TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MARKUS PARVIAINEN

# KRYPTOVALUUTTOJEN ARVONMUODOSTUS

Kandidaatintyö

# TIIVISTELMÄ

**MARKUS PARVIAINEN**: Kryptovaluuttojen arvonmuodostus
Tampereen teknillinen yliopisto
Kandidaatintyö, 21 sivua
Toukokuu 2018
Tekniikan kandidaatin tutkinto-ohjelma
Pääaine: Tuotantotalous
Tarkastaja: Tuomas Korhonen

Avainsanat: kryptovaluutta, lohkoketju, kryptografia, Bitcoin, hajautettu järjestelmä, hintamanipulaatio, hintakupla

Lohkoketjuteknologiaan perustuvat hajautetut kryptovaluutat mahdollistavat varallisuuden siirron osapuolelta toiselle ilman luottamusta kolmanteen osapuoleen, kuten pankkiin tai rahan välittäjään. Vaikka kryptovaluuttojen perimmäinen tarkoitus on olla vaihdannan väline, käytetään niitä enenevässä määrin spekulatiiviseen sijoittamiseen ja arvonnousun tavoitteluun. Kryptovaluuttojen pörssikurssit ovat kasvaneet räjähdysmäisesti viime vuosien aikana, mutta ei voida kuitenkaan yksiselitteisesti sanoa, mikä selittäisi ennennäkemättömän hintakehityksen.

Kirjallisuustutkielmana toteutetussa kandidaatintyössä etsittiin tekijöitä, jotka vaikuttavat kryptovaluutan arvostukseen samansuuntaisesti. Työssä esiteltiin aluksi lohkoketjuteknologian ja sitä hyödyntävien kryptovaluuttojen toimintaperiaatteet. Tämän jälkeen tutkittiin, minkälaisia hinnoittelumalleja kryptovaluutoille on muodostettu akateemisessa kirjallisuudessa, ja hintamanipulaation mahdollisuuksia tutkittiin lähdeaineistoon pohjaten. Myös hintakuplan mahdollisuutta tarkasteltiin sekä talouden hintakuplan teoriaan että kryptovaluutoista kirjoitetun kirjallisuuden kannalta.

Lähdemateriaalin avulla pystyttiin tunnistamaan kryptovaluutan arvoa muodostaviksi tekijöiksi muun muassa hajautettu lohkoketjuverkosto, teknologinen innovaatio, louhintakustannukset, markkinanäkemys ja hyväksyntä tavanomaisissa maksutilanteissa. Bitcoinin hintaa on onnistuttu aikaisemmin manipuloimaan, eikä voida tälläkään hetkellä olla varmoja, etteikö joidenkin kryptovaluuttojen hintoja olisi mahdollista manipuloida. Hintakuplan teoriaa ja aiheesta kirjoitettua kirjallisuutta analysoimalla voitiin perustellusti todeta, että kryptovaluutat ovat tällä hetkellä hintakuplassa. Sitä, onko kupla rationaalinen vai irrationaalinen, ei voitu kuitenkaan suoraan sanoa tutkitun aineiston perusteella.

# ABSTRACT

**MARKUS PARVIAINEN**: Value formation of cryptocurrencies
Tampere University of Technology
Bachelor of Science Thesis, 21 pages
May 2018
Bachelor's Degree Programme in Industrial Engineering and Management
Major: Industrial Engineering and Management
Examiner: Tuomas Korhonen

Keywords: cryptocurrency, blockchain, cryptography, Bitcoin, decentralized system, price manipulation, price bubble

Cryptocurrencies based on blockchain technology enable transfer of wealth from one party to another without trusting a third party, such as a bank or a financial intermediary. Even though the fundamental purpose of cryptocurrencies is to be a medium of exchange, they are increasingly used for speculation and in pursuit of capital gain. Exchange rates for cryptocurrencies have grown explosively in recent years, but one cannot say unambiguously what explains the unprecedented price development.

This Bachelor's thesis, done as a literature review, searched for factors that affect cryptocurrency valuations in a similar manner. First the technical foundation of cryptocurrencies utilizing blockchains was explained. This was followed by investigating different cryptocurrency pricing models suggested by academic literature, and possibility for price manipulation was considered based on the source material. In addition, the possibility for the existence of a price bubble was examined based on bubble theory and academic literature on cryptocurrencies.

Based on the source material, several factors affecting cryptocurrency valuations were identified. Most prominent factors were the decentralized blockchain network, technological innovation, costs of cryptocurrency mining, market sentiment, and acceptance in conventional payment situations. The price of Bitcoin has been manipulated in the past, and one cannot say for sure that it is not possible to manipulate the price of a cryptocurrency today. After analysing the theory of price bubbles and literature written about cryptocurrencies, one can with good reason state that cryptocurrencies are in a bubble. Still, one cannot outright say whether the bubble is rational or irrational.

# ALKUSANAT

Kryptovaluutat ovat tuoneet mukanaan sekä mielenkiintoista teknologista innovaatiota että ennennäkemätöntä nousua markkinahintojen osalta. Kandidaatintyössäni pyrin löytämään selittäviä tekijöitä hintojen kehitykselle ja tarjoamaan lukijalle kokonaisvaltaisen kuvan kryptovaluuttamarkkinoista. Aihevalinta oli työn alusta lähtien kirkkaana mielessä, ja nälkä vain kasvoi syödessä ja työn edetessä. Ilokseni aiheesta on kirjoitettu suhteellisen paljon akateemisesta kirjallisuutta, enkä joutunut jättämään työtä laihaksi aineiston puutteen vuoksi. Vaikka tiesin entuudestaan paljon kryptovaluuttojen teknisestä puolesta, opetti kandidaatintyön tekeminen minulle paljon taloudellisista ilmiöistä ja tieteellisestä tutkimuksesta.

Haluaisin kiittää työni ohjaajaa Tuomas Korhosta ja professori Juho Kanniaista kandidaatintyöni ohjaamisesta, täsmällisestä ja rakentavasta palautteesta sekä hyvistä ideoista työn eteenpäin viemisessä. Tahtoisin myös kiittää opiskelijatovereitani osuvista ehdotuksista ja yleisestä mielenkiinnosta työtäni kohtaan.

Tampereella, 12.5.2018

Markus Parviainen

# SISÄLLYSLUETTELO

# 1. JOHDANTO

Lohkoketjuteknologiaan perustuvat hajautetut kryptovaluutat mahdollistavat varallisuuden siirron osapuolelta toiselle ilman luottamusta kolmanteen osapuoleen, kuten pankkiin tai rahan välittäjään. Tällaiset kryptovaluutat eivät siis ole minkään yksittäisen tahon hallitsemia. Lisäksi näiden kryptovaluuttojen toteutus mahdollistaa sen, että kerran käytettyä kryptovaluuttaa ei voi käyttää toiseen kertaan eli toisin sanottuna kerran suoritettua transaktiota on käytännössä mahdoton perua. Kryptovaluuttojen transaktiot ovat julkisesti tarkasteltavissa lohkoketjussa, mutta valuutan käyttäjien henkilöllisyyttä ei pystytä selvittämään pelkästään transaktioita tarkastelemalla. (Nakamoto 2008)

Koska kryptovaluutat perustuvat siihen, että jokainen sen käyttäjä hallitsee omia varojaan, siirrot tapahtuvat luotettavasti käyttäjien kesken ja luottamusta kolmanteen osapuoleen ei tarvita, pystytään rahan siirtokuluissa säästämään merkittävästi ja kryptovaluutasta riippuen siirrot voidaan lopullisesti varmistaa minuuteissa verrattuna tavanomaisten pankkisiirtojen jopa viikkojen pituisiin viiveisiin. Vaikka kryptovaluuttojen perimmäinen käyttötarkoitus on olla vaihdannan väline, eivät ne ole saavuttaneet merkittävää käyttöönottoa tavanomaisissa maksutilanteissa. Kryptovaluuttojen hajautettu luonne ja riippumattomuus keskitetystä hallinnoitsijasta aiheuttaa sen, että niitä on vaikea arvottaa millään yksiselitteisellä laskukaavalla. Kryptovaluutoilla käydään kauppaa julkisilla markkinapaikoilla, ja koska niiden arvo ei perustu mihinkään konkreettiseen, voi kryptovaluutan kurssi heilahdella merkittävästi lyhyinäkin aikaväleinä (Brandvold et al. 2015). Tämä vaikeuttaa kaupankäyntiä tavanomaisissa maksutilanteissa, ja kryptovaluuttoja käytetäänkin enenevässä määrin spekulointiin ja arvonnousun tavoitteluun valuuttana käytön sijaan (Polasik et al. 2015).

Kaupankäyntiä kryptovaluutoilla ei säännellä yhtä tarkasti kuin arvopaperikauppaa, ja yksittäiset suuret sijoittajat tai epärehelliset toimijat voivat manipuloida valitsemansa kryptovaluutan kurssia ilman riskiä oikeudellisista toimenpiteistä (Gandal et al. 2018). On siis mahdollista, että tällaisen toimijan vaikutuksesta yksittäisen kryptovaluutan hinta nousee, vaikka kryptovaluutalla ei olisi toimivaa toteutusta, hyväksyttyä white paper -julkaisua tai edes yhtään kehittäjää. Riittää, että kryptovaluutta on vain jollain kauppapaikalla listattuna.

## 1.1 Tavoitteet

Tämä kandidaatintyö etsii tekijöitä, jotka muodostavat yleisellä tasolla arvoa kryptovaluutan omistajalle tai käyttäjälle. Näitä tekijöitä etsitään tarkastelemalla Bitcoinin ja yleisimpien kryptovaluuttojen hintojen kehitystä ja niiden tuomia teknologisia innovaatioita.

Syitä hintakehitykselle etsitään alan kirjallisuudesta, ja lopulta päätellään, mitkä ovat kaikista keskeisimmät tekijät kryptovaluuttojen arvon määrityksessä. Mahdollisuuksia hintamanipulaatioon pyritään tunnistamaan näistä tekijöistä. Työssä tutkitaan myös, onko sijoittajien näkemyksellä merkittävää vaikutusta kryptovaluuttojen hintoihin arvoa muodostavista tekijöistä huolimatta ja voidaanko hintakehityksestä löytää kuplan tunnusmerkkejä. Työn tutkimuskysymyksiä ovat siis seuraavat:

- Mitä kryptovaluutan arvostukseen vaikuttavia tekijöitä voidaan tunnistaa?
- Voiko kryptovaluutta saavuttaa korkean arvostuksen ilman näitä tekijöitä?
- Millä tavoin kryptovaluutan hintaa voidaan manipuloida?
- Mitä hintakuplan ominaisuuksia kryptovaluuttojen arvostuksista voidaan tunnistaa?

Ensimmäinen tutkimuskysymys on työn kannalta keskeisin ja siihen kiinnitetään eniten huomiota työn edetessä. Loput tutkimuskysymyksistä tarkastelevat kryptovaluuttojen hinnan muodostusta erilaisista näkökulmista ja ne täydentävät siten kandidaatintyössä tarkasteltavia ilmiöitä ja aihepiirejä holistiseksi kokonaisuudeksi.

## 1.2 Metodologia

Kandidaatintyö toteutetaan kirjallisuustutkielmana. Työssä käsitellään kryptovaluutoista ja lohkoketjuteknologiasta kirjoitettua akateemista kirjallisuutta. Kirjallisuus on löydetty hyödyntämällä Tampereen teknillisen yliopiston tarjoamaa Andor-hakukonetta ja yleisesti saatavilla olevaa Google Scholar -tiedonhakupalvelua. Aiheen uutuuden vuoksi laadukasta lähdemateriaalia on määrällisesti vähän, mikä vaikeuttaa työhön sopivien lähteiden löytämistä. Työssä käytettyjen lähteiden laatu ja tiedon oikeellisuus työssä pyritään kuitenkin varmistamaan valitsemalla aineistot tunnetuista ja laadukkaista tieteellisistä lähteistä. Näiden lähteiden lisäksi hyödynnetään SSRN- ja arXiv-tietokannoissa olevia, lehdissä julkaisemattomia artikkeleita sekä kryptovaluuttojen teknisiä white paper -julkaisuja. Markkinanäkemyksen vaikutusta käsittelevään lukuun on rajatusti sisällytetty laadukkaista ei-tieteellisistä talousjulkaisuista uutisia ilmiön tarkastelun tueksi.

Tiedonhaku aloitettiin etsimällä mainituista tiedonhakupalveluista tieteellisiä julkaisuja hakusanoilla ”cryptocurrency”, ”cryptocurrency value” ja ”cryptocurrency price”. Näillä hakusanoilla löydettyjä julkaisuja käytetään tässä työssä keskeisimpinä lähteinä, ja työn edetessä etsittiin täydentäviä julkaisuja yksittäisistä kryptovaluutoista työn sisällön tueksi.

## 1.3 Rakenne

Kandidaatintyö on jaoteltu neljään osaan, joista jokainen käsittelee omaa pääteemaansa. Ensimmäisessä osassa esitellään lohkoketjuteknologian ja sitä hyödyntävien kryptova-

luuttojen tekninen perusta. Osiossa esitellään keskeisiä termejä ja käsitteitä kryptovaluuttojen toiminnan ja siten sen arvostuksen ymmärtämistä varten. Kryptovaluuttojen louhiminen, siirtojen tekeminen ja transaktioiden varmistaminen käydään läpi ja osiossa käsitellään, miten nämä tekniset ominaisuudet mahdollistavat hajautetun valuutan olemassaolon ja käytön.

Toisessa osassa tarkastellaan kryptovaluuttojen hinnan muodostusta tuotantokustannuksiin, spekulaatioon ja valuuttakauppaan perustuvien mallien avulla. Osiossa käydään läpi alan kirjallisuutta, ja etsitään mahdollisia syitä hintojen kehitykselle. Kolmannessa osiossa tarkastellaan hintamanipulaation mahdollisuutta ja sen vaikutusta kryptovaluuttojen hintoihin. Neljännessä osiossa tarkastellaan hintakuplaa käsitteenä ja etsitään yhtymäkohtia Bitcoinin ja muiden kryptovaluuttojen arvostukseen. Kandidaatintyön viimeisessä luvussa kerätään yhteen johtopäätökset aikaisemmista luvuista ja muodostetaan vastaukset tutkimuskysymyksiin.

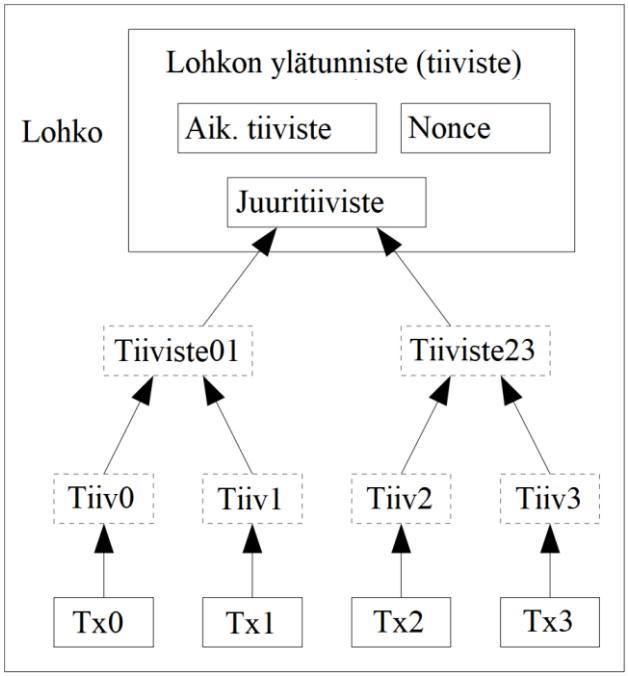
# 2. LOHKOKETJUTEKNOLOGIA JA KRYPTOVALUUTAT

Lohkoketjut koostuvat nimensä mukaisesti peräkkäisistä, toisiinsa yhdistetyistä lohkoista. Lohkoketjun lohkoihin voidaan käytettävän järjestelmän perusteella sisällyttää mitä tahansa dataa, mutta kryptovaluuttojen tapauksessa lohkoihin sisällytetään transaktioita yhdestä valuuttaa sisältävän ”lompakon” osoitteesta toiseen. Kaikille lohkoketjuteknologioille yhteistä on kryptografisten tiivistefunktioiden (engl. cryptographic hash function) käyttö tiedon pysyvyyden ja oikeellisuuden varmistamiseksi. Kun lohko lisätään lohkoketjuun, sen sisältämästä datasta otetaan kryptografinen tiiviste, joka sisällytetään sitä seuraavaan lohkoon. Kryptografisten tiivistefunktioiden ominaisuuksiin kuuluu, että saman tiivisteen saaminen eri syötedatalla on mahdotonta tai ainakin kohtuuttoman laskentatehon vaativaa. Näin ollen datan muuttuessa myös sen muodostama tiiviste muuttuu eikä se ole enää sama kuin seuraavaan lohkoon sisällytetty tiiviste. Lohkoketjua tarkistettaessa voidaankin siis varmistua sisällön oikeellisuudesta laskemalla jokaisen lohkon tiiviste ja vertaamalla sitä ketjussa seuraavan lohkon sisältämään tiivisteeseen. (Nakamoto 2008)

## 2.1 Proof-of-work ja louhiminen

Edellisessä luvussa esitelty yksinkertainen, transaktioita sisältävä lohkoketju ei itsessään takaa, että kaikki transaktiot olisivat kelvollisia. Lohkon ketjuun lisäävä taho voi lisätä haluamaansa lompakkoon mielivaltaisen määrän valuuttaa, kunhan transaktiodata ja sen muodostama kryptografinen tiiviste täsmäävät. Kryptovaluutat välttävät tämän ongelman hajauttamalla lohkojen lisäämis- ja varmistamisprosessin. Bitcoin ja muut louhittavat kryptovaluutat käyttävät Backin (2002) kehittämää proof-of-work-menetelmää, jossa lohkon ylätunnisteen tiivisteen pitää täyttää verkoston sille asettamat vaatimukset. Lohkon ylätunniste sisältää yleensä sitä edeltävän lohkon tiivisteen, tiivisteen kaikista lohkon transaktioista eli juuritiivisteen ja nonce-luvun. Lohkon rakenne on esitetty kuvassa 1. Kuvasta voidaan huomata, että yhden transaktion sisällön muuttuessa sen tiiviste, juuritiiviste ja edelleen lohkon ylätunnisteen tiiviste muuttuvat. Jos lohkoketjuun sisällytetyn lohkon ylätunnisteen tiiviste muuttuisi, lohkoketjua varmistaessa tiivisteiden eroavaisuudet huomattaisiin ja lohko transaktioineen voitaisiin siten mitätöidä.

Proof-of-work -menetelmän mukaisen kelvollisen tiivisteen löytäminen vaatii suuren määrän laskentatehoa, joten yksittäisen toimijan on vaikea hallita lohkoketjun tapahtumia käyttämättä merkittäviä resursseja tarvittavan laskentatehon saavuttamiseen. Muut kryptovaluutat käyttävät joko muunnelmia tästä menetelmästä, tai määrittelevät oman konsensusmenetelmänsä järjestelmän hajauttamiseen ja lohkojen oikeellisuuden varmistamiseen (Lánský 2016).




***Kuva 1.*** *Lohkon rakenne ja transaktioiden sisällytys lohkon ylätunnisteeseen (mukaillen Nakamoto 2008).*

Nakamoton (2008) kehittämässä Bitcoin-kryptovaluutassa jokaisen lohkon tiivisteen alun pitää sisältää tietty määrä nollabittejä, jotta lohkoketjuverkosto hyväksyy sen osaksi lohkoketjua. Lohkoihin sisällytetään tällöin niin kutsuttu mielivaltainen nonce-luku, jonka muuttaminen muuttaa koko lohkon tiivisteen. Kryptovaluuttojen kontekstissa louhiminen tarkoittaa nonce-luvun suurentamista ja tiivisteen uudelleen laskemista siihen asti, että asetettu vaatimus lohkon tiivisteen nollabiteistä toteutuu. Bitcoin-verkosto säätää vaadittujen nollabittien määrää jokaisen 2016 lohkon välein louhijaverkoston laskentatehon mukaan ja tavoittelee lohkojen lisäämisen aikaväliksi noin kymmentä minuuttia. Koska kryptografista tiivistettä ei voi ennustaa ilman sen laskemista, joutuu louhija käyttämään laskentatehoaan jokaisen tiivisteen laskemiseksi. Näin ollen, kun vaatimus nollabiteistä asetetaan tarpeeksi korkeaksi, joutuvat louhijat käyttämään joko paljon aikaa tai paljon laskentatehoa pystyäkseen lisäämään lohkon ketjuun. Kun louhijoiden määrä ja siten koko lohkoketjuverkoston laskentateho kasvaa, yhden yksittäisen louhijan mahdollisuus lisätä lohkoja ketjuun pienenee ilman merkittävää lisäystä omaan laskentatehoonsa. (Nakamoto 2008)

Kryptovaluuttaa voi saada haltuunsa joko tekemällä vaihtokaupan toisen käyttäjän kanssa jotain muuta valuuttaa tai hyödykettä vastaan tai osallistumalla itse louhintaan (Dwyer 2015). Jokainen louhittu lohko tuottaa sen lisääjälle ennalta säädetyn määrän kryptovaluuttaa louhimisen kannustamiseksi (Nakamoto 2008). Bitcoinin tapauksessa alussa säädetty 50 bitcoinin palkkio puolittuu jokaisen 210000 lohkon välein. Tästä seuraa matemaattisesti se, että bitcoinien kokonaismäärä on rajoitettu tasan 21 miljoonaan. Lohkojen lisäämispalkkion lisäksi jokaiseen transaktioon sisällytetään pieni kulu, jotta transaktio hyväksytään ja voidaan lisätä lohkoon (Nakamoto 2008). Louhija saa kaikki lohkon

transaktiokulut itselleen lisäämispalkkion lisäksi. Täten louhiminen voi olla kannattavaa, vaikka lisäämispalkkio suppeneekin nollaan lohkoketjun kasvaessa. (Dwyer 2015)

## 2.2 Vaihtoehtoiset konsensusmenetelmät

Vaikka proof-of-work -menetelmään perustuvat kryptovaluutat tarjoavat käyttäjilleen suuren varmuuden lohkoketjun oikeellisuudesta ja sen hallinnan hajautuksesta, käyttävät ne suuria määriä laskentatehoa ja louhintalaitteiston käyttämää sähköä lohkoketjun varmistamiseen (Bitfury Group 2015). Tätä laskentatehoa ei voida hyödyntää mihinkään muuhun käyttötarkoitukseen kuten tieteelliseen laskentaan. Lohkoketjuverkosto ei tarvitse suurta määrää louhijoita toimiakseen, mutta louhijoiden määrä kasvaa niin pitkään kuin louhiminen on taloudellisesti kannattavaa (Bitfury Group 2015).

Jotkut kryptovaluutat kuten Peercoin (King & Nadal 2012) ratkaisevat suuren energiankäytön käyttämällä lohkon lisääjän määrittämiseen proof-of-stake -menetelmää, jossa lohkon lisääjä määritetään käyttäjän kryptovaluuttaomistuksien perusteella. Tällöin yhden toimijan pitää omistaa merkittävä määrä kryptovaluuttaa saadakseen täyden hallinnan lohkojen lisäämisprosessista, mikä vaatisi miljoonien tai jopa miljardien investoinnin (Bitfury Group 2015). Joissain kryptovaluutoissa louhimista joko laskentatehon käytön tai omistuksien panostamisen muodossa ei tapahdu ollenkaan. Esimerkkinä tällaisesta menetelmästä on Mazieresin (2016) esittelemä Stellar Consensus Protocol, jossa verkoston osalliset äänestävät keskenään kelvollisista transaktioista. Tässä menetelmässä kryptovaluuttaa ei voi louhia, vaan valuutan jakaminen tapahtuu sitä hallinnoivan säätiön toimesta valituille osapuolille.

## 2.3 Julkisen avaimen kryptografia kryptovaluutoissa

Kryptovaluutan luotettava toiminta vaatii sen, että pelkästään valuutan omistajalla on oikeus tehdä transaktioita kryptovaluuttalompakostaan. Tavanomaisissa pankkijärjestelmissä valuutan siirto tapahtuu varmistamalla käyttäjän henkilöllisyys pankin käyttäjätietokannasta, ja antamalla sitten oikeuden siirtää valuuttaa tililtä toiselle. Lohkoketjua hyödyntävät kryptovaluutat eivät pidä millään tapaa kirjaa käyttäjistä ja valuutan siirto-oikeuksista, vaan transaktioiden tekemiseen käytetään niin kutsuttua julkisen avaimen kryptografiaa (Nakamoto 2008).

Julkisen avaimen kryptografiassa käyttäjä generoi itselleen sekä julkisen että salaisen avaimen, joiden avulla transaktioita voidaan allekirjoittaa. Lompakon julkisesta avaimesta voidaan tiivistefunktioiden avulla johtaa kryptovaluuttalompakolle osoite, johon valuuttaa pystytään lähettämään, ja lompakosta lähtevät transaktiot voidaan allekirjoittaa salaisella avaimella siten, että niiden oikeellisuus pystytään todentamaan julkisella avaimella. Salaisen avaimen tulisi nimensä mukaisesti olla vain lompakon omistajan tiedossa, sillä se mahdollistaa varojen siirron pois lompakosta. (Bernstein 2008) Kun uusi transaktio kuulutetaan julki lohkoketjuverkostolle lohkoon lisäämistä varten, verkosto

pystyy tarkastamaan transaktion todentamalla sen allekirjoituksen oikeellisuuden transaktioon sisällytetyn julkisen avaimen avulla (Nakamoto 2008). Tällainen menettely mahdollistaa vain kelvollisten transaktioiden lisäämisen lohkoketjuun ilman erillistä kirjanpitoa käyttäjistä tai erillisistä kryptovaluuttatileistä. Menetelmän käyttö johtaa kuitenkin siihen, että jos käyttäjä kadottaa salaisen avaimensa, ei kryptovaluuttaa pysty enää siirtämään lompakosta toiseen ja kaikki lompakon varat ovat lopullisesti käyttökelvottomia. Käyttäjällä on kryptovaluuttaa käyttäessään siis suuri vastuu avaintensa säilyttämisestä, sillä millään kryptovaluutalla ei ole keskitettyä asiakaspalvelua joka voisi palauttaa avaimen ja siten pääsyn lompakon varoihin.

## 2.4 Lohkoketjuteknologian seuraajat

Lohkoketjua käyttävien kryptovaluuttojen transaktionopeudesta on esitetty paljon kritiikkiä. Esimerkiksi Bitcoinin kymmenen minuutin tavoiteltu lohkojen lisäämisväli tekee siitä käyttökelvottoman tavanomaisissa maksutilanteissa, ellei kauppias halua vastaanottaa varmistamattomia transaktioita ja luottaa siihen, että ne lisätään tulevaisuudessa lohkoketjuun. Jos louhijoilla kestäisi esimerkiksi viikko lisätä uusi lohko ketjuun, kaikki siihen sisällytetyt transaktiot olisivat lukittuna sen ajan ja siten mahdottomia käyttää uusissa maksuissa.

Bitcoinille on kuitenkin kehitetty toisen kerroksen ratkaisuja kiihdyttämään transaktionopeutta, joista kenties tunnetuin on niin kutsuttu Lightning Network (Poon & Dryja 2016). Tässä ratkaisussa avataan maksukanavia erilliseen hajautettuun verkostoon, joissa maksutapahtumat tapahtuvat pitämällä kirjaa jokaisen osallistujan saldoista ja vaihtamalla niitä keskenään. Verkoston avulla voidaan saavuttaa liki viiveettömiä transaktioita lohkoketjun varmistuksen viivästymisen kustannuksella. Verkostossa tilien selvitys lohkoketjuun tapahtuu, kun maksukanavan avaaja päättää sulkea kanavan jolloin kaikki verkostossa tapahtuneet kryptovaluuttasiirrot tapahtuvat yhtenä lohkoketjutransaktiona ja ne voidaan lopullisesti varmistaa louhijoiden toimesta. (Poon & Dryja 2016)

Jotkin kryptovaluutat ratkaisevat transaktioiden hitauden hylkäämällä perinteisen lohkoketjun kokonaan ja käyttämällä suunnattuja syklisiä verkkoja (engl. directed acyclic graph). Tällaisia valuuttoja ovat esimerkiksi IOTA (Popov 2018) ja Nano (LeMahieu 2017). Näissä valuutoissa yksittäinen transaktio muodostaa varmistettavan lohkon ja valuutan käyttäjä joutuu osallistumaan transaktioiden varmistamiseen. IOTAn tapauksessa käyttäjän pitää varmistaa kaksi aikaisempaa transaktiota, jotta voisi lisätä oman transaktionsa Tangle-transaktioverkostoon (Popov 2018). Teoriassa näillä uusilla teknologioilla on mahdollista saavuttaa jopa kymmenien tuhansien transaktioiden sekuntinopeus, mutta niiden uutuuden ja kokeilemattomuuden takia ei voida olla täysin varmoja niiden toteutusten aukottomuudesta ja siten transaktioverkkojen varmuudesta. Bitcoinin pitkäikäisyys ja siihen kohdistettu monumentaalinen, hajautettu laskentateho mahdollistavat sen, että sen lohkoketjuun voidaan luottaa täysin ja kukaan ei pysty muokkaamaan tai peruuttamaan siihen lisättyjä transaktioita. Jos jokin uuden sukupolven kryptovaluutta onnistuisi

luotettavasti todistamaan suorituskykynsä ja hyökkäyskestävyytensä, se saattaisi horjuttaa Bitcoinin asemaa isoimpana kryptovaluuttana ja siten saavuttaa kenties ennennäkemättömän arvonnousun. Toisaalta Lightning Network saattaa osoittaa kelvollisuutensa tavanomaisissa maksutilanteissa, jolloin Bitcoin säilyttäisi asemansa suosituimpana kryptovaluuttana.

# 3. KRYPTOVALUUTTOJEN HINNOITTELU

Tässä luvussa tutkitaan sitä, miten kryptovaluutoilla käydään julkisesti kauppaa, miten niiden hinta kauppapaikoilla muodostuu ja millä tavoin kryptovaluuttaa voidaan hinnoitella. Luvussa tarkastellaan markkinahinnan muodostukseen vaikuttavia tekijöitä kryptovaluutan louhimisen kustannusten, spekulatiivisen sijoittamisen ja valuuttakaupan näkökulmien kautta. Luku muodostaa myös perustan hintakuplien tarkastelemista varten, josta kirjoitetaan tarkemmin työn viidennessä luvussa.

## 3.1 Kryptovaluuttapörssit hinnoittelun mahdollistajana

Gandalin et al. (2018) mukaan kryptovaluutoilla käydään kauppaa pääosin sääntelemättömillä over the counter -markkinoilla, eli kryptovaluuttapörssejä ja -kauppaa ei ole siis säännelty samalla tavalla kuin osake- tai johdannaispörssejä. Kaikkein suurimmilla kryptovaluuttapörsseillä on mahdollista käydä kauppaa dollareilla, euroilla tai muilla valtion liikkeelle laskemilla fiat-valuutoilla, kun taas pienemmät pörssit käyvät kauppaa vain bitcoinia tai muuta kryptovaluuttaa vastaan (Hayes 2015). Kryptovaluuttapörssejä on ollut olemassa vuodesta 2010 lähtien (Li & Wang 2016), jolloin kauppaa käytiin pelkästään bitcoinin ja Yhdysvaltain dollarin välillä, mutta muiden kryptovaluuttojen ilmestyessä pörssit ovat mahdollistaneet kaupankäynnin myös vaihtoehtoisten kryptovaluuttojen kuten Litecoinin tai Ethereumin kanssa.

Sääntelemättömästä pörssikaupankäynnistä johtuen mikään yksittäinen taho ei voi asettaa kryptovaluutan arvoa tai hallita sillä käytävää kauppaa täysin. Kryptovaluutan markkinahinta määräytyy siis pohjimmiltaan yksittäisten kaupankäyjien tekemien rajahintatarjousten määrästä ja suuruudesta kryptovaluuttapörssien tarjouskirjoissa. Cheahin ja Fryn (2015) mukaan kryptovaluutat ovat enemmän omaisuuseriä (engl. asset) kuin valuuttoja, ja mahdollisuus sääntelemättömään kaupankäyntiin mahdollistaa niillä spekulaation suurten tuottojen toivossa. Kryptovaluutan hinnoittelun pohjaksi on kuitenkin esitetty malleja, joilla pyritään löytämään kryptovaluutalle käypä arvo perustuen spekulaatiosta riippumattomiin tekijöihin.

## 3.2 Louhintakustannuksiin perustuva hinnoittelumalli

Louhiminen on elintärkeä toiminto kryptovaluutoille, sillä ilman louhimista uusia lohkoja ei voida lisätä lohkoketjuun. Kun lohkoja ei lisätä lohkoketjuun, uusia transaktioita ei voida varmistaa ja tällöin kryptovaluutan liike omistajalta toiselle lakkaa. (Iwamura et al. 2014) Osa kryptovaluutoista onkin lopettanut toimintansa louhimisen lopetuksen seurauksena. Lánskýn (2016) mukaan noin puolet yli tuhannesta olemassa olleesta kryptovaluutasta on kuollut sukupuuttoon. Näiden kuolleiden kryptovaluuttojen arvo ja niihin

kohdistettu laskentateho on liki olematon, sillä niiden louhiminen ei ole enää kannattavaa. Yli puolet näistä kuolleista kryptovaluutoista menetti arvonsa ensimmäisen 24 viikon aikana olemassaolostaan. Vastaavasti, melkein poikkeuksetta kaikki yli 124 viikkoa olemassa olleet kryptovaluutat ovat vieläkin elinvoimaisia. (Lánský 2016) Voidaan siis päätellä, että kryptovaluutan ikä ja louhintatoiminnan jatkuvuus on merkki sen pitkäaikaisesta selviytymisestä ja arvon säilymisestä.

Kryptovaluuttaa voidaan saada haltuun joko ostamalla tai louhimalla (Dwyer 2015). Kryptovaluutan louhimista varten louhija joutuu tekemään investointeja louhintalaitteiston, sähkön ja mahdollisesti fyysisen tilan hankkimista varten (Hayes 2016). Louhintalaitteiston hankintakustannukset voidaan käsittää uponneiksi kustannuksiksi, joiden vaikutus kryptovaluutan hinnan kehitykseen ei ole enää laitteiston hankinnan jälkeen merkityksellinen. Sähkön kulutus ja hinta ovat kuitenkin muuttujia, joilla voi olla merkittäväkin vaikutus siihen, mitä kryptovaluuttaa on kannattavaa louhia. Louhinnan kuluttama laskentateho kohdistetaan yleensä sellaiseen kryptovaluuttaan, jonka louhimisvaikeus on tarpeeksi alhainen. Kun louhimisvaikeus on suhteellisen alhainen, on louhijalla parempi mahdollisuus löytää proof-of-work -menetelmän mukaisesti kelvollinen tiiviste lohkolle, joka lisätään verkoston hyväksynnällä osaksi lohkoketjua ja siten tuottaa louhijalle tietyn määrän kryptovaluuttaa louhintapalkkiona. Louhimisvaikeuden noustessa laskentatehoa pitää kuluttaa enemmän kelvollisen tiivisteen löytämiseksi, ja täten louhijan pitää arvioida laitteistonsa tehokkuutta jatkuvasti louhimisen kannattavuuden ylläpitämiseksi. Louhijan pitää siis tietää laitteistonsa sähkön kulutus, hinta ja kryptovaluuttojen louhimisvaikeudet. Lisäksi, koska suurinta osaa kryptovaluutoista voi vaihtaa pörsseissä vain bitcoineiksi ja vain sen kautta dollareiksi tai euroiksi, Bitcoinin markkinahinta vaikuttaa myös louhinnan kannattavuuteen. (Hayes 2016) Kryptovaluutan marginaalinen louhintakustannus koostuu siis seuraavista päätekijöistä (Hayes 2016):

- sähkön hinta
- louhintalaitteiston sähkönkulutus laskentatehon yksikköä kohden
- louhimisvaikeus
- Bitcoinin markkinahinta.

Näiden neljän tekijän avulla voidaan muodostaa louhintakustannusten perusteella alaraja jonkun kryptovaluutan markkinahinnalle. Jos kryptovaluutan hinta putoaisi tämän tuotantokustannuksen alle, louhijat voivat vaihtaa louhintakohteensa johonkin kannattavampaan kryptovaluuttaan ja siten pitää toimintansa kannattavana.

Louhijoiden vapaa liikkuvuus eri kryptovaluuttojen välillä aiheuttaa myös sen, että markkina korjaa mahdollisuuden niin sanottuihin nopeisiin voittoihin itsestään. Jos jokin kryptovaluutta on ylihinnoiteltu tai sitä on helppo louhia, louhijat alkavat louhimaan sitä ajaen louhimisvaikeuden korkealle, jolloin louhiminen ei tuota enää samaa määrää kryptovaluuttaa yhtä laskentatehon yksikköä kohden. Samoin tämän kryptovaluutan markkinahinta ohjautuu alas, kun louhijat myyvät alhaisen louhimisvaikeuden aikana louhimiansa

kolikoita korkealla hinnalla markkinoille. Tällöin kryptovaluutan hinta ja siten louhimisen kannattavuus laskevat.

## 3.3 Hinnoittelu valuuttakaupan näkökulmasta

Sijoitusinstrumenttina kryptovaluutat eivät ole kuin osakkeet, sillä ne eivät edusta omistajuutta missään yhtiössä, eivätkä ne siten tuota arvoa tai osinkoja sijoittajalle. Cheah ja Fry (2015) väittävätkin, että kryptovaluutat muistuttavat enemmän kultaa ja fiat-valuuttaa. Kulta ja fiat-valuutta eivät myöskään tuota itsessään hyötyä omistajalle, mutta ovat arvokkaita, sillä ne ovat kaupankäynnin välineitä. Kryptovaluutan käytön helppokäyttöisyys, pienet kustannukset ja mahdollisuudet jakaa pienempiin yksiköihin tekevät kryptovaluutoista siten samankaltaisia fiat-valuuttojen kanssa. (Cheah & Fry 2015)

Samankaltaisuutta fiat-valuuttojen kanssa voidaan tutkia myös inflaation ja korkotason kannalta. Kryptovaluutan osto tai myynti fiat-valuuttaa vastaan on tietynlaista valuuttakauppaa sillä erotuksella, että toista valuuttaa arvottaessa ei voida hyödyntää korkotasoa tai inflaation suuruutta, sillä kryptovaluutat eivät ole sidoksissa minkään valtion tai maantieteellisen alueen talouteen tai inflaatioon. Kansainvälistä Fisher-vaikutusta (engl. International Fisher Effect) käytettäessä vaihtokurssi on siis riippuvainen vain toista valuuttaa jakavan maan korkotasosta kryptovaluutan korkotason pysyessä nollana. Kryptovaluuttojen välisessä kaupassa korkotasoa tai inflaatiota hyödyntävät valuutan hinnoittelumallit menettävät merkityksensä täysin, sillä muuttujat ovat kummallakin kryptovaluutalla olemattomat. Tällöin joudutaan turvautumaan muihin hinnoittelumalleihin tai täysin spekulatiiviseen arvostukseen.

## 3.4 Hintakehitys spekulaation seurauksena

Vaikka kryptovaluutan ominaisuudet mahdollistavat sen käytön vaihdannan välineenä, on niiden kurssien volatiliteetti tehnyt oikean maailman käyttöönotosta monin kerroin haasteellisempaa. Esimerkiksi Bitcoinin markkinahinta on kokenut ±8000 prosentin muutoksia vuosien 2009-2014 välillä (Ciaian et al. 2016). Riskejä välttävän kauppiaan ei ole järkevää ottaa kryptovaluuttaa vastaan kauppaliiketoiminnassa, sillä kryptovaluutan dollari- tai euromääräinen arvo saattaa olla pudonnut merkittävästi siinä vaiheessa, kun sitä vaihdetaan fiat-valuutaksi. Käyttöönotto ja hyväksyntä tavanomaisessa kaupankäynnissä voisi mahdollisesti laskea kryptovaluuttojen volatiliteettia ja luoda positiivisen palautteen syklin arvonnousun, hinnan vakauden ja maksutilanteissa käytön kannalta.

Tällä hetkellä kryptovaluutan hintaan voidaan kuitenkin ajatella louhintakustannuksen lisäksi sisältyvän myös mittava spekulaatiopreemio. Hayesin (2015) mukaan spekulaatiopreemion vaikutus Bitcoinin hintaan on erittäin todennäköinen. Iwamura et al. (2014) esittävät, että kryptovaluutan hinta koostuu marginaalisesta tuotantokustannuksesta, uskottavuuselementin arvosta ja kuplaosuuden arvosta. Tässä hinnoittelumallissa uskottavuuselementin arvo asetetaan nollaksi, sillä kryptovaluutat eivät ole toistaiseksi minkään

valtion tunnustamia virallisia valuuttoja. Mallin kuplaosuuden arvoa ei voi etukäteen määritellä tai ennustaa, vaan sen suuruuden voi nähdä vain *post ante* vähentämällä kryptovaluutan arvosta sen marginaalisen tuotantokustannuksen. (Iwamura et al. 2014)

## 3.5 Markkinanäkemyksen vaikutus arvostukseen

Wang ja Vergne (2017) esittävät, että niin kutsuttu pöhinä (engl. buzz), eli positiivinen mielenkiinto ja innostuneisuus ovat olleet kryptovaluuttojen merkittävän tuoton taustalla. Yleisesti ottaen innovaatiopotentiaali uusissa kryptovaluutoissa koetaan arvokkaaksi, ja se nähdäänkin tärkeimpänä tekijänä tuottojen selittämisessä. Vaikka uusi teknologia ja sen tuomat innovaatiot rahansiirrossa ovat kryptovaluuttoihin sijoittaville ideologisesti tärkeää, osa kuitenkin näkee kryptovaluutat pelkästään vaihtoehtoisena sijoitusvälineenä. Glaser et al. (2014) kirjoittavat, että varsinkin teknologiaan tutustumattomat sijoittavat kryptovaluuttoihin mitä todennäköisimmin vain korkeiden tuottojen toivossa. Teknologian ja fundamenttien tuntemuksen puute mahdollistaa yksittäisen sijoittajan mielipiteiden ailahtelevaisuuden ja siten suuren potentiaalin mielipidevaikutukseen.

Yhdysvaltalaisen suurpankki JP Morganin toimitusjohtajan Jamie Dimonin syyskuussa 2017 Bloomberg-lehdelle antamassaan haastattelussa (Son et al. 2017) hän vertaa Bitcoinia tulppaaneihin viitaten Alankomaiden 1600-luvun tulppaanimaniaan. Dimon käytti myös muita teräviä sanankäänteitä ja uskoi, että kryptovaluutat kokonaisuutena ”eivät pääty hyvin”. Tämä haastattelu ja huhut, että Kiina aikoisi tehdä kryptovaluutoista laittomia, laskivat Bitcoinin hintaa monia kymmeniä prosentteja (CoinMarketCap 2018). Lohkoketjuteknologian ja kryptovaluutat tunteva ja niihin uskova sijoittaja ei välttämättä välittäisi huhupuheista tai herjauksesta, mutta kuten voidaan hintakehityksestä huomata, spekulaatiosijoittajat ja kryptovaluuttamarkkinat kenties ylireagoivat näihin epävarmuutta luoviin uutisiin. Dimon antoi helmikuussa 2018 toisen haastattelun aiheesta Bloombergille (Surane 2018) jossa hän yllättäen katui negatiivisia kommenttejaan kryptovaluuttoja kohtaan ja sanoi uskovansa teknologiaan kryptovaluuttojen takana. Markkinat eivät tällä kertaa reagoineet vastakkaisella tavalla, vaan Bitcoinin hinta pysyi samalla tasolla kuin se oli ennen uutisen julkaisua ollut (CoinMarketCap 2018).

Markkinanäkemyksen vaikutus näkyy myös positiiviseen suuntaan. Marraskuussa 2017 Bloomberg (van der Walt 2017) uutisoi siitä, miten Bitcoinin ostosuositukset ohittivat kullan ostosuositukset Internetin hakulauseiden mukaan mitattuna. Uutinen ei kerro mitään mullistavaa, mutta kuitenkin nostatti markkinoiden optimismia ja Bitcoinin hintatasoa. Bitcoinin markkinahinta nousikin pian kahteenkymmeneen tuhanteen dollariin, korkeimmalle mitä se on ikinä ollut, vain kuukausi uutisen julkaisun jälkeen (CoinMarketCap 2018). Näiden esimerkkien avulla voidaan päätellä, että uutismedialla ja siten markkinanäkemyksellä on suuri, ellei jopa suurin vaikutus kryptovaluuttojen arvostustasoihin. Kun kryptovaluuttojen teknologia ei muutu merkittävästi, voi medianäkyvyys vaikuttaa yleiseen mielipiteeseen ja siten sijoittajien varmuuteen tai epävarmuuteen kryptovaluuttoja kohtaan.

# 4. HINTAMANIPULAATIO KRYPTOVALUUTOISSA

Kryptovaluuttapörssien sääntelemättömyys ja lainsäädännöllisesti toistaiseksi rajoittamaton asema mahdollistavat vapaamman kaupankäynnin sijoittajien kesken, mutta samoista syistä ne ovat mielenkiintoisia myös epärehellisille toimijoille. Eritoten Bitcoinin ekosysteemi on ollut usein taloudellista hyötyä tavoittelevien rikollisten kohteena (Gandal et al. 2018). Esimerkiksi jonkun kryptovaluutan alkuvaiheilla toimineet louhijat ovat voineet saada merkittävän määrän kryptovaluuttaa haltuunsa ennen kuin se on tullut julkisesti saataville mihinkään pörssiin. Tällöin louhijan toimilla voi olla merkittäväkin vaikutus kurssiin.

Gandal et al. (2018) ovat tunnistaneet vuonna 2014 maksukyvyttömyydestä johtuen toimintansa lopettaneen Mt. Gox -pörssin vuodetuista transaktiolokeista kaksi todennäköisesti tietokoneiden ohjaamaa kaupankäyntiagenttia, jotka ovat onnistuneet ostamaan bitcoineja ilman varsinaista maksusuoritusta ja siten nostamaan Bitcoinin markkinahintaa. Silloin kun nämä agentit ovat olleet toiminnassa, Bitcoinin markkinahinta nousi keskimäärin 20 dollaria päivässä, kun taas ei-aktiivisina päivinä markkinahinta laski. (Gandal et al. 2018) Bitcoinin hinnan nousun 150 dollarista yli tuhanteen dollariin vuonna 2013 väitetäänkin johtuneen juuri näiden vilpillisten agenttien toimista (Hayes 2015; Gandal et al. 2018). Bitcoinin hintaa on siis aikaisemmin onnistuttu manipuloimaan hyödyntämällä haavoittuvuutta kaupankäyntialustalla. Kryptovaluuttapörssien lukumäärän kasvaessa ei voida olla täysin varmoja siitä, etteikö niissä olisi vastaavanlaisia haavoittuvuuksia. Hinnan manipulaatio saattaa siis olla mahdollista nykypäivänäkin.

Mahdollisuus manipulaatioon tai muuhun vilpilliseen toimintaan korostuu entisestään kryptovaluuttapörsseissä, joissa ei vaadita kaupankäyjän henkilöllisyyden tunnistusta. Pietersin ja Vivancon (2016) mukaan kryptovaluuttapörsseissä, joissa tunnistautumista ei vaadita, hintavaihtelu on suurempaa kuin tunnistautumisen vaativilla kauppapaikoilla. Anonyymeillä markkinoilla ei käydä kauppaa fiat-valuutalla, sillä kaupankäyjän henkilöllisyys voisi selvitä viimeistään dollari- tai euromääräisen maksusuorituksen tapahduttua. Vain kryptovaluutoilla kauppaa käyvät pörssit pystyvät siten siis toimimaan ilman rahaliikenteen sääntelyn tuomia rajoitteita ja reunaehtoja. Kun kaupankäyntiä ei voida valvoa tai auditoida sääntelyn puuttuessa, motivoituneet toimijat voivat mahdollisesti manipuloida kryptovaluutan kurssia epärehellisin keinoin. Ei voida suoranaisesti päätellä, että vapaammissa pörsseissä hintamanipulaatiota tapahtuisi enemmän tai useammin, mutta se voi olla yksi selittävä tekijä anonyymien pörssien suuremman hintavaihtelun takana.

Anonymiteetti kaupankäynnissä mahdollistaa myös rikollisen toiminnan rahoittamisen pörssin ulkopuolella. Wilson ja Yelowitz (2015) ovat tunnistaneet anekdootillisen aineiston perusteella rikolliset Bitcoinin yhdeksi käyttäjäryhmäksi. Maksusuorituksia rikollisesta toiminnasta on monimutkaista jäljittää, kun ne tapahtuvat kryptovaluutan anonyymissä lohkoketjussa. Pieters ja Vivanco (2016) teorioivat, että kryptovaluuttapörssejä sääntelevällä lainsäädännöllä saattaisi olla suurikin vaikutus kryptovaluuttojen kursseihin. Vaikutuksen laatua on kuitenkin vaikea arvioida. Tunnistautumisen vaatiminen voi vähentää kryptovaluutan käyttöä rikollisuudessa, jolloin rikollisten ostajien määrä, kiinnostus kryptovaluuttoja kohtaan ja siten niiden kurssi laskisi. Toisaalta lainsäädäntö voisi tuoda kryptovaluutat osakkeiden ja muiden sijoitusinstrumenttien tasolle, jolloin ne voisivat olla kiinnostavampia myös institutionaalisille sijoittajille. Lainsäädännön puuttuminen ei kuitenkaan ole vaatimus institutionaalisten sijoittajien mielenkiinnolle, sillä esimerkiksi Bitcoinille on jo olemassa orastava johdannaismarkkina (Hayes 2016).

Uusia kryptovaluuttoja voidaan myös luoda täysin epärehellisin tarkoitusperin. Kryptovaluuttojen avoimen lähdekoodin periaatteiden johdosta uuden kryptovaluutan luonti onnistuu parhaimmillaan minuuteissa kopioimalla Bitcoinin koodi ja aloittamalla uusi lohkoketjuverkosto. Onkin olemassa kryptovaluuttoja, jotka perustuvat melkein täysin Bitcoinin lähdekoodiin, kuten esimerkiksi Litecoin (Hayes 2016). Suurin ero Litecoinin ja Bitcoinin välillä on kymmenen minuutin tavoitteellisen lohkojen lisäämisajan vähentäminen kahteen ja puoleen minuuttiin, ja koska se on niin samankaltainen toteutukseltaan, ei sillä ole omaa white paper -julkaisuaan.

Litecoin ei kuitenkaan ole itsessään epärehellinen, sillä se noudattaa samoja hajautuksen ja tasavertaisuuden periaatteita kuin Bitcoin. Lánskýn (2016) mukaan on kuitenkin kryptovaluuttoja, joissa näitä periaatteita ei noudatettu. Esimerkiksi PayCoin kuuluu näihin epärehellisiin kryptovaluuttoihin. PayCoin ei esitellyt uusia innovaatioita tai teknologioita lohkoketjun parantamista varten, mutta sen hinta saavutti suhteellisen korkean arvostustason uutuusarvon ja innovaation puutteesta huolimatta. PayCoinin arvostus laski kuitenkin murto-osiin alkuperäisestään, kun kävi ilmi, että sen kehittäjät olivat keränneet miljoonien arvosta PayCoinia omaan käyttöönsä ennen louhinnan varsinaista aloittamista. (Lánský 2016) Jos kehittäjä perustaisi oman kryptovaluuttansa sekä oman pörssinsä sen kaupankäyntiä varten, olisi hänellä silloin otollinen mahdollisuus manipuloida kryptovaluutan kurssia ja saavuttaa merkittävää taloudellista hyötyä. Tällöin kehittäjän pitäisi siis kerätä itselleen paljon kryptovaluuttaa ennen sen toiminnan aloittamista tai vaihtoehtoisesti muokata pörssialustaa siten, että voisi saada valuuttaa haltuunsa vilpillisin keinoin ja vain odottaa kryptovaluutan arvonnousua. Wang ja Vergne (2017) esittävät, että joidenkin kryptovaluuttojen tapauksessa arvonnousu onkin ollut epärehellisten tai laittomien keinojen käytön seurausta.

# 5. KRYPTOVALUUTTOJEN HINTAKUPLA

Talouden hintakuplalla tarkoitetaan sellaista markkinatilannetta, missä sijoituspäätöksiä tehdään puhtaasti spekulaatiotarkoituksessa ja päätöksiä ei perusteta sijoituskohteen fundamentteihin tai muihin rationaalisiin tekijöihin. (Cheah & Fry 2015) Voidaan väittää, että kryptovaluuttojen tapauksessa, kun hintaa ei voida perustaa osakkeiden kaltaisiin fundamentteihin ja siten niihin sijoittaminen on pelkkää spekulaatiota, kryptovaluuttojen hinnat ovat alati kuplautuneet. Tässä luvussa esitellään hintakuplien teoriaa ja tutkitaan perusteluja väitteelle kryptovaluuttojen hintakuplasta.

## 5.1 Talouden hintakupla käsitteenä

Kaikki omaisuuserät joilla voidaan käydä julkisesti kauppaa voivat olla hintakuplassa. Hintakuplien teoriassa tarkastellaan kuitenkin useimmiten osakkeita, sillä niiden hintatiedot ovat yleisesti ottaen hyvin saatavilla. Shiller (2014) väittää, että pörssikurssien volatiliteetille ei ole olemassa mitään yksiselitteistä syytä, mutta sijoittajapsykologia voi olla perimmäisenä tekijänä sen taustalla. Jos yhtiöltä ei ole tullut mitään osakekurssiin vaikuttavaa uutta tietoa, hinta kuitenkin liikkuu. Ei voida tietää, onko joillain sijoittajilla muita parempaa tietoa, vai perustuuko liikehdintä toivoon tulevaisuuden arvonnoususta. Ensimmäinen vaihtoehto ei ole välttämättä väärä, sillä kaikilla sijoittajilla ei ole pääsyä samoihin uutislähteisiin ja informaatiokanaviin. Uutismedia voi olla myös epätäydellinen – joitain huonoja asioita voidaan kaunistella tai hyviä asioita vähätellä riippuen siitä mikä on milloinkin markkinatilanteelle edullista (Shiller 2014).

Dalen et al. (2005) mukaan kuplat voivat olla joko rationaalisia tai irrationaalisia. Rationaalisissa kuplissa sijoittajalla on odotus siitä, että saa omaisuuseränsä myytyä ostohintaa korkeammalla. Irrationaalinen kupla voi taas ilmentyä joko sisäsyntyisenä (engl. intrinsic), jolloin omaisuuserän fundamentit vain arvotetaan väärin, tai ulkoapäin tulevana (engl. extrinsic), jolloin hinnoittelu pohjautuu täysin fundamenteista riippumattomiin tekijöihin. Uutismedian vaikutus korostuu entisestään ulkoapäin tulevassa kuplassa, sillä se pystyy vaikuttamaan suuren yleisön mielipiteeseen jostain sijoituskohteesta.

## 5.2 Hintakuplan ilmentymä kryptovaluutoissa

Cheahin ja Fryn (2015) mukaan kupla Bitcoinissa on ilmeisen suuri, ja kryptovaluutalla ei ole perustavanlaatuista arvoa. Koska kryptovaluutta ei edusta omistajuutta yhtiössä tai tuota omistajalle arvoa muuten, ei arvotukseen pystytä käyttämään osakkeiden hinnoittelumalleja. Hinnan kehitys perustuu siis pohjimmiltaan spekulatiivisiin tekijöihin. Tämän lisäksi hinnan liikehdintä mahdollistaa markkinanäkemyksen merkittävän vaikutuksen,

mikä voi aiheuttaa lisää volatiliteettia. Wangin ja Vergnen (2017) mukaan medianäkyvyys voi myös johtaa uusien käyttäjien aaltoihin ja siten kupliin. Ciaian et al. (2016) teorioivat myös, että varsinkin lyhyen aikavälin spekulointi kryptovaluutoilla voi aiheuttaa kuplia.

Cheahin ja Fryn (2015) mukaan kryptovaluuttamarkkinoilla ilmenee useita Shillerin (2014) ehdottamia spekulatiivisen kuplan muodostusta edistäviä tekijöitä. Näitä tekijöitä ovat muun muassa sosiaalipsykologian vaikutus, epätäydellinen uutismedia ja erilaisten informaatiokanavien laatu. Kryptovaluuttojen ollessa sääntelemättömiä omaisuuseriä, osalla sijoittajista saattaa olla tietoa, jota ei voisi uutismedian tai muiden informaatiokanavien kautta saada. Iwamura et al. (2014) teorioivat, että kiinnostus muita kryptovaluuttaa kuin Bitcoinia kohtaan voisi poistaa kryptovaluuttamarkkinan kuplan. Tällöin kryptovaluuttojen hinnoittelu ei olisi riippuvainen Bitcoinin kuplautuneesta hinnasta, vaan hinnoittelu tapahtuisi kunkin valuutan vahvuuksien ja fundamenttien perusteella.

Fundamentteihin perustuva markkinatilanne ei kuitenkaan välttämättä poista kuplaa, vaan muuttaa sen vain rationaaliseksi, sillä on vaikea kuvitella, että kryptovaluuttaa ostettaisiin ilman odotusta arvonnoususta ja korkeammista myyntihinnoista. Rationaalinen hintakupla voi silti kokea massahysterian ajanjaksoja muuttumatta kuitenkaan irrationaaliseksi (Cheah & Fry 2015). Työssä käytetty lähdeaineisto ei ota kantaa siihen, ovatko kryptovaluuttamarkkinat rationaalisessa vai irrationaalisessa kuplassa. Kryptovaluuttamarkkinat ovat kuitenkin pohjimmiltaan kuplautuneet (Cheah & Fry 2015) ja saattaakin olla, että kupla kokee rationaalisuuden ja irrationaalisuuden syklejä. Tässä tilanteessa analyysi kuplan laadusta olisi aina tilannesidonnaista, ja kenties vain jälkeenpäin todettavissa.

# 6. PÄÄTELMÄT

Tämän kandidaatintyön tavoitteena oli etsiä kryptovaluuttojen arvon muodostajia, tutkia hintamanipulaation mahdollisuuksia ja tarkastella kryptovaluuttamarkkinoiden hintakuplaa. Lähdeaineiston perusteella havaittiin useita arvostukseen vaikuttavia tekijöitä, todisteita hintamanipulaatiosta menneisyydestä sekä perusteltuja argumentteja kryptovaluuttojen hintakuplan olemassaolosta.

Kryptovaluutat ovat pohjimmiltaan vaihdannan välineitä kuten kulta tai valtion liikkeelle laskema valuutta (Cheah & Fry 2015). Niiden arvo ei kuitenkaan ole riippuvainen mistään yksittäisestä tekijästä. Tästä johtuen kryptovaluuttoja käytetään yleisemmin spekulatiiviseen sijoitukseen kuin maksusuorituksiin. Huolimatta vähäisestä käyttöönotosta tavanomaisissa maksutilanteissa kryptovaluuttojen arvostus perustuu teknologiseen innovaatioon ja uutuusarvoon (Wang & Vergne 2017). Iwamura et al. (2014) ovat tunnistanet hajautetun lohkoketjuteknologian ja julkisen avaimen kryptografian kryptovaluuttojen keskeisimmiksi innovaatioiksi.

Koska kryptovaluuttaa voi saada haltuunsa joko louhimalla tai ostamalla, on niiden arvon muodostusta mielekästä tutkia joko louhintakustannuksiin tai spekulaatioon perustuvan mallin mukaan. Hayesin (2016) mukaan kryptovaluutan louhintavaikeus, eli valuutan tuotto laskentatehon yksikköä kohden määrittelee mitä kryptovaluuttaa louhijan laitteistolla olisi kannattavaa louhia. Vaikeuden lisäksi sähkön hinta, louhintalaitteiston sähkönkulutus ja Bitcoinin markkinahinta muodostavat kryptovaluutan hinnalle alarajan, jotta kryptovaluutan louhiminen olisi mallin mukaisesti kannattavaa. Jos hinta alittaa tämän rajan, voivat louhijat vaihtaa louhintansa kohdetta ja kohdistaa laskentatehonsa sellaiseen kryptovaluuttaan, jonka louhiminen on kannattavampaa. (Hayes 2016)

Markkinanäkemyksellä on suuri, ellei jopa merkittävin vaikutus kryptovaluuttojen arvostukseen. Koska olemassa olevien kryptovaluuttojen teknologia muuttuu harvoin, positiivinen tai negatiivinen uutisointi aiheesta voi vaikuttaa sijoittajien mielipiteisiin kryptovaluutoista sijoituskohteena ja siten niiden arvostuksiin. Ilmiö korostuu varsinkin niiden sijoittajien kohdalla, joille kryptovaluutat ovat vain yksi sijoituskohde toisten lomassa eikä uusi teknologinen innovaatio. Teknologiaan tutustumattomat sijoittavatkin kryptovaluuttoihin todennäköisemmin vain korkeiden tuottojen toivossa (Glaser et al. 2014).

Keskeisimmät kryptovaluuttojen arvostukseen vaikuttavat tekijät on kerätty taulukkoon 1. Louhimisen kustannuksilla on negatiivinen vaikutus, sillä jos ne nousevat liian korkealle, pystyvät louhijat vaihtamaan louhintansa kohdetta ja siten laskemaan kryptovaluutan arvoa. Markkinanäkemyksen vaikutus voi olla joko positiivista tai negatiivista, mutta se vaikuttaa yleisesti ottaen kaikkiin kryptovaluuttoihin samansuuntaisesti. Kryptovaluutta

pystyy saavuttamaan korkean arvostuksen ainakin hetkellisesti, vaikka sillä ei olisi mitään taulukkoon kerätyistä tekijöistä, kuten kävi PayCoinin tapauksessa (Lánský 2016). Jos tällainen ominaisuuksiltaan kehno kryptovaluutta saavuttaa korkean arvostuksen, on kuitenkin mahdollista, että sen hinta on noussut vilpillisten, kenties jopa laittomien keinojen seurauksena.

| **Tekijä** | **Vaikutus** |
|---|---|
| Hajautettu lohkoketjuverkosto | Positiivinen |
| Teknologinen innovaatio | Positiivinen |
| Käyttöönotto tavanomaisissa maksutilanteissa | Positiivinen |
| Markkinanäkemys | Positiivinen tai negatiivinen |
| Louhimisen kustannukset | Negatiivinen |

***Taulukko 1.*** *Kryptovaluuttojen arvonmuodostukseen vaikuttavat tekijät*

Kryptovaluuttoja on nykyisessä muodossaan ollut olemassa vain noin kymmenen vuotta. Koska kryptovaluutoilla käydään kauppaa sääntelemättömillä pörsseillä, on sen hinta sijoittajien näkemyksen armoilla. Innovatiivinen teknologia yhdistettynä sen uutuuteen vaikeuttaa sen arvon täsmällistä arviointia. Tämän lisäksi kryptovaluutan kurssia on mahdollista manipuloida hyödyntämällä haavoittuvuuksia kryptovaluuttapörssissä. Tunnetuin esimerkki hintamanipulaatiosta tapahtui vuoden 2013 lopulla, kun Bitcoinin kurssi nousi yli tuhanteen dollariin (Hayes 2015; Gandal et al. 2018).

Kryptovaluuttojen hintojen kehitys esittää todisteita siitä, että kryptovaluuttamarkkina on kuplautunut. Kryptovaluuttojen arvotukseen ei ole olemassa mitään yksiselitteistä tai yleiskäyttöistä laskukaavaa, joten kaikki sijoittaminen kryptovaluuttoihin on jossain määrin spekulointia. Markkinanäkemyksellä on tällöin suuri vaikutus hintoihin, ja positiivinen medianäkyvyys voi johtaa ylettömään optimismiin, uusien käyttäjien aaltoihin ja siten kuplien syntymiseen (Wang & Vergne 2017).

Kryptovaluutat ovat tutkimuskohteena uusia, ja olisi mielenkiintoista nähdä uutta tutkimusta kandidaatintyössä käsitellyistä aiheista. Kuten Iwamura et al. (2014) ja Hayes (2016) totesivat, Bitcoin on tällä hetkellä keskeisessä osassa muiden kryptovaluuttojen hinnoittelussa. Tutkimusta voisi tehdä siitä, miten paljon Bitcoinin ylivoimaisuus vaikuttaa muiden kryptovaluuttojen hinnoitteluun ja siitä, voidaanko yksittäiselle kryptovaluutalle muodostaa osakemarkkinoilla yleisesti riskin määritykseen käytettyä beta-kerrointa. Beta-kertoimen avulla pystyttäisiin määrittelemään, miten paljon kryptovaluutan hinta on sidoksissa Bitcoinin tai kryptovaluuttojen markkinaportfolion hinnan muutoksiin.

# LÄHTEET

Back, A. (2002). Hashcash - A Denial of Service Counter-Measure, http://www.hashcash.org/papers/hashcash.pdf.

Bernstein, D.D. (2008). Protecting communications against forgery, in: Anonymous (ed.), Algorithmic Number Theory, Cambridge University Press, pp. 535.

Bitfury Group (2015). Proof of Stake versus Proof of Work, http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf.

Brandvold, M., Molnar, P., Vagstad, K. & Andreas Valstad, O.C. (2015). Price Discovery on Bitcoin Exchanges, Journal of International Financial Markets, Institutions and Money, Vol. 36 pp. 18–35. https://www.sciencedirect.com/science/article/pii/S104244311500027X.

Cheah, E. & Fry, J. (2015). Speculative Bubbles in Bitcoin Markets? An Empirical Investigation into the Fundamental Value of Bitcoin, Economics Letters, Vol. 130 pp. 32-36. https://www.sciencedirect.com/science/article/pii/S0165176515000890.

Ciaian, P., Rajcaniova, M. & Kancs, d. (2016). The economics of BitCoin price formation, Applied Economics, Vol. 48(19), pp. 1799-1815. http://www.tandfonline.com/doi/abs/10.1080/00036846.2015.1109038.

CoinMarketCap (2018). Kuvaaja Bitcoinin markkinahinnasta, https://coinmarketcap.com/currencies/bitcoin/#charts.

Dale, R.S., Johnson, J.E.V. & Tang, L. (2005). Financial markets can go mad, The economic history review, Vol. 58(2), pp. 233-271. http://www.econis.eu/PPNSET?PPN=486278921.

Dwyer, G.P. (2015). The Economics of Bitcoin and Similar Private Digital Currencies, Journal of Financial Stability, Vol. 17 pp. 81-91.

Gandal, N., Hamrick, J.T., Moore, T. & Oberman, T. (2018). Price Manipulation in the Bitcoin Ecosystem, Journal of Monetary Economics, https://www.sciencedirect.com/science/article/pii/S0304393217301666.

Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M.C. & Siering, M. (2014). Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247.

Hayes, A. (2016). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin, Telematics and Informatics, https://www.sciencedirect.com/science/article/pii/S0736585315301118.

Hayes, A. (2015). What factors give cryptocurrencies their value: An empirical analysis, https://ssrn.com/abstract=2579445.

Iwamura, M., Kitamura, Y. & Matsumoto, T. (2014). Is bitcoin the only cryptocurrency in the town? http://www.econis.eu/PPNSET?PPN=786124326.

Iwamura, M., Kitamura, Y., Matsumoto, T. & Saito, K. (2014). Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money, http://hdl.handle.net/10086/26940.

King, S. & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, https://peercoin.net/assets/paper/peercoin-paper.pdf.

LeMahieu, C. (2017). Nano: A Feeless Distributed Cryptocurrency Network, https://nano.org/en/whitepaper.

Li, X. & Wang, C.A. (2016). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin, Decision Support Systems, Vol. 95 pp. 49. https://www.sciencedirect.com/science/article/pii/S0167923616302111.

Lánský, J. (2016). Analysis of Cryptocurrencies Price Development, Acta Informatica Pragensia, Vol. 5(2), pp. 118-137.

Mazieres, D. (2016). The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus, https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

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

Pieters, G. & Vivanco, S. (2016). Financial regulations and price inconsistencies across bitcoin markets, 45 p.

Polasik, M., Piotrowska, A.I., Wisniewski, T.P., Kotkowski, R. & Lightfoot, G. (2015). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry, International Journal of Electronic Commerce, Vol. 20(1), pp. 9-49. http://www.tandfonline.com/doi/abs/10.1080/10864415.2016.1061413.

Poon, J. & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, https://lightning.network/lightning-network-paper.pdf.

Popov, S. (2018). The Tangle, https://www.iota.org/IOTA_Whitepaper.pdf.

Shiller, R.J. (2014). Speculative asset prices, The American economic review, Vol. 104(6), pp. 1486-1517. http://www.econis.eu/PPNSET?PPN=797093621.

Son, H., Levitt, H. & Louis, B. (2017). Jamie Dimon Slams Bitcoin as a 'Fraud', Bloomberg, https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin.

Surane, J. (2018). Dimon Says He Regrets Calling Bitcoin a 'Fraud', Bloomberg, https://www.bloomberg.com/news/articles/2018-01-09/dimon-says-he-regrets-bitcoin-comments-calls-blockchain-real.

van der Walt, E. (2017). 'Buy Bitcoin' Overtakes 'Buy Gold' as Online Search Phrase, Bloomberg, https://www.bloomberg.com/news/articles/2017-11-07/bitcoin-rally-is-eroding-gold-s-appeal-top-online-vaulter-says.

Wang, S. & Vergne, J. (2017). Buzz Factor or Innovation Potential: What Explains Cryptocurrencies' Returns? PLoS One, Vol. 12(1), pp. e0169556. http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0169556.

Yelowitz, A. & Wilson, M. (2015). Characteristics of Bitcoin users: an analysis of Google search data, Applied Economics Letters, Vol. 22(13), pp. 1030-1036. http://www.tandfonline.com/doi/abs/10.1080/13504851.2014.995359.