**Hentter Eloranta**

# Lohkoketjut kryptovaluutoissa

Tietotekniikan kandidaatintutkielma

10. kesäkuuta 2018

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

**Tekijä:** Hentter Eloranta

**Yhteystiedot:** hentter.i.eloranta@student.jyu.fi

**Ohjaaja:** Sanna Juutinen

**Työn nimi:** Lohkoketjut kryptovaluutoissa

**Title in English:** Blockchains in cryptocurrencies

**Työ:** Kandidaatintutkielma

**Sivumäärä:** 22+0

**Tiivistelmä:** Kryptovaluutat ovat kasvattaneet suosiotaan ja niiden pohjana toimiva teknologia, lohkoketju, on saanut huomiota sen ominaisuuksien takia. Tutkielmassa selvitetään, miten lohkoketjuja käytetään apuna kryptovaluuttojen hallinnassa ja miten kaksi isointa kryptovaluuttaa eroaa toteutukseltaan toisistaan. Yksi luku käsittelee myös kryptovaluuttojen markkinoita ja luku pyrkii selvittämään syitä markkinoiden kasvuun/nousuun.

**Avainsanat:** Lohkoketju, Bitcoin, Ethereum, Ether

**Abstract:** Cryptocurrencies are becoming more popular and the technology behind them, blockchain, is attracting attention because its properties. The goal of this study is to find out how blockchains are used with cryptocurrencies and find differences in the two biggest cryptocurrencies. One chapter is about the cryptocurrency market; how and why the market has risen/fallen.

**Keywords:** Blockchain, Bitcoin, Ethereum, Ether

# Kuviot

# Sisältö

# 1 Johdanto

Ensimmäinen kryptovaluutta, Bitcoin, sai alkunsa vuonna 2008. Nimimerkki Satoshi Nakamoto julkaisi tuolloin artikkelin ”Bitcoin: A Peer-to-Peer Electronic Cash System”, jossa esiteltiin uudenlainen valuuttatyyppi, Bitcoin, jonka toiminta perustuu lohkoketjuihin. Lohkoketju on hajautettu ja julkinen tietokanta, joka koostuu lohkoista (Nakamoto 2008). Jokainen lohko sisältää tietoa, Bitcoinin tapauksessa mm. aikaleiman, tiivisteitä ja siirtoja. Käyttäjät voivat itse lisätä uusia lohkoja lohkoketjuun, mutta heidän pitää osoittaa, että heidän lohkonsa on validi, yleensä raskaiden laskutoimituksien avulla. Lohkon lisäyksen jälkeen kaikki käyttäjät saavat tiedon lisätystä lohkosta. Koska käyttäjät joutuvat käyttämään paljon laskentatehoa muuttaakseen ketjua ja koska heillä kaikilla on kopio lohkoketjusta, lohkoketju on turvallinen. Hyökkääjän pitäisi hallita yli 50% lohkoketjun laskentatehosta, jotta hän voisi lisätä omia lohkojaan tai muokata vanhoja kenenkään huomaamatta.

Kryptovaluutat ovat viime vuosina kasvattaneet suosiotaan ja monet ovat sijoittaneet kryptovaluuttoihin tai käyttävät niitä. Hileman & Rauchs (2017) arvioivat, että aktiivisia käyttäjiä on 2,9–5,8 miljoonaa. Lukumäärää on kuitenkin hankala arvioida, koska käyttäjällä voi olla useita lompakoita eri palveluissa. Aktiivisia lompakoita heidän mukaansa on 5,8–11,5 miljoonaa. Jotkin internetkaupat hyväksyvät kryptovaluuttoja maksuvälineinä ja yksi suosituimmista alustoista, Ethereum, on saanut tukijoikseen monia isoja yrityksiä, kuten Intelin ja Microsoftin. Monet yritykset ja ihmiset siis uskovat, että lohkoketjuja apuna käyttävä kryptovaluutta voisi tulevaisuudessa ehkä korvata tavallisen valuutan maksuvälineenä.

Kryptovaluutoista tekee erikoisen se seikka, että käyttäjät luovat itse lisää valuuttaa samalla, kun he käyttävät sitä (Nakamoto 2008). Tätä prosessia kutsutaan louhinnaksi ja jokainen pystyy osallistumaan siihen. Toinen erikoinen kryptovaluuttojen ominaisuus tavallisiin valuuttoihin verrattuna on se, että ne ovat hajautettuja, eikä mikään pankki tai hallitus hallitse niitä. Muutamat maat, kuten Kiina, ovat kuitenkin yrittäneet rajoittaa louhintaa tai kryptovaluuttojen käyttöä.

Kryptovaluuttojen markkinat ovat kasvussa ja niiden yhteenlaskettu markkina-arvo vuoden 2018 maaliskuun alussa oli n. 450 miljardia dollaria (Katso kuvio 4). Kurssit saattavat nousta tai laskea jopa satoja prosentteja päivissä ja siksi sijoittaminen on riskialtista, mutta suuret voitot ovat mahdollisia.

Lohkoketjuja käytettiin aluksi kryptovaluuttojen hallintaan, mutta nykyään niitä voisi käyttää muihinkin käyttötarkoituksiin. Kuten Linn & Koo (2016) kertovat, terveydenhuollossa on mahdollista rakentaa turvallinen ja jaettava tietokanta potilaiden tiedoista ja näin parantaa terveydenhuollon tilaa, kun tutkijoiden olisi mahdollista tehdä jopa vuosikymmenien pitkittäistutkimuksia, koska kaikki tiedot säilyisivät tallessa lohkoketjussa. Elintarvikkeiden alkuperää voisi seurata RFID-sirujen ja lohkoketjujen avulla (Tama ym. 2017).

Ethereum sopii hyvin älykkäiden sopimuksien tekoon (Patel ym. 2017). Älykkäillä sopimuksilla on esimerkiksi mahdollista kerätä joukkorahoitusrahaa projekteihin ilman kolmatta osapuolta. Jos projekti ei saavuta haluttua summaa, rahat palautuvat automaattisesti takaisin rahoittajille.

Kryptovaluuttoja on kritisoitu virrankulutuksen takia. Bitcoin-verkosto käytti vuonna 2017 n. 10 TWh vuodessa, joka vastaa Uruguayn virrankulutusta (Hileman & Rauchs 2017). Tehonkulutus on kuitenkin jo vuodessa moninkertaistunut ja siksi jotkin kryptovaluutat, kuten Peercoin, käyttävät Proof-of-Stake–validointimenetelmää vähentääkseen virrankulutusta (King & Nadal 2012).

Tutkielma on toteutettu tekemällä kirjallisuuskatsaus artikkeleihin, jotka käsittelevät kryptovaluuttoja tai niiden markkinoita. Tutkielman toisessa luvussa avataan käsitteitä ja kerrotaan lohkoketjujen rakenteesta ja kuinka lohkoketjut toimivat. Kolmannessa luvussa tutkitaan kahden isoimman ja kuuluisimman kryptovaluutan, Bitcoinin ja Ethereumin, ominaisuuksia ja vertaillaan niitä. Tarkoituksena on selvittää, miten erot, kuten lohkojen luontinopeus, vaikuttavat käyttöön. Neljäs luku käsittelee kryptovaluuttojen markkinoita. Luvussa yritetään löytää yleisiä syitä kurssien laskuun ja nousuun, ja tutkia hintojen kehitystä. Viimeinen luku on yhteenveto tutkielman löydöistä.

# 2 Käsitteet ja Lohkoketjut

Kryptovaluutat käyttävät lohkoketjuja ja tämä luku käsittelee yleisesti lohkoketjujen rakennetta ja toimintaa. Painotus on kuitenkin kryptovaluutoissa ja niiden käyttämissä tekniikoissa.

## 2.1 Käsitteitä ja avainsanoja

**Lohkoketju (Blockchain) =** Lohkoketju on julkinen ja turvallinen tietokanta. Jokainen lohko sisältää tietoa esimerkiksi siirroista ja käyttäjät voivat lisätä lohkoja lohkoketjuun. Lohkoketjua ei voi muokata jälkikäteen (Nakamoto 2008).

**Lohko (Block) =** Lohko sisältää haluttua dataa ja informaatiota lohkosta, kuten sen indeksin, luontiajan ja tarvittaessa muita tietoja. Lohkoa voi verrata listan alkioon (Bitcoin Dokumentaatio 2018).

**Proof-of-work (PoW) =** Louhija todistaa, että lohko on aito ja validi käyttämällä resursseja, kuten paljon laskentatehoa liittääkseen lohkon lohkoketjuun (Nakamoto 2008).

**Proof-of-stake (PoS) =** Louhijan omistama osuus kryptovaluutasta antaa hänelle tietyn todennäköisyyden louhia lohko. Ei käytä paljoa laskentatehoa (King & Nadal 2012).

**Louhinta (Mining) =** Kryptovaluuttojen louhinta tarkoittaa validin lohkon liittämistä lohkoketjuun.

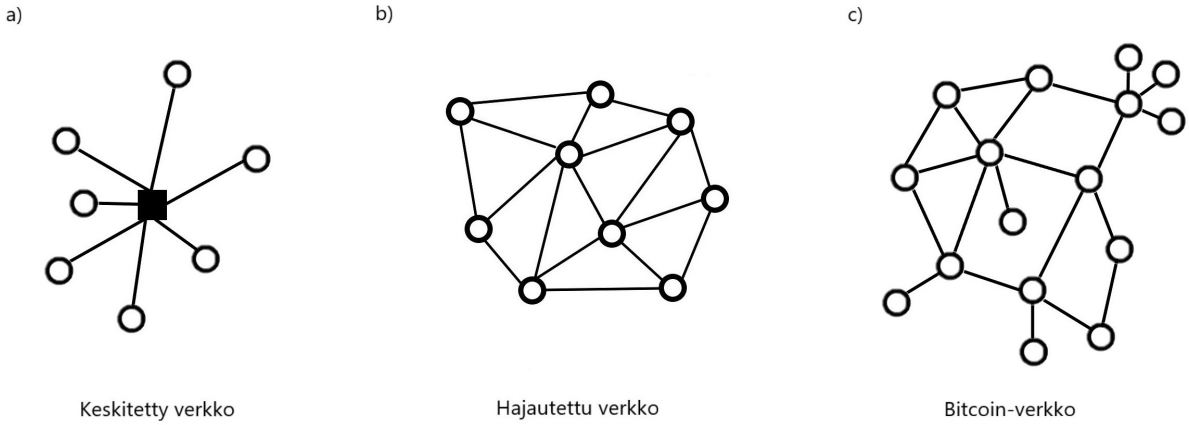
**Tiiviste (Hash) =** Tiiviste on kiinteän mittainen merkkijono, jonka saa syöttämällä tiivistefunktiolle merkkijonon. Tiiviste on nopea laskea merkkijonolle, mutta melkein mahdoton kääntää takaisin merkkijonoksi järkevässä ajassa. Tiivistettä käytetään varmistamaan, että käyttäjät lisäävät valideja lohkoja lohkoketjuun (Patel ym. 2017).

**Älykkäät sopimukset (Smart contracts) =** Käyttäjien luoma elektroninen sopimus,

joka tallennetaan lohkoketjuun. Jos sopimuksen ehdot täyttyvät, sopimus saa siitä tiedon automaattisesti ja sopimuksen sisältö suoritetaan (Patel ym. 2017).

## 2.2 Lohkoketjujen rakenne ja toiminta

Lohkoketju on hajautetussa verkossa eli vertaisverkossa toimiva tietokanta, jonka jokaisella käyttäjällä on kopio siitä (Katso kuvio 1). Aina uuden lohkon lisäyksen jälkeen käyttäjät lähettävät lisätyn lohkon tiedot läheisille käyttäjille, jotka puolestaan lähettävät tiedon eteenpäin. Tietokannan hajautuksella saavutetaan paljon etuja keskitettyyn tietokantaan verrattuna. Käyttäjien ei tarvitse luottaa kolmanteen osapuoleen, kuten palvelimien ylläpitäjään. Hajautetussa verkostossa on enemmän laskentatehoa ja verkosto kestää paremmin hyökkäyksiä (Patel ym. 2017). Hyökkääjän pitäisi hallita yli 50% verkoston solmuista, jotta lohkoketjua voisi muuttaa.

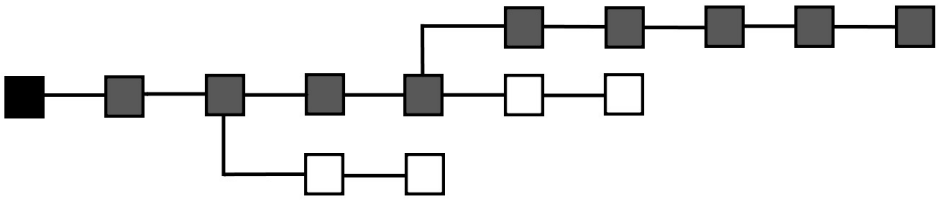



Kuvio 1. Verkkojen eroja

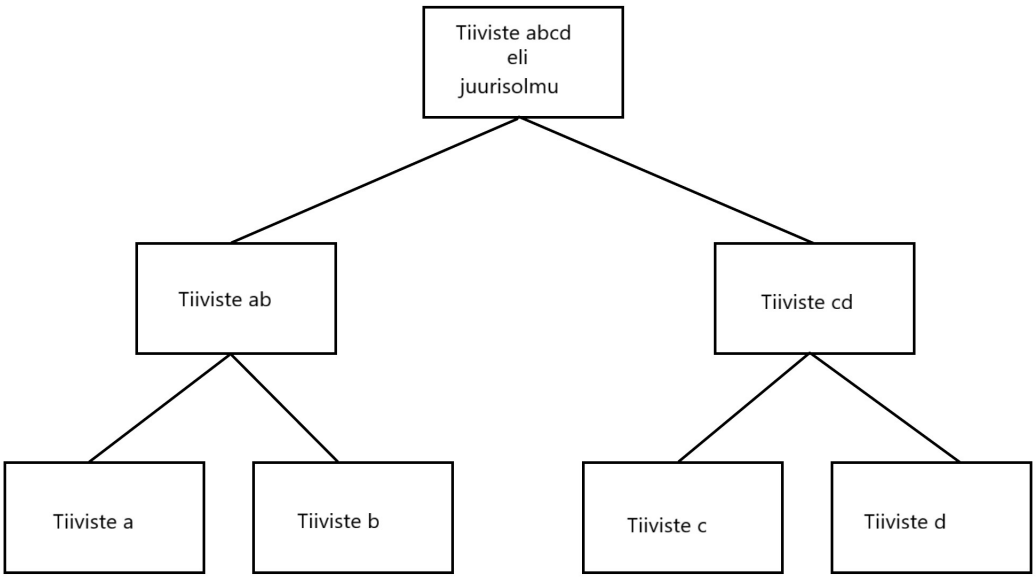
Kuvio 2 selventää lohkoketjun rakennetta. Jokainen lohko on linkitetty vain edelliseen lohkoon, joten lohko ei tiedä muista lohkoista mitään. Lohkoketjua pitkin voi kulkea takaisin tarkastelemaan edellisiä lohkoja aina ensimmäiseen lohkoon asti. On mahdollista, että kaksi käyttäjää lisää lohkoketjuun uuden lohkon lähes samaan aikaan, jolloin lohkoketju haaraantuu. Mutta kuten Nakamoto (2008) selittää, se ei ole ongelma, koska käyttäjät tallentavat lisätyn lohkon tiedot, kunnes jälleen uusi lohko lisätään lohkoketjuun. Uusi lohko voidaan lisätä kumpaan haaraan tahansa, mutta lohkoketjussa ei saa olla kuin yksi haara, joten lyhyemmän haaran lohkot mi-

tätöidään.

Lohkot sisältävät dataa. Kryptovaluuttojen tapauksessa useimmiten siirtoja, joita voi olla tuhansia lohkossa, jonka takia käyttäjän ei ole järkevää tallentaa koko lohkoketjua. Siksi useimmat kryptovaluuttojen lohkoketjut käyttävät Merkle-puuta apunaan siirtojen validoinnissa (Katso kuvio 3). Siirroista rakennetaan tiiviste-puu-tietorakenne ja lehtisolmujen tiivisteet yhdistetään ja tallennetaan niiden vanhempaan. Näin edetään kohti juurisolmua. Juurisolmu on jokaisen lehtisolmun yhdistetty tiiviste ja tämä tiiviste tallennetaan lohkoon (Patel ym. 2017). Käyttäjät voivat tarkastaa siirrot tällä tavoin myös mobiililaitteilla.



Kuvio 2. Lohkoketjun rakenne




Kuvio 3. Merkle-puun toiminta

# 3 Kryptovaluutat

Tässä luvussa käsitellään kahden kryptovaluutan lohkoketjuja, Bitcoinia ja Ethereumia, ja vertaillaan niiden ominaisuuksia ja eroavaisuuksia. Kryptovaluuttojen dokumentaatiota tullaan käyttämään apuna, koska kirjallisuus ei käsittele varsinkaan Ethereumin toteutusta kovinkaan paljoa. Ethereum on Bitcoinin isoin kilpailija ja toiseksi suurin kryptovaluutta-alusta. Sen kehittäjien mielestä Bitcoinin toteutus oli puutteellinen, eikä Bitcoin ollut tarpeeksi modulaarinen tai monipuolinen ja Ethereum yrittää ratkaista nämä puutteet (Ethereum White Paper 2018). Ethereumin lähdekoodi on avoin, ja se on modulaarinen, universaalinen ja helppokäyttöinen lohkoketjualusta, jonka avulla käyttäjät voivat luoda omia kryptovaluuttoja, älykkäitä sopimuksia ja sovelluksia, jotka käyttävät lohkoketjuja. Käyttäjät voivat muuttaa protokollia tarpeen mukaan, joten Ethereum alusta on helposti muokattavissa omaan käyttöön sopivaksi.

## 3.1 Bitcoin

Bitcoin on ensimmäinen ja tällä hetkellä isoin kryptovaluutta, jonka markkinaprosentti kaikista kryptovaluutoista on n. 40% (Katso kuvio 5). Patel ym. (2017) mukaan Bitcoin verkoston laskentateho on yli 40 000 kertainen verrattuna maailman 500 tehokkaimman supertietokoneen yhteenlaskettuun laskentatehoon. Kuten aiemmin on mainittu, hyökkääjän pitäisi hallita yli 50% verkon laskentatehosta muuttaakseen lohkoketjua ja käyttääkseen aiemmin siirretyt rahat uudelleen. Mutta Nakamoto (2008) uskoo että hyökkääjän ei ole järkevää muuttaa lohkoketjua, koska samalla laskentateholla hän saisi louhittua uusia kolikoita todella tehokkaasti ja näin käyttää resurssit paremmin.

Monet tutkijat, kuten Kaushal ym. (2017) sanovat Bitcoinin olevan täysin hajautettu, mutta tämä ei pidä täysin paikkaansa. Kuten Walch (2015) kirjoittaa, Bitcoinverkolla on myös keskitetyn järjestelmän ominaisuuksia (Katso kuvio 1). Käyttäjät voivat perustaa louhintaryhmiä (engl. mining pool) ja Bitcoinin taustalla on pieni

joukko ihmisiä, joilla on valta muuttaa Bitcoinin lähdekoodia. Bitcoin-verkostolla ei kuitenkaan ole keskussolmuja, vaikka lompakoita ylläpitävät yritykset voivatkin vaikuttaa niiltä. Nämä yritykset eivät ole ydinosa Bitcoin-verkostoa ja hyökkäys näitä kohtaan ei vaaranna Bitcoin-verkkoa.

Bitcoinin lohkoketjun yhden lohkon koko voi olla maksimissaan 1MB ja se koostuu seuraavista kentistä;

1. ”taikaluvusta”, joka on aina 0xD9B4BEF9,
2. luvusta, joka kertoo lohkon koon,
3. otsakkeesta,
4. luvusta, joka kertoo siirtojen määrän ja
5. siirroista.

Otsake puolestaan sisältää 6 kenttää ja on aina 80 tavun kokoinen (Nakamoto (2008) & Bitcoin Dokumentaatio (2018)). Otsakkeen kentät ovat:

1. lohkon, eli ohjelman versionumero,
2. edellisen lohkon tiiviste,
3. Merkle-puun juurisolmun tiiviste,
4. aikaleima,
5. ”nBits”-luku, jota pienempi tiivisteen pitää olla, jotta lohko voidaan lisätä ketjuun eli luku kertoo vaikeusasteen ja
6. ”nonce”-luku eli sattumanvarainen luku, jota kasvatetaan tiivisteen muuttamiseksi.

Bitcoinin louhijat luovat Bitcoineja itse aina, kun he saavat lisättyä uuden lohkon lohkoketjuun. Bitcoinin louhinta-aika on 10 minuuttia lohkoa kohden. Lohkon liittämisen jälkeen he saavat louhintapalkkion ja käyttäjien maksamat siirtomaksut. Bitcoinin louhintapalkkio on tällä hetkellä 12,5 BTC ja palkkio puolittuu aina 210 000 lohkon jälkeen eli noin neljän vuoden välein. Aluksi louhintapalkkio oli 50 BTC ja se puolittuu, kunnes palkkio on pienempi kuin 0,00000001 BTC eli 1 satoshi (Bitcoin Dokumentaatio 2018). Tämän jälkeen uusia Bitcoineja ei voi enää luoda, joten nii-

den maksimimäärä on 21 miljoonaa. Nakamoto (2008) uskoo, että siirtomaksut tulevat olemaan tulevaisuudessa tarpeeksi Bitcoinin selviytymisen kannalta. Mutta Nica ym. (2017) spekuloivat, että louhintapalkkion hävitessä Bitcoin saattaa kuolla, koska louhijoilla ei ole tarpeeksi kannustinta jatkaakseen louhimista.

Nakamoto (2008) kehitti tavan muuttaa louhinnan vaikeusastetta, jotta louhinta-aika pysyisi lähes samana. Bitcoin-verkosto tarkkailee lohkojen aikaleimoja, jonka jälkeen otsakkeen ”nBits”-lukua muokataan. Luku kertoo vaikeusasteen eli kuinka monta edeltävää nollaa tiivisteessä pitää olla. Alqassem & Svetinovic (2014) kirjoittavat, että vaikeusastetta muutetaan aina 2016 lohkon jälkeen, mutta Bitcoinin lähdekoodin virheen takia aikaleimat tarkastetaan 2015 lohkosta eikä 2016:sta, kuten alkuperäisenä tarkoituksena oli (Bitcoin Dokumentaatio 2018).

## 3.2 Ethereum/Ether

Ethereum on lohkoketjualusta, jonka päällä Ethereumin oma kryptovaluutta, Ether, toimii. Sillä on kuitenkin isoja eroja verrattuna Bitcoiniin, kuten mahdollisuus luoda omia sovelluksia tai älysopimuksia ja tallentaa niitä lohkoketjuun. Tässä alaluvussa on käytetty kahta päälähdettä, Ethereum White Paper (2018) ja Ethereum Dokumentaatio (2018), ellei toisin mainita, ja alaluvussa keskitytään Ethereumin käyttöön kryptovaluutoissa, eikä Ethereumiin palveluntarjoajana. Mutta käyttäjien on mahdollista luoda omia älysopimuksia ja tallentaa niitä lohkoketjuun. Sopimukset suorittavat itsensä, kun ne saavat ulkopuoliselta tietovirralta herätteen, joka täyttää sopimuksen ehdot. Tällainen ehto voi olla esimerkiksi ilman lämpötila tiettynä päivänä tai tarpeeksi iso ETH/USD-kurssin muutos.

Jokainen siirto, sopimuksen luominen ja komento maksaa ”kaasua” (engl. ”gas”) eli Etheriä, Ethereumin omaa kryptovaluuttaa. Ethereumin skriptikieli on Turing-täydellinen, joten käyttäjät voivat luoda silmukoita, if-lauseita ja laskea periaatteessa kaikki mahdolliset laskutoimitukset. Turing-täydellisyys antaa paremmat ohjelmointimahdollisuudet ja samalla monipuolistaa Ethereumin käyttötarkoituksia, mutta sillä on myös haittapuolia. Yksi haitoista ovat ikuiset silmukat, koska ne voisi-

vat estää louhimisen ja näin kaataa Ethereum-verkoston. Siksi käyttäjien pitää maksaa siirtomaksuja kaasuna. Tällä varmistetaan, että laskentatehoa ei käytetä turhaan.

Käyttäjät asettavat itse kaasun hinnan ja ylärajan, ja louhijat valitsevat haluamansa siirrot lohkoonsa. Tämän takia käyttäjien pitää asettaa kaasun hinta tarpeeksi korkealle, jotta louhijat hyväksyisivät siirrot. Louhijat saavat palkkioksi käyttäjien maksamat kaasut, vaikka kaasun yläraja ylittyisi esimerkiksi sopimusta suorittaessa, jolloin sopimus raukeaa.

Louhinta perustuu Proof-Of-Work-validointimenetelmään. Algoritmina toimii Ethash-funktio, joka suunniteltiin estämään ASIC-piirien käytön louhinnassa tekemällä laskennasta mahdollisimman raskasta muistille. Ethash käyttää n. 1GB kokoista datatiedostoa, josta funktio valitsee sattumanvaraisesti osan tiivistettä varten. Tätä tiedostoa kutsutaan nimellä DAG ja se luodaan aina 30 000 lohkon jälkeen uudestaan lohkon numeron perusteella. Käyttäjät voivat siis luoda DAG-tiedoston etukäteen, mikä on myös suositeltavaa, koska DAG-tiedoston generoimisessa voi kestää useita tunteja, mikä puolestaan aiheuttaisi suuria taukoja louhimisessa. Ethash tarvitsee myös lohkon otsakkeen tietoja tiivisteen laskemiseksi.

Ethereumin lohkon otsake sisältää seuraavat tiedot;

1. Edellisen lohkon tiiviste,
2. lohkon setälohkojen tiiviste,
3. louhijan osoite, jolle palkkiot maksetaan,
4. ”tilapuun” juurisolmun tiiviste eli kaikista tileistä, saldoista ja muista tiloista kasatun puun juurisolmun tiiviste,
5. siirroista kasatun puun juurisolmun tiiviste,
6. ”kuiteista” eli siirtojen tiedoista kasatun puun juurisolmun tiiviste,
7. Bloom-filtterin tiedot,
8. luku, joka kertoo vaikeusasteen,
9. luku, joka kertoo edellisten lohkojen lukumäärän,
10. lohkon kaasun yläraja,
11. lohkon siirtoihin käytetyn kaasun määrä,

12. aikaleima,
13. lohkoon liittyvää lisätietoa,
14. tiiviste, joka saadaan laskemalla tiiviste ”nonce”-luvun ja muiden tietojen avulla,
15. ”nonce”-luku eli sattumanvarainen luku, jota kasvatetaan tiivisteen muuttamiseksi.

Otsakkeen lisäksi lohko sisältää siirrot ja listan ”setä”- lohkojen (engl. ”ommers” tai ”uncle”) otsakkeista (Ethereum Yellow Paper 2018). Nämä setälohkot ovat haarautuneen ketjun lohkoja ja myös niistä maksetaan louhintapalkkio.

Louhijat saavat lisättyä uuden lohkon lohkoketjuun keskimäärin 15 sekunnin välein ja he saavat siitä aina palkkioksi 5.0 ETH, käyttäjien maksamat siirtomaksut eli kaasut ja jos he saavat lisättyä setälohkon lohkoketjuun, he saavat siitä 1/32 osan ekstraa jokaista setää kohden. Setälohkon täytyy olla maksimissaan kuuden lohkon päässä ketjun lopusta, jotta lohko voidaan lisätä lohkoketjuun. Louhinta-aika on mahdollista pitää lyhyenä ilman suuria lohkoketjun haaroittumisia Greedy Heaviest-Observed Sub-Tree-protokollan (GHOST) avulla. GHOST-protokolla etsii pisimmän ketjun laskemalla jokaisen lohkoketjun haaran pituuden ja louhintaan käytetyn laskentatehon. Haaroissa on mukana myös setälohkot.

## 3.3 Eroavaisuudet

Bitcoinin siirtomaksut kasvoivat vuonna 2016 yli kolminkertaisiksi louhintapalkkion puolittuessa (Hileman & Rauchs 2017), joten tulevaisuudessa palkkion puolittuessa sama saattaa toistua. Korkeimmillaan siirtomaksut olivat kuitenkin vuoden 2017 lopussa, jolloin maksujen keskiarvo oli jopa yli 50 $ (bitinfocharts.com 2018). Ethereumin louhintapalkkiot taas pysyvät aina samana, eikä Etherin määrää ole rajattu. 15 sekunnin louhinta-aika nopeuttaa siirtoja ja näin vaikuttaa siirtomaksujen määrään ja Ethereum-verkon siirtomaksut ovatkin olleet murto-osia Bitcoinin siirtomaksuihin verrattuna.

Louhintaryhmien laskentateho Bitcoin-verkossa on suuri ja isoimpien ryhmien yh-

teistyö saattaisi keskittää yli 50% verkon laskentatehosta yhdelle ryhmälle. Ethereum yrittää ratkaista louhintaryhmien muodostumisen maksamalla louhintapalkkioita myös setälohkoista eli haarautuneista lohkoista, joita ei liitetä lohkoketjuun (Ethereum White Paper 2018). Louhijat voivat kuitenkin liittää näitä lohkoja myöhemmin lohkoketjuun lisäämällä tällaisen lohkon tiedot louhittavaan lohkoon. Palkkioksi he saavat 1/32 osan ylimääräistä.

Merkle-puuta on modifioitu Ethereumia varten ja tuloksena on Merkle-Patricia-puu (Ethereum Yellow Paper 2018). Data tiivistetään ja tallennetaan puun solmuihin, mutta puun rakenne on erilainen ja puun solmuja voi lisätä, poistaa tai muuttaa. Puussa on lehtisolmuja, haarasolmuja ja ”laajennus”-solmuja (engl. ”extension”). Lehtisolmut sisältävät datan, jota etsitään ja laajennussolmuja käytetään lyhentämään puun polkuja. Haarasolmut sisältävät listan, jonka 16 ensimmäistä alkiota ovat heksadesimaaleja ja ne osoittavat seuraavaan solmuun. Viimeinen alkio on dataa varten. Merkle-Patricia-puuta ei tarvitse rakentaa aina uudelleen, koska vain osa siitä muuttuu lohkojen välissä, joten puun päivittämisen jälkeen juurisolmun laskeminen on nopeaa. Lisäksi puun juurisolmu pysyy samana, vaikka solmut lisättäisiin puuhun missä järjestyksessä vain. Ja koska Ethereum tallentaa kaikki tilatiedot lohkoon, käyttäjät eivät tarvitse koko lohkoketjua. Ethereum White Paper (2018) mukaan Bitcoinin tarvitseva tila voisi pienentyä jopa 20 kertaisesti, jos Bitcoin käyttäisi samanlaista strategiaa.

# 4 Kryptovaluuttojen markkinat ja niiden kehitys

Kryptovaluuttojen markkina-arvo räjähti kasvuun vuonna 2017 ja kaikkien kryptovaluuttojen yhteenlaskettu markkina-arvo oli parhaimmillaan n. 825 miljardia dollaria (Katso kuvio 4). Vuoden 2017 lopussa Bitcoinin arvo saavutti huippunsa ja kävi n. 20 000 dollarissa. Mutta keväällä 2018 Bitcoinin arvo putosi yli puolella ja huhtikuun alussa Bitcoinin arvo oli n. 7 000 $. Kryptovaluuttojen markkinat ovat välillä todella epävakaita ja kryptovaluuttojen kurssit saattavat nousta ja laskea jopa satoja prosentteja lyhyessä ajassa. Etenkin uusien, vasta liikkeelle laskettujen kryptovaluuttojen kurssit saattavat alussa kasvaa mielivaltaisen nopeasti.


Kuvio 4. Kryptovaluuttojen markkina-arvo vuoden ajalta (CoinMarketCap.com)

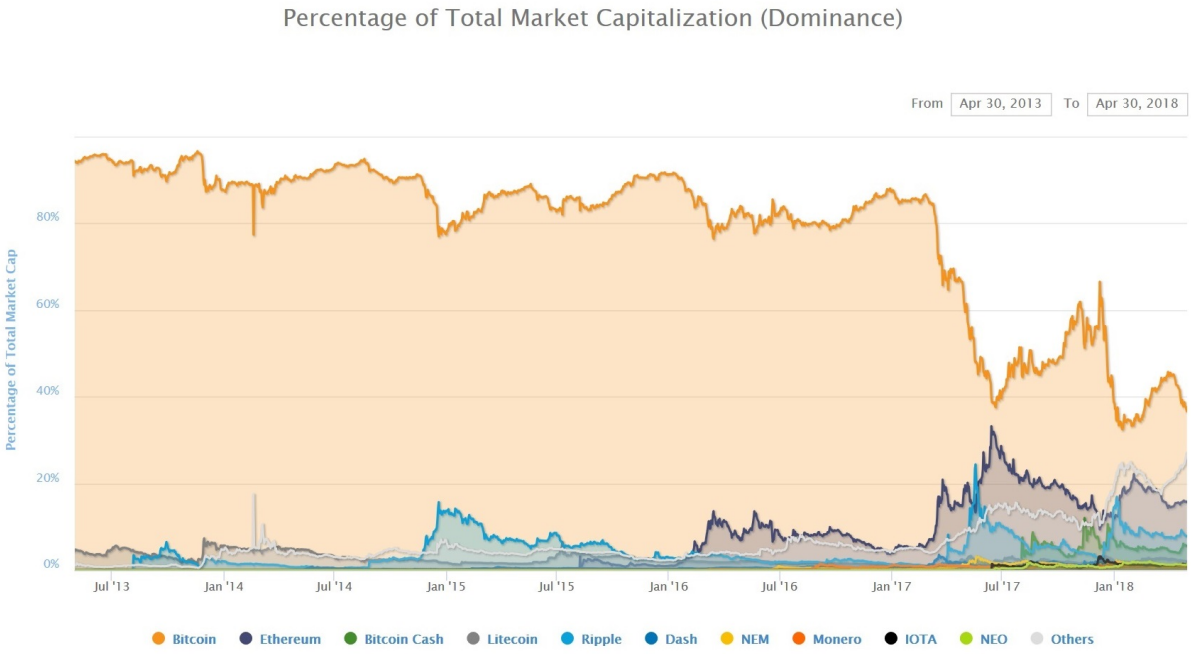
Poliittiset ja taloudelliset maailmantapahtumat, kuten suuret pankkikriisit, vaikuttavat usein kryptovaluuttojen markkinoihin positiivisesti. Corbet ym. (2017) huomasivat, että Brexitin aikana Bitcoinin arvo nousi. Tämä tapahtui myös Kyproksen pankkikriisin aikana (Nica ym. 2017). Koska kryptovaluutat eivät ole pankkien tai hallituksien ohjattavissa, ihmisten menettäessä luottamusta tavalliseen valuuttaan, he kääntyvät kryptovaluuttojen puoleen. Mutta esimerkiksi Kiinan ja Etelä-Korean yritykset säännöstellä kryptovaluuttojen louhintaa ja käyttöä näkyvät kryp-

tovaluuttojen kursseissa negatiivisesti (Bianchetti ym. 2018). Kiina ja Etelä-Korea ovat kaksi suurimmista maista, joissa kryptovaluutat ovat suosittuja ja louhinta suurta.

Vaikka kryptovaluuttamarkkinoilla liikkuu paljon rahaa, kryptovaluuttoja ei pidetä oikeina valuuttoina vaan niitä hankitaan sijoituksina (Gandal & Halaburda 2017). Tämä näkyy myös siinä, että USA:ssa viranomaiset eivät pidä Bitcoinia maksujärjestelmänä, koska Bitcoin ei ole tarpeeksi käytetty maksuväline (Walch 2015). Kryptovaluuttojen pitäminen sijoituksina tulee esille myös siinä, että muiden kryptovaluuttojen kurssit seuraavat Bitcoinin kurssia. Jos Bitcoinin kurssi lähtee laskuun, niin myös monien muiden, kuten Ethereumin, kurssi laskee samalla. Bitcoin toimii suurimpana kryptovaluuttana suunnannäyttäjänä.

Bitcoin oli suurin kryptovaluutta monta vuotta, mutta vuoden 2016 jälkeen muut valuutat alkoivat saamaan enemmän jalansijaa. Bitcoinin prosentuaalinen markkinaosuus keväällä 2018 oli silti vieläkin yli 40% (Katso kuvio 5). Gandal & Halaburda (2017) uskovat Bitcoinin pitävät paikkansa suurimpana kryptovaluuttana, ellei markkinoille ilmesty uutta, paljon parempaa kryptovaluuttaa ja silloinkin Bitcoin saattaa pitää asemansa, koska markkinat suosivat ensimmäistä tulokasta.

Bianchetti ym. (2018) löysivät kryptovaluutoista hintakuplille tyypillisiä piirteitä ja he pystyivät ennustamaan hintojen laskuja ja nousuja. Ihmiset ovatkin olleet skeptisiä kryptovaluuttoja kohtaan ja internetissä on käyty keskustelua, milloin ”kryptokupla” puhkeaa. Bianchetti ym. (2018) mukaan 1 000 ihmistä omistaa n. 40% Bitcoineista, mikä tarkoittaa sitä, että tekemällä yhteistyötä ja laskemalla tarpeeksi Bitcoineja markkinoille, he voisivat hallita Bitcoinin kurssia mielensä mukaan.




Kuvio 5. Kryptovaluuttojen prosentuaalinen markkina-arvo (CoinMarketCap.com)

# 5 Yhteenveto

Lohkoketjut kehiteltiin Bitcoinia varten vuonna 2008, mutta lohkoketjuilla on monia muitakin sovelluksia, kuten potilastietojen tallentaminen terveydenhuollossa tai tuotteiden alkuperän selvittäminen elintarviketeollisuudessa. Lohkoketjut sopivat kryptovaluuttojen hallintaan, koska lohkoketjut ovat muuttumattomia, julkisia ja hajautettuja vertaisverkkoon. Muuttumattomuus saavutetaan erilaisilla validointimenetelmillä, kuten Proof-of-Work tai Proof-of-Stake. Proof-of-Work-menetelmässä louhijoiden pitää käyttää resursseja, kuten tietokoneen laskentatehoa, liittääkseen lohko lohkoketjuun. Hyökkääjän pitäisi hallita yli 50% verkon laskentatehosta muuttaakseen lohkoketjua.

Vanhin kryptovaluutta, Bitcoin on edelleenkin suurin ja käytetyin, mutta Ether ja monet muut ovat saaneet jalansijaa viime vuosina kryptovaluuttojen kasvattaessa suosiota. Suosion kasvun huomaa myös kryptovaluuttojen markkina-arvon noususta. Vuonna 2017 markkina-arvo oli yli 825 miljardia dollaria. Mutta markkinat ovat epävakaita ja esimerkiksi maailmanlaajuiset poliittiset tapahtumat, kuten kryptovaluuttojen säännöstely, saattavat muuttaa kursseja paljon lyhyessä ajassa.

Tutkielmassa selvitettiin Bitcoinin ja Ethereumin eroja, ja sitä miten nämä erot vaikuttavat niiden käyttöön. Ethereumin toteutus parantaa lohkoketjun käyttömahdollisuuksia muuallakin kuin kryptovaluutoissa ja käyttäjät voivat itse tehdä älykkäitä sopimuksia tai rakentaa omia sovelluksiaan Ethereum-verkon päälle. Bitcoinin louhinta-aika on moninkertainen Ethereumiin verrattuna ja Bitcoinin louhintapalkkiot puolittuvat aina tasaisin väliajoin. Tulevaisuudessa tämä saattaa muodostua ongelmaksi, jos siirtopalkkiot kasvavat liian suuriksi. Etherin rajoittamaton määrä ja louhintanopeus suosivat yksittäisiä louhijoita, mutta kehittäjien mukaan Ethereumin pitäisi siirtyä tulevaisuudessa käyttämään Proof-of-Stake-menetelmää louhinnassa (Ethereum White Paper 2018).

Kryptovaluutat kehittyvät koko ajan ja tulevaisuus voi tuoda mukanaan suuria muutoksia niiden toteutukseen tai markkinatilanteeseen.

# Kirjallisuutta


Alqassem & Svetinovic , 2014. *Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural Analysis*. 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)

Bianchetti, Ricci & Scaringi, 2018. *Are Cryptocurrencies Real Financial Bubbles? Evidence from Quantitative Analyses*. http://dx.doi.org/10.2139/ssrn.3092427.

*Bitcoin dokumentaatio*. Saatavilla WWW-muodossa https://bitcoin.org/en/developer-documentation. Viitattu 6.2.2018

*Siirtomaksut*. Saatavilla WWW-muodossa https://bitinfocharts.com/comparison/transactionfees-btc-eth.html. Viitattu 16.4.2018

Corbet, Meegan, Larkin, Lucey & Yarovaya, 2017. *Exploring the Dynamic Relationships between Cryptocurrencies and Other Financial Assets*. http://dx.doi.org/10.2139/ssrn.3070288.

*Ethereum dokumentaatio*. Saatavilla WWW-muodossa http://www.ethdocs.org. Viitattu 5.3.2018

*Ethereum White Paper*. Saatavilla WWW-muodossa https://github.com/ethereum/wiki/wiki/White-Paper. Viitattu 15.4.2018

*Ethereum Yellow Paper*. Saatavilla WWW-muodossa https://ethereum.github.io/yellowpaper/paper.pdf. Viitattu 15.4.2018

Gandal & Halaburda, 2017. *Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market*. http://dx.doi.org/10.2139/ssrn.2506463.

Hileman & Rauchs, 2017. *Global Cryptocurrency Benchmarking Study*. Saatavilla WWW-muodossa https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf. Viitattu 12.3.2018

Kaushal, Bagga & Sobti, 2017. *Evolution of bitcoin and security risk in bitcoin wallets*.

2017 International Conference on Computer, Communications and Electronics (Comptelix)

King & Nadal , 2012. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. Saatavilla WWW-muodossa https://peercoin.net/assets/paper/peercoin-paper.pdf. Viitattu 12.3.2018

Linn & Koo, 2016. *Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research*. Saatavilla WWW-muodossa https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf. Viitattu 4.3.2018

Nakamoto, 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Saatavilla WWW-muodossa https://bitcoin.org/bitcoin.pdf. Viitattu 6.2.2018

Nica, Piotrowska & Schenk-Hoppé, 2017. *Cryptocurrencies: Concept and Current Market Structure*. http://dx.doi.org/10.2139/ssrn.3059599.

Patel, Bothra & Patel, 2017. *Blockchain exhumed*. 2017 ISEA Asia Security and Privacy (ISEASP)

Tama, Kweka, Park & Rhee, 2017. *A critical review of blockchain and its current applications*. 2017 International Conference on Electrical Engineering and Computer Science (ICECOS)

Walch, 2015. *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*. NYU Journal of Legislation and Public Policy, Issue 18, Volume 4