LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Kryptoekonomian perusteet

Juselius, Andre

**Laurea-ammattikorkeakoulu**

# Kryptoekonomian perusteet

Andre Juselius
Liiketalous
Opinnäytetyö
Marraskuu, 2019

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Koulutus
Tutkinto (AMK)

Andre Juselius

**Kryptoekonomian perusteet**

Vuosi 2019 Sivumäärä 32

Tässä opinnäytetyössä on pyritty muodostamaan kryptoekonomialle perustavanlaatuista suomenkielistä viitekehystä aiheen tarkempaa käsittelyä varten. Kryptoekonomian kompleksisuudesta ja monialaisuudesta johtuen tässä opinnäytetyössä aihetta lähestytään kryptografian, talousteorioiden ja lohkoketjujen näkökulmasta tutkien, miltä osin valittujen näkökulmien vallitsevat teoriat mukautuvat kryptoekonomian kanssa tai vastaavasti eroavat kryptoekonomian toimintaperiaatteista.

Tämän opinnäytetyön mukaan kryptoekonomiset järjestelmät toimivat kryptografian fundamenttien mukaisesti täyttäen ainakin osan kryptografian määritelmistä. Kryptoekonomiset järjestelmät hyödyntävät jo olemassa olevia kryptografisia malleja, kuten tiivistealgoritmeja avointa elliptisten käyrien kryptografiaa ja digitaalisia allekirjoituksia. Talousteorian näkökulmasta tarkasteltuna voidaan todeta, että kryptoekonomiset järjestelmät mukautuvat joihinkin taloustoerioiden malleihin, mutta kryptoekonomiset järjestelmät eivät täytä sellaisenaan yhdenkään tietyn talousteorian oppeja. Eri talousteorian koulukuntien malleja mukailemalla jonkinlainen ekonominen toiminnallisuus on saavutettavissa.

Lohkoketjuteknologia osittain yhdistää kryptografian ja talousteorian oppeja yhdeksi teknologiaksi, jonka avulla voidaan luoda kryptoekonomisia järjestelmiä muihinkin käyttötarkoituksiin, kuin virtuaalivaluuttoihin. Aiheen tuoreudesta johtuen lohkoketjuja on tarkasteltu Bitcoinin näkökulmasta ja Bitcoinia tarkastellaan virtuaalivaluutan sijaan teknologiana, jonka malleja voisi hyödyntää muissakin konteksteissa. Tarkoituksena on havainnollistaa, mitkä käytännön tekijät tekevät kryptoekonomisista järjestelmistä poikkeuksellisen, uuden ja hyödynnettävän teknologian eri käyttötarkoituksissa. Kryptoekonomian tulevaisuuden mahdollisista käyttötarkoituksista esitellään muutamia skenaarioita opinnäytetyön lopussa.

Asiasanat: Kryptoekonomia, Kryptografia, Talousteoria, Lohkoketju, Bitcoin

**Laurea University of Applied Sciences**
Degree Programme in Business management
Bachelor's Thesis

**Abstract**

Andre Juselius

**Basics of cryptoeconomics**

Year 2019 Pages 32

This thesis report combines information about the basic principles cryptoeconomics into one of the first Finnish writings on the subject. Because of the complexity and multidisciplinary of the subject this report reviews cryptoeconomics from three different perspectives, which are cryptography, different schools and principles of economics and blockchain, in order to explore which of the dominant theories complies or differs with cryptoeconomics.

The report shows that cryptoeceonomic systems fulfil some parts of the basic definition and fundamentals of cryptography. Cryptoeconomic systems utilize existing cryptographic models like hash-algorithms, elliptic-curve public-key cryptography and digital signatures. From an economic point of view, cryptoeconomic systems comply with some economic models of different schools of economics, but cryptoeconomic systems do not fulfil any specific schools of economics as such. By applying various economic models from different schools of economics, some kind of economic functionality can be achieved.

Blockchain technology combines some principles and fundamentals of cryptography with economic models in a single technology. This technology allows cryptoeconomic systems to be used more widely than only for crypto currencies. Because of the newness of the subject this report reviews blockchain from the perspective of Bitcoin and examines Bitcoin as technology rather than crypto currency. This viewpoint is chosen because Bitcoin cryptoeconomic technology can be utilized in other contexts as well than only for crypto currencies. The purpose of this report is to illustrate which factors make cryptoeconomic systems exceptional, new and usable technology for various contexts. The potential use cases for cryptoeconomic systems are demonstrated in the end of this report.

Keywords: Cryptoeconomy, Cryptoeconomics, Cryptography, Economics, Blockchain, Bitcoin

Sisällysluettelo


1 Johdanto ..... 7
1.1 Dokumenttianalyysi ..... 7
2 Kryptografia ..... 8
2.1 Historia ..... 8
2.2 Määritelmä ..... 8
2.3 Kryptografian tavoitteet ..... 9
2.4 Kryptografian luokittelu ..... 9
2.5 Julkinen kryptografia ..... 10
2.6 Elliptisten käyrien kryptografia ja digitaaliset allekirjoitukset ..... 11
2.7 Julkisten avainten käyttäminen identiteettinä ..... 12
2.8 Tiivistefunktiot ..... 13
2.9 SHA 256 -tiivistefunktio ..... 14
3 Taloustieteen perusteet ..... 14
3.1 Mikrotaloustiede ..... 15
3.2 Nash-tasapaino ..... 16
3.3 Makrotaloustiede ..... 16
3.3.1 Julkistalous & instituutiot ..... 16
3.3.2 Monetarismi ja inflaatio ..... 17
3.3.3 Raha- ja pankkijärjestelmä ..... 18
3.4 Itävaltalainen taloustiede ..... 19
3.4.1 Rahateoria ja hinnan muodostuminen markkinoilla ..... 20
4 Lohkoketjut ja kryptovaluutat ..... 21
4.1 Taustatietoa ..... 22
4.2 Bitcoin kryptojärjestelmänä ..... 22
4.3 Kuinka Bitcoin hyödyntää julkista kryptografiaa ..... 23
4.4 Lohkoketjujen & kryptovaluuttojen desentralisaatio ..... 23
4.5 Konsensusmekanismi ..... 24
5 Talousteoria ja Bitcoin ..... 25
5.1 Mikrotaloustiede Bitcoinin näkökulmasta ..... 25
5.2 Makrotaloustiede Bitcoinin näkökulmasta ..... 26
5.3 Monetarismi ja inflaatio Bitcoin-kryptojärjestelmässä ..... 26
5.4 Raha- ja pankkijärjestelmä Bitcoin-kryptojärjestelmässä ..... 27
5.5 Itävaltalainen taloustiede ja Bitcoin ..... 27
6 Kryptoekonomisten järjestelmien ja lohkoketjujen tulevaisuus ..... 28
6.1 Kryptoekonomiseen järjestelmään pohjautuva suora demokratia ja valtioiden budjetin allakointi sekä seuranta lohkoketjuteknologialla ..... 28

6.2 Keskuspankkien liikkeelle laskemat virtuaalivaluutat ja niihin verrattavat instrumentit ..... 29
6.3 Vaihtoehtoiset talousjärjestelmät ja universaali perustulo ..... 30
7 Yhteenveto ..... 30
Lähteet ..... 32

# 1 Johdanto

Kryptoekonomia (cryptoeconomics) on akateemisessa maailmassa erittäin tuore aihe 2010-luvun lopulta, joka yhdistää kryptografian, talousteorioiden ja lohkoketjuteknologian malleja yhdeksi kokonaisuudeksi. Tässä opinnäytetyössä tutkitaan, mitkä osat kryptografiasta ja talousteorioista ovat olennaisia kryptoekonomiassa mahdollistaen digitaalisen arvonsiirron. Opinnäytetyö on toteutettu dokumenttianalyysinä kirjallisuuskatsauksen muodossa perehtyen olemassa oleviin englanninkielisiin teoksiin, joista on pyritty löytämään kryptoekonomialle tärkeimmät tekijät muodostaen suomenkielisen määritelmän ja viitekehyksen aiheen laajempaa käsittelyä varten. Opinnäytetyön lähteiden etsimiseen on käytetty Google Scholar- ja Finna-tietojärjestelmiä. Aihealueen tuoreudesta johtuen on kuitenkin hyvä huomioida, ettei akateemisia lähteitä ole juurikaan kirjoitettu ja opinnäytetyö on julkaisuhetkellä yksi ensimmäisistä suomenkielisistä teoksista kyseisestä aiheesta. Tästä johtuen opinnäytetyön kirjoittaja on joutunut tyytymään lähdemateriaaleina myös akateemisista kirjoituksista poiketen blogi-kirjoituksiin ja muihin tieteellisesti epävirallisempiin lähteisiin. Monet lähdemateriaalit, kuten Davidson Sinclair, Flippi De Primavera ja Potts Jason (2016, 18) toteavat, että uusia tutkimusohjelmia on perustettava tämän aiheen ympärille, jotta saataisiin luotua teoreettinen viitekehys kryptoekonomiasta. Tämän opinnäytetyön tarkoituksena on luoda suomenkielinen viitekehys, jota voidaan täydentää ja muokata uusien akateemisten tutkimusten valossa. Opinnäytetyön ovat oikolukeneet Henry Brade ja Jeremias Kangas. Opinnäytetyön kirjoittaja haluaa erityisesti kiittää Henryä ja Jeremiasta hyvistä kommenteista ja korjausehdotuksista.

## 1.1 Dokumenttianalyysi

Aiheen uutuuden ja kompleksisuuden vuoksi tässä opinnäytetyössä on sovellettu tutkimusmenetelmänä dokumenttianalyysiä. Dokumenttianalyysi on käytännöllinen tutkimusmenetelmä uusien ilmiöiden tutkimiseen, kun aiheesta on saatavilla niukasti tietoa ja ilmiön keskeisistä kysymyksiä ei tunneta (Anttila 1998). Tässä opinnäytetyössä tulee huomioida, että osa opinnäytetyössä käytetyistä lähteistä on kerätty muuhun tarkoitukseen tai toiseen kontekstiin, mutta tätä on pyritty korjaamaan triangulaatiolla eli useamman lähteen rinnakkaisella ja samanaikaisilla käytöllä (Anttila 1998). Triangulaation avulla kryptoekonomiaa ja sen toimintamalleja on pyritty kuvailemaan mahdollisimman kattavasti eri aihealueista lähestyen ja eri aiheiden lähteitä käyttämällä. Tässä opinnäytetyössä on lähestytty kryptoekonomiaa kryptografian, talousteorioiden, lohkoketjujen ja kryptovaluuttojen näkökulmasta, jotta aiheen kompleksisuutta voitaisiin kuvata mahdollisimman käytännönläheisesti.

# 2 Kryptografia

## 2.1 Historia

Lähteistä riippuen kryptografisia menetelmiä on löydetty ainakin yli 2000 vuotta sitten antiikin Rooman aikakaudella, jolloin Ceaserin shift chipper esiteltiin tiedettävästi ensimmäisen kerran (Delf & Knebl 2002, 1). Menezes ym. (1996, 1) jäljitti krpytografian alkuperän yli 4000 vuoden taakse Egyptin historiaan. Vaikka kryptografian alkuperästä ei olekaan tarkkaa tietoa, se on ollut merkittävässä roolissa molemmissa maailmansodissa ja sen avulla on suojeltu valtion salaisuuksia (Menezes ym. 1996, 1). Kuitenkin vuonna 1976 W. Diffie ja M.E. Hellman julkaisi yhden tunnetuimmista alan teoksista *New directions in Cryptography*, jossa esiteltiin ensimmäisen kerran julkisen avaimen kryptografian (Public-key Cryptography) (Delf & Knebl 2002, 2; Menezes ym. 1996, 1 -2 ).

## 2.2 Määritelmä

Kryptografian tarkoituksena on tarjota luotettava viestin jakaminen kahden tai useamman osapuolen välillä kommunikaatio tavasta tai välineestä riippumatta. Viesti voi itsessään olla tekstiä, numeerista dataa tai mitä tahansa informaatiota, jonka muodolla ei ole väliä. Viestiä kutsutaan tässä kontekstissa selkotekstiksi (plaintext). Kryptografiassa tiedon salaus, luotettavuus, eheys ja aitous varmistetaan erilaisilla matemaattisilla salausmenetelmillä (encryption methods) (Delf & Knebl 20.02, 1 -3 ; Menezes, Oorschot & Vanstone 1996, 4). Tiedon salaamisen lisäksi kryptografisilla alleikrjoituksilla voidaan varmistaa viestin lähettäjän aitous. Kryptoanalyysin fundamentaalisen oletuksen nosti esille ensimmäisen kerran A. Kerkhoff 1800-luvulla. Oletuksen mukaan vihollinen tai salakuuntelija tietää kaikkien kryptojärjestelmien periaatteet mukaan lukien algoritmit ja niiden käytännön sovellukset, joten kryptojärjestelmän turvallisuus voi perustua pelkästään salausavaimiin (secret keys). Tätä pidetään Kerkhoffin periaatteena (Delf &knebi 2002, 4).

Yleisesti käytetyssä, yksinkertaistetussa ja käytännöllisessä kryptografian esimerkissä kommunikoivia henkilöitä kutsutaan nimillä Alice, Bob ja Eve. Joista Alice on viestin lähettäjä, Bob viestin vastaanottaja ja Eve on viestin salakuuntelija, jonka tarkoitus on kaapata tai muuttaa Alicen ja Bobin välistä kommunikaatiota. Vaikka esimerkkien nimet muistuttavat ihmisiä, ne voivat olla myös tietokoneita tai ohjelmistoja, jotka kommunikoivat keskenään. Yksinkertaisessa esimerkissä Alice salaa (encrypt) selkotekstin salausavaimella (encryption key) muodos-

taen salatun tekstin (ciphertext), jonka Alice lähettää Bobille haluamassaan kanavassa. Vastaanottaja Bob purkaa salatun tekstin salausavaimella takaisin selkotekstiksi. Salakuuntelija Eve voi silti kaapata Alicen lähettämän salatun tekstin, mutta hän ei saa salatusta tekstistä ymmärrettävää selkotekstiä ilman Alicen ja Bobin käyttämää salausavainta (Delf & Knebl 2002, 1; Ilmarinen 2016, 29-30; Menezes ym. 1996, 11).

## 2.3 Kryptografian tavoitteet

Kryptografialla pyritään suojaamaan kahden tai useamman tahon välistä kommunikaatiota, kuten edellä mainitulla esimerkillä havainnollistettiin. Kryptografialle voidaan kuitenkin asettaa neljä päätavoitetta, jotka ovat:

1. Luottamuksellisuus,
2. Eheys & integriteetti,
3. Aitous & autentikointi ja
4. Kiistämättömyys.

Käytännössä tämä luokittelu tarkoittaa, että 1. kenenkään ulkopuolisen ei pitäisi pystyä lukemaan alkuperäisten osapuolten luomaa selkotekstiä, 2. tiedon vastaanottajan pitää pystyä varmistamaan viestin alkuperäisyys ja muuttumattomuus, 3. viestin vastaanottajan tulee olla varma viestin lähettäjästä (Alicen ja Bobin pitää tunnistaa toisensa) ja 4. Kumpikaan taho: viestin lähettäjä ja vastaanottaja ei pysty jälkikäteen kiistämään viestin välityksen tapahtumista (Delf & Knebl 2002, 2 - 3; Ilmarinen 2016, 29 - 30). Menezes ym. (1996, 4) mukaan Kryptografian fundamentaalisiin tavoitteisiin kuluu yksinkertaisesti huijaamisen ja muiden haitallisten toimintojen havaitseminen ja estäminen. Esimerkiksi paperille käsin kirjoitettu allekirjoitus tarjoaa tietyn turvallisuuden manipulaatiota ja väärennöstä vastaan. Tästä toimintatavasta ei kuitenkaan ole minkäänlaista hyötyä digitaalisessa toimintaympäristössä.

## 2.4 Kryptografian luokittelu

Vaikka salausmenetelmillä on tuhansien vuosien historia, digitaalisten viestintävälineiden nopea yleistyminen on ajanut integriteetin ja autentikoinnin kehitystä. Tämän kehityksen ansiosta kryptografia voidaan luokitella kahteen eri kategoriaan:

1) Yksityiseen eli symmetriseen kryptografiaan (symmetric-key encryption) ja
2) Julkiseen eli epäsymmetriseen kryptografiaan (public-key cryptography),

joilla voidaan varmistaa lähetettävän viestin integriteetti (Delf & Knebl 2002, 3; Ilmarinen 2016, 30; Menezes ym. 1996, 15). Tämä opinnäytetyö käsittelee elliptisien käyrien epäsymmetristä eli julkista kryptografiaa, joka on olennainen tekijä lohkoketjuissa ja näin myös lohkoketjuihin pohjautuvassa kryptoekonomiassa.

## 2.5 Julkinen kryptografia

Julkisessa kryptografiassa jokaisella osapuolella on julkinen avain ja salattu avain, joita käytetään viestin vastaanottamiseen, salaukseen ja purkamiseen. Ilmarinen (2016, 33) määrittelee julkisen avaimen kryptografialle kolme toiminnallisuutta:

1) Avainten vaihtaminen
2) Digitaalinen allekirjoitus ja
3) Viestin salaus ja purkaminen.

Perinteisellä käsin kirjoitetulla allekirjoituksella on tarkoitus tarjota autentikaatio eli aitous ja kiistämättömyys. Digitaalinen allekirjoitus on mahdollista saavuttaa vain julkisen avaimen kryptografialla, koska digitaalinen allekirjoitus on täysin riippuvainen allekirjoittajan salausavaimesta, jonka voi luoda vain ja ainoastaan viestin alkuperäinen allekirjoittaja. Toisaalta kaikki viestin vastaanottajat voivat varmentaa lähettäjän digitaalisen allekirjoituksen paikkaansa pitävyyden *verifioinnilla*, joka on täysin riippuvainen lähettäjän julkisesta avaimesta (Delf & Knebl 2002, 3). Havainnollistetaan tätä kahdella esimerkillä. Jokaisella julkisen avaimen kryptojärjestelmän osallistujalla tulee olla henkilökohtainen avain $k = (pk, sk)$, jossa $pk$ on julkinen avain ja $sk$ on salainen avain. Jotta kryptojärjestelmän turvallisuudesta on varmuus, täytyy olla mahdotonta laskea salainen avain $sk$ julkisesta avaimesta $pk$ ja avain $k$ tulee valita satunnaisesti isosta joukosta parametrejä. Mikäli Bob haluaa osallistua kryptojärjestelmään, hänen täytyy satunnaisesti valita avain $k = (pk, sk)$, hänen tulee pitää salainen avain sk vain itsellään ja hänen tulee julkaista julkinen avain $pk$, jotta viestin lähettäjät voivat salata Bobille lähetettävät viestit (Delf & Knebl 2002, 24; Narayanan, Bonneau, Felten, Miller & Goldfeder 2016, 15 - 17). Toisessa esimerkissä Alice haluaa allekirjoittaa viestin $m$. Hänen täytyy käyttää allekirjoitus algoritmia *Sign* hänen salaisen avaimen $sk$ kanssa muodostaen allekirjoituksen $Sign(sk,m)$. Bob vastaanottaa allekirjoituksen $s$ viestistä $m$ ja voi täten varmentaa allekirjoituksen kokeilemalla, päteekö $Verify(pk,s,m) = ok$, käyttäen Alicen julkista avainta $pk$. Viesti on mahdollista allekirjoittaa sellaisenaan, mutta on yleisempää käyttää ensimmäiseksi tiiviste algoritmia (hash function) ja vasta sen jälkeen allekirjoittaa tiivistealgoritmin tuottama tiiviste. Tätä toimintatapaa kutsutaan hash-then-decrypt -menetelmäksi (Delf & Knebl 2002, 3 - 4; 24). Tiivistealgoritmeihin paneudutaan seuraavassa alaluvussa.

Menezes ym. (1996, 30) asettaa digitaalisen allekirjoituksen käytännöllisyydelle kolme ehtoa:

1) Allekirjoitus on helppo laskea (allekirjoitusfunktion tulisi olla helppokäyttöinen)
2) Allekirjoituksen tulee olla helposti kaikkien osapuolten verifioitavissa (verifiointifunktion tulisi olla helppokäyttöinen) ja
3) Allekirjoitusalgoritmin eliniän tulisi olla mahdollisimman pitkä (laskentatehon näkökulmasta allekirjoitusalgoritmin tulee olla turvallinen väärentämiseltä ja purkamiselta, kunnes allekirjoitus ei ole enää alkuperäistä tarkoitusta varten ajankohtainen).

Julkisen avaimen kryptojärjestelmien salaus perustuu vaikeisiin laskentatehtäviin, joiden ratkaisemiseen eli salauksen murtamiseen ei tulisi olla olemassa tehokasta tai nopeaa toimintatapaa tai siihen soveltuvaa algoritmia. Yhdensuuntaisia julkisia salausmenetelmiä pidetään William Stallingsin (2011, 300) mukaan rikkoutumattomina mikäli

*Y= f(X)* on helppo ratkaista, ja
*X=f^-1(Y)* on mahdotonta ratkaista

Julkisen avaimen kryptojärjestelmiä käsiteltäessä tulee kuitenkin huomioida, etteivät ne ole matemaattisesti todistettavia. Julkisen avainten järjestelmät ovat aina ehdollisia. Oletus liittyy yleensä tiettyyn funktioon *f*, jonka tulee olla yhdensuuntainen matemaattinen funktio. *F* voidaan laskea tehokkaasti, mutta x:n laskeminen funktiosta *F(x)* tulisi olla epätehokasta tai mahdotonta. Klassisesta turvallisuudesta on olemassa analogioita, kuten Shannonin laskennallinen salaisuus, joka kuuluu näin: ”salaus on vain ja ainoastaan täydellinen, mikäli viestin salakuuntelija tai kaappaaja ei voi erottaa kahta selkotekstiä, vaikka hänellä olisi käytössä loputtomasti laskentatehoa. Havainnollistetaan asiaa esimerkin avulla. Mikäli salakuuntelija Eve tietää, että salattu teksti *c* on salattu versio viestistä *m* tai *m’*, Evellä ei voi olla parempaa todennäköisyyttä kuin ½ oikean viestin valitsemiseksi (Delf & Knebl 2002, 6-8). Tässä opinnäytetyössä oletetaan, että julkisen avaimen kryptojärjestelmät ovat teknillisesti turvallisia eikä niiden matemaattinen todentaminen kuulu tämän opinnäytetyön sisältöön.

## 2.6 Elliptisten käyrien kryptografia ja digitaaliset allekirjoitukset

Digitaalisten allekirjoitusalgoritmien hyödyntäminen riippuu täysin käytettävästä algoritmista, satunnaislukujen satunnaisuudesta ja selkotekstin pituudesta eli viestin koosta. Luvussa 2.8 esitellään tiivistefunktion merkitys ja luvussa 2.9 käsitellään tarkemmin hash-256 -tiivistealgoritmin ominaisuuksia, joka on yksi tärkeimmistä elementeistä Bitcoinin kryptoekonomisessa järjestelmässä. Tässä luvussa käsitellään ECDSA-algoritmia eli elliptisen käyrän perusteita.

ECDSA on vuonna 1992 Yhdysvaltojen hallituksen National Institute of Standards and Technology (NIST) -instituution standardisoima ja lyhenne ECDSA tulee sanoista Elliptic Curve Digital Signature Algoritm. Siitä on tehty vuosien varrella useita kryptoanalyysejä ja sitä pidetään turvallisena. Bitcoin käyttää tarkalleen secp256k1 ECDSA-algoritmia digitaaliseen allekirjoitukseen ja algoritmi muodostaa 128 bittisen suojauksen (security). Kyseistä elliptisen käyrän algoritmia ei juurikaan käytetä missään muualla. Yleisempi ECDSA-algoritmi on secp256r1, jota käytetään esimerkiksi internet-selainten ja sähköpostien suojauksessa. (Narayanan ym. 2016, 17 – 18.) ECDSA täyttää kryptografian, kryptografisen tiivistefunktion ja julkisen salauksen esitellyt määritelmät (Johnson, Menezes, Vanstone 2001, 1 - 2). ECDSAn ominaisuudet ovat Narayanan (2016, 17 – 18) mukaan:

1) 256:n bitin yksityinen avain
2) Kompressoimaton 512:n bitin julkinen avain
3) Kompressoitu 257:n bitin julkinen avain
4) Selkotekstin ja tiivisteen koko on 256 bittiä ja
5) 512:n bitin allekirjoitus.

Tässä tulee huomioida, että ECDSA voi teknisesti allekirjoittaa vain 256:n bitin tiivisteen. Tämä ei kuitenkaan muodostu ongelmaksi, koska selkoteksti tiivistetään luvun 2.8 ja 2.9. mukaisesti ennen digitaalista allekirjoitusta, joten selkotekstin alkuperäisellä koolla ei ole merkitystä (Narayanan ym. 2016, 18).

## 2.7 Julkisten avainten käyttäminen identiteettinä

Edellä esitettyjä julkisia avaimia voidaan käyttää identiteettinä, kun viestin lähettäjä joutuu verifioimaan itsensä julkisella avaimella *pk* ja käyttämään allekirjoituksessaan salaista avaintaan *sk*. Näin julkinen avaimen takana voi olla henkilö, taho tai järjestelmä, jolle on luotu yksilöllinen julkinen avain *pk* sekä yksilöllinen salausavain *sk* ja tästä näkökulmasta julkinen avain toimii identiteettinä, joka on sidottu kyseiseen entiteettiin. Jokaisen julkisen avaimen *pk* haltijan tulee pystyä todistamaan identiteettinsä allekirjoitusalgoritmilla *Sign* tai salaamalla uuden viestin yksityisellä avaimellaan *sk* (Narayanan ym. 2016, 19). Näitä julkisia avaimia on mahdollista luoda käytännössä lukematon määrä. Teoreettinen maksimi osoitteiden määrälle on 2^160 Bitcoinin järjestelmän kohdalla, joka on RIPEMD-160 tiivistealgoritmin kapasiteetti. Tämän tarkempi käsittely ei kuulu opinnäytetyöhön.

## 2.8 Tiivistefunktiot

Tiivistefunktiot (hash function) kuuluvat modernin kryptografian peruspilareihin, koska tiivistefunktioiden avulla voidaan varmistaa kaksi kryptografian päätavoitteista: eheys & integriteetti ja aitous & autentikaatio. Tiivistefunktio nimensä mukaan tiivistää isomman joukon dataa pienemmäksi tiivisteeksi ja tiivisteen koon määrittää tiivistefunktion hash-koodi (hash code tai hash value) (Delf & Knebl 2002, 39 - 46; Menezes ym. 1996, 321).

Tiivistefunktioista käytetään myös lyhennettä MDC (modification detection codes) tai MAC (message authentication code) käyttötarkoituksesta riippuen, jolla on Menezes ym. (1996, 330) mukaan kolme tarkoitusta:

1) Tiedon konfirmointi
2) Avain derivaatio ja
3) Pseudosatunnainen numeroiden generointi.

Delf & Knebl (2002, 39) ja Stallings (2011, 351 - 357) määrittelevät myös muita konkreettisia käyttökohteita tiivistefunktioille, joista tärkeimpinä ovat:

1) Autentikaatio eli tunnistaminen
2) Digitaalinen allekirjoitus ja
3) Muut käyttökohteet, kuten kryptografiset tiivistefunktiot.

Tämä opinnäytetyö tutkii tiivistefunktioita kryptoekonomisesta näkökulmasta ja käsittelee kontekstia Narayananin, Bonneaun, Feltenin, Millerin ja Goldfederin (2016, 1 - 2) esittämän näkökulman mukaan, joka poikkeaa osittain edellä esitetyistä tiivistefunktioiden käyttökohteista. Narayanan (2016, 1 -2) jakaa tiivistefunktioiden toimivuuden kolmeen luokkaan:

1) Yhteentörmäämättömyys ja kompressoitavuus (collision resistance & compression function)
2) Piilotettavuus (hiding)
3) Puzzle-ystävällisyys (puzzle friendliness).

Luokat yksi ja kaksi ovat esitelty aikaisemmin kappaleessa 2.5 Stallingin sekä Delf & Kneblin oppien mukaisesti termillä rikkoutumattomuus, joka pätee Narayananin määritelmän kanssa. Narayanan näkökulma poikkeaa kuitenkin hieman aiemmin esitetystä viimeisen luokan kohdalla. Tiivistefunktio kompressoi alkuperäisen datan pienemmäksi tiivisteeksi (compression

function), jonka avulla esimerkiksi Merkel tree -data-arkkitehtuuri (data structure) on mahdollista. Data-arkkitehtuurin ja Merkel tree:n tarkempi analysointi ei kuulu opinnäytetyön sisältöön.

Yleisesti tiivistefunktiot toimivat hyvin digitaalisina salausmenetelminä, koska tiivisteiden purkaminen alkuperäiseen viestiin tarvitaan joko valtavasti laskentatehoa tai vastaavasti erittäin pitkä aikajänne, jotka tekevät tiivisteestä hyvin luotettavan. Kuitenkin tiivistealgoritmin toimivuus riippuu täysin käytettävästä tiivistealgoritmista.

### 2.9 SHA 256 -tiivistefunktio

SHA on vuonna 1993 standardoitu tiivistefunktio. SHA:n nimi tulee sanoista Secure Hash Algorithm, jonka on kehittänyt National Institute of Standards and Technology (NIST). Vuonna 2002 NIST päivitti standardia, jotta SHA voi muodostaa 256, 384 ja 512 bitin tiivisteet aikaisemman 160 bitin tiivisteen lisäksi (Delf & Knebl 2002, 43; Stallings 2011, 366 - 367). Vuonna 2005 NIST julkaisi suosituksen, jossa se kehotti siirtymään täysin SHA-1:stä SHA-2:n piiriin vuoteen 2010 mennessä. Vähän tiedotteen julkaisemisen jälkeen tutkijaryhmä julkaisi haavoittuvuuden ja mahdollisen yhteentörmäyksen SHA-1 algoritmissa (Stallings 2011, 367).

SHA-2 käyttää modulaarista aritmetiikkaa SHA-1 tiivistefunktion tapaan ja sille on kolme käyttötarkoitusta:

1) Yksisuuntainen salasana (one-way password file)
2) Tunkeutumisen havainnointi (Intrusion detection) ja
3) Kryptografiset tiivistefunktiot.

(Delf & Knebl 2002, 43; Stallings 2011, 366 - 367). Käytännössä SHA-256 -tiivistefunktio muodostaa minkä tahansa kokoisesta selkotekstistä (plaintext) 256-bitin tiivisteen (Narayanan ym. 2016, 2 - 10).

## 3 Taloustieteen perusteet

Nykyisen taloustieteen yhtenä tärkeimpänä oppi-isänä pidetään Alfred Marshallia ja hänen kirjoittamaansa teosta vuodelta 1890 Principle of Economics (Pohjola 2012, 9). Klassisen talousliberalismin suurimpana nimenä pidetään Skotlantilaista Adam Smithiä, joka vaikutti 1700-luvulla (Sipola 2015, 32). Toisin kuin muissa yhteiskuntatieteissä taloustieteelle on muodostunut

omat mikro- ja makrotaloudesta koostuva runko, joista ollaan pitkälti yksimielisiä. Taloustieteen erimielisyydet johtuvat Matti Pohjolan (2012, 11) mukaan näiden perusteorioiden soveltamisesta käytäntöön.

Talousteoria pyrkii Matti Pohjolan (2012, 11 - 13) mukaan vastaamaan kolmeen peruskysymykseen:

1) Miten talous toimii
2) Millaisin perustein talouden toiminnan tuloksia voidaan arvioida ja
3) Millaisin toimenpitein talouden toimintaa voidaan parantaa

Näihin kysymyksiin vastatessa arvoilla on iso merkitys tutkijan kysymysten asetteluun, näkökulman valintaan ja jopa tutkimuksen suoritus- ja esittämistapaan.

Tässä opinnäytetyössä paneudutaan edellä mainittuihin peruskysymysten tulkintoihin kahden koulukunnan näkökulmasta. Nämä kaksi koulukuntaa ovat perinteinen eli liberaalinen taloustiede sekä Itävaltalainen taloustiede. Molemmat koulukunnat tulkitsevat Pohjolan taloustieteen peruskysymyksiä eri fundamenteista. Tälle opinnäytetyölle keskeiset tulkinnalliset erot näiden kahden koulukunnan välillä ovat avointen markkinoiden toimivuus, raha- eli finanssipolitiikka sekä valtion, instituutioiden ja muiden keskitettyjen tahojen puuttuminen markkinoiden toimintaan.

Kryptoekonomiset järjestelmät hyödyntävät molempien edellä mainittujen koulukuntien oppeja, joten tässä luvussa nostetaan esille tärkeimmät tekijät. Kryptoekonomian talousjärjestelmään paneudutaan myöhemmin tässä opinnäytetyössä.

## 3.1 Mikrotaloustiede

Mikrotaloustiede muodostuu yksittäisten kotitalouksien ja yritysten päätöksiin ja toimiin markkinoilla. Tämä opinnäytetyö käsittelee mikrotaloustieteestä vain kysynnän ja tarjonnan tasapainon ja vaihtoehtoiskustannuksen (Boettke 1994, 151 - 152, 137 Pohjola 2012; 9, 49 - 62).

Tässä opinnäytetyössä rajataan sisältöä olettamalla, että markkinat toimivat tehokkaasti ja markkinat pyrkivät pitkän tähtäimen tasapainoon. Eli yhteiskunnan rajahyöty = kuluttajan rajahyöty = hinta = yrityksen kustannus = yhteiskunnan kustannus (Pohjola 2012, 62 - 63). Toinen oletus liittyy markkinaliberalistisen taloustieteen ja Itävaltalaisen taloustieteen tulkintaan mikrotaloustieteestä. Oletetaan, että molemmat edellä mainitut koulukunnat ovat

samaa mieltä mikrotalouden muodostumisesta ja paikkaansa pitävyydestä, koska molempien koulukuntien teoksista löytyy yhteneviä määritelmiä (Boettke 1994, 131 - 133; 138 - 139; 151 - 152; Pohjola 2012, 62 - 63). On hyvä tiedostaa, että Itävaltalainen taloustiede on kuitenkin ristiriidassa tämän opinnäytetyön oletuksen kanssa, koska Itävaltalaisen taloustieteen mukaan kaikilla markkinaosapuolilla ei ole markkinoiden kattavaa symmetristä informaatiota (Boettke 1994, 131 - 133) ja epäsymmetrisestä informaatiosta johtuen markkinoiden tasapainoa ei voi saavuttaa (Boettke 1994, 137 - 141). Epäsymmetrinen informaatio tiedostetaan myös perinteisen taloustieteen teoriassa, mutta sitä ei käsitellä tarkemmin (Pohjola 2012, 117 - 118). Syvällisempi analyysi tehokkaiden markkinoiden toimivuudesta ei kuulu tähän opinnäytetyöhön, eikä sen käsittelemistä pystytä analysoimaan alemman korkeakoulututkinnon tasolla.

## 3.2 Nash-tasapaino

Nash-tasapaino on yksinkertaisimmillaan tilanne, jossa kahden yrityksen hinnoittelupeli, josta kummankaan yrityksen ei kannata yksipuolisesti poiketa. Nash-tasapainon mukaan molempien yritysten pelatessa hinnoittelupeliä kummankaan yrityksen ei kannata vaihtaa strategiaa, koska siitä ei ole mitään hyötyä. John F. Nash palkittiin Nash-tasapainosta ja peliteorian tutkimuksista kahden muun tutkijan kanssa taloustieteen Nobel-palkinnolla vuonna 1994. Nash-tasapainon käsite ja peliteoria on muokannut yleisesti yhteiskuntatieteellistä ajattelua ja erityisesti taloustiedettä korostaen rationaalisen käyttäytymisen merkitystä. Näin päätöstenteon, odotusten rooli, tasapainon käsite ja päätöksiin sitoutumisen merkitys ymmärretään entistä selvemmin (Pohjola 2012, 87 - 88).

## 3.3 Makrotaloustiede

Tässä luvussa kootaan perinteisen taloustieteen ja Itävaltalaisen taloustieteen näkemykset makrotaloustieteestä niiltä osin, kun ne ovat olennaisia kryptoekonomisissa järjestelmissä eli kryptoekonomiassa. Ensimmäiseksi käsitellään perinteisen taloustieteen näkemykset, jonka jälkeen esitellään Itävaltalaisen taloustieteen näkemykset makrotaloustieteestä. Lukiessa tulee huomioida, että tässä opinnäytetyössä ei oteta kantaa, kumpi koulukunta kuvaa realistisemmin makrotaloutta.

### 3.3.1 Julkistalous & instituutiot

Perinteisen talousteorian mukaan julkinen valta voi parantaa markkinoiden toimintaa, mikäli markkinat toimivat tehottomasti ja tulonjako jakautuu epäoikeudenmukaisesti markkinoiden toimesta. Näin valtiot ja instituutiot voivat korjata epätäydellistä kilpailua verotuksen avulla, ulkoisvaikutuksiin puuttumalla, julkisella omistuksella ja julkisella tuotannolla (Pohjola 2012, 106 - 126). Valtion ei kannata puuttua kaikkeen ja tähän on Pohjolan (2012, 120 - 121) kaksi syytä:

1) Markkinoiden epäonnistuminen saattaa lopulta merkitä vain pientä poikkeamaa parhaasta mahdollisesta tilasta
2) Politiikka voi epäonnistua monella tavalla.

Perinteisen talousteorian mukaan julkisen vallan tulee jollain tasolla puuttua avointen markkinoiden tehottomuuteen. Tämän syvällisempi analyysi ei kuulu opinnäytetyön sisältöön.

### 3.3.2 Monetarismi ja inflaatio

Milton Friedmania pidetään monetaristisen taloustieteen tunnetuimpana kehittäjänä ja hänet on palkittu taloustieteen Nobel-palkinnolla vuonna 1976. Monetarismin keskeinen väite on, että makrotalouden tasapainon kannalta tärkein tekijä on liikkeellä olevan rahan määrä. Monetarismin oppien mukaan rahan tasapaino muodostuu tarjonnasta, josta vastaavat keskuspankit. keskuspankit voivat säädellä rahan tarjontaa koroilla sekä ostamalla ja myymällä joukkovelkakirjoja. Vaikka rahan tarjonnan maltillinen lisääminen ei poista kaikkia talouden ongelmia, rahapolitiikka mahdollistaa esimerkiksi taantumien säätelyn. Toinen nostettavan arvoinen Friedmanin päätelmä on pitkään jatkuneen korkean inflaation aiheuttama työttömyys, joka ei kuitenkaan liity opinnäytetyön sisältöön (Sipola 2015, 35 - 36).

Matti Pohjolan (Pohjola 2012, 191 - 192) taloustieteen yhdeksäs perusperiaate kuuluu näin ”rahan tarjonnan kasvu on inflaation perimmäinen syy”. Pohjola perustelee omaa 9. perusperiaatettaan Irving Fisherin kvanttiteorialla. Kvanttiteoria $M \times V = P \times Y$, missä M on rahan määrä, V on rahan kiertonopeus, P on yleinen hintataso ja Y on bruttokansantuote. Pohjolan (2012, 191) mukaan yhtälö on määritelmä, joka pätee aina ja se ei kerro näiden tekijöiden kausaliteetista. Kvanttiteoria muodostaa tekijöille kausaalisuhteen näiden tekijöiden välille kolmen oletuksen avulla:

1) Rahan kiertonopeus V on vakio
2) Bruttokansantuote Y on pitkällä aikavälillä luonnollisella tasollaan ja
3) Oletetaan, että keskuspankki voi säädellä rahavarantoa eli rahan määrää M.

Tämän teorian oletetaan kuvaavan hintatasoa P eli toisin sanoen inflaatiota, mikäli muut yhtälön tekijät ovat tiedossa. On kuitenkin hyvä tiedostaa, että tällä teorialla ei ole vaikutusta työllisyyteen, kokonaistuotantoon eikä suhteellisiin hintoihin (Pohjola 2012, 191 - 192).

Edellä mainittua näkemystä rahan neutraalisuudesta kutsutaan klassiseksi dikotomiaksi, joka Pohjolan (2012, 192) mukaan tarkoittaa reaali- ja rahatalouden kahtiajakoa. Tämä Fisher-efektiksi nimetty oppi tarkoittaa, että nimellinen korkokanta määräytyy reaalisen korkokannan ja inflaatiovauhdin summana. Fisher-efektin mukaan rahan tarjonta muodostaa inflaatiovauhdin ja reaalinen korko määräytyy rahoitusmarkkinoilla kysynnän ja tarjonnan tasapainon mukaan (Pohjola 2012, 192).

### 3.3.3 Raha- ja pankkijärjestelmä

Rahavaranto pitää sisällään ihmisten hallussa olevan rahan, joka muodostuu suppeasta rahasta eli seteleistä ja kolikoista, pankkitalletuksista, joissa ei ole nostorajoituksia ja joilla voidaan suorittaa rajoituksetta tilisiirtoja yksilöiden halujen mukaisesti rajoituksetta. Pankkitalletukset vastaavat käteistä rahaa käytännössä. Lavea raha pitää sisällään määräaikaistalletukset ja nostorajoitukselliset talletukset, jotka ovat vähemmän likvidejä rahoja (Pohjola 2012, 184).

Perinteinen talousjärjestelmä pohjautuu rahapoliittiseen pankkijärjestelmään, jossa keskuspankeilla on Pohjolan (2012, 185) mukaan kolme keskeistä tehtävää:

1) Setelipankki (seteleiden liikkeelle laskeminen)
2) Pankkien pankki (pankit käyttävät keskuspankkia omana pankkinaan talletuksille, lainoille tai muille rahoitusinsturmenteille)
3) Valtion pankki (keskuspankki toimii valtion pankkina ja rahoitustarpeiden turvaajana)

Pohjolan mukaan (2012, 185 - 186) pankkijärjestelmässä pankin luotonantoa rajoittaa kaksi tekijää. Pankin on pidettävä huolta omasta vakavaraisuudestaan ja huomioitava myöntämiensä lainojen riskit.

Rahapolitiikka pitää sisällään keskuspankkien omat toiminnat ja pankkien maksuvalmiuteen liittyvät toimet. Keskuspankki voi vaikuttaa rahapolitiikkaan kolmella tavalla:

1) Kassavarantomääräyksillä
2) Avomarkkinaoperaatioilla
3) Ohjauskoron välityksellä

Käytännössä kassavarantomääräyksiin kosketaan erittäin harvoin ja keskuspankki on viime vuosina keskittynyt avomarkkinaoperaatioihin ja ohjauskorkojen muutoksiin (Pohjola 2012, 188 - 189).

## 3.4 Itävaltalainen taloustiede

Itävaltalaista taloustiedettä voidaan pitää vaihtoehtoisena taloustieteen koulukuntana, joka ei ole saavuttanut merkittävää asemaa nykyisessä talousjärjestelmässä. Ensimmäisenä Itävaltalaisen taloustieteen generaationa pidetään Carl Mengerin kirjoittamaa kirjaa Principles of Economics vuodelta 1871. Itävaltalaisessa taloustieteessä on paljon yhtenevyyksiä neoklassisen taloustieteen kanssa, mutta Itävaltalaiselle taloustieteelle erottavia tekijöitä ovat matemaattisuus ja laskennallisuus, ekonomisten toimintojen dynaamisuus ja sosiaaliset ja poliittiset asiat vaihdannan ja tuotannon ulkopuolella. Itävaltalaisessa talousteoriassa on myös selkeitä yhtenevyyksiä perinteisen eli liberaalisen taloustieteen kanssa, mutta suurimmat erot koulukuntien välillä muodostuvat metodologisesta positioinnista ja analyyttisestä lähestymisestä rahateoriassa, pääomateoriasta ja hinnan muodostumisesta, jota käsiteltiin jo edellisessä alaluvussa. Kärjistetysti Itävalaltalainen taloustiede pohjautuu täysin avoimiin markkinoihin, joissa valtio ja instituutiot eivät puutu markkinoiden toimintaan millään tavalla ja edellä mainittujen tahojen toimet haittaavat markkinoiden toimivuutta. Itävaltalainen taloustiede ei hyväksy perinteisen taloustieteen teorioita julkishyödykkeistä, tulonjakoon puuttumisesta, markkinoiden muodostumisesta, monetarismista, raha- ja pankkiteoriasta, koska näiden toimivuudessa on loogisia puutoksia. (Boettke 1994, 1 - 3.)

Moderni versio Itävaltalaisesta taloustieteestä sai alkunsa Isreal Kirznerin, Murray Rothbardin ja Ludwig Lachmannin havainnoista 1970-luvulla. Vaikkakin Itävaltalainen taloustiede on heterogeeninen, heidän mukaan taloustieteellä on kaksi pääfundamenttia:

1) Taloustieteilijöiden selkeästä kyvystä kuvata taloudellisia ilmiöitä ihmisten käyttäytymisen näkökulmasta ja
2) Taloustietelijöiden on mallinnettava ihmisten tahattomien tekojen seurauksia sellaisenaan.

Itävaltalaisen taloustieteen mukaan nämä kaksi fundamenttia saavutetaan, kun prosessoidaan metodologista individualismia, metodologista subjektiivisuutta ja teoreettista tarkkaavaisuutta ennemmin kuin talouden tasapainotiloja. Itävaltalaista taloustiedettä tutkiessa on hyvä huomioida, etteivät edes sen tutkijat pidä välttämättä itseään Itävaltalaisen taloustieteen

edustajina. Mutta heidän töistään löytyy yhtenevyyksiä ja samankaltaisuuksia, jotka assosioivat Itävaltalaisen taloustieteen kanssa. Itävaltalaisen taloustieteen perusoletus on, että on olemassa vain teoria, joka muodostaa ajattoman ja universaalit käsitykset ihmisten toiminnasta. (Boettke 1994, 3 - 4).

### 3.4.1 Rahateoria ja hinnan muodostuminen markkinoilla

Itävaltalaisen taloustieteen mukaan kansainvälinen rahapolitiikka ja -teoria eli globaali markkinatalous ja valuuttakurssien kehitys on vain lopputuotteiden tuotantokustannukset, johon lisätään logistiset kustannukset lopullisen tuotteen tai palvelun kulutuksen määränpäähän, joka muodostaa tuotteelle hinnan tai valuuttakurssin. Itävaltalainen talousteoria ei usko tehokkaisiin markkinoihin, koska tehokkaat markkinat eivät anna realistista kuvaa markkinoiden toimivuudesta eikä tehokkaita markkinoita ole olemassa. Itävaltalaisen talousteorian mukaan markkinat muodostuvat jatkuvasta yksittäisten karhujen ja härkien yhdistelmästä, jotka muodostuvat yksilöiden kokemuksista ja markkinatilanteista konjuktiossa synnynnäisten ominaisuuksien ja yrittäjäkyvykkyyksien kanssa, joita yksilöt pyrkivät tulkitsemaan ja hyödyntämään oman kykynsä mukaan uuden markkinainformaation tullessa heidän tietoonsa. Jokainen markkinoilla oleva yksilö pyrkii hyödyntämään edellä mainittuja tekijöitä muodostaen oman näkemyksensä markkinamuutoksista ja markkinoiden tulevaisuuden kehityksestä. Itävaltalaisen talousteorian mukaan ei ole olemassa tehokkaita markkinoita, koska kahdella eri markkinapaikalla ei välttämättä ole edes tietoa toistensa olemassaolosta. Optimaalista kysynnän ja tarjonnan tasapainoa ei voi muodostua, koska markkinatoimijoilla ei ole syytä katua tai muuttaa tekemiään päätöksiä, koska he tekevät päätöksensä olemassa olevan tiedon ja kokemustensa pohjalta, eikä heillä ole insentiiviä muuttaa nykytilaa (status quo). Markkinatoimijat reagoivat uuden tiedon valossa, koska heillä on yksilölliset insentiivit hyödyntää uutta tietoa heille parhaalla mahdollisella tavalla, jonka kokonaisuudessaan voi tulkita markkinamuutokseksi, mikäli ilmiö on tarpeeksi laaja globaalin talouden näkökulmasta (Boettke 1994 23; 137 - 141; 249 - 256).

Itävaltalainen taloustieteen arvot lähtevät olettamasta, ettei markkinat tarvitse toimiakseen valtion instituutioita, kuten keskuspankkia rahapolitiikan ja makrotalouden toimimiseen. Itävaltalainen talousteoria antaisi markkinoiden määritellä täysin rahan liikkeet, korot ja kysynnän ja tarjonnan. Kokonaiskysyntä ja -tarjonta pohjautuvat täysin mikrotaloustieteen transaktioihin ilman keskuspankin tai muiden instituutioiden sääntelyä. (Boettke 1994, 249 - 256).

# 4 Lohkoketjut ja kryptovaluutat

Lohkoketju on ykinskertaisimmillaan ellipitisiin käyriin pohjautuva kryptografinen hajautettu avoimeen lähdekoodiin perustuva tilikirja ja luottamusjärjestelmä, jonka toimintaan kuka tahansa voi osallistua, joko täydentämällä kyseistä tilikirjaa (kryptovaluutan käyttö eli arvonsiirto) omilla transaktioilla, louhimalla transaktioita tilikirjaan (louhinta) tai ylläpitämällä koko tilikirjan historiaa (full noden ylläpito). Yksinkertainen määritelmä ei kuitenkaan huomioi muita lohkoketjun mahdollisia ominaisuuksia, esimerkiksi hajautetun tiedon tallentaminen on vain yksi lohkoketjun ominaisuuksista. Yksinkertainen määritelmä ei myöskään ota kantaa, mitkä talousteoriat ovat lohkoketjuille ominaisia, joten tässä opinnäytetyössä on käytetty Bitcoinia esimerkkinä, koska se on ensimmäinen ison suosion saavuttanut lohkoketju, jota kehitetään ja käytetään edelleen.

Laajemman määritelmän mukaan lohkoketju on hajautettu avoimeen lähdekoodiin pohjautuva tietojärjestelmä tai -infrastruktuuri (Distributed Ledger Technologies, DLT), jonka käyttämiseen (arvon luominen, arvon siirtämiseen) ja ylläpitämiseen (louhiminen) kuka tahansa voi vapaaehtoisesti osallistua. Pelkästä tilikirjasta tai kryptovaluutasta (crypto currency) poiketen hajautetuilla tietojärjestelmillä on muitakin käyttökohteita, joista lohkoketju on vain yksi käytännön sovellus DLT-teknologiasta. DLT-alustoille on olemassa neljä erilaista ominaisuutta:

1) Datan hajautus (data distribution)
2) Hallinnon desentralisointi (decentralisation of control)
3) Kryptografian käyttö (use of cryptography)
4) Ohjelmoitavuus ja automaatio (programmability/automation)

(Cryptoassets Taskforce: final report 2018, 8 - 9).

Laajemman määritelmän mukaan hajautettu tietojärjestelmä pitää sisällään, kuka omistaa mitäkin ja mitä kukin taho järjestelmän sisällä on tehnyt. Lähimpänä käytännön esimerkkinä voidaan pitää digitaalista lokikirjaa. Hajautettuun tietojärjestelmään voidaan esimerkiksi tallentaa arvopapereita (pörssiosakkeet tai muut finanssi-instrumentit), omistusoikeuksia (asunto-osakkeet & kiinteistöt yms.) tai muita digitaalisia hyödykkeitä & sopimuksia (Digital assets) (Cryptoassets Taskforce: final report 2018, 8 - 15). Edellä listattujen ominaisuuksien lisäksi DLT- ja lohkoketjujärjestelmien päälle voidaan rakentaa automatisoituja sovelluksia, kuten älysopimuksia (smart contracts).

Tallennettavan datan rajoittamattomuus on avoimen markkinan määritelmän mukainen. Lohkoketjut täyttävät avoimen markkinan ehdot luoden kysyntään ja tarjontaa pohjautuvan arvonmäärityksen, jossa koko ekosysteemi on peliteorian määritelmän mukaan monen Nash-tasapainon summa, koska verkkoa käyttävät ja ylläpitävät tahot saavat paremman palkkion kuin

verkkoa vastaan toimiessa tai verkosta pois pysyessä. Näin esimerkiksi Bitcoinin kryptojärjestelmässä eri käyttäjien ja ylläpitäjien insentiivit ovat linjassa keskenään tukien verkon toimintaa pitkällä aikavälillä.

## 4.1 Taustatietoa

Blockstreamin toimitusjohtajan mukaan Kryptografia on ala, jossa ei koskaan kannata olla ensimmäisten joukossa käyttämässä uusimpia ja mahtavimpia algoritmeja, koska kryptografisten algoritmien historia on hänen mukaansa n. 4-5 vuotta vanha ja yksi kriittinen haavoittuvuus voi kumota algoritmin käytettävyyden. Juurikin tästä syystä on järkevää suosia konservatiivisia ja vakiintuneita kryptografisia algoritmeja. Kyseiset algoritmit ovat ennustettavia ja Bitcoin on suunniteltu tästä näkökulmasta (Tapscott & Tapscott 2016, 28).

Digitaalista käteistä ja rahaa on pyritty kehittämään 1980-luvulta alkaen, joista nimeltä voidaan mainita SET, Digicash ja Hashcash. Kuitenkaan yksikään projekti ei saavuttanut suurta suosiota ja ne kaatuivat muutaman vuoden sisällä julkaisemisesta. Vaikkakin yleisesti väitetään Bitcoinin olevan ensimmäinen lohkoketjusovellus on kuitenkin hyvä tiedostaa, että lohkoihin kirjatut transaktiot toivat ensimmäisenä julki Haber ja Stornetta vuonna 1991 ja edellisistä riippumatta Adam Back vuonna 1997. Näiden tutkijoiden lisäksi on hyvä myös tiedostaa, että ensimmäinen käyttäjältä käyttäjälle eli P2P (peer-to-peer) digitaalinen rahaprojekti oli b-money, jonka Wei Dai kehitti vuonna 1998 (Narayanan ym. 2016, IX - XXVII). Voidaan todeta, ettei Satoshi Nakamoton luoma Bitcoin valkopaperi (white paper), lähdekoodi tai lohkoketju eli tilikirja ole luonut kyseisiä teknologioita täysin itsenäisesti vaan sitä voidaan pitää ensimmäisenä toimivana käytännön sovelluksena, jolla on ainakin satoja tuhansia käyttäjiä ympäri maailmaa.

## 4.2 Bitcoin kryptojärjestelmänä

Bitcoin sai alkunsa Satoshi Nakamoto -nimimerkin julkaisemasta valkopaperista (white paper) Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto 2008, 1). Näin kymmenen toimintavuoden jälkeen voidaan todeta, että Bitcoin on ratkaissut kahdenkertaisenkäytön ongelman (double spend problem) digitaalisessa toimintaympäristössä. Tällä tarkoitetaan tilannetta, jossa samaa digitaalista hyödykettä ei voi käyttää kahteen kertaan. Käytännössä Bitcoin toimii käteisen rahan tai fyysisen kullan kaltaisella tavalla, mutta digitaalisessa toimintaympäristössä.

Bitcoin on ensimmäinen avoimeen lähdekoodiin perustuva julkinen lohkoketju, joka yhdistää kryptografian ja talousteorian insentiivimallit toimivaksi kryptojärjestelmäksi. Bitcoin-protokollan eri toimijoiden kuten käyttäjien, louhijoiden ja kehittäjien insentiivit ovat linjassa verkon sääntöjen kanssa, joten heidän kannattaa toimia Bitcoinin protokollan asettamien sääntöjen mukaan, mikäli haluavat olla osana kyseistä järjestelmää. Insentiivimallien lisäksi Bitcoin on täysin käyttäjältä käyttäjälle (peer-to-peer) vertaisverkon tapaan toimiva järjestelmä, jossa ei tarvita kolmansia osapuolia verifioimaan transaktioita (Ammous 2018, 170 – 174; Narayanan ym. 2016, 28; Tapscott & Tapscott 2016, 27 - 51).

## 4.3 Kuinka Bitcoin hyödyntää julkista kryptografiaa

Bitcoinin toiminta pohjautuu täysin julkiseen kryptografiaan, jonka teoriaa on havainnollistettu luvussa 2. Bitcoin hyödyntää julkisia avaimia *pk* identiteetteinä, joihin voi vastaanottaa Bitcoineja ja vastaavasti Bitcoineja hallinnoidaan ja lähetetään salaisten avainten *sk* avulla (Narayanan ym. 2016, 76). Käytännössä Bitcoineja hallinnoidaan kuten muitakin julkisten kryptografian avaimia (key management). Kuten luvussa 2.6 tarkalleen havainnollistettiin, Bitcoinin julkisten ja salaisten osoitteiden pituudet ovat tiivistämättöminä 512 bittiä ja tiivistettyinä 256 tai 257 bittiä.

SHA256-tiivistefunktio on merkittävässä roolissa Bitcoin-kryptojärjestelmässä. SHA256 mahdollistaa Merkle-Damgård-transformaation, joka tuo monia ominaisuuksia Bitcoinin lohkoketjun data-arkkitehtuuriin ja informaatioverkoston ylläpitämiseen. Merkel-puu, Data-arkkitehtuuri tai lohkoketjun infrastruktuurin tarkempi analyysi ei kuulu tähän opinnäytetyöhön. Käytännössä SHA256 toimii tiivistefunktiona, jota esiteltiin luvuissa 2.8 ja 2.9.

## 4.4 Lohkoketjujen & kryptovaluuttojen desentralisaatio

Tämä kappale käsittelee lohkoketjujen yhtä tärkeintä ominaisuutta desentralisaatiota eli hajautuneisuutta. On syytä huomioida, ettei lohkoketjujen desentralisaatiota käsitellä pelkästään teknillisestä näkökulmasta vaan siihen liittyy myös insentiivimalleja, jotka muistuttavat talousteoriaa. Narayanan (2016, 28) käsittelee Bitcoinin lohkoketjun desentralisaatiota viiden kysymyksen kautta

1) Kuka ylläpitää tilikirjaa ja siihen kirjattavia transaktioita?
2) Kenellä on auktoriteetti transaktioiden hyväksymisestä?
3) Kuka tai mikä taho luo uusia Bitcoineja?

4) Kuka määrittää, miten järjestelmän sääntöjä muutetaan?
5) Kuinka Bitcoinin markkinahinta määritellään?

Ensimmäiset kolme kysymystä ovat pitkälti Bitcoin-protokollan liittyviä teknologisia kysymyksiä. Bitcoinin verkosto on pieniä poikkeuksia lukuun ottamatta täysin desentralisoitu käyttäjältä käyttäjälle (peer-to-peer network), koska kuka tahansa voi ylläpitää Bitcoin-nodea, jonka avulla osallistutaan verkon tilikirjan tallentamiseen ja ylläpitoon. Tämän noden pystyttämiseen on pieni kynnys. Noden pystyttäminen vaatii vain verkosta ladattavan Bitcoin ohjelman ja sen voi asentaa esimerkiksi kannettavalle tietokoneelle. Tällä hetkellä näitä nodeja on tuhansia. Bitcoin Core ohjelmisto toimii MIT-lisenssin alla, joka on erittäin vapaamielinen avoimen lähdekoodin lisenssi (open source license) (Narayanan ym. 2016, 196). Bitcoinin verkkoon eli tilikirjaan uudet transaktiot lisätään louhimalla ja teknisesti sitä voi tehdä kuka vaan. Louhinta tapahtuu käytännössä niin, että louhiva taho luovuttaa tietokoneiden laskentatehoa yksinkertaiseen, mutta erittäin työlääseen laskentatehtävään. Tämän lottoa tai arvontaa muistuttavan matemaattisen laskentatehtävän ratkaisemisesta palkitaan uusilla Bitcoineilla ja transaktiokustannuksilla, joita käyttäjät maksavat siirtäessään bitcoineja verkon sisällä osoitteesta toiseen. Louhintatehon lisääminen parantaa louhivan tahon todennäköisyyttä löytää oikea ratkaisu matemaattiseen laskutehtävään.

Bitcoin-protokollan säännöksiä muutetaan kahdella tasolla, joko soft forkin tai hard forkin kautta. Soft fork on kevyempi päivitys, joka säilyttää yhteensopivuuden vanhojen Bitcoin-protokollaversioiden kanssa. Hard fork on puolestaan isompi päivitys, jossa yhteensopivuus vanhoihin Bitcoin-protokollaversiohin ei säily ja hard fork pakottaa kaikkia uuteen versioon osallistuvia päivittämään ohjelmistonsa. Soft forkin ja hard forkin tarkempi analyysi ei kuulu opinnäytetyön sisältöön, mutta on hyvä tiedostaa, että kaikki Bitcoin-protokollan päivitykset tehdään Bitcoin Improvement Proposal (BIP) metodin mukaisesti. Käytännössä muutokset tehdään Bitcoin-yhteisön konsensuksen mukaan ja sen syntyminen voi olla hidas ja pitkäkestoinen prosessi, josta kaikki yhteisön jäsenet eivät ole yhtä mieltä. (Narayanan ym. 2016, 128; 170 - 175). Opinnäytetyö käsittelee Bitcoinin hinnanmuodostumista myöhemmässä luvussa.

## 4.5 Konsensusmekanismi

Konsensusmekanismi on yksi tärkeimmistä lohkoketjujen ominaisuuksista.
Narayanan (2016, 33) kiteyttää Bitcoinin konsensus-algoritmin viideksi yksinkertaistetuksi kohdaksi:

1) Kaikki transaktiot lähetetään kaikille nodeille.
2) Jokainen node kirjaa transaktiot lohkoihin.

3) Jokaisella kierroksella satunnainen node pääsee lähettämään oman lohkonsa verkkoon
4) Muut verkon nodet hyväksyvät uuden lohkon vain, jos kyseisen lohkon sisältämät transaktiot ovat valideja verkon kryptografisten sääntöjen mukaisesti (kts. kryptografia).
5) Nodet ilmoittavat uuden blokin hyväksymisestä lisäämällä uuden blokin tiivisteen seuraavaan lohkoon, joka verkkoon pääsee.

Bitcoin on ensimmäinen sovellus, joka on ratkaissut hajautetun konsensuksen ylläpitämisen (distributed consensus) (Narayanan ym. 2016, 28).

Narayananin näkemys Bitcoinin konsensusalgoritmista on yksinkertaistettu määritelmä algoritmin toiminnasta. Hänen määritelmä ei ota huomioon erilaisten node-tyyppien ominaisuuksia. Erilaisten nodien ominaisuudet eivät kuulu tähän opinnäytetyöhön.

# 5 Talousteoria ja Bitcoin

Bitcoin eroaa perinteisestä talousteoriasta merkittävästi ja sen voidaan katsoa soveltavan sekä neo-klassisen, liberaalin ja Itävaltalaisen taloustieteen oppeja. Pohjimmiltaan Bitcoinilla ja siihen pohjautuvilla muilla kryptoekonomisilla järjestelmillä on muutamia perusperiaatteita, jotka voidaan jaotella seuraavasti:

1) Bitcoinien tarjonta on rahan tarjonnan näkökulmasta niukka ja muuttumaton ei inflatorinen valuutta
2) Maksimi määrä on asetettu 21 miljoonaan Bitcoiniin
3) Bitcoinien liikkeelle lasku on ennalta selkeästi määritelty matemaattisesti
4) Mikään keskushallinto tai taho ei voi vaikuttaa käyttäjien tekemiin transaktioihin
5) Bitcoin käyttää julkisen kryptografian avaimia identiteetteinä.

Jaottelussa tulee huomioida, että tässä kontekstissa valuutta ei ole perinteistä eli virallista valuuttaa, koska se ei ole yhdenkään keskuspankin liikkeelle laskemaa rahaa. Myös muut jaottelun kohdat ovat kirjoittajan soveltamia talousteorian oppeja tässä kontekstissa. Tärkeätä on myös tiedostaa, että muut mahdolliset kryptojärjestelmät eivät täytä kaikkia edellä mainittuja perusperiaatteita.

## 5.1 Mikrotaloustiede Bitcoinin näkökulmasta

Mikrotaloustiede pyrkii mallintamaan yksittäisten toimijoiden tekemiä päätöksiä ja luomaan niistä yleispäteviä malleja. Bitcoinin talousjärjestelmässä mikrotalous toimii hyvin yksinkertaisten perusperiaatteiden mukaisesti. Kuka tahansa voi luoda itselleen Bitcoin-osoitteita sisältäviä lompakoita, joihin Bitcoin varallisuutta voi siirtää ilman keskushallinnon luomia rajoituksia. Näin voidaan katsoa, että Bitcoinin mikrotalous on aina Nash-tasapainossa, koska sen markkina toimii puhtaasti kysynnän ja tarjonnan mukaan ja käyttäjät päättävät itse omista siirroistaan. Bitcoin-markkina toimii tehokkaasti, koska siinä ei ole olemassa keskustahojen tai muiden instituutioiden luomia rajoituksia, joita voi olla esimerkiksi käteisnostorajoitukset tai rahan siirtoihin liittyvät säännökset. Vaikka Bitcoinin mikrotalous on aina tasapainossa se ei tarkoita, etteikö sen keskuspankkipohjainen hinta voisi muuttua merkittävästi kysynnän ja tarjonnan lyhytaikaisten muutosten seurauksena. Bitcoinin hinnanvaihteluita käsitellään myöhemmin tässä luvussa.

On kuitenkin hyvä tiedostaa, että Bitcoinin markkinatasapaino ei sisällä järjestelmän ylläpidosta aiheutuvia yhteiskunnallisia ulkoisvaikutuksia, joista energian kulutus on merkittävässä roolissa. Koska Bitcoinin louhintamekanismi ei kuulu tähän opinnäytetyöhön, tämä opinnäytetyö ei myöskään käsittele sen aiheuttamia ulkoisvaikutuksia.

## 5.2 Makrotaloustiede Bitcoinin näkökulmasta

Perinteisen makrotalouden oppien mukaisesti Julkistalous ja instituutiot pyrkivät omilla toimillaan korjaamaan markkinoiden tehottomuutta ja epäoikeudenmukaisuutta. Bitcoinin kryptojärjestelmässä ei ole olemassa julkistaloutta eli keskushallintoa tai muitakaan instituutioita, jotka voisivat puuttua itse bitcoin-kryptojärjestelmän toimintaan. Täten Bitcoinin kryptojärjestelmässä ei voi hyödyntää perinteisen talousteorian oppeja julkistaloudesta ja instituutioista. Julkishallinto ja julkiset instituutiot voivat välillisesti vaikuttaa bitcoin-kryptojärjestlemän toimintaan puuttumalla yksilöiden ja yritysten tekemiin päätöksiin lainsäädännöllä ja sen tulkinnalla.

## 5.3 Monetarismi ja inflaatio Bitcoin-kryptojärjestelmässä

Monetarismin ja inflaation soveltamisen kohdalla on myös merkittäviä eroja perinteisiin talousjärjestelmiin makrotalouden kontekstissa. Luvussa 3.2.2 esitetty kvanttiteoria ei päde Bitcoinin hinnan muodostumiseen tai määrittämiseen, koska kvanttiteorian oletus perustuu siihen, että jokaista valuuttaa hallinnoi keskuspankki. Keskuspankki voi halutessaan kontrol-

loida rahavarantoa eli rahan määrää, rahan liikkeitä ja inflaatiota kvanttiteorian oppien mukaisesti. Yksinkertaisesti Bitcoin ei ole inflaatiopohjainen valuutta, Koska Bitcoinissa ei ole keskustahoa, eikä sen tarjontaa voida mielivaltaisesti lisätä. Bitcoinin hinta muodostuu puhtaasti kysynnän ja tarjonnan tasapainon mukaisesti. Tähän tasapainoon palataan myöhemmin tässä luvussa.

## 5.4 Raha- ja pankkijärjestelmä Bitcoin-kryptojärjestelmässä

Bitcoinin talousjärjestelmässä ei ole olemassa keskuspankkia tai setelipankkia luotottamassa rahajärjestelmää. Voidaan yksinkertaisesti todeta, ettei teoriaa voida käyttää tässä kontekstissa. Bitcoinin liikkeelle lasku ei noudata rahapolitiikan perusperiaatteita. Bitcoineja luodaan verkon ylläpidosta maksettavista palkkioista, joita louhijat saavat sattumanvaraisesti käyttämälleen laskentateholle ja tämän toiminnan tuloksena Bitcoinin rahavaranto kasvaa. Kasvu on kuitenkin perinteisestä raha- ja pankkijärjestelmästä poiketen ei inflatorista (disinflationary), koska uusien Bitcoinien määrä puolittuu 210 000 lohkon eli noin neljän vuoden välein, kunnes 21 miljoonan Bitcoinin määrä tulee täyteen (Ammous 2018, 172 - 178).

## 5.5 Itävaltalainen taloustiede ja Bitcoin

Bitcoinin kryptojärjestelmällä ja Itävaltalaisella taloustieteellä on selkeitä yhtenevyyksiä. Kuten aikaisemmin todettiin, Itävaltalaisen taloustieteen arvot perustuvat olettamaan, ettei markkinat tarvitse toimiakseen valtion instituutioita tai keskuspankkia rahapolitiikan ylläpitämiseen. itävaltalaisen taloustieteen oppien mukaisesti tehokkaita markkinoita ei ole olemassa, koska markkinat muodostuvat täysin yksittäisten taloudellisten toimijoiden tekemien päätösten summasta.

Bitcoinin toiminta ja sen hinta perustuu edellisiin olettamiin, jossa markkinat muodostavat itsenäisesti kysynnän ja tarjonnan tasapainon. Tästä syystä Bitcoinin hinnanmuutokset keskuspankkirahan näkökulmasta katsottuna saattavat vaikutta erittäin rajuilta, koska vain kysyntä ja tarjonta vaikuttavat hinnan muodostumiseen. Bitcoinin hinnan oletetaan muodostuvan tarjonnan näkökulmasta lopputuotteen tuotantokustannuksista, johon lisätään logistiset kustannukset kulutusmääränpäähän. Eli Bitcoinin hinta muodostuu tarjonnan puolelta siihen käytettävän laskentatehon tarvitseman sähköntuotannon kustannuksiin eli toisin käytettävään louhintateknologiaan tehokkuuteen ja sähkön hintaan. Bitcoinin hinnan voidaan nähdä määräyty-

vän kysynnän muutoksen mukaan, koska Bitcoinien rahavaranto on ennalta määritelty ja lopputuotteen tuotantokustannukset on teoriassa mahdollista määrittää ja ennakoida hyvinkin tarkasti.

# 6 Kryptoekonomisten järjestelmien ja lohkoketjujen tulevaisuus

Tämä luku käsittelee kryptoekonomisten järjestelmien tulevaisuuden käyttömahdollisuuksia. Luvun sisältö pohjautuu pääosin opinnäytetyön kirjoittajan henkilökohtaisen osaamiseen ja hiljaiseen tietoon, koska lohkoketjuteknologian käytännön kokeiluista löytyy niukasti tietoa ja näin ollen avoin perusteltu ja lähteisiin pohjautuva tarkastelu on lähtökohtaisesti haasteellista. Mattila, Seppälä, Hukkinen, Laikar, markkanen, Kolu, & Jia (2019, 16) ovat myös todenneet tiedon niukkuuden haasteeksi lohkoketju- ja DLT-teknologian käytännön sovelluksia arvioitaessa. Käytettävän tiedon niukkuudesta ja aiheen tuoreudesta johtuen kryptoekonomisten järjestelmien tulevaisuutta käsitellään täysin hypoteettisesti pitkän aikavälin eli 5-20 vuoden aikajänteellä ja on myös hyvin mahdollista, ettei yksikään tämän luvun skenaarioista tule käytännössä toteutumaan.

Kryptoekonomiset järjestelmät eroavat perinteisistä toimintatavoista merkittävästi, kuten tässä opinnäytetyössä on osoitettu. Vaikka ero perinteisiin toimintamalleihin on valtava, voidaan tälle teknologialle nähdä erilaisia käyttömahdollisuuksia. Tulevaisuudessa voi olla keskuspankkien omia digitaalisia valuuttoja (Central Bank Digital Currency, CBDC), globaalissa mittakaavassa lohkoketjuteknologialla voidaan vähentää kansainvälistä rahanpesua, veronkiertoa tai muita rikollisia aktiviteetteja. Vaikka kryptoekonomiset järjestelmät ovat totuttu näkemään keskushallinnoista ja instituutioista irrallisina sovelluksina, se ei tarkoita, etteivätkö perinteiset toimijat voisi hyödyntää kyseistä teknologia nykyisten toimintojen tukena. Alaotsikoissa tarkastellaan mahdollisia skenaarioita aihe kerrallaan.

## 6.1 Kryptoekonomiseen järjestelmään pohjautuva suora demokratia ja valtioiden budjetin allakointi sekä seuranta lohkoketjuteknologialla

Eduskuntavaalien ja hallituksen muodostamisen yhteydessä käydään usein keskustelua valtion budjetin suuruudesta ja budjetin allakoinnista tulevan hallituskauden aikana. Mitä tapahtuisi, jos koko valtion budjetti ja varojen allakointi pohjautuisi kryptoekonomiseen järjestelmään eli lohkoketjupohjaisiin ratkaisuihin? Teoriassa koko edustuksellisen demokratian voisi korvata suoralla demokratialla, jossa jokaisella Suomen kansalaisella olisi järjestelmään sopiva yksityinen avain, jonka avulla hän voisi äänestää suoran demokratian mukaan, mitä poliittisia

toimenpiteitä henkilö haluaisi tukea äänestämällä. Tässä skenaariossa kaikki kansalaiset voisivat seurata reaaliajassa, mitä valtion rahoilla tehdään ja kuinka hyvin kyseiset varat allakoituvat niihin käyttökohteisiin, joista on sovittu äänestämällä. Teoriassa älysopimuksilla voitaisiin jopa varmistaa, ettei kukaan taho pystyisi väärinkäyttämään kyseisiä varoja. Mikäli väärinkäytös kuitenkin onnistuisi, jäisi siitä yksilöitävä jälki avoimeen tilikirjaan, joka tekisi kiinnijäämisestä ja rikoksen todistamisesta läpinäkyvää ja selkeää. Tämä läpinäkyvyys voisi jopa ennaltaehkäistä rikosten tai muiden väärinkäytösten syntymistä, koska kiinnijäämisen riski olisi ilmeinen. Käytännössä tämä tarkoittaisi sitä, että esimerkiksi Kelan varojen käyttöä voitaisiin seurata reaaliajassa ja poliittisten päätösten toimivuutta voitaisiin arvioida objektiivisesti. Globaalissa mittakaavassa valtiollisten kryptoekonomisten järjestelmien avulla voitaisiin välttyä kansainväliseltä rahanpesulta, veronkierrolta ja muilta epäeettisiltä ratkaisuilta, mikäli maailman valtiot haluaisivat aidosti sitoutua kyseisten aktiviteettien kitkemiseen.

## 6.2 Keskuspankkien liikkeelle laskemat virtuaalivaluutat ja niihin verrattavat instrumentit

Keskuspankkien liikkeelle laskemat virtuaalivaluutat (Central Bank Digital Currency, CBDC) voivat olla myös potentiaalinen kryptoekonomian käyttömahdollisuus. Tämä voidaan toteuttaa muutamalla eri tavalla. Keskuspankit voivat laskevat liikkeelle euron ja dollarin tueksi erillisiä digitaalisia valuuttoja, jotka mahdollistavat esimerkiksi käteisestä rahasta siirtymisen täysin digitaalisiin valuuttoihin.

kryptoekonomisia järjestelmiä voi myös hyödyntää muissa keskuspankkien, pankkien ja muiden instituutioiden settlementeissä (settlement accounts). Käytännössä edellä mainittujen tahojen käyttämät instrumentit voitaisiin toteuttaa yhdellä kryptoekonomisella järjestelmällä, jossa jokaiselle instrumentille luodaan erilliset tokenit. Näin eri instrumenttien kokonaiskuva selkeytyisi, joka mahdollistaisi paremman tilanne- ja kokonaiskuvan hahmottamisen markkinoista mikro- ja makrotasolla.

Luvun toisena skenaariona on, että perinteiset FIAT-valuutat tulevat jatkossa perustumaan lohkoketjuteknologiaan. Käytännössä tämä tarkoittaa sitä, että Euron tai muun mahdollisen FIAT-valuutan tarjontaa aletaan ennalta määrittämään pidemmälle aikavälille, jotta kokonaiskysynnän osatekijät voisivat paremmin valmistautua rahapolittiisiin muutoksiin, kun tarjontaan vaikuttavat muutokset ovat hyvissä ajoin ennakoitavissa. Tässä esimerkissä rahan tarjonta perustuu täysin matemaattiseen malleihin, joiden vaikutukset ovat ennalta laskettavissa. On kuitenkin haasteellista nähdä keskuspankkien luopuvan yhdestä sen tärkeimmistä työkaluista, koska rahapolitiikkaan vaikuttaminen on keskuspankkien yksi päätehtävistä (Pohjola 2012, 191 - 192) perinteisen ja vallitsevan talousteorian mukaan.

### 6.3 Vaihtoehtoiset talousjärjestelmät ja universaali perustulo

Radikaalimpana skenaariona voidaan kyseenalaistaa koko keskuspankkien, instituutioiden ja valtioiden roolin pitkällä aikavälillä. Mikä on kyseisten tahojen rooli yhteiskunnassa, jossa avoimeen lähdekoodiin pohjautuvat ohjelmat mahdollistavat täysin automatisoidun rahan liikkeellelaskun, rahapolitiikan, autonomiset organisaatiot ja älykkäät sopimukset? Älykkäät sopimukset mahdollistavat autonomiset organisaatiot ja älykkäät laki- ja regulaatiokokonaisuudet ilman ihmisten puuttumista järjestelmän toimintaan. Mikä rooli keskuspankeilla, instituutioilla tai jopa valtioilla on skenaariossa, jossa algoritmit voivat tehdä paljon vakaampia, objektiivisempia ja pitkäaikaisempia ratkaisuja poistaen ihmisten luomat epävakaudet? Näitä epävakauksia ovat esimerkiksi PESTE-analyysin osatekijät.

Käyttöönottotavasta riippuen kryptoekonomisilla järjestelmillä olisi myös mahdollista toteuttaa koko maapallon mittakaavassa toteutettava perustulo, jossa kaikille maailman ihmisille mahdollistettaisiin toimeentulo perustarpeiden täyttämiseksi. Tämän skenaarion pohdinta voisi itsessään olla oma opinnäytetyön aihe, joten skenaarion tarkempi analyysi ei kuulu tähän opinnäytetyöhön.

## 7 Yhteenveto

Tässä opinnäytetyössä on tutkittu kryptoekonomisia järjestelmiä dokumenttianalyysin ja tarkemmin kirjallisuuskatsauksen muodossa. Kryptoekonomisia järjestelmiä on tarkasteltu kryptografian perusteiden kautta, talousteorioiden ja Bitcoinin kryptoekonomisen järjestelmän käytännön toiminnan näkökulmasta havainnollistettuna.

Kryptoekonomiset järjestelmät toimivat kryptografian perusteiden mukaisesti täyttäen ainakin osan kryptografian määritelmistä ja hyödyntäen kryptografian fundamentteja. Kryptoekonomisia järjestelmiä on myös tarkasteltu taloustieteen oppien mukaisesti ja voidaan todeta, että kryptoekonomiset järjestelmät mukautuvat joihinkin talousteorioiden oppeihin. On kuitenkin syytä huomioida, että kryptoekonomiset järjestelmät eivät täytä yhdenkään tietyn talousteorian oppeja sellaisenaan, mutta eri talousteorian koulukuntien malleja mukailemalla jonkinlainen ekonominen toiminnallisuus on saavutettavissa. Talousteoria on kuitenkin ihmisen käyttäytymistä tutkivaa tiedettä. Tätä väitettä tukee yksinkertainen havainto, että opinnäytetyötä kirjoittaessa Bitcoin sekä useat muut kryptovaluutat ovat edelleen toiminnassa ja

niillä käydään vaihdantaa. Matti Pohjolan (2012, 11 - 13) mukaan talousteoriat pyrkivät kuvailemaan taloudellisia aktiviteetteja muodostaen niistä matemaattisia malleja ja tämä opinnäytetyö on pyrkinyt yhtenä ensimmäisistä suomenkielisistä teoksista luomaan viitekehystä kryptoekonomian perusteille.

Lähteet

Ammous S. 2018. The Bitcoin Standard. Hoboken; New Jersey: John Wiley & Sons, Inc.

Anttila P. 1998. Tutkimisen taito ja tiedonhankinta. Viitattu 23.10.2019. https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/

Boettke P. 1994. The Elgar Companion to Austrian Economics. Cheltenham, Northampton: Edward Elgar Publishing Limited.

Catalini Christian & Gans S. Joshua. Some Simple Economics of the blockchain. Viitattu 30.11.2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598.

Cryptoassets Taskforce: final report. Crown Copyright 2018.

Davidson S., De Flippi P. ja Potts J. 2016. Economics of Blockchain. Viitattu 29.11.2018. http://www.ssrn.com/abstract=2744751.

Delf, H. & Knebl H. 2002. Introdction to cryptography. Berlin; Heidelberg; New York; Barcelona; Hong Kong; London; Milan; Paris; Tokyo: Springen.

Ilmarinen H. 2016. Elliptisten käyrien kryptografia. Pro gradu –tutkielma. Matematiikan ja tilastotieteen laitos.

Johnson D., Menezes A. & Vanstone S. 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). Viitattu 3.4.2019. https://link.springer.com/article/10.1007/s102070100002.

Mattila J., Seppälä T., Hukkinen T., Laikar A., markkanen K., Kolu R., ja Jia K. 2019. Lohkoketjuteknologian hyödyntämismahdollisuudet palkkatulojen verotuksessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2019:30. Valtioneuvoston kanslia.

Menezes A., van Oorschot P. & Vanstone S. 1996. Handbook of Applied Cryptography. CRC Press.

Nakamoto S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Narayanan A., Bonneau J., Felten E., Miller A. ja Goldfeder S. 2016. Bitcoin and Cryptocurrency Technologies. Princeton and Oxford: Princeton University Press. Kindle Edition.

Pohjola M. 2012. Taloustieteen oppikirja. 7., uudistettu painos Helsinki: Sanoma Pro Oy.

Sipola S. 2015. Rahavallan jälj€t. Helsinki: Kustannusosakeyhtiö Teos.

Stallings W. 2011. Cryptography and Network Security Principles and Practice. 5., uudistettu painos. Boston; Columbus; Indianapolis; New York; San Francisco; Prentice Hall; Upper Saddle River; Amsterdam; Cape Town; Dubai; London; Madrid; Milan; Munich; Paris; Montreal; Toronto; Delhi; Mexico City; Sao Paulo; Sydney; Hong Kong; Seoul; Singapore; Taipei; Tokyo: Prentice Hall.

Tapscott D. & Tapscott A. 2016. Blockchain Revolution. New York: An imprint of Penguin Random House LLC.