Anton Osenius

LOHKOKETJUTEKNOLOGIAN SÄÄNTELY EUROOPAN UNIONISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Osenius, Anton
Lohkoketjuteknologian sääntely Euroopan Unionissa
Jyväskylä: Jyväskylän yliopisto, 2022, 37 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Pentti Marttiin

Tämän tutkielman tarkoitus on antaa yleiskuva lohkoketjuteknologian toiminnasta ja termistöstä sekä kartoittaa EU:n suunnitelmia sääntelyyn ja kehitykseen. Kappaleessa kolme sivutaan myös Suomen tilannetta lohkoketjuteknologian käyttöönottajana osana EU:n strategiaa. Tutkielma toteutettiin kuvailevana kirjallisuuskatsauksena. Lohkoketjuteknologian kehitys asettaa painetta lainsäätäjille, joiden tehtävänä on ehkäistä riskit mahdollisuuksia tukahduttamatta. Jokainen maa haluaa näyttää sääntelyn valossa houkuttelevalta kohteelta suuryrityksille, mikä aiheuttaa lainsäädännöllistä kilpailua unionin maiden välille. EU:n lukuisten eri teknologiastrategioiden keskiössä onkin yhteisen harkitun linjan löytäminen. Unionin tasolla tunnistetaan lohkoketjun tuomat mahdollisuudet ja lainsäädäntöä pyritään kehittämään suuntaan, joka tukee kehitystä muun muassa minimoimalla verotusta koskevaa byrokratiaa. Suomi on sääntely-kehityksessä verrattain jäljessä, eikä suurta kasvua voida lohkoketjusektorilla ilman uudistuksia odottaa. Saksa sen sijaan on toiminut lainsäädännön suhteen edelläkävijänä säätäen lakeja jo ennen EU:n mukaantuloa. Saksan malli perustuu kevyeen kasvua edistävään verotukseen, joka tukee kryptovaluutta-transaktioiden yleistymistä ja laajaa käyttöönottoa. Euroopan Unionin strategiaan kuuluu tiivis yhteistyö maidenvälisen lohkoketjuverkon toteuttamiseksi. EU säätää myös aktiivisesti lakeja rikollisen toiminnan poiskitkemiseksi ja teknologian käyttäjien turvaamiseksi. Lakien määräämä henkilötietojen kerääminen aiheuttaa ristiriitaa lohkoketjuteknologian pohjimmaisen ajatuksen kanssa, jossa käyttäjät tulisi voida siirtää valuuttaa irrallaan sääntelystä ja keskitetyistä toimijoista. Lohkoketjuteknologian ja kryptovaluuttojen mahdollisuudet ovat mittavat sääntelystä huolimatta. Nousevaa teknologiaa tullaan hyödyntämään esimerkiksi esineiden Internetin rakentamiseen, hajautettuun varainsiirtoon sekä pilvi- ja tietokantapalvelujen tietoturvan parantamiseen.

Asiasanat: lohkoketju, älysopimus, kryptografia, louhinta, kryptovaluutta, lainsäädäntö, verotus, Euroopan unioni

ABSTRACT

Osenius, Anton
Blockchain technology in EU-legistlation
Jyväskylä: University of Jyväskylä, 2022, 37 pp.
Information systems science, bachelor's thesis
Supervisor(s): Pentti Marttiin

The goal of this study is to provide an overview of the operation and terminology of blockchain technology as well as map out the plans of the European Union regarding blockchain legislation and development. There is also a brief chapter on Finland as a part of EU's strategy. This study was done as a literature review. The evolution of blockchain technology builds pressure on legislators, who's responsibility it is to ensure safety without restricting growth. Every country wants to be seen as an attractive ground for investments which generates competition inside the union. Consequently, one of the main objectives in the EU's strategy is to unify the members and work together. The possibilities brought about by blockchain technology are recognized on all levels of the union and the subsequent legislation is being prepared in a way that supports growth. This could for example be done by minimizing bureaucracy caused by complicated taxation. Finland is slightly behind in what comes to developing blockchain technology and no major growth can be expected without legislative reform. Germany on the other hand has become a legislative forerunner – acting even before the union stepped in. Germany's legislation model is based on light taxation. This is expected to accelerate growth and widespread adoption of the technology. The European Union's blockchain strategy contains plans of close co-operation in hopes of building a union wide network. The EU is also doing its best to ensure its citizen's safety by combating criminality by means of active legislation. The collection of sensitive information allowed by these anti-criminality actions generates conflict with the foundations of blockchain technology: being able to transfer funds clear of third-party regulation and centralization. Regardless, the potential upside of the blockchain is massive. This emerging technology will be utilized in decentralized fund transfers, expanding the Internet of things and making cloud-based data storage safer.

Keywords: blockchain, smart contract, cryptography, mining, cryptocurrency, legislation, taxation, The European Union

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Lohkoketjuteknologia kehitettiin alun perin luotettavien varainsiirtotransaktioiden mahdollistamiseksi verkossa, jossa osapuolet eivät luota toisiinsa. Perinteisesti luottamus luodaan keskitetyn välikäden, kuten pankin avulla. Lohkoketju kuitenkin rikkoo perinteisen varainsiirtomallien rajoja poistamalla tarpeen kolmannelle osapuolelle. Peitenimeä Satoshi Nakamoto käyttävä henkilö tai ryhmä esitteli vuonna 2008 projektin, jossa käyttäjät pystyisivät siirtämään valuuttaa vertaisverkossa itsenäisesti ilman huolta väärinkäytöksistä. Nakamoto (2008) kuvailee, kirjoituksessa luomastaan vertaisverkosta, luottamuksen syntyvän välikäden sijaan aikaleimattujen, laskentateholla vahvistettujen lohkojen ketjun avulla. Kyseinen lohkoketju tunnetaan nimellä Bitcoin, ja alkuvuodesta 2022 verkossa suoritettiin päivittäin jo noin 250 tuhatta transaktiota (Statista.com, 2022).

Uuden mullistavan teknologian kehittäminen suurten ihmismassojen käyttöön sisältää kuitenkin paljon riskejä. Ano- ja pseudonyymiset varainsiirrot mahdollistavat verkot luovat puitteet korkealle yksityisyydelle, mutta myös rikollisuudelle. Väärinkäytösten minimoimiseksi tarvitaan rohkeaa ja asiantuntevaa lainsäädäntöä. Euroopan unionilla on vastuu kansalaistensa turvallisuuden lisäksi kasvavien teknologioiden tukemisesta digitalisaation ja talouden kehittymiseksi. Tarvitaan siis strategia, jolla Eurooppa pysyy kehityksen kärjessä. Tällaisen strategian keskiössä tulee epäilemättä olemaan lainsäädäntö.

Bitcoin on kuitenkin vasta alkua lohkoketjuteknologian aikajanalla ja uusia projekteja ja käyttösovelluksia syntyy jatkuvasti. Kulunut viittaus lohkoketjuteknologian roolista suurimpana innovaationa sitten Internetin ei siis ole kaukaa haettu. Teknologia mahdollistaa muun muassa tiedon tallentamisen ja varainsiirron nykyisiä toimintamalleja ja rakenteita järisyttävällä tavalla. Lohkoketjuteknologialla on merkittävä rooli World Wide Web:in siirtymisessä sen kolmanteen sukupolveen. Myös Web 3.0:ksi kutsuttu murros tarkoittaa erään määritelmän mukaan siirtymistä hajautetumpiin toimintatapoihin (Alabdulwahhab, 2018). Nykyinen Web 2.0 sisältää lukuisia ongelmia ja heikkouksia, joita verkon käyttäjät ovat tottuneet sietämään. Nykyisellään Internetin tieto ja ylläpito on erittäin keskittynyttä ja pienellä määrällä suuryrityksistä on paljon valtaa (Alabdulwahhab, 2018). World Wide Web:in kehittäjä Tim Berners-Lee (2018) sanoi vuoden 2016 puheessaan toivovansa hajautuksen palauttamista ja WWW-järjestelmän palauttamista juurilleen, jossa jokaisella käyttäjällä on mahdollisuus omistaa oma datansa ja ylläpitää palvelinta. Keskitetty toiminta asettaa riskejä kuluttajan tietoturvalle, tiedon suvereniteetille ja joissain maissa jopa altistaa laajalle sensuurille. Lohkoketjuteknologia on vain osa World Wide Webin murrosta, mutta sen vahvuudet sopivat hyvin yhteen nykyisen mallin heikkouksien kanssa.

Lohkoketjuteknologia voidaan siis nähdä työkaluna keskitetyn vallan siirtämiseksi kansalle. Useimmat lohkoketjuverkot eivät kuitenkaan ole anonyymejä, vaan kaikki tiedot ovat julkisia ja vapaasti seurattavissa ja

yhdistettävissä käyttäjiin. Terrorismin rahoituksen, rahanpesun ja veronkierron estämiseksi tehdään EU-tasolla toimenpiteitä käyttäjien henkilöllisyyksien liittämiseksi pseudonyymisiin osoitteisiin verkossa. Muun muassa tästä syystä lainsäädännölliset toimenpiteet näyttelevät merkittävää roolia teknologian ja kryptovaluuttojen tulevaisuudessa.

Toteutettu kirjallisuuskatsaus on luonteeltaan kuvaileva ja työtä voi luonnehtia melko vapaamuotoiseksi yleiskatsaukseksi lohkoketjuteknologiaan näkökulman tuomien rajausten piirissä. Katsaukseen on pyritty sisällyttämään mahdollisimman paljon teknistä näkökulmaa esiintuovaa kirjallisuutta, sekä julkisin varoin tuotettuja lainsäädäntölähteitä. Kirjallisuuden valintaan vaikutti merkittävästi julkaisuajankohta, sillä varsinkin lainsäädäntöä koskevat tiedot muuttuvat jatkuvasti. Lähdevalintoihin vaikuttivat myös viittausmäärät, sekä vertaisarviot. Numeerista statistiikkaa sisältävät lähteet valittiin riippumattomilta sivuilta ja niitä verrattiin muiden lähteiden ilmoittamiin lukuihin. Suuri osa lohkoketjuteknologiaa koskevasta kirjallisuudesta haettiin IEEE Xplore, Jykdok, ScienceDirect, sekä Google Scholar tietokannoista. Muutamia poikkeuksia lukuun ottamatta teknologiaa kuvaavat lähteet ovat englanninkielisiä. Vieraskielisten teosten sisältämä termistö on pyritty kääntämään asiantuntijoiksi tunnistettujen suomalaisten kirjoittamien lähteiden sanavalintoja mukaillen. Lainsäädäntöä koskevat tiedot on valittu suureksi osin Euroopan Unionin ja komission virallisilta sivustoilta, tai kyseessä olevan EU-maan hallinnon virallisesta dokumentaatiosta.

Valtaosa kirjallisuudesta löytyi hyödyntämällä hakusanoja ”lohkoketju”, sekä ”Euroopan unioni”. Lohkoketjuteknologiaa pääpiirteittäin kuvailevien tieteellisten julkaisujen lähdeluetteloita seuraamalla päästiin syvemmälle kunkin kappaleen vaatimaa tarkempaan kirjallisuuteen. Avainteknologioita kuvaileviin kappaleisiin on lisäksi pyritty valitsemaan osa-alueen tunnetumpien ja arvostetuimpien tutkijoiden kirjallisuutta. Käytettyjen lähteiden valinnassa on otettu huomioon kirjoittajan asema ja mahdollinen suora taloudellinen hyötyminen lohkoketjusektorin kasvusta. Tästä syystä varsinkin yksittäisiä nousevia lohkoketjuprojekteja käsitteleviä yksityisesti rahoitettuja teoksia ei tiedon kyseenalaisen luotettavuuden vuoksi valittu.

Tutkielma on jaettu viiteen osaan alkaen motivoinnilla ja johdattelulla tulevaan aiheeseen. Kappaleiden kaksi ja kolme on tarkoitus avata taustaa lohkoketjuteknologian toimintaperiaatteisiin ja mahdollisuuksiin ennen seuraavaa EU-näkökulman sisältävää pääosiota. Viimeisessä kappaleessa tiivistetään tutkimuksen loppupäätelmät ja mahdolliset jatkotutkimuskohteet.

Tämä tutkielma pyrkii vastaamaan seuraavaan kysymykseen:

- Mitkä ovat Euroopan unionin aikeet lohkoketjuteknologian kehityksen ja sääntelyn suhteen?

2 LOHKOKETJU

Tämän kappaleen tarkoituksena on selittää lohkoketjun määritelmä ja avata tärkeimpien aiheeseen liittyvien termien merkityksiä. Kappaleessa 2.1 määritellään lohko, ketju sekä niiden yhdessä muodostama kokonaisuus. Seuraavassa kappaleissa 2.2 tuodaan esiin erityyppisiä tapoja toteuttaa lohkoketjuverkko käyttäjäkunnasta riippuen. Lohkoketjutyyppien erityispiirteet vaikuttavat merkittävästi verkon rakenteeseen ja ratkaisujen erot tuodaan tässä osiossa esiin. Viimeisessä kappaleessa paneudutaan lohkoketjuteknologian tuomiin mahdollisuuksiin, sekä vahvuuksiin nykyisin laajassa käytössä oleviin ratkaisuihin.

2.1 Määritelmä

D. Yaga ym. määritelmän mukaan lohkoketjut (blockchain) ovat hajautettuja tilikirjoja, joiden avulla voidaan muun muassa ylläpitää tietoturvallista tietokantaa (Yaga, Mell, Roby & Scarfone, 2018). Ketjun sisältämä tieto on pakattu suureen määrään toisiinsa sidottuja lohkoja. Jokainen lohko vahvistetaan ennen sen liittämistä osaksi ketjua, eikä sen muokkaaminen jälkikäteen ole käytännössä mahdollista. Yhteistä lohkoketjua ylläpitävät laitteet muodostavat yhdessä kokonaisuuden, jota kutsutaan lohkoketjuverkoksi. Tällaisen verkon toiminta on hajautettu käyttäjien vastuulle, jolloin mikään yksittäinen taho ei kykene hallitsemaan sen toimintaa tai väärentämään tietoja. Lohko koostuu ylätunnisteesta ja varastoitavasta tiedosta. Ylätunniste sisältää metadataa lohkon sisällöstä. Näihin tietoihin kuuluu muun muassa: lohkon järjestysluku ketjussa, aikaleima, lohkon koko, edellisen lohkon ylätunnisteen tiivistearvo sekä lohkon tietoa vastaava uniikki tiiviste. Lisäksi laskentatehoon perustuvaa vahvistusprosessia hyödyntävien lohkoketjujen lohkoissa on nonce-arvo, jota käytetään tiivistelaskennan apuna. Lohkon sisältämä varsinainen tieto voi olla esimerkiksi lista suoritetuista kryptovaluuttatransaktioista. (Yaga ym., 2018)

Ennen kuin lohko voidaan liittää osaksi lohkoketjua, täytyy sen sisältämät transaktiot varmistaa aidoiksi. Tämä tapahtuu tarkistamalla, että listattujen

transaktioiden molemmilla osapuolilla on hallussaan varoja vastaavat yksityiset avaimet. Mikäli tiedot täsmäävät voi lohkon vahvistusprosessi alkaa. Kun uusi lohko on vahvistettu käyttämällä jotakin ennalta määritettyä konsensusmallia, voidaan sen sisään liittää lista aiemmin vahvistettuja transaktioita. Uuden lohkon lisäämisen jälkeen lähetetään kaikille verkon täyssolmuille ketjun uusi versio. (Yaga ym., 2018)

2.2 Lohkoketjutyypit

Lohkoketjut voidaan jakaa avoimiin ja suljettuihin lohkoketjuihin. Rajanveto perustuu siihen, onko pääsy verkon käyttäjäksi avointa vai rajoitettua. Avoimissa lohkoketjuissa (Permissionless blockchain), kuten Bitcoinissa, kuka tahansa voi tarkastella lohkojen tietoja ja suorittaa transaktioita ilman rajoitteita (Swathi, 2021). Tällaisessa vertaisverkossa käyttäjät eivät tunne toisiaan ja väärinkäyttöyritysten todennäköisyys on korkea. Juuri tällaisia lähtökohtia varten lohkoketjuteknologia alun perin kehitettiin. Konsensusmallien ja läpinäkyvyyden ansiosta ympäri maailmaa levittäytynyt käyttäjäkunta voi turvallisesti ja luotettavasti kommunikoida, tallentaa tietoa ja siirtää varallisuutta (Kryptovaluutta.fi, 2021). Julkiset lohkoketjuverkot ovat täysin irrallaan paikallisista rajoitteista ja pankeista ja ne mahdollistavat maailmanlaajuisen kaupankäynnin myös kehitysmaissa ja diktatuureissa. Transaktiot ovat avoimessa lohkoketjuverkossa julkisia. Avoin lohkoketju tarvitsee toimiakseen aina kryptovaluutan. Valuutta toimii automatisoituna palkkiomenetelmänä louhijoille, jotka käyttävät omia laitteitaan lohkoketjun liikenteen suorittamiseen ja lohkojen vahvistamiseen (Alasaarela, 2018).

Suljetussa lohkoketjuverkossa (Permissioned blockchain) ei ole tarvetta resursseja kuluttaville konsensusmalleille, sillä verkkoon liittyminen vaatii usein keskitetyn ylläpitäjän luvan (Swathi, 2021). Tällaisessa verkossa käyttäjät tuntevat toisensa ja sen käyttö on yleensä suunnattu johonkin tiettyyn liiketoiminnalliseen tavoitteeseen. Transaktiot suljetussa lohkoketjuverkossa ovat salattuja ja niiden tarkastelu vaativat luvan (Kryptovaluutta.fi, 2021). Suljetussa lohkoketjussa ei myöskään ole yleensä tarvetta kryptovaluutalle, sillä verkon ylläpidosta muodostuvista kuluista sovitaan yksityisesti esimerkiksi yrityksen sisällä (Alasaarela, 2018).

2.3 Lohkoketjuteknologian vahvuuksia

Lohkoketjuteknologia käsittää lohkoketjuverkon ylläpitoon vaadittavat laitteet sekä ohjelmiston, jolla saavutetaan verkon konsensus ja määritellään toimintaperiaatteet. Teknologian suurimpia vahvuuksia on sen hajautettu ja julkinen luonne. Hajautettuna tieto on turvassa hyökkäyksiltä ja onnettomuuksilta. Kaikkea tietoa ei ole varastoitu yhteen tiettyyn konesaliin tai maantieteelliselle alueelle, vaan se on jaettu käyttäjien vastuulle. Solmuilla on hallussaan kopioita lohkoketjusta ja sen sisältämästä tiedosta. Tästä syystä

lohkojen datan muokkaaminen ei ole mahdollista ilman julkista hyväksyntää. Hajautus myös pitää huolen, ettei kukaan yksittäinen taho pysty kontrolloimaan lohkojen luontia tai transaktioita. Ketjun sisältämät lohkot ja niiden tiivisteet ovat julkisia, mutta niiden sisältämä data voi olla käyttötarkoituksesta riippuen salattua. Salattuun tietoon pääsee käsiksi vain yksityisellä avaimella, jota pitää hallussaan lukuoikeuden omistava taho. Tämä salatun tiedon tallentaminen julkiseen tietokantaan mahdollistaa erittäin korkean tietosuojan ja luotettavuuden saavuttamisen (Miraz & Ali, 2018).

Konkreettinen esimerkki lohkoketjun tarjoamista vahvuuksista ovat kryptovaluutat. Lohkoketjuteknologia luo perustan turvallisille ja luotettaville Peer-to-Peer (P2P) transaktioille. Käytännössä esimerkiksi tilitapahtumia voidaan käsitellä lohkoketjussa ilman keskitettyä tahoa, kuten pankkia. Kryptovaluutan tapauksessa käyttäjät itse ylläpitävät julkista tilikirjaa kirjaamalla tehdyt transaktiot ketjun lohkoihin. Tilikirjaan tallentuu pysyvä rekisteri tapahtuneista siirroista, joita on lähes mahdotonta väärentää. Konsensustekniikoiden (PoW & PoS) ansiosta käyttäjän ei tarvitse murehtia kenen käsiin lohkojen validoinnin luottaisi. Kyseiset tilitapahtumat ovat julkisia, mutta niiden osapuolten henkilöllisyydet pysyvät salassa. (Miraz & Ali, 2018).

Avainsana perinteisen keskitetyn ja hajautetun tilikirjanpidon erolle on luottamus. Keskitetyssä verkossa käyttäjän täytyy sokeasti luottaa palveluntarjoajaan tiedon eheyden, säilyvyyden ja turvan suhteen. Hajautettu toteutus jakaa vastuun käyttäjille. Hajautus yhdistettynä kryptografiaan ja tiivistefunktioihin tarjoaa ratkaisun luottamuspulaan (Miraz & Ali, 2018).

Kryptovaluutat ovat kuitenkin vasta alkua lohkoketjuteknologian tuomille mahdollisuuksille. Miraz & Ali (2018) mukaan lohkoketjut tulevat mullistamaan tietojenkäsittelyn tuomalla rajattoman määrän uusia mahdollisuuksia muun muassa oikeudellisten asiakirjojen ja potilastietojen varastointiin, esineiden Internettiin ja pilvipalveluihin. Lohkoketjupohjainen pilvipalveluratkaisu saattaisi lisätä organisaatioiden välistä luottamusta tarjoamalla hajautetun ja koskemattoman alustan tiedon varastoinnille. Lisäksi tiedon saatavuus ja tietosuoja paranisi. Samoja vahvuuksia voitaisi hyödyntää esineiden Internetin tapauksessa luomaan luotettavuutta ihmisten sijasta laitteiden välille. Luottamuspula on avainongelma massiivisen laiteverkoston kommunikoinnissa. Miljoonia laitteiden välisiä yhteydenottoja voitaisiin seurata kirjaamalla tiedot hajautettuun ja tietoturvalliseen tietokantaan. Lohkojen käyttämät kryptograafiset menetelmät saattaisivat tuoda paremman turvan verkon datalle, mutta niiden vahvistamiseen vaadittavat laskentaresurssit luovat toistaiseksi esteen käyttöönotolle.

Lohkoketjuteknologiat eivät vielä näyttele merkittävää roolia tämänhetkisissä arvonluontiverkostoissa, mutta potentiaalinen vaikutus on kiistaton. Lohkoketjut ovat nopeimmin kasvava yksittäinen teknologia ja se on todennäköisesti matkalla kohti kärkiteknologian asemaa. Europarlamentin päätöslauselmassa (Rahkola, 2019, s. 32) todetaan lohkoketjuilla olevan merkittäviä mahdollisuuksia muun muassa toimitusketjuissa, liikenteessä, terveydenhuoltoalalla, rahoitusalalla sekä koulutuksessa. Teknologiaa voitaisiin

myös hyödyntää tekijänoikeusasioissa sekä ympäristöystävällisten sovellusten kehityksessä.

3 LOHKOKETJUTEKNOLOGIAN TOIMINTAPERIAATTEET

Tässä kappaleessa kuvaillaan, miten lohkoketjuteknologian mahdollistaa hajautetun ja turvallisen verkon ylläpidon. Keskiössä on lohkoketjun osa-alueiden ja toiminnallisuuksien avaaminen yksi aihe kerrallaan. Kappaleet 3.1–3.4 kuvaavat verkon toiminnalle ehdottomia kulmakiviä, joihin lohkoketjun toiminta ja vahvuudet vahvasti nojaavat. Kappaleissa 3.5 ja 3.6 syvennytään Proof-of-Work-konsensusmallin mukaisiin toimintamalleihin ja niiden tarkempiin toiminnallisuuksiin. Kyseinen malli on alkuperäinen lohkoketjun turvalliseen ylläpitoon kehitetty menetelmä, joka ei kuitenkaan enää vuonna 2022 ole ainoa varteenotettava vaihtoehto. Osiossa 3.7 kuvataan, miten lohkoketjuverkko selviää ongelmatilanteista, joissa ketju pääsee haarautumaan. Viimeinen kappale 3.8 pyrkii tuomaan esille teknologian laajoja hyödyntämismahdollisuuksia älysopimusten muodossa. Lohkoketjuun tallennettavien ohjelmien rooli tulee olemaan tulevaisuudessa merkittävä ja ne avaavat muun muassa kryptovaluutan käytölle yhä moniulotteisempia mahdollisuuksia.

3.1 Solmut

Lohkoketjuverkkoa ylläpitää suuri joukko Internettiin kytkettyjä laitteita, joita voidaan verrata perinteisiin palvelimiin. Erona on kuitenkin palvelinkapasiteetin hajauttaminen ympäri maailmaa. Tämä tekee tietokannan väärentämisestä tai tuhoamisesta erittäin vaikeaa. Verkkoa ylläpitäviä palvelimia kutsutaan solmuiksi (Node). Solmut voidaan jakaa vastuutehtäviensä mukaan kahteen pääryhmään, täys- ja kevytsolmuihin (Geroni, 2021).

Täyssolmut turvaavat tiedon säilyvyyden tallentamalla kokonaisen kopion lohkoketjusta ja sen tilikirjasta. Verkon iästä riippuen lohkoketjun tiedostokoko voi olla jopa satoja gigatavuja (Bitcoin, 2021). Lohkoketjun tietojen tuhoutuminen vaatisi kaikkien täyssolmujen levyjen yhtäaikaisen pyyhkiytymisen. Tallennustilan lisäksi täyssolmuilla on äänioikeus verkkoa koskevien muutosten

suhteen. Hajautetun hallinnan vuoksi lohkoketjuverkon päivityksistä päätetään äänestyksillä, joissa yli 50 % täyssolmuista on äänestettävä muutoksen puolesta toimeenpanon aloittamiseksi (Geroni, 2021). Nämä solmut myös vastaavat transaktioiden ja luotujen lohkojen vahvistamisesta (Bitcoin, 2021).

Täyssolmut palvelevat kevytsolmuja vastaanottamalla transaktioita ja välittämällä tietoa muualle verkkoon. Kevytsolmun ei tarvitse omistaa kopiota koko lohkoketjusta, minkä ansiosta järjestelmävaatimukset kyseiselle laitteelle ovat pienet. Tällainen solmu soveltuu esimerkiksi kryptovaluuttalompakoksi, jota voi käyttää kannettavalta laitteelta (Geroni, 2021).

Uusia lohkoja luovat louhijat eivät aina ole täyssolmuja, vaan ne toimivat yhteistyössä niiden kanssa. Täyssolmun niin sanottuun memory-pooliin kertyy vahvistamattomia transaktioita odottamaan vuoroaan. Täyssolmu tarkistaa konsensusmallin mukaan transaktioiden aitouden, jonka jälkeen louhija voi poimia ne uuteen luomaansa lohkoon. Louhijan on myös mahdollista ylläpitää omaa täyssolmua, jolloin tämä voi hoitaa prosessia täysin itsenäisesti. Tämä ei kuitenkaan ole pienille toimijoille tarpeellista tai tehokasta. Useat louhijat voivat muodostaa yhdessä louhintayhtymiä yhteisen louhintasolmun ympärille (Bitstamp, 2021).

3.2 Lohkon tiiviste

Jokainen tietolohko sementoidaan paikoilleen luomalla sille uniikki tiiviste (hash). Tiiviste luodaan usein SHA256-funktion (Secure Hash Algorithm) avulla. Funktio muodostaa 256-bittisen binäärisen arvon, joka esitetään 64-merkkisenä heksadesimaalimerkkijonona. Funktion syötteenä käytetään lohkon dataa sekä edellisen lohkon tiivistettä. Tämä tarkoittaa, että mahdollisia syötteitä funktioon on ääretön määrä, mutta eri syötteillä on teoriassa mahdollista saada sama lopputulos. Todennäköisyys päällekkäisyydelle on 1/2^128, mikä riittää SHA-256-funktion luokittelemisiksi päällekkäisyysvapaaksi. Tiivistefunktion luoma tiiviste pysyy muuttumattomana, mikäli syötteisiin ei tehdä muutoksia. Pienikin muutos edellisen lohkon tiivisteeseen tai lohkon dataan aiheuttaisi täysin uuden lopputuloksen ja tiivisteen. Funktion luoman tiivisteen muuttumista havainnollistaa taulukko 1, jossa vertaillaan eri syötteiden ulostuloja. Funktion avulla voidaan siis luoda datasta tiivistearvo, mutta olemassa olevasta tiivisteestä ei voida tulkita sen aikaansaaneita syötteitä. Tämä ominaisuus on tärkeä tiedon salauksen kannalta. Koska edellinen lohko vaikuttaa seuraavan tiivisteen muodostamiseen, saavutetaan lohkoketjun tiedon maksimaalinen eheys. Yhdenkin lohkon sisältämän tiedonpalasen muuttaminen mitätöi kyseisen ja seuraavien lohkojen tiivisteiden matemaattisen oikeellisuuden. Koska ketjun tiedon voimassaolon ja oikeellisuuden perustana on funktion muodostamat tiivisteet, pitäisi kaikki muutosta seuraavat lohkot uudelleenvahvistaa laskemalla niille uudet tiivisteet (Yaga ym., 2018).

TAULUKKO 1 SHA256-funktion tuloksia kolmella eri syötteellä

SYÖTE	SHA256
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
€	0xc4cc90ed3d26f12d4b08a75140970a7904035c31cbb4515a83f19b9003c00d1d
lohkoketju	0x75ad5d4200242d5b36327be3eced090963faeb7efc348677cf3e1202d0043c84

3.3 Kryptografia

Lohkoketjuteknologiassa käytetään epäsymmetristä kryptografiaa, eli salaustekniikkaa. Tässä tekniikassa käytetään yhden sijaan kahta erillistä avainta: julkista- ja yksityistä avainta. Julkinen avain ei vaikuta salauksen vahvuuteen, joten sen voi huoletta julkaista muille käyttäjille. Yksityinen avain sen sijaan on syytä pitää salassa, sillä sen avulla voi muun muassa avata viestien salauksia tai päästä käsiksi kryptovaluuttalompakkoon. Epäsymmetrisellä salauksella voidaan luoda luottamusta tahojen välille, jotka eivät tunne toisiaan. Transaktioiden luotettavuus voidaan varmistaa säilyttäen julkinen tapahtumahistoria. Salattuja viestejä lähettäessä julkista avainta voidaan verrata postiosoitteeksi ja yksityistä avainta postilaatikon avaimeksi. Salatun viestin lähettäjä salaa viestin käyttäen vastaanottajan julkista avainta, jolloin viestin sisällön pystyy avaamaan vain tätä julkista avainta vastaavalla yksityisellä avaimella. Yksityistä avainta voidaan käyttää myös digitaalisena allekirjoituksena, jolloin itse salaus tehdään yksityistä avainta käyttämällä (Yaga ym., 2018). Vaikka avainten välillä on matemaattinen yhteys, ei julkisesta avaimesta pystytä tulkitsemaan yksityistä avainta (Szabo, 1996). Kuka tahansa voi siis purkaa salauksen julkista avainta käyttämällä ja vahvistaa tiedon lähettäjän olevan yksityisen avaimen haltija (Yaga ym., 2018). Kryptovaluuttatransaktioissa ei yleensä käytetä salausta, sillä tilikirja on julkinen. On kuitenkin olemassa kryptovaluuttoja, kuten Monero, jonka lohkoketjussa transaktiot salataan summien ja osapuolien piilottamiseksi (Shobith, 2021).

Julkista avainta voidaan käyttää myös osoitteiden luontiin lohkoketjuverkostossa. Muun muassa kryptovaluuttatransaktioihin käytettävä osoite voidaan johtaa julkisesta avaimesta käyttämällä kryptograafista tiivistefunktiota. Osoite on julkinen avainta pidempi aakkosnumeerinen merkkijono. Käyttäjäystävällisyyden lisäämiseksi osoite voidaan muuntaa myös QR-koodiksi. Osoitteita ja avaimia voidaan säilyttää lompakoksi (Wallet) kutsun ohjelmiston avulla. Lompakko laskee ja esittää myös mahdollisten kryptovaluuttaomistusten summat. Sillä yksityisen avaimen salassapito on lohkoketjuverkossa ensiluokkaisen tärkeää, on suunniteltu laitteistoa, jonka ainut tehtävä on säilyttää lompakko-ohjelmistoja ja avaimia. Yksityisen avaimen anastaminen on ainoa realistinen tapa varastaa kryptovaluuttaa. Tällaisia laitteita voidaankin pitää erittäin turvallisina, sillä lompakon hakkerointi

erilliseltä Internetin ulkopuolella toimivalta laitteelta on mahdotonta (Yaga ym., 2018).

3.4 Konsensusmallit

Uuden lohkon vahvistajan määrittämiseksi käytetään konsensusmalleja. Mallien avulla voidaan luoda toisilleen tuntemattomien käyttäjien välille luotettava verkko. Mallien tarkoituksena on pitää seuraavan lohkon vahvistaja mahdollisimman satunnaisena ja estää yksittäisten tahojen mahdollisuudet prosessin hallitsemiseen (Yaga ym., 2018). Konsensusmallien algoritmit ovat Li ym. (2021) mukaan lohkoketjun avainteknologiaa. Mallin valinta vaikuttaa suoraa lohkoketjun laajennettavuuteen, energiankulutukseen ja tehokuuteen. Avoimissa lohkoketjuissa, joihin kuka tahansa voi liittyä anonyymisti, on erityisen tärkeää, että malli toimii myös väärinkäyttäjien läsnäolleessa. Suljetuissa verkoissa, joissa käyttäjät ovat julkisia, ei ole suurta tarvetta resursseja kuluttavalle konsensusmallille. Mitä vähemmän luottamusta verkon käyttäjien välillä vallitsee, sitä enemmän luottamuksen luomiseen käytetään resursseja. Väärinkäytökset näissä yksityisissä lohkoketjuissa voivat johtaa suoriin lakitoimiin käyttäjää vastaan (Yaga ym., 2018).

Uusien lohkojen luomista, kutsutaan louhinnaksi. Nimitys on peräisin kyseistä menetelmää hyödyntävien kryptovaluuttojen vahvistusprosessista, jossa kärjistetysti, raskaan työn seurauksena syntyy perinteisen louhinnan tavoin uutta valuuttaa (Yaga ym., 2018).

Proof-of-Work- konsensusmallissa (PoW) ns. louhijat kilpailevat keskenään, siitä kuka saa luoda uuden lohkon ja lunastaa siitä maksettavan palkkion. Käytännössä käyttäjät yrittävät ratkaista matemaattista pulmaa käyttäen avukseen tietokoneiden laskentatehoa. Pulman ratkaisu toimii verkolle todisteena tehdystä työstä, eli käytetyistä resursseista (Swathi, 2021). Lohkon vahvistamiseen vaadittava suuri laskentatyö varmistaa sen sisältämän tiedon eheyden. PoW -mallia hyödyntävän lohkoketjun väärentäminen on käytännössä mahdotonta ja vaatisi valtavan määrän laskentatehoa ja aikaa. Jotta ketju voitaisiin väärentää, pitäisi väärentäjän kyetä ratkaisemaan yksin tekemiänsä muutoksia seuraavien lohkojen pulmat ja kasvattaa oma muokattu ketjunsa olemassa olevaa versiota pidemmäksi. Tästä syystä lohkoketjun tietojen luotettavuus on erinomaisella tasolla. Joissain tapauksissa louhintaa ja uusien lohkojen luontia jatketaan, vaikka lohkoketjuverkossa ei tapahtuisi transaktioita. Ketjun jatkuva pidentäminen vaikeuttaa lohkoketjun väärentämistä (Yaga ym., 2018).

Voimassa oleva, kaikille täyssolmuille jaettava lohkoketju valitaan pisimmän vahvistetun olemassa olevan ketjun perusteella. Mikäli uusien lohkojen lisääminen lakkaa, on väärinkäyttäjillä paremmat mahdollisuudet louhia alkuperäinen lohkoketju kiinni ja korvata se omalla versiollaan. Pulma on vaikea ratkaista, sillä ainoa tapa selvittää ratkaisu, on kokeilla erilaisia vaihtoehtoja, kunnes oikea löytyy. Pulmaa ei ole mahdollista selvittää älykkäästi, vaan lohkon vahvistaminen täytyy aina suorittaa mekaanisesti. Vaikka pulman

selvittäminen on hankalaa, voidaan löydetty ratkaisu tarkistaa helposti. Kun ratkaisu uuden lohkon pulmaan on löydetty, voi kyseinen käyttäjä lähettää lohkon ratkaisuineen täyssolmulle vahvistettavaksi. Vain täyssolmut voivat liittää uuden lohkon osaksi lohkoketjua (Yaga ym., 2018).

Proof-of-Work on edelleen vuonna 2021 yleisin lohkoketjuissa käytetty konsensusmalli. Se esiteltiin alunerin osana Bitcoin-projektia vuonna 2008 ja on siitä lähtien toiminut lähtökohtana uusien konsensusmallien muodostumiselle. PoW on suoraviivainen ja turvallinen tapa luoda verkkoon luottamus. Kasvavien ilmastopaineiden vuoksi se on kuitenkin joutunut suurennuslasin alle mittavan resurssivaatimustensa vuoksi (Li ym., 2021).

Energiatehokkaampi vaihtoehto Proof-of-Work-mallille on omistuksiin keskittyvä Proof-of-Stake-malli. Tässä mallissa käytetään arvontamenetelmää, jolla satunnaisesti valitaan, kuka käyttäjä luotetaan lohkojen vahvistajaksi. Valituksi tulemisen todennäköisyys riippuu käyttäjän panoksesta lohkoketjussa. Panos mitataan usein lohkoketjun kryptovaluuttaomistuksina, mikä vaikuttaa valituksi tulemisen todennäköisyyteen. Valintaprosessista on muitakin variaatioita, mutta niitä kaikkia yhdistää omistusten määrän suora vaikutus todennäköisyyksiin. Tämä lisää suurten omistajien vaikutusvaltaa, mutta heillä voidaan yleisesti katsoa olevan puhtaimmat intressit kyseisen lohkoketjun menestykseen (Appelbaum & Smith, 2018). Jotta käyttäjä voi asettua ehdolle lohkon vahvistajaksi, täytyy tämän lukita varallisuuttaan väliaikaisesti käyttökelvottomaan tilaan. Lukittu panos toimii myös kannustimena käyttää valtaansa oikein. Mikäli käyttäjä päättää vahvistaa väärennetyn lohkon, saattaa tämä menettää pantanneensa varallisuuden. Siksi on myös tärkeää, että vahvistuksesta maksettava palkkio on aina pienempi, kuin vahvistajan panos. Proof-of-Stake-mallissa uhrataan osa hajautuksen tuomasta turvallisuudesta resurssien säästämiseksi (Aponte-Novoa ym., 2021).

3.5 Lohkon pulman ratkaiseminen eli ”Hashing”

Proof-of-Work- mallin hyödyntämän matemaattisen pulman ratkaisuyrittämistä kutsutaan ”hashing:iksi”. Laajasti käytössä oleva tapa toteuttaa pulma on luoda lohkon ylätunnisteen tiivistearvolle hyväksyntää edellyttävät parametrit. Ylätunnisteen tiedoista SHA256-algoritmin avulla muodostettavan tiivisteen arvon (hash) täytyy esimerkiksi alkaa tietyllä määrällä nollia (Georhiades ym., 2019).

Ratkaisuksi kelpaavan tiivistearvon alun nollien määrä on suoraan verrannollinen pulman vaikeustason kanssa. Pieni, usealla nollalla alkava, tiiviste on hankala löytää, sillä pulman parametrit täyttävien arvojen määrä on pienempi. Pulman vaikeustasoa voidaan säädellä, jotta ratkaisun selvitysaika pysyy vakiona. Harvinaisen, usealla nollalla alkavan, merkkijonon löytäminen satunnaisesti kokeilemalla kestää pidempään, jolloin lohkon vahvistaminen vaatii enemmän laskentatehoa tai aikaa. Pitämällä pulman ratkaisuaika vakiona, lohkoketjuverkon turvallisuus säilyy, eikä kukaan taho pysty hallitsemaan lohkojen vahvistamista kasvattamalla laskentatehoaan. Esimerkiksi Bitcoin

hyödyntää Proof-of-Work- mallia ja pulman vaikeusastetta kohdistetaan 2016 lohkon välein. Pulman ratkaisuaika pyritään Bitcoin-verkossa pitämään noin kymmenessä minuutissa (Yaga ym., 2018).

Yrittäessään ratkaista pulmaa käyttäjän tietokone muodostaa lohkon tiedoista tiivistearvoja (hashing). Shahsavari ym. (2019) mukaan arvo luodaan syöttämällä esimerkiksi SHA256- funktioon lohkon data yhdistettynä ns. nonce-arvoon. Nonce-arvo on numeerinen luku, jota muuttamalla saadaan muutettua funktion ulostuloa. Uusia tiivisteitä luodaan, kunnes löydetään nonce-arvo, jolla saavutetaan parametrit täyttävä ratkaisu. Tiivisteiden luonti ja kokeilu vaatii merkittävän määrän laskentatehoa ja sähköä (Shahsavari ym., 2019).

Taulukko 2 havainnollistaa esimerkin, jossa pulman ratkaisuun vaadittiin 10730895 yritystä. Lohkon sisältö pysyy muuttumattomana, mutta numeerista nonce-arvoa kasvatetaan lineaarisesti. Pulman ratkaisuvaatimus yhtälönä kuvattuna:

SHA256(“lohkon tieto” + Nonce) = Lohkon tiiviste, joka alkaa arvoilla “000000”

TAULUKKO 2 Esimerkki kolmesta nonce-arvoa muuttamalla löydetystä ratkaisusta, joista alin täyttää asetetut vaatimukset (Yaga ym., 2018)

SHA256("lohko0") = 0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938 (ei ratkaistu)
SHA256("lohko1") = 0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10 (ei ratkaistu)
SHA256("lohko10730895") = 0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587 (ratkaistu)

3.6 Louhijat

Käyttäjiä, jotka tarjoavat lohkoketjun vahvistamiseen vaadittavaa laskentatehoa, kutsutaan louhijoiksi. Louhija saa korvauksena laitteidensa työstä palkkion, joka koostuu usein lohkoketjun päällä toimivasta kryptovaluutasta. Esimerkiksi Bitcoin-lohkojen luontiin tarvittava laskentateho on niin suuri, ettei yksittäinen tietokone kykene tähän taakkaan yksin. Lohkon tiivisteen ratkaisusta maksettava palkkio toimii kuitenkin sopivana kannustimena omien laitteiden valjastamisesta lohkoketjun käyttöön. Louhintaa suoritetaan niin yritysten kuin yksityishenkilöidenkin toimesta. Yksittäisen lohkon ratkaisemisesta maksettavaa palkkiota ei jaeta kaikkien louhijoiden kesken, vaan koko potti kuuluu pulman ensimmäisenä ratkaisseelle käyttäjälle. Louhijat siis käytännössä kilpailevat

keskenään lohkon vahvistamisesta. Pienellä laskentatehokapasiteetilla louhivan on huomattavan epätodennäköistä ratkaista lohkon tiiviste ensimmäisenä. Tästä syystä on syntynyt niin sanottuja louhintayhtymiä (mining pool), joissa suuri määrä louhijoita tekee yhteistyötä jakaen voitot jäsenten kesken laskentatehopanoksen mukaan. Louhintaryhmän sisällä voidaan työ jakaa siten, että jokaiselle käyttäjälle määritetään tietty nonce-arvojen väli. Tällöin ryhmä toimii tehokkaasti, eikä kukaan yritä samaa ratkaisua kahdesti (Yaga ym., 2018).

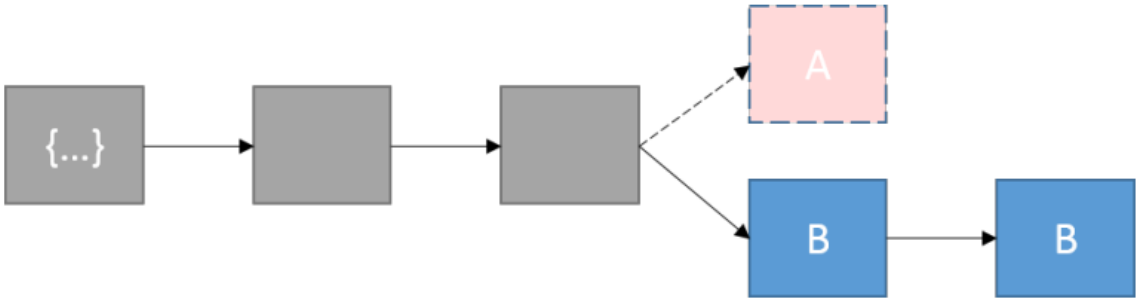
Proof-of-Work- ja Proof-of-Stake-mallit altistuvat mittavasta turvallisuudestaan huolimatta niin sanotulle 51 %- hyökkäykselle. Teoreettisesti yksittäinen taho voisi hallita uusien lohkojen luontia täydellisesti saavutettuaan 51 prosentin osuuden vahvistajan valintaan vaikuttavista tekijöistä (Aponte-Novoa ym., 2021). PoW tapauksessa hyökkäyksen onnistumiseksi hyökkääjän täytyisi hallita suurinta osaa lohkoketjuun kohdistuvasta laskentatehosta. Tällöin hyökkääjä voi estää uusien transaktioiden suorittamisen verkossa. Myös suoritettuja transaktioita voitaisiin tällaisessa tilanteessa peruuttaa, mikä johtaisi valuutan käyttämiseen kahteen kertaan (double spending). 51 prosenttia laskentatehosta omaava taho hallitsee louhintaa täydellisesti estäen muiden louhijoiden mahdollisuudet osallistua prosessiin. Louhintamonopoli tarkoittaa hyökkääjien kykyä kerätä kaikki louhintatuotot. Teoriassa valtaosaa laskentatehosta hallitseva taho voisi rakentaa omaa rinnakkaisketjua muuta käyttäjäkuntaa nopeammin ja lopulta nostaa oman lohkoketjunsa viralliseksi pisimmäksi ketjuksi (Frankenfield, 2021b).

Hyökkäykselle altistuvat lähinnä lyhyet vähän laskentatehoa käyttävät lohkoketjut, joille hyökkäyksen suorittaminen on vaadittaviin resursseihin nähden mahdollista. Mitä kauempaa menneisyydestä lohkoketjua halutaan väärentää, sitä kauemmin hyökkääjällä kestää louhia aito ketju kiinni. Valtavirran tunnistamille lohkoketjuille, kuten Bitcoinille tai Ethereumille, uhka on lähinnä teoreettinen, sillä hyökkäykseen vaadittavan laskentatehon ja pääoman määrä on tähtitieteellisen suuri. Suljetuille verkoille uhkaa ei ole, sillä kilpailevia ketjuja ei yleensä ole, eikä lohkoketjun luonne ole yhtä hajautettu. Näillä verkoilla on usein omistaja tai hallinnoiva osa, joka voi tarvittaessa poistaa väärinkäytöksistä epäillyt käyttäjät verkosta kokonaan (Aponte-Novoa ym., 2021). Esimerkkinä tapahtuneesta 51 %-hyökkäyksestä toimii Bitcoin Gold lohkoketjun kokema väärinkäyttö vuonna 2018. Hyökkääjä hallitsi verkon laskentatehoa useita päiviä aiheuttaen yli 18 miljoonan dollarin vahingot (Frankenfield, 2021a).

3.7 Lohkoketjun konfliktit ja haarautuminen

Usean käyttäjän julkaistessa uusia lohkoja samanaikaisesti, syntyy väliaikainen konflikti lohkoketjuversioiden välille. Lohkon samaan aikaan luoneilla käyttäjillä, on kaikilla hallussaan aito vahvistettu versio lohkoketjusta, joita voi konfliktin aikana olla useita. Voimassa olevia, muille käyttäjille jaettavia, ketjuja voi kuitenkin olla vain yksi, jolloin osa rinnakkaisketjuista täytyy hylätä. Oikean ketjun valinta määrittyy seuraavan lisättävän lohkon mukaan. Kuvio 1 esittää,

miten lohkoketjuversio, johon seuraavaksi liitetään uusi lohko, jää voimaan pisimpänä aitona ketjuna. Tällöin rinnakkaisten ketjujen lohkojen sisältämien tilikirjojen voimassaolo lakkaa. Mikäli tilikirjoissa on eroja, saattaa osa jo vahvistetuista transaktioista peruuntua. Tästä syystä on turvallista odottaa uusien lohkojen lisäämisiä ennen kuin luottaa transaktion suoritukseen. Mitä useampia lohkoja tietyn transaktion sisältävän lohkon perään on lisätty, sitä epätodennäköisempää on, että kyseinen tieto mitätöityisi. Konfliktien ratkaiseminen on ensiluokkaisen tärkeää varsinkin avoimissa lohkoketju-verkoissa, joissa lohkon lisäämisestä kilpailevia käyttäjiä on paljon. Laajalle hajautetussa verkossa, osa käyttäjistä on jatkuvasti poissa ajan tasalta. Ennalta määritetty konfliktien ratkaisumenetelmä estää lohkoketjun pysähtymisen. Jatkuvasti kasvavaa ketjua on vaikeampi väärentää luomalla rinnalle pidempi väärennetty lohkoketju (Yaga ym., 2018).



KUVIO 1 Haaroittunut lohkoketju, jossa lyhyemmäksi jäänyt haara A poistuu voimasta (Yaga ym., 2018)

Lohkoketjuverkkoa kehitetään ohjelmistopäivityksillä. Näitä muutoksia, joita toteutetaan verkon protokollaan, kutsutaan ”haaroiksi” (fork). Haaroittumiset jaetaan niiden vaikutuksen mukaan pehmeisiin- ja koviin haarautumisiin (soft fork ja hard fork). Niin sanottu pehmeä haarautuminen tarkoittaa usein pienempää muutosta, esimerkiksi verkkoon lisättyä uutta ominaisuutta. Rajanveto näiden kahden haarautumistapahtuman luokittelulle riippuu kuitenkin päivityksen vaikutuksesta eri ohjelmistoversioita käyttävien solmujen yhteistyöhön (Yaga ym., 2018).

Kovassa haarautumisessa muutos on rakenteeltaan sellainen, etteivät vanhan ohjelmistoversion omistavat käyttäjät enää pysty vahvistamaan uuden version käyttäjien luomia lohkoja. Tällöin lohkoketju usein haarautuu konkreettisesti. Käytännössä tämä tarkoittaa kahden rinnakkaisen lohkoketjun muodostumista, yksi kummallekin ohjelmistoversiolle. Rinnakkaisketjujen käyttäjät eivät pysty tekemään transaktioita keskenään tai luomaan lohkoja toistensa ketjuihin. Suljetuissa lohkoketjuissa haarautuminen voidaan estää muuttamalla päivitys pakolliseksi tunnettujen käyttäjien kesken. Myös avoimissa verkoissa päivitys tulee aikanaan pakolliseksi. Ajankohta määritellään usein päättämällä tietty lohkon järjestysluku, jonka luonnin hetkellä vaatimus astuu voimaan. Päivittämättömät solmut eivät kykene toimimaan päivitetyssä

verkossa, sillä uudet lohkot eivät enää täytä vanhan version mukaisia määritelmiä (Almeida ym., 2019).

Useimmat kovat haarautumiset ovat suunniteltuja, mutta päivityksen taustalla voi olla myös ohjelmistovirhe. Myös lohkoketjun kryptografiassa havaitut puutteet voivat aiheuttaa kyseisen toimenpiteen. Esimerkiksi tiivistealgoritmin vaihtaminen haavoittuvuuden vuoksi vaatii kovaa haarautumista. Tällöin varmistutaan, että vähintäänkin alkuperäisen lohkoketjun turvallisuus ei vaarannu ja korjaus saadaan aktiiviseksi kaikille käyttäjille (Yaga ym., 2018).

Esimerkki kovasta haarautumisesta on Bitcoin Cash- kryptovaluutan syntyminen. Kyseinen lohkoketju haarautui Bitcoin-ketjusta vuonna 2017, tavoitteenaan korjata alkuperäisen verkon ongelmia. Bitcoin-verkon suuri ongelma on sen heikko skaalautuvuus. Ongelma huomattiin jo vuonna 2015, kun käyttäjämäärät lähtivät rajuun nousuun. Bitcoin-transaktioiden määrän kasvaessa kasvoi myös niiden suorittamiseen vaadittava aika, sekä kulut. Ratkaisuna ongelmaan nähtiin lohkon koon kasvattaminen. Tällöin transaktioita voidaan kirjata lohkoihin useampia kerralla, lyhentäen valuuttasiirtojen jonotusaikoja ja kuluja. Alkuperäisen lohkoketjun rinnalle kopioitiin uusi, päivitettyjä protokollia noudattava, ketju, jolloin jokainen Bitcoin-omistaja sai haltuunsa vastaavan määrän uutta kryptovaluuttaa. Bitcoin Cash on muilta toimintaperiaatteeltaan edelleen lähes samanlainen kuin Bitcoin. Se muun muassa käyttää samaa PoW-konsensusmenetelmää (Frankenfield, 2021a).

Pehmeässä haarautumisessa (Soft fork) eri ohjelmistoversiota käyttävät solmut voivat jatkaa toimintaa yhteisymmärryksessä. Päivittämättömät solmut voivat jatkaa uudemman version alaisuudessa toimivien solmujen lohkojen vahvistamista ja transaktioiden suorittamista (Almeida ym., 2019). Yaga ym. (2018) esittämässä fiktiivisessä esimerkissä pehmeän haarautumisen aiheuttava päivitys voisi olla muutos lohkon sallittuun maksimikokoon. Lohkon tiedostokoko voitaisiin esimerkiksi muuttaa kokonaisesta megabitistiä puolikkaaseen. Tällöin päivittämättömätkin solmut voisivat jatkaa verkossa toimimista, kunhan niiden luomat lohkot täyttävät myös uuden version vaatimukset. Käytännössä uudistus ei siis pakota käyttäjiä päivittämään ohjelmistoaan, sillä uusi puolikkaan megabitin lohkokoko täyttää edelleen myös vanhan version vaatimuksen.

3.8 Älysopimukset

Lohkoketjuun tallennettavia ohjelmia kutsutaan älysopimuksiksi (Smart Contracts). Ohjelma koostuu yksinkertaisesta pätkästä koodia, joka määrittää ehdot sopimuksen täyttymiselle tai purkautumiselle. Sopimusten avulla toisilleen tuntemattoman tai anonyymit käyttäjät voivat tehdä luotettavia transaktioita ilman tarvetta kolmansille osapuolille. Lohkoketjuteknologian vahvuuksiin kuuluva varastoidun tiedon eheys poistaa perinteisiin sopimuksiin liittyvän väistämättömän epävarmuuden. Sopimuksen sisältöä ei voi muuttaa sen lohkoketjuun liittämisen jälkeen, eikä sen suoriutumista ehtojen täyttyessä

pysty estämään (Wang ym., 2018). Amerikkalainen tietojenkäsittelytieteilijä Nick Szabo määritteli älykkäät sopimukset alun perin koneellisesti luettaviksi transaktioprotokolliksi, jotka toteuttavat sopimuksen ennalta määritetyt ehdot (Lauslahti ym., 2016).

Sopimuksen kirjoittavien tahojen tulee ennen ohjelman julkaisua olla yksimielisiä sopimuksen ehdoista. Tämän jälkeen sopimus voidaan liittää lohkoketjuun, missä se säilyy muuttumattomana odottaen koodin ehtolausekkeiden täyttymistä. Julkaisunsa jälkeen älysopimus toimii täysin itsenäisesti luoden luottamuksen allekirjoittaneiden tahojen välille. Mattilan (2016) mukaan juuri ihmiselementin tuoman epävarmuuden poistamalla sopimusprosessista saadaan luotettavampi ja kustannustehokkaampi.

Lohkoketjuteknologian mahdollistamat älysopimukset ovat olleet etenkin finanssi- ja pankkialan kehityskohteena, sillä niiden soveltaminen liiketoiminnaksi on näissä yhteyksissä yksinkertaisinta. Teknologian tuomat mahdollisuudet ovat käytännössä rajattomat, mutta toistaiseksi muilla aloilla soveltaminen on vielä alkuvaiheessa (Lauslahti ym., 2016).

Nick Szabo (1996) kuvaili jo vuonna 1994 esimerkin älysopimusten käytöstä IoT-ympäristössä kirjoittamalla niin sanotusta älykkäästä omaisuudesta. Esimerkissä ajoneuvon käyttöoikeutta kontrolloidaan automatisoitujen älysopimusten avulla. Pankki pystyisi lunastamaan ajoneuvon omistukseensa automaattisesti, mikäli omistaja ei maksa lainanlyhennyksiään ajoissa. Kyseisessä tapauksessa ajoneuvon käyttöoikeutta kontrolloidaan ohjelmistoa sisältävän autonavaimen avulla. Älysopimukseen kirjatut ehtolausekkeet vaihtavat ajoneuvon oven avaamiseen vaadittavan digitaalisen allekirjoituksen itsestään, mikäli pankki ei vastaanota asiakkaaltaan maksua. Toiminnallisuus myös estäisi ajoneuvon käytön varastetuilla avaimilla.

Szabon 1990-luvulla kuvailemat älyesineet voidaan nyt muuttaa todeksi lohkoketjuteknologian mahdollistamilla älysopimuksilla. Ilmiötä, jossa esineet pystyvät siirtämään dataa verkossa ilman ihmisen väliintuloa kutsutaan esineiden Internetiksi (Internet of things – IoT). Näitä verkkoja voidaan käyttää muun muassa terveysalalla, kodin automaatiossa ja liikenteessä. Verkkoon kytketty sensori pystyy kommunikoimaan automaattisesti havaitessaan ympäristön muutoksia. Sensori huomaa niin kotonaan kaatuneen vanhuksen kuin kuljettajan kuolleessa kulmassa ajavan ajoneuvonkin (Ramson ym., 2020).

Lohkoketjuteknologian pioneerikryptovaluutta Bitcoin ei toiminnallisten puutteidensa vuoksi tue täysvaltaisia älyominaisuuksia. Nimenomaan näitä puutteita korvaamaan syntyi lohkoketjualusta Ethereum. Kyseisen alustan perustaja Vitalik Buterin (2013) kertoo julkaisussaan ”Ethereum Whitepaper”, miten itse lohkoketjuteknologian synty on Bitcoinin valuuttajärjestelmään tuomaa mullistustakin tärkeämpi asia. Hän näkee Ethereumin välineenä jatkaa Satoshi Nakamoton keksimän teknologian kehitystä kohti monikäyttöisempää suuntaa. Keskiössä tässä kehityksessä ovat uudenlaiset älykkäät ominaisuudet, joiden toteutuksessa älysopimukset ovat keskeisessä roolissa (Buterin, 2013). Ethereumin tuomat uudenlaiset mahdollisuudet olivat niin laajoja, että sen perustamisesta katsotaan alkaneen lohkoketjujen toinen sukupolvi. Ajatus

Ethereumin taustalla oli luoda lohkoketjuympäristöön räätälöity ohjelmoitava virtuaalikone ohjelmakoodin ajamista varten. Projektin voidaan katsoa onnistuneen, sillä suurin osa vuoden 2019 älysopimuksista toteutettiin Pinna ym. (2019) mukaan juuri Ethereum-alustalla.

Valmiissa Ethereum-älysopimuksessa on ohjelmakoodin lisäksi sopimusehdot. Ehdoissa määritellään tarkasti, milloin sopimus aktivoituu, ja mitä tällöin tapahtuu. Sopimusta ei voi muokata sen julkaisun jälkeen, jolloin osapuolet voivat rauhassa antaa automaation hoitaa sopimuksen suorittamisen. Jotta sopimuksia prosessoiva virtuaalikone olisi turvassa palvelunestohyökkäyksiltä ja turhalta liikenteeltä, täytyy käyttäjien maksaa verkon käytöstä transaktioiden laskentatehovaatimusten mukaan. Maksuja varten luotiin Ethereum-verkon päälle myös kryptovaluutta, Ether. Ethereum-älysopimuksia ovat muun muassa finanssisovellukset, joita voidaan käyttää kryptovaluuttatransaktioissa, sekä pelisovellukset, joiden avulla suoritetaan arvontoja. Kaupanvahvistussovellukset sen sijaan toimivat perinteisen sopimuksen tavoin tallentaen tahojen väliset sopimukset lohkoketjuympäristöön (Pinna ym. 2019). Lukuisat älysopimukset yhdessä voivat muodostaa niin sanotun hajautetun applikaation (Decentralized Application – Dapp). Toimiakseen oikein, tällainen applikaatio tarvitsee toiminnallisuuksista vastaavan back-end-ohjelmiston, sekä käyttöliittymän tarjoavan front-end-ohjelmiston. Älysopimukset toimivat siis hajautettujen applikaatioiden back-end-osana. Tällainen applikaatio on hajautettujen osien summa, eikä täten ole minkään yksittäisen tahon hallinnassa tai omistuksessa (Ethereum, 2021).

4 LOHKOKETJUTEKNOLOGIAN SÄÄNTELY EUROOPAN UNIONISSA

Euroopan unioni haluaa olla maailman kärjessä mitä tulee lohkoketjuteknologiaan. EU-komissio on luonut strategian, jolla se luo arvojaan vastaavan standardin teknologian kehittämiselle ja lainsäädännölle. Strategian tavoitteena on luoda suotuisat puitteet alan suurille yrityksille toimintansa kehittämiseen. Niin sanottuun 'kultaiseen standardiin' (gold standard) sisältyvät pääkohdat ovat: kestävä kehitys, tietosuoja, digitaalinen identiteetti, kyberturvallisuus ja yhteistoiminta. Standardin mukainen lohkoketjuratkaisu olisi siis energiatehokkaasti toteutettu Euroopan vahvat tietosuojasäännökset täyttävä turvallinen verkko, joka vastaa EU:n kehittyvää digitaalista identiteettiä. Toimintatehokkuuden kasvattamiseksi lohkoketjun tulisi lisäksi olla yhteensopiva kaikkien, myös Euroopan ulkopuolisten, toimijoiden kanssa (Europan Comission, 2021a).

Tässä kappaleessa käsitellään Euroopan unionin ja sen eräiden jäsenmaiden linjauksia lohkoketjuteknologioiden suhteen. Sääntely käsittää niin tulevat lakiesitykset kuin olemassa olevat säännöt teknologian käytölle ja verotukselle. Sääntelyn kehitys liittyy myös läheisesti komission luomaan strategiaan, sillä se luo pohjan yksittäisten EU-maiden omalle lohkoketjulainsäädännölle. Sääntely ei kuitenkaan tarkoita vain rajoitteita ja sääntöjä, vaan myös sen positiivisia vaikutuksia tuodaan esiin muun muassa tukevan rahoituksen muodossa.

4.1 Euroopan komission lohkoketjustrategia

Strategian keskiössä on koko unionin kattava yhteistyö. Tavoitteena on luoda julkisen sektorin käyttöön lohkoketju, jonka avulla hallinto ja tieto säilyy ja liikkuu luotettavasti koko Euroopan alueella. Projektin toteuttamista varten perustettiin vuonna 2018 yhteistyöhanke, johon osallistuvat kaikki 27 EU-maata, Norja sekä itse komissio (European Commission, 2021c). European Blockchain Partnershipin (EBP) on tarkoitus rakentaa Euroopan lohkoketjuinfrastruktuuria

(European Blockchain Services Infrastructure, EBSI). Yhteistyön avulla pyritään pitämään kehitys yhtenäisenä ja läpinäkyvänä. Yhteistyöverkosto toimii myös päättäjien työkaluna tutustua teknologiaan ja sen lainsäädäntömahdollisuuksiin (European Commission, 2021a). Suomea hankkeessa edustaa Valtionvarainministeriö (Europan Commission, 2021b).

EBSI:n toiminnallisuudet tähtäävät aluksi julkisen sektorin prosessien tehostamiseen ja palveluiden parantamiseen. Projektiin on kuitenkin kaavailtu laajennustavoite yhteistoiminnan avaamiseksi myös yksityisen sektorin toimijoiden kanssa. Yhteistoiminta parantaisi julkisen ja yksityisen sektorin kustannustehokkuutta ja nopeuttaisi prosesseja. EU-maiden yhteisen lohkoketjun kehitys etenee iteratiivisesti. Aluksi on tarkoitus keskittyä pieneen määrään avaintoiminnallisuuksia ja myöhemmin jatkaa uusien ominaisuuksien lisäämistä. Avaintoiminnallisuuksiin kuuluu muun muassa tiedon pysyvyyden ja koskemattomuuden varmistaminen, kansalaisten koulutustodistusten kustannustehokas käsittely sekä hajautettu identiteettihallinta. Suunnitelmissa olevia lisäominaisuuksia ovat muun muassa pienten ja keskisuurien yritysten lohkoketjupohjainen rahoittaminen, henkilötunnukseen perustuva tietokanta sosiaalipalveluiden tarjoamiseksi vieraassa maassa sekä rekisteri turvapaikan hakuprosessien hallintaan (Europan Commission, 2021d).

Toinen strategian pääkohta on ammattitaitoisen asiantuntijaosaamisen kehittäminen ja saatavuuden varmistaminen. Euroopan digitalisaatio-ohjelma (Digital Europe Programme) tarjoaa rahoituksen osaamisen kehittämiseen EU-alueella. Komission mukaan on tärkeää, että Eurooppa on omavarainen myös teknologiaratkaisujen suhteen. Ohjelmalle on myönnetty 7.5 miljardin euron budjetti, jolla se tähtää yritysten, kansalaisten ja julkisen sektorin digitalisaatioon nousevia teknologioita hyödyntämällä. Osaamisen kehittämisen lisäksi ohjelmalla rahoitetaan muun muassa superlaskentaa, tekoälyä ja kyberturvallisuutta (Europan Commission, 2021g).

Komissio toimii yksityisen sektorin yritysten kanssa INATBA-yhteistyösopimuksen (International Association of Trusted Blockchain Applications) avulla. Yhteistyömallin avulla EU-maat pääsevät lähemmäs muita sidosryhmiä ja voivat suunnitella yleishyödyllisten lohkoketjuratkaisujen kehitystä. Eri sektorien ja maiden lohkoketjujärjestelmien yhteistoimivuus on erittäin tärkeää ja tämän varmistamiseksi komissio uskoo vahvasti alan standardeihin. Teknologian toivotaan kehittyvän nopeasti, mutta sen on tapahduttava Euroopan unionin arvot täyttävällä tavalla. Tämä tarkoittaa muun muassa ympäristöystävällistä ja kestävästi kehittyvää lähestymistapaa (Europan Commission, 2021c).

Lohkoketjustrategian läpiviemiseksi EU on päättänyt nostaa tutkimukseen ja innovaatioihin allokoitua rahoitusta. Rahoitusta annetaan apurahapakettien ja sijoitusten muodossa. Apurahaa EU-komissio myöntää Horizon-ohjelmansa kautta. Vuosina 2016–2019 komissio myönsi 180 miljoonaa euroa apurahaa kyseisen ohjelman kautta. Horizon-ohjelmaa uudistetaan ja lohkoketjuteknologiaprojektien apurahabudjettia ollaan hyvin todennäköisesti nostamassa. Uuden ohjelman nimi on Horizon Europe ja sen kokonaisbudjetti

vuosille 2021–2027 on noin 95 miljardia euroa. Uuden ohjelman tarkoitus on nostaa EU:n kilpailukykyä ympäristön kannalta kestävällä tavalla sijoittamalla kasvuun tutkimuksen ja innovaatioiden kautta (Europan Commission, 2021e). Lohkoketjuteknologian kehittämiseksi on myös perustettu rahasto, johon komissio on Horizon 2020-ohjelman kautta myöntänyt 100 miljoonaa euroa. Rahastoon on myös luvassa yksityistä rahaa ja kokonaispotin odotetaan kasvavan. EIF (The European Investment Fund) ilmoitti loppuvuodesta 2020 yhdessä komission kanssa lohkoketjuja ja tekoälyä Euroopassa rahoittavien rahastojen arvon olevan jo noin 700 miljoonaa euroa (Europan Commission, 2020). Rahastoilla pyritään alkuvaiheessa olevia ja kasvavia projekteja tukemalla edistämään teknologian laajaa käyttöönottoa (Europan Commission, 2021f).

4.2 Kryptovaluuttalait

EU näkee tarpeelliseksi kontrolloida kryptovaluuttamarkkinaa rahanpesun ja terrorismin rahoittamisen estämiseksi. Sääntelyä varten kehitettiin MiCA-viitekehys (The European Commission's Regualtion of Markets in Crypto-assets). Komissio esitteli kesällä 2021 lakiehdotuksista koostuvan paketin, jonka tarkoitus on tehdä laittomien transaktioiden havaitseminen lohkoketjuverkoissa helpommaksi. Pakettiin sisältyy myös lakiuudistus varojen liikkeiden seuraamista määrittelevään pykälään. Uudistus laajentaa olemassa olevan lain kattamaan myös kryptovaluuttatransaktioiden jäljittämisen. Tarkoitus on luoda yhtenäinen linja rahanpesun ja rikollisuuden torjuntaa varten. Lakiehdotus saapui verrattain myöhään ja muutamat EU-maat, kuten Saksa, olivat jo ehtineet säätää omia vastaavia lakejaan. Nyt valvonta tuodaan EU-tasolle. Lakeja säädetään FATF (Financial Action Task Force) suositusten mukaan, kaikki arvopaperiluokat kattavan yhtenäisen linjan saavuttamiseksi. Transaktiotietojen valvonta herättää kysymyksiä, myös EU:n korkeassa arvossa pitämän, yksilön tietosuojan suhteen. Lakiehdotuksen 15. artiklan mukaan kryptovaluuttojen transaktiotietojen datankäsittelyssä noudatetaan yleisen tietosuoja-asetuksen (2016/679) mukaisia toimintatapoja. Asetus (GDPR) määrittelee tietosuojan osaksi ihmisen perusoikeuksia ja pyrkii parantamaan yksilön tietoturvaa (Euroopan unioni, 2016). Tämä on tärkeää, sillä laki sallii mittavien sensitiivisten henkilötietojen keräämisen. Kryptovaluutta-alustojen täytyy muun muassa säilyttää asiakkaidensa tietoja vähintään viisi vuotta tilitapahtumien jälkeen. Tietojen säilyttäminen mahdollistaa rikollisten varainsiirtojen tutkinnan takautuvasti. Artikla 14 täsmentää tietoja, joita palveluntarjoajan täytyy asiakkaistaan säilyttää. Dokumentaatiosta täytyy löytyä kryptovaluuttasiirron suorittajan nimi, tilinumero, osoite, henkilötunnus ja syntymäaika. Varojen vastaanottajan osalta tiedossa on oltava vähintään henkilön nimi (Notabene, 2021a). Mainittujen tietojen keräämisen rajana on 1000 euroa ylittävät varainsiirrot. Summa voi kertyä myös useammista pienemmistä siirroista. Alle raja-arvon jäävistä transaktioista kerätään vain lähettäjän ja vastaanottajan nimet ilman tarkempia henkilötietoja. Mikäli valuuttaa siirretään ulos EU-alueelta, kerätään siirron osapuolista kaikki mahdollinen tieto terrorismin vastaiseen

tarkkailuun vedoten. Artikla 12 määrää kryptovaluutta-alustojen varmistamaan tarvittavien tietojen olemassaolon, ennen transaktioiden hyväksymistä. Kohdassa annettaan myös muistutus alustan velvollisuudesta kieltäytyä suorittamasta varainsiirtoja tiedonkeräystä laiminlyövän alustan kanssa (Notabene, 2021b).

Tämän lisäksi syyskuussa 2020 käyttöönotettiin niin sanottu digitaalisen rahoituksen paketti, jolla mahdollistetaan kansalaisille turvallinen ja mutkaton siirtymä digitaalisen valuutan käyttöön. Paketti koostuu digitaalista rahoitusta käsittelevästä strategiasta ja lakiesityksistä. Muutoksilla pyritään päivittämään lakeja vastaamaan saatavilla olevaa edistynyttä digitaalista teknologiaa. Tavoitteena on myös luoda synergioita isojen toimijoiden ja innovatiivisten start-up-projektien välille (Euroopan unionin Komissio, 2016).

4.3 Teknologiahankkeita ja lainsäädäntöä Suomessa

Erityisasiantuntija Markus Rahkola esittää eduskunnan tulevaisuus-valiokunnalle kirjoittamassaan raportissa (Rahkola, 2019) näkemyksensä, jonka mukaan lohkoketjuteknologia tulisi nostaa Suomen politiikka- ja toteutusohjelmiin. Suomen edun mukaista on olla aktiivisesti mukana kansainvälisessä lainsäädäntökeskustelussa. Aktiivisella lähestymistavalla varmistetaan Suomen asema houkuttelevana kohteena lohkoketjuteknologiaa hyödyntäville yrityksille. Euroopan unionin sisäinen kilpailu parhaan kasvuympäristön tarjoamisesta on johtanut hyvin epäyhtenäiseen sääntelyyn jäsenvaltioiden välillä. Epävarmasta tilanteesta huolimatta Suomen tulisi tunnistaa uusien teknologioiden tuomat mahdollisuudet ja varmistaa, että politiikkatoimet ja sääntely tukevat muutoksia. Lainsäädännöllisiä puutteita voidaan tunnistaa ja korjata käytännön kokeilujen kautta. Sääntelyvalmistelussa tulee olla rohkea, eikä antaa riskien hallita keskustelua (Rahkola, 2019).

Lohkoketjuteknologia on paljon esillä Suomessa, mutta valtavaa innostusta se ei ole onnistunut muihin maihin verrattuna ihmisissä luomaan. Kiinnostus kuitenkin näkyy muun muassa tutkimushankkeiden, lainsäädäntövalmistelujen ja kryptovaluuttojen suosion kasvun muodossa. Lisäksi valtionvarainministeriö perusti vuonna 2018 verkoston, jonka tarkoituksena on kehittää teknologian käyttömahdollisuuksia yhteistoiminnassa yritysten kanssa sekä jakaa tietoa (Rahkola, 2019).

Euroopan komission rahoittaman lohkoketjufoorumin loppuvuodesta 2020 tuottamassa raportissa kuvaillaan EU-jäsenmaiden nykytilaa teknologian omaksujina. Raportin mukaan Suomen lohkoketjuprojektit keskittyvät vahvasti julkiselle sektorille ja jäävät lähes poikkeuksetta kokeilutasolle. Korkeasta digitalisaatioasteesta huolimatta konkreettiset nousevia teknologioita hyödyntävät ratkaisut puuttuvat. Suomessa oli vuonna 2020 noin 150 lohkoketjupohjaista start-up projektia ja yhdessä lainsäädännön uudistamisen kanssa Suomella on mahdollisuus nousta pohjoismaiden johtavaksi maaksi teknologian suhteen. Suomesta puuttuu eritelty lainsäädäntö kryptovaluutoille, mutta muutoksia tilanteeseen on luvassa lähitulevaisuudessa (Giaglis ym., 2021).

Vuonna 2018 toteutetussa kuntien tietotekniikkakartoituksessa selvisi, että 31 vastanneesta kunnasta 20 prosentilla on ainakin osittain käynnissä lohkoketjuhankkeita. Lisäksi kaikissa vastanneissa kunnissa oli suunnitteilla käynnistää hankkeita seuraavan kolmen vuoden sisällä. Vielä tuolloin ei kunnilla kuitenkaan ollut konkreettisia julkaistuja lohkoketjutoteutuksia (Hyvärinen & Parviainen, 2018). Esimerkkinä yksityisistä suomalaisista lohkoketjuhankkeesta oli S-ryhmän Kuhatutka, jonka tarkoituksena on tehdä ruokaketjusta läpinäkyvää. Sovellus oli edelläkävijä elintarvikealan lohkoketjumukautuksessa vuonna 2018 (Rahkola, 2019).

TAULUKKO 3 Lohkoketjuteknologioita hyödyntävät hankkeet Suomessa (Rahkola, 2019)

Hanke tai palvelu	**Toteutusorganisaatio**
Lohkoketjuteknologian ja ohjelmoitavan rahan hyödyntämismahdollisuudet palkkatulojen verotuksessa. Hankkeen toteutus: 3/2018–3/2019.	Valtioneuvoston kanslia/valtiovarainministeriö, VN TEAS –tutkimushanke
Lohkoketjuteknologian mahdollisuudet ja hyödyt sosiaali- ja terveydenhuollossa. Hankkeen toteutus: 2/2017–1/2018.	Valtioneuvoston kanslia/valtiovarainministeriö, VN TEAS –tutkimushanke
SEED-valmisteverotuksen järjestelmän testaaminen Hyperledger-alustalla (Proof-of-Concept).	Verohallinto (EU-hanke: komissio + 8 EU-maata)
Digitaalinen asunto-osakekauppa (www.dias.fi) mahdollistaa asunto-osakekaupan toteuttamisen täysin digitaalisena palveluna. Palvelu on toteutettu yritysten ja viranomaisten yhteistyönä.	DIAS (Digitaalinen asunto-osakekauppa)
Tavoitteena on luoda uutta arvoa avoimen kehitysalustan avulla toimitusketjuprosesseihin ja niihin liittyvään tiedon yhdistelyllä.	DBE (Digital Business Ecosystem) Core -konsortio
Ammattikuljettajille tarkoitetun lohkoketjuun perustuvan uuden palvelun pilotointihanke	Trafi, Liikennelabra, Suomen tilaajavastuu
AuroraAI toimii hajautettuna verkostona, jossa eri toimijat yhdessä muodostavat tekemiselle päämäärän. AuroraAI kehittää tapoja, joilla tehokkaimmin voidaan luoda markkinoita ihmiskeskeisten ja ennakointikykyisten hyvinvointipalveluiden tuottajille tilanteessa, jossa digitaalisten palveluiden tuotantoon yhä enemmän osallistuvat oppivat tekoälyt.	Valtiovarainministeriö, mukana yli 40 organisaatiota ja näissä noin 220 henkilöä
Turvapaikanhakijoiden vastaanottorahan ja palkan maksamiseen tarkoitetut Moni-kortit.	Maahanmuuttovirasto MIGRI
Listaamattomien osakkeiden kaupankäynnin ja osakashallinnan digitalisointi lohkoketjun avulla	Asiakastieto, Nordea, OP Ryhmä, Privanet ja Tieto

Yhteiskunnallisen uskottavuuden ja luotettavuuden lisäämiseksi Suomessa tuli toukokuussa 2019 voimaan laki, joka asettaa velvoitteita lohkoketjujen päällä toimivien kryptovaluuttojen tarjoajille. Laki asettaa edellytyksiä asiakkaiden

varallisuuden suojaamiselle sekä velvoittaa palveluntarjoajan rekisteröitymisen Finanssivalvonnan rekisteriin. Lain määrittämien velvoitteiden täyttäminen voi olla hankalaa ja osa kryptovaluutan tarjoajista joutuu todennäköisesti siirtämään toimintansa muualle. Suurimmaksi ongelmaksi uudessa laissa muodostuu kuitenkin sen tuoma kryptovaluutan määritelmä. Lain mukaan kryptovaluutta ei ole lainmukainen maksuväline, mutta sitä voi silti käyttää maksuvälineenä lohkoketjuympäristössä. Epäselvä lainsäädäntö yhdistettynä sen yrittäjälle tuomiin valvontakustannuksiin vaikeuttavat lohkoketjupohjaisten palveluiden toteuttamista ratkaisevasti (Rahkola, 2019).

Kryptovaluuttojen verotus määräytyy Suomessa Verohallinnon vuonna 2020 antaman ohjeistuksen perusteella. Inbotin toimitusjohtaja Mikko Alasaarela toteaa eduskunnalle kirjoittamassaan asiantuntijalausunnossa Suomen verotusmallin olevan syrjivä ja estävän Suomen nousun teknologian globaaliin eturintamaan. Verohallinto luokittelee kaikki kryptovaluutat käyttötarkoituksesta riippumatta yhteen kategoriaan, mikä johtaa syrjivään verotukseen yksityishenkilön muihin sijoitusmuotoihin nähden. Alasaarelan mukaan tasa-arvoinen verotus vaatisi kryptovaluutan verotuksen määrittämisen niiden käyttötarkoituksen mukaan (Alasaarela, 2018).

Suomessa veroseuraamuksiin johtaa muun muassa valuutanvaihto sekä louhiminen. Mikä tahansa tapahtuma, jossa kryptovaluuttaa vaihdetaan toiseen kryptovaluuttaan, myydään virallista valuuttaa vastaan tai käytetään hyödykkeiden ostamiseen, realisoi sen arvonnousun. Mikäli kryptovaluutan arvo on noussut sen hankintahetkestä, verotetaan arvonmuutos pääomatulona. Erissä hankittu kryptovaluutta katsotaan käytetyksi sen hankintaerien aikajärjestyksen mukaan vanhimmasta uusimpaan. Vaikka kryptovaluuttoja ei kohdella Suomessa arvopapereina, voi kaupankäynnistä koituneet tappiot vähentää verotuksessa (Verohallinto, 2020).

Kahta epävirallista valuuttaa keskenään vaihdettaessa voi ilmaantua tilanne, jossa kummankaan vaihdon kohteena olevan valuutan euromääräistä arvoa ei voida määrittää. Tällöin vaihdossa saatujen rahakkeiden arvoksi merkitään luovutettujen rahakkeiden alkuperäinen euromääräinen hankintahinta. Tapahtumasta ei koidu veroseuraamuksia ennen kuin vaihdossa vastaanotettua valuuttaa käytetään uuteen transaktioon (Verohallinto, 2020).

Proof of work-konsensusmenetelmää hyödyntävälle lohkoketjuverkolle laskentatehoaan luovuttanut louhija saa korvaukseksi kryptovaluuttaa. Tämä rahanarvoinen palkkio nähdään verotuksen näkökulmasta ansiotulona. Louhinnasta saatu tuotto realisoituu, kun se siirtyy louhijan hallinnoimaan lompakkoon. Vastaanotettujen rahakkeiden (token) verotusarvo määräytyy niiden lompakkoon siirtymisen hetkellä vallitsevan kurssin mukaan. Vaihtoehtoisesti louhija voi käyttää säännöllisiin palkkioihin esimerkiksi kuukauden keskihintaa, olettaen, että hintatiedot ovat johdonmukaisia. Mikäli louhinnalla tienattujen rahakkeiden arvo nousee ennen niiden käyttämistä, realisoituu arvonnousu pääomaverotuksen alaisuuteen. Ansiotulon hankintaan koituneet kulut voi kuitenkin vähentää verotuksessa. Tällaisia kuluja ovat sähkömaksut ja laitehankinnat. Sähkölaskusta voi vähentää verotuksessa

louhinnan osuuden kokonaan. Laitehankinnoissa louhijan on kyettävä todistamaan laitteen käyttöaste tulonhankintaan. Mikäli laitetta käytetään muuhun kuin tulonhankintaan, on vähennettävä osuus pienempi (Verohallinto, 2020).

Proof of stake-konsensusmenetelmää käyttävän verkon ylläpidosta maksettava kryptovaluutta on niin ikään veronalaista tuloa. Omistuksiaan poislukinnut veronalainen saa korvauksena panokseensa verrannollisen määrän uutta valuuttaa. Verotuksen silmin kyseessä on olemassa olevaan varallisuuteen perustuvaa tuottoa, mikä verotetaan pääomatulona. Tämäkin tulos realisoituu verotettavaksi sillä hetkellä, kun se ilmestyy kryptovaluuttaa vastaanottaneen lompakkoon (Verohallinto, 2020).

Alasaarela ehdottaa Saksan verotusmalliin siirtymistä, missä kryptoomistuksia kohdellaan arvopaperien tavoin. Saksassa lainsäädäntö on teknologian suosion kasvulle suotuisampi. kryptovaluuttan käyttäminen hyödykkeiden tai palveluiden suoraan ostamiseen ei aiheuta verotoimenpiteitä. Virtuaalirahakkeen tasa-arvoinen kohtelu virallisen valuutan kanssa mahdollistaa suoraviivaisen ja kustannustehokkaan lohkoketjua hyödyntävä maksutavan kehittymisen. Saksassa louhinta nähdään yleishyödyllisenä, yhteiskunnalle arvoa tuovana, toimintana. Tämän vuoksi louhintatuotoista ei tarvitse maksaa veroja, kannustaen yhä useampia liittymään mukaan lohkoketjuverkkojen ylläpitoon (Alasaarela, 2018).

4.4 Lainsäädäntöä eräissä muissa EU-maissa

Lohkoketjuteknologian lainsäädännön haasteen luo tasapainon löytäminen kepin ja porkkanan välillä. Sääntely ei saa olla liian tiukkaa teknologiaa hyödyntävien yritysten houkuttelemiseksi korkean kansainvälisen kilpailun ilmapiirissä. Löysä sääntely sen sijaan voi mahdollistaa rikollisen toiminnan leviämisen muun muassa rahanpesun muodossa. Lohkoketjujen hajautettu luonne rikkoo rajoja perinteisen lainsäädännön näkökulmasta, mikä haastaa olemassa olevat sääntelyprosessit. Suurimmassa osassa EU-maista lainsäädäntö kohdistuukin teknologian sivutuotteisiin, kryptovaluuttoihin, ollen täten teknologianeutraalia (Rahkola, 2019).

Maltaa voidaan pitää erinomaisena esimerkkinä onnistuneesta lainsäädäntökehityksestä. Sen hyväksymä digitaalisen innovoinnin sääntelykehyksen tuoma suotuisa ilmapiiri on toiminut erinomaisena kannustimena suurille kryptovaluutan vaihtoalustoille. Muun muassa käyttäjämäärissä mitattuna markkinaa hallitseva Binance ilmoitti alkuvuodesta 2018 siirtävänsä hallinnollisen päämajansa Maltalle (Coinmarketcap, 2021). Valtion kantaa kryptovaluuttoihin ja uusiin teknologioihin kuvaa maan pääministerin henkilökohtainen Binancelle suunnattu tervetuliaisjulkaisu Twitterissä. Maltan määrätietoinen ja rohkea ote lainsäädännön suhteen näyttää toimivan ja maahan odotetaan lisää suuria kryptovaluutta-alan toimijoita. Lainsäädäntökokonaisuus ei kuitenkaan ole vielä valmis. Tulevat uudistukset

kohdistuvat muun muassa uusien kryptovaluuttalistautumisten (initial coin offering) valvontaan ja yritysten sertifiointiin (Garg, 2018).

Viro on laatinut lohkoketjuihin vaikuttavan kryptovaluuttalainsäädäntönsä yhtenä ensimmäisistä EU-maista. Virtuaaliset rahakkeet on Virossa jaoteltu neljään eri osa-alueeseen niiden käyttötarkoituksen mukaan. Arvopaperi- ja hyödykerahakkeet luokitellaan niiden myöntämien oikeuksien mukaan. Arvopaperirahake toimii esimerkiksi todisteena yhtiön omistusosuudesta tai äänioikeudesta yhtiön päätöksenteossa. Hyödykerahakkeet sen sijaan toimivat etukäteismaksuina tuotteista tai palveluista. Kolmas rahakekategoria ovat hyväntekeväisyysrahakkeet, joita käytetään vain varainkeruuseen. Nämä rahakkeet eivät tuota ostajalleen minkäänlaista konkreettista hyötyä. Itse kryptovaluutat, joilla voi käydä suoraa kauppaa, luokitellaan maksurahakkeisiin. Näitä rahakkeita verotetaan Virossa tavalliseen tapaan, kuten muutakin veronalaisen vastaanottamaa tuloa (Rahkola, 2019).

5 PÄÄTELMÄT

Lohkoketjuteknologian suurimpia vahvuuksia on sen luotettava hajautettu luonne. Lohkojen sisältämän tiedon eheys varmistetaan yhdistämällä ketjut toisiinsa tiivistefunktioiden avulla ja varastoimalla aidoksi varmistettu tieto ympäri maailmaa. Tällöin tietoa on käytännössä mahdotonta väärentää ilman massiivisia laskentatehoresursseja. Luottamus verkon käyttäjien välille saavutetaan hyödyntämällä konsensusmallien mukaisia protokollia lohkojen luomisen yhteydessä. Ketjun tietoa ei voi muokata kuka tahansa, eikä laajalti hyväksytyn muutoksen suorittaminen ole mahdollista ilman laskentatehoa tai todistetta rahallisesta panoksesta verkossa.

Tutkielman johdannossa määriteltiin tutkimuskysymys: Mitkä ovat Euroopan unionin aikeet lohkoketjuteknologian kehityksen ja sääntelyn suhteen? Euroopan unioni tunnistaa lohkoketjuteknologian potentiaalin ja on luonut strategian tavoitteidensa saavuttamiseksi. Korkein tavoite on maailman kärkipaikan ottaminen teknologian omaksujana ja kehittäjänä. Strategian keskiössä on unionin maiden välinen tiivis yhteistyö ja sen tuomat yhteiset lohkoketjuhankkeet. Euroopan komissiolla on tärkeä rooli strategian läpiviennissä muun muassa rahoittajana. Uusien innovaatioiden ja projektien edistämiseksi apurahapakettien suuruuksia on nostettu ja ammattitaidon saatavuuteen panostettu merkittävästi. Yksi strategian etenemisen ja teknologian kehityksen suurimpia haasteita on onnistuminen lainsäädännössä. Kokonaisen maanosan kansojen käyttöön kehitettävän teknologian on oltava turvallista, jonka saavuttamisessa sääntelyllä on keskeinen rooli. Liian tiukka sääntely sen sijaan karkottaa sijoittajat. Päättäjien on siis löydettävä sääntelyn ja houkuttelevuuden välille tasapaino.

Tämä tutkimus antaa laajan yleiskuvan lisäksi syvemmän katsauksen lohkon muodostamiseen ja vahvistamiseen. Tarkoituksena on, poikkeuksena muista aihetta käsittelevistä tuotoksista, havainnollistaa louhimisprosessia konkreettisesti esimerkkien avulla. Tämän lisäksi on valittuun näkökulmaan, Euroopan unionin sääntelyyn, tehty kattavaa selvitystä. Lainsäädäntö vaihtelee maailmalla valtavasti, minkä vuoksi rajaus on tarpeellinen. Työ valaisee myös sektorin yksityisten toimijoiden roolia lohkoketjuteknologian leviämisessä.

Esimerkiksi kryptovaluutan vaihtoalustat ovat valtavan lainsäädännöllisen paineen alla, ennen täysin säätelemättömän markkinan muovautuessa kohti perinteisempää suuntaa. Juuri kyseiset alustat ovat Euroopan unionille tärkeitä rahantuojia, eli kärsivällisyyttä vaaditaan kummaltakin osapuolelta.

Europan komission strategian ja sen tuoman lainsäädännön onnistumisen määrittelyyn tarvitaan kuitenkin vielä lähivuosien aikana lisätutkimusta. Perusteet onnistumiselle ovat olemassa, mutta siirtymät uusien teknologioiden ja järjestelmien käyttöön sujuvat harvoin täysin suunnitellusti. Lisäksi itse lohkoketjuteknologian konsensusmallirakenne saattaa olla mullistuksen partaalla PoW-mallin vaatiman massiiviseen energiankulutukseen kohdistuvan paineen vuoksi. Ympäristöaktivistit ovat lobanneet mallin kieltämisen puolesta, mikä saattaisi olla lamauttava isku teknologian kehitykselle. EU-tasolla tehtävän kiellon toimeenpanon vaikutusten tutkiminen olisi siis tällä hetkellä ajankohtaista.

LÄHTEET

Alabdulwahhab, F. A. (2018). Web 3.0: The Decentralized Web Blockchain networks and Protocol Innovation. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS), 2018, (1-4,).*

Alasaarela, M. (2018). *Virtuaalivaluutat ja verotus.* Asiantuntijalausunto eduskunnan tulevaisuusvaliokunnalle 3.10.2018. Haettu 7.12.2021 osoitteesta https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-209325.pdf

Almeida, T., Francois, P. & Frénot, S. (2019). Forkmon: Monitoring the Networks Supporting Bitcoin Hard Forks. Haettu osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/stamp/stamp.jsp?tp=&arnumber=8939731

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco R. & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access, vol. 9, (140549-140564)*

Appelbaum, D., & Smith, S. S. (2018). Blockchain basics and hands-on guidance: Taking the next step toward implementation and adoption: Certified public accountant. The CPA Journal, 88(6), 28–37. Haettu osoitteesta https://www.proquest.com/scholarly-journals/blockchain-basics-hands-on-guidance-taking-next/docview/2185467602/se-2?accountid=192583

Berners-Lee, T. (2016). Keynote Address: Re-decentralizing the web - some strategic questions. *Decentralized Web Summit 2016. San Francisco, June 8-9.* Haettu osoitteesta https://archive.org/details/DWebSummit2016_-Keynote_Tim_Berners_Lee

Bitcoin (1.12.2021). Bitcoin's website. Haettu osoitteesta https://bitcoin.org/en/full-node#what-is-a-full-node

Bitstamp (2021, 23. elokuuta). Bitstamp's blog. Haettu 3.12.2021 osoitteesta https://blog.bitstamp.net/post/what-are-blockchain-nodes

Buterin, V. (2013). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. Haettu osoitteesta https://ethereum.org/en/whitepaper/

Coinmarketcap (2021). Top Cryptocurrency Spot Exchanges. Haettu 5.12.2021 osoitteesta https://coinmarketcap.com/rankings/exchanges/

Ehdotus Euroopan parlamentin ja neuvoston asetus varainsiirtojen ja tiettyjen kryptovarojen siirtojen mukana toimitettavista tiedoista (2021) COM (2021) 422 final. Haettu osoitteesta https://eurlex.europa.eu/-resource.html?uri=cellar :08cf467e-ead4-11eb-93a8-01aa75ed71a1.0007.02/DOC_1&format=PDF

Ethereum (28.11.2021). Ethereum's website. Haettu osoitteesta https://ethereum.org/en/dapps/#what-are-dapps

Euroopan parlamentin ja neuvoston asetus 2016/679 (27.4.2016). Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). *Euroopan unionin virallinen lehti 4.5.2016*

European Comission (2021a). European Blockchain Partnership. Haettu 5.12.2021 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/-blockchain-partnership

European Comission (2021b). List of EBP representatives. Haettu 5.12.2021 osoitteesta https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/-List+of+EBP+representatives

European Comission (2021c). Blockchain Strategy. Haettu 7.12.2021 osoitteesta https://digital-strategy.ec.europa.eu/en/policies /blockchain-strategy

European Comission (2021d). European Blockchain Services Infrastructure. Haettu 7.12.2021 osoitteesta https://digital-strategy.ec.europa.eu-/en/policies/european-blockchain-services-infrastructure

European Comission (2021e). Horizon Europe. Haettu 8.12.2021 osoitteesta https://ec.europa.eu/info/research-and-innovation /funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

European Comission (2021f). Blockchain funding and investment. Haettu 8.12.2021 osoitteesta https://digital-strategy.ec.europa.eu/en/policies-/blockchain-funding

European Comission (2021g). The Digital Europe Programme. Haettu 9.12.2021 osoitteesta https://digital-strategy.ec.europa.eu/en/activities/digital-programme

European Comission (2020, 28. elokuuta). First six Artificial Intelligence and Blockchain Technology funds backed by InnovFin raise a total of EUR 700m. Haettu 9.12.2021 osoitteesta https://ec.europa.eu/commission/-presscorner/detail/en/IP_20_1991

Frankenfield, J. (2021a, 22 heinäkuuta). Investopedia: Bitcoin Cash. Haettu 22.12.2021 osoitteesta https://www.investopedia.com/terms/b/bitcoin-cash.asp

Frankenfield, J. (2021b, 25. lokakuuta). Investopedia: 51% Attack. Haettu 15.12.2021 osoitteesta https://www.investopedia.com/terms/1/51-attack.asp

Garg, P. (2018, 3. toukokuuta). The Growth and Development of Malta the "Blockchain Island". Haettu osoitteesta 5.12.2021 https://blockonomi.com/malta-blockchain-island/

Georhiades, Y., Flolid, S. & Vishwanath, S. (2019). HashCore: Proof-of-Work Functions for General Purpose Processors. Haettu osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/stamp/stamp.jsp?tp=&arnumber=8884814

Geroni, D. (2021, 5. huhtikuuta). 101Blockchains: Blockchain Nodes: An In-Depth Guide. Haettu osoitteesta 1.12.2021https://101blockchains.com-/blockchain-nodes/

Giaglis, G., Dionysopoulos, L., Der Avedissian, N., Charalambous, M., Kostopoulos, N., Vlachos, I., Damvakeraki, T., Noszek, Z., Krasnov, H., Chykhradze, K., Oshkhneli, S., Strukov, D., Papoutsoglou, I., Votis, K. (2020). *EU Blockchain Ecosystem Developments.* Haettu 11.12.2021 osoitteesta https://www.eublockchainforum.eu/sites/default/files/reports/EU%20Blockchain%20Ecosystem%20Report_final_0.pdf

Hyvärinen, S. & Parviainen, J. (2018). *Kuntien tietotekniikkakartoitus 2018 - Kuntien tietotekniikan tunnusluvut, organisointi, toiminnan kehittäminen ja haasteet.* Kuntaliitto. Haettu osoitteesta https://www.kuntaliitto.fi/sites-/default/files/media/file/Tietotekniikkakartoitus2018_loppuraportti.pdf

Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle - EU:n digitaalisen rahoituksen strategiasta. COM (2020) 591 final. 24.9.2020. Haettu 10.12.2021 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/PDF-/?uri=CELEX:52020DC0591&from=EN

Kryptovaluutta.fi (2021). Haettu 3.12.2021 osoitteesta https://www.kryptovaluutta.fi/lohkoketju

Lauslahti, K., Mattila, J. & Seppälä, T. (2016). *Älykäs sopimus – Miten blockchain muuttaa sopimuskäytäntöjä?* (ETLA Raportit No 57). Haettu osoitteesta https://www.etla.fi/wpcontent/uploads/ETLA-Raportit-Reports-57.pdf

Li, W., He, M. & Haiquan, S. (2021). An Overview of Blockchain Technology: Applications, Challenges and Future Trends. *IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2021, (31-39)*

Mattila, J. (2016). The Blockchain Phenomenon. Haettu osoitteesta https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-38.pdf

Miraz, M. H. & Ali, M. (2018). Applications of Blockchain Technology beyond Cryptocurrency. *Annals of Emerging Technologies in Computing (AETiC) 2(1),* (1-6). Haettu osoitteesta http://www.aetic.theiaer.org/archive/-v2/v2n1/p1.html

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Haettu t12.12.2021 osoitteesta https://bitcoin.org/bitcoin.pdf.

Notabene (2021a). Crypto Travel Rule in European Union by European Banking Authority (EBA). Haettu 10.12.2021 osoitteesta https://notabene.id/world/eu

Notabene (2021b, 10. lokakuuta). Top 10 Takeaways from the European Commission's Crypto Travel Rule Proposal. Haettu 10.12.2021 osoitteesta https://notabene.id/post/top-10-takeaways-from-the-european-commissions-crypto-travel-rule-proposal

Pinna, A., Ibba, S., Baralla, G., Tonelli R. & Marchesi, M. (2019). A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics, *in IEEE Access, vol. 7,* (78194-78213), 2019, Haettu osoitteesta doi: 10.1109/ACCESS.2019.2921936.

Rahkola, M. (2019). *Katsaus lohkoketjuteknologioiden hyödyntämiseen Suomessa.* Eduskunnan tulevaisuusvaliokunnan julkaisu 1/2019. Haettu osoitteesta https://www.eduskunta.fi/FI/naineduskuntatoimii/julkaisut/Documents/NETTI_TUVJ_1_2019_Lohkoketjuteknologiat.pdf

Ramson, S. R. J., Vishnu, S. & Shanmugam, M. (2020). Applications of Internet of Things (IoT) – An Overview, 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), 2020, (92-95), Coimbatore, India, March 5-6. Haettu osoitteesta doi: 10.1109/ICDCS48716.2020.243556.

Shahsavari, Y., Zhang, K. & Talhi, C. (2019). A Theoretical Model for Fork Analysis in the Bitcoin Network. Haettu osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/stamp/stamp.jsp?tp=&arnumber=8946275

Shobith, S. (2021, 24 elokuuta). Investopedia: Explaining the Crypto in Cryptocurrency. Haettu 21.11.2021 osoitteesta https://www.investopedia.-com/tech/explaining-crypto-cryptocurrency/

Statista.com (2022). Number of daily transactions on the blockchain of Bitcoin. Haettu 22.3.2022 osoitteesta https://www.statista.com/statistics/730806/-daily-number-of-bitcoin-transactions/

Swathi, B. H., Meghana, M. S. & Lokamathe, P. (2021). An Analysis on Blockchain Consensus Protocols for Fault Tolerance. Haettu osoitteesta: https://ieeexplore-ieee-org.ezproxy.jyu.fi/stamp/stamp.jsp?tp=&arnumber=9456310

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. Haettu osoitteesta http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf

Verohallinto (2020). *Virtuaalivaluuttojen verotus.* VH/5083/00.01.00/2019. Haettu osoitteesta https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen-verotus3/

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R. & Wang, F. -Y. (2018) An Overview of Smart Contract: Architecture, Applications, and Future Trends, *2018 IEEE Intelligent Vehicles Symposium (IV), 2018,* (108-113), Changshu, China, June 26-30, 2018

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. arXiv: Cryptography and Security. Haettu osoitteesta https://arxiv.org/ftp/arxiv/papers/1906/1906.11078.pdf