Tampereen yliopisto

Riikka Oksanen

KRYPTOVALUUTTA BITCOIN

Lohkoketjuteknologiaan pohjautuva riskialtis sijoituskohde

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Helmikuu 2021

TIIVISTELMÄ

Riikka Oksanen: Kryptovaluutta Bitcoin – Lohkoketjuteknologiaan pohjautuva riskialtis sijoituskohde
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Helmikuu 2021

Tämän tutkielman tarkoitus oli tutkia kryptovaluutta Bitcoinia sijoittamisen näkökulmasta avaten sen taustalla toimivaa lohkoketjuteknologiaa. Tutkielman aiheen valinta perustuu ajankohtaisuuteen, sillä Bitcoin on ollut vuosina 2020 ja 2021 huomattavasti esillä talousaiheisissa medioissa. Lohkoketjuteknologialla on useita käyttökohteita myös muilla aloilla kuin finanssi- ja rahoitusalalla. Yksi tutkielman tarkoitus oli tuottaa tietoa Bitcoinista sijoituskohteena kiinnostuneille ja auttaa heitä ymmärtämään lohkoketjuteknologian toimintaa. Valitun näkökulman pohjalta tutkimuskysymyksiksi muodostuivat seuraavat kysymykset: (1) Minkälainen teknologia Bitcoinin taustalla oleva lohkoketjuteknologia on, ja mitä se pitää sisällään? (2) Millainen Bitcoin on sijoituskohteena, ja miltä sen tulevaisuus näyttää sijoittamisen näkökulmasta?

Tutkielman menetelmänä oli kirjallisuuskatsaus ja sen lähteinä käytettiin mahdollisimman uusia tieteellisiä artikkeleita ja tutkimuksia. Muita lähteitä olivat aiheeseen liittyvät kirjat, verkkojulkaisut sekä kaksi kandidaatintutkielmaa. Lohkoketjusta sekä Bitcoinista löytyi kattavasti ja laaja-alaisesti lähteitä. Osa käytetyistä lähteistä oli tietojenkäsittelyn julkaisuja ja osa taloustieteen julkaisuja. Monia tutkielmassa käytettyjä lähteitä käytettiin myös muiden tutkimusten lähteinä. Lisäksi monet tutkielmassa käytetyt lähteet olivat tulleet samaan tulokseen Bitcoinista sijoituskohteena, minkä pohjalta tutkielmassa sai muodostettua kattavan kokonaiskuvan niin lohkoketjun toiminnasta kuin Bitcoinista sijoituskohteena.

Lohkoketjuteknologia on pseudonyymillä Satoshi Nakamoto tunnetun tahon kehittämä teknologia, jonka avulla toisilleen tuntemattomat osapuolet voivat luoda ja ylläpitää hajautettua tietokantaa ilman kolmansia osapuolia. Lohkoketjuteknologia hyödyntää tiivistefunktiota, kryptografiaa sekä vertaisverkon ominaisuuksia. Sijoituskohteena Bitcoin vaatii riskinsietokykyä, sillä kryptovaluuttamarkkinoilla suuret arvonvaihtelut ovat tyypillisiä. Bitcoinin tulevaisuutta on hankalaa arvioida ja arviot perustuvat pitkälti spekulaatioon. Vaikka varmuutta Bitcoinin tulevaisuudesta ei ole, lohkoketjuteknologian odotetaan yleistyvän eri alojen käytössä.

Avainsanat: Bitcoin, kryptografia, kryptovaluutta, lohkoketjuteknologia, sijoittaminen, tiivistefunktio

Sisällysluettelo

1 Johdanto

Tässä tutkielmassa käsittelen kryptovaluutta Bitcoinia sijoituskohteena avaten sen taustalla toimivaa *lohkoketjuteknologiaa* (engl. blockchain). Yksi tutkielman tarkoitus oli tarjota tietoa niin, että kuka tahansa Bitcoinista sijoituskohteena kiinnostunut saa riittävän kattavan kuvan lohkoketjuteknologiasta. Valitsin tutkielman aiheen myös, koska sen takana toimivaa teknologiaa voidaan hyödyntää kryptovaluuttojen lisäksi monilla muilla eri aloilla, kuten kirjanpidossa, terveydenhuollossa sekä rahoitus- ja energia-alalla (Euroopan parlamentti, 2018). Sijoittamisen näkökulman taas valitsin siksi, että Bitcoin on ajankohtainen aihe, josta myös uutisoidaan talousaiheisissa medioissa, kuten Kauppalehdessä. Bitcoinin eettisyys herättää usein keskustelua, sillä se kuluttaa valtavasti sähköä ja se yhdistetään rikollisuuteen, mutta en käsittele sitä tässä tutkielmassa.

Tämän lähestymistavan pohjalta tutkimuskysymyksiksi muodostuivat seuraavat kysymykset: (1) Minkälainen teknologia Bitcoinin taustalla oleva lohkoketjuteknologia on, ja mitä se pitää sisällään? (2) Millainen Bitcoin on sijoituskohteena, ja miltä sen tulevaisuus näyttää sijoittamisen näkökulmasta? Viittaan tutkielmassa Bitcoin-sanalla Bitcoin-järjestelmään ja bitcoin-sanalla bitcoin-kolikkoon. Samaa viittaustapaa käyttivät myös Raina ja Sillanpää (2014) omassa tutkielmassaan. Tämän tutkielman tutkimusmenetelmä on kirjallisuuskatsaus, jonka tulee pohjautua aiempiin tutkimuksiin. Käyttämiäni lähteitä etsin hakusanoilla ”bitcoin”, ”bitcoin AND cryptocurrency”, ”cryptocurrency”, ”blockchain”, ”blockchain AND bitcoin” ja ”bitcoin AND investing”. Hakuja tein seuraavista tietokannoista: Andor, IEEE, O'Reilly ja ProQuest.

Tutkielman lähteinä käytin mahdollisimman uusia tieteellisiä ja vertaisarvioituja aiheeseen liittyviä artikkeleita. Yksi relevanteimpia lähteitä oli Bitcoinin kehittäjän Satoshi Nakamoton vuonna 2008 julkaisema teoreettinen malli Bitcoinille. Nakamoton alkuperäinen julkaisu toimi lähteenä myös monissa muissa käyttämissäni lähteissä. Muut käyttämäni lähteet koostuivat mahdollisimman uusista akateemisista tutkimuksista, kryptovaluutta-aiheisista kirjoista sekä sijoittamiseen liittyvien palveluiden, kuten NorthCrypto-palvelun verkkokirjoitelmista.

Osa lähteistä oli tietojenkäsittelyn julkaisuja, osa puolestaan taloustieteen julkaisuja. Koska tämä tutkielma on tietojenkäsittelytieteen kandidaatintutkielma, pääpaino lähteissä on tietojenkäsittelyn julkaisuissa. Monissa lähteissä oli tultu samoihin tuloksiin, joiden pohjalta lähteistä sai muodostettua kattavan kokonaiskuvan niin lohkoketjusta kuin myös Bitcoinista sijoituskohteena. Tarkastelin aluksi myös muita aiheeseen liittyviä kandidaatintutkielmia, joista yhtä käytin tutkielmassani lähteenä, Rainan ja Sillanpään (2014) termien viittauksen lisäksi. Kyseinen tutkielma vertasi hyvin Bitcoinia kuplana 1600-luvun Alankomaiden tulppaanikuplaan (Parviainen, 2018, 12).

Tutkielman aiheen valitsemiseen vaikutti ajankohtaisuuden lisäksi oma mielenkiintoni sijoittamista kohtaan sekä halu tutustua lohkoketjuteknologiaan tarkemmin. Monet suomalaiset ovat sijoittaneet Bitcoiniin jo ennen kuin sen arvo nousi rajusti vuonna 2017, jolloin monet onnistuivat saamaan sillä valtavat tuotot (MikroBitti, 2017; Tivi, 2017; Yle, 2018). Bitcoinin arvo on noussut huomattavasti vuoden 2020 kesän jälkeen, mikä on kasvattanut sen suosiota sijoituskohteena merkittävästi (Ylä-Anttila, 2021b). Siksi onkin erittäin mielenkiintoista seurata sen arvonkehitystä tulevaisuudessa: romahtaako arvo pian, nousisiko arvo romahtamisen jälkeen, vai jatkaako arvo vain nousuaan ilman romahdusta? Bitcoiniin sijoittavan tulee kuitenkin ymmärtää, että riski koko pääoman menettämiseen on suuri (NorthCrypto, 2020b).

Kesän 2020 jälkeen yhden bitcoinin arvo on noussut noin 400 prosenttia ylittäen 50 000 dollarin rajan vuoden 2021 helmikuussa. Se tekee euroissa yli 42 000 euroa bitcoinilta. Tämän tutkielman kirjoittamisen aikana yhden bitcoinin arvo on noussut 30 000 dollarista yli 50 000 dollariin. (Investing.com, 2021a, Ylä-Anttila, 2021b). Bitcoinin arvonnousussa on yhtäläisyyksiä myös sähköautojen valmistaja Teslan voimakkaasti nousseeseen osakkeen arvoon, johon Bitcoinia usein verrataan. Teslan osakkeista moni on kuullut puhuttavan kuplana, joka spekulaatioiden mukaan puhkeaa jossakin vaiheessa.

Lohkoketjuteknologia ei ole nykyisin enää uusi teknologia, ja se hyödyntää erilaisia teknologioita ja tekniikoita, joista kerron tässä tutkielmassa. Sijoituskohteena Bitcoin on riskialtis ja siihen liittyy monia erilaisia riskejä, joita ei esimerkiksi perinteisiin sijoituskohteisiin liity (FIN-FSA, 2019; Hu ja muut, 2019, 4). Lisäksi Bitcoinin tai yleisesti kryptovaluuttojen tulevaisuutta ei kukaan pysty tietämään etukäteen. Siksi tulevaisuuden näkemykset eroavatkin toisistaan huomattavasti ja ne pohjautuvat pääsääntöisesti spekulaatioon (M2 Presswire, 2020; Zaghloul ja muut, 2020, 10289).

Seuraavassa luvussa (luku 2) esittelen tutkielman keskeiset käsitteet. Käsitteiden esittelyn jälkeen kerron lyhyesti kryptovaluutoista (luku 3), jotta lukija saa lyhyen kuvauksen niistä yleisesti. Sen jälkeen perehdyn Bitcoiniin (luku 3.1) ja vertaan sitä lyhyesti kryptovaluutta Ethereumiin (luku 3.2). Niiden jälkeen avaan lohkoketjuteknologiaa tarkemmin (luku 4), kyseinen luku on jaettu seuraaviin alalukuihin: tiivistefunktio (luku 4.1), Proof-of-Work ja bitcoinin louhinta (luku 4.2), vertaisverkko ja konsensus (luku 4.3), kryptografia (luku 4.4), ja kryptovaluuttalompakot (luku 4.5).

Muutamiin lohkoketjuteknologian alalukuihin on sisällytetty kuvia eri teknologisten aiheiden havainnollistamiseksi. Lisäksi luvut ja alaluvut pyrkivät etenemään loogisessa järjestyksessä, jossa edellinen luku liittyy aina seuraavaan lukuun. Luvun 4 jälkeen tarkastelen Bitcoinia sijoituskohteena (luku 5), siihen liittyviä riskejä (luku 5.1) sekä lyhyesti Bitcoinin tulevaisuutta sijoittamisen sekä lohkoketjuteknologian yleistymisen näkökulmasta (luku 5.2). Lopuksi kokoan yhteen tutkielman sisältöä ja muodostan vastaukset tutkimuskysymyksiin (luku 6).

2 Keskeiset käsitteet

Keskeisiä käsitteitä tässä tutkielmassa ovat Bitcoin, konsensus, kryptografia, kryptovaluutta, kryptovaluuttalompakko, lohko, lohkoketjuteknologia, louhinta, transaktio, tiivistefunktio sekä vertaisverkko. Tässä luvussa esitellään tutkielman keskeiset käsitteet lyhyesti.

Bitcoin = Bitcoin on pseudonyymi Satoshi Nakamoton vuonna 2008 kehittämä kryptovaluutta, joka hyödyntää lohkoketjuteknologiaa. Bitcoinin pienintä siirrettävää osaa kutsutaan satoshiksi, joka on 0.00000001 bitcoinia. (Frisby, 2014, 2–5; Hu ja muut, 2019, 1; Nakamoto, 2008, 1–8; Zaghloul ja muut, 2020, 10288)

Konsensus = Vertaisverkko noudattaa konsensusprotokollaa uusien lohkojen hyväksymiseksi lohkoketjuun. Kun vertaisverkossa on saavutettu konsensus, transaktion tiedot sisältävä lohko liitetään lohkoketjuun aiempien lohkojen jatkeeksi. Transaktio ja vertaisverkko määritellään myöhemmin tässä luvussa. (Bouraga, 2020, 2–3)

Kryptografia = Kryptografia on tiedon salaukseen keskittyvä tieteenala, jota hyödynnetään lohkoketjuteknologiassa. Bitcoin hyödyntää julkisen avaimen salausmenetelmää, jossa käytetään julkista ja yksityistä avainta kryptovaluuttojen siirtämiseen ja vastaanottamiseen kryptovaluuttalompakossa. (Franco, 2015, 51–52, 123–124; Nakamoto, 2008, 1–8)

Kryptovaluutta = Kryptovaluutat ovat hajautettuja digitaalisia virtuaalivaluuttoja, joista tunnetuin ja menestynein on Bitcoin ja toiseksi tunnetuin Ethereum. Kryptovaluutat hyödyntävät lohkoketjuteknologiaa hajauttamisen saavuttamiseksi. Kryptovaluutat kehitettiin alun perin vaihtoehtoiseksi tavaksi siirtää rahaa. (Franco, 2015, 3; Zaghloul ja muut, 2020, 10288)

Kryptovaluuttalompakko = Kryptovaluuttalompakko on sovellus, joka sisältää käyttäjän avainpareja, eli julkisia ja yksityisiä avaimia. Bitcoinin kohdalla lompakkoa kutsutaan usein lyhyesti bitcoin-lompakoksi. Lompakko on pääsääntöisesti tiedoston muodossa oleva yksityinen avain, josta kryptovaluutta-varoihin pääsee käsiksi. Kryptovaluuttalompakko voi olla laite-, ohjelmisto- tai paperinen lompakko. Lompakko-termi on hieman harhaanjohtava, sillä kryptovaluutta-varat eivät sijaitse lompakossa, vaan lohkoketjussa. (Antonopoulos, 2017; Kaushal ja muut, 2017, 172; Szmigielski, 2016, 1–23; Zaghloul ja muut, 2020)

Lohkoketjuteknologia = Lohkoketjuteknologia on yksi tämän päivän suurimmista trendeistä ja mahdollisuuksista. Se mahdollistaa julkisen ja hajautetun tietokannan toisilleen tuntemattomien osapuolten välille. Bitcoin-järjestelmässä lohkoketju mahdollistaa maksutapahtumat ilman kolmatta osapuolta. Lohkoketju koostuu lohkoista, jotka sisältävät tietoja ja ovat yhteydessä toisiinsa. Lohkoketju on siis dataa ketjun muodossa. (Dhulavvagol ja muut, 2020, 2507; Franco, 2015, 105–106; Nakamoto, 2008, 2–4; Zaghloul ja muut, 2020, 10288)

Lohko = Lohko on lohkoketjun osa, johon Bitcoin-järjestelmän transaktioiden tiedot ovat tallennettu. Jokaisesta lohkosta lasketaan tiivistefunktiolla tiiviste, ja edellisen lohkon tiiviste sisällytetään aina seuraavaan lohkoon. Tiivisteen ja transaktion tietojen lisäksi lohkot tallentavat transaktion aikaleiman. Lohkoihin voidaan tallentaa mitä tahansa dataa, josta halutaan pitää kirjanpitoa. (Nakamoto, 2008, 2–3, 6; Zaghloul ja muut, 2020)

Louhinta = Bitcoinien louhinnalla tuotetaan uusia bitcoineja. Louhinta on transaktioiden suorittamiseen liittyvä toiminto, jolla kaikki transaktiot suoritetaan ja lisätään hyväksymisen kautta osaksi lohkoketjua. (Franco, 2015, 143)

Transaktio = Transaktiolla tarkoitetaan tapahtumaa Bitcoin-verkossa. Tapahtumia ovat esimerkiksi bitcoinien lähettäminen ja vastaanottaminen (Nakamoto, 2008, 1–2). Taloustieteessä transaktiolla tarkoitetaan yksittäistä kauppaa.

Tiivistefunktio = Jokaisen lohkoketjun lohkon sisällöstä lasketaan tiivistefunktiolla tiiviste. Edellisen lohkon tiiviste sisällytetään aina seuraavaan lohkoon. Bitcoin hyödyntää SHA256-tiivistefunktiota kahteen kertaan, mikä tekee tiivisteestä turvallisemman. (Lone & Naaz, 2020, 2–4; Nakamoto, 2008, 2–5; Song, 2019)

Vertaisverkko = Vertaisverkko on lohkoketjuteknologian ominaisuus. Vertaisverkossa ei ole perinteisissä verkoissa olevia kiinteitä palvelimia, vaan jokainen verkossa oleva käyttäjä toimii palvelimena verkon muille käyttäjille. Tärkein vertaisverkon ominaisuus on se, että transaktion tiedot saavuttavat nopeasti kaikki verkon käyttäjät, joiden tulee saavuttaa transaktion tiedoista konsensus. Tällöin transaktiot hyväksytään muiden käyttäjien toimesta osaksi lohkoketjua, eikä kolmannen osapuolen toimesta. (Zaghloul ja muut, 2020, 10290)

3 Kryptovaluutta yleisesti

Kryptovaluutta (engl. cryptocurrency) on digitaalinen virtuaalivaluutta, joka hyödyntää lohkoketjuteknologiaa (Franco, 2015, 3). Vuonna 2008 kehitettiin ensimmäinen kryptovaluutta Bitcoin, joka on tänäkin päivänä tunnetuin ja suosituin kryptovaluutta (Beck, 2018, 54; Nakamoto, 2008; 1–8). Kryptovaluuttojen suosio nousi vuonna 2017 räjähdysmäisesti, ja ne ovat edelleen ajankohtainen aihe eri medioissa. Kryptovaluuttojen määrä on tunnusomaisesti rajattu toisin kuin perinteisten käteisvaluuttojen: esimerkiksi bitcoinin enimmäismäärä on 21 miljoonaa kappaletta, joista on louhimatta enää noin 3 miljoonaa kappaletta. Bitcoinin markkina-arvo vuoden 2021 alussa oli 779,75 miljardia dollaria. (Investing.com, 2021a)

Alun perin kryptovaluutat luotiin siksi, että haluttiin luoda raha, joka on riippumaton rahoituslaitoksista. Niiden kokonaismäärä on rajattu, jotta keskuspankit eivät voi luoda lisää valuuttaa markkinoille. (Beck, 2018, 54; Bergman, 2021; Nakamoto, 2008, 1–2) Kryptovaluutat hyödyntävät lohkoketjuteknologiaa ja lähes kaikkia lohkoketju-projekteja nimitetään yleisesti kryptovaluutoiksi, sillä eri kategorioiden nimet eivät ole vielä vakiintuneet. Esimerkiksi Bitcoinilla ja Ethereumilla on suuria eroavaisuuksia, mutta silti ne molemmat mielletään kryptovaluutoiksi. (Dhulavvagol ja muut, 2020; Zaghloul ja muut, 2020, 10288)

Vuoden 2017 lopun jälkeen uutisoitiin miljonääreistä, jotka olivat rikastuneet sijoittamalla kryptovaluuttoihin (MikroBitti, 2017; Tivi, 2017; Yle, 2018). Silloin kryptovaluuttoja ja lohkoketjuteknologiaa pidettiin uutena ilmiönä ja ne nousivat keskiöön, vaikka todellisuudessa ne olivat olleet olemassa jo vuosikymmenen ajan. Viimeisen kolmen vuoden aikana Bitcoin on noussut eniten epäilyksiä, spekulaatiota ja innostusta herättäväksi mediassa pinnalla olevaksi sijoitusinstrumentiksi (Burniske & Tatar, 2017; TechTree.com, 2020a; Vellava, 2019, 66). Bitcoinin perusidea valuuttana on kaikkien ymmärrettävissä, mutta lohkoketjuteknologian, valuuttojen louhinnan ja kryptografisten menetelmien ymmärtäminen vaatii jo enemmän perustietoja aiheesta. Bitcoinin menestyksen myötä on kehitetty myös tuhansia muita kryptovaluuttoja. Niitä kutsutaan nimellä ”*altcoin*”, joka tulee sanoista *alternative to Bitcoins:* vaihtoehto Bitcoinille. (Bouraga, 2020, 1; Sebastião & Godinho, 2021, 2)

3.1 Bitcoin

Talousaiheisia uutissivustoja seuranneet eivät ole voineet välttyä vuoden 2020 lopun ja vuoden 2021 alun uutisoinneilta bitcoinin valtavaan arvonnousuun ja sen uusiin arvonnousuennätyksiin liittyen. Viimeisin arvonnousu tapahtui vuoden 2021 helmikuussa, jolloin yhden bitcoinin arvo ylitti aiemman vuoden 2021 tammikuun ennätyksensä yltämällä jopa 51 000 dollarin arvoon. Tämä arvonnousun on arvioitu aiheutuneen sähköautovalmistaja Teslan 1,5 miljardin dollarin bitcoin-ostosta, jolloin myös Teslan osakkeen arvo nousi. (Investing.com, 2021a; Ylä-Anttila, 2021a, Ylä-Anttila, 2021b)

Bitcoin sai alkunsa, kun vuoden 2008 maailmanlaajuinen finanssikriisi aiheutti pelon koko rahoitusjärjestelmän romahtamisesta, eikä luottamus rahoitusjärjestelmiä kohtaan ole vieläkään täysin toipunut (Beck, 2018, 54; Frisby, 2014, 2–5). Vuonna 2008 Bitcoinin ja lohkoketjuteknologian teoreettisen idean esitti Satoshi Nakamoto, jolloin hän julkaisi kahdeksansivuisen teknisen dokumentin Bitcoinin perustaksi. ”Bitcoin: A Peer-to-Peer Electronic Cash System” -nimisen dokumentin nimi tarkoittaa Bitcoinin olevan sähköinen rahajärjestelmä vertaiselta vertaiselle. Tämä mahdollistaa sähköiset rahasiirrot ilman välikäsiä. (Beck, 2018, 54; Nakamoto, 2008, 1–3)

Bitcoinin tarkoitus oli alun perin olla digitaalisessa muodossa oleva käteinen raha, joka ylläpitäisi kirjaa arvonsiirroista. Lohkoketjun, eli hajautettuun tietokoneverkkoon jaetun kirjanpitojärjestelmän, avulla on tarkoitus estää valuutan kopiointi, useampaan kertaan käyttäminen sekä rahan lisääminen. Täten Bitcoinilla on ideologinen lataus, joka kyseenalaistaa ja kritisoi perinteisiä vallitsevia asiantuntijoita ja instituutioita. Nakamoton tavoite olikin, että Bitcoinista tulisi itsenäinen elektroninen maksujärjestelmä. (Nakamoto, 2008, 1–8; Vellava, 2019, 67)

Suomalainen ohjelmoija Martti Malmi oli ensimmäinen Bitcoinin kehittäjä Nakamoton jälkeen. Hän otti Nakamotoon yhteyttä tarjoten ajatuksiaan ja kykyjään Bitcoinin kehittämisestä. Malmia kiinnosti Bitcoinissa uuden teknologian potentiaali syrjäyttää nykyinen poliittinen järjestelmä. Eli kyse ei ollut vain voittojen saamisesta, vaan kiinnostuksesta teknologiseen innovaatioon, joka antaisi varallisuuden hallinnan yksilöiden käsiin. Rahaa on aiemminkin käytetty poliittisen ja sosiaalisen muutoksen ajamiseen, ja sellaisena myös Bitcoinia on pidetty. (Vellava, 2019, 67–68)

Myös kuvitelma uudistuneesta yhteiskunnasta, jossa vanhat hierarkiat vaihdettaisiin ihmisten voimaantumiseen, yksilöiden päätösvaltaan ja demokratisoitumiseen, vaikutti Malmin kiinnostuksen taustalla. Kyseiseen ideologiaan liittyy vahvasti hajauttamisen käsite, jolla on vaikutusta myös tämän päivän organisaatioiden ja startup-yritysten johtamistyyleihin, joissa hierarkiaa on madallettu ja vastuita hajautettu. (Vellava, 2019, 67–68) Siksi Bitcoinin filosofiaa on kuvattu myös sosioekonomiseksi utopiaksi, joka määritetään vapailla markkinoilla, hajauttamisella ja henkilökohtaisella autonomialla ja jonka IT-ammattilaiset ovat luoneet uuden, avoimen ja rehellisen talouden rakentamiseksi (TechTree.com, 2020b).

Bitcoinin arvonkehitys on ollut hurjaa vuosina 2009–2021 (kuva 1). Vuonna 2009 ensimmäiset bitcoinit luotiin, eli *louhittiin*, jolloin ne olivat käytännössä arvottomia (Frisby, 2014, 4; Investing.com, 2021a). Vuonna 2013 bitcoin koki ensimmäisen suuremman arvonnousunsa, jolloin yhden bitcoinin arvo nousi yli 1000 dollariin. Sen jälkeen alkoi kuitenkin pitkä laskusuhdanne, joka päättyi vuonna 2017 hurjaan arvonnousuun. Silloin yhden bitcoinin arvo ylitti 13 000 dollaria. Huima arvonnousu kuitenkin laski seuraavien vuosien aikana pudottaen yhden bitcoinin arvon alle 5 000 dollariin. Vuonna 2020

bitcoinin arvo ampaisi kuitenkin uudestaan räjähdysmäiseen nousuun ja ylitti 30 000 dollarin arvon. Nyt vuoden 2021 helmikuussa yhden bitcoinin arvo on käynyt jo yli 50 000 dollarissa. Kuvasta 1 nähdään, kuinka vuoden 2020 jälkeen bitcoinin arvo on moninkertaistunut yltäen yli 51 000 dollariin. (Investing.com, 2021a)

Kuva 1. Bitcoinin arvon kehitys vuosina 2013–2021 (Investing.com, 2021a).

3.2 Ethereum

Bitcoinin jälkeen toiseksi suosituin kryptovaluutta on *Ethereum*, joka kehitettiin vuonna 2015. Se on siis huomattavasti nuorempi kryptovaluutta kuin Bitcoin, ja sen kehittäjä on ohjelmoija Vitalik Buterin. Ethereumia kutsutaan usein toisen sukupolven virtuaalivaluutaksi, kun taas Bitcoin on ensimmäisen sukupolven virtuaalivaluutta. Ethereum on lohkoketjuteknologiaa hyödyntävä hajautettu, luotettava ja autonominen tietojenkäsittelyympäristö. Se ei Bitcoinin tavoin ole tarkoitettu virtuaalivaluutaksi, vaan lohkoketjuteknologiaa hyödyntäväksi *alustaksi* (engl. platform), johon voidaan rakentaa erilaisia sovelluksia, kuten *älykkäitä sopimuksia* (engl. smart contract). Ethereumista tekee erityisen se, että sitä voidaan hyödyntää rahasiirtojen lisäksi myös muihin tarpeisiin. Ethereumin kehittäjä Buterin kutsuu lohkoketjuteknologiaa ”taikatietokoneeksi”, johon kuka tahansa voi rakentaa itsensä suorittavia ohjelmia. (Beck, 2018, 54; NorthCrypto, 2021a)

Ethereumin ja Bitcoinin yhtäläisyydet voidaan tiivistää siihen, että ne ovat molemmat kryptovaluuttoja, joita voidaan ostaa, myydä sekä louhia, ja molemmat hyödyntävät lohkoketjuteknologiaa. Ethereum alustalla toimiva avoin lähdekoodi sekä ohjelmoitava lohkoketju mahdollistavat kuitenkin käyttäjien luomat hajautetut sovellukset. Tällöin ohjelmoijat voivat hyödyntää Ethereumia esimerkiksi oman kryptovaluutan suunnitteluun

ja toteutukseen. Ethereum alustalle voi myös tallentaa erilaisia dokumentteja ja kauppakirjoja, kuten testamentin, tiedostoja tai kuvia. (Franco, 2015, 9–19; Li & Whinston, 2019, 20)

Ethereumin ja Bitcoinin eroavaisuus voidaan puolestaan kuvata niin, että Ethereum on ekosysteemi, jota voidaan hyödyntää erilaisissa sovelluksissa. Bitcoin puolestaan on ensisijaisesti pelkästään vaihdannan välineeksi tarkoitettu virtuaalivaluutta. Lisäksi älykkäiden sopimusten suorittaminen lohkoketjussa on uusi ominaisuus, jota Ethereum tukee, mutta Bitcoin taas ei. Älykkäät sopimukset koskevat ohjelmistoja tai sovelluksia, jotka on tallennettu lohkoketjuun, yleensä Ethereum-ketjuun, ja ne toteutetaan ilman ihmistä, kun määritetyt ehdot täyttyvät. (Franco, 2015, 9–19; Li & Whinston, 2019, 20)

Ethereum ei bitcoinin tavoin ollut juuri minkään arvoinen sen alkuaikoina vuosina 2015–2016. Myös ethereum koki kuitenkin vuoden 2017 paikkeilla räjähdysmäisen arvonnousun, jolloin sen arvo nousi yli 1 000 dollariin. Arvo kuitenkin laski bitcoinin tavoin seuraavien vuosien aikana muutaman sadan dollarin paikkeille (kuva 2). Myös ethereum on vuoden 2020 kesän jälkeen taas moninkertaistanut arvonsa. Nyt vuoden 2021 helmikuussa yhden ethereumin arvo on ylittänyt 1 800 dollaria ja ethereumin markkina-arvo on 141,67 miljardia dollaria. Tämän tutkielman teon aikana yhden ethereumin arvo on noussut noin 600 dollarista yli 1800 dollariin. (Investing.com, 2021b)

Kuva 2. Ethereumin arvon kehitys vuosina 2016–2021 (Investing.com, 2021b).

Molempien, bitcoinin ja ethereumin, arvokäyristä (kuva 1 & kuva 2) nähdään, että ne ovat nousseet ja laskeneet suurin piirtein samoina aikoina. Täten niistä toisen arvon romahtamisella on todennäköisesti vaikutusta myös toisen valuutan arvoon. Tosin niiden käyttötarkoituksella on eroa, joten edellä mainittu arvio perustuu spekulaatioon. Lisäksi bitcoi-

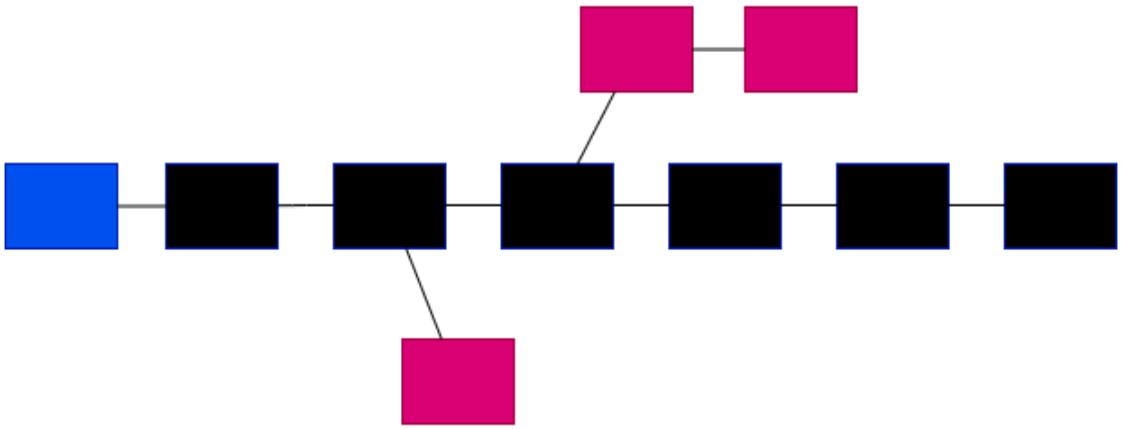
nin ja ethereumin käyristä myös nähdään, että ne ovat nousseet ja laskeneet rajusti olemassaolonsa aikana. Myös Balvers ja McDonald (2017) toteavat tämän artikkelissaan ja mainitsevat, että globaalin digitaalisen valuutan tulisi olla suhteellisen vakaa.

4 Kryptovaluuttojen hyödyntämä lohkoketjuteknologia

Lohkoketjuteknologian on mainittu olevan suurin keksintö internetin jälkeen. Bitcoinin kohdalla lohkoketju varastoi kaikki aiemmat Bitcoin-transaktiot samaan lohkoketjuun, josta kuka tahansa voi niitä tarkkailla. Nykyisin lohkoketjuteknologiaa voidaankin hyödyntää kryptovaluuttojen lisäksi esimerkiksi sähköisissä sopimuksissa, rahan siirtämisessä ja sähköisessä äänestämisessä, eli luottamusta vaativissa tehtävissä. (Beck, 2018, 55–56; Dhulavvagol ja muut, 2020, 2507; Nakamoto, 2008, 2–5; Zaghloul ja muut, 2020, 10288)

Nimi ”lohkoketju” tulee siitä, että kyseessä on monille eri tietokoneille hajautettu transaktioiden ketju (kuva 3). Lohkot ovat linkitetty toisiinsa ja jokainen lohko sopii vain seuraavaan lohkoon. Lohkot tallentavat transaktioiden tiedot, edellisen lohkon tiivisteen sekä transaktion aikaleimauksen. Lohkoketjun toimijoiden henkilöllisyydet eivät paljastu, eli lohkoketju pohjautuu anonyymiyden kautta luottamukseen. (Dhulavvagol ja muut, 2020, 2506–2507; Nakamoto, 2008, 2–3, 6; Zaghloul ja muut, 2020)

Kuvassa 3 on oma hahmotelmani lohkoketjusta, joka alkaa vasemmalta sinisestä suorakulmiosta, joka kuvastaa aivan ensimmäistä lohkoa ketjussa. Kuvassa lohkoketju päättyy oikean reunan mustaan suorakulmioon, joka on viimeisin ketjuun lisätty lohko, eli nykyinen lohko. Mustat suorakulmiot peräkkäin ovat lohkoketjun pääketju, johon kaikki hyväksytyt lohkot lisätään. Punaiset suorakulmiot kuvastavat pääketjun ulkopuolisten haarojen lohkoja, joita ei ole hyväksytty pääketjuun. (Dhulavvagol ja muut, 2020, 2508–2509; Nakamoto, 2008, 1–8)



Kuva 3. Hahmotelmani seitsemän lohkon pituisesta lohkoketjusta mukautuen lähteisiin (Dhulavvagol ja muut, 2020, 2508–2509; Franco, 2015, 109; Nakamoto, 2008, 1–8).

4.1 Tiivistefunktio

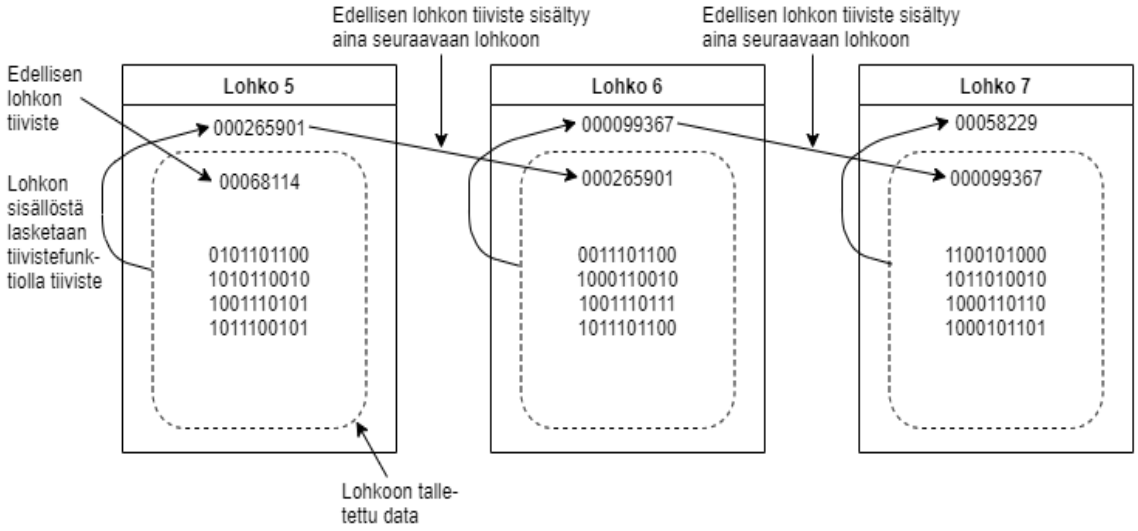
Lohkoketjun lohkoista lasketaan tiivisteet *tiivistefunktiolla* (engl. hash function). Tiivistefunktio on kryptografiaan perustuva matemaattinen algoritmi, joka tekee satunnaisen kokoisesta *syötteestä* (engl. input) kiinteän kokoisen merkkijonon, jota kutsutaan *tiivisteeksi* (engl. hash). Esimerkiksi syötteen ollessa *"I love Bitcoin"* tiivistefunktio antaisi *tulosteena* (engl. output) tiivisteen *"aCb194D11dE".* Tällöin tiivistefunktion ei tule antaa eri syötteestä, esimerkiksi merkkijonosta "*Bitcoin sucks*", samaa tiivistettä *"aCb194D11dE".* (Franco, 2015, 96; Lone & Naaz, 2020, 2–4; Nakamoto, 2008, 2–5)

Tiivistefunktio on *yksisuuntainen tiivistefunktio* (engl. one-way hash function). Tämä tarkoittaa sitä, että ainoa tapa selvittää syöte tiivistefunktion tulosteesta on yrittää *raakavoimalla* (engl. brute-force) etsiä ja kokeilla kaikki mahdolliset syötevaihtoehdot ja katsoa, tuottavatko ne samat tiivisteet. Toisin sanoen, tiivistefunktion tulosteesta ei saada selville funktioon annettua syötettä. (Chowdhury, 2020, 37) Raakavoimahyökkäys voidaan estää lisäämällä tiivistefunktioon annettuun syötteeseen *suola* (engl. salt). Suola on kiinteän pituinen satunnainen arvo. Se lisätään tiivistefunktioiden syötteeseen luomaan yksilöllisiä tiivistearvoja jokaiselle syötteelle, jolloin esimerkiksi kahden identtisen syötteen lasketut tiivistearvot eivät ole samat. Suolausta käytetään esimerkiksi käyttäjien salasanojen säilyttämisessä tiedostoissa tai tietokannoissa. Silloin mahdolliset samat salasanat eivät saa samaa tiivistettä, jolloin hyökkääjän on vaikeampaa selvittää mahdollinen salasana. (Franco, 2015, 98)

Tiivisteen lisäksi jokainen lohkoketjun lohko pitää sisällään *aikaleiman* (engl. timestamp) sekä tiedot hyväksytystä transaktiosta. Jokaisen lohkon sisällöstä lasketaan tiiviste, joka sisällytetään seuraavaan lohkoon, mitä kuvassa 4 havainnollistetaan (kuva 4). Liitettäessä transaktiota lohkoketjuverkostoon transaktion sisältävä lohko saa kopion pääketjun lohkojen tiedoista, joihin sisältyvät kaikki ketjussa aiemmin tehdyt ja hyväksytyt transaktiot. Lohkoketju on luotettava ja läpinäkyvä, sillä kaikki ketjussa tehdyt transaktiot ovat jäljitettävissä ketjun ensimmäiseen lohkoon asti. Lisäksi jälkikäteen lohkon tietojen peukaloimiseksi tulisi muuttaa kaikkien edeltävien lohkojen tietoja, jotta peukaloinnista ei jäisi kiinni. (Franco, 2015, 95–99; Nakamoto, 2008, 2–6)

Tiivistefunktioita on olemassa useita, kuten MD5, SHA1, SHA256 ja SHA512, joista Bitcoin käyttää kaksi kierrosta SHA256-tiivistefunktiota. Funktion käyttäminen kahteen kertaan tekee tiivisteestä turvallisemman estämällä tai hidastamalla joitakin hyökkäyksiä (Franco, 2015, 96; Song, 2019). Ihanteellisella tiivistefunktiolla on viisi ominaisuutta: (1) sama viesti johtaa aina samaan tiivisteeseen, (2) tiivistearvon laskeminen minkä tahansa pituiselle viestille on nopeaa, (3) viestin selvittäminen tiivistearvosta on mahdollista vain kokeilemalla kaikkia mahdollisia yhdistelmiä, (4) pienen muutoksen tekeminen viestiin muuttaa tiivistearvoa niin, että uudella tiivistearvolla ei näytä olevan

yhteyttä vanhan tiivistearvon kanssa, ja (5) kahden eri viestin löytäminen samalla tiivistearvolla on mahdotonta. (Chowdhury, 2020, 37; Franco, 2015, 95–96; Nakamoto, 2008, 3; Zaghloul ja muut, 2020, 10292–10293)



Kuva 4. Havainnollistava ja tarkempi kuvaus lohkoketjun rakenteesta pohjautuen lähteisiin (Chowdhury, 2020, 37; Franco, 2015, 95–99; Nakamoto, 2008, 2–5).

4.2 Proof-of-Work ja Bitcoinin louhinta

Lohkoketjuun talletettua tietoa ylläpidetään hajautetusti vertaisverkossa, jota käsitellään tarkemmin seuraavassa alaluvussa. Verkolla ei ole keskusviranomaista, ja siksi on välttämätöntä, että joku toimii lyhyen ajan johtajana valittaessa seuraavaa lohkoa lisättäväksi ketjuun. Proof-of-Work (lyh. PoW) on algoritmi, joka mahdollistaa kryptovaluutan toiminnan ilman valvovaa kolmatta osapuolta. Se myös ratkaisee valuutan kahteen kertaan käyttämiseen liittyvän ongelman tekemällä siitä todella vaikeaa. PoW toimii niin, että lohkoketjun osallistuvat *solmut* (engl. nodes), joita kutsutaan *louhijoiksi* (engl. miners), valitsevat lyhyen ajan johtajan käyttämällä PoW-algoritmia. Se sitouttaa louhijat etsimään lohkoketjun kriteerit täyttävän tiivisteen. Tiivisteen löytävä solmu valitsee seuraavan lohkon ketjuun, jolloin lohkosta tulee virallinen osa lohkoketjua. Täten Proof-of-Work on välttämätön osa lohkojen lisäämisessä ketjuun ja se toimii ikään kuin jokaisen lohkon aitousleimana vahvistamalla lohkon virallisuuden ja oikeellisuuden. (Beck, 2018, 55; Chowdhury, 2020, 57; Dhulavvagol ja muut, 2020, 2506–2507; Hertig, 2020; Nakamoto, 2008, 3)

Bitcoinien *louhinta* (engl. mining) on transaktioiden suorittamiseen liittyvä toiminto, jolla kaikki transaktiot suoritetaan ja lisätään hyväksymisen kautta osaksi lohkoketjua. Kaikki transaktiot vahvistetaan osaksi lohkoketjua louhintaverkoston avulla, mikä

vaatii laitteiston lisäksi erillisen louhintaohjelman, jolla liitytään Bitcoin-louhintaverkkoon. Louhintaohjelmat hyödyntävät näytönohjaimia, prosessoreja tai mikropiirejä, jotka ovat suunniteltu louhinta-algoritmin suoritukseen. Tällaisia ovat esimerkiksi FPGA-piirit (Field-Programmable Gate Array) tai ASIC-piirit (Application-specific Integrated Circuit). Täten kuka tahansa pystyy aloittamaan bitcoinien louhimisen riittävän laitteiston avulla ja yhdistämällä itsensä Bitcoin-verkkoon. (Franco, 2015; 143–147)

Transaktion hyväksymiseksi Bitcoin-verkon louhijasolmu vahvistaa transaktion tiedot sisältävän lohkon tiivistearvon. Tiivistearvoa verrataan kohdelukuun, joka on 256-bittinen luku, jonka arvoa tiivistearvo ei saa ylittää. Kaikki Bitcoin-verkon louhijasolmut ovat tietoisia kohdearvosta. Kohdearvo kontrolloi lohkojen vahvistamistahtia suhteutettuna Bitcoin-verkon laskentatehoon, jotta lohkojen vahvistaminen tapahtuisi noin 10 minuutin välein. Louhijasolmun löytäessä tiivistearvon, joka on alle kohdearvon, transaktion tiedot sisältävä lohko vahvistetaan osaksi lohkoketjua. Tällöin louhija saa palkkioksi bitcoineja. Käytännössä eniten louhinta-algoritmia suorittanut louhija saa eniten bitcoineja palkkioksi, jolloin *laskentanopeudella* (engl. hash rate) on suuri merkitys. (Chowdhury, 2020, 222)

Louhintaa säädetään säännöllisesti ajan myötä noin 14 päivän välein sen mukaan, kuinka paljon louhijoiden verkko on käyttänyt louhijaverkkoa. Louhinta on kokenut merkittäviä teknisiä muutoksia laskentatehon kasvaessa, ja louhintalaitteisto onkin kehittynyt nopeasti Bitcoinin keksimisestä lähtien. Myös louhintaan käytetyt paikat ovat muuttuneet ajan myötä: louhijat esimerkiksi muuttavat paikkoihin, joissa sähkön hinta on alhainen. (Hu ja muut, 2019, 2)

Nakamoto on määritellyt louhintaverkon koostuvan kuudesta osasta: (1) uusien transaktioiden lähettäminen kaikille verkon solmuille, eli louhijatietokoneille, (2) jokainen solmu kerää uusien transaktioiden tiedot lohkoon, (3) jokainen solmu vahvistaa lohkon PoW-algoritmilla, jonka jälkeen (4) lohko lähetetään kaikille verkon solmuille hyväksytettäväksi, (5) kaikki solmut hyväksyvät uuden lohkon ketjuun, ja (6) solmut vahvistavat lohkon oikeellisuuden ja hyväksymisen siirtymällä työstämään seuraavaa lohkoa käyttämällä viimeksi hyväksytyn lohkon tiivistettä seuraavan lohkon tiivisteenä. (Nakamoto, 2008, 3)

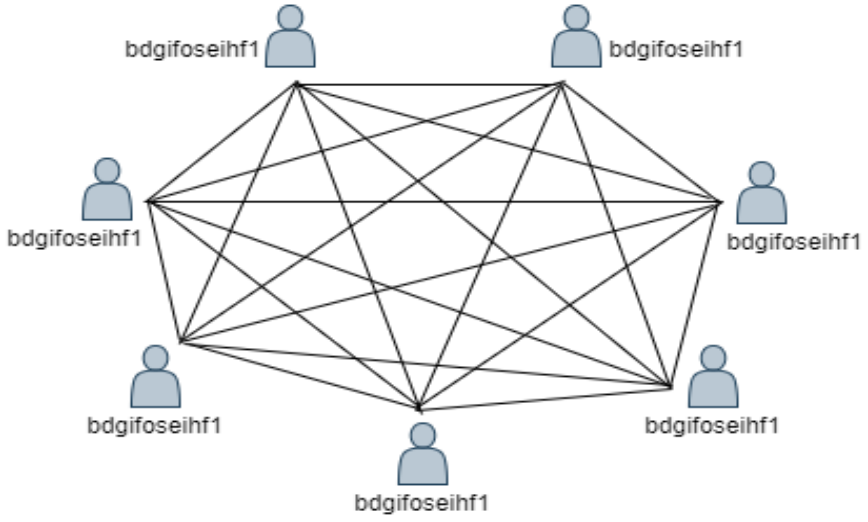
Ensimmäisen 210 000 lohkon vahvistamisesta louhija on saatu palkkioksi 50 bitcoinia, mikä tekee nykyisellä bitcoinin arvolla valtavan määrän rahaa. Palkkio kuitenkin puoliintuu noin joka neljäs vuosi, aina 210 000 lohkon vahvistamisen jälkeen. Viimeisin ja kolmas puoliintuminen tapahtui vuoden 2020 keväällä. Aiemmin toteutetut puoliintumiset ovat tapahtuneet vuosina 2012 ja 2016. Tutkielman kolmannen luvun bitcoinin arvokäyrästä (kuva 1) näemme, ettei vuoden 2012 puoliintumisella ollut vaikutusta bitcoinin arvoon ja vuoden 2016 puoliintumisen jälkeenkin arvonnousu tapahtui vasta vuonna 2017. (NorthCrypto, 2020a)

On arvioitu, että puoliintumisen vaikutus näkyy arvossa vasta kuukausien päästä. Käyrästä nähdään (kuva 1), että vuoden 2020 puoliintumisen jälkeen alkoi hurja arvonnousu. Se voi kuitenkin johtua myös kryptovaluuttojen yleistymisestä ja niihin liittyvän tietoisuuden kasvusta. Louhintapalkkion puoliintuminen kuitenkin tarkoittaa, että uusien bitcoinien määrä vähenee, mikä voi nostaa tulevaisuudessa bitcoinin arvoa. Bitcoinia voidaan verrata kultaan, ja nykyisin bitcoineja louhitaan itse asiassa vähemmän kuin ”kultaa kaivetaan”. Jää nähtäväksi, nouseeko bitcoinin arvo seuraavankin puoliintumisen jälkeen, mutta historian perusteella se on mahdollista. (NorthCrypto, 2020a)

4.3 Vertaisverkko ja konsensus

Lohkoketjuteknologia yhdistää tiivistefunktion ja louhinnan lisäksi muitakin teknologioita, kuten vertaisverkkojen tiedonvaihtoa. *Vertaisverkko* (engl. peer-to-peer network) on verkko, joka mahdollistaa transaktion hyväksymisen lohkoketjuun ilman kolmatta osapuolta. Kryptovaluuttojen kohdalla transaktioiden tietojen suojaus, ylläpito ja hyväksyminen tapahtuvat lohkoketjun avulla vertaisverkossa kaikkien verkon käyttäjien toimesta. Tällöin kolmannen osapuolen sijaan transaktiot hyväksytään verkon muiden käyttäjien toimesta. (Hertig, 2020; Nakamoto, 2008, 3–8; Zaghloul ja muut, 2020, 10288–10290)

Vertaisverkko noudattaa kollektiivisesti konsensusprotokollaa (kuva 5) uusien lohkojen hyväksymiseksi lohkoketjuun. Kun konsensus, eli yksimielinen päätös tietystä transaktiosta, on saavutettu, transaktion tiedot sisältävä lohko liitetään lohkoketjun aiempien lohkojen jatkeeksi. Täten Proof-of-Work menetelmää käytetään tämän yksimielisyyden saavuttamisen perustana. Kuvassa 5 on seitsemästä lohkoketjuverkon jäsenestä muodostuva verkosto, jossa jokaisella käyttäjällä on kopio verkon viimeisimmästä lohkosta *bdgifoseihf*. Tällöin vallitsee konsensus. (Beck, 2018, 55; Bouraga, 2020, 1–3; Nakamoto, 2008, 3–8)



Kuva 5. Hahmotelma konsensusmekanismista pohjautuen lähteisiin (Beck, 2018, 55; Bouraga, 2020, 1–3; Nakamoto, 2008, 3–8).

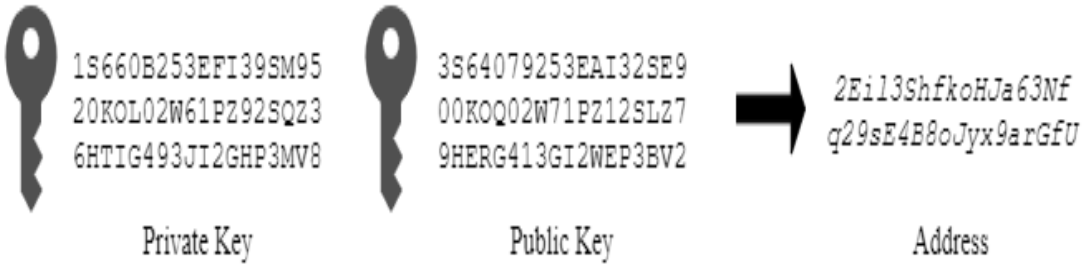
Jos joku kuvan 5 verkon jäsenistä tekisi uuden transaktion, transaktion tiedot sisältävä lohko siirtyisi verkostoon muiden jäsenten hyväksyttäväksi. Tällöin muut jäsenet saisivat ilmoituksen, ettei kaikkien jäsenten viimeisin lohkoversio ole sama. Muilla jäsenillä olisi siis edelleen viimeisimpänä versiona *bdgifoseihf1*, mutta transaktiopyynnön tekijällä viimeisin versio olisi vaikkapa *rkgifoseihf102*. Tässä tapauksessa koko verkoston on hyväksyttävä tai hylättävä transaktiopyyntö, jotta kaikkein viimeisin lohkoversio saadaan samanlaiseksi. (Bouraga, 2020, 1–3)

4.4 Kryptografia

Lohkoketjuteknologia hyödyntää *kryptografiaa* (engl. cryptography), joka on tiedon salaukseen keskittyvä tieteenala. Bitcoin hyödyntää epäsymmetristä salausta, eli julkisen avaimen kryptografiaa, joka on kehitetty jo 1970-luvulla. Epäsymmetristä salausta käytetään siksi, että se mahdollistaa *digitaalisten allekirjoituksien* (engl. digital signature) tekemisen. (Antonopoulos, 2017; Franco, 2015, 51–52) Kryptografian myötä lohkojen sisältö ei ole muokattavissa, käyttäjät ovat anonyymeja ja toteutuneiden transaktioiden muuttaminen jälkikäteen on äärimmäisen vaikeaa. (Lone & Naaz, 2020, 1–3; Nakamoto, 2008, 2–8)

Lohkoketjuteknologian kryptografia perustuu julkiseen ja yksityiseen avaimeen, jotka ovat sarjoja kirjaimia ja numeroita (kuva 6). Henkilön julkinen ja yksityinen avain ovat yksilöllisiä, eikä käyttäjän henkilöllisyys ole selvitettävissä niiden kautta. Henkilön julkinen avain muodostetaan yksityisestä avaimesta, ja se mahdollistaa transaktioiden vastaanottamisen. Julkinen avain on joka kerralla erilainen, mutta se luodaan kuitenkin aina samasta yksityisestä avaimesta (kuva 6). Yksityinen avain puolestaan mahdollistaa pääsyn bitcoin-lompakon sisältöön. (Antonopoulos, 2017; Lone & Naaz, 2020, 1–3)

Julkisesta avaimesta voidaan johtaa *osoite* (engl. address), johon esimerkiksi bitcoinit voidaan lähettää. Bitcoin-osoitetta kutsutaan myös *digitaaliseksi sormenjäljeksi* (engl. digital fingerprint). Se on satunnainen numeroista ja kirjaimista koostettu merkkijono, esimerkiksi *”2Eil3ShfkoHJa63Nfq29sE4B8oJyx9arGfU”* (kuva 6). Osoite voidaan antaa lähettäjälle aivan kuten sähköpostiosoite tai tilinumero. Vastaavasti yksityinen avain on verrattavissa tunnistautumiseen, kuten salasana, allekirjoitus, pankkitunnukset tai mobiilivarmenne. Yksityistä avainta voidaan kutsua digitaaliseksi allekirjoitukseksi, joka todentaa transaktiot aidoiksi ja bitcoinit alkuperältään oikeaksi. (Antonopoulos, 2017; Lone & Naaz, 2020, 1–3; Nakamoto, 2008, 2–8; Song, 2019)



Kuva 6. Hahmotelmani yksityisestä avaimesta, julkisesta avaimesta sekä bitcoin-osoitteesta pohjautuen lähteeseen (Antonopoulos, 2017).

On ehdottoman tärkeää, että yksityinen avain pysyy salassa ja tallessa. Vieraan henkilön saadessa toisen henkilön yksityisen avaimen haltuunsa on hänellä myös pääsy toisen henkilön bitcoin-lompakon sisältöön. Vastaavasti jos yksityinen avain katoaa, ei lompakon omistajalla ole enää pääsyä lompakon varoihin. Julkisen avaimen voi puolestaan kertoa muille, kuten aiemmin jo todettiin. (Antonopoulos, 2017; Lone & Naaz, 2020, 1–3)

Avainten luominen voidaan rinnastaa luvun valitsemiseen väliltä $1–2^{256}$. Tarkalla menetelmällä ei ole väliä, kunhan se ei ole ennustettavissa tai toistettavissa. Bitcoin-järjestelmä käyttää satunnaislukugeneraattoreita tuottamaan 256-bittiä *entropiaa*, eli satunnaisuutta. Tarkemmin ottaen yksityinen avain voi olla mikä tahansa luku, joka määritetään Bitcoinin käyttämällä elliptisen käyrän salausmenetelmällä. Tällöin avaimeksi valitaan satunnainen 256-bittinen luku, joka on pienempi kuin vakio $n = 1{,}1578 * 10^{77}$. Ohjelmoinnin kannalta edellä mainittu toteutetaan syöttämällä kryptografisista lähteistä muodostettu laajahko satunnainen merkkijono SHA256-tiivistefunktioon, joka tuottaa 256-bittisen luvun. Luvun valinta on onnistunut, jos luku on pienempi kuin n. Jos niin ei ole, tulee kokeilla toisella satunnaisluvulla. (Antonopoulos, 2017)

Yksityisestä avaimesta muodostettu digitaalinen allekirjoitus toteutetaan algoritmilla, esimerkiksi algoritmilla *Elliptic Curve Digital Signature Algorithm,* (ECDSA). Tällöin $eG = P$, jossa e on yksityinen avain, G bittijono ja P julkinen avain. Julkinen avain johdetaan yksisuuntaisten salausalgoritmien avulla yksityisestä avaimesta niin, että yksityisen avaimen päättely julkisesta avaimesta on lähes mahdotonta (kuva 6). Tällöin esimerkkinä tarvittava avaintoiminto julkisen avaimen selvittämiseen on $P = eG$. P voidaan laskea helposti, kun e ja G tunnetaan, mutta avainta e ei voida helposti laskea, kun tunnetaan P ja G. (Song, 2019)

4.5 Kryptovaluuttalompakot

Kryptovaluuttalompakko (engl. cryptocurrency wallet) on sovellus, joka sisältää käyttäjän julkisia ja yksityisiä avainpareja. Avaimet ovat täysin irrallaan lohkoketjujärjestelmästä ja internetistä, sillä ne luodaan ja säilytetään kryptovaluuttalompakoissa. On olemassa ohjelmistolompakoita ja laitteistolompakoita, mobiili- ja työpöytäversiota sekä paperisia lompakoita. Paperisella lompakolla tarkoitetaan yksityisen avaimen kirjaamista

paperille ja paperin säilyttämistä turvallisessa paikassa. Yksityinen avain voidaan säilöä paperille esimerkiksi QR-koodin muodossa, jolloin sen saa helposti muutettua digitaaliseksi. On myös isännöityjä lompakoita, joita esimerkiksi palveluntarjoajat ylläpitävät käyttäjien mukavuuden vuoksi. (Antonopoulos, 2017; Franco, 2015, 123–124; Kaushal ja muut, 2017, 172; Szmigielski, 2016, 1–2)

Sekä Szmigielski (2016), että Zaghloul kumppaneineen (2020) mainitsevat lompakko-termin olevan hieman harhaanjohtava, sillä bitcoinit eivät sijaitse niissä, vaan lohkoketjussa. Bitcoin-lompakot vain mahdollistavat pääsyn lohkoketjuun sekä bitcoin-siirrot henkilöltä toiselle, joten ilman niitä koko Bitcoin-järjestelmä olisi hyödytön. Bitcoin-lompakko myös mahdollistaa Bitcoin-järjestelmän tutkimisen, sillä sen avulla voi tarkastella tietoja järjestelmästä, lohkoketjusta ja louhinnasta. Tulee kuitenkin tiedostaa, että kaikissa lompakkotyypeissä on omat riskinsä, eikä mikään lompakkotyyppi suojaa bitcoin-varoja kaikkia mahdollisia uhkia vastaan. (Szmigielski, 2016, 1–23; Zaghloul ja muut, 2020)

Kryptovaluuttalompakot voidaan jakaa deterministisiin, indeterministisiin ja hierarkkisesti determinoituihin lompakoihin. Indeterministiset lompakot eivät ole käytännöllisiä, ja ne pyritään korvaamaan deterministisillä lompakoilla. Deterministisen lompakon idea on, että se sisältää yhdestä lähteestä luotuja yksityisiä avaimia, joista käyttäjä voi luoda monia eri osoitteita yhteen lompakkoon. Armory on varhainen bitcoin-lompakko, joka on ensimmäisenä esitetty deterministinen lompakko. (Franco, 2015, 132–136; Song, 2019)

Kryptovaluuttalompakoihin on kehitetty myös standardeja, kuten BIP0032 ja BIP0044. BIP0032-lompakoissa, eli hierarkkisesti determinoiduissa (lyh. HD) lompakoissa on useita kerroksia ja avaimia, jotka ovat arvojärjestyksessä. Niiden tekniset tiedot on määritelty BIP0032-standardissa. Vastaavasti BIP0044-standardi määrittelee, mitä kukin BIP0032-hierarkian taso voi tarkoittaa. Monet lompakot, kuten Trezor ja Coinomi, toteuttavat molemmat standardit, kun taas jotkut lompakot ohittavat BIP0044:n kokonaan ja käyttävät omaa BIP0032-hierarkiaansa. Niin tekeviä lompakoita ovat esimerkiksi Electrum ja Edge. (Song, 2019)

5 Bitcoin sijoituskohteena

Tietoisuus kryptovaluutoista on kasvanut huomattavasti viimeisten vuosien aikana ja monet sijoittajat ovat onnistuneet tekemään niillä suuria voittoja. Rahoitusasiantuntijoiden mielipiteet vaihtelevat huomattavasti Bitcoiniin liittyen: jotkut ylistävät sitä tulevaisuuden maksutapana, kun taas toiset varoittavat sen epävakaista arvonnousuista ja arvon romahtamisesta. Näistä mielipiteistä huolimatta Bitcoinin suosio kasvaa edelleen, ja monet hyödyntävät sen korkeaa valuuttakurssia tuottoisana sijoituksena. (TechTree.com, 2020a)

Bitcoin ja muut kryptovaluutat ovat saaneet suurten arvonvaihtelujen myötä nopeasti mainetta puhtaana spekulatiivisena omaisuutena. Siksi sijoittajan tulee ymmärtää, että kryptovaluuttamarkkinoiden suuret arvonnousut ja -laskut sekä markkinoiden manipuloinnit ovat jokapäiväisiä tapahtumia kryptomarkkinoilla. Suurten arvonvaihtelujen myötä kryptovaluutat eivät sovi heikkohermoiselle sijoittajalle, sillä kärsimätön sijoittaja voi tehdä harkitsemattomia päätöksiä. Tällöin riski pääoman menettämisestä kasvaa entisestään. (NorthCrypto, 2020b; Sebastião & Godinho, 2021, 2)

Kryptovaluuttoihin sijoittaminen ei ole nykyään enää kovin hankalaa, kuten ei osake- tai rahastosijoittaminenkaan. Tämä johtuu siitä, että palveluntarjoajien määrä on kasvanut, tiedon määrä lisääntynyt, eikä kryptovaluuttoihin sijoittavalta vaadita esimerkiksi niiden säilyttämistä (Burniske & Tatar, 2017). Suomessa rekisteröityjä kryptovaluuttojen tarjoajia ovat esimerkiksi NorthCrypto, Coinmotion, LocalBitcoins ja Prasos. (NorthCrypto, 2021b; Yle, 2019)

Lánskýn (2016) mukaan kryptovaluutan ikä ja louhinnan jatkuminen ovat merkkejä kryptovaluutan arvon säilymisestä ja pitkäaikaisesta selviytymisestä. Tämä näkemys perustuu siihen, että vuonna 2016 olleista 1278 kryptovaluutoista 688 on ”kuollut”. Kuolleista kryptovaluutoista yli puolet menetti arvonsa ensimmäisen 24 viikon kuluessa, ja vastaavasti 21 kryptovaluuttaa kuoli ensimmäisen 100–124 viikon aikana. Vain 3 kryptovaluuttaa kuoli yli 124 viikon olemassaolon jälkeen, joista yksi kuoli 150–174 viikon jälkeen. Tuolloin vuonna 2016 oli 64 kryptovaluuttaa, jotka olivat olleet olemassa enemmän kuin 124 viikkoa, ja 107 kryptovaluuttaa, jotka olivat olleet olemassa 100–124 viikkoa. (Lánský, 2016, 124–125)

Bitcoin on kryptovaluutoista vanhin, ja se on ollut toiminnassa pian 12 vuoden ajan. Jokainen sen arvonnousu on lisännyt tietoisuutta kryptovaluutoista, kerännyt huomiota medioissa ja houkutellut uteliaita ihmisiä, mutta myös aiheuttanut varoituksia sekä väheksymistä. Uteliaisiin, varoittelijoihin sekä väheksyjiin kuuluu niin virkamiehiä, sijoittajia, pankkialan toimijoita, yrittäjiä kuin tavallisia kansalaisiakin. (Vellava, 2019, 66)

Monet etenkin vanhemmista ihmisistä suhtautuvat kryptovaluuttoihin sijoittamiseen negatiivisesti, mikä voi johtua esimerkiksi kokemuksista aiemmista markkinakuplista, tai uuden vierastamisesta eli *muutosvastarinnasta*. Lisäksi kryptovaluuttoja kritisoivat henkilöt eivät yleensä ole perehtyneet lohkoketjuteknologiaan tai kryptovaluuttoihin, jolloin negatiivinen suhtautuminen voi johtua tiedon puutteesta. (Burniske & Tatar, 2017) Yleinen käsitys myös on, ettei kryptovaluuttojen arvo perustu mihinkään. Todellisuudessa kryptovaluutoiksi nimitetyt projektit, alustat ja niihin pohjautuvat teknologiat kehittävät muutakin kuin virtuaalista valuuttaa, kuten aiemmin mainittuja älykkäitä sopimuksia. (Dhulavvagol ja muut, 2020, 2506–2514; Li & Whinston, 2019, 20; Zaghloul ja muut, 2020, 10288)

Kryptovaluuttojen arvo vaihtelee kysynnän ja tarjonnan mukaan kuten osakkeidenkin arvo. Niiden arvo ei myöskään korreloi perinteisten sijoitusluokkien kanssa. Lisäksi esimerkiksi bitcoinin arvoa nostaa sen rajallisuus: kun kaikki ostavat sitä ja kukaan ei myy, on hinnannousu välttämätöntä. Vastaavasti myös kasvanut mielenkiinto ja innostus kryptovaluuttoja kohtaan voi johtaa valtaviin arvonnousuihin: kun yhä suurempi määrä ihmisiä kiinnostuu niistä, eli kysyntä ylittää tarjonnan. (Sebastião & Godinho, 2021, 2, 4; NorthCrypto, 2020b)

Kryptovaluuttojen hintaan vaikuttaa myös se, mitä tulevaisuuden odotuksia esimerkiksi valuutan kehittäjä tai muut merkittävät tahot antavat tai mitä sosiaalisessa mediassa valuutasta puhutaan ja spekuloidaan. Tästä hyvä esimerkki on Teslan bitcoin-oston aiheuttama suuri arvonnousu vuoden 2021 helmikuussa. Teslan bitcoin-osto on herättänyt spekulaatiota myös Teslan pitkän tähtäimen Bitcoin-strategiasta, jolla voi olla vaikutusta bitcoinin arvoon myöhemmin tulevaisuudessa. (Ylä-Anttila, 2021a)

Lisäksi on merkittävää, että myös institutionaaliset sijoittajat ja muut merkittävät tahot ovat lisänneet viime vuosien aikana kryptovaluuttoja osaksi portfolioitaan. Huomattavaa on myös, että maailman vanhimpiin pankkeihin kuuluva Bank of New York Mellon (BNY Mellon) on kertonut aloittavansa palveluiden tarjoamisen kryptovaluuttojen säilyttämiseksi. Teslan markkinaliikkeen myötä myös muiden suuryhtiöiden, kuten Applen, odotetaan seuraavan Teslan jalanjälkiä tulevaisuudessa. (Erkkilä, 2020; Sebastião & Godinho, 2021, 2; Ylä-Anttila, 2021a; Ylä-Anttila, 2021b)

5.1 Bitcoiniin liittyvät riskit

Bitcoinin avulla rikastuneiden rinnalle kuuluu myös suuri määrä ihmisiä, jotka ovat menettäneet pääomansa tai tehneet tappiota sijoittamalla Bitcoiniin. Sijoituskohteena se voikin olla erittäin tuottoisa, mutta samalla se on myös erittäin riskialtis. (Burniske & Tatar, 2017) Lisäksi kryptovaluuttoja on tuhansia, eikä suurin osa niistä ole noussut julkisuuteen tai suureen suosioon. Siksi sijoittajan tulee kiinnittää erityistä huomiota kryptovaluuttaan tutustumiseen, sillä riski toimia kannattamattomasti tuntemattoman sijoituskohteen suhteen on suuri. Sama pätee kuitenkin kaikkiin sijoituskohteisiin. (NorthCrypto, 2020b)

Kryptovaluuttoja pidetään erityisen riskialttiina. Riskin ottaminen pelottaa monia, mutta se myös usein mahdollistaa suuremmat tuotot vähäriskisiin sijoituskohteisiin verrattuna. (Burniske & Tatar, 2017). Valvovan viranomaistahon puute ja muuttuva lainsäädäntö ovat riskejä kryptovaluuttasijoittamisessa, sillä monissa maissa ei vielä tiedetä, miten suhtautua kryptovaluuttoihin. Täten esimerkiksi bitcoin-kauppaa voidaan hidastaa ja säännellä lainsäädännöllä, tai se voidaan jopa kieltää valtioiden toimesta. Riskinä on, että lainsäädäntöä toteuttavien tahojen tietämys aiheesta ei ole riittävää, jolloin kryptovaluutoille epäedullinen lainsäädäntö on mahdollista. (Hu ja muut, 2019, 2)

Lisäksi, koska kryptovaluutat ovat digitaalisia ja sähköisiä, liittyy niiden säilyttämiseen aina hakkeroimisen ja sitä kautta myös varastamisen riski. Vaikka sijoittaja pitäisi

bitcoin-varojensa tiedot käyttämänsä palveluntarjoajan hallussa eikä omassa bitcoin-lompakossaan, sisältyy siihenkin riski, sillä mainittuja palveluitakin on onnistuttu hakkeroimaan. Tämä riski voidaan poistaa säilyttämällä kryptovaluuttaomistuksia omavalintaisessa lompakossa, mutta myös jokaiseen niistä liittyy omat riskinsä, kuten hakkerointi, salasanan tai yksityisen avaimen unohtaminen, tai esimerkiksi fyysisen lompakon varastaminen tai häviäminen. (NorthCrypto, 2020c)

Bitcoin, kuten muutkaan kryptovaluutat, ei ole viranomaisten tai pankin takaama tai liikkeelle laskema, eikä kryptovaluutoilla ole samanlaista oikeudellista asemaa kuin virallisilla valuutoilla ja rahalla. Tällöin niiden arvonmuodostus ei kuulu viranomaisten valvontaan, mikä vaikuttaa kryptovaluuttojen arvonmuodostumiseen voimakkaasti. Lisäksi niihin liittyvä turvallisuus ja saldo perustuvat vain käyttäjien välisiin luottamussuhteisiin. Siksi ne ovatkin sijoituskohteina spekulatiivisia ja niiden hyödyntäminen maksamisessa vielä toissijaista. Lisäksi Bitcoin ei tarjoa varsinaista tuottoa tai arvoa esimerkiksi osinkojen tai koron muodossa, jolloin tuotto-odotus perustuu siihen, että joku ostaa kryptovaluutan myöhemmin kalliimmalla. Myös sijoittajille annetut tiedot ovat usein puolueellisia, harhaanjohtavia ja puutteellisia. Siksi Finanssivalvonta on varoittanut sijoittajia kryptovaluuttoihin liittyvistä riskeistä. (FIN-FSA, 2019)

Bitcoiniin liitetään usein sijoituskupla etenkin silloin, kun sen arvo on ennätyslukemissa, kuten vuoden 2021 alussa. Silloin oletetaan ja spekuloidaan kuplan puhkeavan ja arvon romahtavan. Bitcoin-kuplaa on verrattu esimerkiksi Alankomaiden 1600-luvun tulppaanimaniaan, jolloin tulppaanisipuleiden hinnat kohosivat rajusti ja lopulta romahtivat. Kiinnostus muita kryptovaluuttoja kohtaan vähentäisi kryptovaluuttamarkkinoiden spekuloitua kuplaa. Silloin muiden kryptovaluuttojen arvo ei pohjautuisi bitcoinin korkeaan arvoon, vaan tapahtuisi jokaisen valuutan ominaisuuksien ja vahvuuksien perusteella. Se ei kuitenkaan automaattisesti poistaisi kuplaa, vaan muuttaisi sitä, sillä sijoituskohteelta haetaan kuitenkin lähtökohtaisesti arvonnousua ja korkeampaa myyntihintaa. (Parviainen, 2018, 12; Sebastião & Godinho, 2021, 3)

Bitcoinin arvonnousujen tutkimustulokset viittasivat kuplan olemassaoloon vuosina 2013–2014, mutta eivät esimerkiksi vuonna 2017, jolloin bitcoinin arvo nousi huomattavasti enemmän kuin vuosina 2013–2014. Kuplan arviointi on haastavaa, sillä tulevat kassavirrat ovat epävarmoja, ja arvio edellyttää näiden arvojen ennustamista koko tulevalle ajanjaksolle. Esimerkiksi bitcoinin kohdalla arvojen ennustus perustuu pääosin spekulaatioon, ja täten myös mahdollinen kupla perustuu spekulaatioon. (Chaim & Márcio, 2018, 222–224)

Tarkastellaan seuraavaksi bitcoinin viimeaikaisia arvonvaihteluita (kuva 1): bitcoinin arvo kävi kaikkien aikojen ennätyslukemissa vuoden 2021 tammikuun alussa. Sen jälkeen arvo romahti muutamaksi päiväksi ennen tammikuun puoliväliä yli 10 prosentilla.

Tämän jälkeen bitcoinin arvo nousi kuitenkin yli 10 prosentilla muutamassa päivässä takaisin lähelle sen aiempia ennätyslukemia. Vielä siitä myöhemmin helmikuun 2021 puolessa välissä bitcoinin arvo kävi uudessa ennätyksessään. NorthCrypton sivuilta tarkistettuna bitcoinin arvo tippui euroina vuoden 2021 tammikuussa yli 31 000 euron arvosta muutamassa päivässä reiluun 25 000 euroon, josta se nousi taas yli 31 000 euroon. Tämän arvonvaihtelun on sosiaalisessa mediassa käytyjen spekulointien perusteella arveltu tapahtuneen siksi, että suuret bitcoin-omistajat kotiuttivat voittojaan myymällä omistuksiaan silloin, kun arvo oli silloin kaikkien aikojen huipussa. Sen seurauksena bitcoinin arvo laski. Vastaavasti spekulaation mukaan he ostivat seuraavina päivinä bitcoineja takaisin halvemmalla, jolloin bitcoinin arvo nousi takaisin muutamassa päivässä.

5.2 Tulevaisuus tuo jännitystä

Tähän asti kryptovaluutoista on tullut pääasiassa voittoa tavoittelevien sijoittajien kohde eikä niinkään maksuväline, millaiseksi esimerkiksi Bitcoin alun perin suunniteltiin ja luotiin. Akateeminen yhteisö on käyttänyt aikaansa kryptovaluuttakaupan tutkimiseen koneoppimisen (engl. machine learning) algoritmeilla. Arvon ennakoiminen on kuitenkin vaikeaa, sillä kryptomarkkinoihin vaikuttavat monet eri tekijät, eikä dataa ole kuin reilulta kymmeneltä vuodelta. Sebastiãon & Godinhon (2021) tutkimuksessa koneoppimisen algoritmien keskimääräinen onnistumisaste kolmen suurimman kryptovaluutan Bitcoinin, Ethereumin ja Litecoinin arvon ennustamisessa oli reilu 50 % vuosina 2018–2019. Tosin ei ole varmuutta, käyttivätkö he parhaita mahdollisia algoritmeja arvojen ennustukseen. (Sebastião & Godinho, 2021, 2–3, 24, 27–28)

Tekoälyn neuroverkkojen hyödyntämiseen pohjautuvissa ennustuksissa puolestaan on todettu, että pitkän aikavälin ennusteella on todennäköisempää saavuttaa korkeampi tulos kuin lyhyemmällä aikavälillä. Tämä tulos saatiin kahdella eri mallilla: Multilayer Perceptron-mallilla (lyh. MLP) ja Recurrent Neural Networks-mallilla (lyh. RNN). Kuten osakemarkkinoiden hintaennusteessa, pitkän aikavälin hintaennuste osoittaa suhteellisen korkean tarkkuuden myös kryptovaluutan hintaennusteessa 60–80 % tarkkuudella. (Albariqi & Winarko, 2020, 4)

Sijoittamisen lisäksi bitcoineja voidaan käyttää nykyään päivittäisenä maksuvälineenä, sillä monet jälleenmyyjät, kauppiaat ja yritykset hyväksyvät bitcoinit laillisena maksutapana perinteisten maksutapojen rinnalla. (TechTree.com, 2020a) Suomessakin on tällä hetkellä jo yli 60 yritystä, verkkokauppaa ja palvelua, jotka hyväksyvät bitcoinin maksuvälineenä. Näihin 60 yritykseen tai palveluun kuuluu monien eri alojen yrityksiä, kuten elektroniikka kauppoja, auto- ja autotarvikeliikkeitä, tekstiililiikkeitä sekä kello- ja pyöräliikkeitä. (Bittiraha.fi) Lisäksi maailmalla kryptovaluuttojen käyttö on hieman yleistynyt ja joissakin maissa sallitaan esimerkiksi myös palkanmaksu kryptovaluutoilla. Kryptovaluuttojen suuret arvonvaihtelut, eli *volatiliteetti*, tekee niistä kuitenkin haastavan virallisena valuuttana. Monet tahot ovat spekuloineet, ettei Bitcoinista voi tulla sen vuoksi

globaalia tai virallista maksuvälinettä. Bitcoinin käyttöönotto ja hyväksyntä kaupankäyntiin sekä vaihdannan välineeksi kuitenkin mahdollisesti laskisi volatiliteettia tehden arvonnoususta ja hinnasta tasaisemman. (Sebastião & Godinho, 2021, 3–5)

Maksutavat ovat myös muuttuneet valtavasti viimeisen 3 vuoden aikana: käteisen käyttö on vähentynyt ja isot yritykset, kuten Facebook, Amazon ja Booking.com kehittävät omia maksutapojaan kustannusten vähentämiseksi ja kerätäkseen tietoja asiakkaistaan. M2 Presswiren (2020) julkaisun mukaan edellä mainitut maksutavat isoilta yrityksiltä ovat varmasti tulossa korvaamaan nykyisiä maksujärjestelmiä, mutta kryptovaluutat eivät niin tee. Sen mukaan bitcoinilla on arvoa, koska kansainväliset maksut ovat kalliita, hitaita, eivätkä ne ole avoimia, kun taas bitcoinin siirtokustannukset eivät ole kalliita ja siirrot tapahtuvat reaaliajassa. Kryptovaluuttaratkaisut eivät kuitenkaan ole tarpeeksi skaalautuvia toimiakseen vaihtoehtona olemassa oleville maksujärjestelmille, joiden on käsiteltävä satoja tapahtumia sekunnissa. (M2 Presswire, 2020; Zaghloul ja muut, 2020, 10294–10296)

Kryptovaluuttojen tulevaisuudesta ei ole yksimielistä näkemystä, ja arviot tulevaisuudesta vaihtelevat arvion antajan mukaan. Pitkällä tähtäimellä lohkoketjuteknologian odotetaan kuitenkin tekevän merkittävän muutoksen yritysten toimintaan sekä vaikuttavan koko yhteiskuntaamme monien eri toimialojen kautta (Bergman, 2021). Tätä näkemystä tukee se, että lohkoketjuteknologiaa voidaan käyttää jo nyt moniin eri tarkoituksiin esimerkiksi elektronisena rahana tai arvonsiirtona, viestinvälityksenä allekirjoitetuissa viesteissä, tai yritysten velkakirjojen ja osaketietojen säilytyksessä, jolloin ne ovat luotettavasti turvassa muuttumattomina. Samalla myös bitcoinin arvon odotetaan nousevan pitkällä aikavälillä, sillä bitcoin käyttäytyy deflaatiomaisesti (Szmigielski, 2016, 13–14).

6 Pohdinta

Tämän tutkielman tavoitteena oli tutkia kryptovaluutta Bitcoinia sijoituskohteena sekä avata sen taustalla toimivaa lohkoketjuteknologiaa niin, että kuka tahansa Bitcoinista sijoituskohteena kiinnostunut saisi riittävän kattavan kuvan sen takana toimivasta teknologiasta. Aihe valikoitui oman kiinnostuksen ja Bitcoinin ajankohtaisuuden pohjalta, joiden myötä tutkimuskysymyksiksi muodostuivat:

- Minkälainen teknologia Bitcoinin taustalla oleva lohkoketjuteknologia on, ja mitä se pitää sisällään?
- Millainen Bitcoin on sijoituskohteena, ja miltä sen tulevaisuus näyttää sijoittamisen näkökulmasta?

Bitcoin on luotu vuonna 2008 virtuaalivaluutaksi ja vaihdannan välineeksi, josta Bitcoin on noussut pääosin omaisuudeksi ja sijoituskohteeksi (Nakamoto, 2008, 1–8;

TechTree.com, 2020a; NorthCrypto, 2020b; Vellava, 2019, 72–73). Bitcoin-järjestelmä ei ole minkään valtion tai viranomaisen hallinnoitavissa, vaan järjestelmä toimii vertaisverkossa käyttäjien toimesta. Yksi syy, miksi Bitcoin ei ole yleistynyt valuuttana ja maksutapana on se, että suuri volatiliteetti tekee siitä haastavan ja epätasapainoisen valuutan. (Sebastião & Godinho, 2021, 2–5; NorthCrypto, 2020b) Lisäksi vaikka Bitcoinilla on valuutaksi ja vaihdannan välineeksi sopivia piirteitä, ainutlaatuisuuden takia on sen yleistymiseen valuuttana vielä matkaa ja haasteita. Virallisena valuuttana se tarvitsisi esimerkiksi suurempaa sääntelyä. Siksi Bitcoinia voisi kuvastaa tällä hetkellä arvon varastona. Samanlainen sijoituskohde on vaikkapa kulta, johon Bitcoin usein rinnastetaankin. (Beck, 2018, 54)

Kryptovaluutat ei ole vielä tulleet kaikkien ihmisten tietouteen ja niiden käyttö aiheuttaakin ihmisissä hämmennystä ja negatiivisia asenteita. Tällä hetkellä näyttääkin hieman siltä, että Bitcoinin ympärille on muodostunut globaalisti kasvava kuilu teknologiaa ymmärtävien ja muiden ihmisten välille. Silti Bitcoin on menestynyt kryptovaluutta ja onnistunut kasvattamaan käyttäjäkuntaansa yli 12 vuoden ajan. Samalla sen takana toimivaa lohkoketjuteknologiaa voidaan hyödyntää eri toimialoilla, mikä viittaa lohkoketjuteknologian entistä suurempaan yleistymiseen tulevaisuudessa (Euroopan parlamentti, 2018).

Sijoituskohteena Bitcoin herättää kiinnostusta ja innostusta, mutta myös kysymyksiä, oletuksia ja väheksyntää, jotka pohjautuvat usein tiedonpuutteeseen tai uuden asian pelkoon (Vellava, 2019, 66). On kuitenkin totta, että kryptovaluuttoihin sijoittaminen on riskialtista ja mahdollisuus koko pääoman menettämiseen on suuri, mutta suuret riskit mahdollistavat usein myös tavallista suuremmat voitot. Sijoittajan tulee perehtyä kryptovaluuttoihin ja niiden toimintaan ennen sijoituspäätöksen tekemistä, eikä sijoittamisessa tule sijoittaa omaisuutta sen enempää, kuin on varaa menettää. Lisäksi tulee tiedostaa, että kryptovaluutoille on tyypillistä perinteisiä sijoituskohteita suuremmat arvonvaihtelut, joten ne vaativat sijoittajalta riskinsietokykyä ja itsensä tuntemista (Sebastião & Godinho, 2021, 2–5; NorthCrypto, 2020b). Digitaalisuutensa myötä kryptovaluuttoihin liittyy myös monia muita riskejä, kuten kryptovaluuttavarojen säilyttämiseen liittyvät riskit (NorthCrypto, 2020c).

Kryptovaluuttoihin liittyen internetissä ja mediassa on hyvin erilaisia kirjoituksia sekä uutisointeja, joihin tulee suhtautua varautuneesti. Myös finanssivalvonnan mukaan ihmisille tarjotut tiedot ja uutisoinnit kryptovaluutoista ovatkin monin tavoin puutteellisia (FIN-FSA, 2019). Esimerkkinä tästä voidaan todeta, että monissa eri medioissa uutisoidaan siitä, kuinka asiantuntijat ovat kryptovaluutoista jotakin mieltä ja he ennustavat bitcoinin tulevaisuudelle jotakin tiettyä tapahtumaa. Nämä tapahtumat voivat olla esimerkiksi arvon romahdus, tai että kryptovaluutat eivät voisi toimia virallisena valuuttana tai ylipäätään yleistyä maksuvälineenä. Toisin sanoen mielipiteitä on yhtä monia kuin on

kryptovaluutta-asiantuntijoitakin. Lisäksi näitä asiantuntijoita harvoin esitellään tai kerrotaan, mistä he ovat asiantuntijuutensa aiheeseen liittyen saaneet.

Tutkielman lähdeaineistojen pohjalta korostui lohkoketjuteknologian ainutlaatuisuus ja sen mahdollisuudet tulevaisuudessa. Lähdeaineistoista myös korostui kryptovaluuttoihin sijoittamisen riskialttius, ennustamisen vaikeus, mahdollisuus pääoman menettämiselle sekä kryptovaluuttojen tulevaisuuden epävarmuus. (Albariqi & Winarko, 2020, 1–4; Bergman, 2021; Euroopan parlamentti, 2018; FIN-FSA, 2019; Go-dinho & Sebastião, 2021, 2; M2 Presswire, 2020; NorthCrypto, 2020b, 2020c; Zaghloul ja muut, 2020) On fakta, että Bitcoin ja kryptovaluutat ovat edelleen kaikille suhteellisen uusia aiheita, eikä kukaan pysty ennustamaan niiden tulevaisuutta. Kun tarkastellaan maksuvälineiden kehitystä historiallisesti, yhteiskunnan maksutavat ovat muuttuneet oravannahoista käteisen rahan kautta maksukortteihin. Kukaan ei voi tietää mihin suuntaan maksutavat kehittyvät seuraavien vuosikymmenten aikana, joten kryptovaluuttojen yleistymistä maksuvälineenä ei myöskään voida poissulkea.

Bitcoinin ja ethereumin arvokäyrien tarkastelulla voi todeta, että niiden arvot ovat aiemmin nousseet räjähdysmäisesti kaksi kertaa ja suurin piirtein samaan aikaan. Tutkielman pohjalta ei voi kieltää, etteikö niiden arvon nousulle olisi mahdollisuutta myös tulevaisuudessa, etenkin pitkällä aikavälillä. Joidenkin arvioiden mukaan bitcoinin arvo tulee ylittämään 100 000 dollaria (Ylä-Anttila, 2021b). Joidenkin arvioiden mukaan 100 000 dollarin ylitys tapahtuu vuoden 2021 aikana, toisten arvioiden mukaan useiden vuosien kuluttua, kun taas kolmansien arvioiden mukaan bitcoinin arvo ei tule enää nousemaan vaan se romahtaa.

Tutkielmassa käytettyjen lähteiden perusteella on yhtä todennäköistä, että bitcoinin arvo nousee tai sen arvo romahtaa. Tai se ei koskaan yleisty maksuvälineenä sen enempää kuin tähänkään asti. Tämän tutkielman teon, eli kahden kuukauden aikana, bitcoin kuitenkin saavutti kolme kertaa merkittävän arvoennätyksensä: ensin 30 000 dollaria, sitten 40 000 dollaria ja viimeisimpänä 50 000 dollaria. Vaikka Bitcoiniin liittyen moni asia on epävarmaa, varmaa on kuitenkin se, että sijoituskohteena se tarjoaa jännitystä suurine arvonmuutoksineen.

Lähdeluettelo

Albariqi, R. & Winarko, E. (2020). Prediction of Bitcoin Price Change using Neural Networks. *International Conference on Smart Technology and Applications (ICo-STA).* 20–20.2.2020, Surabaya, Indonesia. https://doi.org/10.1109/ICo-STA48221.2020.1570610936

Antonopoulos, A.M. (2017). *Mastering Bitcoin – Second Edition – Programming the Open Blockchain*. O'Reilly Media, Inc.

Balvers, R. J. & McDonald, B. (2017). *Designing a global digital currency.* https://dx.doi.org/10.2139/ssrn.3049000

Beck, R. (2018). Beyond Bitcoin: The Rise of Blockchain World. *Computer*, 51(2), 54–58. https://doi.org/10.1109/mc.2018.1451660

Bergman, S. (2021). *Kryptovaluutat ja niihin sijoittaminen 2021.* Sijoitusrahastot.org. https://sijoitusrahastot.org/kryptovaluutat/

Bittiraha.fi. *Bitcoin-maksupaikat Suomessa.* https://bittiraha.fi/bitcoin-maksupaikat-suomessa/ (Haettu 19.01.2021)

Bouraga, S. (2020). A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Systems with Applications.* https://doi.org/10.1016/j.eswa.2020.114384

Burniske, C. & Tatar, J. (2017). *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond.* McGraw-Hill Education.

Chaim, P. & Márcio, P.L. (2018). Is Bitcoin a bubble? *Physica A: Statistical Mechanics and its Applications.* 517, 222-232. https://doi.org/10.1016/j.physa.2018.11.031

Chowdhury, N. (2020). *Inside Blockchain, Bitcoin, and Cryptocurrencies.* CRC Press

Dhulavvagol, P.M., Bhajantri, V.H. & Totad, S.G. (2020). Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application. *International Conference on Computational Intelligence and Data Science (ICCIDS 2019).* 167, 2506-2515. https://doi.org/10.1016/j.procs.2020.03.303

Euroopan parlamentti. (2018). *Lohkoketjuteknologia: "Haluamme tehdä EU:sta edelläkävijän".* Euroopan parlamentti – ajankohtaista. https://www.europarl.europa.eu/news/fi/headlines/economy/20180514STO03406/lohkoketjuteknologia-haluamme-tehda-eu-sta-edellakavijan (Haettu 22.01.2021)

Erkkilä, J. (2020). *Suuret institutionaaliset sijoittajat ovat innostuneet bitcoineista.* Salkunrakentaja.fi https://www.salkunrakentaja.fi/2020/12/institutionaaliset-sijoittajat-bitcoin/

FIN-FSA Finanssivalvonta. (2019). *Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu?* https://www.finanssivalvonta.fi/kuluttajansuoja/kysymyksia-ja-vastauksia/virtuaalivaluutat/ (Haettu 20.01.2021)

Franco, P. (2015). *Understanding Bitcoin: Cryptography, Engineering and Economics.* Wiley.

Frisby, D. (2014). *Bitcoin: The Future of Money?* Unbound Publishing.

Hertig, A. (2020). What Is Proof-of-Work? Coindesk.com. https://www.coindesk.com/what-is-proof-of-work (Haettu 10.02.2021)

Hu, Y., Hou, Y.G. & Oxley, L. (2019). What role do futures markets play in Bitcoin pricing? Causality, cointegration and price discovery from a time-varying perspective? *International Review of Financial Analysis.* 72. https://doi.org/10.1016/j.irfa.2020.101569

Investing.com. (2021a). *Bitcoin.* https://fi.investing.com/crypto/bitcoin (Haettu 17.02.2021)

Investing.com. (2021b). *Ethereum.* https://fi.investing.com/crypto/ethereum (Haettu 17.02.2021)

Kaushal, P.K., Bagga, A. & Sobti, R. (2017). Evolution of Bitcoin and Security Risk in Bitcoin Wallets. *International Conference on Computer, Communications and Electronics (Comptelix).* 1–2.7.2017, Jaipur, India. https://doi.org/10.1109/COMPTELIX.2017.8003959

Li, X. & Whinston, A.B. (2019). Analyzing Cryptocurrencies. *Information Systems Frontries,* 22, 17–22. https://doi.org/10.1007/s10796-019-09966-2

Lone, A.H. & Naaz, R. (2020). Demystifying Cryptography behind Blockchains and a *Vision* for Post-Quantum Blockchains. *International Conference for Innovation in Technology (INOCON).* 6–8.11.2020, Bangluru, India. https://doi.org/10.1109/IN-OCON50539.2020.9298215

Lánský, J. (2016). Analysis of Cryptocurrencies Price Development. *Acta Informatica Pragensia*. Vol. 5(2), 118–137. *http://dx.doi.org/10.18267/j.aip.89*

MikroBitti. (2017). *12-vuotias sijoitti 1000 dollaria bitcoiniin vuonna 2011 – nyt poika on miljonääri.* https://www.mikrobitti.fi/uutiset/12-vuotias-sijoitti-1000-dollaria-bitcoiniin-vuonna-2011-nyt-poika-on-miljonaari/67f90f9d-0c12-3ade-8b76-6487da28bf06 (Haettu 22.01.2021)

M2 Presswire. (2020). *The future of payments.* Normans Media Ltd.

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

NorthCrypto, (2020a). *Blogi: Bitcoinin puoliintuminen.* https://www.northcrypto.com/announcement/113 (Haettu 19.01.2020)

NorthCrypto, (2020b). *Blogi: Bitcoinin ostaminen.* https://www.northcrypto.com/announcement/108 (Haettu 19.01.2020)

NorthCrypto, (2020c). Blogi: Kryptovaluuttojensäilyttäminen. https://www.northcrypto.com/announcement/133 (Haettu 19.01.2021)

NorthCrypto, (2021a) *Mikä on Ethereum?* https://www.northcrypto.com/fi/about/ethereum (Haettu 10.01.2021)

NorthCrypto, (2021b). *Etusivu. NorthCrypto.* https://www.northcrypto.com/fi (Haettu 19.01.2021)

Parviainen, M. (2018). *Kryptovaluuttojen arvonmuodostus.* Kandidaatintutkielma, Tampereen teknillinen yliopisto. Haettu osoitteesta http://urn.fi/URN:NBN:fi:tty-201805141659

Raina, J. & Sillanpää, J. (2014). *Bitcoin – Edut, haasteet ja tulevaisuus.* Kandidaatintutkielma, Lappeenrannan teknillinen yliopisto. http://urn.fi/URN:NBN:fi-fe2014050825744

Sebastião, H. & Godinho, P. (2021). Forecasting and trading cryptocurrencies with machine learning under changing market conditions. *Financial Innovation*. https://doi.org/10.1186/s40854-020-00217-x

Szmigielski, A. (2016). *Bitcoin essentials: gain insights into Bitcoin, a cryptocurrency and a powerful technology, to optimize your Bitcoin mining techniques.* Birmingham: Packt Publishing.

Song, J. (2019). *Programming Bitcoin: Learn How to Program Bitcoin from Scratch.* O'Reily Media, Inc.

TechTree.com (2020a). *Cryptocurrency: The Currency of the Future*. Athena Information Solutions Pvt. Ltd. India, Bangalore.

Techtree.com (2020b). *Know the Ideology about Bitcoin and its features.* Athena Information Solutions Pvt. Ltd. India, Bangalore.

Tivi. (2017). *18-vuotias bitcoin-miljonääri voitti erikoisen vetonsa – aloitti isoäidin 1000 dollarilla.* https://www.tivi.fi/uutiset/18-vuotias-bitcoin-miljonaari-voitti-erikoisen-vetonsa-aloitti-isoaidin-1000-dollarilla/97e57603-c98e-35c3-b436-af404c8cd715 (Haettu 22.01.2021)

Vellava, S. (2019). Osta paikkasi tulevaisuudesta! Kryptovaluutta-aktivistit rahamarkkinoilla. *Kansantaloudellinen aikakauskirja.* https://www.taloustieteellinenyhdistys.fi/wp-content/uploads/2019/02/KAK_1_2019_WEB-68-81.pdf

Yle. (2018). *Uutiset. Bitcoin teki 28-vuotiaasta miljonäärin - 500 euron sijoituksella 2 miljoonan euron tulot.* https://yle.fi/uutiset/3-10487285 (Haettu 22.01.2021)

Yle. (2019). Uutiset. *Finanssivalvonta rekisteröi viisi virtuaalivaluutan tarjoajaa – muut eivät saa toimia Suomessa.* https://yle.fi/uutiset/3-11047047 (Haettu 19.01.2021)

Ylä-Anttila, A. (2021a). Tesla pisti rahojaan bitcoiniin, onko seuraavaksi vuorossa Apple? – Suomalainen kryptovälittäjä: "Yritykset ovat lähteneet hajauttamaan kassaansa bitcoiniin". *Kauppalehti. https://www.kauppalehti.fi/uutiset/tesla-pisti-rahojaan-bitcoiniin-onko-seuraavaksi-vuorossa-apple-suomalainen-kryptovalittaja-yritykset-ovat-lahteneet-hajauttamaan-kassaansa-bitcoiniin/3ee22ff3-f65b-4f12-b5ba-62684bdeb61e?fbclid=IwAR2SoyeEDqOE-aNnTs_w64Mmy0oDi7YIoZ6E4bR4a4A5MNQPZwJHZlu38KwI (Haettu 10.02.2021)*

Ylä-Anttila, A. (2021b). Rajapyykki rikkoutui – Bitcoinin hinta ylitti ensi kertaa 50 000 dollaria. Kauppalehti. https://www.kauppalehti.fi/uutiset/rajapyykki-rikkoutui-bitcoinin-hinta-ylitti-ensi-kertaa-yli-50-000-dollaria/3db81ee8-f18a-4691-9ab1-b8d4ccd1b7af *(Haettu 17.02.2021)*

Zaghloul, E., Li, T., Mutka, M.W. Ren, J. (2020). Bitcoin and Blockchain: Security and Privacy. *Internet of Things Journal.* 7(19), 10288-10313. https://doi.org/10.1109/JIOT.2020.3004273