huipentui marraskuussa 2019 vaatimukseen, jonka perusteella kaikki P2P-lainoja tarjoavat alustat muuttuvat säännellyiksi pienlainan tarjoajiksi kahden vuoden sisään tai ne suljetaan. P2P-lainat Kiinassa ja viimeisin Wirecard-epäonnistuminen Saksassa osoittavat FinTech:iä koskevan asianmukaisen sääntelyn ja valvonnan tarpeen. Suuret teknologiayhtiöt ovat jo saattaneet joissain talouksissa, kuten Kiinassa saavuttaa systeemisen merkityksellisyyden tason (liian suuri kaatuakseen). Viranomaiset pyrkivätkin aktiivisesti muodostamaan asianmukaista sääntelyä vastauksena näille riskeille. (Feyen et al., 2021, p. 12)

Rahoituspalveluiden digitaalinen muutos kasvattaa myös kyberturvallisuuden riskejä. Kyberturvallisuus on haaste kaikilla sektoreilla ja kaikille finanssialan palveluntarjoajille, myös FinTech-yhtiöille sekä suurille teknologia-alan yhtiöille. Yhteenliitettävyyden (interconnectivity) lisääntyessä ja palvelukohtaisten käyttöliittymien määrän kasvaessa myös kyberhyökkäyksille altistettu pinta-ala kasvaa. Nämä tekijät voivat myös lisätä operatiivista riskiä, kun entistä suurempi määrä erillisiä tahoja saattaa olla mukana vaikuttamassa yksittäisen tuotteen tai palvelun tuottamiseen tai toimittamiseen, luoden monimutkaisia riippuvuussuhteita. Kyseiset riskit ovat saattaneet kasvaa entisestään COVID 19 -pandemian aikana. Samalla tiettyjä ydinpalveluita on keskitetty entisestään (esimerkiksi pilvipalveluihin) kasvattaen yhden vikapisteen riskin (Single point of failure) mahdollisuutta aiheuttaa koko järjestelmään vaikuttava häiriötilanne. (Feyen et al., 2021, p. 12)

Esimerkiksi useilla markkinapaikoilla P2P-palveluita on pidetty sijoittajien toimesta vaihtoehtona pankkien säästötuotteille, vaikka niillä on todellisuudessa suora

luottotappioriski ilman minkäänlaisia talletusvakuutuksia. Usein sijoittajat eivät ole tietoisia tästä riskistä. Robotti-neuvojat ja pelillistetyt treidaus-alustat altistavat kuluttajia markkinariskeille, jotka muodostuvat kuluttajien rajallisesti ymmärtämistä uusista sijoitusinstrumenteista. DLT-teknologiaan perustuvia markkinapaikkoihin ja jopa konsensusmekanismiin liittyy operatiivisia riskejä, joita ei DLT-maksujen yhteydessä ymmärretä riittävästi. (Feyen et al., 2021, p. 43)

Lisäksi yksityisyyteen ja asiakkaan suojaan liittyy uusia riskejä. Uusia asiakkaita tavoittelevien palveluntarjoajien ja räätälöityjen rahoituspalveluiden leviäminen lisää riskiä yksityisyyden vaarantamisesta sekä loukkaavista tai virheellisistä toimintatavoista asiakkaiden tietämättä. (Feyen et al., 2021, p. 12)

6.6 Älysopimusten riskit

Huolimatta älysopimusten mahdollisuuksista kasvattaa yritysten kustannustehokkuutta, ne voivat myös altistaa ylimääräisille kustannuksille ja riskeille. Näitä voivat aiheuttaa oraakkeliongelma, älysopimusten joustamattomuus, turvallisuuteen liittyvät riskit, älysopimusten kalleus sekä juridiset ongelmat. (Mattila et al., 2019, pp. 74–75, 84; Murray et al., 2019, pp. 16, 42)

6.6.1 Oraakkeliongelma

Oraakkeliongelmalla tarkoitetaan sekä älysopimusten kirjoittamiseen sekä virheellisesti toteutettujen älysopimusten jälkikäteisestä korjaamisesta aiheutuvia kustannuksia. (Murray et al., 2019, p. 19)

Vaikka lohkoketjut voivat poistaa välikäsiä ja kolmannen osapuolen toimijoita, on hyvä huomata, että useat älysopimukset hyödyntävät useissa tapauksissa yhtä tai useampaa kolmannen osapuolen tietolähdettä eli oraakkelia. Oraakkeleita hyödyntäville tahoille kuten yrityksille voi kuitenkin olla haasteellista löytää riittävän tarkkoja, luotettavia, turvallisia, nopeita ja kustannuksiltaan sopivia oraakkeleita, mikä taas saattaa vaikuttaa suoraan älysopimusten toiminnallisuuteen. Otetaan esimerkiksi tilanne, jossa toimittaja saa (älysopimuksen toimeksiantona) maksun, mikäli öljyn hinta nousee. Tässä tapauksessa on

siis tärkeää, että öljyn hintatieto on luotettavaa, tarkkaa ja suojattuna ulkoiselta häirinnältä vähintäänkin kilpailukykyisillä kustannuksilla suhteessa perinteisiin ulkoistuskustannuksiin. Sopimuksen ehdoista riippuen myös datan päivitysten nopeus voi olla yksi tekijä, sillä epätarkka oraakkelidata voi aiheuttaa myös sopimusten jälkiseurauksiin liittyviä kustannuksia. Jos valitun oraakkelin kautta saatu öljyn hintatieto on virheellinen tai viivästynyt, voi yhtiö joutua kompensoimaan älysopimuksesta virheellisesti aiheutunutta transaktiota. (Murray et al., 2019, p. 18)

Oraakkeliongelmaan voidaan liittää myös ihmisen tuottaman tiedon virheellisyys. Esimerkiksi The Wall Street Journal -lehteä voitaisiin käyttää oraakkelirajapintana älysopimuksille. Ihmisen tuottamana julkaisuna on kuitenkin huomioitava mahdollisuus, että alkuperäisissä artikkeleissa on asiavirheitä, mikä saattaisi jälleen aiheuttaa älysopimusten virheellisiä toimeenpanoja. Yhtiöt tulevat tulevaisuudessa käyttämään varoja luotettavien ja sopivien oraakkeleiden löytämiseksi sekä varmistaakseen älysopimusten toimivuuden – ja välttääkseen sitä kautta virheellisistä sopimusten toimeenpanoista aiheutuneita kustannuksia. (Murray et al., 2019, p. 19)

6.6.2 Älysopimusten kalleus

Lohkoketjuperusteiset älysopimusalustat ovat avoimia ja hajautettuja, ja niiden tietotekniset resurssit ovat ostettavissa kenen tahansa käyttöön markkinahinnoittelun puitteissa. Käytännössä kukan tahansa voi määritellä vapaasti loogisia ohjelmointirakenteita lohkoketjuverkon suoritettavaksi. Vapaaseen ohjelmoitavuuteen liittyy kuitenkin riski, että järjestelmään ladattaisiin loputtomia suoritussilmukoita tai järjestelmän lamaantumista (halting problem) aiheuttavaa, ääretöntä laskentakapasiteettia edellyttävää ohjelmointikoodia. Tästä syystä älysopimusalustat veloittavat ohjelmointikoodin suorittamisesta esimerkiksi Ethereum:issa laskentaoperaatiokohtaisesti ja Hyperledger Fabricissa eri toimintojen suorittamiselle on sovellettu maksimiaikarajoituksia. (Mattila et al., 2019, pp. 74–75)

Esimerkiksi Ethereum-älysopimusalustalla ohjelman suorittamisesta maksetaan ’gas’-nimisillä laskentayksiköillä, joiden hinta vaihtelee Ethereumin käyttötarpeen mukaisesti. Tästä syystä tietyn ohjelman suorittaminen välittömästi älysopimusalustalla voi tulla erittäin

kalliiksi. Ethereumin laskentaoperaatiokohtaisesta kustannusrakenteesta johtuen älysopimusten käyttökustannukset voivat vaihdella radikaalisti perinteisiin pilvipalvelualustoihin nähden. Esimerkiksi erään vuonna 2017 suoritetun arviolaskelman perusteella miljoona yksinkertaista liukuluku-laskutoimitusta suoritettuna Ethereum-älysopimusalustalla maksaisi joitakin satoja miljoonia kertoja enemmän kuin perinteisellä pilvipalvelualustalla (esim. Amazon Web Services). (Mattila et al., 2019, p. 75)

On kuitenkin huomioitava, että esimerkiksi edellä mainittu Ethereum perustuu energiankulutukseltaan kuormittavaan Proof of Work -konsensusmekanismiin. Tämä saattaa osaltaan vaikuttaa älysopimusten verrattain korkeaan operaatiokohtaiseen hinnoitteluun. (Business Insider, 2022)

Vuoden 2021 aikana on julkaistu myös energiankulutukseltaan merkittävästi ympäristöystävällisempään Proof of Stake -konsensukseen perustuvia, älysopimukset mahdollistavia lohkoketjuja kuten Cardano, Polygon, Tezoz ja EOS. Myös Ethereum on suunnitellut jo useamman vuoden ajan alustansa muuttamista Proof of Stake -perustaiseksi. (Kaplan, 2021)

Vaikka älysopimuksilla onkin potentiaalia vähentää tiettyjä ylläpitokustannuksia, ne voivat myös lisätä pääomistajien ylimääräisiä kustannuksia ja riskejä. Vaikka lohkoketjuteknologiaan perustuvissa ratkaisuissa on potentiaalia kustannustehokkuuteen, tulee älysopimuksien ja niiden ympärille rakennettuja autonomisten organisaatiohallintomallien pitkäaikaisvaikutuksia tarkastella kriittisesti. (Murray et al., 2019, p. 42)

6.6.3 Älysopimusten hallinnolliset ja juridiset riskit

Yhtenä lohkoketjupohjaisten älysopimusten riskinä voidaan pitää terminologiaa, sillä älysopimusta saatetaan virheellisesti pitää oikeudellisesti pitävän sopimuksen synonyymina. Älysopimuksia tulkittaessa ongelmaksi voi muodostua esimerkiksi koodin ja luonnollisen kielen heikko yhteensovitettavuus. Lisäksi älysopimusten tekniseen toteutukseen perustuva automaattinen toimeenpano tuo esille prosessioikeudellisia näkökulmia sopimusten toimeenpanoon ja riitatilanteiden ratkaisuun liittyen. (Mattila et al., 2019, pp. 84–85)

Älysopimuksia eivät koske perinteiset sopimusoikeuden suojatoimet. Normaalin sopimusoikeuden puitteissa pätemättömänä pidettävä sopimus, voisi älysopimuksena toimeenpanna siihen määriteltyjä toimintoja, jopa pakkoon, vahinkoon tai petokseen liittyvissä tilanteissa. Laittomiin älysopimuksiin ei ole tällä hetkellä olemassa erillisiä suojatoimia. (Eenmaa-Dimitrieva & Schmidt-Kessen, 2019, p. 76)

Siirtymä kohti älysopimuksia ja itsestään suoriutuvaa koodia voi myös aiheuttaa hallinnollisia sekä vastuuseen liittyviä kysymyksiä. On määriteltävä, missä määrin ohjelmistokehittäjiä ja järjestelmien ylläpidosta vastaavia henkilöitä voidaan pitää vastuussa, mikäli älysopimukset eivät toimi toivotulla tavalla. (FSB, 2019, p. 16)

7 Talousrikostorjunnan näkökulma

Kansainvälinen yhteisö on määrittänyt prioriteeteikseen rahanpesun (Anti Money Laundering, AML) ja terrorismin rahoittamisen estämisen (Combating the Financing of Terrorism, CFT). Sen tavoitteena on kansainvälisen rahoitusjärjestelmän stabiliteetin sekä eheyden suojeleminen, terroristien resurssien vähentäminen sekä vaikeuttaa rikollisesta toiminnasta saatuja taloudellisia hyötyjä. Kansainvälinen valuuttarahasto (IMF) on erityisen huolissaan rahanpesusta sekä terrorismin rahoittamisesta omien jäsenmaidensa talouksissa. Ongelma on globaali; rahanpesua suorittavat sekä terrorismia rahoittavat tahot hyödyntävät porsaanreikiä sekä eri kansallisten AML/CFT-järjestelmien eroavaisuuksia ja siirtävät varojaan lainkäyttöalueille, joissa juridiset ja institutionaaliset rakenteet ovat heikkoja. (International Monetary Fund, n.d.)

FATF (The Financial Action Task Force) on itsenäinen kansainvälinen toimija, jonka tehtävänä on kehittää ja ohjata toimintamalleja kansainvälisen talousjärjestelmän suojelemiseksi rahanpesua, terrorismin rahoittamista sekä massatuhoaseiden rahoittamista vastaan. FATF:in suositukset määrittävät rahanpesun estämisen ja terrorismin rahoittamisen torjunnan kansainväliset standardit. (FATF, 2019, p. 0)

Esimerkiksi Suomessa noudatetaan rahanpesulakia, jonka taustalla vaikuttavat kansallisen lainsäädännön ja EU-oikeuden lisäksi myös FATF:in kansainväliset suositukset. Rahanpesulaki velvoittaa tietyillä aloilla toimivia elinkeinonharjoittajia tunnistamaan sekä tuntemaan asiakkaansa sekä laatimaan riskiarvioin toimintaansa liittyvistä väärinkäytösriskeistä. Toimijoiden on omilla toimillaan pyrittävä ehkäisemään rahanpesua ja terrorismin rahoittamista ja velvollisuus ilmoittaa mahdollisista epäilyttävistä liiketoimista keskusrikospoliisin rahanpesun selvittelykeskukselle. (Rahanpesu.fi, n.d.)

7.1 Kryptovaluutat rahanpesun ja terrorismin rahoittamisen välineinä

Tietyillä kryptovaluutoilla on mahdollista suorittaa maksuja ja varojen siirtoja entistä tehokkaammin, mutta tietyt kryptovaluuttojen ominaisuudet tekevät niistä riskisempiä rahanpesun ja terrorismin rahoittamisen näkökulmasta. Erityisesti kryptovaluuttojen transaktioiden nopeus, globaali saavutettavuus sekä mahdollisuus lisääntyneeseen

anonymiteettiin ja maksuliikenteen hämärtymiseen sekä maksujen vastapuoliin tekevät kryptovaluutoista käyttökelpoisia rikollisiin tarkoituksiin. Lisäksi transaktiot voidaan suorittaa ilman välikätenä toimivaa sääntelyn alaista rahoitusalan toimijaa, minkä vuoksi rahanpesua ja terrorismin rahoittamista estäviä toimia kuten asiakkaan tuntemista, tiedon tallentamista tai epäilyttävän maksutapahtuman raportointia ei voida toteuttaa. (Coelho et al., 2021, p. 3)

AML/CFT-sääntelyn, -valvonnan sekä lainsäädännön merkitys kryptovaluuttoihin liittyen on äärimmäisen tärkeää, sillä kryptovaluuttojen käytön osuus laittomissa toimissa on merkittävä. Erään yksityisen sektorin toimijan arvion mukaan vuonna 2019 n. 1,1% (n. 11 miljardia USA:n dollaria) kaikista kryptovaluuttatransaktioista olivat laittomuuksiin liittyviä. Toisen yhtiön arvion mukaan pelkästään Bitcoinia hyödynnettiin rikollisissa tarkoituksissa vuonna 2020 yhteensä 3,5 miljardin USA:n dollarin arvosta. (Coelho et al., 2021, p. 3)

7.2 Kryptovaluuttojen tarjoajien riskisyys talousrikostorjunnan näkökulmasta

Valtiovarainministeriön tuottaman vuoden 2021 kansallisen rahanpesun ja terrorismin rahoittamisen riskiarvion yhtenä päähavaintona nousi, että riskillisimpinä rahanpesun ja terrorismin rahoittamisen sektoreita ovat hawala-toimijat sekä virtuaalivaluutan tarjoajat. Riskiarvion mukaan maksupalvelujen tarjoajiin kohdistuvaa riskitasoa voidaan pitää merkittävänä. Maksupalveluiden tarjoajien sektorin riskinä pidetään uusia toimialalle tulevia ja uutta tekniikkaa soveltavia maksupalveluiden tarjoajia, joiden toiminnallisuuksien ymmärtäminen ja sitä kautta valvonta voi olla haastavaa. Pienten toimijoiden rahanpesun estämisen toiminnot voivat olla puutteellisia tai niitä ei ole, ja tästä syystä myöskään epäilyttävien liiketoimien tunnistamiseen ei välttämättä ole selkeitä toimintatapoja. Myös asiakkaan tuntemisen menetelmät (Know your customer, KYC) voivat olla puutteellisia. Erityisesti tosiallisten edunsaajien ja tosiasiallisten rahanlähettäjien puutteellinen tunnistaminen mahdollistaa tiettyjä riskejä, kuten muuli- ja bulvaanitoiminnan maksupalveluissa. (Isoaho & Kaski, 2021, pp. 10, 47–48)

Analyytikoiden mukaan yksi merkittävä Yhdysvaltalainen kryptovaluuttapörssi vastaanotti vuoden 2020 aikana yhteensä 3,5 miljoonan USA:n dollarin arvosta Bitcoineja suoraan rikollisiin tahoihin yhdistetyistä kryptovaluuttalompakoiden osoitteista vahvasta asiakkaan tuntemisen prosessistaan huolimatta. Sama palveluntarjoaja myös lähetti yhteensä 36,7

miljoonan USA:n dollarin arvosta Bitcoineja rikollisiin tahoihin yhdistettyihin kryptovaluuttalompakoiden osoitteisiin saman tarkastelujakson aikana. Nämä transaktiot olisi voitu pysäyttää riittävän AML-ohjelmiston avulla. (CipherTrace, 2021, p. 9)

Myös FATF:in vuonna 2020 julkaisi uuden rahanpesun estämisen ohjeistuksen virtuaalivaluutoista ja virtuaalivaluuttojen palveluntarjoajista. Julkaisun mukaan virtuaalivaluuttoihin liittyviä varoitusmerkkejä ovat seuraavat:

- Asiakas muuntaa suuren määrän fiat-valuuttaa virtuaalivaluutaksi ilman loogista tai järkevää selitystä
- Asiakas suorittaa samanaikaisesti P2P-maksuja sekä rekisteröitymättömänä virtuaalivaluuttapalvelun tarjoajan sivustolla että pankkitilinsä kautta
- Asiakas käyttää yhtä tai useita virtuaalilompakkoon linkitettyjä pankkikortteja nostaakseen suuria summia fiat-rahaa tai ostaakseen virtuaalivaluuttoja rahalla, joiden alkuperä on käteistalletuksista
- Asiakas on potentiaalinen kryptovaluuttamuuli tai väärinkäytöksen uhri. (CipherTrace, 2021, pp. 54–55)

Kryptovaluuttojen tarjoajien globaali valvonta on toistaiseksi vasta luontivaiheessa. Vaikka kansainväliset AML/CFT-standardit ovatkin voimassa, monet lainkäyttöalueet alkavat vasta nyt valvoa ja panna niitä täytäntöön. (Coelho et al., 2021, p. 1)

FATF on määrittänyt vuonna 2018 virtuaalivaluuttojen palveluntarjoajille kohdistettuja AML/CFT-tarkoituksiin määriteltyjä suosituksia, joiden perusteella palveluntarjoajien tulee olla lisensoituja tai rekisteröityneitä, ja niitä koskevat samat tehokkaaseen monitorointiin ja valvontaan liittyvät vaatimukset kuin muitakin finanssialan toimijoita. (Coelho et al., 2021, pp. 3–4)

7.3 Keskuspankkien digitaaliset valuutat talousrikostorjunnassa

On perusteltua olettaa, että perinteisten fiat-valuuttojen tavoin myös keskuspankkien digitaalisia valuuttoja tullaan siirtämään toistuvasti yli valtiorajojen. Tästä syystä onkin ehdottoman tärkeää, että keskuspankkien digitaalisten valuuttojen (CBDC) kehitys

pilottivaiheista kuluttajien käyttöön priorisoi AML/CFT-sääntelyä. Keskuspankkien digitaalisten valuuttojen lopullisia vaikutuksia maailman taloudelle arvioidaan edelleen ja keskuspankkien digitaalisten valuuttojen vaihteleva kehitys eri maissa herättävät kysymyksiä lopullisesta käyttöönotosta sekä yhteistoimivuudesta toisiinsa nähden. Vaikka useat maat ovat jo ottaneet merkittäviä askeleita keskuspankkien digitaalisten valuuttojen osalta, monien maiden lainsäädännön rakenteet keskuspankkien digitaalisille valuutoille ovat edelleen puutteellisia. (CipherTrace, 2021, p. 63)

Kuluttajakäyttöä varten keskuspankkien digitaaliset valuutat edellyttävät valtavia operatiivisia toimenpiteitä mm. maksuliikenteen, tilien sekä rahanpesun ja terrorismin rahoittamisen estämisen näkökulmista. On perusteltua olettaa yksityisen sektorin hallitsevan näitä toimenpiteitä keskuspankkeja tehokkaammin. (Auer & Böhme, 2021, p. 4)

Valtiollisten hallintojen sekä keskuspankkien näkökulmasta laittoman rahaliikenteen havainnointi tulee kuitenkin helpottumaan keskuspankkien digitaalisten valuuttojen avulla. (Binance, 2021)

7.4 Stablecoinit talousrikostorjunnassa

Stablecoinien markkina-arvo on yli kaksinkertaistunut Covid 19 -pandemian alun jälkeen ja samanaikaisesti myös stablecoinien käyttö on lisääntynyt merkittävästi. Tämä markkinakehitys on pakottanut viranomaisia ympäri maailmaa määrittelemään sääntelyä ja linjauksia stablecoinien ympärille. EU:n määritelmän mukaan merkittävät stablecoinit aiheuttavat kohonneen riskin taloudelliseen stabiliteettiin, rahapolitiikkaan ja rahaan liittyvään suvereniteettiin, mitä ei ole havaittavissa niin kutsutusti vähäisemmän käyttötarkoituksen valuutoilla. Stablecoineja voidaan pitää systeemisesti merkittävinä maksujärjestelminä, mikä korostaa sääntelyn merkityksellisyyttä. (Arner et al., 2020, pp. 8, 13–14)

Stablecoinit kasvattavat merkittävästi myös muita sääntelyyn ja valvontaan liittyviä riskejä ja erityisesti FATF sekä G20 ovat kiinnittäneet huomiota rahanpesuun sekä terrorismin rahoittamiseen liittyviin riskeihin, jotka muiden kryptovaluuttojen tavoin liittyvät myös stablecoineihin. (Arner et al., 2020, p. 14)

Historiassa on esimerkkejä rahan liikkeellelaskijoista, joiden menestyksekäs liiketoiminta on saanut ne osallistumaan entistäkin kannattavampiin liiketoimintoihin, kuten lainanantoon. Viimeisimpänä esimerkkinä markkina-arvoltaan (tämän opinnäytetyön kirjoitushetkellä 14.12.2021) suurin stablecoin Tether, joka on väittänyt kaikkien liikkeelle laskemiensa varojen olevan 100%:sti sidottuja fiat-valuuttaan. Vuodesta 2019 asti New Yorkin yleinen syyttäjä on syyttänyt Tetheriä ainakin 700 miljoonan USA:n dollarin lainaamisesta Bitfinex-nimiselle kryptovaluuttojen välitysalustalle. Syyte kyseenalaistaa Tetherin todellisen arvon, kun sitä ei tällöin voidakaan pitää täysin turvalliseen varallisuuteen sidottuna varallisuusluokkana vaan ainoastaan vaihtelevasti turvallisiin varallisuuksiin sidottuna varallisuusluokkana. (Arner et al., 2020, p. 15)

Yhdysvaltain valuutanvalvojan toimisto (US Office of the Comptroller of the Currency, OCC) linjasi kirjeessään tammikuussa 2021, että kansalliset pankit ja liittovaltion säästöyhdistykset voivat käyttää stablecoineja sekä toimia riippumattomana noodina toteuttamassa ja varmentamassa maksujentoimintoja, hallinnoida sekä kirjata maksutransaktioita. Toiminnan ehtona on, että käytettävä stablecoin mahdollistaa kaikkien transaktioihin osallistuvien osapuolten tunnistamisen, mukaan lukien yksityiset virtuaalivaluuttalompakot. Linjaus on merkittävä askel yhdysvaltalaisen talousjärjestelmän laajentamisesta myös stablecoinien piiriin, mutta linjauksessa varoitetaan myös potentiaalisista riskeistä, joita kehitys voi aiheuttaa toimijoille sekä operatiivisesta, juridisesta että väärinkäytösten näkökulmasta. Uudet teknologiat edellyttävät riittävää teknologista erityisosaamista, jotta pankit kykenevät hallitsemaan näitä riskejä. Kirjeessä tuodaan esiin, että pankkien tulisi tehdä huolelliset esiselvitykset ja arvioida AML- ja compliance-riskejä toimiessaan stablecoinien liikkeellelaskijoiden kanssa, sekä varmistaa yleisesti riittävä ymmärrys kryptovaluuttoihin liittyvistä riskeistä. (CipherTrace, 2021, pp. 63–64)

7.5 Lohkoketjun käyttäjän yksityisyys ja asiakkaan tunteminen

Pankkien kaltaiset maksunvälittäjinä toimivat kolmannet osapuolet ovat sääntelyn ja lain puitteissa velvollisia estämään rahanpesua ja terrorismin rahoittamista, tuntemaan asiakkaansa sekä huolehtimaan asiakkaan tuntemisen prosesseistaan, kirjaamaan ja

taltioimaan suoritettuja transaktioita sekä raportoimaan epäilyttävistä tilitapahtumista. (Coelho et al., 2021, p. 3)

Jotta lohkoketjuteknologia voitaisiin ottaa käyttöön taloudellisiin järjestelmiin, tulisi asiakkaan tuntemisen prosessien (Know-Your-Customer, KYC) sekä asiakkaan perusteellinen tunteminen (Customer Due Diligence, CDD) olla linjassa talousrikostorjuntaan (AML) ja terrorismin rahoittamisen vastaiseen työhön (CFT) liittyvän sääntelyn kanssa. (Natarajan et al., 2017, p. 19)

Useissa avoimissa DLT-pohjaisissa teknologioissa verkon jäsenten yksityisyys pyritään nimenomaisesti salaamaan, mikä mahdollistaa esimerkiksi transaktiot tuntemattomien osapuolten kanssa, aiheuttaen samalla ristiriitatilanteen edellä mainitun AML/CFT-sääntelyn kanssa. Luvanvaraisissa DLT-järjestelmissä asiakkaan tuntemiseen liittyvät haasteet ratkeavat järjestelmän luvanvaraisuuden turvin, koska järjestelmään pääsee vain sovitusti. Tällöin myös AML/CFT-näkökulma voidaan tarpeen mukaan toteuttaa sääntelyn mukaisella tavalla. (Natarajan et al., 2017, p. 19)

Kaikissa keskitetyissä kryptovaluutan vaihtopalveluihin keskittyneissä pörsseissä on lähtökohtaisesti kirjautumisprosessi, jossa lainsäädännöstä riippuen käyttäjien tulee tunnistautua esimerkiksi sähköpostin, puhelinnumeron tai viranomaisen myöntämällä henkilöllisyystodistuksella. Edellä mainitun rahanpesun ja terrorismin rahoittamisen estämiseen liittyvän lainsäädännön ja sääntelyn puitteissa pörssien tulee kerätä riittävä määrä tietoa asiakkaistaan voidakseen tarjota heille palveluitaan. Lohkoketjuteknologiaan perustuvissa hajautetuissa kryptovaluuttojen välityspalveluissa (Decentralized Exchanges, DEX) tunnistautumistietoja ei sen sijaan edellytetä vaan välityspalvelut ovat käyttäjien vapaassa käytössä. Ainoa jaettu informaatio on lohkoketjuun tallennettu kryptovaluuttalompakon osoite, joka näkyy kryptovaluuttatransaktion toisena osapuolena DEX:in lisäksi. DEX:ien etu niiden helppokäyttöisyys kryptovaluuttojen vaihdannassa, mutta vastaavasti niiden heikkous on, että ne eivät tue perinteisiä fiat-valuuttoja kuten Yhdysvaltain dollaria tai euroa, jotka on sidottu keskitettyihin hallintoihin kuten pankkeihin tai vastaaviin finanssi-instituutioihin. (Lorne & Cawrey, 2020, pp. 172–173)

7.6 Älysopimusten hyödyntäminen väärinkäytösten ja petosten estämisessä

Älysopimukset ovat koodimuotoisia sopimuksia, jotka toteuttavat itseään automatisoidusti lohkoketjussa sopimukseen ohjelmoitujen komentojen mukaisesti. Älysopimus siis määrittää tarkat kriteerit, jotka transaktion osapuolten, lähettäjän ja vastaanottajan, tulee täyttää transaktion toteuttamiseksi. Pysyvä merkintä toteutuneesta transaktiosta tallentuu tämän jälkeen lohkoketjuun. Tämä voi osaltaan hyödyttää väärinkäytösten ja petosten vähentämisessä. (Davies, n.d.; Murray et al., 2019, p. 8)

7.7 Hajautetut rahoituspalvelut talousrikostorjunnassa

Hajautetut rahoituspalvelut (Decentralized Finance, DeFi) ovat seuraava merkittävä uhka väärinkäytösten ja rahanpesun näkökulmasta. Vuonna 2020 yhteensä puolet kaikista varkauksista, yhteensä 129 miljoonaa USA:n dollarin kokonaissumma, liittyi DeFi-palveluihin kohdistuneisiin hakkerointeihin. DeFi-sektorin eksponentiaalinen pääoman kasvu sekä selkeän sääntelyn puuttuminen ovat houkutelleet rikollisia toimijoita DeFi-sektorille ja suurin osa DeFi-hakkeroinneista on toteutettu viimeisimmän vuoden aikana.
(CipherTrace, 2021, p. 11)

Vuoden 2020 suurin varkaus kohdistui keskitettyyn kryptovaluuttapörssi KuCoiniin, josta hakkeroitiin varoja yhteensä 281 miljoonan USA:n dollarin arvosta. Varkaus liittyy olennaisesti myös DeFi-palveluihin, kun KuCoinin hakkeroineet rikolliset yrittivät pestä varastamiaan varoja maailman suurimman hajautetun rahoituspalveluiden tarjoajan, Uniswapin kautta. On selvää, että DeFi-sektori on kasvanut yhdeksi suurimmista kryptovaluutta-alan trendeistä ja tästä syystä kyseisiin palveluihin tulee suhtautua varauksella myös rahanpesuriskin näkökulmasta. Hajautetut palveluntarjoajat eivät useimmiten kerää KYC-tietoja käyttäjistään, eikä niillä oli keskitettyjen palvelutarjoajien tavoin mahdollisuuksia varojen jäädyttämiseen. (CipherTrace, 2021, pp. 11–12)

DeFi-palvelut on suunniteltu vapaasti käytettäviksi. Puutteellisesta sääntelystä ja KYC-prosesseista johtuen DeFi-palveluista on tullut rahanpesun keskittymiä vuoden 2020 loppupuolella. Viranomaiset ovat selkeästi kiinnittäneet huomiota DeFi-palveluihin sekä niihin liittyviin compliance-vaatimuksiin. DeFi-sektorin kasvun myötä voidaan odottaa myös

viranomaistahojen huomion kiinnittymistä DeFi-projekteihin. FATF tulkitsee jo nyt hajautettujen rahoituspalveluiden palveluntarjoajat virtuaalisten varojen palveluntarjoajiksi. (CipherTrace, 2021, pp. 13–14)

8 Lohkoketjuteknologian tulevaisuus pankkisektorilla

Lohkoketjuteknologia on edelleen aikaisessa kehitysvaiheessa ja tulevaisuuden skenaarioita on lukuisia: osa uskoo alan lopulta kehittyvän kohti yhtä (maailmanlaajuisen internetin kaltaista) maailmanlaajuista julkista lohkoketjua, sekä lukuisia yksityisiä intranetien kaltaisia lohkoketjuja, kun taas toiset uskovat lukuisten julkisten lohkoketjujen rinnakkaiseloon. Alun perin internet oli informaation internet, jonka vaikutuksena oli demokraattinen tiedon saatavuus. Mahdollinen lohkoketjun tulevaisuuden skenaario voisi olla arvon internet eli demokraattinen mahdollisuus digitaalisen varallisuuden saavutettavuuteen sekä varastointiin. (Natarajan et al., 2017, p. 12)

Accenture on arvioinut jo vuonna 2018, että kansainvälinen pankkisektori voisi säästää jopa 20 miljardia USA:n dollaria vuoteen 2022 mennessä innovatiivisten lohkoketjuteknologian sovellusten avulla. (Garg et al., 2021, p. 2)

Lohkoketjuteknologiaan kohdistuu odotuksia erityisesti luotettavan sähköisen tunnistautumisen toteuttamisessa. Nykyisten tunnistautumistapojen digitalisoinnin sijaan tulisi pohtia mahdollisuutta kokonaan uuden digitaalisen tunnistautumisen yleiskäyttöisestä arkkitehtuurista. Sähköinen tunnistaminen voidaan jaotella kolmeen osa-alueeseen: henkilön yksilöinti, käyttöoikeuden yhdistäminen kyseiseen henkilöön sekä käyttöoikeuden pätevyyden varmentaminen. Yhtenä perinteisten sähköisten tunnistautumisjärjestelmien kehityksen haasteena on eri järjestelmien keskinäinen yhteensopivuus. Lohkoketjuteknologian ajatellaan voivan helpottaa käyttöoikeuksien hallintaa sekä varmentamista ympäristössä, jossa erilaisia käyttöoikeuksia tulee pystyä hallitsemaan ja varmentamaan useiden eri tahojen toimesta. (Mattila et al., 2019, pp. 27–28)

Arvioiden mukaan lohkoketjuteknologian hyödyntäminen tunnistautumisessa ja asiakashallinnassa parantaisi asiakkaiden palvelukokemusta. Lisäksi tällä voitaisiin saavuttaa merkittäviä säästöjä pienentyneinä toiminnan kuluina sekä petosten vähenemisenä. Esimerkiksi finanssilaitosten R3-yhteenliittymä kehittää omaa KYC-sovellustaan. Suomessa on myös käynnissä yhteishanke, jossa lohkoketjurekisteriin säilötään asiakkaiden laskutustietoja. (Honkanen, 2017, p. 15)

Tulevaisuudessa lohkoketjua voitaisiin hyödyntää jopa finanssialan toimijoiden yhteisenä asiakkaan tuntemisen alustana. Tämä mahdollistaisi tarvittaessa rajattoman dokumenttien tiedonvaihdon eri finanssialan toimijoiden välillä. (Garg et al., 2021, p. 4)

Yhteisten KYC- ja AML-prosessien mahdollistaman kuormituksen vähenemisen lisäksi yhteistä lohkoketjua hyödyntävät pankit voisivat esimerkiksi luoda älysopimuksia, turvata kauppakirjoja ja automatisoida varojen vapautuksia tavaroiden toimituksia vastaan. Uusien kyvykkyyksien käyttöönotto osaksi tulevaisuuden pankkien strategiaa mahdollistaa luottoriskien hallinnan parantamisen ja väärinkäytösten tehokkaamman estämisen lisäksi myös dokumenttien käsittelyyn ja sääntelyyn liittyvien kustannusten vähentämisen. (Brus & Rus, 2021, p. 38).

8.1 FinTech-yritysten vaikutus pankkisektorin tulevaisuuteen

Visan, PayPal:in ja SWIFT:in kaltaiset keskitetyt maksujärjestelmät helpottavat online- ja offline-kaupankäyntiä, mutta veloittavat yleensä melko korkeita hintoja palveluistaan, erityisesti valtiolliset rajat ylittävissä maksuissa. Maksamisen hinnat ovat säilyneet korkeina, vaikka internet on merkittävästi laskenut kustannuksia lukuisissa palveluissa. Hajautukseen perustuvat maksujärjestelmät lupaavat halvempia, nopeampia kansainvälisiä maksuja ratkaisten juuri perinteisten maksupalveluiden ongelmia. Hajautetut maksupalvelut luottavat lohkoketjuteknologiaan ja kryptovaluuttoihin, jotka ovat globaaleja, ja joilla valtiolliset rajat ylittävät maksut voidaan suorittaa nopeasti ja halvalla. (Chen & Bellavitis, 2020, pp. 4–5)

Informaation ja tavoitettavuuden kehitys on johtanut finanssipalveluiden kulutuksen eriyttämiseen. Asiakkailla on nyt enemmän tietoa eri palveluntarjoajista ja parantuneet mahdollisuudet toimia eri palveluntarjoajien välissä, voiden valita käyttämiään finanssituotteita eri palveluntarjoajilta. Samoin palveluntarjoajilla on entistä enemmän mahdollisuuksia saada tietoa uusista tai potentiaalisista asiakkaista, joille tarjota palveluita suoraan kohdennetun markkinoinnin avulla. Ennen vain yhden finanssialan toimijan tarjoamat palvelut voivat nykyään olla useiden nimenomaiseen palveluun erikoistuneiden yritysten tarjoamia. Kuluttajien käyttöliittymät siirtyvät fyysisistä toimipisteistä kätevästi digitaalisesti saataviksi mistä sijainnista tahansa. Digitaaliset kuluttajien käyttöliittymät

(kuten internet, mobiili) mahdollistavat kuluttajia suoraan lähestyvät uudet toimijat sekä lähellä että kaukana. Käyttämällä eri kilpailijoiden applikaatioita kuluttajat voivat rakentaa oman kokonaisen pankkinsa ja saavuttaa personoidumman pankkipalvelukokonaisuuden. Tämä on todennäköisesti vähentänyt vanhojen fyysisten verkostojen arvoa sekä vakiintuneiden toimijoiden otetta asiakkaistaan, jotka voivat helposti siirtää varojaan muille toimijoille saadakseen käyttöönsä haluamansa palvelut. (Feyen et al., 2021, pp. 14–15)

Teknologia on vähentänyt perinteisen, niin kutsutun back office -infrastruktuurin kustannuksia ja muuttanut niiden tarvetta paperin prosessoinnista datakeskuksiksi. Prosessiautomaatio sekä ohjelmistojen ja IT-järjestelmien kehitys aiheuttavat finanssialan toimijoille uudelleen järjestelyjä sekä henkilöstön vähentämistä. Kokonaiset prosessit sekä useat taidot, joihin aiemmin palkattiin osaajia, voidaan nykyään korvata automaatiolla tai tekoälypohjaisilla asiantuntijajärjestelmillä. Tämä on luonut tilaa kolmannen osapuolen toimijoille, kuten pilvipalveluiden tarjoajille ja FinTech-yrityksille, jotka ovat erikoistuneet SaaS-palvelujen tuottamiseen pankeille. Esimerkkejä tällaisista palveluista ovat esimerkiksi datan prosessointi, luottoriskipisteytykset ja elektroniset asiakkaan tuntemisen palvelut (e-KYC). Pankki voi esimerkiksi toimia yhteistyössä uniikkia dataa hyödyntävän, luottoriskipisteytysten erityisosaamista tarjoavan yhtiön kanssa, mahdollistaen näin saumattoman asiakaskokemuksen. (Feyen et al., 2021, pp. 15–16)

8.2 Toimenpiteet lohkoketjuteknologian käyttöönottoon

Lohkoketjuteknologian käyttöönottoon on ehdotettu neljää strategista lähestymistapaa riskien mitigoimiseksi. ”Kokonaisen toimialan strategia” (The all-industry strategic maneuver) on yleisesti tunnettu strategia, jossa toimialan yhtiöt siirtyvät samanaikaisesti hyödyntämään lohkoketjuteknologiaa. Tällöin minimoidaan yksittäisen yhtiön lohkoketjuteknologian käyttöönoton ajoitukseen liittyvää riskiä. Näin korkeatasoinen yhteistyö edellyttää kuitenkin luottamusta ja läpinäkyvyyttä kaikkien siirtymään osallistuvien välillä. Kyseinen strategia on mahdollinen, kun alan vakiintuneet johtavat tahot kohtaavat suhteellisen samankaltaisia uhkia ja lohkoketjuratkaisujen hyödyt ja kustannukset voidaan jakaa tasan kyseisten toimijoiden kesken. (Malhotra et al., 2021, p. 14)

”Aidatun puutarhan strategia” (The walled garden strategic maneuver) on strateginen lähestymistapa, jossa osallistujat luovat suljetun lohkoketjun saavuttaakseen hyötyjä ei-osallistuviin tahoihin nähden. Alan johtava yhtiö voi määrittää lohkoketjun standardit, joiden puitteissa muiden osallistujien on toimittava kyetäkseen yhteistyöhön. Pienempi, muutamasta organisaatiosta muodostettu hallinnollinen ryhmä voi kuitenkin välttää konsensuskehityksen päätyen vain osin hajautettuun järjestelmään. IBM on todennut aidatun puutarhan strategian suosituksi. Tämä mahdollistaa nopeamman markkinoille siirtymisen, järjestelmän nopeamman käytettävyyden arvon luomiseen ilman tarvetta noodien hallintaan sekä lohkoketjusovelluksen keskitetyn hallinnan ja kehityksen. Samanaikaisesti haittapuolia ovat lohkoketjulle ominaisen hajautuksen puutteellisuus, osallistujien ja ei-osallistujien eriytyminen ja sitä kautta kilpailevien puutarhojen luonti. Lisäksi kilpailevien ratkaisujen yhteentoimivuuden ongelmat voivat johtaa kannattamattomaan ratkaisuun. (Malhotra et al., 2021, pp. 15–16)

Aidatun puutarhan strategia minimoi turvallisuus- ja tietoturvaan liittyviä riskejä, kun dataa kontrolloidaan ”puutarhan sisällä”. Sekä koko toimialan strategia että aidatun puutarhan strategia perustuvat onnistuneeseen kumppaneiden valintaan ja suunnitteluun sekä näiden valintojen onnistuneeseen implementointiin. Strategiat toimivat, kun käyttöön otettu lohkoketjuratkaisu ei uhkaa arvoketjun suurimpia toimijoita ja osallistujien poisjäänti ei aiheuta hallinnollisia ongelmia. (Malhotra et al., 2021, p. 17)

”Useiden puutarhojen strategia” (The many gardens strategic maneuver) tarkoittaa, että yritys sitoutuu samanaikaisesti useisiin aidattuihin puutarhoihin. Tämä strategia hajauttaa riskiä ja lisää yhtiön sietokykyä sekä joustavuutta. Sietokyky on korkealla tasolla, koska yhtiö kestää takaiskuja yksittäisten puutarhojen osalta, kunhan muut menestyvät. Strategia myös mahdollistaa yritystä panostamaan menestyksekkäämpiin puutarhoihin ja hylkäämään heikommin menestyvät. JP Morgan on viisaasti jakanut resurssejaan erityyppisten lohkoketjuhankkeiden (puutarhojen) kehittämiseen, kuten Interbank Information Network (IIN) ja Dromaius. IIN on lohkoketjuun perustuva P2P-verkosto, joka kehittää pankkien välistä tiedonjakoa yli valtiorajojen. Dromaius on lohkoketjuun perustuva alusta, jonka tarkoituksena on parantaa pääomamarkkinoita kehittämällä rahoitusinstrumentteja yksinkertaisemmiksi ja saumattomammiksi. (Malhotra et al., 2021, pp. 17–18)

Useiden puutarhojen käyttö mahdollistaa joustavan liikehdinnän eri puutarhojen välillä tulevien tapahtumien etenemisen mukaan. Strategian vahvuus on sen tiedostavuudessa, ettei kaikkia päätöksiin ja implementointiin liittyviä virheitä voida välttää epävarmassa ympäristössä. Tärkeää onkin mahdollistaa rajattu kokeilu ja oppiminen (aidatut puutarhat) ja hyödyntää opittuja asioita vakiintuneemmissa liiketoiminnoissa, kuten JP Morgan tekee perinteisen pankkiliiketoiminnan saralla. Tämä mahdollistaa JP Morganin perinteisen liiketoiminnan parantamisen ja minimoi riskiä työn imun häiriöstä tai huolestuneista työntekijöistä. (Malhotra et al., 2021, p. 18)

“Useita vaihtoehtoja lähestyvä strategia” (The Options Approach Strategic Maneuver) on lohkoketjuteknologian käyttöönotossa hyvin samankaltainen kuin useiden puutarhojen strategia siinä mielessä, että vaihtoehdoissa tiedostetaan ympäristön nimenomainen epävarmuus. Samoin kuin useiden puutarhojen strategia, useita vaihtoehtoja lähestyvä strategia voi olla suositeltavampi sovellutuksissa, joissa lohkoketjuteknologian standardit eivät ole vielä valmiiksi muodostuneita. Useiden puutarhojen strategiaan verrattuna useita vaihtoehtoja lähestyvä strategia voi olla alkuvaiheessa vähemmän resursseja sitova, sillä yhtiöt tekevät vain pieniä sijoituksia varmistaakseen niin sanotusti osallistumisoikeuden. Tämä strategia mahdollistaa vain matalan juridisen ja teknologisen riskin säilyttäen samalla yhtiölle korkean joustavuuden ja mahdollisuuden exitiin, mikäli vaihtoehto muodostuu vaikeasti hallittavaksi. (Malhotra et al., 2021, pp. 18–19)

Lohkoketjujen levitessä erilaiset yhtiöt tulevat tekemään erilaisia ratkaisuja. Olemme edelleen lohkoketjuteknologian leviämisen alkuvaiheessa ja yksittäisten valintojen tulokset eivät vielä ole tiedossa. Voittajan arvaaminen on tyypillisesti helpompaa epävarmuuden hälvetessä ajan myötä, mutta myös odottaminen voi osoittautua kalliiksi. Mobiililaitteiden käyttöjärjestelmämaailmassa Applen OS, aidattu puutarha, ja Androidin avoin puutarha levisivät nopeasti ja skaalautuivat laajasti vieden tilan muilta potentiaalisilta käyttöjärjestelmiltä, kuten Nokian Symbianilta. (Malhotra et al., 2021, pp. 19–20)

8.3 Tulevaisuuden ilmiöt

Kuten Covid-19 on osoittanut, jakeluketjut ja ekosysteemit ympäri maailman ovat alttiita katastrofaalisille häiriöille. Covidin jälkeisessä lisääntyneiden häiriöiden maailmassa tarvitaan

arvonluonnin ja ekosysteemien suunnittelua uudelleen. Yksi esimerkki tästä on IBM:n Digital Health Pass -sovellus, joka mahdollistaa käyttäjilleen halutessaan testaus- ja rokotushistoriansa jakamisen jakamatta kuitenkaan muuta tunnistettavaa henkilötietoa. Digital Health Pass edustaa massiivista siirtymää, missä yksityistä ja suojattua lääketieteellistä dataa voidaan turvallisesti jakaa. Tähän ongelmaan ei olisi ollut ratkaisua vielä vuonna 2019. Lohkoketjuteknologiaan perustuva Digital Health Pass varmistaa henkilökohtaisen ja yksityisen datan jakamisen lukuisten eri tahojen järjestelmässä turvallisesti, hyödyntäen älysopimusten logiikkaa ilman datan tarpeetonta varastointia. (Malhotra et al., 2021, p. 20)

Älysopimukset voisivat tulevaisuudessa mahdollistaa tiettyjen transaktioiden automatisoinnin, kuten esimerkiksi asunnon kauppahinnan siirron vasta asunnon kuntotarkistuksen vahvistuksen jälkeen. Älysopimukset voisivat myös toteuttaa mikromaksuja niin kutsutussa asioiden internetin (Internet of Things) ympäristössä, kuten esimerkiksi itsestään ajavat autot maksaisivat toisilleen mikromaksuja kaistanvaihdoista, jotta kiireisemmät pääsisivät etenemään ruuhkaisessa liikenteessä nopeammin tai tietokoneet maksaisivat toisilleen prosessitehon tai tallennustilan käytöstä. Hallitukset voisivat hyödyntää ”ohjelmoitua rahaa” stablecoinien tai CBDC:ien muodossa rajatakseen kyseisen rahan käyttötarkoituksia esimerkiksi siten, että hallitukselta henkilölle maksettuja varoja voitaisiin käyttää vain ruokaostoksiin ja kyseiset varat erääntyisivät määrättyyn ajankohtaan mennessä. (Arner et al., 2020, p. 7)

9 Johtopäätökset ja pohdinta

Lohkoketjuteknologiaa voidaan lähtökohtaisesti pitää vallankumouksellisena teknologiana, jonka vaikutukset tulevat hyvin suurella todennäköisyydellä vaikuttamaan nykyisiin järjestelmiimme erityisesti pitkällä aikavälillä. Nykyisessä mediaympäristössä lohkoketjuteknologia on kuitenkin ajautunut trendinomaiseksi puheenaiheeksi, jossa varsinaisen teknologian ymmärtäminen jää osin huomiota herättävän otsikoinnin ja mitä mielikuvituksellisempien ideoiden varjoon. Kryptovaluutat ovat erityisen hyvä esimerkki tästä ilmiöstä. Jos kuitenkin pohditaan nykyistä globaalia tilannetta, missä sadat miljoonat (jopa miljardit) ihmiset ovat edelleen vailla pankkipalveluita sen useissa eri muodoissa, tai elävät yhteiskunnissa, joissa ei ole käytössä luotettavia ja ajantasaisia rekistereitä, voidaan nimenomaan lohkoketjuteknologian mahdollistamia ratkaisuja pitää mullistavina pitkällä aikavälillä.

9.1 Merkityksellisyys pankkisektorille

Yhtenä todisteena väittämälle lohkoketjuteknologian poikkeuksellisesta merkittävyydestä voidaan pitää lukuisten eri kokoisten ja ympäri maailmaa sijaitsevien yhtiöiden lohkoketjuteknologiaan liittyviä tutkimus- ja kehityshankkeita. Erityisesti toimitusketjuista sidonnaiset toimijat sekä finanssialan toimijat toimivat tämän tutkimus- ja kehitysaallon harjalla. Yksi syy juuri kyseisten alojen toimijoiden lohkoketjuteknologiaan liittyvään kiinnostukseen liittynee lohkoketjuteknologian perustavanlaatuisiin ominaisuuksiin hajautetun tilikirjan läpinäkyvyydestä, nopeudesta, turvallisuudesta sekä muista teknologisista ominaisuuksista, jotka mahdollistavat erilaisten sovellutusten laajamittaisen hyödyntämisen. Esimerkiksi globaali maksunvälittäjä Visa esitteli syyskuussa 2021 projektinsa, jonka tarkoituksena on luoda ”universaali maksukanava”, joka yhdistää useita eri lohkoketjuja mahdollistaen esimerkiksi kryptovaluuttojen, stablecoinien sekä keskuspankkien digitaalisten valuuttojen (CBDC) siirtämisen eri lohkoketjujen ja lompakkojen välillä. Toinen syy suuriin tutkimus- ja kehityshankepanostuksiin voi toki myös liittyä tarpeeseen lohkoketjuteknologian riskien ymmärtämisestä ja hallitsemisesta jo ennen teknologian laajamittaisempaa globaalia käyttöönottoa.

Jo pelkästään lohkoketjuteknologiaan sidoksissa olevien kryptovaluuttojen vuoksi

lohkoketjuteknologian vaikutus pankkisektoriin on merkittävä. Uudet maksutapahtumiin liittyvät innovaatiot pakottavat pankkeja tarkastelemaan omaa toimintaansa sekä nykyisten prosessiensa tehokkuutta useista eri näkökulmista ja samalla varmistamaan, ettei uusi ja toistaiseksi puutteellisesti säännelty lohkoketjuteknologia eri sovellutuksineen aiheuta tarkan sääntelyn alla toimiville pankkisektorin toimijoille hallitsemattomia riskejä.

Teknologinen kehitys tulee perinteisten pankkisektorin toimijoiden ja FinTech-yhtiöiden muodostamassa markkinassa mahdollistamaan tulevaisuudessa kuluttajille suunnattuja digitaalisia pankkipalveluita, jotka mahdollistavat jokaiselle käyttäjällä henkilökohtaisesti sopivimman palvelukokonaisuuden. Tässä kokonaisuudessa saattaa olla yhden sijasta lukuisia eri rahoituspalveluiden tarjoajia, joiden välillä kuluttajan varat liikkuvat saumattomasti käyttötarpeen mukaan. Pankkisektorin perinteisten toimijoiden on kilpailukykynsä varmistamiseksi pystyttävä vastaamaan tähän kehityssuuntaan, mikä tarkoittaa suurella todennäköisyydellä merkittäviä panostuksia tutkimukseen ja kehitykseen, myös lohkoketjuteknologian saralla. Huomionarvoista kuitenkin on, että teknologisesta kehityksestä puhuttaessa Suomi on teknologisesti merkittävästi edellä monien muiden maiden pankkisektorin toimijoita ja näin ollen tutkimuksen ja kehityksen aallonharjalla pysyminen on tietyiltä osin suhteellista.

Kansainvälinen konsulttiyhtiö McKinsey on kyseenalaistanut blogissaan vuonna 2021, ovatko pankkisektorin nykyiset rakenteet eri osa-alueilla riittävän mukautumiskykyisiä tulevaa teknologista kehitystä silmällä pitäen. Tällä teknologisella kehityksellä viitataan lohkoketjuteknologian lisäksi myös tekoälyyn (AI) sekä syväoppimiseen (deep learning). On myös aiheellista pohtia, ovatko pankkisektorin toimijat riittävän mukautumiskykyisiä tästä nopeasta teknologisesta kehityksestä aiheutuviin sääntelyyn liittyviin ja institutionaalisiin muutoksiin (‚joita väistämättä seuraa uuden teknologian mahdollistamista reaaliaikaisista maksuista), uusista viestistandardeista sekä hallinnollisiin, väärinkäytöksiin ja yksityisyyteen liittyviin riskeihin. On selvää, että nämä vaatimukset tulevat kuormittamaan pankkisektorin toimijoita erityisesti vähemmän tai heikoimmin kehittyneissä maissa, mutta uskoakseni näihin riskeihin ja muutoksiin olisi hyvä varautua ennalta myös niiden toimijoiden parissa, jotka ovat prosesseiltaan ja teknologisesti alansa edelläkävijöitä.

Tietyissä yhteyksissä lohkoketjuteknologian merkittävyyttä on jopa verrattu internetin

ensivaiheisiin. Yhtäläisyyksiä voidaan löytää mm. internetin alkuvaiheen massiivisen käyttöönoton jopa trendimäisestä lähestymisestä, jonka vuoksi ihmisillä oli alkuhuumassa kova into hyödyntää internetiä kaikessa ymmärtämättä sen riskejä sekä tiettyjä teknisiä rajoitteita. Lohkoketjuteknologiassa on jo nyt havaittavissa samoja piirteitä ja tämä tulee hyvin suurella todennäköisyydellä korostumaan vielä nykyisestään lähivuosina. Pankkisektorin toimijoiden tasolla lohkoketjuteknologian vaikutukset tulevatkin tästä johtuen näkymään erityisesti tarpeena kehittää henkilöstön osaamista ja ymmärrystä kyseisestä teknologiasta, sen mahdollisuuksista, hyödyistä, haitoista ja riskeistä. Erityisesti juridisesta näkökulmasta osaamisen jatkuva kehittäminen tulee olemaan ensisijaisen tärkeää, sillä lohkoketjuteknologia tulee aiheuttamaan uusia epävarmuuksia oikeudellisten vastuiden ja esimerkiksi kuluttajansuojan näkökulmista. Yksi olennainen esimerkki teknologisen ja juridisen yhteistyön tiiviistä tarpeesta tulevaisuudessa ovat älysopimukset, joiden soveltaminen voi parhaimmillaan mahdollistaa paljon, mutta aiheuttaa samalla puutteellisen tietotaidon seurauksena valtavia taloudellisia, teknisiä ja mainehaittoihin liittyviä riskejä. Pahimmillaan näiden epävarmuuksien ja riskien realisoituminen voi aiheuttaa kuluttajille huomattavaa epäluottamusta koko nykyistä rahoitusjärjestelmää kohtaan.

9.2 Lohkoketjuteknologian käyttöönotto yhteiskunnan ja talouden prosesseihin

Tällä hetkellä lohkoketjuteknologialle ei vielä nähdä selkeää käyttötarvetta perinteisemmissä talouden ja yhteiskunnan prosesseissa, mutta se näyttää narratiivinsa ansiosta toimineen tietynlaisena katalyyttina arkisemmalle digitaalisten järjestelmien väliselle integraatiokehitykselle. Nykyisen sääntelyprosessin hitaus suhteessa nopeisiin teknologisiin kehitysharppauksiin lienee kuitenkin hyvä syy olla vielä ajamatta lohkoketjuteknologiaa liian impulsiivisesti yhteiskunnalliseen infrastruktuuriin. On tärkeää varmistua, että sekä kansallinen että kansainvälinen sääntely ja lainsäädäntö ovat riittävän ajantasaisia ennen massiivia teknologisia muutoksia yhteiskunnan rakenteisiin. Ketterämpinä toimijoina yksityisen sektorin toimijoiden on hyödyllistä tutkia ja kehittää erilaisia lohkoketjuteknologian variaatioita ennen niiden laajempimittaista yhteiskunnallista käyttöönottoa. Ajankohtaisena esimerkkinä turhan impulsiivisesta etenemisestä yhteiskunnallisen infrastruktuurin kannalta merkittäviin ja perinteisempiin prosesseihin voidaan pitää El Salvadorin päätöstä ottaa maailman ensimmäisenä valtiona kryptovaluutta Bitcoin viralliseksi maksuvälineeksi syyskuussa 2021. El Salvadorin hallitus ei kuitenkaan ole

kyennyt tämän opinnäytetyön kirjoitushetkeen, helmikuuhun 2022 mennessä, luomaan teknisiä puitteita, joissa bitcoinit todellisuudessa toimisivat maksuvälineinä. Tämä johtuu sekä valtion tarjoaman kryptovaluuttalompakon teknisestä puutteellisuudesta että Bitcoin-lohkoketjun suorituskyvyn rajallisuudesta, jonka vuoksi se ei sovellu lyhyellä aikavälillä tapahtuvien valtavien transaktiomäärien käsittelyyn, mitä se virallisena valtiotasoisena maksuvälineenä edellyttäisi. Vaikka tämänkaltaiset kokeilut kuormittavat ensisijaisesti yhteiskunnan asukkaita ja rakenteita, näkyvät vaikutukset väistämättä suoraan ja välillisesti myös pankkisektorilla.

9.3 Lohkoketjuteknologia pankkisektorin riskien aiheuttajana ja mitigoijana

Kryptovaluutat yhtenä lohkoketjuteknologian sovellutuksena ja samalla uutena valuuttamuotona aiheuttavat merkittävästi päänvaivaa pankkisektorilla. Capgemini Research Institute arvioi syyskuussa 2021, että lähes 45% maailman kuluttajista käyttää kryptovaluuttaa maksuvälineenä vuoteen 2023 mennessä. Tämänhetkiset kyvykkyydet kryptovaluuttatransaktioiden seurantaan ovat osin puutteellisia sekä osaajien puutteesta että kryptovaluuttojen teknisistä ominaisuuksista johtuen. Lohkoketjuteknologia itsessään tarjoaa kuitenkin myös mielenkiintoisia mahdollisuuksia yleisemmin pankkisektorin toimijoiden sääntelyn mukaiseen pakoteseurannan toteuttamiseen, asiakkaan tuntemisen prosessien kehittämiseen ja väärinkäytösten, terrorismin rahoittamisen sekä rahanpesun estämiseen.

Lohkoketjuteknologia mahdollistaa muun muassa nollatietosopimusten hyödyntämisen, mitä rahanpesun ja terrorismin rahoittamisen estämisen näkökulmasta nollatietotodistuksia (Zero Proof of Knowledge) voidaan pitää äärimmäisen mielenkiintoisena. Teoriassa esimerkiksi eri viranomaistahojen ja/tai pankkien välinen yhteinen yksityinen lohkoketju mahdollistaisi nollatietotodistukset esimerkiksi eri pankkien välisistä transaktioista sellaisissa tapauksissa, joissa on havaittavissa rahanpesuun tai terrorismin rahoittamiseen, väärinkäytöksiin tai muihin laittomiin toimiin viittaavia tekijöitä. Nollatietotodistukset mahdollistaisivat esimerkiksi epäilyttävässä rahaliikenteessä pikaisen varmistuksen transaktioon liittyvien varojen alkuperästä ja käyttötarkoituksesta ilman asiakkaan yksityisyyden vaarantumista. Samalla varmistukseen liittyvä prosessi olisi jo itsessään melko

pitkälle automatisoitu, eikä näin edellyttäisi merkittäviä henkilöstöresursseja kyseessä olevan varmistuksen käsittelemiseksi. Esimerkki tällaisesta nollatietotodistuksen hyödyntämisestä voisi olla tilanne, jossa pankkiin äskettäin tuntemattomasta alkuperästä talletettuja käteisvaroja siirretään heti talletuksen jälkeen toisen pankin tilille. Nollatietotodistuksella voitaisiin varmistaa, onko siirretyt varat esimerkiksi nostettu toisen pankin tililtä uudelleen käteiseksi heti tilisiirron jälkeen. Tässä tapauksessa vastausvaihtoehto ”Kyllä” saattaisi indikoida rahanpesuun viittaavasta toiminnasta.

Toinen esimerkki rahanpesun ja terrorismin rahoittamisen estämiseen sekä muiden väärinkäytösten estämiseen soveltuvasta lohkoketjuteknologian sovellutuksesta ovat älysopimukset. Esimerkiksi huijauksissa ja väärinkäytöksissä sekä rahanpesussa usein ilmenevien niin kutsuttujen muulitilien käyttöä voitaisiin nykyistä tehokkaammin kontrolloida älysopimuksilla, kun esimerkiksi älysopimukseen kirjatut transaktioiden vastatilit voitaisiin etukäteen todentaa kuuluvaksi juuri tarkoitetulle taholle. Jos esimerkiksi älysopimukseen on ohjelmoitu komento, missä henkilö A siirtää varoja sijoitustarkoituksessa taholle B, voidaan taho B älysopimuksen puitteissa määritellä siirtämään kyseiset varat esimerkiksi ainoastaan tiettyihin, määrättyihin sijoitustuotteisiin. Jos varat pyrittäisiin siirtämään tahon B tililtä eteenpäin ennalta määrittelemättömälle tilille, sopimuksen ehdot eivät toteutuisi ja suoritettu transaktio palautuisi automaattisesti henkilön A tilille täysimääräisenä. Vaihtoehtoisesti älysopimukseen voitaisiin esimerkiksi ohjelmoida ehto, jonka mukaisesti henkilöltä A siirrettyjä varoja taholle B ei voida nostaa tai siirtää tililtä lainkaan ennen tiettyjen varmennustoimenpiteiden toteutumista. Yllä mainitusti kaikki transaktiot kirjautuvat automaattisesti lohkoketjuun ja ovat jälkikäteen muuttamattomia, mikä mahdollistaisi osaltaan väärinkäytösten havaitsemisessa, tutkimisessa sekä mahdollisissa jatkotoimenpiteiden toteuttamisessa.

Edellä mainitulla logiikalla esimerkiksi edunvalvonnan alaisia tai alaikäisiä henkilöitä voitaisiin nykyistä tehokkaammin suojella väärinkäytöksiltä sekä kontrolloida tarvittaessa heidän rahaliikennettään älysopimusten avulla. Samaa ideaa voitaisiin soveltaa myös esimerkiksi haastavissa perinnönjakotilanteissa määrittämällä tarkasti esimerkiksi omaisuuden myyntiä seuraavat transaktiot jo ennalta käsin.

Edellä mainituista esimerkeistä johdettuna voidaankin pohtia, voisiko pankkien välille luoda oman suljetun hajautetun tilikirjan, jonka sisällä jaettaisiin avoimesti määrättyjen sääntöjen puitteissa rahanpesun- ja terrorismin rahoittamisen tai väärinkäytösten estämisen työtä tukevaa tietoa? Hyötyjä tässä olisivat tehokkaan reaaliaikaisen tiedonjaon lisäksi dataa hallinnoivan kolmannen osapuolen tarpeettomuus, mutta vastaavasti epävarmuuksia voivat aiheuttaa mm. GDPR-näkökulma ja tietojen turvallisuus sekä niihin liittyvät vastuukysymykset.

9.4 Keskeneräinen, mutta kiinnostava tulevaisuuden teknologia

Osa pitää lohkoketjuteknologiaa jopa internetin vertaisena disruptiivisena muutoksena, jonka vaikutukset tulevat heijastumaan globaalisti lähes kaikkiin nykyisiin järjestelmiin ja sitä kautta ihmisten arkeen. Henkilökohtaisesti suhtaudun teknologiaan vielä toistaiseksi varauksella, vaikkakin suurella mielenkiinnolla. Mielestäni lohkoketjuteknologiaan liittyvän trendimäisyyden takana on äärimmäisen oivaltava teknologia, jonka mahdollisuudet tulevat varmasti näkymään pankkisektorilla vielä nykyistäkin enemmän. Teknologia on mielestäni toistaiseksi verrattain epäkypsää ja kehitysvaiheessa olevaa liian aggressiiviselle käyttöönotolle. Esimerkkeinä tästä voidaan pitää esimerkiksi lukuisia DeFi-hakkerointeja ja muita lohkoketjuihin kohdistuneita väärinkäytöksiä, jotka toistaiseksi osoittavat, ettei tietoa tai varallisuutta voida täysin turvallisesti sitoa lohkoketjuun. Kun riittävä turvallisuuden ja vakauden taso todennäköisesti jossain vaiheessa saavutetaan, on myös pankkisektorin hyvä olla ensimmäisten joukossa ottamassa käyttöön lohkoketjuteknologiaa oman suorituskykynsä ja palvelutarjontansa varmistamiseksi kansainvälistyvässä ja jatkuvasti kovenevassa kilpailussa. Kuten tässä opinnäytetyössä on aiemmin sanottu, kaikissa lohkoketjuteknologian käyttöönottoon liittyvissä lähestymistavoissa on riskejä. Pitkällä aikavälillä tulee kuitenkin melkoisella varmuudella olemaan vähemmän riskistä ohjata tutkimus- ja kehitysresursseja lohkoketjuteknologian hyödyntämiseen eri tavoin, kuin jäädä seuraamaan tämän teknologian kehityskaarta kokonaan sivusta.

10 Yhteenveto

Tämän opinnäytetyön tutkimuskysymyksiä olivat:

- Miten lohkoketjuteknologia toimii?
- Mitä vaikutuksia lohkoketjuteknologialla on pankkisektorille?
- Mitä hyötyjä lohkoketjuteknologialla voidaan saavuttaa pankkisektorilla?
- Mitä riskejä lohkoketjuteknologian hyödyntämiseen pankkisektorilla liittyy?

Tutkimuskysymyksiin vastaaminen onnistui mielestäni erittäin hyvin ja kattavasti. Lohkoketjuteknologia on teknisesti melko laajamittainen kokonaisuus ja tästä johtuen lohkoketjuteknologian toiminnan selittäminen sekä sen eri sovellutukset vaativat perusteellista läpikäyntiä, ennen kuin opinnäytetyössä voitiin siirtyä käsittelemään teknologian vaikutuksia pankkisektorille. Kaikkia tutkimuskysymyksiä käsitellään tässä opinnäytetyössä objektiivisesti useista eri näkökulmista, ja mielestäni teknologiaan sekä käytettyihin lähteisiin suhtaudutaan koko opinnäytetyön ajan riittävällä kriittisyydellä.

Tämän opinnäytetyön kautta olen oppinut lohkoketjuteknologiaan liittyvien teknisten kyvykkyyksien lisäksi erittäin paljon sen monitahoisista vaikutuksista yhteiskunnallisesti, yritystasolla sekä kuluttajatasolla. Tämä opinnäytetyöprosessi on opettanut suhtautumaan myös vertaisarvioituihin lähteisiin siinä mielessä kriittisesti, että vertaisarvioiduissa lähteissä ei kaikissa tapauksissa erikseen korostettu tutkimustulosten maantieteellistä vaikutusta tai hyödynnetty lähteinä uusimpia vertaisarvioituja lähteitä, vaan myös vanhempia lähteitä, joiden sisältö saattoi olla jo osin teknologisesti vanhentunutta.

Tämä opinnäytetyö tullaan julkaisemaan Theseuksessa ja tätä opinnäytetyötä voivat tulevaisuudessa hyödyntää erityisesti pankkisektorin toimijat, mutta myös yleisemmin yritykset sekä kuluttajat, jotka ovat kiinnostuneet lohkoketjuteknologian vaikutuksista pankkisektorilla.

Lähteet

Arner, D., Auer, R., & Frost, J. (2020). *Stablecoins: risks, potential and regulation*. www.bis.org

Auer, R., & Böhme, R. (2021). *BIS Working Papers No 948 Central bank digital currency: the quest for minimally invasive technology*. www.bis.org

Beattie, A. (2021, December 13). *The Role of Commercial Banks in the Economy*. https://www.investopedia.com/articles/investing/062513/role-commercial-banks-economy.asp

Binance. (2018). *Sybil Attacks Explained*. https://academy.binance.com/en/articles/sybil-attacks-explained

Binance. (2019). *What Is a Crypto Wallet?* https://academy.binance.com/en/articles/crypto-wallet-types-explained

Binance. (2020). *Selfish Mining Explained*. https://academy.binance.com/en/articles/selfish-mining-explained

Binance. (2021). *Central Bank Digital Currencies (CBDC) Explained*. https://academy.binance.com/en/articles/central-bank-digital-currencies-cbdc-explained

Bitcoinkeskus.com. (2020). *Erilaiset konsensusalgoritmit esittelyssä*. https://bitcoinkeskus.com/erilaiset-konsensusalgoritmit-esittelyssa/

Brus, & Rus. (2021). *Building the AI bank of the future*.

Business Insider. (2022, January 20). *Ethereum may not have too long to get its high gas fee issue in check, according to JPMorgan | Business Insider India*. https://www.businessinsider.in/cryptocurrency/news/ethereum-may-not-have-too-long-to-get-its-high-gas-fee-issue-in-check-according-to-jpmorgan/articleshow/89021370.cms

Chandler, S. (2019). *What Is the Difference Between Blockchain and DLT?* https://cointelegraph.com/news/what-is-the-difference-between-blockchain-and-dlt

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, *158*. https://doi.org/10.1016/j.techfore.2020.120166

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

CipherTrace. (2021). *Cryptocurrency Crime and Anti-Money Laundering Report*.

Coelho, R., Fishman, J., & Ocampo, D. G. (2021). *Supervising cryptoassets for anti-money laundering*. https://www.bis.org/fsi/publ/insights31.pdf

Davies, A. (n.d.). *How to Use Blockchain to Prevent Money Laundering*. Retrieved January 13, 2022, from https://www.devteam.space/blog/how-to-use-blockchain-to-prevent-money-laundering/

Digiconomist. (n.d.). *Bitcoin Energy Consumption Index*. Retrieved October 17, 2021, from https://digiconomist.net/bitcoin-energy-consumption/

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law and Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

FATF. (2019). *Financial Action Task Force 30 Years*. www.fatf-gafi.org

FATF. (2020). *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*. www.fatf-gafi.org

Feyen, E., Frost, J., Gambacorta, L., Natarajan, H., & Saal, M. (2021). *Fintech and the digital transformation of financial services implications for market structure and public policy*. https://www.bis.org/publ/bppdf/bispap117.htm

FSB. (2019). *Decentralised financial technologies: Report on financial stability, regulatory and governance implications*. https://www.fsb.org/wp-content/uploads/P060619.pdf

Garg, P., Gupta, B., Chauhan, A. K., Sivarajah, U., Gupta, S., & Modgil, S. (2021). Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological Forecasting and Social Change*, *163*. https://doi.org/10.1016/j.techfore.2020.120407

Gomathi, S., Soni, M., Dhiman, G., Govindaraj, R., & Kumar, P. (2021). A survey on applications and security issues of blockchain technology in business sectors. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.02.088

Hall, M. (2021, June 23). *How the Banking Sector Impacts Our Economy*. https://www.investopedia.com/ask/answers/032315/what-banking-sector.asp#toc-the-bottom-line

Hargrave, M. (2020, October 23). *Investment Bank Definition*. https://www.investopedia.com/terms/i/investmentbank.asp

Harju, N. (2020). *Blockchain | Mikä on lohkoketju? – Lohkoketjun anatomiaa*. https://www.cgi.com/fi/fi/blogi/mika-on-lohkoketju

Honkanen, P. (2017). *Impulsseja Lokakuu 2017*. www.sorsafoundation.fi

IBM. (n.d.). *What is Blockchain Technology?* Retrieved October 9, 2021, from https://www.ibm.com/topics/what-is-blockchain

International Monetary Fund. (n.d.). *Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)*. Retrieved November 7, 2021, from https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

Isoaho, E., & Kaski, I.-E. (2021). *Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021*. http://urn.fi/URN:ISBN:978-952-367-715-9

Johansson, P. E., Eerola, M., Innanen, A., & Viitala, J. (2019). *Lohkoketju - Tiekartta päättäjille*. Alma Talent Oy.

Kaplan, E. (2021, May 25). *Cryptocurrency goes green: Could "proof of stake" offer a solution to energy concerns?* https://www.nbcnews.com/tech/tech-news/cryptocurrency-goes-green-proof-stake-offer-solution-energy-concerns-rcna1030

Kenton, W. (2021, June 29). *Financial Sector Definition*. https://www.investopedia.com/terms/f/financial_sector.asp

Kinnunen, T. K., Leviäkangas, P., Kostiainen, J., Nykänen, L., VTT Oy, Rouhiainen, K., Finlow-Bates, K., & Chainfrog Oy. (2017). *Lohkoketjuteknologian soveltaminen ja vaikutukset liikenteessä ja viestinnässä*. http://urn.fi/URN:ISBN:978-952-243-528-6

Laikari, A., Backman, J., Helaakoski, H., & Suomalainen, T. (2018). *European blockchain analysis*.

Liang, Y. C. (2020). Blockchain for dynamic spectrum management. In *Signals and Communication Technology* (pp. 121–146). Springer. https://doi.org/10.1007/978-981-15-0776-2_5

Lorne, L., & Cawrey, D. (2020). *Mastering Blockchain*. O'Reilly Media, Inc.

Malhotra, A., O'Neill, H., & Stowell, P. (2021). THINKING STRATEGICALLY ABOUT BLOCKCHAIN ADOPTION RISKS and RISK MITIGATION. *Business Horizons*. https://doi.org/10.1016/j.bushor.2021.02.033

Mattila, J., Seppälä, T., Hukkinen, T., Laikari, A., Markkanen, K., Koulu, R., & Jia, K. (2019). *Lohkoketjuteknologian hyödyntämismahdollisuudet palkkatulojen verotuksessa*.

Murray, A., Kuban, S., Josefy, M., & Anderson, J. (2019). Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance. *Academy of Management Perspectives*. https://doi.org/10.5465/amp.2018.0066

Natarajan, H., Krause, S., & Gradstein, H. (2017). *Distributed Ledger Technology (DLT) and Blockchain Acknowledgments III*. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/177911513714062215/distributed-ledger-technology-dlt-and-blockchain

R3. (n.d.). *Blockchain 101 - Blockchain Technology & DLT Explained*. Retrieved October 10, 2021, from https://www.r3.com/blockchain-101/

Rahanpesu.fi. (n.d.). *Lainsäädäntö - Rahanpesun ja terrorismin rahoittamisen estäminen*. Retrieved November 7, 2021, from https://rahanpesu.fi/lainsaadanto

Rangwala, A. (2017). *Do insurers need to pay attention to ICOs?* https://insuranceblog.accenture.com/do-insurers-need-to-pay-attention-to-icos

Segal, T. (2020, September 29). *Central Bank Definition*. https://www.investopedia.com/terms/c/centralbank.asp

Sharma, R. (2022, January 13). *Decentralized Finance (DeFi) Definition*. https://www.investopedia.com/decentralized-finance-defi-5113835

Steinmetz, F., von Meduna, M., Ante, L., & Fiedler, I. (2021). Ownership, uses and perceptions of cryptocurrency: Results from a population survey. *Technological Forecasting and Social Change*, *173*. https://doi.org/10.1016/j.techfore.2021.121073

Velissarios, J. (2021a). *CBDC for Commercial Banks - What you need to know, Part 2*. https://www.accenture.com/us-en/blogs/blockchain-mps/cbdc-for-commercial-banks-part-2-how-to-prepare

Velissarios, J. (2021b). *CBDC for Commercial Banks: What you Need to Know*. https://www.accenture.com/us-en/blogs/blockchain-mps/cbdc-for-commercial-banks-what-you-need-to-know

Wang, H., Ma, S., Dai, H. N., Imran, M., & Wang, T. (2020). Blockchain-based data privacy management with Nudge theory in open banking. *Future Generation Computer Systems*, *110*, 812–823. https://doi.org/10.1016/j.future.2019.09.010

Liite 1: Aineistonhallintasuunnitelma

Tämä opinnäytetyö on tutkimuksellinen opinnäytetyö ja kaikki opinnäytetyössä käytetyt aineistot ovat peräisin julkisista lähteistä. Tässä opinnäytetyössä ei ole käytetty kolmansien osapuolten aineistoja eikä tällä opinnäytetyöllä ole toimeksiantajaa.