VAASAN YLIOPISTO

KAUPPATIETEELLINEN TIEDEKUNTA

TALOUSTIETEEN LAITOS

Tuomas Kukkonen

BITCOIN–VIRTUAALIVALUUTTA
Uhkakuvat, mahdollisuudet sekä medianäkyvyyden ja osakemarkkinoiden vaikutus hintaindeksiin

Taloustieteen
pro gradu -tutkielma

VAASA 2016

SISÄLLYSLUETTELO

KUVIOLUETTELO

VAASAN YLIOPISTO
Kauppatieteellinen tiedekunta
Tekijä: Tuomas Kukkonen
Tutkielman nimi: Bitcoin-virtuaalivaluutta: uhkakuvat, mahdollisuudet sekä medianäkyvyyden ja osakemarkkinoiden vaikutus hintaindeksiin
Ohjaaja: Juuso Vataja
Tutkinto: Kauppatieteiden maisteri
Yksikkö: Taloustiede
Oppiaine: Taloustiede
Aloitusvuosi: 2009
Valmistumisvuosi: 2016
Sivumäärä: 51

TIIVISTELMÄ

Tavoitteena on selvittää bitcoin-virtuaalivaluutan toimintamalli ja arvioida sitä taloustieteellisestä näkökulmasta. Tämän selvittämiseksi on tarkasteltu hyötyjä ja haittoja sekä uhkakuvia. Empiirinen osio esittelee bitcoinin medianäkyvyyden ja arvon välistä yhteyttä ekonometrisesti. Myös USA:n osakemarkkinoiden kehitys on otettu mukaan hintaa selittävänä tekijänä, koska bitcoin on lyhyen historiansa aikana ollut spekulatiivisen sijoittamisen kohteena.

Bitcoinon uusi ilmiö ja niin myös sitä käsittelevät tieteelliset artikkelit. Suurin osa tämän tutkielman lähteinä käytetyistä artikkeleista olivat yliopistojen teknillisten tiedekuntien tuottamia jasuhteellisen äskettäin julkaistuja. Näiden pohjalta on kirjoitettu suuri osa hyöty- ja haittaelementtien analyysistä, josta teoriaosuus koostuu. Tämän perusteella on tehty johtopäätöksiä bitcoinin tulevaisuutta koskien.Bitcoin on tekniseltä toteutukseltaan monimutkainen, vaikka sen käyttö ei vaadi keskimääräistä korkeampaa tietoteknistä asiantuntemusta.

Keskeisimpinä havaintoina esiin nousivat rakenteelliset seikat, jotka rajaavat bitcoinin kykyähaastaa nykyinen elektroninen maksujärjestelmä. Toisaalta monet seikat puhuvat sen puolesta, että bitcoin tai muu vastaavalla teknologialla toimiva järjestelmä tulee olemaankäytössä tulevaisuudessa nykyisten järjestelmien rinnalla. Empiirinen osio viittaa siihen, että bitcoin on ollut monille korkean riskin sijoituskohde ja että siihen on liittynyt hintakupla, jota medianäkyvyys on osittain ollut aiheuttamassa.

AVAINSANAT: bitcoin, virtuaalivaluutta, vertaisverkko, BTC, p2p

1 JOHDANTO

Tutkielman tarkoituksena on selvittää vertaisverkkoperiaatteella operoivan bitcoin-virtuaalivaluutan toimintaa ja valottaa käytännön tasolla sen teknistä toteutusta. Onko bitcoin tai vastaava järjestelmä olemassa vielä 5-10 vuoden kuluttua ja voiko se joskus korvata nykyisen elektronisen maksujärjestelmän? Onko bitcoinilla edellytyksiä vakiinnuttaa paikkansa kiinteänä osana globaalia taloutta, vai jääkö se vain lyhytikäiseksi ilmiöksi?Järjestelmän toimintamallin tutkiminen sisältää omalta osaltaan teknisen toteutuksen tarkastelua, joka on kuitenkin pyritty tekemään mahdollisimman suppeasti päähuomion keskittyessä reaalimaailman ulottuvuuksiin ja käytännön ilmiöihin.Tutkielman teoriaosuudessa esitetään bitcoinien transaktioprosessi ja toinen verkon keskeinen prosessi, louhinta. Louhinta ei ainoastaan luo uudet bitcoinit, vaan pitää myös samalla huolen verkon turvallisuudesta. Tutkielman empiirisessä osiossabitcoinin arvon vaihtelua on tutkittu ekonometrisesti.

Tänä päivänä käyttämämme raha on suurimmaksi osin vain sähköisiä merkintöjä pankkien tietojärjestelmissä. Pankkijärjestelmässä näiden merkintöjen tuottaminen vaatii vain vähäisen työmäärään ilman merkittäviä raaka-aine- tai energiakustannuksia. Fiat-valuutta, esimerkiksi euro, on siis suurimmilta osin Bitcoinin tapaan aineetonta ja sen arvo perustuu luottamukseen. Tästä näkökulmasta voidaan siis olettaa Bitcoinin olemassaolon ja aseman täysin elektronisena ja samalla yleisesti hyväksyttynä maksuvälineenä olevan uskottavaa, jos se kykenee saavuttamaan vastaavan luottamuksen tason tarpeeksi suuren yleisön silmissä.

Tutkielmassa on arvioitu järjestelmän kustannuksia suhteessa nykyiseen elektroniseen maksujärjestelmään sekä yleisimpiä hyötyjä ja haittoja joita virtuaalinen luonne on tuonut esille. Haittapuoleksi luokiteltavien rikollisuutta mahdollistavien ominaisuuksien ja niiden seurausten tutkiminen eivät ole pääasiallinen tarkastelun kohde, mutta myös ne on tuotu esille ja käsitelty pikaisesti tutkielman loppupuolella.

Bitcoinia käsittelevien mediajulkaisujen luonne vaihtelee suuresti julkaisijasta riippuen. Toisaalla se esitetään hyvin negatiivisessa valossa ja uhkakuvana, kun taas toisaalla kehityskelpoisena ja tervetulleena teknistaloudellisena

innovaationa. Siksi myös kirjoitushetkellä vallinnut tilanne mediassa on huomioitu sille varatuissa kappaleissa.

Hyötyjen ja haittojen analysoinnin lisäksi teoriaosuudessa vertaillaan bitcoinia taloustieteellisestä näkökulmasta perinteisiin ja yleisesti käytössä oleviin Fiat-valuuttoihin. Bitcoin on ollut yleisessä käytössä vasta muutamia vuosia, mutta sen suosio on kasvussa ja yhä useampi taho hyväksyy sen maksuvälineenä perinteisten valuuttojen rinnalla. Tästä syystä sen tarkastelu ei ole vain ajankohtaista, vaan myös tarpeellista.

Tutkielman empiirisessä osiossa esitetään regressioanalyysi, jonka tarkoituksena on tutkia bitcoinin arvon vaihtelua sijoitushyödykkeenä ja sitä, onko bitcoinin medianäkyvyydellä tilastollisesti selittävää vaikutusta valuutan hintaindeksin kehitykseen. Medianäkyvyyttä kuvaava muuttuja on google-hakujen määrä aihetta koskevalla hakusanalla (”bitcoin”). Hintaindeksin rajut vaihtelut sekä räjähdysmäinen piikki syystalvella 2013 viittaavat jonkinlaiseen kuplaan sekä ”hypeen”, joka bitcoinin ympärille muodostui tai osittain jopa tarkoituksella luotiin.Toisena selittävänä muuttujana on otettu mukaan USAn osakekurssien kehitys tarkasteltavalta aikaväliltä.Sitä kuvaamaan on otettu Standard &Poor's 500 –indeksi. Se on sisällytetty analyysiin, koska bitcoinin olemassaolon ensimmäisten vuosien räjähtävä arvonnousu on väistämättä kasvattanut sen kiinnostavuutta sijoituskohteena, eikä niinkään sen alkuperäisen funktion mukaisesti maksuvälineenä. S&P 500 antaa informaatiota siitä, seuraileeko bitcoinin hintaindeksin kehitys osakemarkkinoiden yleistä kehitystä, vai ovatko ne sijoitushyödykkeinä ajateltuna toimineet mahdollisesti toistensa substituutteina.

Koska bitcoin perustuu vertaisverkkoon, siinä ei ole keskuspankin lailla toimivaa keskitettyä ohjaajaa. Ohjaavana tekijänä voidaan kuitenkin pitää sisäänrakennettua deflaatiota, johtuen elliptiseen käyrään perustuvasta kryptografiasta. Yksi keskeisistä tavoitteista on selvittää, onko keskusvallan puuttuminen ja sisäänrakennettu, ennalta odotettavissa oleva deflaatio käytännössä suurempi hyöty vai haitta bitcoinin tulevaisuudelle.

Aiheen tutkiminen on tärkeää, koska bitcoin on ilmiönä vielä uusi ja melko tuntematon. On siis perusteltua tehdä selonteko bitcoiniin liittyvistä mahdollisuuksista ja uhkakuvista, sekä analysoida medianäkyvyyden ja

osakekurssien muutosten vaikutusta sen hintaan. Lisäksi on kiinnostavaa ja tarkoituksenmukaista pyrkiä analysoimaan sen potentiaalia osana globaalia talousjärjestelmää. Yksikään aiempi yritys luoda kokonaan virtuaalinen valuuttajärjestelmä ei ole pysynyt pystyssä yhtä kauan kuin bitcoin. Siksi siihen oletettavasti liittyy tekijöitä, jotka voivat tehdä siitä pysyvän taloudellisen instituution.

Vasta muutamia vuosia sitten perustettu järjestelmä on heilahdellut arvossaan huomattavasti ja siksi jonkinlaisesta hintakuplasta puhuminen on perusteltua. Medianäkyvyyden voidaan olettaa vaikuttaneen arvoon huomattavasti ja mahdollisesti nostaneen sen suhteettoman korkealle, jolloin kyseessä on ns. kupla.

Arvon noustessa myös sijoitusmielenkiinto on epäilemättä noussut ja omistajat ovat pyrkineet spekulatiivisella käytöksellään lyhyen aikavälin sijoitushyötyihin. Koska kyse on uudesta sijoituskohteesta jonka arvon kehityksestä ei löydy aiempaa aineistoa, voidaan bitcoinia pitää erittäin korkean riskin sijoituksena. Se toimii itsenäisesti ilman perinteisiin sijoituskohteisiin liittyviä instituutioita ja niiden tarjoamaa suojaa, minkä takia riskit ovat entistä korkeammat. Kun osakemarkkinoiden tilanne on hyvä, sijoittajilla voidaan ajatella olevan enemmän varoja ja mielenkiintoa korkean riskin sijoituskohteisiin. Tämän takia hintaindeksin voidaan olettaa muuttuvan samansuuntaisesti osakemarkkinoiden tilanteen kanssa. Näiden edellä lueteltujen tekijöiden perusteella hypoteesit ovat:

H1: Bitcoin ei ole vain ohimenevä ilmiö, vaan virtuaalivaluutat muodossa tai toisessa ovat tulleet jäädäkseen.

H2: Bitcoinin saama mediahuomio on nostanut sen arvoa ja ollut osaltaan luomassa hintakuplaa.

H3: Bitcoin on korkean riskin sijoituskohde ja sen arvo muuttuu samansuuntaisesti osakemarkkinoiden kehityksen kanssa.

Tutkielma koostuu kuudesta luvusta sekä liitteistä ja lähdeluettelosta. Toisessa luvussa käydään läpi bitcoinin keskeinen idea ja tekniset toimintaperiaatteet. Kolmannessa luvussa käsitellään siihen liittyviä hyötyjä ja haittoja, sekä niihin liittyviä mahdollisia tulevaisuuden skenaarioita. Neljäs luku on katsaus

tutkimusaineistoon sekä menetelmiin, joilla tutkimuksen empiirinen osio on toteutettu. Viides luku koostuu tutkimustuloksista ja kuudennessa käydään läpi niiden perusteella tehdyt johtopäätökset.Viimeinen luku on lähdeluettelo.

2 BITCOIN

Bitcoin on ilman keskusvaltaa toimiva virtuaalivaluutta, jossa julkinen tapahtumaketjun historia estää rahan moninkertaisen käytön. Sen esitteli ensimmäisenä SatoshiNakamoto (todennäköisesti pseudonyymi) itse julkaisemassaan artikkelissa ja häntä pidetään myös järjestelmän tärkeimpänä kehittäjänä. (Nakamoto 2008)

Bitcoin (BTC) on siis ilman välikäsiä tai keskuspankkia toimiva ja vertaisverkkoteknologiaan perustuva, täysin elektroninen valuuttajärjestelmä. Bitcoinin keskeinen tarkoitus on tarjota käyttäjilleen mahdollisuus siirtää maksu suoraan osapuolelta toiselle peruuttamattomasti sekä ilman rahoituslaitoksen osallistumista ja siten vähentää maksuun sisältyviä transaktiokustannuksia sähköisessä kaupankäynnissä (Nakamoto 2008). Luonnollisesti myöskään rahan liikkellelaskijana toimivaa keskusvaltaa ei tarvita eikä liikkeellelaskemisena tuntemamme käsite ole bitcoinin tapauksessa edes mahdollinen, johtuen vertaisverkkoteknologiasta. Yhdelläkään verkon jäsenellä ei ole toista suurempaa lähtökohtaista auktoriteettia tai kontrollia bitcoin-taloudessa.

Teknisten yksityiskohtien ja järjestelmän takana olevan ohjelmoinnin hallitseminen vaatii todellista, ammattimaista asiantuntijuutta tai vähintään vahvaa tietoteknistä harrastuneisuutta. Yleisten toimintaperiaatteiden ymmärtäminen ei kuitenkaan ole tavalliselle tietokoneen käyttäjälle millään tavalla mahdoton tehtävä.

2.1 Transaktiot ja toimintamalli

Koska bitcoin on kryptografiaan perustuva P2P-valuutta, on syytä tarkastella sen toimintaa teknisestä näkökulmasta. bitcoin on teknisesti kuitenkin niin monimutkainen, että tässä tutkimuksessa pyritään käymään tekninen puoli läpi vain pääpiirteittäin ja tavalla, jonka jokainen vähän aiheeseen perehtynyt kykenee ymmärtämään.

Koska bitcoin-verkossa ei ole keskusvaltaa tai pankkien keskinäistä selvittelyä suorittavaa osapuolta, jonossa olevat transaktiot ja uuden rahan levitys varmentuu verkon konsensus-periaatteella. Jonossa olevat transaktiot lähetetään julkisesti kronologisessa järjestyksessä ja kootaan blokeiksi. Louhijat ovat antaneet verkon käyttöön tietokoneidensa laskentatehoa ja pyrkivät ratkaisemaan salausavaimen, joka varmistaa että uusi blokki sisältää vain valideja transaktioita. Kun blokki on varmennettu, se lisätään pääkirjaan, jota sanotaan blokkiketjuksi.

Bitcoin on siis nimensä mukaisesti biteistä koostuva kolikko. Käydään läpi esimerkkitilanne, miten bitcoin muodostuu ja siirtyy luotettavasti todelliselta omistajalta halutulle osapuolelle.

Osapuolilla A ja B on molemmilla oma bitcoin-lompakko, joka on käyttäjän hallussaan pitämä tiedosto, tyypillisesti muotoa wallet.dat. Se koostuu useista osoitteista ja mahdollistaa pääsyn näihin osoitteisiin, jotka ovat bitcoineja. Yksi osoite ei siis vastaa perinteistä pankkitiliä, vaan se on usean osoitteen summa. Nämä osoitteet koostuvat numeroista ja kirjaimista. Jokaisella osoittetta vastaa sille määritetty tietty summa kolikoita. Kun henkilö A lähettää henkilölle B rahaa, henkilö A luo uuden osoitteen johon summa lähetetään. Jokaisella osoitteella on sähköinen avainpari, joka koostuu julkisesta ja yksityisestä avaimesta. Henkilö A hyväksyy omassa lompakossaan siirron henkilön A osoitteeseen yksityisellä avaimellaan. Nyt kuka tahansa verkon muu osapuoli C voi varmentaa osoitteen julkisen avaimen ja siten hyväksyä transaktion tulleen oikealta omistajalta.

Tämän jälkeen kuvaan astuvat ns. louhijat, joiden tietokoneet keräävät yhteen verkon transaktiot viimeisen 10 minuutin ajalta ns. blokiksi ja luovat sen perusteella salausfunktion (hashfunction).

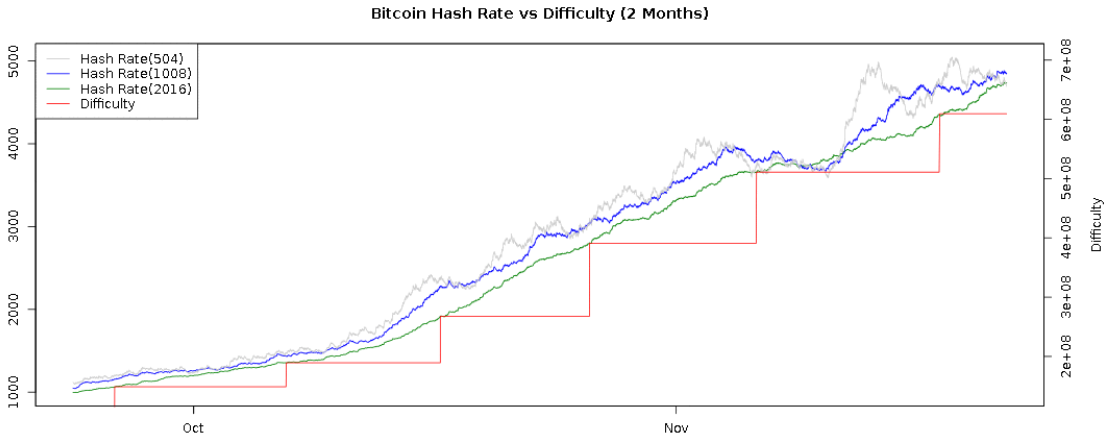
2.2 Louhinta - valuutan syntyprosessi

Louhijoiden tietokone on asetettu laskemaan datalle eli verkon uusille transaktioille salausfunktion, joka on määrätyn pituinen alfanumeerinen koodi. Louhintaa suorittavat tietokoneet laskevat uudelle blokille salausfunktioita ja

kilpailevat siitä, kuka löytää oikean koodin ensimmäisenä ja lunastaa siitä jaettavan palkinnon uusien kolikoiden muodossa. Voittaja valikoituu satunnaisesti, mutta mitä suurempi laskentateho louhijalla on käytössään, sitä suurempi on todennäköisyys löytää ratkaisu ensimmäisenä. Oikea koodi on se, jonka laskennallinen vaikeusaste on korkein; verkko hylkää pääkirjan haarat, joissa enemmistö varmennuksen suorittajista ei hyväksy koodin avullavarmennettavaatransaktiohistoriaa alkuperäiseksi. Louhijat siis osaltaan varmentavat tehtyjä transaktioita, mutta myös luovat uusia kolikoita talouteen. Lisäksi louhija saa omakseen uuden blokin transaktioiden palkkiomaksut.

Eräs louhintaan liittyvä seikka on myös syytä tuoda esille. Järjestelmä on rakennettu siten, että blokin luomisen vaikeusaste vaihtelee verkon laskentatehon mukana. Yksi uusi blokki syntyy keskimäärin 10 minuutissa ja aina kun 2016 blokkia on luotu, järjestelmä laskee vaikeusasteen uudelleen, verkon kokonaislaskentatehon mukaisesti. Toistaiseksi bitcoin-verkossa laskentaa suorittavien yksikköjen määrä, kuten myös niiden suorituskyky on jatkanut kasvuaan, joten vaikeustaso on kasvanut. Tämä siksi, että uuden blokin ratkaisuun tarvittavan ajan keskiarvo pysyisi arvossa 10 minuuttia.

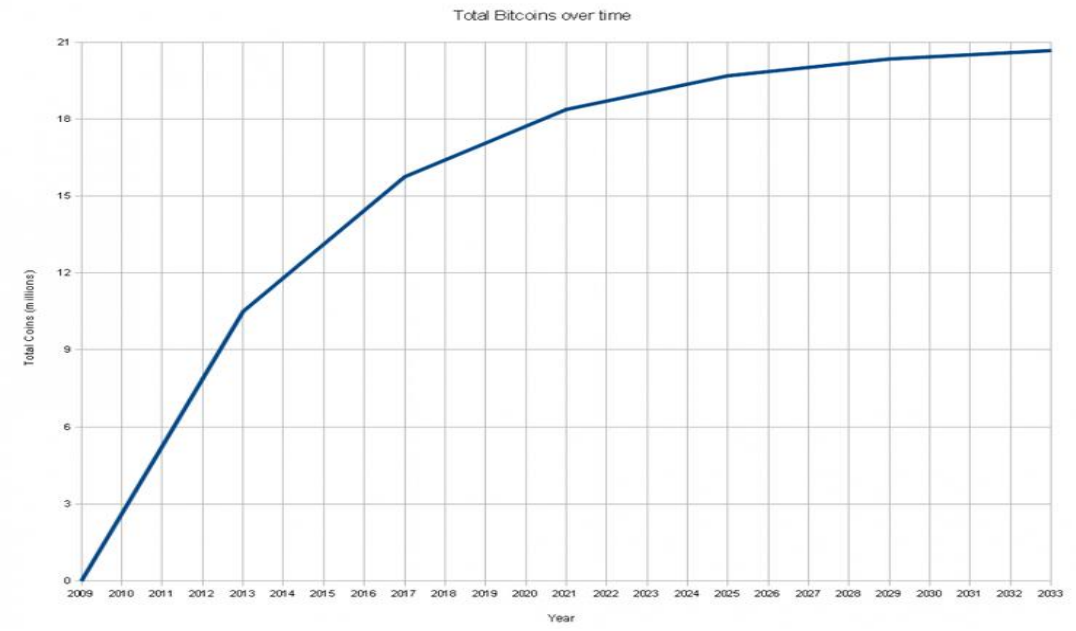
Alla olevasta kuviosta näkyy, kuinka vaikeusaste nousee harppauksittain tasaisin väliajoin. Vasemmalla näkyvät luku on *hashrate*, joka kuvaa viimeisimmän 504 blokin ratkaisemisen laskemiseen vaadittujen hash-arvojen määrää. Oikealla näkyy vaikeusaste, joka kertoo kuinka monta kertaa vaikeampaa blokin ratkaisu on suhteessa ensimmäiseen ikinä luotuun blokkiin.



Kuvio 1: Vaikeusaste

Louhinnasta saatu palkinto pienenee jatkuvasti, kuten myös uusien bitcoinien määrä. Tämä perustuu bitcoinin elliptisen käyrän kryptografiaan; uusien kolikoiden määrä puolittuu joka neljäs vuosi ja maksimissaan niitä voi syntyä noin21 miljoonaa. Bitcoin voidaan jakaa kahdeksanteen desimaaliin asti ja pienin yksikkö 1 BTC x 10^-8 on nimetty satoshiksi, pääkehittäjä SatoshiNakamoton mukaan (Jeong 2013). Tarpeen niin vaatiessa, myös useammat desimaalit ovat tulevaisuudessa mahdollisia.

Järjestelmän tekninen luotettavuus perustuu siis tapahtumaketjun julkiseen historiaan; Jokainen bitcoin-transaktio sisältää verkon koko transaktiohistorian kaikki aiemmat tapahtumat. Omistuksen varmenteena käytetään edellisessä kappaleessa käsiteltyjä digitaalisia allekirjoituksia ja vertaisverkko hyödyntää tapahtumaketjun POW-mekanismia (proof-of-work) estäen rahan käyttämisen useaan kertaan. Luotettavuus perustuu siis puhtaasti matematiikkaan.



Kuvio 2: Yli puolet kaikista bitcoineista on jo louhittu.

Kuvasta 2 näkyy, kuinka uusien kolikoiden määrä vähenee ajan myötä. Ennusteen mukaan vuoden 2035 jälkeen uusia kolikoita ei enää ole mahdollista louhia.

3 HYÖDYT JA HAITAT

Hyötyjen ja haittojen tutkimuksessa on käyty läpi tiettyjä teknisten uhkakuvien ja tulevaisuudessa potentiaalisesti realisoituvien ongelmien skenaarioita, sekä käytännön vaikeuksia ja etuja joita bitcoinin käyttöön liittyy. Hyödyt ja haitat sisältävät sekä koko systeemiä koskevia makrotason ilmiöitä, kuten myös yksittäisen käyttäjän näkökulmasta välittömiä käytännön asioita.

3.1 Hyödyt

Selkeimpinä hyötyinä teoreettisessa tarkastelussa esiin nousevat kustannussäästöt, joita peruuttamattomat ja ilman välittäjää tapahtuvat maksusuoritukset voivat mahdollistaa. Eräästä näkökulmasta myös vähäisin toimenpitein saavutettava anonymiteetti voi olla etu, mutta koska sitä ei voida varauksettomasti pitää järjestelmää parantavana ominaisuutena, ei sitä myöskään ole luokiteltu hyödyksi.

3.1.1 Kustannussäästöt

Digitaalinen rahan voidaan katsoa tarjoavan joitain merkittäviä hyötyjä verrattuna perinteisiin fiat-valuuttoihin. Eräs näistä on osapuolten fyysisen läsnäolon tarpeettomuus maksun loppuun saattamiseksi, sekä sen välittömyys. Käytössä olevassa sähköisessä maksujärjestelmässä pankkien välillä siirtyvät sähköiset suoritukset ottavat aikansa, erityisesti niiden tapahtuessa maiden rajojen yli. Bitcoin maksu voidaan suorittaa ajasta, paikasta ja osapuolten läsnäolosta riippumatta heti.

Tämä etu luo useita taloudellisia hyötyjä. Fyysisen rahan tuotantoon, kuljetukseen ja käsittelyyn liittyvät kustannukset voivat olla merkittäviä (Plassaras 2013). Yhdysvaltojen keskuspankin painaman paperisen rahan arvioitu vuosittainen kustannus jälleenmyyjille ja pankeille on 60 miljardia dollaria, joka sisältää käsittely- ja kirjanpitokustannukset säilyttämisestä,

kuljettamisesta ja turvaamisesta. Vastaava kustannus sähköisen järjestelmän (Bitcoin) korvatessa paperisen vaihtelisi kolmanneksen ja puolikkaan välillä edellä mainitusta. (Plassaras 2013)

Siirtyminen kokonaan digitaalisiin valuuttoihin vähentäisi kokonaistransaktiokustannuksia siirrettäessä rahaa eri tilien, pankkien ja maiden välillä. Järjestelmä epäilemättä tehostaisi ja halventaisi valuutan siirtelyä sekä yksittäisen käyttäjän että finanssi-instituution kannalta. Tässä arviossa ei kuitenkaan oteta huomioon itse verkon ylläpitoon ja toimintaan liittyviä energiakustannuksia, jotka ovat järjestelmän kasvaessa ja nykyteknologialla toteutettuna huomattava kustannus yhteiskunnalle. Kyseistä ongelmaa on käsitelty myöhemmin erikseen tässä tutkielmassa.

Bitcoinin yleistymisellä voisi olla myös positiivinen kouluttava ulkoisvaikutus, sillä sen käyttö vaatii ohjelmistoa. Tämä voisi teoriassa edesauttaa ihmisten kykyä omaksua ohjelmistojen käyttö talousasioidensa hoitamiseen ja optimoimiseen.

3.1.2 Peruuttamattomatmaksusuorituksetjakeskusvallantarpeettomuus

Bitcoinin tärkein kehittäjä, SatoshiNakamoto korostaa alkuperäisessä julkaisussaan bitcoinin hyötynä ja oleellisena piirteenä sillä suoritetun transaktion peruuttamisen mahdottomuutta. Tämän näkökannan ymmärtämiseksi on tarkasteltava hieman nykyisiä internet-kaupankäynnissä vallitsevia metodeja ja verrattava niitä bitcoiniin.

Bitcoinin virallisen julkaisun (white paper) mukaan käytössä oleva, kolmannen osapuolen sisältämä maksujärjestelmä toimii tarpeeksi hyvin suurimpaan osaan transaktioita, mutta ei kuitenkaan välty tietyiltä sisäsyntyisiltä heikkouksilta. (Nakamoto 2008)

Internetissä tapahtuvassa kaupankäynnissä vallitsee lähes täysin perinteinen maksujärjestelmä, jossa rahoituslaitos tai muu maksunvälittäjä välittää maksun osapuolelta toiselle. Tässä järjestelmässä täysin peruuttamaton transaktio on käytännössä mahdotonta. Välikäden olemassaolo luo tietynlaista turvaa molemmille osapuolille, mutta näkyy myös rahan käyttäjiin kohdistuvina,

ylimääräisinä transaktio- ja muina kustannuksina. Esimerkiksi maailman suurimmassa elektronisessa huutokaupassa, eBayssa, käyttäjien suosiota nauttiva PayPal-maksupalvelu tai käyttäjän siihen liittämän maksukortin tarjonnut luotottaja, esimerkiksi Visa, joutuvat usein sovittelijoiksi riitatilanteissa. Ostaja voi myös peruuttaa maksusuorituksen maksukorttinsa liikkellelaskijan avulla (takaisinperintä), joka puolestaan päättää viime kädessä maksun toteutumisesta. Myös tilanne, jossa kauppa paljastuu luottokorttipetoksen avulla tehdyksi, myyjä voi jäädä lopulta täysin ilman korvausta.

Maksusuorituksen peruuntumisen ollessa useissa tilanteissa mahdollista, luottamuksen tarve kasvaa. Myyjien on oltava tarkkoja asiakkaistaan ja mahdollisesti pyrittävä keräämään tietoja heistä, jotka olisivat muuten täysin tarpeettomia. Tietty petoksen määrä on välttämätöntä ja hyväksyttyä ja ikäänkuin systeemistä hävikkiä, jonka myyjät ja ostajat lopulta maksavat (Nakamoto 2008). Eräässä julkaisussa oli maininta myyjästä, jonka kauppatavaraa olivat harvinaiset aikakausilehdet. Bitcoinin transaktion peruuttamattomuus mahdollisti kauppa-alueen laajentamisen myös maihin, jotka hän ennen oli pitänyt poissa listaltaan niissä ilmenevien luottokorttihuijausten suuren määrän takia (Barber, Boyen,Shi&Uzun 2012).

Keskusvallasta vapaan valuuttajärjestelmän suurimpana hyötynä Nakamoto nostaa esiin sen, että tämän päivän elektroninen maksujärjestelmä nojaa raskaasti niitä prosessoivien instituutioiden työhön. Nämä instituutiot nauttivat yleisesti laajaa luottamusta ja hoitavat sähköiset maksut ja varmistavat koko systeemin lahjomattomuuden globaalissa mittakaavassa. Vastapainoisesti nämä instituutiot maksattavat tekemänsä työn yhteiskunnalla. Bitcoinin tavoite on korvata rahoitusinstituutioiden ja keskusvaltojen nauttima luottamus vastaavalla luottamuksella PoW-toimintaperiaatteeseen ja tehdä rahoituslaitosten osallistuminen turhaksi. Instituutioiden käyttämät resurssit voisivat täten vapautua muuhun hyötykäyttöön.

On kuitenkin pidettävä mielessä, että bitcoin ei ole myöskään ilmainen järjestelmä. Laskennallisen tehon tarve varmistustyön tekemiseen on hankittava, mahdollistettava ja pidettävä yllä.

3.2 Haitat

Haittapuolet ja ongelmat bitcoinin kaltaisessa rahajärjestelmässä jakautuvat pääpiirteittäin järjestelmän omiin, sisäänrakennettuihin rajoituksiin ja toisaalta käyttöön liittyviin ulkoisiin ongelmiin. Sisäänrakennetuista ongelmista esimerkkeinä ovat energiatehokkuus ja valuutan määrän rajallisuus. Ulkoiset ongelmat ovat suurimmilta osin yksittäistä käyttäjää tai käyttäjäryhmää koskevia turvallisuusriskejä ja mikrotason taloudellisia ongelmia, mutta osittain myös ison mittakaavan ilmiöitä. Esimerkkejä jälkimmäisestä ovat mm. rahanpesu sekä huumekauppa.

3.2.1 Ulkoiset ongelmat

Ulkoisina ongelmina esitetään valuutan käyttöön ja käytettävyyteen liittyviä, järjestelmän ulkopuolelta peräisin olevia ilmiöitä. Näistä huomattavimpina nousevat esiin valuutanvaihtoa suorittaviin yrityksiin kohdistuvat tietomurrot sekä valuutan arvon heilahtelut.

3.2.2 Tietomurrotsekävarkaudet

Bitcoin tai tarkemmin sanottuna sillä kauppaa käyvät yritykset ovat kohdanneet lyhyen historiansa varrella hyökkäyksiä hakkereiden taholta ja myös kärsineet niiden takia huomattavaa vahinkoa. Kuuluisimpana esimerkkinä voidaan mainita kesäkuussa 2011 suosittuun japanilaiseen Mt. Gox-kauppapaikkaan kohdistuneet kavallukset, jotka koettelivatbitcoinin arvoa ja yleisön luottamusta kovalla kädellä.

3.2.3 Hintaerot

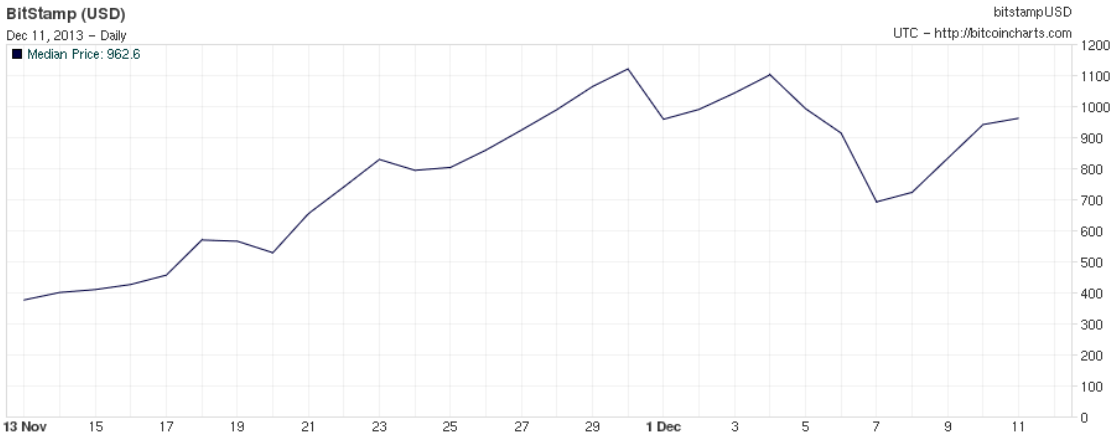
Bitcoinia välittävien palveluntarjoajien kursseja tarkasteltaessa niistä löytyy huomattavia eroavaisuuksia. Seuraavista kuvioista nähdään, että volyymilla mitattuna vuoden 2013 suosituimmalla bitcoineja välittävällä kauppapaikalla, japanilaisella Mt. Goxilla 9.12.2013 8.50 Suomen aikaa yhdestä bitcoinista joutui maksamaan 876 dollaria (USD). Sloveniassa, missä BitStamp-kauppapaikka sijaitsee, vastaava hinta oli 854,67 dollaria, eli yli 20 dollaria vähemmän. Kiinalaisen BTC-Chinan myyntihinta oli 5280 juania joka vastasi tuolla hetkellä 866,75 dollaria.

Teoriassa järjestelmällä ei ole rajoja siinä mielessä, että se on virtuaalinen ja internetiin rakennettu. Todellisuudessa, äsken tarkasteltujen lukujen perusteella voidaan todeta että sen arvoon vaikuttaa kuitenkin valtavasti maantieteellinen sijainti. Vaikka itse bitcoin onkin hajautettu eli keskusvallasta vapaa, sen kaupankäynti keskittyy toistaiseksi suurilta osin muutamiin, ison kokoluokan kauppapaikkoihin.

	Symbol	Latest Price	30 days	Average	Volume
▲	BTC China CNY btcnCNY	5280 0 min ago		4796.23 483.77 10.09%	2,164,386.60 10,380,892,367.11 CNY
▲	Mt. Gox USD mtgoxUSD	876 0 min ago		742.55 133.45 17.97%	1,260,419.59 935,930,361.06 USD
▲	BitStamp USD bitstampUSD	854.67 2 min ago		681.29 173.38 25.45%	1,084,942.31 739,165,126.45 USD
▲	btc-e USD btceUSD	867.1 0 min ago		680.28 186.82 27.46%	1,066,928.05 725,814,712.09 USD
▲	Mt. Gox EUR mtgoxEUR	644 0 min ago		527.68 116.32 22.04%	168,177.06 88,744,444.74 EUR
▲	Mt. Gox JPY mtgoxJPY	90000 0 min ago		69377.68 20622.32 29.73%	60,491.77 4,196,778,778.68 JPY
▲	bitcoin.de EUR btcdeEUR	629 0 min ago		526.24 102.76 19.53%	53,151.44 27,970,570.85 EUR

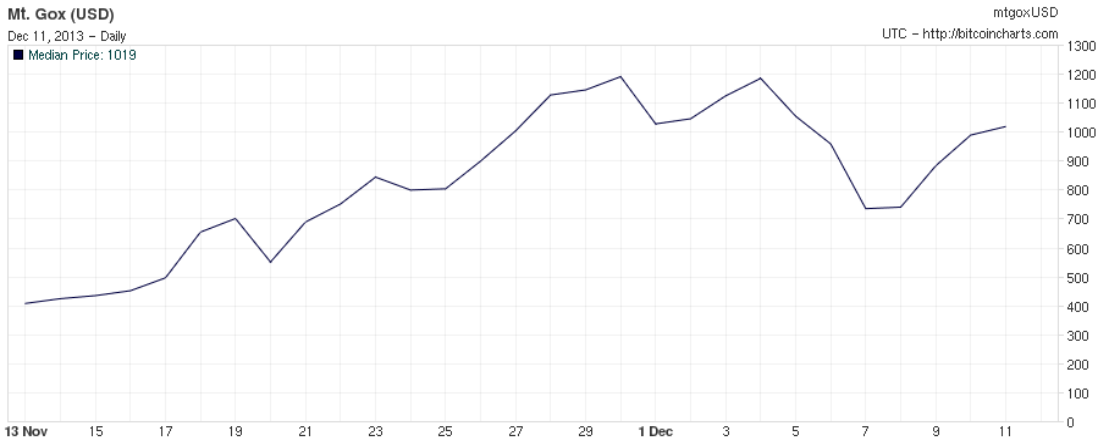
Kuvio 3: Hintaindeksit 9.12.2013

Missä tahansa kehittyneessä taloudellisessa järjestelmässä valuutan tai hyödykkeen hinta on käytännössä sama sijainnista riippumatta. Tämä johtuu suurilta osin arbitraasin mahdollisuudesta, eli paikkojen välisten hintaerojen hyödyntämisestä. Erityisesti valuuttakaupassa sitä tapahtuukin jatkuvasti ja sillä on taipumus tasoittaa kurssivaihteluja.



Kuvio 4: BitStampin USD/BTC 13.11 - 11.12.2013

Seuraavissa kuvioissa on Mt. Goxin ja BitStampin mediaanihinta bitcoinille samalta 30 päivän ajalta. Niitä vertaillessa huomataan, että jokaisena päivänä Mt. Goxin hinta on ollut vähintään kymmeniä tai jopa yli 100 dollaria BitStampia suurempi.



Kuvio 5: Mt. Goxin USD/BTC 13.11 - 11.12.2013

Tästä voisi päätellä jatkuvan arbitraasin näiden paikkojen välillä olevan kannattavaa. Näin ei kuitenkaan ole. Vaikka bitcoinien liikuttelu on nopeaa ja halpaa, ns. oikean rahan liikuttelu kansainvälisten rajojen yli on edelleen kallista ja hankalaa.

Kesäkuussa 2013 USAn hallitus sulki Mt. Goxin markkinoiltaan jäädyttämällä sen varat Dwolla-palvelussa, joka oli oleellinen osa Mt. Goxin dollarirahoitusta(Motherboard 2013).Tällöin ainoa keino saada tarvittavat dollarivarat kaupankäynnin suorittamiseen on käyttää paikallista japanilaista pankkia (mahdollisesti useampia) ja tämä saattaa vaatia dollarien ostoa japanin juaneilla. Prosessi on kallis ja sisältää transaktiomaksuja joka välikäden kohdalla. Nämä kustannukset selittävät pitkälti Mt. Goxin korkeamman hintaindeksin, sillä BitStampilla vastaavaa ongelmaa ei ole. Lisäksi Mt. Goxilla vaikuttaa suositun bitcointalk.org-keskustelufoorumin kirjoitusten perusteella olevan käyttäjien keskuudessa yleisesti ottaen hyvä maine, joka voi myös tehdä siitä hieman kalliimman.

Halvemman hinnan tarjoavat kauppapaikat sijaitsevat fyysisesti usein maissa, joissa sääntelyn ja valvonnan tasot ovat matalampia. Esimerkiksi BTC-E on bulgarialainen, jolloin varojen lunastaminen tarkoittaa rahojen siirtoa kyseisestä

maasta. Viranomaisvallan ja lainvoiman heikomman tason vuoksi myös palvelun taso voi olla arvaamatonta. bitcoin-pörsseille yhteinen tekijä on niiden vapaus tiukoista reservivaatimuksista likvidin rahan suhteen, joka myös helposti vaikeuttaa ja pitkittää lunastusprosessia käyttäjän kannalta. Kauppapaikka onkin syytä valita huolella. Bitcoin on vain 4 vuotta vanha, siinä missä luottamukseen rakennetut rahoitusinstituutiot ovat tyypillisesti useiden vuosikymmeniä kestäneen työn tulosta. BTC-Chinan toimitusjohtaja Bobby Lee toi esiin taloustietotoimisto Bloombergin haastattelussa joulukuussa 2013 tilastofaktan, että puolet kaikista bitcoin-välittäjistä lopettavat toimintansa vuoden kuluessa aloittamisesta keskimääräisen elinkaaren ollessa kirjoitushetkellä n. 380 vuorokautta. (Bloomberg 2013)

Hyvä varoittava esimerkki on Hong Kongissa toiminut GBL, joka oli olemassa vain 4 kuukautta hävittäen sinä aikana 4,1 miljoonaa dollaria käyttäjien ja sijoittajien varoja suljettuaan äkillisesti lokakuussa 2013. Huomattava määrä käyttäjistä pidättäytyi vaihdannasta arvon heilahtelujen takia, joka johti kassavirran kuivumiseen. Vihaiset asiakkaat saapuivat internetsivulla ilmoitettuun käyntiosoitteeseen vain huomatakseen sen olevan tekaistu. (The Standard 2013)

Bitcoinin arvon noustua viimeisen vuoden aikana räjähdysmäisesti, sitä välittävistä kauppapaikoista on tullut erittäin suosittu kohde hakkereiden keskuudessa. Tyypillinen strategia on järjestelmällinen palvelunestohyökkäys (DDoS, Direct Denial of Service) joka voi tietoturvariskin lisäksi vaikuttaa valuuttakurssiin huomattavasti. DDoS on virtuaalihyökkääjien yleisesti käytössä oleva tapa varastaa tietokantojen sisältöä, tyypillisesti käyttäjätunnuksia ja salasanoja.

Bitcoin-kauppaa harjoittavat yritykset ovat kohdanneet lyhyen historiansa varrella hyökkäyksiä hakkereiden taholta ja myös kärsineet niiden takia huomattavaa vahinkoa. Surullisenkuuluisia esimerkkejä tästä ovat kesäkuussa 2011 sekä huhtikuussa 2013 suosittuun japanilaiseen Mt. Gox-kauppapaikkaan kohdistuneet hyökkäykset, jotka koettelivat bitcoinin arvoa ja yleisön luottamusta kovalla kädellä. Huhtikuun hyökkäysten jälkeen valuutan arvo romahti 40 prosenttia käytyään jo yli 200 dollarissa, saavuttaen saman tason uudelleen vasta 28.10.2013. (bitcoincharts 2013)

Tietomurtojen riski sekä niiden aiheuttama heilahtelu huomioon ottaen USAn hallituksen skeptinen ja tiukan oloinen suhtautuminen bitcoiniin ja sen rajoittamiseen on ymmärrettävissä ja perusteltu. Yhdysvaltojen viranomaiset ovat pyrkineet rajoittamaan bitcoinia varsin kovalla kädellä ja käytännössä niin paljon kuin se järjestelmän ulkopuolelta on mahdollista ja virtuaalivaluutan kelpoisuuden selvittämisen näkökulmasta se on pitkälti perusteltua. Bitcoinien ostaminen ja myyminen sisältävät edelleen runsaasti riskiä ja kauppapaikkojen negatiiviset tapahtumat ovat siitä hyvä esimerkki.

Bitcoin on nykytilassaan täysin riippuvainen muista valuutoista, erityisesti USAn dollarista; sen arvo määritellään yleisesti suhteessa dollariin ja koska Bitcoinin valuuttana hyväksyvät kauppapaikat ovat vasta yleistymässä, sen elinehto on toistaiseksi vaihdettavuus johonkin keskuspankkien painamaan yleisesti hyväksyttyyn rahaan.Koska vaihto fiat-valuutaksi ei suju läheskään yhtä helposti kuin transaktioprosessi, Bitcoinin hinta vaihtelee suuresti maantieteellisten rajoitusten ja vaihtopaikkojen kohtaamien ongelmien seurauksena. Tämän kaltaiset ongelmat voivat olla mahdollisia korjata ajan kanssa ja markkinavoimien kautta, jos lainsäädäntö ja rajoitukset saadaan ajan tasalle ja uutta toimintamallia vastaaviksi. Yhä useampien suhtautuessa järjestelmään ennenkaikkea maksuvälineenä sijoituskohteen sijaan, epävakaisuudet voivat tasoittua pois.

Tietoturvaan liittyviä riskejä arvioitaessa on hyvä pitää mielessä, että valuutan protokolla ja sitä välittävät kauppapaikat ovat kaksi eri asiaa. Järjestelmän ollessa vielä uusi, sen luotettavuus on tällä hetkellä kovassa testissä, mutta toistaiseksi tietoturva-aukkoja järjestelmässä itsessään ei ole havaittu. Sitä vastoin bitcoineja välittäviin palveluihin kohdistuneet hyökkäykset ovat nousseet useita kertoja uutisotsikoihin, menetysten ollessa pahimmillaan miljoonien eurojen arvoisia. Näissä tapauksissa on kuitenkin huomioitava, että kyseessä on ulkoisesta palveluntarjoajan tai käyttäjän oman huolimattomuuden takia syntynyt tietoturvariski, eikä sillä ole tekemistä bitcoin-järjestelmän transaktioprosessin kanssa.

3.2.4 Rakenteellisetongelmat

Bitcoin on syrjäyttänyt kaikki muut aiemmat yritykset luoda elektroninen käteinen raha, huolimatta kolmen vuosikymmenen tutkimustyön aiheen tiimoilta (Barber ym.2012). Sen suosio on ollut erittäin nousujohteista ja onkin

syytä selvittää syitä sen taustalla. Kuten tulemme huomaamaan, bitcoin on kaukana täydellisestä, vaikka sitä voidaan nykytilassaan pitää suhteellisen toimivana järjestelmänä.

3.2.5 Rakenteellinen deflaatio

Bitcoinin huomattavin rakenteellinen eroavaisuus perinteisestä keskuspankin kontrolloimasta valuutasta on sen äärimmäisen deflatorinen luonne. Ensimmäinen tätä seikkaa tukeva tosiasia on elliptiseen käyrään perustuva algoritmi, jonka mukaan uusien kolikoiden määrä puolittuu joka neljäs vuosi ja tietyn pisteen jälkeen (n. 21 miljoonaa) niitä ei enää synny. Myös louhinnasta eli uusia kolikoita synnyttävästä koneellisesta laskentatyöstä saatava palkinto pienenee jatkuvasti, vaikka samalla vaadittavan laskentatehon määrä kasvaa jatkuvasti. Tästä syystä koko ekosysteemin käynnissä pysyminen ja toiminta voi olla vaakalaudalla ja pahimmillaan jo hyvissä ajoin ennen kolikoiden teoreettista maksimimäärää käytännön katto voi tulla vastaan.(Barber ym. 2012) Lisäksi deflaatiota edesauttavat kaikki kolikot, joiden yksityinen salasana on unohtunut tai hävitetty. Tällaisia ns. zombie-kolikoita ei voida enää saada uudestaan käyttöön, vaan ne ovat poissa taloudesta kunnes salasana mahdollisesti saadaan tietoon. Kirjoitushetkellä bitcoinien kokonaismäärä on n. 7 miljoonaa ja kolikoita on raportoitu "zombeiksi" useita kymmeniä tuhansia. Deflatorinen spiraali on siis todellinen ja ehkä suurin yksittäinen uhkakuva koko järjestelmän tulevaisuudelle, eikä siihen ole toistaiseksi kehitetty hyväksi todettua ratkaisua.

Rahan määrän rajallisuus bitcoin-taloudessa johtaa tilanteeseen, jossa merkittävä arvonnousu on väistämätöntä, mikäli suosio nousee nykyistä, suhteellisen marginaalista tasoa suuremmaksi. Esimerkkinä voidaan ajatella kuvitteellinen tilanne, jossa bitcoin on saavuttanut eräänlaisen kypsien markkinoiden aseman, jossa 1% koko USAnBKT:sta vaihdetaan bitcoineissa (BTC) ja loput 99% Yhdysvaltojen dollareina (USD). Tällöin niiden reaalinen ostovoima nousee ajan myötä, sillä yksi BTC vastaisi jatkuvasti samaa osuutta tässä tapauksessa kasvavaksi oletetusta tuotannon määrästä. Kuten todettua, bitcoinien määrä on vakio toisin kuin dollarin, jota USAn keskuspankki voi halutessaan painaa lisää ilman teoreettista ylärajaa. Pitääkseen osuutensa kokonaisvaihdannan arvosta, BTC:n arvostuksen on noustava jos dollari samaan ei inflatoidu merkittävästi. Onkin hieman paradoksaalista, että bitcoin välttyy lähes kaikkia Fiat-valuuttoja vaivaavalta inflaatiolta, mutta sen

ainutlaatuinen elementti saattaa olla sen suurin ja lopulta romahduttava ongelma. Koska ennustettavissa oleva deflaatio on käyttäjien tiedossa, voidaan pitää melko todennäköisenä, että omalla käytöksellään he edesauttavat ja nopeuttavat sen tapahtumista. Valuutta, jonka arvo on korkealla ja oletettavasti jatkaa nousuaan, on erittäin houkutteleva sijoituskohde eikä kannusta vaihdantaan. Tämän teorian mukaan käytössä olevan rahan määrä pienenee edellä mainittujen tekijöiden lisäksi entisestään ja siten deflatorinen spiraali kiihtyy. Uusien blokkien luominen eli louhinta tulee entistä vähemmän kannattavaksi vaihdannan volyymin pienentyessä, kun laskentatyön palkintoja on vähemmän kerättävänä. Bitcoin-verkko saattaa rapistua käyttäjämäärän vähentyessä, sillä varmistustyötä tekevien noodien vähentyminen voi johtaa niin vakavaan heikentymiseen, ettei järjestelmä enää pysty toimintaperiaatteen mukaisesti suojaamaan ja korjaamaan itseään. (Barber ym. 2012)

Pahimmillaan arvonnousu voi aiheuttaa koko talouden jäätymisen ja sen myötä käyttäjien uskon romahtamisen ja koko systeemin sortumisen. Tämä voi tapahtua myös petoksen kautta, jota tarkastellaan seuraavassa kappaleessa. Tätä ns. jäätymisteoriaa vastaan voidaan toistaiseksi kuitenkin argumentoida käytännön olosuhteiden pakotteilla; Bitcoin on mahdollistanut monia valtiovallan estämiä rahansiirtoja ja lahjoituksia esimerkiksi Wikileaksille sekä laittomiksi luokiteltujen tuotteiden kaupankäyntiä ja on edelleen elinehto niiden toteutumiseksi jatkossakin. Niin kauan, kun vastaavaa, valtiovallasta vapaata ja yhtä hyvin toimivaa maksujärjestelmää ei ole, bitcoin on tärkeä maksuväline eikä ensisijaisesti sijoitusten ja spekulaatioiden kohde.

3.2.6 Uhkakuvana historian väärentäminen

Bitcoin sisältää koko transaktiohistorian, joten joka hetki sen louhinta, kuten myös käyttö vaatii aiempaa enemmän laskentatehoa tietokoneelta ja siten myös sen käytön kustannukset kasvavat ja siitä saatava hyöty yksikkömääräisesti pienenee.

Äärimmäinen, mutta ei millään tapaa poissuljettu skenaario on petos, jossa yksi osapuoli kykenisi kirjoittamaan koko Bitcoinin transaktiohistorian uudestaan ja syrjäyttämään jo olemassaolevan, aidon version. Tälläisen petoksen suorittaminen vaatisi huomattavaa koneellista suoritustehoa, muttei ole teoreettinen mahdottomuus vaan vakavasti otettava uhka.

Verkon luotettavuus perustuu eräänlaiseen äänestykseen; kun uudet transaktioketjut luodaan blokiksi, verkossa toimivista varmennusta suorittavista louhijoista yli puolien täytyy hyväksyä uusi ketju oikeaksi. Vääriä transaktioita voi syntyä hetkellisesti, mutta tämä näkyy vain hieman viivästyneinä transaktioina, kunnes verkko syrjäyttää väärän ketjun ja lopulta hyväksyy sen aidon ketjun jatkeeksi suuremman laskennallisen vaikeusasteen seurauksena. Louhijat siis ikäänkuin laskevat kilpaa uusia mahdollisia blokkiketjuja ja vaikeusasteeltaan korkeimman uuden ketjun löytäjä palkitaan bitcoineilla. On siis mahdollista löytää uusi blokkiketju joka on melkein oikein, mutta koska sen kelpuuttavat oikeaksi alle puolet koko verkon varmentajista, se hylätään ja vasta riittävän vaikeusasteen saavuttanut ketju voittaa. Tämä järjestelmä on erittäin turvallinen, paitsi tilanteessa jossa yhden osapuolen laskentateho ylittää koko muun verkon laskentatehon. Tällöin olisi mahdollista hyväksyttää verkolla kokonaan uusi, lähes transaktiohistorian alusta uudelleen kirjoitettu historia, jonka vaikeusaste on suurempi kuin yhdenkään toisen ketjun. Tässä tilanteessa oikea transaktiohistoria väistyisi uudelleenkirjoitetun, petollisen historian tieltä.

Yllä mainittu skenaario kumpuaa Mooren laista, joka empiirisesti osoittaa laskentatehon kustannusyksikköä kohden tuplaantuvan n. joka toinen vuosi. Toinen, edellä mainittua skenaariota tukeva tekijä on bitcoinin voimakkaasti deflatorinen luonne. Tarkastellaan ensin laskentatehon kasvua. Oletetaan, että varmennusta suorittavien yksikköjen määrä on melkolailla stabiili. Järjestelmä asettaa blokin laskennan vaikeusasteen keskimääräisen aikavälin pysymään kymmenessä minuutissa. Vaikeusaste on sitenajaneksponenttifunktiomuotoa:

$$(1)\ f(t) = \alpha e^{t/\tau}$$

Tästä seuraa, että blokkiketjun kokonaisvaikeusaste on valittuna ajankohtana likimääräisesti integraalifunktio:

$$(2)\ F(t) = \int_{t0}^{t} F(t')dt'\ \alpha f(t)$$

Tästä seuraa, että riippumatta ketjun pituudesta, järjestelmää vastaan hyökkäävän osapuolen pystyessä kokoamaan kaksinkertaisen laskentatehon

koko muun verkon laskentatehoon nähden ja aloittaessa hyökkäyksen ajankohtana $t = t_1$ on kykenevä luomaan haarautumisajankohdasta $t = t_0$ alkavan uuden, kokonaan vaihtoehtoisen blokkiketjun, joka vaikeusasteellaan $F'(t)$ voittaa olemassaolevan aidon ketjun vaikeusasteen $F(t)$ tulevaisuudessa hetkellä $t = t_2$, jossa hyökkäyksen keston pituus on $\Delta t = t_2 - t_1$. Alleviivatakseen uhan todellisuutta, esimerkkinä tarvittavan laskentatehon mittakaavasta voidaan käyttää deepbit-louhintayhteisöä, jossa käyttäjät ovat yhdistäneet voimansa louhimistyön tekemiseen ja jakavat tulokset keskenään. Joidenkin arvioiden mukaan deepbitin osuus oli 40 % koko verkon laskentatehosta keväällä 2012. Kaksinkertaistamalla tämän osuutensa, Mooren lain perusteella se voisi väärentää historian yhdessä vuodessa. Hakkerit ja valtion instituutiot voivat potentiaalisesti olla jo toteuttamassa sitä. (Barber ym. 2012)

Tämän skenaarion taloudellisen toteuttamisen suurena insentiivinä toimii voimakas deflaatio. Vaikka hyökkäyksen täysimittainen toteuttaminen vaatisi suhteellisen pitkän ajanjakson, ei ole mitään syytä olettaa ettei sitä mahdollisesti toteutettaisi. Bitcoinin arvo kasvaa väistämättä ajan myötä, ceterisparibus, joten myös varkaus käy entistä houkuttelevammaksi. Koska rahan luomisesta saatava palkinto vähenee ajan myötä ja se vaatii entistä suurempaa laskennallista energiaa, insentiivi osallistua louhimiseen ja siten verkon kyky pitää vaikeustaso tarpeeksi korkeana, vähenee ajan myötä. Toisin sanoen, vaikka vielä jonkin aikaa tulevaisuudessa blokin luomisen vaikeusaste jatkaa kasvuaan, pitkällä tähtäimellä se itseasiassa laskee. Täten historian väärentäminen muuttuisi vain helpommaksi ajan myötä. Barber käsittelee julkaisussaan erilaisia mahdollisuuksia kolikon kaksinkertaiseen kulutukseen (double-spending) ja arvioi hyökkääjän siitä saamaa rahallista hyötyä, perustuen järjestelmän senhetkiseen tilaan. (Barber ym. 2012)

On tärkeää huomioida, että motivaatio edellä kuvatun hyökkäyksen toteuttamiseksi ei välttämättä ole taloudellisen hyödyn tavoittelu. Se voi yhtä hyvin olla järjestelmän tuhoaminen esimerkiksi terrorismin muodossa. Tilanteessa, jossa tällainen tuhoamisyritys toteutuisi, hyökkääjän voisi olla mahdollista esimerkiksi estää kaikkien uusien transaktioiden aikaleima. Tämä johtaisi nopeasti tilaan, jossa käyttäjät eivät ole enää varmoja transaktion toteutumisesta, jolloin luottamus romahtaisi nopeasti devalvoiden koko valuutan.(Becker, Breuker, Heide, Holler, Rauer& Boehme 2012)

3.2.7 Energiankulutusjahiilijalanjälki

Eräs toinen potentiaalisesti ongelmallisena nähtävä ominaisuus Bitcoinissa on sen ympäristövaikutus. Sähkökustannusten muodostaessa suurimman osan järjestelmän laskentatehon vaatimista kokonaiskustannuksista, sen toiminta kuluttaa huomattavan määrän energiaa. Tällöin se saattaisi olla vastuussa merkittävän suurista hiilidioksidipäästöistä ja edistää ilmaston lämpenemistä (Beckerym. 2012)

Vuonna 2012 Münsterin yliopiston informaatiojärjestelmien laitos Saksassa julkaisi artikkelin *CanWeAffordIntegritybyProof-of-Work? ScenariosInspiredby the BitcoinCurrency*. Siinä suoritettiin vertailu nykyisen käytössä olevan, keskusvaltaisen sähköisten maksujen varmennusjärjestelmän ja Bitcoinin kaltaisen PoW-pohjaisen järjestelmän kustannuksista. Kyseisen tutkimuksen tavoitteena oli tarkastella Bitcoinin puolestapuhujien väitettä, että keskusvallasta vapaa valuuttajärjestelmä aiheuttaa yhteiskunnalle pienemmät transaktiokustannukset kuin käytössä oleva instituutioiden valtaan perustuva järjestelmä. Tämä oli yhteydessä yleisempään kysymykseen siitä, onko yhteiskunnalla varaa käyttää Bitcoinin kaltaisen järjestelmän varmennusmekanismia vahvistaakseen ja ylläpitääkseen eheyttä ja luotettavuutta hajautetussa järjestelmässä. Vastaus kysymykseen on pitkälti riippuvainen tulevaisuuden informaatiojärjestelmien infrastruktuurista ja niiden hallinnasta.(Becker ym. 2012)

Tutkimuksessa laskettiin varovainen kustannusarvio sekä talouden että ympäristön kannalta. Nimellisarvoisina tulokset viittasivat siihen, että nykyisellään käytössä olevan järjestelmän hintainen Proof-of-workiin perustuva vaihtoehto kestäisi helposti supertietokoneen hyökkäyksen ja todennäköisesti kykenisi puolustautumaan bottiverkkoja vastaan, mutta sen ympäristövaikutus ja hiilijalanjälki olisivat käytännössä samaa luokkaa kuin koko maailman kaupallinen lentoliikenne yhteensä. (Becker ym. 2012)

Tutkimuksen yhteenvetona todettiin, että vaikkei analyysi suoraan hylkää bitcoinin kaltaiseen varmennukseen perustuvaa verkkoa, virhemarginaalit huomioon ottaen ei voida pitää lainkaan varmana että se on kustannustensa arvoinen. Se ei kuitenkaan tarkoita että keksintö olisi turha; Tulevaisuuden teknologiset innovaatiot voivat muuttaa kustannus-hyöty-suhdetta täysin uudella tavalla ja mahdollisesti PoW-järjestelmän hyväksi. Louhinnan

energiatehokkuuden voidaan perustellusti olettaa paranevan tulevaisuudessa (Courtois, Grajek, Naik 2013). Algoritmipohjaisen varmennustyön sivutuotteiden hyödyntäminen voisi myös olla mahdollista; kyseinen laskentatyö voitaisiin hyödyntää jonkun muun ongelman ratkaisuun bitcoininhash-funktion sijasta.Tutkimuksessa todetaankin verkon laskentatyön nykyisessä tarkoituksessaan olevan resurssien tuhlausta. Pitkällä tähtäimellä bitcoinin kaltaisen verkon ylläpito ei yksinkertaisesti olisi tämän teorian mukaan kannattavaa. Luetellun kaltaiset päätelmät tukevat teoriaa, että bitcoin nykymuodossaan on vain väliaikainen ja ilman merkittäviä parannuksia sen protokollassa tai sitä hyödyntävässä teknologiassa, se tulee tiensä päähän ennenaikaisesti. (Becker ym. 2012)

Avoin tutkimuksen kohde onkin, mihin bitcoinin toimintamallin kaltaista teknologiaa voitaisiin hyödyntää muodossa, jossa hajautettu verkko ratkaisee algoritmin ja ratkaisu olisi helposti varmennettavissa. Kuka tahansa joka haluaisi ongelmansa ratkaistavan, voisi muodostaa siitä PoW-mallisen funktion ja palkita ratkaisijan laskentatyöstä, rahoittaen verkon toimintaa tällä tavalla. Tällainen toimintamalli voisi merkittävästi vähentää verkkoon liittyviä kustannuksia ja haastaa edellä käsitellyn tutkimustuloksen verkon huonosta kannattavuudesta pitkällä tähtäimellä (Beckerym.2012).

Samassa tutkimuksessa on hahmoteltu vielä yksi mielenkiintoinen skenaario, jossa verkon kannattavuus voisi nousta riittävälle tasolle. Verkon tuottama hukkalämpö voitaisiin käyttää uudestaan talojen lämmittämiseen. Tietokoneen laskentatyö muuttaa nimittäin sähkön lämmöksi suhteellisen energiatehokkaalla tavalla. Koska verkon hajanaisuus on yksi tärkeimpiä periaatteita, pienen mittakaavan paikallinen yhteistuotanto voisi olla mahdollinen toteutustapa lämmön keräämiseksi ja jakelemiseksi.

3.2.8 Anonymiteettijarahanpesu

Bitcoinista puhuttaessa siihen liitetään usein anonymiteetti tai sitä luonnehditaan elektroniseksi käteiseksi. Jälkimmäinen termi onkin suhteellisen osuva sen pieniin maksusuorituksiin soveltuvan luonteen vuoksi ja myös aiemmin mainittu pätee, tosin tietyin varauksin. Siksi bitcoinia lieneekin parempi luonnehtia termillä pseudonyymi. Julkisen transaktiohistorian takia kaikki tapahtunut liikenne on kenen tahansa saatavilla olevaa tietoa ja jos yksittäiseen transaktioon pystytään yhdistämään henkilöllisyys, ei varsinaista

anonymiteettiä ole. Onkin hyvä tuoda esille tekninen tosiasia, että bitcoinilla on mahdollista saavuttaa melko vahva anonymiteetti ja tehdä transaktion alkuperän takana olevan henkilöllisyyden selvittäminen käytännössä mahdottomaksi, mutta se ei suinkaan automaattisesti toimi niin vaan edellyttää käyttäjältään tiettyjä toimenpiteitä.

Kuten aiemmin todettua, jokainen transaktio ja siten rahayksikkö sisältää koko tapahtumahistorian. Bitcoinin teknisemmän käyttäjäkunnan sisällä vallitsee ymmärrys siitä, ettei anonymiteetti ole järjestelmän merkittävin tavoite. Joka tapauksessa mielipiteet anonymiteetistä ja sen tasosta käytännössä vaihtelevat käyttäjäpiireissä. Jeff Garzik, Bitcoinin kehittäjätiimin jäsen, sanoo seuraavaa:

> "*Ei olisi viisasta yrittää suurta laitonta transaktiota Bitcoinin avulla, ottaen huomioon olemassaolevat tilastollisen analyysin menetelmät jotka lainvalvojilla on käytössään*." (Reid, Harrigan 2011)

Tällä hän tarkoittanee sitä, että yhden transaktion alkuperän selvitettyään hyökkääjä voi saada selville kaikki kyseisen tahon transaktiot. Tästä syystä tilanteissa, joissa käyttäjä haluaa pysyä tuntemattomana, tulisi käyttää muista transaktioista erillistä, yhtä tai useampaa bitcoin-lompakkoa. Tällöin aiempia transaktioita on lähtökohtaisesti lähes mahdotonta yhdistää kyseiseen suoritukseen.

3.2.9 Rahanpesu

Rahanpesu on prosessi, jossa laittomalla toiminnalla tai kaupankäynnillä saavutetut rahalliset hyödyt saadaan näyttämään lainmukaisilta. Rikolliset tahot toteuttavat rahan pesun tyypillisesti kolmivaiheisesti. Ensimmäisessä vaiheessa "likainen" raha tuodaan systeemiin ulkopuolelta (tyypillisesti käteisenä). Toisessa, ns. kerrostusvaiheessa rahan pesijät siirtelevät tai muuntavat rahan muotoa hämmentääkseen sen yhteyttä alkuperäiseen laittomaan lähteeseen. Kolmas vaihe on ns. integrointi, jossa puhdistetut rahat palautetaan systeemiin näennäisesti laillisesta lähteestä. Arviot pestyn rahan osuudesta globaalissa taloudessa vaihtelevat, mutta YK:n huume- ja rikosyksikön vuoden 2009 raportin mukaan se oli keskimäärin n. 2,7% koko maailman BKT:n arvosta tai 1,6 biljoonaa dollaria (USD).

Kiihtyvästi digitalisoituvassa maailmassa tästä seuraa kysymys: Tekevätkö virtuaalivaluutat rahanpesun määrän arvioimisen ja sitä rajoittavien lakien säätämisen sekä valvonnan viranomaisille tulevaisuudessa vaikeammaksi? (Bryans 2013)

Koska bitcoin-talous on vertaisverkko ilman keskusvaltaa, transaktiot tapahtuvat ilman välikäsiä ja järjestelmä on käytännössä immuuni palvelintakavarikolle tai keskeisen tietokannan joutumiselle hakkereiden käsiin. Johtuen rikollisista käyttömahdollisuuksista kuten rahanpesu, bitcoinin pseudonyymi luonne on vaikuttanut negatiivisesti mielikuvaan tulevaisuuden virtuaalisista valuuttajärjestelmistä ja jotkut viranomaiset näkevätkin bitcoinin ainoastaan toimintakenttänä laittomuuksille. On edelleen huomioitava, että vaikka anonymiteetti on mahdollista saavuttaa, bitcoinia ei koskaan suunniteltu sellaiseksi. (Becker ym. 2012; Bryans 2013)

Bitcoin antaa potentiaalisesti mille tahansa laittomalle tai lailliselle käyttäjälle mahdollisuuden siirrellä rahaa lähes välittömästi hyvin pienin tai olemattomin kustannuksin jättämättä jälkiä joiden perusteella alkuperää voitaisiin selvittää. Toisin sanoen, se tarjoaa erinomaisen alustan rahanpesulle. Koska bitcoin on suhteellisen helppo vaihtaa toiseen valuuttaan tai tavaroihin ja käyttää samalla loputtoman monia eri osoitteita alkuperän hämäämiseksi, se itsessään ja samaan teknologiaan perustuvat vaihdon välineet voivat mahdollistaa rahan pesijöille varojen siirtelyn nopeammin, halvemmin ja huomaamattomammin kuin koskaan aikaisemmin. Ilman mahdollisuutta yhdistää käyttäjän henkilöllisyys yksittäiseen bitcoin-osoitteeseen, systeemiin rahaa työntäneen osapuolen jäljittäminen ja sen jälkeen tapahtuneiden siirtojen seuraaminen sekä takaisin reaalitalouteen siirretyn pestyn rahan alkuperän selvittäminen olisi erittäin hankala tehtävä viranomaisille. Myös koko verkon sulkeminen on käytännön mahdottomuus, sillä se vaatisi kaikkien louhintatyötä tekevien koneiden toiminnan estämistä. (Bryans 2013)

3.3 Mediahuomio ja poliittinen asema

Bitcoin on mahdollistanut monia ilmiöitä suhteellisen anonyyminä ja suoraan osapuolelta toiselle siirtyvänä maksuna ilman kolmannen osapuolen

väliintuloa. Osa näistä ilmiöistä on hyviä ja suotavia, toiset taas enemmän tai vähemmän kyseenalaisia. Esimerkkinä yksi merkittävimmistä nykyhetken ilmiöistä, jonka jatkuvuuden Bitcoin on mahdollistanut (USAn hallituksen jäädytettyä sen lahjoitus- ja rahavirrat) on WikiLeaks. Otsikoihin ovat nousseet myös anonyymit markkinapaikat, joissa toiminta perustuu Bitcoinien käyttöön maksuvälineenä. Kaupankäynnin kohteina ovat olleet niin laittomat kuin lailliset palvelut ja hyödykkeet, kuten useissa maissa laittomiksi luokitellut päihteet. Kuuluisimpana esimerkkinä uutisaiheeksi noussut anonyymi markkinapaikka Silk Road, jossa kaikki kaupankäynti tapahtui Bitcoineilla sen mahdollistaman anonymiteetin takia.

On kuitenkin huomioitava, että vaikka mahdollisesti suuri osa Bitcoinilla käytävästä kaupasta liittyisi maksuvälineenä käytön sijaan esimerkiksi spekulatiiviseen sijoittamiseen tai laittomiin hyödykkeisiin, sillä on paljon laillisia käyttäjiä, joiden tarkoitusperät ovat kulttuurisia tai sosiaalisia (Jeong 2013). Tällä tarkoitetaan esimerkiksi sitä, että bitcoin on perinteistä tilisiirtoa halvempi ja nopeampi tapa lähettää maksu toisessa maassa sijaitsevalle henkilölle. Joillekin virtuaalirahan käyttö voi olla myös kannanotto; viimeaikaiset tapahtumat pankki- ja rahoitusalalla ovat mahdollisesti heikentäneet instituutioiden nauttimaa luottamusta suuren yleisön silmissä.

Bitcoinin uskottavuus sai runsaasti nostetta joulukuussa 2013, kun tunnettu amerikkalaispankki JP Morgan uutisoi patentoineensa bitcoinin kaltaisen teknologian (BBC 2013), jonka avulla sähköisten maksujärjestelmien operointi voidaan tulevaisuudessa toteuttaa. Myös suomalainen tietoturva-asiantuntija Mikko Hyppönen sanoo Youtubeen 13.11.2013 ladatussa haastattelussa, että uskoo kryptovaluuttojen toimintaperiaatteiden muuttavan maailmaa ja sähköisiä maksujärjestelmiä, vaikka se ei välttämättä olisikaan bitcoin. (Hyppönen 2013)

Hurjimmissa spekulaatioissa bitcoinille on povattu jopa arvonnousun jatkumista peräti satakertaiseksi nykyisestä, n. 1000 dollarista. Kalifornian Silicon Valleyssa operoiva riskipääomasijoittaja Chris Dixon on yksi tälläisen näkemyksen kannattajista. Ohjelmointitaustainen sijoittaja vertaa bitcoinia verkko-osoitteiden nimiin. Hän toteaa, että 90-luvun alussa olisi ollut täysin yleisen uskomuksen vastaista väittää, että 2010-luvulla yksittäisen verkko-osoitteen nimen hinta voisi olla miljoonia dollareita. (wired 2013)

Arvostettu ekonomisti Paul Krugman kirjoittaa New York Timesin verkkosivustolla sijaitsevassa blogissaanbitcoinista kriittiseen sävyyn. Hän kritisoi 28.12.2013 julkaistussa kolumnissaan virtuaalivaluuttaa siitä, ettei sillä ole edellytyksiä olla tarpeeksi stabiili arvonsäilyttäjä. Se onkin yksi isoimmista argumenteista sen puolesta, että bitcoin ei voi olla olemassa ilman muita valuuttoja joilla sen arvo mitataan. Krugman haluaakin erottaa toisistaan kaksi kysymystä. Ensin sen, onko bitcoin pelkkä kupla, sekä erikseen kysymyksen siitä, onko se hyvä vai huono asia. (Krugman 2013)

USAn hallitus järjesti virtuaalivaluutoista istunnon 18.11.2013, jossa maan sisäisestä turvallisuudesta ja valtion suhteista vastaava neuvosto (Committee on Homeland Security and GovernmentalAffairs) käsitteli aihetta. Neuvoston puheenjohtaja Tom Carper vertasi Bitcoinin nykyhetkeä internetin alkuaikoihin, johon yhtyi myös valtiovarainministeriön talousrikoksista vastaavan yksikön (FINCEN) johtaja Jennifer ShaskyCalvery, sanoen seuraavaa:

> "*Usein finanssiteollisuudessa uuden rahoituspalvelun tai pelaajan astuessa esiin, rahanpesusta tai terrorismin rahoittamisesta huolestuneiden ensimmäinen reaktio kohdistuu mukana tuleviin haavoittuvuuksiin tai aukkoihin joita uusi järjestelmä mahdollistaa. On kuitenkin tärkeää pitää mielessä, että innovaatio on tärkeä osa talouttamme*."

Tämä viittaakin bitcoinin (tai vastaavaan teknologiaan perustuvan järjestelmän) tulevaisuuden kannalta mahdollisesti hyvään kehityssuuntaan, jossa sitä ei hallituksen ja sitä kautta suuren yleisön silmissä pidetä ainoastaan rikollisia toimintoja mahdollistavana työkaluna, vaan potentiaalisesti merkittävänä innovaationa tulevaisuuden finanssiteollisuudessa.

Vaikka luomisprosessiltaan ja inflaatioherkkyydeltäänbitcoin eroaafiat-valuutoista perustavanlaatuisesti, niitä molempia yhdistää ja käyttäjien luottamus rahan arvoon. Täysin virtuaalisen olemuksensa vuoksi arvostettu amerikkalainen ekonomisti Paul Krugman luonnehtiikin bitcoiniablogissaanultimaattiseksifiat-valuutaksi, jonka arvo loihditaan täysin tyhjästä(Krugman 2013). Toisin kuin paperisilla seteleillä tai kultakolikolla, biteistä koostuvalla rahayksiköllä ei ole minkäänlaista käyttöarvoa jos se ei kelpaa maksun suorittamiseen.

3.3.1 Poliittinenasema

Nakamoton ja muiden projektia kehittäneideninsentiivit keskusvaltaisista instituutioista vapaan rahatalouden toteuttamiseen saattavat olla virallisessa julkaisussa ilmoitettua laajemmat ja suurena motiivina on mahdollisesti toiminut rajoituksista ja valvonnasta irtautuminen. Syntyhistorian ymmärtämistä edesauttaakseen SarahJeong tarkasteliartikkelissaan Cypherpunks-verkkoyhteisön postituslistaa. Sähköinen postituslista oli aktiivisimmillaan vuosina 1992-2001 ja se koostui lähinnä hakkereista, kryptograafikoista ja yksityisyyden suojan parantamiselle omistautuneista internetin käyttäjistä. Myös WikiLeaksin myötä tunnetuksi tullut Julian Assange oli kyseisellä listalla. (Grinberg 2011)

Cypherpunks-yhteisö otti käyttöönsä kryptografianja ryhtyi kehittämään sitä omiin tarpeisiinsa. Siihen asti kyseinen teknologia oli ollut vain valtiollisten instituutioiden käytössä poliittisten salaisuuksien suojaksi(Jeong 2013). Cypherpunks-jäsenillä ei ollut yhteisesti määriteltyä poliittista agendaa, mutta sen voidaan katsoa edesauttaneen internet-anarkististen aatteiden leviämistä suuremman yleisön tietoon.Bitcoinia ei siis voi varauksettomasti luonnehtia vain loistavaksi teknologiseksi innovaatioksi, koska sen kehitykseen ja kannattajakuntaan liittyy paljon ideologiaa keskusvaltaisista instituutioista irtautumiseksi. Vaikka bitcoinin luojat pyrkivät julkaisussaan omaksumaan poliittisesti varauksettoman linjan, on se silti alusta asti poliittinen projekti ja kehittyvä sellainen, sisältäen visiota, tavoitteita ja varauksia. (Jeong 2013)

Mahdollisesta poliittisesti varautuneesta luonteestaan huolimattabitcoin tosiasiallisesti tarjoaa vaihtoehdon, jossa kryptografiseen varmentamiseen perustuva järjestelmäkorvaa keskusvaltaisenkolmannen osapuolen mukanaolon ja tekee siitäteknisen toimivuuden kannalta tarpeetonta. Maksut, joiden peruminen on käytännön mahdottomuus, suojaavat myyjiä petoksilta. Toisaalta ostajan kannalta tilanne on osittain päinvastainen: kerran tehtyä bitcoin-maksusuoritusta ei voi peruuttaa.Sama pätee kuitenkin myös käteiseen rahan ojentamiseen toiselle ihmiselle, eikä sitä nähdä yleisesti ongelmallisena.

4 TUTKIMUSAINEISTO JA MENETELMÄT

Regressioanalyysin tarkoituksena on tutkia, onko bitcoinin medianäkyvyydellä tilastollisesti selittävää vaikutusta valuutan hintaindeksin kehitykseen. Hintaindeksin rajut vaihtelut sekä räjähdysmäinen piikki syystalvella 2013 viittaavat jonkinlaiseen kuplaan sekä ”hypeen”, joka bitcoinin ympärille muodostui tai osittain jopa tarkoituksella luotiin. Analyysia ennen on tehty johtopäätös, että suurempi medianäkyvyys bitcoinin kaltaisen, suurelle yleisölle uuden ja tuntemattoman ilmiön kohdalla johtaa kasvaneisiin google-hakuihin kyseistä aihetta parhaiten kuvaavalla hakusanalla.

4.1 Aineisto

Bitcoinin hintaindeksi on haettu päivädatana osoitteesta www.coindesk.com ja muutettu sitten viikkohavainnoiksi laskemalla keskiarvo jokaista seitsemää päivää kohden. Medianäkyvyyttä kuvaa Googlen Trends-ominaisuuden avulla ladattu data. Se kertoo tietyn hakusanan (tässä tapauksessa ”bitcoin”) viikottaisen suhteellisen suosion valitulla aikavälillä. Kun hakumäärä on ollut alimmillaan, arvo on 0 ja hakumäärien ollessa ylimmillään se saa arvon 100. Toisena selittävänä muuttujana on otettu mukaan USAn osakekurssien kehitys tarkasteltavalta aikaväliltä. Kurssien kehitystä kuvaamaan on ladattu Standard &Poor’s 500-indeksi viikkottaisina havaintoina St. Louisin keskuspankin sivuilta osoitteessa www.stlouisfed.org. Muuttuja on sisällytetty analyysiin, koska bitcoinin olemassaolon ensimmäisten vuosien räjähtävä arvonnousu on väistämättä kasvattanut sen kiinnostavuutta sijoituskohteena, eikä niinkään sen alkuperäisen funktion mukaisesti maksuvälineenä. S&P 500 antaa informaatiota siitä, seuraileeko bitcoinin hintaindeksin kehitys osakemarkkinoiden yleistä kehitystä, vai ovatko ne sijoitushyödykkeinä ajateltuna toimineet mahdollisesti toistensa substituutteina. Hintaindeksin ja sitä selittävien muuttujien välisen suhteen tutkimiseksi on suoritettu lineaarisia regressioita pienimmän neliösumman (PNS) menetelmää hyväksikäyttäen (Wooldridge 2006). Regressioanalyysissä on käytetty myös Newey-West-estimaattoria mallin estimaattien t-arvojen luotettavuuden varmistamiseksi. Menetelmä poistaa autokorrelaation sekäheteroskedastisuudenvaikutuksen. Newey-West -estimaattorin keskivirheiden laskeminen perustuu ennalta määriteltyyn viiveen(eng. ”*lag*”) maksimiarvoon. Ne lasketaan OLS-residuaalien hajautetuilla

viiveillä ja testiä tehdessä on määriteltävä viiveen maksimiarvo. (Newey& West 1987) Tässä tutkimuksessa tehtyjen Newey-West–estimaattorin avulla toteutettujen regressioanalyysien viiveen maksimiarvo on 5, joka tarkoittaa että autokovarianssien laskeminen tapahtuu maksimissaan viiden aikaperiodin viiveellä.

Kuviossa 6 on esitelty google-hakujen ja bitcoinin hintaindeksin keskenään samankaltaista kehitystä tarkasteluajanjaksolla. Google-haut saavat suhdeluvun välillä 0-100 ja hintaindeksi puolestaan absoluuttisen arvonsa kerrottuna sadalla.

Kuvio 6. Google-Trends hakusanalla ”bitcoin” sekä bitcoinin arvon kehitys (USD x 100) tarkasteluajanjaksolla.

4.2 Menetelmät

Ennen analyysin tekemistä muuttujista on otettu arvot niiden luonnollisina logaritmeina eli Neperin luvun eksponentteina. Luvulle 0 ei voida määritellä luonnollista logaritmia, joka aiheuttaa ongelman regressioanalyysin tekemisessä Stata-ohjelmistolla. Koska Trends-muuttujan 261 havainnon aikasarjan alkupäässä on 30 havaintoa arvolla 0, on logaritmisen transformaation mahdollistamiseksi muutettu ne arvoiksi 1. Aineistoa

tarkastellessa voitiin päätellä, ettei tällä muutoksella ole merkittävää vaikutusta analyysin tulosten kannalta. Havaintojen saattaminen logaritmiseen muotoon on tehty, jotta mallin tulkinta helpottuisi. Logaritmimuoto myös stabiloi muuttujien välisiä variansseja.Voidaan sanoa, että regressioyhtälö on muotoa:

$$(3)\ \ln y = \beta_0 + \beta_1 \ln x + \text{□}$$

jossa y on selitettävä muuttuja, $\beta_0$vakiotermi, β_1 selittävän muuttujan kerroin, x selittävä muuttuja, μ virhetermi ja ln luonnollinen logaritmi. Tästä seuraa, että voidaan päätellä 1 % muutoksen x:ssä viittaavan likimain β_1:n arvoa vastaavan suruiseen muutokseen Y:ssä. (Wooldridge 2006) Tarkasti määriteltynä Y muuttuu prosentuaalisen määrän:

$$(4)\ \Delta Y = 1 - (e^{\beta_1 \times \log(1.01)})$$

Logaritminen transformaatio on yleisesti käytetty menetelmä tilanteissa, joissa riippuvien ja riippumattomien muuttujien välillä vallitsee epälineaarinen suhde. Muuttujien logaritmisten muotojen käyttäminen alkuperäisten sijaan tarkoittaa, että niiden välinen suhde on epälineaarinen, mutta itse mallin lineaarisuus säilyy (Benoit 2011).

Regressioanalyysi on suoritettu myös muuttujien differensseillä. Tämä menetelmä on selitetty tarkemmin sille varatussa osiossa luvussa 5. Aineisto on myös empiirisen analyysin viimeisessä osassa jaettu kahtia siten, että havainnot ennen vuotta 2013 muodostavat oman regressionsa ja havainnot vuoden 2012 jälkeen omansa. Tällä on tarkoitus tutkia, onko mediahuomion vaikutus hintaan mahdollisesti voimistunut viime vuosina.

Empiiristen tulosten analysoinnissa tulokset on tulkittu suuntaa antaviksi ja siten suurpiirteiset arvot ovat riittäviä johtopäätösten tekemiseksi (kaava 4). Regressioanalyysissä tulkinta annetaan odotettuna muutoksena selitettävässä muuttujassa, kun selittävä muuttuja muuttuu annetun määrän.Muuttujien välisiä suhteita joissa sekä Y (selitettävä) että X (selittävä) ovat logaritmeja, sanotaan ekonometriassa yleensä elastisiksi ja selittävän muuttujan kerrointa elastisuudeksi tai joustoksi. (Benoit 2011)

5 TUTKIMUSTULOKSET

Tähän lukuun on koottu empiirisen osion tulokset taulukoiden ja niiden perusteella tehtyjen analyysien muodossa. Tutkimusajankohtana 1.8.2010 – 2.8.2015 sekä bitcoin että S&P 500 ovat heilahdelleet arvossaan huomattavasti, mikä tekee regressioanalyysista mielenkiintoisen. Lisäksi se saattaa pienentää aikasarjan sisällä esiintyvän autokorrelaation mahdollisuutta myöhempien havaintojen ollessa vähemmän riippuvaisia niitä edeltäneistä havainnoista.

5.1 Google-hautbitcoinin hintaindeksin selittävänä tekijänä

Ensimmäisessä taulukossa regressio on toteutettuNewey-West–estimaattorilla t-arvojen luotettavuuden varmistamiseksi. Selittäviä muuttujia on aluksi vain yksi (Google-haut). Mallin selitysasteen lukema (0,867) on erittäin korkea ja mallia voidaan pitää hyvänä. Sen perusteella voidaan siis sanoa, että lähes 87 % arvon vaihtelusta on selitettävissä mallin avulla. Selittävän muuttujan t-arvon perusteella nollahypoteesi voidaan hylätä ja p-arvo viittaa 1 % merkitsevyystasoon, jonka perusteella testi on tilastollisesti erittäin merkitsevä. Google-hakujen määrää kuvaavan muuttujan lngoogtre kerroin 2,01 on korkea. Sen perusteella voidaan päätellä 1 % suuruisen nousun Google-hakujen määrässä nostavan bitcoinin arvoa 2 %. Tämän perusteella medianäkyvyys on ollut suuressa roolissa arvon kehityksen kannalta ja sen lisääntyminen johtaa suhteellisesti kaksinkertaiseen kasvuun bitcoinin arvossa.

Taulukko 1. $\ln BTCwkly = \beta_0 + \beta_1 (\ln googtre) + \mu$

lnBTCwkly	**Coef.**	**Std. Err.**	**t**	**P>t**
lngoogtre	2,014	0,139	14,54	0,000
C	-0,460	0,291	-1,58	0,115
		Menetelmä:	Newey-West	
R^2(=Korjattuselitysaste)	0,867	Maksimiviive:	5	

Seuraavassa taulukossa sama on toteutettu siten, että selittävän muuttujan arvoa on viivästytetty yhdellä aikaperiodilla. Arvot ovat lähes vastaavat kuin ilman viivästyksen käyttöä. Sama analyysi toteutettiin myös kuukausittaisena jaksotuksena aikasarjan vaihtelun sisäisten painotusten tutkimiseksi. Niiden

perusteella johtopäätösten tekeminen on kuitenkin vaikeaa eivätkä p-arvot ole edes lähellä riittävää tasoa tulosten tilastollisen merkitsevyyden kannalta, joten kuukausivaihtelua kuvaavat taulukot on jätetty tutkielmasta pois.

Taulukko 2. $\ln BTCwkly = \beta_0 + \beta_1 (\ln googtre)_{t-1} + \mu$

Muuttuja	Kerroin	Keskivirhe	t	P>t
L.lngoogtre	1,994	0,049	40,85	0,000
C	-0,391	0,108	-3,61	0,000
R^2	0,866			

5.2 Google-haut ja osakemarkkinat hintaindeksin selittävinä tekijöinä

Seuraavaksi sama analyysi on toteutettu ottamalla mukaan osakekurssien kehitys toisena selittävänä muuttujana. Tätä varten on kerätty aikasarja-aineisto S&P 500–indeksin kehityksestä viikoittaisina havaintoina. Koska Bitcoin on tarkasteltavana ajanjaksona ollut suosittu sijoituskohde, on loogista ajatella sen arvon kehityksen seurailevan yleistä kehitystä osakemarkkinoilla tai vastaavasti toimivan vaihtoehtona perinteisemmille sijoituskohteille.

Taulukossa 3 on tehty kahden riippumattoman muuttujan regressioanalyysi, jossa havaintoaineiston muuttujat lnsp500 (osakekurssit) ja lngoogtre selittävät Bitcoinin hintaindeksiä (lnBTCwkly).Taulukosta ilmenee, että selitysaste onerittäin korkealla tasollaja myös p-arvot ovat erittäin matalia. Sen perusteella voidaan sanoa, että malli vaikuttaa hyvältä ja tilastollinen merkitsevyys on erittäin korkealla tasolla. Muuttujan lngoogtre kerroin 1,24 viittaa jälleen medianäkyvyyden merkittävään rooliin valuutan hintakehityksessä. Kertoimen ollessa arvoltaan enemmän kuin 1, bitcoinin hinnan voidaan päätellä kehittyvän samaan suuntaan hakumäärien kanssa ja niitä suhteellisesti enemmän. Tulos vahvistaa siltä osin tutkielman alkuperäistä oletusta hype-ilmiön olemassaolosta ja sen havaittavasta vaikutuksesta valuutan arvoon. S&P 500–indeksi toisena selittävänä tekijänä on kertoimeltaan 5,81 ja siten vielä huomattavasti Google-hakujen kerrointa korkeampi. Yhden prosentin nousu osakekursseissa näkyy lähes 6 prosentin nousuna virtuaalivaluutan hintaindeksissä. Sen perusteella näyttää siltä, että bitcoin on herkkä yleisten sijoitusmarkkinoiden muutoksille ja vaihtelee samansuuntaisesti niiden kanssa.

Selitysasteen perusteella mallia voidaan pitää hyvänä ja osakekurssien mukaan ottaminen toisena selittävänä tekijänä tekee siitä aiempaa paremman. Google-hakujen kertoimen perusteella medianäkyvyyden vaikutus on edelleen huomattava, mutta selkeästi pienempi, kun se ei ole enää mallin ainoa selittävä muuttuja. Saatujen tulosten perusteella voidaan ajatella, että bitcoin on nähty houkuttelevana sijoituskohteena maailman ja Yhdysvaltojen talouden hyvinä aikoina, jolloin korkean riskin sijoituskohteisiin löytyy enemmän varoja ja kiinnostusta. Tulos myös kumoaa osaltaan ajatuksen siitä, että bitcoin olisi nähty vaihtoehtoisena sijoituskohteena pörssikaupan tarjoamille tuotteille.

Taulukko 3. $\ln BTCwkly = \beta_0 + \beta_1 (\ln googtre) + \beta_2 (\ln sp500) + \mu$

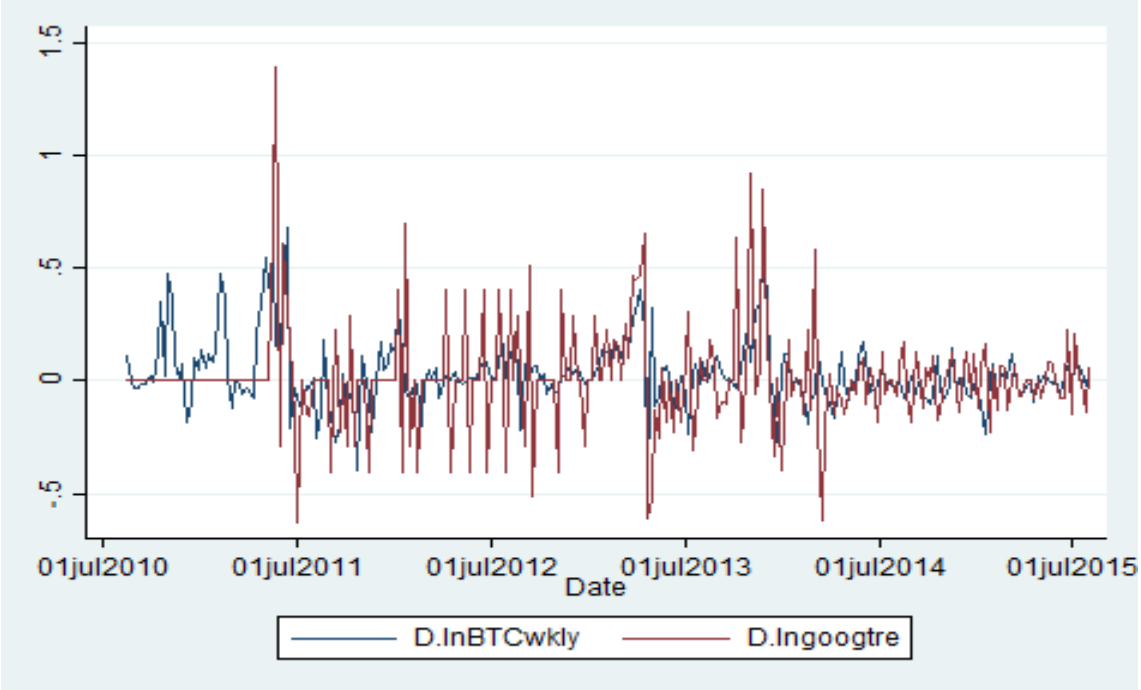
Muuttuja	**Kerroin**	**Keskivirhe**	**t**	**P>t**
lngoogtre	1,249	0,112	11,17	0,000
lnsp500	5,812	0,691	8,41	0,000
C	-41,743	4,988	-8,37	0,000
		Menetelmä:	Newey-West	
R^2	0,938	Maksimiviive:	5	

5.3 Regressio differenssiyhtälön avulla

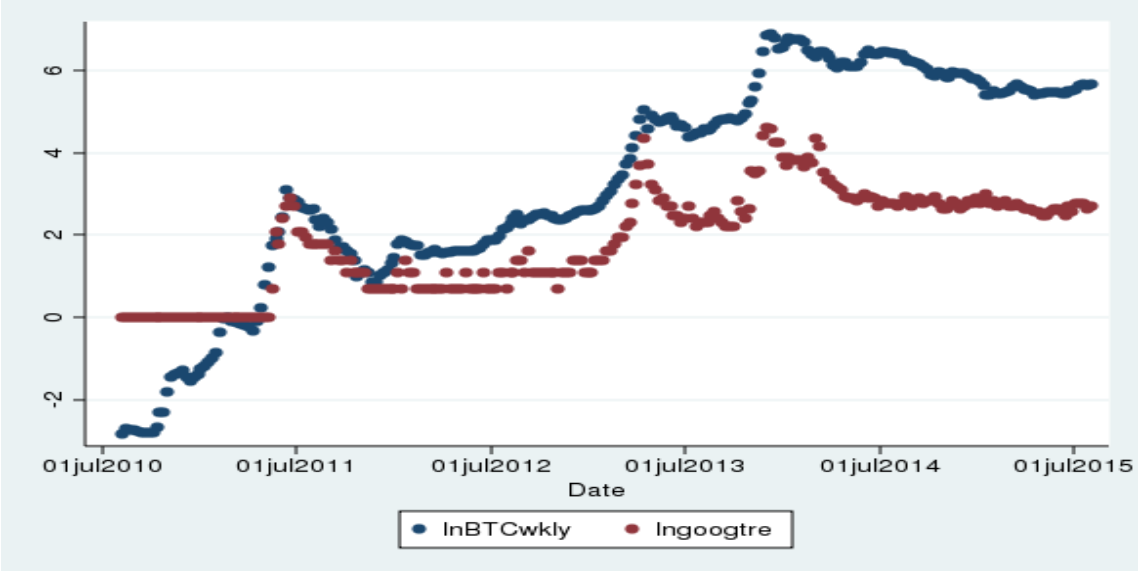
Muuttujien muutosnopeuden tutkimiseen voidaan käyttää differenssifunktiota. Erona tutkielman aiempaan analyysiin on, että jokainen muuttuja on differenssimuodossa. Differenssiyhtälö on siten kunkin muuttujan kohdalla muotoa:

$$(5)\ \Delta y = \ln y\,(t) - \ln y\,(t-1)$$

Tällä menetelmällä toteutettuna on luonnollista, että regressioyhtälön selitysaste on alhainen. Tulokset ovat silti itsessään tutkimisen arvoisia, vaikka malli ei olekaan ennustamisen näkökulmasta paras mahdollinen. Seuraavana esitetyissä kuvissa 7 ja 8 havainnollistetaangoogle-hakujen ja hintaindeksin muutosten toisiaan muistuttavia trendejä. Kuvaajat ovat kahdessa kuvassa; ensin differenssimuotoisina, jota seuraa logaritminen esitysmuoto.



Kuvio 7. Bitcoinin ja Google-Trendsin kehitys differensseinä.



Kuvio 8. Bitcoinin ja Google-Trendsin kehitys logaritmisissa muodoissaan.

Hintaindeksin muutoson taulukossa 5 selitettävä muuttuja ja Google-hakujen sekä osakekurssienmuutokset selittäviä muuttujia. Taulukon kertoimia

tarkasteltaessa nähdään, että ne tukevat aiempia havaintoja samansuuntaisesta muutoksesta muuttujien välillä. Osakekurssien kerroin 1,32 on suurempi kuin 1, joka tarkoittaa suhteellisesti suurempaa muutosnopeutta Bitcoinin hintaindeksiin verrattuna ja Google-hakujen 0,18 puolestaan suhteellisesti heikompaa. Osakekurssien muutos selittää siis bitcoinin arvon muutosta varsin hyvin ja myös google-hakujen muutoksella on bitcoinin muutosta selittävää vaikutusta. Taulukossa 4 regressio on tehty siten, että Google-haut on ainoa selittävä muuttuja. Taulukosta nähdään, että kerroin ei juurikaan muutu.

Taulukko 4. $\Delta lnBTCwkly = \beta_0 + \beta_1 (\Delta lngoogtre) + \mu$

Muuttuja	Kerroin	Keskivirhe	t	P>t
D.lngoogtre	0,181	0,037	4,86	0,000
C	0,031	0,009	3,49	0,001
R^2	0,080			

Taulukko 5. $\Delta lnBTCwkly = \beta_0 + \beta_1 (\Delta lngoogtre) + \beta_2 (\Delta lnsp500) + \mu$

Muuttuja	Kerroin	Keskivirhe	t	P>t
D.lngoogtre	0,187	0,037	5,04	0,000
D.lnsp500	1,327	0,570	2,33	0,021
C	0,027	0,009	3,11	0,002
R^2	0,096			

Taulukossa 6 on puolestaan pyritty tarkastelemaan, kuinka bitcoinin arvon muutos näkyy tehtyjen Google-hakujen määrän muutoksessa. Kertoimen perusteella korrelaatio on positiivinen (0,46). Esimerkiksi 100 prosentin nousu bitcoinin arvossa tarkoittaisi lukeman perusteella 46 prosentin kasvua google-hauissa hakusanalla ”bitcoin”. Nopeasti arvioituna tulos vaikuttaa uskottavalta ja sitä voi pitää vähintään suuntaa antavana.Voidaan päätellä, että ihmisten mielenkiinto aihetta kohtaan ja sitä koskevien hakujen määrä on noussut hintaindeksin mukana enemmän tai vähemmän.

Taulukko 6. Δlngoogtre = $\beta_0 + \beta_1 (\Delta$BTCwkly) + μ

Muuttuja	Kerroin	Keskivirhe	t	P>t
D.lnBTCwkly	0,462	0,095	4,86	0,000
C	-0,005	0,014	-0,32	0,747
R^2	0,080			

Taulukossa 7 selitettäväksi muuttujaksi on otettu S&P 500 –indeksin muutos ja pyritty tutkimaan, kuinka google-hakujen sekä bitcoinin arvon muutokset selittävät osakekurssien kehitystä. Taulukosta nähdään, että kertoimet ovat arvoiltaan pieniä ja google-muuttujant-arvoa ei voida pitää varmuudella luotettavana. Tämä tukee ennakko-oletusta siitä, ettei bitcoinin kaltaisella, makrotaloudellisesti mikroskooppisella ilmiöllä ole juurikaan vaikutusta osakemarkkinoiden kehitykseen. Vaikutus näkyy siten vain osakemarkkinoilta bitcoinin suuntaan, eikä toisinpäin.

Taulukko 7. Δlnsp500 = $\beta_0 + \beta_1 (\Delta$lnBTCwkly) +$\beta_2 (\Delta$lngoogtre) + μ

Muuttuja	Kerroin	Keskivirhe	t	P>t
D.lngoogtre	-0,006	0,004	-1,33	0,186
D.lnBTCwkly	0,016	0,007	2,36	0,019
C	0,005	0,003	1,46	0,145
R^2	0,036			

5.4 Aineiston tarkastelu ennen ja jälkeen vuotta 2013

Tutkimustulosten viimeisenä osiona on regressioanalyysi, mutta tässä tapauksessa aineisto on jaettu kahteen osaan. Koska vuosi 2013 oli bitcoinin arvonnousun, suosion kasvun sekä mediahuomion kannalta merkittävä, on aineistoa tarkasteltu ensin vuoden 2012 loppuun ja sen jälkeen vuodesta 2013 eteenpäin. Ainoana selittävänä muuttujana on google-hakujen määrä viivästettynä yhdellä aikaperiodilla. Tällä on tarkoitus tutkia, onko

mediahuomiolla ollut suhteellisesti suurempi vai pienempi vaikutus bitcoinin arvoon ennen vuoden 2013 tapahtumia. Kyseisenä vuonna bitcoinia ostettiin jopa lähes 1400 USAn dollarin hintaan ja yhtä korkeaa lukemaa ei ole nähty sen jälkeen. Lisäksi vuonna 2013 suosittuja bitcoineja välittäviä kauppapaikkoja lopetti toimintansa ja osa niistä enemmän tai vähemmän epäselvissä olosuhteissa. Esimerkkinä tästä voidaan mainita vaihdon määrällä mitattuna tuolloin selvästi suosituin, Japanista toimintaansa harjoittanut Mt. Gox. Kaiken tämän perusteella on siis hyvin mahdollista, että mediahuomion vaikutus arvoon on ollut suhteellisesti korkeampaa vuoden 2012 jälkeen.

Taulukossa 8 havainnot ovat elokuulta 2010 aina joulukuulle 2012. Kerroin 2,11 on vain hieman korkeampi, kuin aiemmin tutkielmassa koko aineistolla toteutetun, vastaavan regression tapauksessa. Tulos on myös tilastollisesti erittäin merkitsevä. Taulukossa 9 aineisto sisältää havainnot vuoden 2013 alusta aina elokuuhun 2015 asti. Nyt kerroin on 1,22 eli huomattavasti pienempi. Tulosten perusteella mediahuomion vaikutus hintaan on vastoin ennakko-oletusta pienentynyt vuoden 2012 jälkeen. Selitysasteiden perusteella mallit ovat hyviä, sillä ne ovat molemmissa tapauksissa yli 60 %. Kertoimen pienentymistä voi selittää se, että suurin hype ja spekulaatio ilmiön ympärillä on rauhoittunut sitten vuoden 2013. Asia voidaan päätellä arvon kehityksestä kuvassa 6. Käyrä on ollut piikin saavutettuaan tasaisesti laskeva ja vasta vuoden 2015 aikana indeksi on pysynyt tasaisempana. Tällöinkin bitcoin on sekä valuuttana että sijoituskohteena melko volatiilinen.

Taulukko 8: $\ln BTCwkly = \beta_0 + \beta_1 (\ln googtre)_{t-1} + \mu$, havainnot ennen vuotta 2013.

Muuttuja	**Kerroin**	**Keskivirhe**	**t**	**P>t**
L.lngoogtre	2,111	0,144	14,71	0,000
C	-0,625	0,307	-2,04	0,004
R^2	0,676			

Taulukko 9: $\ln BTCwkly = \beta_0 + \beta_1 (lngoogtre)_{t-1} + \mu$, havainnot vuoden 2012 jälkeen.

Muuttuja	**Coef.**	**Std. Err.**	**t**	**P>t**
L.lngoogtre	1,222	0,090	13,57	0,000
C	1,767	0,295	5,98	0,004
R^2	0,609			

6 JOHTOPÄÄTÖKSET

Tähän lukuun on koottu tärkeimmät johtopäätökset, joita tutkielman perusteella voidaan tehdä. On huomioitava, että muutokset lainsäädännössä ympäri maailman sekä esimerkiksi uudet teknologiset innovaatiot voivat muuttaabitcoinintoimintaympäristöä dramaattisesti hyvin lyhyenkin ajan sisällä ja siten vaikuttaa tehtyihin johtopäätöksiin myös niitä kumoavalla tavalla. Lisäksi niihin liittyy paljon spekulaatiota, jonka vain aika todistaa oikeaksi tai vääräksi.

Puhuttaessa bitcoinin potentiaalista korvata tulevaisuudessa koko elektroninen maksujärjestelmä ja vapauttaa se keskusvallasta, on todettava, ettei kyseiselle väitteelle löydy nykyisissä olosuhteissa lainkaan perusteita. Lähtökohtaisesti suurimpana ongelmana voidaan pitää raha -ja finanssipolitiikan estyneisyyttä ja sitä kautta kansantalouden häiriöiden korjaamisen mahdottomuutta. Toisena suurena ongelmana on hiilijalanjälki järjestelmän kasvaessa. Tämä voi tosin olla korjattavissa paremmalla teknologialla, mutta lähtökohtaisesti sen ylläpitoon tarvittavan energian määrä tekee siitä mahdottomuuden.

Vaikka bitcoin-järjestelmä ei voisikaan olla nykyisen elektronisen maksujärjestelmän korvaaja, on täysin mahdollista ja jopa oletettavissa, että se tai uusi ja samankaltaiseen,blokkiketjun teknologiaan perustuva järjestelmä tulee globaaliin talouteen pysyväksi elementiksi. Siinäkin tapauksessa, että bitcoin kaatuisi tutkielmassa esitettyihin uhkakuviin energiatehokkuudesta tai järjestelmän kaappamisesta väärennetyllä historialla, tekninen toimintaperiaate todennäköisesti tuotaisiin uutena ja parempana käyttöön ennemmin tai myöhemmin.

Ongelmallisessa valossa useissa julkaisuissa esitetty deflatorinen luonne ei loppujen lopuksi vaikuta niin tuhoisalta ongelmalta kuin on annettu ymmärtää; koska yksi bitcoin on jaettavissa loputtoman pieniin osiin, valuutan arvo voi teoriassa jatkaa kasvuaan loputtomiin talouden kasvaessa ja rahayksikköjä riittää jatkossakin kaikkien käyttöön. Suurempi ongelma, jonka deflaatio tuo mukanaan on käyttäjien spekulatiivinen käytös, joka heiluttelee arvoa ja vähentääinsentiiviä käyttää bitcoinia maksuvälineenä.

Toinen arvoa heilutteleva tekijä on lainsäädäntö ja sen avulla toteutetut paikalliset rajoitukset, joilla ei kuitenkaan ole saatu aikaan pysyviä muutoksia

suosioon tai kurssikehitykseen. Siksi lainsäädäntöä on vaikea nähdä pitkällä tähtäimellä bitcoinia rajoittavana tekijänä. Internetin aikakaudella rajoitusten kiertämiseen löytyy lähes aina uusi tapa tai teknologia. Asia voidaan itseasiassa nähdä toisinpäin, sillä nykyistä sallivampi lainsäädäntö voi teoriassa edesauttaa järjestelmän kehittymistä paremmaksi tai vastaavasti nopeuttaa sen yhtenä uhkakuvana esitettyäennenaikaista tuhoa.

Bitcoinin tulevaisuus riippuu myös oleellisesti siitä, löytyykö todellista maksukäyttöä tarpeeksi, eikä kysyntä ole vain seurausta spekulatiivisesta sijoittamisesta. Käyttöä ja kysyntää sille varmasti riittää ainakin lähitulevaisuudessa, mutta Fiat-valuuttojen korvaajaksi bitcoinista ei nykymuodossaan ole. Toimintaperiaatteen suurin taloudellinen potentiaali lieneekin elektronisissa maksujärjestelmissä ja niiden teknologian muuttamisessa nykyistä paremmaksi.

Empiiriset tutkimukset tukivat oletusta siitä, että bitcoinin arvo on kehittynyt samansuuntaisesti osakemarkkinoiden kehityksen kanssa. Kun sijoitusmarkkinoilla tilanne on suotuisa, se näkyy myös bitcoinin arvossa. Vaikka pahimmat romahdukset hintaindeksissä ovat olleet suoraan seurausta järjestelmän sisäisistä ongelmista ja instituutioiden pettämisestä (valuutanvaihtopaikkojen kokemat palvelunestohyökkäykset ja konkurssit ym.), voidaan todeta osakemarkkinoiden kehityksen selittäneen tarkasteltavalla aikavälillä bitcoinin hintaindeksin kehitystä merkittävästi. Vastaavalla tavalla medianäkyvyyden vaikutus hintaindeksiin on aineiston tarkastelun perusteella selkeästi havaittavissa, vaikkei läheskään yhtä voimakkaasti.

Tutkielman alussa listatut hypoteesit olivat:

H1: Bitcoin ei ole vain ohimenevä ilmiö, vaan virtuaalivaluutat muodossa tai toisessa ovat tulleet jäädäkseen.

H2: Bitcoinin saama mediahuomio on nostanut sen arvoa ja ollut osaltaan luomassa hintakuplaa.

H3: Bitcoin on korkean riskin sijoituskohde ja sen arvo muuttuu samansuuntaisesti osakemarkkinoiden kehityksen kanssa.

Nämä hypoteesit saivat tutkielman myötä vahvistuksensa. Välissä esitetty olettamus siitä, että mediahuomion vaikutus hintaindeksiin olisi ollut

voimakkaampaa vuoden 2012 jälkeen, ei saavutettujen mittaustulosten perusteella pitänyt paikkaansa.

7 LÄHDELUETTELO

Barber Simon, Xavier Boyen, Elaine Shi &ErzinUzun (2013).*Bitter to Better — How to Make Bitcoin a Better Currency*.Saatavillainternetistä http://robotics.stanford.edu/~xb/fc12/bitcoin.pdf

Becker Jörg, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer& Rainer Böhme (2012). *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency*. Saatavilla internetistä http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2041492

Benoit Kenneth (2011). *Linear regression models with logarithmic transformations*. Saatavilla internetistä http://www.kenbenoit.net/courses/ME104/logmodels2.pdf

Bloomberg (2013). *China's Largest Bitcoin Exchange Seeks Recognition for Currency*. Saatavilla internetistä http://www.bloomberg.com/news/2013-12-02/china-s-largest-bitcoin-exchange-seeks-recognition-for-currency.html

British Broadcasting Corporation. *JP Morgan files for anonymous online payment system*. Saatavilla internetistä http://www.bbc.co.uk/news/business-25326289

BryansDanton (2013). *Bitcoin And Money Laundering: Mining For An Effective Solution*. Saatavilla internetistä http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2317990

Courtois Nicolas, Marek Grajek& Rahul Naik (2013).*The Unreasonable Fundamental IncertitudesBehind Bitcoin Mining*. Saatavillainternetistä http://arxiv.org/abs/1310.7935

Grinberg Reuben (2011). *Bitcoin:An Innovative Alternative Digital Currency*. Saatavillainternetistä http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857

Hyppönen Mikko (2013). Haastattelu. Saatavilla internetistä http://www.youtube.com/watch?v=T3gRTU3fz_c

Jeong Sarah (2013). *The Bitcoin Protocol as Law, and the Politics of a Stateless Currency*.Saatavilla internetistä http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124

Krugman Paul (2013). *The Concience of a Liberal: Bitcoin is evil*. Saatavilla internetistä http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_php=true&_type=blogs&_r=0

Krugman Paul (2013). *The Concience of a Liberal:Adam Smith Hates Bitcoin*. Saatavilla internetistä http://krugman.blogs.nytimes.com/2013/04/12/adam-smith-hates-bitcoin/?_php=true&_type=blogs&_r=0

Motherboard (2013).*Feds Seize Funds of Largest Bitcoin Exchange*. Saatavilla internetistä http://motherboard.vice.com/blog/feds-seize-funds-of-largest-bitcoin-exchange

Nakamoto Satoshi (2008). Bitcoin: *A Peer-to-Peer Electronic Cash System*. Saatavilla internetistä http://bitcoin.org/bitcoin.pdf

Newey, W. & K. West (1987). *A simple positive semi-definite, heteroskedasticity and autocorrelation consistent covariance matrix*.Econometrica 55, 703–708. Saatavilla internetistä http://www.ssc.wisc.edu/~kwest/publications/1980/A%20Simple%20PSD%20HAC%20Covariance%20Matrix.pdf

Plassaras Nicholas (2013). *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*.Saatavilla internetistä http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419

Reid Fergal, Harrigan Martin (2011). *An Analysis of Anonymity in the Bitcoin System*.Saatavillainternetistä http://arxiv.org/pdf/1107.4524.pdf

The Standard (2013).*Bitcoin Punters Take Big Hit*. Saatavillainternetistä http://www.thestandard.com.hk/news_detail.asp?pp_cat=1&art_id=139428&sid=40855704&con_type=1&d_str=20131111&isSearch=1&sear_year=2013

Wired (2014).*Silicon Valley VC Thinks a Single Bitcoin Will Be Worth $100,000*. Saatavilla internetistä http://www.wired.com/wiredenterprise/2014/01/chrisdixon/

WooldridgeJeffrey (2006). *Introductory Econometrics: A Modern Approach*.4th edition.

YK (2011).*United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes*. Saatavilla internetistä https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf