Open your mind. LUT.
Lappeenranta University of Technology

TUOTANTOTALOUDEN TIEDEKUNTA

Kustannusjohtaminen

Bitcoin – Edut, haasteet ja tulevaisuus

Bitcoin – Advantages, challenges and future

Kandidaatintyö

Janne Raina

Jarkko Sillanpää

TIIVISTELMÄ

Tekijät: Janne Raina ja Jarkko Sillanpää

Työn nimi: Bitcoin – Edut, haasteet ja tulevaisuus

Vuosi: 2014 **Paikka: Lappeenranta**

Kandidaatintyö. Lappeenrannan teknillinen yliopisto, tuotantotalous.
40 sivua, 4 kuvaa ja 1 taulukko
Tarkastaja(t): Lasse Metso

Hakusanat: Bitcoin, virtuaalivaluutat, virtuaaliraha
Keywords: Bitcoin, virtual currencies, virtual money

Bitcoin on ensimmäinen maailmanlaajuinen hajautettu ”peer-to-peer” virtuaalivaluutta, jonka toimintaa ei säätele mikään taho, esimerkiksi keskuspankki tai valtio. Tässä kandidaatintyössä pyritään selvittämään Bitcoinin etuja verrattuna perinteisiin maksumenetelmiin, kuten pankkien, luottoyhtiöiden ja muiden maksuvälitysyhtiöiden tarjoamiin palveluihin. Tämän lisäksi työssä tutkitaan Bitcoiniin liittyviä ongelmia sekä haasteita, kuten rikollista käyttöä, turvallisuusongelmia sekä volatiliteettia. Työn lopussa käsitellään Bitcoinin tulevaisuutta sekä luuodaan arvio Bitcoinin kehityksestä jatkossa. Bitcoinin vahvuuksia ja etuja verrattuna perinteisiin maksumenetelmiin ovat edullisuus, anonymiteetti, arvon määräytyminen sekä transaktioiden nopeus. Perinteiset maksumenetelmät veloittavat asiakkailtaan huomattavia välityspalkkioita, vaativat tunnistuksia palveluihinsa sekä transaktioiden suorittaminen kestää päivistä viikkoihin. Bitcoinin avulla kustannukset ovat minimaaliset sekä transaktiot käyttäjien välillä ovat välittömiä ja anonyymeja. Voidaan nähdä, että Bitcoinilla on tulevaisuudessa kaksi mahdollista suuntaa; Bitcoinin käyttö tulee kasvamaan vaihdonvälineenä tai jokin toinen virtuaalivaluutta tulee korvamaan Bitcoinin tulevaisuudessa parempana maksuvälineenä.

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Työn tausta ja tavoitteet

Bitcoin on avoimeen lähdekoodiin perustuva hajautettu ”peer-to-peer” virtuaalivaluutta. Se on maailman ensimmäinen kryptovaluutta, jolla ei ole keskitettyä keskushallintoa, kuten keskuspankkia tai muuta kolmatta osapuolta, joka ohjailisi sen toimintaa. Bitcoinin historia on lyhyt, sillä sen on kehittänyt alun perin nimimerkki ”Satoshi Nakamoto” vuonna 2008. Bitcoin ei ole enää pelkkä ohimenevä ilmiö, vaan siitä on tullut vakavasti otettava kilpailija perinteisille maksumenetelmille, esimerkiksi pankkien ja luottoyhtiöiden tarjoamille palveluille.

Bitcoin on maailmanlaajuinen järjestelmä ja sen avulla voidaan siirtää varallisuutta nopeasti, edullisesti sekä anonyymisti käyttäjältä toiselle. Bitcoin on saanut niin positiivista kuin negatiivista julkisuutta mediassa. Bitcoinin mahdollistamaa anonymiteettiä on käytetty hyväksi rikollisessa toiminnassa, kuten huume- ja asekaupassa nyt jo suljetulla Silk Road-verkkosivulla. Tämän lisäksi ekonomit ja keskuspankit ovat huolissaan Bitcoinin arvon heilahteluista sekä kauppapaikkojen turvallisuudesta. Bitcoin on kokenut lyhyen olemassaolonsa aikana useita arvon romahduksia, jotka ovat vähentäneet Bitcoinin uskottavuutta markkinoilla. Epävarmuus on kasvanut entisestään, kun suurin bitcoinien vaihtamiseen perustuva kauppapaikka Mt. Gox sulkeutui yllättäen helmikuussa 2014. Tämän seurauksena yhtiö itse ja sen asiakkaat menettivät yli 400 miljoonan dollarin arvosta bitcoineja.

Bitcoin on mielenkiintoinen tutkimuksen kohde, sillä siitä ei ole tehty kovinkaan paljon tutkimusta aikaisemmin ja on aiheena erittäin ajankohtainen. Bitcoin jakaa mielipiteitä ekonomien ja asiantuntijoiden keskuudessa. Monet ovat ylistäneet Bitcoinia vallankumouksellisena maksumenetelmänä, joka tulee korvaamaan useat maksumenetelmät tulevaisuudessa. Suurin osa ekonomeista ja asiantuntijoista on varoitellut julkisuudessa Bitcoinin käytöstä viime aikoina ja jopa Suomen Pankki on varoittanut siihen liittyvistä riskeistä. Varoitukset liittyvät siihen, että Bitcoin ei ole virallista rahaa ja sen arvon vaihtelu luo riskejä käyttäjälle (Suomen Pankki 2014). Bitcoin herättää paljon epävarmuutta ja ennakkoluuloja, ja jotkut ovat epäilleet sen esimerkiksi olevan maailman suurin pyramidihuijaus.

Tässä kandidaatintyössä pyritään selvittämään Bitcoinin etuja verrattuna perinteisiin maksumenetelmiin, kuten pankkien, luotto- ja maksuvälitysyhtiöiden tarjoamiin palveluihin. Työssä tutkitaan myös minkälaisia ongelmia ja haasteita Bitcoiniin ja sen käyttämiseen liittyy. Lisäksi pyritään muodostamaan kattavan analyysin Bitcoinin kehityksestä tulevaisuudessa.

1.2 Tutkimuskysymykset

Olemme asettaneet työllemme kolme tutkimuskysymystä, joita tutkitaan työssä.

- Mitkä ovat Bitcoinin edut verrattuna perinteisiin maksumenetelmiin?
- Minkälaisia ongelmia ja haasteita liittyy Bitcoiniin?
- Miten Bitcoin tulee kehittymään tulevaisuudessa?

1.3 Työn rakenne ja rajaukset

Työn alkupuolella perehdytään lyhyesti markkinoilla oleviin yleisempiin maksumenetelmiin, kuten pankkien, luottoyhtiöiden ja muiden maksuvälitysyhtiöiden tarjoamiin palveluihin. Alussa esitellään myös lyhyesti kryptorahan käsite. Tämän jälkeen siirrytään Bitcoinin tarkempaan käsittelemiseen ja tarkasteluun. Tarkastelussa käydään läpi Bitcoinin tausta ja tutustutaan Bitcoin-verkon toimintaan, kuten sen turvallisuuteen, louhintaan sekä transaktioiden suorittamiseen. Työn keskiosassa keskitytään tutkimuskysymysten käsittelemiseen kirjallisuuteen perustuen. Ensin perehdytään Bitcoinin etuihin verrattuna perinteisiin maksumenetelmiin. Etuja tarkastellaan erilaisista näkökulmista. Tämän jälkeen pohditaan Bitcoiniin liittyviä ongelmia ja haasteita, kuten turvallisuutta, rikollisuutta ja lainsäädäntöä. Työn lopuksi on vuorossa pohdintaa Bitcoinin tulevaisuudesta. Tutkimuksen päättävät johtopäätökset, johon on tiivistetty työn tärkeimmät asiat sekä koostettu taulukko Bitcoinin eduista, haitoista ja ongelmista.

Työssä käytetään ”bitcoinia” kahdessa eri merkityksessä. Isolla alkukirjaimella kirjoitettuna Bitcoinilla viitataan koko järjestelmään ja pienellä kirjoitettuna bitcoin-kolikkoon. Työ on rajattu Bitcoinin käsittelemiseen. Muista maksumenetelmistä käsitellään vain yleisimmin käytetyt menetelmät ja muut yleisimmät virtuaalivaluutat.

2 MAKSUMENETELMÄT

2.1 Yleistä

Nykymaailmassa vaihdon välineenä käytetään yleisesti rahaa. Yksi virallisen rahan ominaisuuksista on sen arvon säilyvyys. Toinen ominaisuus on, että rahaa säätelee jokin valtio tai keskusjärjestö, esimerkiksi pankki. Valuutalla tarkoitetaan, jonkin tietyn valtion rahaa, kuten esimerkiksi Yhdysvaltain dollaria. Valuuttaa voi käyttää myös jokin muu valtio virallisena rahanaan. Valuutta voi olla sidottu lisäksi johonkin toiseen reaalimaailman kohteeseen, kuten kullan arvoon. (Mankiw 2002, 76-77)

Suurin osa nykyisistä yleisimmin käytetyistä maksumenetelmistä perustuu perinteisen rahan vaihtoon. Yksinkertaisin tapa on vaihto tai maksaminen käteisellä rahalla. Nykyään suurin osa rahan liikkeistä tapahtuu kuitenkin elektronisesti. (Kauko 2011) Erilaisia sähköisiä rahan vaihdannan välineitä ovat tilisiirrot ja esimerkiksi pankkikortit. Luottokortteja tarjoavat taas erilaiset luottoyhtiöt, kuten Visa (Visa 2014). Käteisen rahan käyttäminen on käytännössä käyttäjälleen ilmaista eli siinä ei ole välikäsiä. Pankkien ja luottoyhtiöiden toiminta on sen sijaan liiketoimintaa. Tällöin jokainen tilisiirto tai maksutapahtuma luottokortilla maksaa. Maksu suoritetaan joko suoraan siirrettävästä summasta tai vuosittaisilla palvelumaksuilla tai epäsuorasti muiden järjestelyjen kautta.

Pankkien ja luottoyhtiöiden lisäksi on yrityksiä, jotka ovat erikoistuneet verkossa tapahtuvaan maksamiseen. Vaihtomäärältään suurin maksuvälityspalvelu on tällä hetkellä PayPal (Coinometrics 2014). PayPalin avulla käyttäjät voivat pienillä välityspalkkioilla siirtää rahaa reaaliaikaisesti PayPalin palvelimien kautta vastaanottavalle henkilölle. PayPalin toiminta perustuu siihen, että ostaja ei joudu antamaan tietojaan myyjälle, vaan tiedot syötetään ainoastaan PayPalin tietoihin. Palvelulla on henkilökunta, joka valvoo vaihtoa ja siirtoja. Tällä tavoin PayPal on ostajalle turvallisempi palvelu, kuin esimerkiksi luottokortin käyttäminen verkkomaksamisessa, jossa ostajan pitää syöttää myyjälle omat luottotietonsa. (Paypal 2014) Myös esimerkiksi Skrillin toiminta perustuu samaan ideaan, ja on ensisijaisesti tarkoitettu PayPalin tapaan verkkomaksamiseen (Skrill 2014).

Uusimpana maksumenetelmänä on tullut virtuaaliraha, josta voidaan käyttää myös nimitystä virtuaalivaluutta. Virtuaaliraha voidaan jakaa kahteen joukkoon. Ensimmäinen ja selvästi suurin joukko koostuu kryptografisesta eli kryptorahasta, suurimpana näistä Bitcoin. Tämä työ keskittyy käsittelemään tätä joukkoa. (Coinmarketcap 2014) Toiseen joukkoon kuuluu virtuaalirahat, joiden toiminta ei perustu kryptografiaan, ja ne ovat sidottuja johonkin viralliseen valuuttaan tai muuhun reaalimaailman hyödykkeeseen. Toisen joukon esimerkkinä on Ven-raha, joka on erilaisiin valuuttakursseihin sidottu ja hyvin rajatussa käytössä oleva virtuaaliraha. (Ven 2014)

2.2 Kryptoraha

Käsite kryptoraha tai kryptovaluutta määriteltiin ensimmäisen kerran vuonna 1998. Idea sisälsi uudenmallisen rahan ja järjestelmän, joka hyödyntäisi kryptografiaa rahan luomisessa ja siirroissa. Kryptorahan idea on se, että raha ja sen vaihdanta olisi riippumatonta kolmannesta osapuolesta, kuten pankista. Tällä tavoin saavutetaan erilaisia etuja, kuten lisääntynyt anonymiteetti ja pienentyneet kulut. Kryptorahan toiminnan perusteena ovat hajautettu verkko ja sen käyttäjät. Ensimmäinen kaupallinen sovellus kryptorahasta on virtuaalivaluutta Bitcoin, jonka perusteet julkaistiin vuonna 2008 ja toiminta alkoi tammikuussa vuonna 2009. (Bitcoin 2014)

Bitcoinia on seurannut suuri määrä muita samaa toimintatapaa noudattavia virtuaalirahoja, jotka ovat kuitenkin vielä markkina-arvoltaan Bitcoinia selkeästi pienempiä. Erilaisia muita suosituimpia virtuaalirahoja ovat Litecoin ja Peercoin. Päiväkohtaisessa vaihdossa Litecoin on samalla tasolla Bitcoinin kanssa. Molemmissa valuutoissa vaihdannan vaihtelu on kuitenkin vielä suurta samoin kuin niiden arvon vaihtelu (Coinmarketcap 2014). Bitcoinia seuranneet rahat tai kolikot pyrkivät hankkimaan markkinaosuutta niiden pienillä parannuksilla Bitcoinista. Esimerkiksi Bitcoinia jäljittelevä Litecoin markkinoi itseään nopeammalla transaktioiden varmistusajalla. Peercoin kertoo edukseen energiatehokkuuden, sillä sen toimintamalli tarvitsee vähemmän laskentatehoa verkon ylläpitämiseen ja näin kuluttaa vähemmän energiaa. (Kerner 2014)

3 BITCOIN

3.1 Yleistä

Bitcoin on tällä hetkellä maailman laajimmalle levinnein ja ylivoimaisesti käytetyin ”peer-to-peer” virtuaalivaluutta. Bitcoin on ensimmäinen hajautettu maksujärjestelmä, jolla ei ole omaa keskushallintoa tai omistajaa, esimerkiksi keskuspankkia. Järjestelmää pidetäänkin yllä käyttäjien toimesta ja käyttäjien välisten siirtojen välillä ei ole välikäsiä veloittamassa välitysmaksuja (Ron & Shamir 2013, 6-8). Transaktiot käyttäjien välillä ovat välittömiä ja bitcoineja voidaan siirtää käyttäjien välillä globaalisti. Bitcoinin arvo perustuu täysin kysyntään ja tarjontaan, täten sitä ei voida kontrolloida esimerkiksi keskuspankkien toimenpiteillä. Bitcoinin toiminta kuvailtiin ensimmäisen kerran vuonna 2008 Satoshi Nakamoton julkaisussa ”Bitcoin: A Peer-to-Peer Electronic Cash System”. Nakamoton oikeaa henkilöllisyyttä ei ole onnistuttu varmentamaan tähän päivään mennessä, vaikka julkisuudessa onkin esiintynyt erinäisiä arvailuja siitä. (Drainville 2012, 10-11) Bitcoinin arvo on kehittynyt nopeasti viimeisen vuoden aikana. Yhden bitcoinin arvo oli vuoden 2012 lopussa alle 100 dollaria, käyden korkeimmillaan joulukuussa 2013 yli 1100 dollarissa. Bitcoinin arvo on kuitenkin romahtanut useita kertoja olemassaolonsa aikana ja sen volatiliteetti onkin suuri verrattuna perinteisiin valuuttoihin. (Bitcoincharts 2014)

Kuluttaja voi hankkia bitcoineja itsellensä muutamalla eri tavalla. Yleisin ja helpoin tapa hankkia bitcoineja on vaihtaa perinteisiä valuuttoja virtuaalivaluutaksi tähän keskittyneiltä palveluntarjoajilta. Kauppapaikoissa voidaan vaihtaa käypää valuuttaa, esimerkiksi Yhdysvaltain dollareita, euroja ja yeneja bitcoineihin voimassa olevan vaihtokurssin mukaan. Vaihtokurssit määräytyvät kysynnän ja tarjonnan mukaan. Käyttäjät voivat ansaita bitcoineja itselleen niin sanotun louhinnan avulla, jonka avulla uusia bitcoineja luodaan järjestelmään. Louhinta perustuu monimutkaisten matemaattisten ongelmien ratkaisemiseen. Monet palveluntarjoajat antavat myös ilmaisia bitcoineja pienien laskutoimitusten tekemisestä internetsivuilla. Tämän lisäksi bitcoineja voi ansaita myymällä hyödykkeitä tai palveluja bitcoineja vastaan. (Drainville 2012, 11-12; Plassaras 2013, 8)

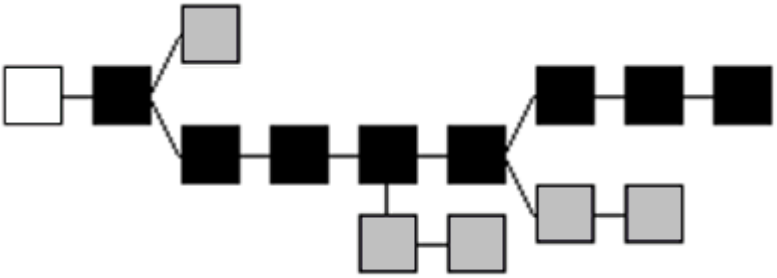
3.2 Toimintaperiaate

Bitcoinin toiminta perustuu käyttäjien ylläpitämään julkiseen vertaisverkkoon. Käyttäjät ylläpitävät tätä vertaisverkkoa ja varmistavat sen turvallisuuden ja oikeanlaisen toiminnan. Käyttäjät saavat ylläpidosta korvaukseksi bitcoineja, jonka avulla motivoidaan käyttäjiä pitämään huolta järjestelmästä. Bitcoinin voidaan sanoa olevan julkinen tietokanta, sillä järjestelmä säilyttää kaikkien bitcoinien täydellisen siirtohistorian lohkoketjussa. Lohkoketju sisältää transaktiot aina ensimmäisestä siirrosta lähtien. Transaktioita voi kuka tahansa seurata ja tutkia lohkoketjun avulla, mutta niistä ei voi päätellä kuka on Bitcoin-osoitteiden takana. (Brito & Castillo 2013,1-9) Bitcoineja syntyy järjestelmään keskimäärin kymmenen minuutin välein niin kutsutun louhinnan seurauksena siten, että bitcoinien kokonaismäärä tulee olemaan vuonna 2140 yhteensä 21 miljoonaa kappaletta. Louhintaa käsitellään tarkemmin luvussa 3.4. Vuoden 2140 jälkeen uusia bitcoineja ei enää synny. Bitcoin voidaan jakaa kahdeksan desimaalin tarkkuudella, jonka seurauksena sitä voidaan käyttää jatkossakin suuremmassa mittakaavassa, vaikka uusia bitcoineja ei synny lisää tulevaisuudessa. (Bitcoin 2014)

Louhinnan avulla luodaan uusia lohkoja, jotka liitetään osaksi lohkoketjua. Lohko sisältää uudet transaktiot käyttäjien välillä ja liittämällä lohkon osaksi lohkoketjua, transaktiot varmistuvat ja ovat sen jälkeen peruuttamattomia. Lohkoketjun ja proof-of-workin avulla pyritään tekemään Bitcoinin väärinkäyttämisestä niin vaikeaa ja kallista, että se ei ole taloudellisesti kannattavaa rikollisille. (Bitcoin 2014)

3.3 Lohkoketju ja lohko

Lohkoketjuun on tallennettu kaikki bitcoinien siirrot kautta aikojen, aina ensimmäisestä siirrosta asti. Lohkoketju muodostuu siten, että lohkoketjuun liitetään aina uusin lohko ketjun perään. Jokaisessa uudessa lohkossa on yhteys aikaisempaan lohkoon. Uusin lohko, joka liitetään lohkoketjun osaksi, sisältää edellisen lohkon tiivisteen. (Bradbury 2013) Tällä on pyritty siihen, että lohkoketju on yhtenäinen katkeamaton ketju. Kun lohko on liitetty osaksi lohkoketjua, sen sisältämät transaktiot ovat pysyvä osa järjestelmää ja niitä on mahdoton muokata enää jälkikäteen (Arias & Yongseok 2013). Lohkojen muokkaaminen jälkikäteen vaatisi erittäin suuren määrän laskentatehoa, sillä tällöin tulisi muuttaa kyseisen lohkon lisäksi myös kaikki sitä seuranneet lohkot. (Bitcoin 2014)



Kuva 1. Lohkoketjun muodostuminen (Bitcoin Wiki 2014a)

Lohkoja syntyy keskimäärin kymmenen minuutin välein, mutta on kuitenkin mahdollista, että syntyy kaksi uutta lohkoa lyhyen ajan sisällä. Lohko, jonka liittämällä koko lohkoketjun vaikeusaste on suurin, liitetään osaksi varsinaista lohkoketjua. Kuvassa 1 valkoiseen alkuperäiseen lohkoon on liitetty uusia lohkoja. Musta lohkoketju on vaikein mahdollinen ketju. Kuvassa olevat harmaat lohkot ovat syntyneet samaan aikaan kuin varsinaiseen lohkoketjuun liitetyt mustat lohkot. Ketjut, joiden perään on liitetty harmaa lohko, eivät ole kuitenkaan vaikein mahdollinen lohkoketju. Näiden harmaiden lohkojen sisältämät siirrot eivät ole mukana pisimmässä lohkoketjussa eikä niitä ole täten varmistettu. Tällä vaikeimman lohkoketjun menetelmällä pyritään estämään louhijoita tekemästä useita helppoja lohkoja ja liittämään niitä lohkoketjuun ja tätä kautta luomaan uusia bitcoineja liian nopeasti. (Drainville 2012, 14-15; Arias & Yongseok 2013)

Lohko sisältää kaikki tai osan bitcoin-siirroista, jotka eivät ole vielä tallennettuna viimeisimpään lohkoketjuun. Tämän lisäksi lohkossa on aikaisemman lohkon tiiviste, jonka avulla lohkot ovat linkittyneet toisiinsa. Lohko sisältää myös vastauksen monimutkaiseen matemaattiseen ongelmaan, joka on ainutlaatuinen jokaiselle lohkolle. Uusia lohkoja ei voi liittää lohkoketjuun ilman oikeaa vastatusta tähän ongelmaan. Bitcoineja syntyy, kun louhijat löytävät ratkaisun tähän monimutkaiseen matemaattiseen ongelmaan ja lohko liitetään osaksi lohkoketjua. Ratkaisun löytäjä saa palkinnoksi bitcoineja sekä lohkon sisältämät vapaaehtoiset siirtopalkkiot (Brito & Castillo 2013, 6-7). (Arias & Yongseok 2013)

3.4 Proof-of-work ja louhinta

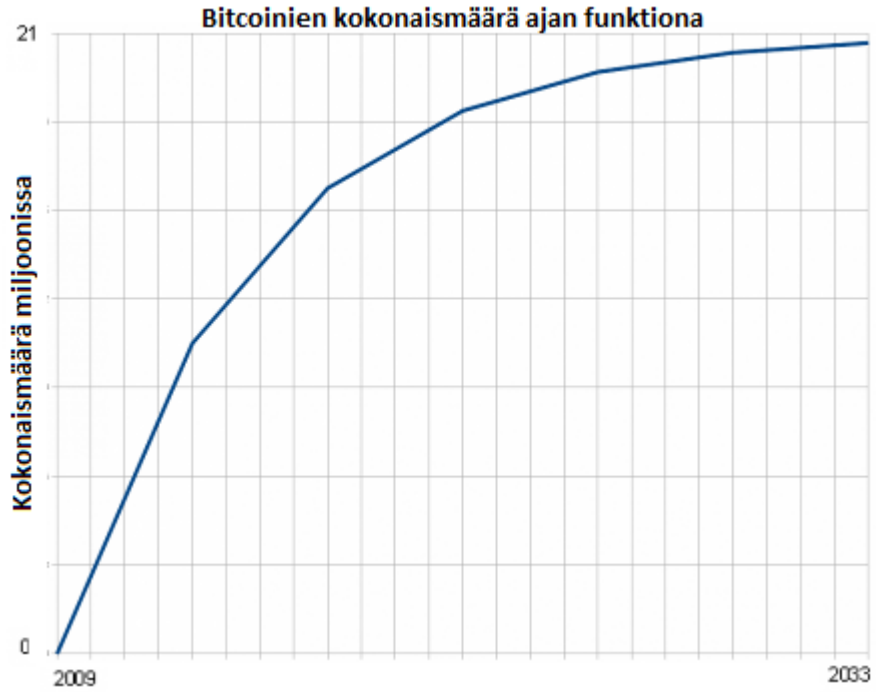
Bitcoinilla ei ole olemassa kolmatta osapuolta, joka varmistaisi transaktioiden oikeellisuuden ja sen, ettei bitcoineja ole käytetty useaan kertaan. Proof-of-workin avulla pyritään hallitsemaan

lohkojen luontia sekä varmistamaan, että lohkot on luotu laskentatehon avulla, eikä käyttäen rikollisia menetelmiä. Järjestelmän muut käyttäjät varmistavat, että uuden lohkon sisältämät transaktiot ovat valideja. Lohko liitetään osaksi lohkoketjua vasta, kun muut käyttäjät ovat tarkistaneet transaktioiden oikeellisuuden. Tällä pyritään estämään bitcoinien kaksinkertainen käyttö, niin kutsuttu ”double spending”. (Arias & Yongseok 2013)

Bitcoinilla ei ole omaa keskitettyä tietohallintoa, joka vastaisi järjestelmän toiminnasta. Koko järjestelmän toiminta perustuu tähän hajautettuun malliin, jossa käyttäjät ylläpitävät järjestelmää. Kuka tahansa voi ladata koneelleen ohjelman, jonka avulla voi aloittaa louhinnan ja järjestelmän ylläpidon. (Bitcoin 2014) Louhinta perustuu arvontaan, jossa louhijat pyrkivät arvaamaan seuraavan lohkon tiivisteen. Louhijat pyrkivät löytämään uudelle lohkolle tiivisteen, jonka arvo on pienempi tai yhtä suuri kuin järjestelmän antama tavoitearvo. Jokainen louhija tietää kyseisen arvon ja mikäli onnistuu löytämään pienemmän tai yhtä suuren arvon, niin kyseisen louhijan lohko liitetään osaksi lohkoketjua ja louhija saa palkinnoksi bitcoineja. (Nakamoto 2008)

Louhinnan avulla synnytetään uusia bitcoineja siten, että uusia bitcoineja syntyy tällä hetkellä 25 kappaletta aina, kun syntyy uusi lohko (Wiener, Zelnik, Tarnish & Rodgers 2013, 35-36). Järjestelmässä on pyritty siihen, että uusia lohkoja syntyy keskimäärin kymmenen minuutin välein. Louhinnan vaikeustason tarkistus tehdään 2016 lohkon välein siten, että uusien lohkojen syntymisen välinen aika säilyy noin 10 minuutissa. Laskentatehon kasvaessa vaikeustaso kasvaa, kun taas laskentatehon pienentyessä myös vaikeusaste pienenee. Vaikeusaste on kasvanut huomattavasti Bitcoinin alkuajoista, sillä tällä hetkellä louhiminen on yli 4000 miljoonaa kertaa vaikeampaa kuin vuonna 2009 (Bitcoindifficulty 2014). Vaikeusasteen kasvaessa järjestelmän antama tavoitearvo louhijoille pienenee, jolloin myös mahdollisten oikeiden ratkaisujen määrä pienenee. Louhijoiden saamien bitcoinien määrä uusien lohkojen luomisesta tulee kuitenkin puoliintumaan 210 000 lohkon välein, jotta bitcoinien määrä ei tule kasvamaan loputtomasti ja valuutta pysyy vakaana. Kuvassa 2 on esitetty bitcoinien lukumäärän kehittyminen ajan funktiona. Järjestelmä on luotu siten, että bitcoinien kokonaismäärä tulee olemaan lopulta 21 miljoonaa kappaletta vuonna 2140. (Bitcoin 2014) Tämän syntymekanismin seurauksena kuitenkin vuonna 2040 bitcoineja on liikkeellä 99,9 % maksimaalisesta määrästä (Forbes 2013). Uusien lohkojen luomisesta saatavien korvausten

pienentyessä louhijoiden saamat tulot tulevat pienentymään tältä osin. Tästä johtuen tulevaisuudessa louhijat tulevat saamaan korvauksia vapaaehtoisten siirtokorvausten muodossa, joiden osuus tällä hetkellä on hyvin marginaalinen (Brito & Castillo 2013,7). (Bitcoin Wiki 2014b)



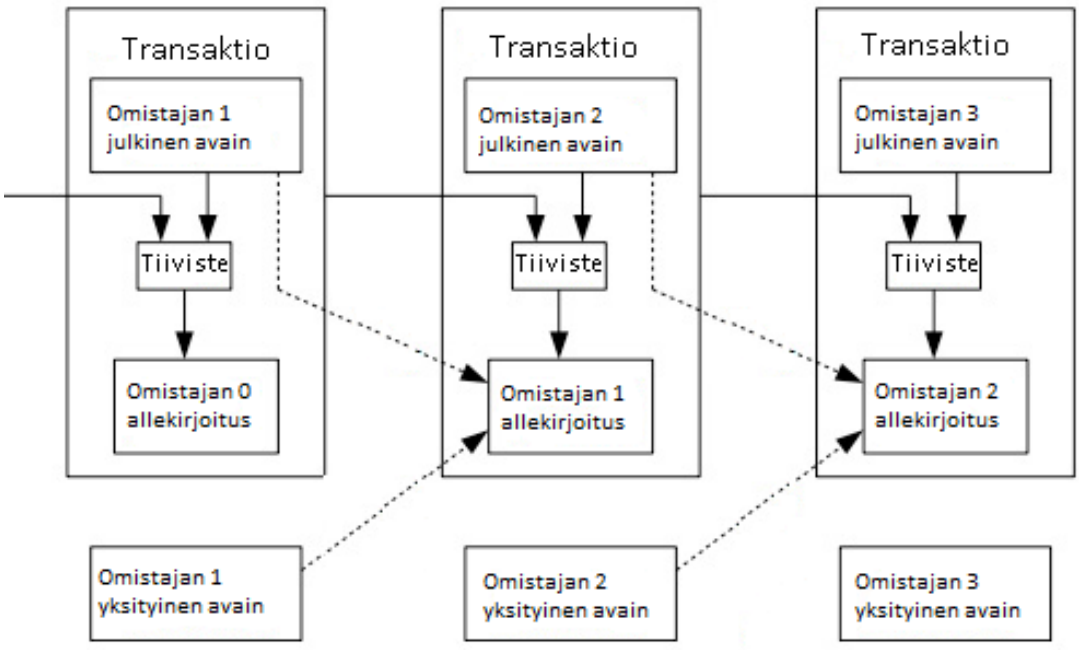
Kuva 2. Bitcoinien määrän kehittyminen (Bitcoin Wiki 2014c)

Yksittäiset henkilöt ovat onnistuneet luomaan lohkoja Bitcoinin alkuaikoina, kun louhijoiden kollektiivinen laskentateho oli alhainen ja siten louhinnan vaikeustaso oli matala. Tällä hetkellä louhijoiden määrä ja kollektiivinen laskentateho ovat kasvaneet huomattavasti ja laskutoimitukset ovat niin vaikeita, että yksittäiset henkilöt eivät voi ratkaista ongelmia yksin. Tästä johtuen louhinnasta on tullut ammattimaista toimintaa ja yksityiset henkilöt ovat muodostaneet niin sanottuja ”mining-pooleja” eli louhintayhteisöjä. Nämä yhteisöt pyrkivät yhdessä etsimään uuden lohkon ja jakamaan tästä saadut bitcoinit kaikkien käyttäjien kesken. (Eyal & Sirer 2013, 1-3; Bitcoin 2014)

3.5 Transaktiot

Kuvassa 3 on Nakamoton kuvailema menetelmä, jonka avulla bitcoinit siirtyvät käyttäjältä toiselle. Transaktio käyttäjien välillä tapahtuu siten, että kolikon luovuttaja allekirjoittaa

digitaalisesti kyseisen kolikon edellisen transaktion tiivisteen sekä vastaanottajan julkisten avaimen eli bitcoin-osoitteen. Tämän jälkeen luovuttaja liittää nämä tiedot kyseiseen kolikkoon. Tällä tavalla kuka tahansa voi varmistaa kyseisen transaktion oikeellisuuden. (Nakamoto 2008; Androulaki, Karame, Roeschelin, Scherer & Capkun 2013, 35-36)



Kuva 3. Bitcoin-kolikoiden siirtyminen käyttäjältä toiselle (Nakamoto 2008)

Transaktiot varmistetaan muiden käyttäjien toimesta lohkojen luomisen yhteydessä. Transaktio varmennetaan, kun se hyväksytään uusimpaan lohkoon ja lisätään lohkoketjuun. Kun lohko on liitetty osaksi lohkoketjua, siirtoa on mahdoton enää muuttaa jälkikäteen. Uuden lohkon syntymisessä kestää keskimäärin kymmenen minuuttia. On kuitenkin mahdollista, että syntyy useampi lohko samaan aikaan ja tällöin ainoastaan yksi lohko liitetään osaksi lohkoketjua. Tällöin on mahdollista, että siirtoa ei hyväksytä. (Drainville 2012, 12-13) Tämän seurauksena suurissa siirroissa tuleekin odottaa kuusi varmennusta, jotta voidaan olla varmoja siirron oikeellisuudesta sekä siitä, että siirto on peruuttamaton. (Bitcoin 2014)

3.6 Bitcoin-verkon toiminta

Tässä luvussa esitellään Bitcoin-verkon toiminnan eri vaiheet ja kuinka lohkossa olevat transaktiot hyväksytään ja lohko liitetään osaksi lohkoketjua.

1. Järjestelmään syötetään uudet transaktiot kaikkien louhijoiden nähtäväksi.
2. Louhijat valitsevat transaktiot omaan lohkoonsa ja pyrkivät lisäämään sen osaksi lohkoketjua.
3. Louhijat pyrkivät löytämään laskentatehoa käyttäen proof-of-workin mukaista tavoitearvoa pienemmän tai yhtä suuren tiivisteen ja luoda uuden lohkon.
4. Kun louhija löytää oikeanlaisen tiivisteen uudelle lohkolle, se tuodaan julki jokaiselle verkon louhijalle.
5. Muut louhijat pyrkivät varmistamaan, että kaikki kyseisen lohkon sisältämät transaktiot ovat valideja. Tällä pyritään estämään bitcoinien kaksinkertainen käyttö.
6. Lohko liitetään osaksi lohkoketjua ja louhijat alkavat liittää uusia lohkoja kyseisen lohkon perään. (Nakamoto 2008; Hobson 2013)

3.7 Käyttö ja säilyttäminen

Bitcoineja voidaan säilyttää usealla eri menetelmällä. Vaihtoehdot eroavat toisistaan ja käyttäjien tulisikin tutustua eri menetelmiin ja valita itselleen sopivin. Osa menetelmistä sopii satunnaisille käyttäjille, joilla ei ole kovinkaan suuria summia bitcoineja hallussaan, kun taas osa menetelmistä käyttäjille, joilla on huomattavia määriä bitcoineja. Yksinkertaisin tapa säilyttää omia bitcoinejaan on selainpohjainen lompakko. Tämän lisäksi on olemassa omalle tietokoneelle ladattavia ohjelmia, jotka ovat yhteydessä itse bitcoin-verkkoon. Suuria summia säilytetään yleensä offline-lompakoissa ja muistitikuilla, sekä erilaisilla palveluntarjoajien omilla servereillä. (Bitcoin 2014)

Bitcoineja voidaan käyttää tuhansissa kauppapaikoissa ympäri maailmaa. Bitcoineja käytetään kuitenkin enemmän yksityisten käyttäjien välisessä rahansiirrossa kuin hyödykkeiden ostamiseen virallisista kauppapaikoista. Bitcoineja käytetään useammin internetissä tapahtuvissa kaupoissa kuin fyysisissä kauppapaikoissa. Käyttäjät ovat viimeaikoina myös omaksuneet bitcoinien käyttämisen erilaisten tippien ja lahjoitusten tekemiseen, esimerkiksi

Wikileaks, 4Chan, Piratebay ja Mega hyväksyvät bitcoineja lahjoituksina. (Bitcoin Wiki 2014d)

4 EDUT VERRATTUNA PERINTEISIIN MAKSUMENETELMIIN

4.1 Anonymiteetti

Kaikki bitcoineilla suoritettavat transaktiot tallennetaan julkiseen lohkoketjuun, josta kuka tahansa voi käydä tutkimassa yksittäisiä transaktioita. Transaktioista ei kuitenkaan pysty tunnistamaan henkilöitä tai tahoja niiden takana. Julkiset osoitteet ovat ainoastaan satunnaisia numeroita sekä kirjaimia, joissa ei ole tunnistetietoja käyttäjästä. Kukaan tai mikään kolmas osapuoli ei myöskään valvo bitcoinien vaihdantaa, toisin kuin perinteisessä pankkimaksujärjestelmässä, jossa kolmas osapuoli käytännössä suorittaa vaihdon. (Bitcoin 2014)

Bitcoineja käytetäänkin nykyään hyvin paljon erilaisten lahjoitusten ja tippien maksamiseen juuri anonymiteetin varjolla. Esimerkiksi Wikileaks on saanut yli 2,5 miljoonan dollarin arvosta lahjoituksia Bitcoinin kautta (Blockchain 2014). Käyttäjien tulee kuitenkin huolehtia omasta anonymiteetin säilyttämisestä itsenäisesti. Lohkoketju toimii myös käyttäjää vastaan, mikäli joku taho onnistuu selvittämään bitcoin-osoitteen omistajan henkilöllisyyden. Lohkoketjusta voidaan täten selvittää kaikki transaktiot, jotka käyttäjä on tehnyt ja linkittää ne kyseiseen henkilöön. (Lee 2011)

4.2 Edullisuus

Yksi Bitcoinin suurin vahvuus on sen edullisuus verrattuna muihin maksumenetelmiin. Tehtäessä transaktioita käyttäjien välillä kustannukset ovat huomattavasti alhaisemmat kuin muita menetelmiä käyttäen. Bitcoinia käytettäessä ei ole kolmatta osapuolta, joka veloittaisi korkeita siirtomaksuja siirtojen välittämisestä. Perinteistä käteistä rahaa pidetään hyvänä maksuvälineenä, mutta suurien ostotapahtuminen tekeminen käteisenkin avulla maksaa, koska transaktion tekemiseen tarvitaan usein pankin tai jonkun muun palveluntarjoajan apua. Pankki- ja luottokorttien avulla rahan käytöstä on tullut helpompaa, mutta palveluntarjoajat veloittavat niiden käytöstä palvelumaksuja niin käyttäjiltä kuin kauppiailtakin. Erityisesti pienet yksityisyrittäjät menettävät 2-5 % tuloistaan erilaisten maksujen muodossa pankeille ja luottoyhtiöille. Yrittäjät voivat tämän lisäksi menettää asiakkaita, mikäli he vaativat asiakkaitaan maksamaan käteisellä rahalla luottokorttien sijaan. (Farrel 2007)

Luottokorttien käyttäminen altistaa yrittäjät myös ongelmalle, jossa kuluttajat eivät maksa ostoksiaan saatuaan tuotteen etukäteen. Asiakkaat maksavat hyödykkeen tai palvelun luotolla, mutta tämän jälkeen eivät maksa sitä jälkikäteen myyjälle. Myyjä voi menettää itse tuotteen sekä siitä saatavan maksun kokonaisuudessaan. Bitcoineilla maksettaessa myyjä saa suuremmalla todennäköisyydellä maksun suoritteistaan ja täten voi huomioida sen hinnoittelussa. (Brito & Castillo 2013, 10-12; Moore 2013)

Viime vuonna tehdyssä tutkimuksessa vertailtiin bitcoineilla maksamista muihin maksumenetelmiin. Tutkimuksessa tultiin siihen tulokseen, että bitcoineilla maksaminen on halvempaa kuin perinteisillä menetelmillä, kuten luottoyhtiöiden ja pankkien välityksellä. Tutkimuksessa suoritettiin rahansiirto Yhdysvalloista Eurooppaan ja vertailtiin siitä aiheutuvia kustannuksia. Bitcoineilla maksettaessa Yhdysvalloista 1000 dollarin maksu, kustannukset olisivat keskimäärin 15 dollaria. Mikäli maksun välittämiseen käytettäisiin luottoyhtiötä, kustannukset nousivat 40 dollariin ja pankkien välityksellä 80 dollariin. (Hochstein 2014)

Bitcoinista voi tulla tulevaisuudessa suurin rahansiirron väline kansainvälisissä rahansiirroissa. Maahanmuuttajat siirtävät hyvin suuria summia rahaa takaisin kehitysmaihin. Rahansiirrot tulevat kasvamaan tulevaisuudessa, kun yhä useammin kehitysmaista muutetaan ulkomaille paremman työllisyyden perässä (Pryke 2013). Vuonna 2015 kansainvälisten rahansiirtojen summan odotetaan nousevan 515 miljoonaan dollariin. Tällä hetkellä suurin osa rahoista lähetetään välitysyhtiöiden, kuten Western Unionin kautta. Siirtojen tekemiseen kuluu useita päiviä ja kustannukset ovat markkinoilla keskimäärin 9 %. Bitcoineja käyttäen kustannukset on mahdollista pudottaa yhden prosentin luokkaan. (Brito & Castillo 2013, 12-13) Bitcoinin odotetaankin muuttavan tulevaisuudessa koko markkinoiden toimintaa, sillä se on tällä hetkellä ylivoimaisesti nopein ja halvin maksumenetelmä (Holdgaard 2014).

Bitcoineja siirrettäessä on mahdollista maksaa vapaaehtoinen välityspalkkio, jonka avulla voi edesauttaa oman transaktionsa hyväksymistä seuraavaan lohkoon (Bitcoin 2014). Tämän välityspalkkion suuruus on kuitenkin hyvin marginaalinen verrattuna pankkien ja muiden kolmansien osapuolien maksuihin. Välityspalkkioiden suuruus tulee kuitenkin kasvamaan tulevaisuudessa, kun louhijoiden saamat tulot pienentyvät. Bitcoineilla maksaminen tulee

kuitenkin olemaan jatkossakin edullisempaa kuin kolmansia osapuolia käyttävät menetelmät, kuten Visan ja PayPalin välityksellä. (Bitcoin 2014)

4.3 Arvon määräytyminen ja nopeus

Keskuspankeilla tai muilla kolmansilla osapuolilla ei ole vaikutusta bitcoinin arvon muodostumiseen. Bitcoinin arvo perustuu täysin markkinoilla vallitsevaan kysyntään ja tarjontaan. Bitcoinien määrään ei voi myöskään vaikuttaa, vaan niitä syntyy ennalta määrätyn matemaattisen mallin mukaan, kunnes määrä saavuttaa maksimaalisen 21 miljoonan lukumäärän. Tästä johtuen Bitcoinin on vaikeaa kokea inflaatiota, sillä ei ole olemassa tahoa, joka voisi luoda suuria määriä bitcoineja lyhyen ajan sisällä, kuten keskuspankkia. (Vitt 2013, 3-5)

Bitcoineja voidaan siirtää äärimmäisen nopeasti eri puolille maailmaa. Transaktiot käyttäjien välillä tapahtuvat sekunneissa ja ovat käytännössä peruuttamattomia, ellei väärinkäytöksiä esiinny. Ainoa rajoittava tekijä, joka voi vaikuttaa siirtojen nopeuteen, on se, että siirron varmistus vie noin 10 minuuttia. Tämä saattaa rajoittaa bitcoinien välitöntä siirtoa eteenpäin. Tavallisia maksumenetelmiä käyttäen transaktion tekeminen käyttäjien välillä voi kestää useista päivistä aina viikkoihin. Pankkimaksamista saattaa rajoittaa esimerkiksi pankkien rajatut aukioloajat. Bitcoinin avulla transaktion tekeminen on nopeaa sekä yksinkertaista, sillä käyttäjän tarvitsee tietää ainoastaan vastaanottajan julkinen osoite eli Bitcoin-osoite. (Bitcoin 2014)

Kysyntään ja tarjontaan perustuva arvon määräytyminen ja keskushallinnon puuttuminen kuitenkin aiheuttavat riskejä Bitcoinin arvon kehitykselle. Bitcoinin arvoon voidaan vaikuttaa lyhyellä aikavälillä, koska arvo perustuu täysin markkinoilla vallitsevaan kysyntään ja tarjontaan. Mikäli yksittäinen henkilö tai taho hallitsee suurta määrää bitcoineja tai omistaa tarpeeksi varallisuutta, hän voi vaikuttaa yksin bitcoinin kurssin kehitykseen lyhyellä aikavälillä ostamalla tai myymällä suuren määrän bitcoineja markkinoilta. Bitcoinilla ei ole olemassa keskuspankkia tai -hallintoa vakauttamassa kurssin kehitystä tämän kaltaisissa tilanteissa. Pitkällä aikavälillä kuitenkin markkinoiden toiminta tasaa lyhyen aikavälin muutoksia arvossa. (Bitcoin 2014)

5 ONGELMAT JA HAASTEET

5.1 Turvallisuus

Yksi Bitcoinin leviämistä hidastavana tekijä on ollut virtuaalivaluutan alkutaipaleella esiintyneet varkaustapaukset ja huijaukset. Nämä tapaukset ovat ongelmallisia, sillä mikäli bitcoinien käyttäjä joutuu huijauksen uhriksi, hävittää tai unohtaa oman tilinsä tiedot, menettää hän samalla myös bitcoininsa lopullisesti. Käyttäjiä suositellaankin käyttämään turvalliseksi luokiteltuja palveluita ja pitämään omat tunnuksensa tallessa sekä tekemään tarvittaessa varmuuskopiota omista tiedostoistaan. (Bitcoin 2014)

Suurin osa turvallisuusongelmista liittyy kauppapaikkoihin ja niissä tehtyihin varkauksiin. Yksi varkauksien muodoista on tekaistujen kauppapaikkojen perustaminen. Rikolliseen toimintaan käytetyn Silk Roadin kaatumisen jälkeen perustettu Sheep Marketplace -niminen kauppapaikka suljettiin, kun sivusto kertoi, että siltä oli varastettu miljoonien dollarien arvosta bitcoineja. Paljastui kuitenkin, että kenelläkään sivuston käyttäjistä ei ollut enää pääsyä bitcoineihinsa, ja edelleen, että sivuston ylläpitäjät olivat varkauden takana. Varastettujen bitcoinien arvo oli tapahtumahetkellä yli 40 miljoonaa dollaria, jonka jälkeen arvo on vielä noussut. Kauppapaikkahuijausten lisäksi hakkereiden tekemät suorat varkaudet ovat olleet varsin yleisiä. Esimerkiksi Tanskassa bitcoinien maksuprosessori BIPS joutui hakkerien hyökkäyksen kohteeksi ja yritys menetti 1 miljoonan dollarin edestä bitcoineja. Australialainen bitcoinien lompakkopalvelu joutui hyökkäyksen kohteeksi ja menetti noin 1,2 miljoonan dollarin edestä kolikoita. Edellä mainitut hyökkäykset ovat tapahtuneet ennen vuonna 2013 tapahtunutta Bitcoinin suurta arvonnousua. Nykyisellä markkinahinnalla samankaltaiset varkaustapaukset olisivat esimerkiksi dollareissa mitattuna huomattavasti merkittävämpiä. (Mansfield-Devine 2013) Bitcoinin arvonnousu vuonna 2013 yli 1000 dollariin lisäsi myös haittaohjelmien määrää. Bitcoin-lompakkoja vastaan luoduista 140 erilaisesta haittaohjelmasta yli 100 ilmestyi vuoden 2013 aikana. (Wagstaff 2014)

Helmikuussa 2014 tuli julkisuuteen Bitcoinin historian toistaiseksi suurin varkaustapaus. Japanilainen ja yhdessä vaiheessa maailman suurin bitcoinien kauppapaikka ja lompakkopalvelu Mt. Gox hakeutui konkurssiin. Yhtiö ilmoitti, että syynä tähän oli hakkerihyökkäys. Yhtiö arvio, että se oli menettänyt jopa 850 000 bitcoinia, joista 750 000 oli

asiakkaiden omaisuutta ja 100 000 kappaletta yhtiön omaa varallisuutta. Silloisella kurssilla mitattuna menetettyjen bitcoinien arvoksi olisi tullut 480 miljoonaa dollaria. (Laurent 2014; Rusli 2014) Mt. Goxin lisäksi vuodesta 2010 lähtien 40 avatusta kauppapaikasta 18 on sulkeutunut erinäisistä syistä johtuen (Moore 2013).

Turvallisuusongelma on myös niin kutsuttu 51 % -hyökkäys. Bitcoinin toiminta perustuu siihen, että se toimii hajautetusti ja yli puolet sitä ylläpitävistä käyttäjistä ovat rehellisiä. Teoriassa on kuitenkin mahdollista, että bitcoinien siirtoihin käytettävien lohkojen louhinnassa käytettävästä kollektiivisesta laskentatehosta yli puolet on hallussa yhdellä tekijällä, esimerkiksi henkilöllä tai todennäköisemmin jollakin yhteisöllä. Tällöin voi syntyä väärinkäytön mahdollisuus. (Bradbury 2013) Tällä hetkellä suurin yksittäinen yhteisö, jolla tällainen mahdollisuus on olemassa, on nimeltään Ghash. Korkeimmillaan yhteisön laskentateho on yltänyt jopa 45 %:n kaikesta laskentatehosta. Toisaalta, kun tällainen nousu huomattiin vuoden 2014 alussa, putosi Ghashin osuus lyhyen ajan sisällä. Tämä kertoo Bitcoinin järjestelmän itsesäätelykyvystä. (Bershidsky 2014) Uhan nopeaan pienentämiseen vaikutti myös aktiivinen Bitcoinin etua ajava yhteisö. Erilaiset Bitcoinin etuja ajavat ja sitä seuraavat sivustot ja foorumit julkaisivat tiedotteita, joissa ne vetosivat yksittäisiin louhijoihin jättämään Ghashin. (Bitcoinexaminer 2014) Lisäksi Ghash julkaisi itse tiedotteen, jossa se myönsi tiedostavansa syntyneen uhan, mutta kielsi, että yhteisöllä olisi minkäänlaisia aikomuksia syyllistyä väärinkäytöksiin ja että yhteisö aikoo myös ryhtyä toimiin tämän uhan pienentämiseksi (Ghash 2014).

Mahdollisuus väärinkäytöksiin on verrattain pieni ja laskentatehon kasvaessa se käy koko ajan yhä vaikeammaksi esimerkiksi yksittäiselle henkilölle. Eräässä Bitcoinia jäljittelevässä virtuaalivaluutassa uhka on kuitenkin jo ainakin kerran toteutunut. Litecoiniin pohjautuva Feathercoin joutui tällaisen hyökkäyksen kohteeksi kesäkuussa 2012, jolloin koko järjestelmän kollektiivinen laskentateho oli kuitenkin huomattavasti alhaisempi kuin esimerkiksi mitä Bitcoinilla on tällä hetkellä. (Bradbury 2013)

Yhden lohkon laskennan oikeellisuus perustuu yleiseen hyväksyntään louhijoiden keskuudessa. Kun yksi tekijä hallitsee suurinta osaa laskentatehosta, voi tämä haluamallaan tavalla muokata lohkojen sisältämiä transaktioita. Eräs väärinkäytön tavoista on niin kutsuttu ”double spending”

eli bitcoinien kaksinkertainen käyttö. (Karame, Androulaki & Capkin 2012) Tässä tapauksessa käyttäjä voi siirtää samoja bitcoineja useaan eri osoitteeseen. Mikäli yksittäinen taho pystyy hallitsemaan suurinta osaa laskentatehosta, pystyy se hallitsemaan lohkoketjun luontia ja näin tekemään kaksinkertaisia siirtoja. (Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker & Savage 2013, 127-129) Kaksinkertainen käyttö on mahdollista myös ilman 51 % -hyökkäystä perustuen nopeisiin vaihtoihin. Tämä perustuu siihen, että bitcoinien vaihdon varmistaminen kestää yleensä noin 10 minuuttia. Kuitenkin vastaanottaja voi nähdä bitcoinien siirron tapahtuneen jo ennen tapahtuman varmistumista ja näin siirtää toiselle käyttäjälle esimerkiksi hänen bitcoineilla ostamansa tuotteet. Kun muut ulkopuoliset käyttäjät lopulta varmistavat tapahtuman, vain ensimmäinen bitcoinien siirto hyväksytään. Kaksinkertaisen käytön tapauksessa myyjä jää kokonaan ilman sovittuja bitcoineja. (Huang 2014,7-9)

Kaksinkertaisen käytön lisäksi on myös muita hyökkäystyyppejä tai tapoja tehdä haittaa Bitcoin-verkolle. Yksi näistä on niin kutsuttu ”dust transaction” eli bitcoinien siirto hyvin pieninä summina kerrallaan, esimerkiksi 0,00000001 BTC. Jokainen bitcoinien siirto täyttää lohkoja ja sitä kautta kuormittaa verkkoa. Kun pieniä siirtoja tehdään useita samanaikaisesti, voi tämä aiheuttaa suuria ongelmia Bitcoin-verkolle. Lisäksi on olemassa myös esimerkiksi koodiperusteinen hyökkäystyyppi, jossa hyökkäys ja haitan teko kohdistuu suoraan Bitcoinin lähdekoodiin ja voi aiheuttaa järjestelmän toiminnalle ongelmia. (Bradbury 2013)

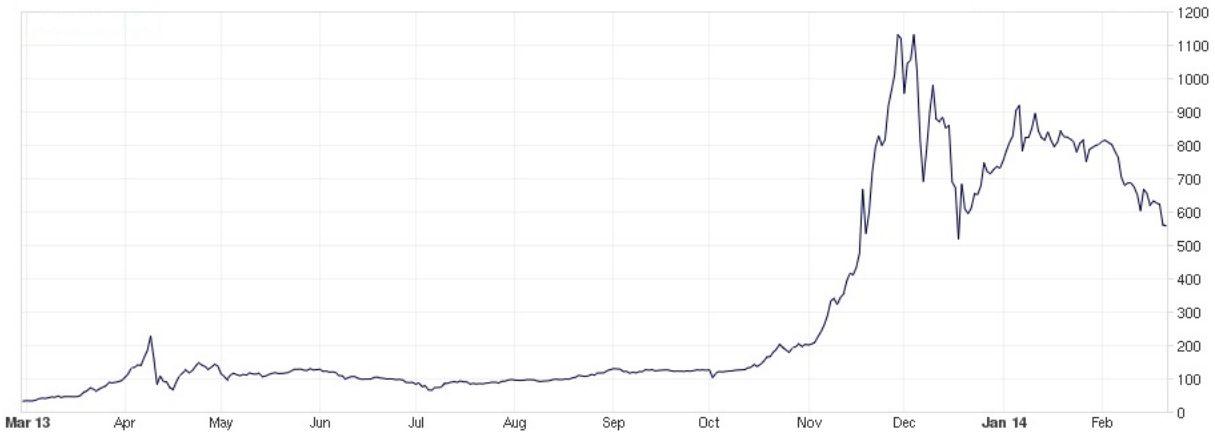
Erilaisia turvallisuuteen liittyviin ongelmiin pyritään myös varautumaan. Samalla tavoin kuin esimerkiksi Yhdysvalloissa valtiollinen Federal Deposit Incurance Corporation suojaa pankkitilejä, pyritään samaan Bitcoinissa yksityisen sektorin avulla. Suojaukseen ovat alkaneet panostaa erilaiset säilytyspalvelut. Yksi ensimmäisistä vakuutussuojaa tarjoavista yrityksistä on Iso-Britanniassa toimiva Elliptic. (Hochtein 2014) Yritys tarjoaa bitcoinien säilytyspalveluita ja se toimii iso-britannialaisen Lloyds pankki- ja vakuutusyhtiön alaisuudessa. Elliptic tarjoaa bitcoinien ja käyttäjien avaimien kylmäsäilytystä eli säilytystä Internetistä irrallaan olevissa palvelimissa. Palvelimissa sijaitsevat tiedot ovat lisäksi vielä suojattu erilaisilla salauksilla. Yhtiön tarjoama vakuutuspalvelu suojaa sekä varkauksilta että bitcoinien arvon alenemiselta. Suojaus arvon alentumista vastaan tapahtuu siten, että yhtiö sitoutuu säilyttämään käyttäjän bitcoinien dollarimääräisen arvon, mutta tallettajan bitcoinien määrä voi vaihdella. Suojaus tapahtuu bitcoinien arvon alentumista vastaan, mutta toisaalta myös hyöty bitcoinien arvon

noususta jää saamatta käyttäjälle. (Miller 2014) Myös muut yhtiöt yrittävät parantaa Bitcoinin luotettavuutta ja kaupan turvallisuutta. Esimerkiksi kauppapaikka Coinbase säilyttää 97 % käyttäjien tiedoista kylmäsäilytyksenä. Ellipticin tapaan vakuutusmahdollisuutta bitcoineille tarjoaa yhdysvaltalainen Xapo. Yhtiön liiketoimintamalli eroaa hieman Ellipticistä. Yhtiö tarjoaa bitcoinien ja käyttäjien tietojen kylmäsäilytystä suojatuissa pankkiholveissa. Yhtiön vakuutus sen sijaan suojaa vain yhtiön omaa toimintaa vastaan kohdistuneista varkauksista, eikä se suojaa arvon vaihtelua tai käyttäjän omia toimia vastaan. (Rusli 2014)

5.2 Arvon säilyminen

Bitcoinin yksi suurimmista riskeistä sen käyttäjälle ja omistajalle on sen arvon vaihtelu. (Moore 2013). Bitcoinin arvoa ei ole sidottu mihinkään ja sen arvo perustuu täysin kysyntään ja tarjontaan. Tällä hetkellä mikään valtio ei takaa bitcoinin arvoa, kuten perinteisissä valuutoissa, eikä mikään toimi arvon vakauttajana (Bitcoin 2014)

Bitcoinin arvo on vaihdellut useita kertoja olemassaolonsa aikana, kuten kuvasta 4 voidaan nähdä. Volatiliteetti on tähän asti ollut suurimmillaan syys-joulukuussa 2013. Bitcoinin arvo kävi ylimmillään yli 1100 dollarissa joulukuun 1. päivä. Noin kaksi viikkoa myöhemmin Bitcoinin arvo oli enää alle 600 dollaria, joten arvo laski 50 % alle kuukaudessa. Tätä laskua oli kuitenkin edeltänyt vielä suurempi nousu, sillä Bitcoin oli vielä marraskuun alussa arvoltaan 200 dollaria, joten arvonnousu huippulukemiin oli yli 500 %. (Bitcoincharts 2014)



Kuva 4. Arvonkehitys dollareissa 2013-2014 (Bitcoincharts 2014)

Rahan ominaisuuksiin kuuluu sen toiminta vaihdon välineenä ja sen arvon vakaa säilyminen. Syy, miksi Bitcoinia ei voi lukea viralliseksi rahaksi onkin arvon suuri vaihtelu. Bitcoiniin sidottuna ei voi siis tällä hetkellä säilyttää omaisuutta siinä uskossa, että omistuksen arvo olisi suurin pirtein sama pidemmän ajan kuluttua. Yalen yliopiston professori Robert Shiller ehdottaakin, että Bitcoinin ei tulisi keskittyä näiden rahan kahden ”väärän” ominaisuuden tavoitteluun. Hänen mielestään virtuaalivaluutan tulisi keskittyä rahan alkuperäiseen ideaan eli toimimiseen mittayksikkönä ja vaihdonvälineenä. Bitcoiniin voisi lisäksi sitoa jonkin omistuksen, esimerkiksi talon. (Shiller 2014)

5.3 Rikollinen käyttö

Rikolliset ovat olleet virtuaalivaluuttojen ensimmäisiä käyttäjiä. Rikolliset ovat hyödyntäneet laajasti virtuaalivaluuttoja, koska niiden avulla voidaan suorittaa maksuja anonyymisti, sekä liikuttamaan varallisuutta luotettavasti maasta toiseen ilman välikäsiä (Trautman 2014). Virtuaalivaluuttoja, kuten Bitcoinia ja Liberty Reserveä on käytetty hyvin paljon rikollisten välisessä kaupankäynnissä sekä rahanpesussa. Rahanpesussa laittomasti hankitun omaisuuden yhteys rikolliseen toimintaan pyritään poistamaan ja näyttämään siltä, että omaisuus on ansaittu rehellisesti. Perinteisillä valuutoilla rahanpesun suorittaminen on haasteellisempaa ja pankeilla on oikeus jäädyttää tilejä sekä ilmoittaa viranomaisille epäilyttävistä rahansiirroista. Virtuaalivaluuttojen avulla rikolliset pystyvät suorittamaan rahanpesua huomattavasti tehokkaammin ja pienemmällä kiinnijäämisen riskillä. Rikollinen käyttö on lisääntynyt viime aikoina ja viranomaiset ovat alkaneet pohtia keinoja sen vähentämiseksi lainsäädännön kautta. Yhdysvaltalaiset viranomaiset ovat käyttäneet myös pakkokeinoja rikollisuuden estämiseksi. Viranomaiset sulkivat Liberty Reserven vuonna 2013 rikollisten toiminnan takia, mutta rikolliset ovat siirtyneet muiden virtuaalivaluuttojen, kuten Bitcoinin käyttämiseen. (Brito & Castillo 2013, 25-27)

Vuonna 2011 Bitcoin nousi suuren yleisön tietoisuuteen The Silk Road -sivuston toimesta. Sivuston kautta saattoi ostaa huumeita ja aseita anonyymisti käyttäen bitcoineja maksuvälineenä. Yhdysvaltain viranomaiset puuttuivat kuitenkin tilanteeseen ja sulkivat sivuston pitkällisen painostuksen jälkeen. (Moore 2013) Sivustolle syntyi kuitenkin useita seuraajia ja bitcoineja käytetään edelleen useilla internetsivuilla rikollisten maksuvälineenä.

Bitcoinien kokonaisvaihdosta on kuitenkin arvioitu liittyvän rikolliseen toimintaan ainoastaan 1 %. (Liew 2013)

Bitcoin-verkko olettaa, että louhintaan vaadittava laskentateho kuuluu sille, joka onnistuu luomaan uusimman lohkon. Usein tämä pitääkin paikkaansa, mutta järjestelmässä on myös rikollisia, jotka pyrkivät käyttämään hyväksi muiden käyttäjien koneiden laskentatehoa. Nämä rikolliset ovat onnistuneet luomaan ja levittämään haittaohjelmia, joiden avulla he varastavat saastuneiden koneiden laskentatehoa omaan käyttöönsä. Tämänkaltaiset ”botnetit” ovat lisääntyneet bitcoinin arvon kehityksen myötä. Rehelliset louhijat investoivat suuria summia koneiden laskentatehon ostamiseen sekä sähkönkulutuksen kattamiseen. Rikolliset hyödyntävät rehellisen louhijoiden panostuksia lähes ilmaiseksi. Täten he voivat louhia bitcoineja suurella määrällä laskentatehoa, ilman että siitä aiheutuu heille merkittäviä kuluja. Kiinnijäämisen riski on alhainen, sillä anonymiteetti suojaa rikollisia vahvasti. Tutkijat ovat arvioineet, että rikollisten pyörittämät ”botnetit” ovat onnistuneet louhimaan bitcoineja useiden miljoonien dollareiden arvosta ja määrän odotetaan kasvavan kokoajan. (Huang 2014, 9-10)

5.4 Käytön kieltäminen ja säätelyn puuttuminen

Useat valtiot ympäri maailmaa ovat pohtineet Bitcoinin tilannetta lainsäädännön kannalta. Tällä hetkellä ei ole olemassa yhtenäistä linjaa Bitcoinin säätelylle maailmanlaajuisesti. On erimielisyyksiä siitä, pidetäänkö bitcoineja valuuttana, hyödykkeenä vai aivan jonain muuna. Tämä määrittely on erityisen tärkeää lainsäädännön kannalta, koska se vaikuttaa monien valtioiden lainsäädäntöjen tulkintaan, kuten verotukseen. Tämän lisäksi Bitcoinin anonymiteetti sekä transaktioiden globaalisuus aiheuttavat haasteita lainsäätäjille (Trautman 2014). Säätelyn puuttuminen heikentää Bitcoinin houkuttelevuutta kuluttajien sekä varsinkin yrittäjien kohdalla, sillä Bitcoin on erittäin altis erilaisille riskeille, kuten turvallisuus-, likviditeetti- ja operationaalisille riskeille. Säätelyn avulla voidaan edesauttaa Bitcoinin käyttöönottoa ja laajentumista tavallisten ihmisten ja yrittäjien keskuuteen ja parantaa järjestelmän luotettavuutta. (Holdgaard 2014)

Luottamusta Bitcoinia kohtaan sekä volatiliteettia voitaisiin parantaa oikeanlaisen säätelyn avulla. Tällä hetkellä bitcoinien vaihdantaan erikoistuneita kauppapaikkoja ei säädellä lainsäädännöllä avulla, mikä aiheuttaa epävarmuutta markkinoilla. Tarkemman säätelyn ja

ohjeistuksen avulla kuluttajien ja yrittäjien luottamus kauppapaikkoja kohtaan parantuisi ja sitä kautta käyttö lisääntyisi. Mikäli kuluttajien bitcoinien hankintaa helpotetaan ja nopeutetaan, sen leviäminen tulee kiihtymään ja käyttö kasvamaan. Säätelyn avulla voidaan myös vähentää Bitcoinin käyttöä rikollisessa toiminnassa (Moore 2013). Toisaalta on kuitenkin mahdollista, että Bitcoinin käyttö, hallussapito ja vaihtaminen kiellettäisiin kokonaan lainsäädännön avulla yksittäisissä valtioissa. (Holdgaard 2014)

Bitcoinin käytön lisääntyminen, sekä arvon kasvaminen voivat aiheuttaa vakavia ongelmia kansainvälisen talouden tasapainolle sekä valuuttakurssien vaihdannalle. Tämän lisäksi Bitcoinin taustalla ei ole valtiota säätelemässä sen toimintaa eikä Kansainvälisellä valuuttarahastolla ole mahdollisuuksia vaikuttaa Bitcoiniin (Trautman 2014). Bitcoinin avulla on mahdollista hyökätä heikkoja kansainvälisiä valuuttoja kohtaan ja heikentää niiden arvoa entisestään. Spekulatiivisessa hyökkäyksessä jokin taho haluaa hyödyntää heikkoa kansainvälistä valuttaa ja tehdä sen avulla voittoa lyhyellä aikavälillä. Tämän kaltaisessa tilanteessa hyökkääjä lainaa pankilta heikompaa valuuttaa ja vaihtaa sen edelleen paremmalla vaihtokurssilla vahvempaan valuuttaan. Tarkoituksena on ostaa heikkoa valuuttaa myöhemmin takaisin pienemmällä rahamäärällä, koska hyökkääjä odottaa heikomman valuutankurssin heikentyvän entisestään vahvemman suhteen. Mikäli vahvemmalla valuutalla saa enemmän heikkoa valuuttaa myöhemmin, hyökkääjä pystyy vaihtamaan lainansa takaisin heikompaan valuuttaan ja maksamaan lainansa takaisin heikommalla valuutalla sekä jäämään voitolle. Hyökkääjät tekevät voittoa pankkien kustannuksella ja heillä on entistä enemmän varallisuutta jatkaa hyökkäysten tekemistä ja pankeille vähemmän keinoja varautua niihin. Mikäli pankit eivät onnistu vastaamaan näihin hyökkäyksiin valuutan arvo heikkenee entisestään ja aiheuttaa epävakautta kansainvälisessä valuutanvaihdossa. (Plassaras 2013, 17-18)

Tällä hetkellä spekulatiiviset hyökkäykset ovat vasta teorian tasolla mahdollisia, mutta mikäli Bitcoinin käyttö ja arvo lisääntyvät tulevaisuudessa, sen mahdollisuus tulee kasvamaan. Spekulatiivisen hyökkäyksen riskiä on mahdollista pienentää kansainvälisellä lainsäädännöllä sekä Kansainvälisen valuuttarahasto IMF:n toimenpiteillä. Keskuspankeilla ja Kansainvälisellä valuuttarahastolla ei ole tällä hetkellä mahdollisuuksia estää tämän kaltaisia hyökkäyksiä, sillä näillä tahoilla ei ole olemassa bitcoineja valuuttavarannoissaan eikä Bitcoin ole Kansainvälisen valuuttarahaston jäsen. (Plassaras 2013, 17-18)

5.5 Deflaatiokierre

Useat asiantuntijat ja ekonomit ovat ennustaneet, että Bitcoin tulee kärsimään vakavasta deflaatiosta. Deflaatiossa Bitcoinin arvo kasvaisi huomattavasti ja kulutus pienentyisi sen seurauksena. Deflaatiossa käyttäjät eivät kuluta bitcoineja, vaan odottavat arvon nousua, sillä samalla määrällä bitcoineja saa enemmän hyödykkeitä tulevaisuudessa. Tämä johtaa siihen, että kukaan ei kuluta bitcoineja ja järjestelmästä tulee hyödytön. Tämän seurauksena koko Bitcoinin arvo saattaa romahtaa kulutuksen pienentyessä ja markkinoiden menettäessä uskonsa järjestelmään. (Barber, Boyen, Shi & Uzun, 2012, 404-405)

Osa ekonomeista kuitenkin puolustaa Bitcoinia ja ovat antaneet ennusteita siitä, että deflaatiosta ei tule suurta ongelmaa. Ennusteet perustuvat siihen, että mikäli markkinoilla on pitkän ajan kasvuodotuksia Bitcoinin arvolle, niin markkinat nostavat nykyisen markkinahinnan lähelle tätä tulevaisuuden odotusta. Lee antaa artikkelissaan esimerkin, että mikäli yhden bitcoinin arvon odotetaan olevan vuonna 2018 tuhat dollaria, niin markkinat nostavat nykyisen hinnan sen lähelle, kuten 950 dollariin. Tämän seurauksena ei tule olemaan pitkiä ajanjaksoja, jolloin käyttäjät odottaisivat hintojen nousua ja vähentäisivät kulutustaan. (Lee 2013)

6 TULEVAISUUS

Bitcoinin tulevaisuudesta ei ole yksimielistä näkemystä. Osa ekonomeista arvioi Bitcoinin käytön lisääntyvän entisestään ja bitcoineja on mahdollista käyttää maksuvälineenä yhä laajemmassa mittakaavassa jokapäiväisessä elämässä. Bitcoinin kehitykselle tulevaisuudessa voidaan nähdä kuitenkin erilaisia skenaarioita. Yksi vahva näkemys on se, että Bitcoin ei tule saamaan viralliseen rahaan tai valuuttaan verrattavissa olevaa muotoa. Sen sijaan Bitcoinilla olisi mahdollisuus tulevaisuudessa kehittyä ja yleistyä maksuvälineenä eli vaihdannan välineenä. (Scott 2014) Kehitykselle maksuvälineenä vaikuttaa kuitenkin se, miten Bitcoinin arvon vaihtelu tulee kehittymään. Mikäli arvon vaihtelu jatkuu tulevaisuudessa suurena, hankaloittaa se vakaan ja turvallisen vaihdon toteuttamista. Eräs ratkaisu tähän on jo kehittymässä sellaisessa muodossa, että käyttäjän ei itse tarvitsisi pitää bitcoineja hallussaan kuin vain vaihdon vievän ajan. Bitcoinit olisi mahdollista vaihtaa välittömästi maksun tai vaihdon toteuduttua viralliseksi vakaammaksi valuutaksi, ja näin arvon vaihtelun synnyttämä riski jäisi pieneksi. Tällaista vaihtopalvelua on alkanut kehittämään esimerkiksi kauppapaikka Coinbase. (Hardy, Descoteaux & Tang 2014) Yleistymistä maksuvälineenä puoltaa lisäksi se, että erilaiset kustannukset ovat bitcoineilla maksettaessa pienemmät, kuin esimerkiksi nykyisten luottokorttiyhtiöiden tai esimerkiksi PayPalin tarjoamat palvelut.

Toinen tulevaisuudenkuva on se, että Bitcoinista kehittyy vaihdonvälineenä nykyistä rahaakin edistyneempi menetelmä. Näkemys on, että Bitcoiniin voisi suoraan sitoa jotakin omaisuutta, kuten esimerkiksi talon omistuksen. Idea on, että kun tietty omaisuus sidotaan bitcoineihin, tulee omistuksen vaihdos todistetuksi bitcoinien vaihdolla. Tämä perustuu siihen, että yhden bitcoinin koko siirtohistorian voi nähdä sen lohkoketjusta. Näin omistuksien vaihdokset voi nähdä lohkoketjusta ja lisäksi ne ovat täysin julkisia. Tämä olisi etu esimerkiksi talokaupassa, sillä suuri osa talon tai asunnon kaupan kustannuksista syntyy siihen liittyvistä vaadittavista asiakirjojen laadinnoista ja lupaprosesseista koskien omistusta. Tehtäessä kauppa bitcoinien välityksellä näiden kulujen tilalle tulisi vain bitcoinien vaihdon siirtomaksu ja lohkoketjusta tulisi esiin uusi omistaja. Talokaupan lisäksi bitcoinien käyttö omistuksen vaihdossa sopisi myös muihin kauppoihin, esimerkiksi osakekauppaan. Tämä perustuu siihen, että kolmas osapuoli aiheuttaa aina ylimääräisiä kustannuksia jollakin tasolla ja etenkin rahamääräisesti arvokkaissa kaupoissa prosentuaalisestikin pieni kulu voi olla rahassa mitattuna suuri menoerä.

Omistuksen sitomista bitcoineihin kutsutaan myös Bitcoinin värittämiseksi. (Hodson 2014; Scott 2014)

Eräs näkemys tulevaisuudesta on se, että Bitcoinista tulee jonkin valtion virallinen valuutta. Skenaario on, että jokin valtio heikommalla taloudellisella infrastruktuurilla joutuu vaikeuksiin ja valtion virallinen valuutta menettää arvoansa huomattavasti. Tämä voi saada valtion kansalaiset vaihtamaan virallista valuuttaa bitcoineihin. Ajan kuluessa yhä useampi varastoi omaisuuttaan bitcoineihin ja lopulta valtio itse määrää bitcoinin virallisen käyttöönoton ja määrää viralliset maksut myös ulkomailta tehtäviksi bitcoinein. Tällaisessa tapauksessa Bitcoin menettää tarkoituksensa valtiosta riippumattomasta valuutasta tai rahasta. (Scott 2014)

On tullut esille myös pohdintaa siitä, onko Bitcoin olemassa tulevaisuudessa ollenkaan. Uskoa on siihen, että jokin virtuaalivaluutta tai -raha tulee olemaan myös tulevaisuudessa. Tämä raha voi olla Bitcoinin sijaan esimerkiksi jokin jo tällä hetkellä olemassa oleva rakenteeltaan kehittyneempi kryptoraha, kuten Litecoin. Pohdintaa on herännyt esimerkiksi siitä, rajoittavatko jotkin Bitcoinin luonteeseen perustuvat ominaisuudet sen yleistymistä tulevaisuudessa. Yksi näistä ominaisuuksista on bitcoinien kiinteä määrä, joka saavutetaan vuonna 2140. Epäily on, että kiinteä määrä olisi liian rajaava tekijä, koska se aiheuttaisi Bitcoinin arvon noustessa deflaatiota. Deflaation seurauksena käyttäjät vähentävät bitcoinien kuluttamista ja kaupankäynti pienenee. Ongelma voidaan tosin ratkaista osittain siten, että bitcoininit voi jakaa hyvin pieniin osiin, ja näin vaihto olisi mahdollista laajemmassakin mittakaavassa. (Bitcoin 2013) Muilla kryptorahoilla on useimmiten myös kiinteä lopullinen määrä, mutta esimerkiksi Litecoinilla raja on 84 miljoonassa kappaleessa Bitcoinin 21 miljoonaa vastaan. Epäilyjä on kohdistunut myös Bitcoinin hitauteen eli siihen, että siirtojen varmistus kestää noin 10 minuuttia. Esimerkiksi Litecoinilla kesto on ainoastaan 2,5 minuuttia. (Litecoin 2014) Bitcoinin yhtenä heikkona puolena voi nähdä myös sen verkon ylläpitämisen vaatiman laskentatehon energiankulutus. Laskentateho vaatii energiaa ja on suuri menoerä koko järjestelmän ylläpidolle. Arvioiden mukaan laskentatehon aiheuttamat kulut olisivat tällä hetkellä noin 10 % Bitcoinin markkina-arvosta. Esimerkiksi, jos arvo olisi 1,7 miljardia dollaria, kulut olisivat 170 miljoonaa dollaria. (Larimer 2014) Bitcoinin kaltainen kryptoraha Peercoin markkinoi itseään energiatehokkaampana mallina Bitcoinista, mutta kuitenkin turvallisuuden säilyessä samalla tasolla. (Peercoin 2014; Kerner 2013)

7 JOHTOPÄÄTÖKSET

Bitcoin on vertaisverkkoon pohjautuva virtuaalivaluutta, joka kehitettiin vuonna 2008. Bitcoin-verkko hyödyntää kryptografiaa rahan siirrossa, uusien kolikoiden luonnissa ja verkon ylläpitämisessä. Järjestelmässä ei ole mukana kolmatta osapuolta välittäjänä, vaan toiminta perustuu käyttäjien ylläpitämään hajautettuun verkkoon. Järjestelmää ylläpitäviä käyttäjiä kutsutaan louhijoiksi. Louhijat käyttävät omien laitteistojensa laskentatehoa laskutoimitusten suorittamiseen ja kilpailevat muita louhijoita vastaan uusien lohkojen luonnissa. Lohko ja lohkoketju ovat verkon toiminnan perustekijöitä, joihin tallentuu kaikkien bitcoinien siirtohistoria julkisesti nähtäväksi. Bitcoineja voi hankkia joko louhimalla tai ostamalla niitä erilaisista kauppapaikoista verkossa. Bitcoineilla on kiinteä määrä ja yhden bitcoinin voi jakaa hyvin pieniin osiin.

Bitcoinin edut verrattuna perinteisiin maksumenetelmiin?

Tutkimuksemme tarkoituksena oli selvittää Bitcoinin etuja verrattuna perinteisiin maksumenetelmiin, kuten pankkien, luottoyhtiöiden ja muiden maksuvälityspalveluihin tarjoamiin palveluihin. Tunnistimme tutkimuksemme edetessä Bitcoinin eduiksi seuraavat ominaisuudet: anonymiteetti, edullisuus, arvon määräytyminen sekä nopeat transaktiot. Tutkimuksemme mukaan edullisuus ja nopeus ovat painoarvoltaan suuremmassa roolissa, kuin anonymiteetti ja arvon määräytyminen, sillä kahteen jälkimmäiseen liittyy myös osaltaan haasteita ja ongelmia.

Pankit, luottoyhtiöt ja maksuvälitysyhtiöt vaativat asiakkailtaan usein henkilötietojen luovuttamista, jotta käyttäjät voivat aloittaa palveluiden käytön. Perinteisillä maksumenetelmillä anonymiteetin säilyttäminen on vaikeaa ilman laittomien keinojen käyttämistä ja kolmannet osapuolet pystyvät seuraamaan transaktioiden tekemistä ja selvittämään niiden osapuolet. Bitcoinin avulla käyttäjät pystyvät säilyttämään anonymiteetin transaktioiden suorittamisessa ja pystyvät siirtämään varallisuutta ilman, että kukaan kolmas osapuoli pystyy varmistamaan heidän henkilöllisyyttään. Rikolliset ovat kuitenkin hyödyntäneet anonymiteetin tuomaa suojaa rikollisessa toiminnassa.

Bitcoinin suurimpia vahvuuksia perinteisiin maksumenetelmiin on edullisuus. Perinteisillä menetelmillä maksettaessa kolmannet osapuolet veloittavat siirtomaksuja transaktioiden suorittamisesta ja palveluiden käyttämisestä. Luottokortilla maksaessa kustannukset ovat keskimäärin 2-3 % transaktion loppusummasta ja siirrettäessä rahaa ulkomaille kustannukset voivat nousta jopa kymmeneen prosenttiin. Bitcoinin avulla transaktiot käyttäjien välillä ovat huomattavasti edullisempia kuin perinteisillä menetelmillä. Transaktioihin sisältyy ainoastaan vapaaehtoinen siirtokustannus, jonka suuruus riippuu käyttäjästä itsestään. Bitcoinin käyttöönotosta maksuvälineeksi on hyötyä myös pienille yrittäjille, koska Bitcoinin avulla voidaan välttää siirtokustannusten aiheuttaman maksut luottokorttiyhtiöille sekä vähentää maksamattomien asiakkaiden määrää.

Bitcoinilla ei ole olemassa kolmatta osapuolta, kuten keskuspankkia säätelemässä Bitcoinin toimintaa. Keskuspankit ja Kansainvälinen valuuttarahasto säätelevät tarkkaan perinteisten valuuttojen toimintaa ja vaihdantaa. Kolmannet osapuolet voivat vaikuttaa kansainvälisiin valuuttakursseihin erilaisilla taloudellisilla toimenpiteillä ja säätelyllä. Keskuspankeilla on myös oikeus laskea liikkeelle lisää rahaa markkinoille mikä aiheuttaa inflaatiota eli hintojen nousua. Bitcoinilla ei ole olemassa tahoa, joka laskisi liikkeelle bitcoineja. Bitcoineja syntyy ennalta määrätty määrä keskimäärin kymmenen minuutin välein ja kokonaismäärä on rajattu 21 miljoonaan bitcoiniin. Tämän jälkeen uusia bitcoineja ei enää synny markkinoille. Bitcoinin avulla voidaan välttää inflaation toteutuminen ja arvon määräytyminen perustuu täysin markkinoiden kysyntään ja tarjontaan.

Bitcoinin etuja perinteisiin maksumenetelmiin verrattuna on transaktioiden nopea välittyminen. Perinteisillä menetelmillä transaktioiden suorittaminen käyttäjien välillä kestää pahimmillaan useista päivistä viikkoihin. Bitcoinien siirtäminen käyttäjältä toiselle on äärimmäisen nopeaa suorittaa globaalissa mittakaavassa. Bitcoinin toiminta on yhtä nopeaa, oli käyttäjien välimatka mikä tahansa. Transaktiot ovat käytännössä välittömiä käyttäjien välillä, mutta ne varmennetaan järjestelmään keskimäärin kymmenen minuutin välein.

Minkälaisia ongelmia ja haasteita Bitcoiniin liittyy?

Bitcoinilla on kuitenkin ongelmia ja haasteita verrattuna perinteisiin menetelmiin. Osa ongelmista liittyy kolmannen osapuolen puuttumiseen. Yksi Bitcoinin luonteesta johtuva ongelma on se, että bitcoinien siirrot ovat peruuttamattomia. Tämä altistaa ostajan suuremmalle riskille kuin esimerkiksi maksaessa luotolla, jolloin on mahdollisuus vielä maksun peruutukseen myöhemmin. Kolmannen osapuolen puuttuminen vaikuttaa myös siinä tilanteessa, jossa bitcoinien omistaja hävittää tilitietonsa. Mikäli tiedot ovat lopullisesti hävinneet, ovat myös käyttäjän bitcoinit lopullisesti menetetty. Jos käyttäjä sen sijaan säilyttäisi rahojaan pankissa ja käyttäisi maksamiseen tilisiirtoja, olisi hänellä pääsy tilillensä aina jollakin keinolla, viimeistään asioimalla pankin konttorissa ja todistamalla henkilöllisyytensä.

Suurimmat ongelmat Bitcoinin kohdalla liittyvät turvallisuuteen. Ongelmia aiheuttavat hakkereiden tekemät varkaudet, jotka ovat kohdistuneet ensisijaisesti kauppapaikkoihin. Varkauksien myötä bitcoinien käyttäjät ovat menettäneet virtuaalivaluutan historian ensimmäisten viiden vuoden aikana useiden satojen miljoonien dollareiden edestä bitcoineja. Perinteisillä maksuvälityspalveluilla turvallisuudesta on yleensä vastuussa kolmas osapuoli yhdessä käyttäjän toiminnan kanssa. Lisäksi erilaiset vakuutusmahdollisuudet koskien virallista rahaa ovat huomattavasti kattavammat kuin Bitcoinilla. Monet Bitcoin-kauppapaikat ovat panostaneet yhä enemmän turvallisuuteen. Turvallisuudessa Bitcoin häviää vielä pankkien lisäksi PayPaylin kaltaiselle maksupalvelulle, joka tarjoaa turvallisen säilytyksen ja mahdollisuuden ostajalle tehdä kauppaa nimettömänä PayPalin kautta. Teoreettinen uhka on myös 51 % -hyökkäykselle, mutta toistaiseksi tämän uhan kasvaessa on Bitcoin-yhteisö vastannut siihen nopeasti, mikä kertoo järjestelmän hyvästä itsesäätelykyvystä. Bitcoinin toiminnasta johtuva ongelma on kaksinkertainen käyttö, jonka kaltaista ongelmaa muilla maksumenetelmillä ei ole. Tämän lisäksi itse verkkoa uhkaa niin kutsuttu ”dust transactions”, joissa aiheutetaan tarkoitetusti haittaa verkon toiminnalle ja hidastetaan sitä. ”Dust transactions” -hyökkäys on mahdollista, koska bitcoineija on mahdollista siirtää hyvin pienissä osissa. Muilla menetelmillä siirtoa tehdessä alaraja on varsin korkea ja viimeistään korkeammat siirtokustannukset tekevät tällaisen haitanteon kannattamattomaksi.

Eräs ongelma, joka Bitcoinia on haitannut sen alkutaipaleella, on arvon heilahtelu. Tämä luo arvon säilymisen ongelman eli sen, että bitcoiniin ei voi turvallisesti varastoida omaisuuttaan, sillä olettamuksella, että sillä olisi edes lähestulkoon sama arvo kuin talletushetkellä. Myös nykyisissä virallisissa valuutoissa esiintyy arvon vaihtelua, mutta vaihtelu ei ole samaa tasoa, mitä Bitcoinilla on jopa päivittäin. Arvon heilahtelu on myös yksi suurimmista syistä, miksi erilaiset pankit ja rahoituslaitokset ovat varoitelleet Bitcoinin käytöstä. Arvon säilymistä pidemmällä aikavälillä uhkaa Bitcoinin deflaatio-ongelma. Koska bitcoineja on rajattu kiinteä määrä, voi lisääntynyt käyttö ja arvon nousun odotus aiheuttaa deflaatiota, joka taas voi jossain vaiheessa romahduttaa rahan. Perinteisellä rahalla rahan painaminen mahdollistaa terveen inflaation taloudellisen kasvun aikanakin.

Bitcoinin luoma anonymiteetti ja säätelyn puuttuminen on tehnyt sen suosituksi rikollisessa käytössä. Rikollisen käytön osuus on prosentuaalisesti pientä, mutta on saanut paljon julkisuutta. Bitcoinia on käytetty esimerkiksi huume- ja asekauppaan ja lisäksi osana rahanpesua. Rikollisuutta on esiintynyt myös itse bitcoinien luonnissa, jossa rikolliset ovat onnistuneet varastamaan laskentatehoa niiden oikeilta omistajilta. Rahamäärissä mitattuna perinteisen rahan käyttö rikollisessa toiminnassa on kuitenkin maailmanlaajuisesti huomattavasti yleisempää kuin bitcoinien. Bitcoin on kuitenkin säätelyn ulkopuolella eikä sen valvonta ole samalla tavoin mahdollista kuin perinteisellä rahalla. Tämän vuoksi rikollinen käyttö herättää epäluottamusta virtuaalivaluutan käyttöön ja voi aiheuttaa sen käytön kieltämisen esimerkiksi valtiokohtaisesti.

Taulukko 1. Yhteenveto Bitcoinin eduista, ongelmista ja haasteista

Edut	Ongelmat ja haasteet
• Edullisuus käyttäjille ja yrittäjille • Erittäin nopeat transaktiot • Anonymiteetti • Inflaation puuttuminen • Maailmanlaajuinen maksumenetelmä	• Hyökkäykset ja varkaudet • 51 % -hyökkäykset • Rikollinen käyttö • Arvon säilyminen • Deflaatiokierre • Säätelyn puuttuminen ja mahdollinen kieltäminen • Luottamus tulevaisuuteen

Miten Bitcoin tulee kehittymään tulevaisuudessa?

Tutkimuksen perusteella voi nähdä kaksi varsin mahdollista skenaariota Bitcoinille tulevaisuudessa. Lähitulevaisuutta on vaikea ennustaa, sillä esimerkiksi lainsäädäntö voi vaikuttaa huomattavasti Bitcoinin leviämiseen. Bitcoinin tulevaisuus riippuu hyvin paljon Yhdysvaltojen, Kiinan ja muiden kehittyneiden valtioiden kannanotoista sen käyttöön ja kuinka ne tulevat säätelemään sitä. Pidemmällä aikavälillä sen sijaan yksi todennäköinen skenaario on Bitcoinin yleistyminen, kuitenkaan ei rahana, vaan vaihdannan välineenä. Tämä tarkoittaa sitä, että bitcoineja ei hankita omaisuuden säilyttämiseksi, vaan pelkkien maksutapahtumien tai siirtojen suorittamiseen. Tällä tavoin bitcoinien siirtojen edullisuus tulee hyödynnettyä samoin kuin anonymiteetti, mutta sen arvon säilymisen ongelma minimoidaan. Tämä kehitys vaatii osaltaan vielä kauppa- ja vaihtopaikkojen kehittymistä jonkin verran. Bitcoinin suosio ja levinneisyys ovat olleet kasvussa jo nyt. Turvallisuuden kehittyessä ja luotettavuuden lisääntyessä säätelyn seurauksena myös käytön voi odottaa lisääntyvän edelleen. Bitcoin ei siis tulisi kuitenkaan korvaamaan perinteistä rahaa, joka mahdollistaisi omaisuuden turvallisen säilyttämisen

Toinen mahdollinen skenaario tulevaisuudessa pidemmällä aikavälillä on, että Bitcoinin korvaa jokin toiminnaltaan kehittyneempi virtuaalivaluutta ja itse Bitcoinin käyttö vähenee. Tämä ajatus perustuu siihen, että virtuaalivaluutan käytön yleistyessä myös kilpailu valuuttojen välillä

lisääntyy. Tämä johtaa siihen, että tällä hetkellä vielä pienempien rahojen kehittyneemmät ominaisuudet puoltavat niiden kasvua ohi Bitcoinin. Esimerkiksi Litecoinilla siirtojen nopeampi varmentaminen ja suurempi kolikoiden kiinteä määrä ovat positiivisia ominaisuuksia. Litecoinilla on jo varsin suuri käyttäjäkunta tälläkin hetkellä, joten sen yleistyminen on hyvin mahdollista. Toisaalta eräs Bitcoinin heikkous tälläkin hetkellä on sen verkon ylläpitämisen vaatima laskentateho ja sen viemä energiamäärä. Esimerkiksi Peercoin tarjoaa mahdollisuuden yhtä turvalliseen verkkoon, mutta huomattavasti pienemmällä laskentateholla. Tulevaisuudessa laskentatehon lisääntyessä, voi tämä ominaisuus korostua yhä enemmän.

Näiden lisäksi on myös esitetty näkemyksiä, että Bitcoinista kehittyisi rahaa suurempi. Bitcoiniin pystyisi sitomaan omaisuutta, kuten asunnon tai osakkeet. Bitcoinit ”väritettäisiin” ja omistuksen vaihtuminen käyttäjien välillä näkyisi lohkoketjussa. Tämä vähentäisi mahdollisesti kolmannen osapuolen käytöstä johtuvia ylimääräisiä kuluja, kuten talokaupassa erilaisten asiakirjojen ja lupahakemusten laadinnasta johtuvia kuluja. Tutkimuksemme perusteella päädyimme siihen, että tällainen kehitys on epätodennäköistä, sillä se vaatisi useiden eri osapuolien hyväksynnän ja lainsäädännön muuttamista.

Jatkotutkimuskohteita

Bitcoinia ei ole juurikaan tutkittu vielä kustannusjohtamisen näkökulmasta. Jatkotutkimuksena olisi mielenkiintoista tutkia Bitcoinin käytön todellisia kustannuksia yritystasolla. Tutkimuksessa voitaisiin tutkia kustannushyötyjä pienyrityksissä, jotka hyväksyvät bitcoineja maksuvälineenä.

LÄHTEET

Androulaki, E., Karame, G., Roeschlin, M., Scherer, T. & Capkun, S. 2013. Evaluating User Privacy in Bitcoin. Finacial Cryptography and Data Security. s. 34-51.

Arias, M. & Yongseok, S. 2013. There are two sides to every coin—even to the bitcoin, a virtual currency. The Regional Economist October. Saatavissa: https://www.stlouisfed.org/publications/re/articles/?id=2427

Barber, S., Boyen, X. Shi, E. & Uzun, E. 2012. Bitter to Better – How to Make Bitcoin a Better Currency. Financial Cryptography and Data Security. s. 399-415.

Bershidsky, L. 2014. Did Ukrainians Almost Take Over Bitcoin? Bloomberg. [WWW-dokumentti]. [viitattu 27.03.2014]. Saatavissa: http://www.bloombergview.com/articles/2014-01-14/did-ukrainians-almost-take-over-bitcoin-

Bitcoin. 2014 [WWW-dokumentti]. [viitattu 20.03.2014]
Saatavissa: https://bitcoin.org/en/faq

Bitcoin. Bitcoin Wiki 2014a. Avoin tietosanakirja. [viitattu 20.03.2014]. Saatavissa: https://en.bitcoin.it/wiki/Blockchain

Bitcoin. Bitcoin Wiki 2014b. Avoin tietosanakirja. [viitattu 20.03.2014]. Saatavissa: https://en.bitcoin.it/wiki/Mining

Bitcoin. Bitcoin Wiki 2014c. Total Bitcoin over time. Saatavissa: https://en.bitcoin.it/wiki/File:Total_bitcoins_over_time_graph.png

Bitcoin. Bitcoin Wiki 2014d. Avoin tietosanakirja. [viitattu 20.03.2014]. Saatavissa: https://en.bitcoin.it/wiki/Bitcoin

Bitcoincharts. 2014. Bitcoinin arvon kehittyminen. Bitcoincharts. [WWW-dokumentti].[viitattu 29.3.2014] Saatavissa: http://bitcoincharts.com/charts/bitstampUSD#rg360ztgCzm1g10zm2g25

Bitcoinexaminer. 2014. Mining pool growth startles Bitcoin community for fear of a 51% attack [UPDATED]. Bitcoinexaminer. [WWW-dokumentti]. [viitattu 27.03.2014]. Saatavissa: http://bitcoinexaminer.org/mining-pool-growth-startles-bitcoin-community-for-fear-of-a-51-attack/

Blockchain. Blockchain 2014. Wikileaks bitcoin-accoount. Saatavissa: http://blockchain.info/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

Bradbury, D. 2013. The problem with Bitcoin. *Computer Fraud & Security*. Vol 2013. nro 11. s. 5-8

Brito, J. & Castillo, A. 2013. Bitcoin: A Primer for Policymakers. Mercatus Center: Geroge Mason University. s.43.

Coinmarketcap. 2014. Crypto-Currency Market Capitalizations. [WWW-dokumentti]. [viitattu 19.03.2014]. Saatavissa: https://coinmarketcap.com/

Drainville, D. 2012. An Analysis of the Bitcoin Electronic Cash System. University of Waterloo. s. 45.

Eyal, 1. & Sirer, G. 2013. Majority is not Enough: Bitcoin Mining is Vulnerable. Cornell University. s. 17.

Farrel, M. 2007. Saving On Credit Card Processing Fees. Forbes. [WWW-dokumentti] [viitattu 25.3.2014]. Saatavissa: http://www.forbes.com/2007/02/20/visa-americanexpress-globalpayment-ent-fin-cx_mf_0220creditcard.html

Ghash. 2014. Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power. Ghash. [WWW-dokumentti]. [viitattu 27.03.2014]. Saatavissa: https://ghash.io/ghashio_press_release.pdf

Hardy, R., Descotaux, D. & Tang, T. 2014. THE BITCOIN DILEMMA. Canadian *business*. Vol. 87. nro. 2. s. 22-22.

Hobson, D. 2013. What is bitcoin? XRDS: Crossroads, The ACM Magazine for Students 20.1 s. 40-44.

Hochtein, M. 2014. Why Bitcoin Matters for Bankers. American Bankers Magazine. [WWW-dokumentti]. [viitattu 27.3.2014]. Saatavissa: http://www.americanbanker.com/magazine/124_02/why-bitcoin-matters-for-bankers-1065590-1.html

Hodson, H. 2014. Bitcoin moves beyond money. *New Scientist*. Vol. 220. nro 2945. s. 24-24.

Holdgaard, L. 2014. An exploration of the Bitcoin ecosystem. IT University of Copenhagen, E-Business. Pro-gradu tutkielma. Saatavissa: http://bitcoin-expert.net/wp-content/uploads/2014/01/Thesis.pdf

Huang, D. 2014. Profit-Driven Abuses of Virtual Currencies. University of California, San Diego. s. 14.

Karame, G., Androulaki, E. & Srdjan, C. 2012. Double-spending fast payments in bitcoin. CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security. s 906-917.

Kerner, Sean M. 2013. Bitcoin has Company on Cryptocurrency Stage. eWeek. [WWW-dokumentti]. [viitattu 12.04.2014]. Saatavissa: http://www.eweek.com/cloud/slideshows/bitcoin-has-company-on-cryptocurrency-stage.html

Kauko, K. 2011. Lyhyt johdatus rahaan. Suomen Pankki. [WWW-dokumentti]. [viitattu 19.03.2014]. Saatavissa: http://www.suomenpankki.fi/fi/julkaisut/selvitykset_ja_raportit/bof_online/Documents/BoF_Online_05_2011.pdf

Larimer, D. 2014. The Hidden Costs of Bitcoin. Let's Talk Bitcoin. [WWW-dokumentti]. [viitattu 29.3.2014]. Saatavissa: http://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security/#.UzanMRBallE

Laurent, L. 2014. UK lawyer says 'hundreds' ready for bitcoin class action. Reuters. [WWW-dokumentti]. [viitattu 28.03.2014]. Saatavissa: http://uk.reuters.com/article/2014/03/05/uk-bitcoin-lawsuit-idUKBREA231W820140305

Lee, T. 2013. Bitcoin Doesn't Have a Deflation Problem. Forbes. [WWW-dokumentti]. [viitattu 21.03.2014]. Saatavissa: http://www.forbes.com/sites/timothylee/2013/04/11/bitcoin-doesnt-have-a-deflation-problem/

Lee, T. 2011. How Private Are Bitcoin Transactions? Forbes. [WWW-dokumentti]. [viitattu 20.03.2014]. Saatavissa: http://www.forbes.com/sites/timothylee/2011/07/14/how-private-are-bitcoin-transactions/

Liew, J. 2013. "Think Big.Move Fast". Lightspeed Venture Partners. [WWW-dokumentti]. [viitattu 25.03.2014]. Saatavissa: http://lsvp.com/2013/08/15/about-half-a-percent-of-bitcoin-transactions-are-to-buy-drugs/

Litecoin. 2014. Litecoin. [WWW-dokumentti]. [viitattu 29.03.2014]. Saatavissa: https://litecoin.org/

Mankiw, G. 2002. Macroeconomics (5th ed.) New York: Worth Publisher. S.547

Mansfield-Devine, S. 2013. Massive Bitcoin thefts and seizures leave many users nervous and poorer. *Computer Fraud & Security*. Vol 2013. nro 12. s. 1-3.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. & Savage, S. 2013. A fistful of bitcoins: characterizing payments among men with no names. IMC '13 Proceedings of the 2013 conference on Internet measurement conference. s. 127-139.

Miller, J. 2014. Bitcoin vault offering insurance is 'world's first'. BBC. [WWW-dokumentti]. [viitattu 27.3.2014]. Saatavissa: http://www.bbc.com/news/technology-25680016

Moore, Tyler. 2013. The promise and perils of digital currencies. *International Journal of Critical Infrastructure Protection*. Vol 6. nro 3. s. 147-149.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electornic Cash System. Saatavissa: https://bitcoin.org/bitcoin.pdf

Peercoin. 2014. Peercoin. [WWW-dokumentti]. [viitattu 29.3.2014]. Saatavissa: http://www.peercoin.net/

Plassaras, N. 2013. Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF. *Chicago Journal of International Law*, vol 14. s. 26.

Pryke, J. 2013. Visualising the incredible rise of remittances. [WWW-dokumentti] [viitattu 27.3.2014]. Saatavissa: http://devpolicy.org/in-brief/visualising-the-incredible-rise-of-remittances-20130807-1/

Ron, D. & Shamir, A. 2013. Quantitative Analysis of the Full Bitcoin Transaction Graph. Finacial Cryptography and Data Security. s. 6-24.

Rusli, E. 2014. Latest Bitcoin Craze? Actual Bank Vaults; Startup Xapo Raises $20 Million to Store Digital Currency Underground. Wall Street Journal. [WWW-dokumentti]. [viitattu 28.03.2014]. Saatavissa: http://online.wsj.com/news/articles/SB10001424052702303546204579437462303753346

Shiller, Robert J. 2014. In Search of Stable Electronic Currency. New York Times. [WWW-dokumentti]. [viitattu 17.3.2014] Saatavissa: http://www.nytimes.com/2014/03/02/business/in-search-of-a-stable-electronic-currency.html?_r=0

Scott, B. 2014. Many possible paths. *New Scientist*. Vol. 221. nro 2955. s. 21-21.

Skrill. 2014 [WWW-dokumentti]. [viitattu 19.03.2014]. Saatavissa https://www.skrill.com/en/

Suomen Pankki. 2014.[WWW-dokumentti]. [viitattu 19.03.2014]. Saatavissa: http://www.suomenpankki.fi/fi/suomen_pankki/ajankohtaista/muut_uutiset/pages/uutinen_140114.aspx

Trautman, L. 2014. Virtual Currencies: Bitcoin & What not after Liberty Reserve, Silk Road, and Mt.Gox? *Richmond Journal of Law and Technology*. Vol. 20. nro 4. s.88

Visa. 2014. Tietoja meistä. [WWW-dokumentti]. [viitattu 19.03.2014]. Saatavissa: http://www.visa.fi/fi/tietoja-meista/

Vitt, D. 2013. Breaking Bitcoin: Does Cryptocurrency Exchange Activity Lead to Increased Real Activity Outside Cryptocurrency Exchanges? Florida International University. s. 36

Ven. 2014. [WWW-dokumentti]. [viitattu 19.03.2014] Saatavissa: http://ven.vc/about

Wagstaff, J. 2014. Mind your wallet: why the underworld loves bitcoin. Reuters. [WWW-dokumentti]. [viitattu 28.3.2014]. Saatavissa: http://www.reuters.com/article/2014/03/14/us-bitcoin-criminals-insight-idUSBREA2D09820140314

Wiener, H., Zelnik, J., Tarshish, I. & Rodgers, M. 2013. Chomping at the Bit: U.S. Federal Income Taxation of Bitcoin. *Jornal of Taxation of Financial Product*. Vol 73. nro 4. s.35-47.