Johannes Stenberg

BITCOIN ELEKTRONISESSA LIIKETOIMINNASSA – HAASTEET JA MAHDOLLISUUDET

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Stenberg, Johannes
Bitcoin elektronisessa liiketoiminnassa – haasteet ja mahdollisuudet
Jyväskylä: Jyväskylän yliopisto, 2016, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Seppänen, Ville

Digitaalinen raha ja maksujärjestelmä Bitcoin on herättänyt paljon huomiota viime vuosina. Elektronisen liiketoiminnan toimijat ovat kuitenkin olleet hitaita hyväksymään Bitcoinin maksuvälineenä. Syynä tähän on sen kyseenalainen maine ja riskit. Tämän kandidaatintutkielman tarkoituksena oli selvittää Bitcoinin hyödyt ja haitat elektronisessa liiketoiminnassa. Toisena tavoitteena oli selvittää, miten Bitcoinia on ehdotettu kehitettäväksi, jotta siitä tulisi varteenotettavampi maksuväline. Tutkimusmenetelmänä käytettiin kirjallisuuskatsausta. Bitcoinin tärkeimmiksi hyödyiksi havaittiin muun muassa alhaiset transaktiokustannukset etenkin mikromaksumarkkinoilla ja sen pohjalla olevan teknologian tarjoamat jatkokehitysmahdollisuudet. Suurimmiksi haitoiksi havaittiin valuutan taloudelliset heikkoudet, eli korkea volatiliteetti ja deflaatio, sekä tietoturvariskit kauppapaikoilla, mitkä hankaloittavat sen käyttöä maksuvälineenä. Bitcoinille löydettiin kuitenkin lähdekirjallisuuden pohjalta useita kehitysehdotuksia. Keskeisimpänä havaintona huomattiin, että nykyisellään Bitcoinin heikkoudet haittaavat sen laajempaa käyttöä elektronisessa liiketoiminnassa ja jättävät sen vahvuudet osittain varjoonsa.

Asiasanat: Bitcoin, e-commerce, elektroninen kaupankäynti, kryptovaluutat, maksujärjestelmät

ABSTRACT

Stenberg, Johannes
Bitcoin in e-commerce – challenges and opportunities
Jyväskylä: University of Jyväskylä, 2016, 31 p.
Information Systems, Bachelor's thesis
Supervisor: Seppänen, Ville

The digital money and payment systems Bitcoin has caused a lot of speculation in the past few years. However, the electronic commerce has been slow in accepting Bitcoin as a way of payment due to its dubious fame and inherent risks. The purpose of this Bachelor's thesis was to find the risks and benefits of Bitcoin in the field of electronic commerce. The secondary purpose of the study was to find out what kind of improvement suggestions have been made to make Bitcoin a more feasible form of payment. The most crucial benefits found were low transaction costs particularly in the micropayment market, and the further development opportunities presented by the technology that Bitcoin is based on. The greatest risks found were the economic weaknesses of the currency, which are high volatility and deflation, and security risks in the Bitcoin marketplaces, which make it difficult to utilize as a form of payment. However, based on the source material, multiple improvement suggestions were found. The most central finding was that currently the weaknesses of Bitcoin hinder its usage in e-commerce and partially underscore its strengths.

Keywords: Bitcoin, e-commerce, electronic commerce, cryptocurrencies, payment systems

KUVIOT

SISÄLLYS

1 JOHDANTO

Kehittyvälle tietoyhteiskunnalle on olennaista se, että yhä useampi palvelu siirtyy verkon välityksellä suoritettavaksi. Tätä myöten monille elektronisen liiketoiminnan toimijoille koituu sekä uusia haasteita että myös mahdollisuuksia toteuttaa liiketoimintaansa. Tämän muutoksen myötä asiakkaat ovat helpommin saatavilla, mutta perinteiset kaupankäyntimenetelmät eivät enää välttämättä toimi niin tehokkaasti kuin ennen. Uudet innovaatiot ja teknologiat ovat muuttaneet maailmaamme merkittävästi, ja uusia toimintatapoja tarvitaan.

Eräänä esimerkkinä palvelun digitalisoitumisesta voisi mainita postivälityksen. Ennen postivälitys oli yksin postilaitoksen vastuulla. Mutta sitten keksittiin sähköposti ja myöhemmin muut digitaaliset keinot välittää viestejä, joista merkittävämpänä nykyesimerkkinä mainittakoon sosiaalinen media, sekä e-laskut. On siis varsin loogista tätä ajatuskaavaa seuraten olettaa, että myös raha voisi kokea samanlaisen kehityskulun. Vuoden 2008 finanssikriisin seurauksena moni taho alkoi kyseenalaistaa keskitettyä rahanhallintaa. Tästä ilmapiiristä esiin nousikin Bitcoin, hajautettu digitaalinen valuutta ja maksujärjestelmä, joka on synnystään saakka jakanut varsin paljon mielipiteitä ja ollut suuri spekuloinnin kohde. Mediassa Bitcoin on saanut osakseen etenkin huonoa mainetta, sillä sitä on sen hajautetun luonteen vuoksi hyödynnetty myös rikollisessa toiminnassa (ks. Christin, 2012).

Sana ”Bitcoin” viittaa siis sekä maksujärjestelmään että valuuttaan. Selvyyden vuoksi käytetään tässä tutkielmassa tästä edespäin termiä ”Bitcoin” isolla alkukirjaimella, kun puhutaan maksujärjestelmästä tai yleisesti teknologiasta, ja termiä ”bitcoin” pienellä alkukirjaimella, kun puhutaan yksinomaan valuutasta.

Bitcoin on vuonna 2009 Satoshi Nakamoto -salanimeä käyttävän henkilön tai henkilöiden kehittelemä digitaalinen valuutta ja maksujärjestelmä, joka perustuu vertaisverkon välityksellä tehtäviin maksuihin käyttäjien välillä. Bitcoinia ei siis ohjaa mikään taloudellinen instituutio kolmantena osapuolena maksutapahtumissa, joten bitcoinia voisi kuvailla hajautetuksi valuutaksi. Kaikki bitcoineilla tehtävät transaktiot ovat julkisia, vain osapuolet ovat salattuja. Jokainen maksutapahtuma tallennetaan eräänlaiseen julkiseen tilikirjaan, eli

blockchainiin, jossa jokainen bitcoineilla suoritettu transaktio on tallessa. (Nakamoto, 2008.)

Muutamat elektroniset kaupankävijät ovat jo huomanneet Bitcoinin potentiaalin. Vaihtelevasta menestyksestään ja jopa tittelistään epäonnistuneena valuuttana huolimatta bitcoinin käyttö on kasvanut, ja elektronisen liiketoiminnan piiriin on muodostunut aivan uudenlaisia Bitcoiniin perustuvia markkinoita (White, 2014). Lisäksi elektronisten maksujärjestelmien alati kehittyessä on tullut kysyntää sille, että maksuja voisi suorittaa verkossa helpommin ja ilman välikäsiä (Sumanjeet, 2009).

Tämän tutkielman tarkoituksena onkin tarkastella tätä varsin ajankohtaista aihetta, sillä Bitcoinilla voi olla suotuisia tulevaisuudennäkymiä elektronisessa liiketoiminnassa, mutta toisaalta se saattaa myös epäonnistua. Tutkielmassa ei oteta mitään ideologista kantaa eikä tarkastella esimerkiksi Bitcoinin sosioekonomisia vaikutuksia, vaan tavoitteena on tarkastella Bitcoinia elektronisessa liiketoiminnassa mahdollisimman objektiivisesta asemasta.

1.1 Tutkimuskysymykset

Tutkielman ensimmäinen tutkimuskysymys on, mitä ovat Bitcoinin hyödyt ja haitat elektroniselle liiketoiminnalle. Hyötyjä tarkastellaan sekä ostajien että kauppiaiden osalta. Hyötyjen ja haittojen pohjalta johdetaan haasteet ja mahdollisuudet toista tutkimuskysymystä ajatellen.

Toinen tutkimuskysymys taas on, miten Bitcoinista voisi kehittää paremman valuutan ja toisaalta myös paremman maksujärjestelmän. Mielipiteet Bitcoinin asemasta ovat olleet hyvin vaihtelevia, joten tämän kysymyksen tarkoituksena on löytää jonkinlainen yhtymäkohta ja koostaa lähdekirjallisuuden pohjalta synteesi.

1.2 Tutkimusmenetelmä ja -aineisto

Tutkimusmenetelmänä tässä tutkielmassa käytetään kirjallisuuskatsausta. Keskeisimmät lähteet ovat peräisin eri tutkimusjulkaisuista, ja ne on valittu tutkimuskysymykset huomioon ottaen. Aineiston valinnassa on pyritty myös ottamaan monipuolisesti lähteitä, joissa voi olla vastakkaisiakin näkemyksiä Bitcoinista ja sen roolista. Näin pyritään muodostamaan mahdollisimman objektiivinen kuva nojaamatta sen enempää Bitcoinin intohimoisten kannattajien kuin vihaajien suuntaan. Tavoitteena on siis eri aineistojen synteesi.

Tutkimuskysymysten kannalta tärkeimmät yksittäiset julkaisut ovat Barberin, Boyenin, Shin ja Uzunin (2012) *Bitter to Better – how to make bitcoin a better currency*, jota hyödynnetään etenkin toiseen tutkimuskysymykseen vastatessa, sekä Tascan (2015) perinpohjaisesti aihetta käsittelevä tutkimusartikkeli *Digital Currencies: Principles, Trends, Opportunities, and Risks*. Tärkeä lähde on myös

Bitcoinin perustajan Satoshi Nakamoton (2008) julkaisu *Bitcoin: A Peer-to-Peer Electronic Cash System*, jossa Bitcoinin idea esitettiin ensimmäistä kertaa.

1.3 Tutkielman rakenne

Bitcoin valuuttana ja maksujärjestelmänä -luvussa analysoidaan Bitcoinia tarkemmin ja esitellään sen merkittävimmät ominaisuudet yksityiskohtaisesti. Ensin käsitellään Bitcoinia valuuttana, sitten Bitcoinin pohjalla olevaa maksujärjestelmää, jota on pidetty Bitcoinin merkittävimpänä innovaationa (Ali, Barrdear, Clews & Southgate, 2014b). Lopuksi otetaan kantaa siihen, onko Bitcoinin yhteydessä mielekästä puhua valuutasta.

Seuraavassa luvussa, Elektroninen liiketoiminta ja Bitcoin, kuvaillaan elektronisen liiketoiminnan nykytilaa ja etenkin digitaalisia maksujärjestelmiä ja peilataan näihin seikkoihin liittyen Bitcoinin ja muiden hajautettujen rahajärjestelmien markkinoita. Myös Bitcoinin ekosysteemiin perehdytään tarkemmin.

Bitcoinin hyödyt ja haitat -luvussa tutkitaan ja vertaillaan lukuisissa eri tutkimuksissa esitettyjä haasteita ja mahdollisuuksia Bitcoinia ajatellen. Hyötyjä tarkastellaan niin asiakas- kuin kauppiasnäkökulmasta. Haitoista tarkastellaan muun muassa Bitcoinin korkeaa volatiliteettiä, mahdollista deflaatiota ja tietoturvariskejä.

Bitcoinin kehittämismahdollisuudet -luvussa tarkastellaan lähdekirjallisuuden pohjalta esitettyjä ja jo muissa kryptovaluutoissa käyttöönotettuja kehitysmenetelmiä, joilla haittoihin on pyritty vastaamaan. Tarkoituksena on siis tarkastella, miten Bitcoinista saisi paremman valuutan kaupankäyntiin ja onko sillä suotuisia tulevaisuudennäkymiä, vai onko sen kohtalona jäädä marginaaliseen osaan jääväksi kuriositeetiksi.

Lopuksi yhteenvetoluvussa käsitellään tiivistetysti aiemmat asiat ja esitetään selkeästi vastaukset tämän tutkielman tutkimuskysymyksiin. Sitten esitellään tutkielmassa ilmenneitä havaintoja ja pohditaan mahdollista jatkotutkimusta.

2 BITCOIN VALUUTTANA JA MAKSUJÄRJESTELMÄNÄ

Tässä luvussa syvennytään tarkastelemaan Bitcoinia yksityiskohtaisemmin. Samalla määritellään keskeiset käsitteet, jotta lukijan olisi helppo ymmärtää seuraavia lukuja, joissa käsitellään aihetta tarkemmin tutkimuskysymyksiin vastatessa. Tätä lukua voi siis pitää eräänlaisena johdantona Bitcoiniin.

Bitcoinia lähdetään tarkastelemaan kahdesta näkökulmasta: ensin kuvaillaan Bitcoinia valuuttana ja sitten maksujärjestelmänä. Ensin kuvaillaan Bitcoinia yleisemmin kryptovaluuttojen kontekstissa ja määritellään, mitä kyseisellä termillä tarkoitetaan. Sitten bitcoinin ominaisuuksia valuuttana tarkastellaan ja eri lähteisiin nojaten pohditaan, miten hyvin se toimii valuuttana näillä osa-alueilla. Tämä antaa pohjaa hyötyjen ja haittojen kartoittamiseen ensimmäiseen tutkimuskysymykseen vastatessa.

Kuvailtaessa Bitcoinia maksujärjestelmänä keskitytään enemmän sen pohjalla oleviin teknologioihin ja siihen, miten Bitcoin loppujen lopuksi toimiikaan maksujärjestelmänä. Erityisesti tarkastellaan Bitcoinin varsinaista innovaatiota, *blockchainia*, joka on yksiselitteisesti julkinen tietokanta, johon kaikki bitcoineilla tehtävät transaktiot tallentuvat hajautetusti. Myös louhinta (engl. *Bitcoin mining*) kuvaillaan, koska sillä on keskeinen rooli koko järjestelmän ylläpidon ja rahakannan kasvattamisen kannalta. Lopuksi tutkitaan, minkälaisia kryptologisia menetelmiä Bitcoinissa käytetään.

2.1 Bitcoin valuuttana

Bitcoinia valuuttana voisi kuvailla eräänlaiseksi digitaaliseksi käteiseksi. Sillä on nimittäin monia käteisen rahan ominaispiirteitä: transaktiossa ei ole mukana välikäsiä ja sen voi suorittaa vain kerran (Velde, 2013). Maksutapahtumat ovat siis peruuttamattomia. Digitaalinen käteinen on kuitenkin periaatteessa aina monistettavissa, jolloin saman rahan voisi käyttää useaan kertaan. Tätä ongelmaa kutsutaan termillä kaksoiskulutusongelma (engl. *double spending problem*)

(Nakamoto, 2008). Ennen Bitcoinia ratkaisuna siihen pidettiin keskitettyä tahoa transaktioiden valvonnassa. Keskitettyyn hallintaan perustui esimerkiksi 90-luvulla Bitcoinin henkinen edeltäjä DigiCash, jossa käytettiin kehittäjänsä David Chaumin patentoimia salausmenetelmiä, joista osan myös Bitcoin on perinyt (Chaum, 1983). Bitcoin sen sijaan välttää tämän digitaalisille valuutoille ominaisen kaksoiskulutusongelman innovatiivisella maksujärjestelmällään.

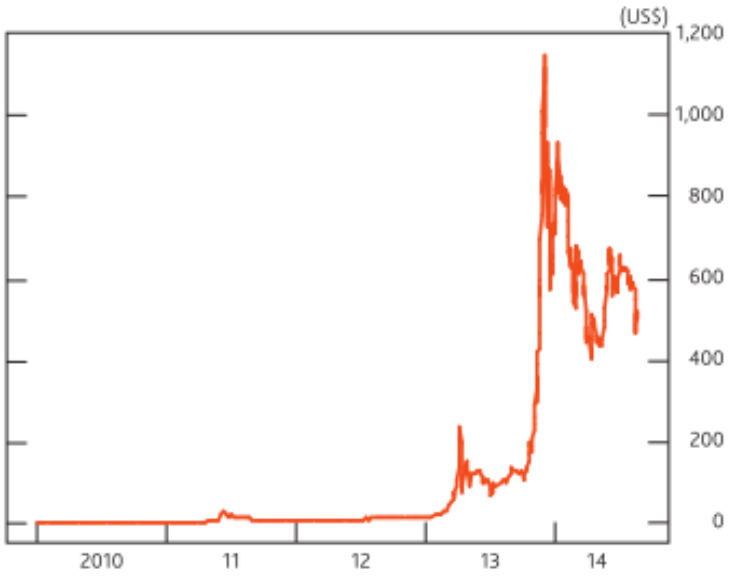
Bitcoin, samoin kuin perinteisemmät valuutat kuten Yhdysvaltain dollari, on niin sanotusti luottamukseen perustuva valuutta. Sen arvo ei siis perustu mihinkään arvometalliin tai vastaavaan, vaan markkinoiden muodostamaan luottamukseen siitä, että bitcoinilla on arvoa. Normaaleilla valuutoilla luottamuksen takaa keskuspankki tai valtio. Bitcoinin tapauksissa luottamus jää vain ja ainoastaan vertaisverkon vastuulle. (Velde, 2013.)

Bitcoinia kuten myös lukuisia sen vanavedessä kehitettyjä digitaalisia valuuttoja kuvataan yleisesti termillä kryptovaluutta. Varsin yksiselitteinen määritelmä kryptovaluutoille on, että ne ovat digitaalisesti siirrettäviä ja salausmenetelmin suojattuja, hajautettuja valuuttoja ja maksujärjestelmiä (White, 2014). Salausmenetelmiä käytetään niin transaktioiden varmistamiseen kuin järjestelmän ylläpitoon. Tämä mahdollistaa sen, ettei tarvita kolmannen osapuolen keskitettyä hallintaa transaktioiden varmistamiseksi, vaan kaikki transaktiot tapahtuvat vertaisverkossa, suoraan käyttäjältä käyttäjälle.

On syytä huomioida, että kryptovaluutat tekevät selkeän eron tavalliseen digitaaliseen rahaan. Bitcoinille, kuten muille kryptovaluutoille, on olennaista se, että se on täysin uusi valuutta ja sen takana on myös täysin uusi maksujärjestelmä. Täten esimerkiksi Google Walletissa käytettävä raha kuten myös nettipeleissä käytettävät valuutat (esim. SecondLifen *Linden dollar*) eroavat merkittävästi kryptovaluutoista, sillä ne perustuvat keskitettyyn hallintaan ja keskuspankkien valuuttoihin. (Ali ym., 2014b.)

Ominaista bitcoinille on myös korkea arvonvaihtelu, eli volatiliteetti (Yermack, 2013). Tämä on samalla yksi sen suurimmista heikkouksista. Volatiliteetti perustuu siihen, että bitcoineille on asetettu enimmäismäärä (21 miljoonaa bitcoinia), mikä tekee siitä deflatorisen valuutan (Barber ym., 2012). Toisin kuin normaalirahan hinta, bitcoinin hinta siis kasvaa bitcoinien lukumäärän lisääntyessä. Bitcoinin voi kuitenkin jakaa murto-osiin, mikä mahdollistaa pienempien transaktioiden suorittamisen. Nykysillään yhden Bitcoin pystyy jakamaan kahdeksan murto-osan tarkkuudella (Böhme, Christin, Edelman & Moore, 2016).

Rahallisen arvon määrittää vain ja ainoastaan kysyntä – mitä enemmän Bitcoinia käytetään, sitä arvokkaammaksi se tulee ja sitä enemmän myös Bitcoineja luodaan markkinoille louhinnan kautta. Seuraavassa kuvassa näkyy, kuinka paljon bitcoinin arvo suhteessa Yhdysvaltain dollariin on heitellyt vuodesta 2010 lähtien (kuvio 1).



KUVIO 1 Bitcoinin arvon vaihtelu (Ali ym., 2014b: 266)

Bitcoinia valuuttana käsiteltäessä on järkevää tarkastella, kuinka hyvin se täyttää rahan tehtävät. Perinteisesti rahalla on kolme tehtävää: se on vaihdon väline, arvon mitta ja arvon säilyttäjä (Yermack, 2013). On kyseenalaista, voiko bitcoinin tapauksessa edes puhua rahasta, miten se nykyään käsitetään.

Yermack (2013) käsittelee artikkelissaan bitcoinin asemaa valuuttana. Yermackin mukaan bitcoin toimii jokseenkin maksuvälineenä, mikä on ilmeistä, sillä useat tahot käyttävät sitä kasvavissa määrin. Haasteena on kuitenkin, että bitcoineja on vaikea ansaita. Arvon mittana ja säilyttäjänä bitcoin kuitenkin toimii kehnosti juuri volatiliteetin takia. Lisäksi bitcoinin arvo ei ole yksiselitteinen, vaan usealla valuutanvaihtajalla on sille eriävät valuuttakurssit. Tämä asettaa haasteita elektroniselle kaupankäynnille.

Puhetta on ollut myös viime vuosina siitä, onko bitcoin valuuttana maksuväline vai kenties pikemminkin investoinnin kohde (Glaser, Zimmermann, Haferkorn, Weber & Siering, 2014; Yermack, 2013). Koska bitcoineille on asetettu enimmäismäärä, on havaittu, että niitä haalitaan enemmän säästettäväksi kuin käytetään (Glaser ym., 2014). Käyttäjät tahtovat säilyttää bitcoineja, koska ne voivat olla ja todennäköisesti ovatkin tulevaisuudessa arvokkaampia. Bitcoin on siis ennen kaikkea taloudellisen spekuloinnin kohde. Tämä voi hidastaa bitcoinien hyväksymistä elektronisessa kaupankäynnissä. Tähän haasteeseen palataan ensimmäiseen tutkimuskysymykseen vastatessa.

2.2 Bitcoin maksujärjestelmänä

Bitcoinin taustalla on monimutkainen ja innovatiivinen maksujärjestelmä, jota lähdetään avaamaan tässä luvussa. Kuten edellisessä luvussa kerrottiin, on erilaisia digitaalisia valuuttoja ollut jo ennen Bitcoinia, mutta Bitcoinin vertais-

verkkoon ja hajautukseen perustuva maksujärjestelmä oli ilmestyessään ennennäkemätön keksintö. Idean oli kuitenkin esitellyt jo vuonna 1998 Wei Dai ehdottaessaan hajautettua rahajärjestelmää, joka olisi täysin erillinen keskuspankkien ja valtioiden rahajärjestelmistä (Nakamoto, 2008).

Bitcoinin toiminta perustuu vertaisverkon käyttöön. Verkko rakentuu toisiinsa liitetyistä noodeista, joiden tehtävinä on tuottaa sarjanumerot bitcoineille, pitää yllä tietoa siitä, mille käyttäjille kukin bitcoin kuuluu, varmistaa transaktioiden oikeellisuus sekä välittää viestejä toisille noodeille (Tasca, 2015). Käyttäjän ja bitcoinien louhijat muodostavat omat noodinsa verkkoon.

Käytännön tasolla maksujärjestelmän käyttö onnistuu vapaan lähdekoodin ohjelman kautta. Bitcoinin käyttäjä tekee itselleen tilin, jolla on oma yksilöllinen osoitteensa; tilejä voi olla myös useita. Transaktiot tapahtuvat ikään kuin viestejä lähettämällä osoitteesta osoitteeseen vertaisverkon välityksellä. Bitcoinit tallentuvat käyttäjien digitaalisiin lompakkoihin. Lompakko on usein joko työpöytäsovellus, tai sitten kolmannen osapuolen tarjoama mobiili- tai websovellus, joiden tietoturva on ollut varsin kyseenalaista (Androulaki, Karame, Roeschlin, Scherer & Capkun, 2013; Yermack, 2013).

Bitcoinin maksujärjestelmän tavoitteina on olla luotettava, tehokas ja täysin vapaa keskitetystä hallinnasta (Kaplanov, 2012). Seuraavaksi tarkastellaan, miten Bitcoin pyrkii saavuttamaan nämä tavoitteet. Koska kyseessä on varsin monimutkainen kokonaisuus ymmärrettäväksi, esitellään maksujärjestelmän perusteet sen kolmen merkittävimmän ominaisuuden kautta: ensin kuvataan blockchainia, sitten Bitcoinien louhintaa (engl. *Bitcoin mining*) ja lopuksi maksujärjestelmässä käytettäviä salausmenetelmiä. Huomattavaa on, että kaikki nämä liittyvät olennaisesti toisiinsa.

2.2.1 Blockchain

Jokainen bitcoineilla tehty transaktio tallennetaan julkiseen tilikirjaan, joka tunnetaan nimellä blockchain. Transaktioiden täytyy olla julkisia, sillä muuten maksujärjestelmän hajautetun luonteen vuoksi yksittäiset tahot saattaisivat muokata transaktiohistoriaa. Jokaiselle transaktiolle annetaan yksilöllinen tunniste ja ne koostetaan lohkoiksi, jotka aikaleimataan (engl. *timestamp*) niiden oikeellisuuden takaamiseksi (Nakamoto, 2008). Jokainen lohko sisältää hajautetun viitteen sitä edeltäneeseen lohkoon, mikä tekee lohkoista ketjun, mistä juontuukin nimi blockchain. Ketjutuksen vahvuus perustuu siihen, että jokainen uusi lohko vahvistaa koko maksujärjestelmää entisestään. Järjestelmä ei siis perustu luottamukseen tai keskitetyn tahon hallintaan, vaan vertaisverkon vahvuuteen.

Kun uusi lohko on luotu ketjuun, se tallentuu vertaisverkon kautta jokaisen Bitcoinin käyttäjän kopioon tilikirjasta, jolloin jokaisella on sama transaktiohistoria. Lohkojen lisääminen on tehty siten, että uusi lohko lisätään aina 10 minuutin välein. Mutta miten käy, jos esimerkiksi yksittäinen taho yrittää muokata transaktiohistoriaa kaksoiskuluttaakseen saman bitcoinin? Vastaus tähän on Bitcoinin louhintamekanismi, jota kuvataan seuraavaksi.

2.2.2 Bitcoinien louhinta

Louhinnan perimmäisenä tarkoituksena on paitsi lisätä uusia bitcoineja järjestelmän kiertokulkuun, mutta myös ylläpitää koko järjestelmän eheyttä (Nakamoto, 2008). Bitcoinien louhinnassa on pohjimmiltaan kyse siitä, että louhijat koettavat varmistaa viimeksi lisätyn lohkon oikeellisuuden. Tämä tapahtuu siten, että lohkoon on sisälletty laskennallisesti haastava ongelma, jota louhijat lähtevät ratkomaan louhintaan tarkoitettuja ohjelmistoja ja laitteita käyttäen. Mitä enemmän konetehoa käytetään, sitä nopeammin ongelma saadaan ratkaistua ja lohko todennettua. Kun lohko on saatu todennettua ensimmäisen louhijan toimesta, se todentuu myös muille louhijoille. Kannustimena louhija palkitaan tietyllä (ja alati vähenevällä) määrällä bitcoineja. (Eyal & Sirer, 2014.)

Tällä monimutkaiselta kuulostavalta louhintamekanismilla pyritään imitoimaan oikean maailman kullanlouhintaa (Nakamoto, 2008). Louhijat palkitaan siitä hyvästä, että käyttävät laskentatehoa ja sähköä lohkon todentamiseksi, ja bitcoinien kokonaismäärä pidetään keinotekoisesti rajallisena. Lisäksi jokaisen lisätyn lohkon myötä lohkon ratkaiseminen vaikeutuu käytetyn laskentatehon mukaan, jotta kaikkia bitcoineja ei saisi louhittua liian nopeasti.

Bitcoinin louhintamekanismi siis pitää vertaisverkon eheyttä yllä ja suojaa kaksoiskulutukselta sekä muilta väärinkäytöksiltä eräänlaisen konsensuksen muodostumisen kautta. Kun valtaosa louhijoista muodostaa yksimielisyyden lohkon oikeellisuudesta, voi olla melko varma, ettei verkossa ole tapahtunut väärinkäytöksiä. Riskinä tietty on, että valtaosa louhijoista ei toimikaan rehellisesti ja pyrkii tahallisesti hyväksymään virheellisiä transaktioita. Tämä kuitenkin vaatisi erittäin suuren määrän laskentatehoa, etenkin, kun Bitcoinin maksuverkko alati laajene.

2.2.3 Kryptologia Bitcoinin taustalla

Kuten on jo mainittu, Bitcoin perustuu kryptologisiin menetelmin, joita hyödynnetään transaktioiden suorittamisessa, louhinnassa sekä käyttäjien yksityisyyden säilyttämisessä (Nakamoto, 2008). Seuraavaksi tarkastellaan olennaisimpia kryptologisia teknologioita, joita Bitcoin käyttää.

Eräs Bitcoinin lupauksista on käyttäjiensä yksityisyyden suojeleminen maksutapahtumien julkisuudesta huolimatta (Nakamoto, 2008). Tämä onnistuu digitaalisten avaimien salausalgoritmin avulla: jokaisella käyttäjällä on yksilöllinen julkinen avain, jota käytetään transaktioiden salaamiseksi, sekä salainen avain, jota käytetään saapuvien transaktioiden avaamiseksi (Woo, Gordon & Iaralov, 2013). Koska *blockchain* on julkinen tilikirja, on käyttäjien julkisten avaimien pohjalta helppo yksilöidä maksutapahtumat. Tästä syystä monen eri osoitteen käyttö on suositeltavaa yksityisyyden takaamiseksi; tosin tutkimuksen mukaan tämäkään ei välttämättä riitä (Androulaki ym., 2013).

Bitcoinien louhinnan taustalla on Adam Backin kehittämä Hashcash-teknologia (Back, 2002; Nakamoto, 2008). Hashcash on niin sanottu *proof-of-work* -järjestelmä, joka perustuu Bitcoinin tapauksessa siihen, että louhija käyttää laskentatehoa ratkaistakseen ongelman saadakseen lisätä lohkon järjestelmään.

Järjestelmä takaa sen, ettei kuka tahansa voi mielivaltaisesti lisätä lohkoja ketjuun esimerkiksi lukuisten huijaustilien kautta, vaan lisäyksestä pitää maksaa laskentatehoa (Back, 2002). Ja koska useat louhijat kilpailevat saman lohkon varmistamisesta, voi olla lähestulkoon varma, että lisättävä lohko on oikeellinen. Tämä on hyvä esimerkki vertaisverkon tehokkuudesta.

3 ELEKTRONINEN LIIKETOIMINTA JA BITCOIN

Tässä luvussa tarkastellaan Bitcoinin asemaa elektronisen liiketoiminnan kontekstissa. Elektronisen liiketoiminnan nykytila esitellään lyhyesti, ja erityisesti kuvaillaan maksujärjestelmiä. Tärkeinä tarkastelun kohteina ovat myös useat Bitcoinia pääasiallisesti hyödyntävät toimijat, kuten maksupalveluntarjoajat ja bitcoinien vaihdantapaikat (esim. BitPay ja Coinbase), joilla on olennainen rooli toimia rajapintana Bitcoinin maksujärjestelmän ja perinteiseen valuuttaan perustuvien maksujärjestelmien välillä. Myös Bitcoiniin liittyvää rikollista toimintaa tarkastellaan pintapuolisesti, muun muassa Silk Road-verkkokauppaa.

Maksujärjestelmiä tarkastellessa kuvaillaan etenkin Bitcoinin eroavaisuuksia ja mahdollisia etuja luottokorttimaksuihin verrattuna. Tarkastelun kohteiksi otetaan luottokorttimaksujärjestelmät ja selvitetään, minkälaisia ongelmia kyseisillä järjestelmillä on. Näin saadaan perusteltua sitä, miksi tai miksi ei elektronisen liiketoiminnan toimijat ylipäänsä haluaisivat hyväksyä Bitcoinin osana liiketoimintaansa.

Bitcoinin markkinoita ja ekosysteemiä tarkasteltaessa selvitetään, miten Bitcoin on otettu vastaan elektronisessa liiketoiminnassa ja minkälaisia markkinoita Bitcoinin ympärille on muodostunut. Ekosysteemillä tarkoitetaan kaikkien Bitcoinia pääasiallisesti hyödyntävien toimijoiden alati kasvavaa kokonaisuutta, johon kuuluvat muun muassa vaihdantapaikat, maksupalvelut, tilastontarjoajat ja louhintayhtymät (Grinberg, 2011). Tämä auttaa selkeyttämään sitä kenttää, missä Bitcoin tällä hetkellä pääosin toimii ja toisaalta missä sen kasvu on todennäköisintä tulevaisuudessa.

3.1 Elektronisen liiketoiminnan maksujärjestelmät

Internet-teknologioiden kehittyminen on tuonut monia uusia mahdollisuuksia toteuttaa liiketoimintaa elektronisesti. Tästä syystä erilaisten elektronisen liiketoiminnan muotojen kirjo on laajentunut. Tämän tutkielman kannalta elektro-

ninen liiketoiminta käsitetään Internetin välityksellä käytäväksi kaupaksi, jossa palvelu tai tuote vaihtuvat maksua vastaan ostajan ja myyjän välillä.

Elektronisen liiketoiminnan kehittymisen myötä on myös kehitelty erilaisia maksujärjestelmiä, sillä eri toimijoilla ja asiakkailla on erilaisia tarpeita maksujen suorittamisen suhteen. Esimerkiksi verkkohuutokaupat ovat luoneet tarpeen sille, että maksuja pystyisi suorittamaan suoraan käyttäjältä käyttäjälle, minkä Bitcoin mahdollistaa (Sumanjeet, 2009). Yhteistä kaikille maksujärjestelmille kuitenkin on, että niiden käytön pitää olla asiakkaille mahdollisimman helppoa ja turvallista, mikä on jo pitempään ollut yksi elektronisen liiketoiminnan keskeisimmistä haasteista (Zwass, 1996).

Singh Sumanjeet (2009) jakaa artikkelissaan *Emergence of Payment Systems in the Age of Electronic Commerce: The State of Art* elektroniset maksujärjestelmät neljään pääkategoriaan: luottokortti-, sirukortti-, digitaalista rahaa käyttäviin ja digitaalisiin shekkijärjestelmiin. Näiden lisäksi nykyään voidaan katsoa olevan vielä viides kategoria, mobiilimaksujärjestelmät, jotka ovat huomattavasti yleistyneet viime vuosina (Ali ym., 2014b). Elektronisessa kaupankäynnissä näistä kiistatta yleisimpiä ovat kuitenkin edelleen luottokorttijärjestelmät, joista PayPal lienee kaikista suurin ja tunnetuin. Tämän takia ja aiheen rajaamisen vuoksi tässä tutkielmassa keskitytään tarkastelemaan nimenomaan luottokorttijärjestelmiä suhteessa Bitcoiniin.

3.1.1 Luottokorttijärjestelmät

Luottokorttijärjestelmien valta-asema on perusteltu, sillä ne ovat olleet jo pitkään olennainen osa elektronista kaupankäyntiä. Käyttäjät ovat halukkaampia käyttämään tuttua ja turvallista maksujärjestelmää, vaikka tarjolla olisi muitakin vaihtoehtoja (Sumanjeet, 2009). Luottokorttijärjestelmissä riski on aina olemassa käyttäjän antaessa henkilökohtaisia luottokorttitietojaan kolmansille osapuolille, mutta on havaittu, etteivät anonymiteetin menettäminen ja keskeisen tahon hallinta maksutapahtumissa ole käyttäjille suurikaan huolen aihe (Grinberg, 2011).

Luottokorttijärjestelmillä on selviä etuja verrattuna Bitcoiniin ja muihin kryptovaluuttoihin. Koska luottokorttijärjestelmät ovat olleet jo pitkään markkinoilla, on tehokkuuteen, turvallisuuteen, maksamisen helppouteen ja käyttäjäystävällisyyteen panostettu paljon (Sumanjeet, 2009). Esimerkiksi Bitcoinissa käyttäjiä ei suojata huijauksilta, vaan suojausmenetelmät ovat käyttäjien omalla vastuulla, kun taas PayPal ja muut suuryritykset ovat investoineet miljoonia turvallisuuden takaamiseksi (Grinberg, 2011). On selvää, että käyttäjät suosivat mieluiten järjestelmää, jossa transaktioiden suojaaminen on taattu.

Elektroniselle kaupankäynnille luottokorttijärjestelmät ovat siis olennainen osa, mutta niissä on omat heikkoutensa ja riskinsä etenkin kauppiaille. Luottokorttien transaktiokustannukset voivat olla haitallisia. Suuremmissa maksusummissa tämä tuskin on suuri menetys kauppiaille, mutta pienemmissä maksuissa saattaa voittomarginaali kaventua merkittävästi. Nykyisin mikromaksujen määrä on lisääntynyt, mutta niiden suorittaminen ei ole mielekästä

luottokorttijärjestelmien korkeiden transaktiokustannusten takia. (Sumanjeet, 2009.)

Kenties merkittävin riski ovat luottokorttihuijaukset. Luottokorttien käyttäjät ovat yleisesti ottaen hyvin suojattuja tällaisissa tapauksissa, mutta kauppiaille tämä voi tietää takaisinveloitusten suorittamista ja ylimääräisiä kustannuksia. Jos esimerkiksi asiakas vaatii takaisinveloitusta luottokorttinsa väärinkäytön tai sen epäilyn seurauksena, luottokorttia kontrolloiva pankki joutuu tarkistamaan, onko huijausta tapahtunut. Tästä yleensä koituu kauppiaille vähintään käsittelykustannuksia, sekä täydet takaisinveloituskustannukset, mikäli huijauksen katsotaan tapahtuneen. (Bhatla, Prabhu & Dua, 2003.)

Kaikilla keskitettyyn hallintaan perustuvilla maksujärjestelmillä on myös ominaista luotto- ja maksukykyriskit johtuen luottamuksen tarpeesta ja välittäjän (eli pankin) osallisuudesta maksutapahtumissa. Luottoriski tulee eteen, jos pankista tulee maksukyvytön velkojen takia. Maksukykyriski taas koituu, jos pankilla ei ole varoja käsitellä maksua tietyllä hetkellä. Molemmat riskit siis johtuvat maksujärjestelmän keskitetystä luonnosta (Ali ym., 2014b.)

3.1.2 Bitcoin ja muut hajautetut maksujärjestelmät

Hajautetut, digitaalista rahaa käyttävät maksujärjestelmät ovat vielä varsin uusia tulokkaita elektronisessa liiketoiminnassa. Keskeinen ominaisuus on se, ettei maksutapahtumissa tarvita välittävää osapuolta, vaan transaktiot siirtyvät suoraan käyttäjältä käyttäjälle. Bitcoin ja muut kryptologiaan perustuvat maksujärjestelmät siis edustavat selkeästi tätä kategoriaa. Koska luottamusta ja välittäjää ei tarvita, ei hajautetuilla maksujärjestelmillä ole samanlaisia maksukyky- ja luottoriskejä kuin keskitetyillä järjestelmillä.

Merkittävin yksittäinen innovaatio, johon moni nykyinen hajautettu maksujärjestelmä perustuu, on Bitcoinin esittelemä blockchain-teknologia. Ennen sitä digitaaliseen rahaan perustuvat maksujärjestelmät perustuivat aina keskitettyyn hallintaan. Mielenkiintoinen esimerkki blockchain-teknologian käytöstä on muun muassa Ripple[1], joka toimii business-to-business -rajapinnassa tarjoten pankeille mahdollisuutta suorittaa keskenään transaktioita ilman välittäjiä. Ripple käyttää Bitcoinin louhinnasta poikkeavaa protokollaa, joka mahdollistaa transaktiot jopa muutamassa sekunnissa eri maiden pankkien välillä (White, 2014).

Hajautuksen ja vertaisverkon vuoksi huijaukset ovat huomattavasti epätodennäköisempiä kuin luottokorttijärjestelmissä, joissa huijaukset ovat kaikista yleisimpiä (Sumanjeet, 2009). Riskinä hajautetuissa järjestelmissä on kuitenkin koko järjestelmän laajuinen huijaus, jos yksi taho onnistuu hallitsemaan valtaosaa vertaisverkosta (Ali ym., 2014b). Tähän haasteeseen syvennytään tarkemmin Bitcoinin hyödyt ja haitat -luvussa.

[1] https://ripple.com/

3.2 Bitcoinin markkinat ja ekosysteemi

Bitcoinin käyttö elektronisessa liiketoiminnassa on ollut tähän asti hyvin marginaalista, mutta kasvu on ollut jatkuvaa (White, 2014). Verkkokaupoista muun muassa Overstock, matkatoimisto Expedia, elektroniikkauppa Newegg ja lahjakorttipalvelua tarjoava Gyft ovat tähän mennessä ottaneet käyttöön Bitcoin-maksut (Böhme ym., 2016). Marginaalinen asema johtuu paitsi Bitcoinin suhteellisesta uutuudesta markkinoilla, mutta myös aiemmin mainituista hajautettujen maksujärjestelmien riskitekijöistä ja bitcoinin korkeasta volatiliteetistä. Nykyisellään myyjät ja ostajat ovat halukkaampia käyttämään totuttuja, luotettavia maksujärjestelmiä kuin omaksumaan kokonaan uutta ja vielä vaikeasti ymmärrettävää järjestelmää (Sumanjeet, 2009).

Elektronisessa liiketoiminnassa on kuitenkin ilmennyt jonkin verran kysyntää Bitcoinin kaltaisille maksujärjestelmille. Kaplanov (2012) katsoo, että kysyntä perustuu neljään asiaan: alhaisiin transaktiokustannuksiin, keskitetyn hallinnan puuttumiseen, transaktioiden oletettuun anonymiteettiin ja bitcoinien käyttöön sijoituskohteena. Mutta kuten Dwyer (2015) huomauttaa, Bitcoin ei ole anonymiteettiin perustuva järjestelmä, eikä se koskaan ollut Nakamoton (2008) tarkoituksena.

Bitcoin ei suinkaan kilpaile yksin perinteisten maksujärjestelmien kanssa, vaan Bitcoinin jälkeen on kehitetty yli 500 eri kryptovaluuttaa (Tasca, 2015). Osa näistä perustuu hyvin vahvasti Bitcoinin protokollaan, kuten transaktioaikoja vähentävä LiteCoin, kun taas osa käyttää hyvinkin poikkeavia teknologioita. Bitcoin on edelleen ylivoimaisesti suosituin, mutta sille on tullut myös haastajia: esimerkiksi aiemmin mainittu kryptovaluutta Ripple on saavuttanut 10 %:n osuuden kaikkien kryptovaluuttojen markkinoista (Tasca, 2015).

Meiklejohn ym. (2013) tutkivat, minkälaisissa palveluissa bitcoineja pääasiassa käytetään. Tutkimusta varten tutkijat perustivat useita Bitcoin-tilejä ja tekivät ostoksia saadakseen selville myyjien Bitcoin-osoitteita. Tutkimuksessa saatiin selville, että valtaosa bitcoineilla tehtävistä transaktioista keskittyy vaihdantapaikkoihin, jotka esitellään ekosysteemin yhteydessä tarkemmin.

Bitcoinin ympärille on muodostunut varsin elinvoimainen ekosysteemi, joka koostuu erilaisista Bitcoinia pääasiallisesti hyödyntävistä elektronisen liiketoiminnan palveluista. Tämän avoimen ja monipuolisen kokonaisuuden takana on Bitcoinin hajautettu luonne ja avoin lähdekoodi: kuka tahansa voi aloittaa uuden palvelun Bitcoinia hyödyntäen (Barber ym., 2012). Tyypillisimpiä palveluita ovat muun muassa vaihdantapaikat, maksupalvelut, verkkokaupat ja louhintayhtymät (engl. *mining pools*). Seuraavaksi kuvaillaan näitä tarkemmin.

Bitcoinin vaihdantapaikoille on tarvetta, sillä ne tarjoavat ensinnäkin toimivimman mahdollisuuden saada bitcoineja ja toiseksi rajapinnan vaihtaa ansaittuja bitcoineja markkinoilla käyväksi valuutaksi (Papp, 2014). Yksittäiselle käyttäjälle bitcoinien ansaitseminen louhinnan kautta on miltei mahdotonta korkeiden laskentatehovaatimusten ja kovan kilpailun takia, joten vaihdantapaikoissa on mahdollista ostaa bitcoineja normaalivaluuttoja vastaan. Toisaalta

koska bitcoinia hyödyntävien verkkokauppojen määrä on rajallinen ja bitcoinien käyttö verkon ulkopuolisissa ostoksissa vielä alkutekijöissään, mahdollistavat vaihdantapaikat myös normaalivaluuttojen ostamisen bitcoineilla.

Vaihdantapaikoista suurin ja tunnetuin oli MtGox, joka käsitteli vuosien 2012 ja 2013 välillä jopa 70 – 80 % bitcoineilla tehdyistä transaktioista (Tasca, 2015). MtGox kuitenkin ajautui konkurssiin menetettyään selittämättömästi 473 miljoonan Yhdysvaltain dollarin arvosta bitcoineja. Tämä ja monet muut vastaavanlaiset tapaukset ovat herättäneet kysymyksen siitä, ovatko vaihdantapaikat kovinkaan luotettavia (Moore & Christin, 2013).

Maksupalvelut tarjoavat kauppiaille mahdollisuuden integroida Bitcoinmaksut osaksi liiketoimintaansa. Eräitä suurimpia maksupalveluntarjoajia ovat muun muassa BitPay ja CoinBase. Toiminta perustuu siihen, että palveluntarjoaja tarjoutuu ostamaan asiakkaan bitcoinin ja maksamaan siitä kauppiaalle perimällä maksusummasta pienen transaktiokustannuksen. Maksupalvelut siis tarjoavat rajapinnan, jossa kauppiaat voivat riskittömästi ottaa vastaan bitcoineja, kun maksupalvelut hoitavat varsinaisten bitcoinien käsittelyn. (White, 2014.)

Vaikka suurista verkkokaupoista vain harva on tähän mennessä omaksunut Bitcoinin maksuvaihtoehdoksi, on markkinoille tullut paljon Bitcoinia pääasiallisesti käyttäviä verkkokauppoja. Näistä pahamaineisimpina mainittakoon viranomaisten alas ajama verkkokauppa Silk Road, joka keskittyi huumeiden ja muiden kieltotavaroiden peer-to-peer -myyntiin salatussa verkossa. Tutkimusten mukaan Silk Roadin liikevaihto oli jo ensimmäisen vuotensa jälkeen 15 miljoonaa Yhdysvaltain dollaria (Christin, 2012). Pahamaineisuudestaan huolimatta Silk Roadin tapaus kuitenkin osoittaa ainakin sen, että laajamittaisen verkkokauppaliiketoiminnan toteuttaminen Bitcoinia käyttäen on mahdollista.

Bitcoinien louhinnasta on muodostunut varteenotettava toimiala, jossa monet yksittäiset louhijat ovat muodostaneet yhtymiä laskentatehon optimoimiseksi. Näin lohko saadaan todennäköisemmin ratkaistua, ja palkkioksi saadut bitcoinit jaetaan kaikkien osallisten kesken. Tutkimuksen mukaan nykyisellään bitcoinien louhinta on noin 5-6 suuren louhintayhtymän hallitsemaa, ja valtaosa louhintatoiminnasta keskittyy Kiinaan (Tasca, 2015). Yksittäisille louhijoille ei siis juuri löydy sijaa louhintatoiminnasta, vaan toiminta alkaa olla enemmissä määrin vain muutaman yhtymän hallitsemaa.

4 BITCOININ HYÖDYT JA HAITAT

Edellisissä luvuissa kuvailtiin, mikä Bitcoin tarkalleen ottaen, minkälaisia ovat elektroniset maksujärjestelmät ja minkälaiset markkinat Bitcoinilla on elektronisessa liiketoiminnassa. Samalla esille nostettiin esiin jo alustavasti Bitcoiniin liittyviä hyötyjä ja haittoja, joita lähdetään tässä luvussa käsittelemään tarkemmin. Tarkoituksena on muodostaa selkeä, yhteenvedonomainen kuva, jolla vastataan ensimmäiseen tutkimuskysymykseen. Lisäksi muodostetaan perusteet seuraavassa luvussa esitettäville kehitysmahdollisuuksille.

Ensin analysoidaan Bitcoinin hyötyjä elektronisessa liiketoiminnassa. Samalla pyritään tunnistamaan ne mahdollisuudet, joita Bitcoin voi tarjota elektronisen liiketoiminnan osapuolille.

Hyötyjen jälkeen tarkastellaan Bitcoinin haittoja ja heikkouksia. Esille nostetaan jo aiemmin tässä tutkielmassa esitettyjä ongelmakohtia ja syvennytään niihin tarkemmin. Haitoista mainitaan taloudelliset ongelmat, louhinnan ja blockchainin heikkoudet, sekä tietoturvaan ja kaupankäyntiin liittyvät riskit.

4.1 Hyödyt ja mahdollisuudet elektronisessa liiketoiminnassa

Kuten tässä tutkielmassa on jo aiemmin mainittu, Bitcoinin yleisiä hyötyjä maksutapahtumissa ovat alhaiset transaktiokustannukset, keskitetyn hallinnan puuttuminen ja yksityisyys. Nämä ovat myös ne periaatteet, joiden takia Bitcoin alun perin kehitettiin (Nakamoto, 2008). Lisäksi Bitcoin ja etenkin blockchain-teknologia ovat luoneet uusia sovellutuksia ja liiketoimintamahdollisuuksia, kuten edellisessä luvussa kuvailtiin.

Bitcoin voi olla erittäin hyödyllinen mikromaksumarkkinoilla alhaisten transaktiokustannustensa vuoksi. Koska mikromaksut eivät ole kannattavia esimerkiksi luottokorttijärjestelmissä, tarjoaa Bitcoin selvän mahdollisuuden mikromaksujen toteuttamiseen. Tässä juuri edesauttaa se, että bitcoineja voi pilkota murto-osiin. Bitcoin voi olla hyödyllinen etenkin erilaisissa verkkopeleissä, joissa pieniä maksuja (alle euron suuruisia) tapahtuu tiheällä tahdilla ja

joissa ei ole niin väliä, onko hinnat ilmoitettu reaalimaailman valuuttoina. (Grinberg, 2011.)

Bitcoin on myös hyödyllinen kansainvälisessä kaupankäynnissä, sillä kaupankäynti Bitcoinilla tapahtuu maantieteellisestä sijainnista ja siten esimerkiksi valtioiden säännöksistä riippumatta (Grinberg, 2011). Bitcoin voi olla siten myös soveltuva maksuväline kansainvälisille työntekijöille, jotka siirtävät rahalähetyksiä kotimaahansa. Esimerkiksi kansainvälisissä maksuissa maksupalveluvälittäjät (kuten Western Union ja MoneyGram) perivät jopa 10 % maksuista transaktiokustannuksia (White, 2014).

On esitetty, että blockchain on kenties Bitcoinia itseään tärkeämpi innovaatio elektroniselle liiketoiminnalle (Ali ym., 2014b; Tasca, 2015). Blockchainia on hyödynnetty tietenkin muissa kryptovaluutoissa, joista osa on pyrkinyt vastaamaan Bitcoinin heikkouksiin. Esimerkiksi aiemmin mainitun LiteCoinin etu on se, että transaktioiden käsittelyyn ei mene niin kauan aikaa kuin Bitcoinilla. Toisaalta myös blockchainille on paljon sovellutuksia maksujärjestelmien ulkopuolella: esimerkiksi Tasca (2015) mainitsee, että blockchainia voi soveltaa ylipäänsä kaikessa toiminnassa, jossa hajautettu hallinta olisi hyödyllistä. Esimerkkeinä mainittakoon varallisuuden hallintaan tarkoitettu ColoredCoins, joka rakentuu blockchain-protokollan päälle, sekä Ethereum[2], joka tarjoaa alustaa hajautettujen sovellusten rakentamiseen.

4.2 Bitcoinin heikkoudet ja riskit

Nykyisellään Bitcoinilla on lukuisia heikkouksia, jotka selkeästi hidastavat sen käyttöönottoa elektronisessa liiketoiminnassa. On syytä huomioida, että riskit ovat limittyneitä toistensa kanssa: esimerkiksi heikkouden louhinnassa aiheuttavat taloudellisia riskejä. Seuraavaksi käydään läpi Bitcoinin heikkoudet kategorioittain.

4.2.1 Taloudelliset ongelmat

Bitcoinin taloudelliset ongelmat liittyvät ennen kaikkea sen käyttöön valuuttana. Kuten tässä tutkielmassa on jo aiemmin alustettu, suurimmat ongelmat liittyvät bitcoinin deflaatioon ja volatiliteettiin. Seuraavaksi lähdetään käsittelemään näitä ongelmia tarkemmin.

Deflaatio johtuu siitä, että bitcoineille on asetettu enimmäismäärä. Tästä syystä käyttäjät ovat halukkaampia säästämään kuin käyttämään bitcoineja. Bitcoin on siis taloudellisen spekuloinnin kohde: vuosien 2011 ja 2015 välillä kiertokulussa olevien bitcoinien määrä oli 25 – 50 % luokkaa (Tasca, 2015: 59). Valtaosaa ansaituista bitcoineista ei siis käytetä kaupankäynnissä, vaan säästetään (Glaser ym., 2014). Lisäksi, jos bitcoin häviää kiertokulusta, eli esimerkiksi käyttäjä onnistuu hävittämään bitcoinin yksityisen tunnisteavaimen, kyseinen

[2] https://www.ethereum.org/

bitcoin on poissa peruuttamattomasti, ja koko rahakanta pienenee. Molemmissa tapauksissa siis bitcoineja häviää kiertokulusta, mikä ruokkii deflaatiota entisestään. Lisäksi deflaation myötä bitcoinien varastamisesta tulee rikollisille toimijoille kannattavampaa (Barber ym., 2012). Bitcoinien varastamiseen palataan kaupankäynnin riskien yhteydessä.

Bitcoinin korkea volatiliteetti johtuu paitsi deflaatiosta ja spekuloinnista, mutta myös sen suhteellisesta tuoreudesta markkinoilla. On myös havaittu, että bitcoinin arvo korreloi sen mediassa saaman huomion kanssa (Glaser ym., 2014). Bitcoin on siis erittäin herkkä suhdannevaihteluille. Tämä johtuu siitä, että bitcoineja on verrattain vähän markkinoilla. Myös yksittäiset transaktiot vaikuttavat bitcoinin hintaan, etenkin suuria rahamääriä käsittävät. Tämä tunnetaan ohuiden markkinoiden ongelmana (Böhme ym., 2016).

Voisi olettaa, että Bitcoinin käyttäjäkunnan kasvaessa ja bitcoinien kaupankäynnin lisääntyessä markkinat syvenisivät ja volatiliteetti siten pienenisi. Näin ei kuitenkaan välttämättä käy, sillä kuten on jo sanottu, bitcoinien arvo kasvaa niiden määrän lisääntyessä, mikä kannustaa käyttäjiä säästämään bitcoineja (Tasca, 2015). Tämä taas aiheuttaa lisää deflaatioita, mikä vuorostaan lisää volatiliteettiä. Toisin sanoen, Bitcoinin taloudellinen malli joutuu noidankehään, jossa sillä ei ole muuta vaihtoehtoa kuin ajautua yhä syvempään deflaatioon (Barber ym., 2012).

Bitcoinin enimmäismäärään perustuva talous siis aiheuttaa selkeitä ongelmia sen käyttöön kaupankäynnissä. Keskeisintä on löytää jonkinlainen ratkaisu deflaatioon. Tätä käsitellään toiseen tutkimuskysymykseen vastatessa.

4.2.2 Louhinnan ja blockchainin heikkoudet

Ali ym. (2014a) esittävät, että louhinta käy jatkuvasti kalliimmaksi louhijoille. Tämä johtuu siitä, että lohkojen lisäämisen laskennallinen vaikeusaste lisääntyy jokaisen ratkaistun lohkon myötä, koska järjestelmän eheyden takaamiseksi lohkojen lisäysvälin pitää pysyä vakiona. Tästä syystä louhinnassa vallitsee kilpavarustelu, jossa louhintayhtymät jopa yli-investoivat louhintaan vaadittavan laskentatehon lisäämiseksi, jolloin kilpailijat voittotodennäköisyytensä maksimoimiseksi vastaavat samalla mitalla (Woo ym., 2013).

Pitemmällä aikavälillä kilpavarustelu johtaa siihen, että louhijoiden kokonaismäärä pienenee laskentatehovaatimusten noustessa ja louhinnasta saatavan palkkion pienentyessä. Kuten on jo tullut ilmi, jo nykyisellään louhinta on muutaman suuren louhintayhtymän hallitsemaa. Tämä taas lisää sitä tietoturvariskiä, että yksittäinen taho kykenee ottamaan koko Bitcoin-verkon haltuunsa. Bitcoin ei siis ole enää siinä vaiheessa hajautettu järjestelmä, vaan keskitetyn tahon hallitsema. (Eyal & Sirer, 2014.)

Louhinnan kannustimet eivät riitä nykyisellään takaamaan sitä, että louhinta toimisi pitkällä aikavälillä tehokkaasti. Kun kaikki 21 miljoonaa bitcoinia on saatu louhittua, ei bitcoineja enää makseta jokaisesta lisätystä lohkosta, vaan louhijoiden kannustimina toimivat vain jokaisesta transaktiosta perittävät käsittelymaksut (Nakamoto, 2008). Babaioffin ym. (2012) mukaan tämä kuitenkin saa aikaan sen, että louhijat ovat alkavat suosia suurten transaktioiden käsitte-

lyä isompien transaktiomaksujen toivossa ja toisaalta pimittämään tiedon transaktioista muulle vertaisverkolle, jotta voisi itse hyötyä niiden käsittelystä. Tämä tietenkin vaarantaa vertaisverkon avoimuuden periaatteen.

Blockchainin suurin ongelma on sen heikko skaalautuvuus (Barber ym., 2012; Poon & Dryja, 2016). Skaalautuvuusongelmat johtuvat siitä, että muutokset blockchainissa pitää välittää jokaiselle vertaisverkon käyttäjälle: kun käyttäjiä ja transaktioita on useita, vaaditaan verkolta enemmän tehoa ja käsittelyajat pitenevät.

Tässä tutkielmassa on aiemmin mainittu, että Bitcoin voisi soveltua hyvin mikromaksumarkkinoille, mutta skaalautuvuus asettaa sen suhteen ongelmia. Nykyisellään pitkien transaktionkäsittelyaikojensa takia Bitcoin toimii huonosti nopeiden maksujen yhteydessä, eli maksuissa, joissa raha ja palvelu vaihtuvat käyttäjien välillä nopeasti. On jopa havaittu, että nopeat maksut mahdollistavat bitcoinien kaksoiskulutuksen, jonka estäminen on Bitcoinin teknologian päätavoitteista (Karame ym., 2012). Kyky käsitellä transaktiot nopeasti olisi tärkeää Bitcoinin tulevaisuuden kannalta; tähän haasteeseen palataan kehitysmenetelmiä tarkasteltaessa.

4.2.3 Tietoturvariskit

Bitcoinin vertaisverkko on suunniteltu olemaan lähestulkoon murtamaton. Hajautetun luonteen vuoksi jos yksi vertaisverkon noodeista joutuu hyökkäyksen alaiseksi, ei sillä ole vaikutusta järjestelmän toimintaan, koska hyökkäämättömät noodit pitävät vielä valtaosaa verkosta pystyssä. Keskitetyissä verkoissa on niin sanottu heikko kohta (engl. *single point of failure*), jonka kaatuessa koko järjestelmä lamaantuu. Bitcoin-järjestelmä sen sijaan ei kaadu siihen, jos esimerkiksi yhteen noodiin kohdistetaan palvelunestohyökkäys. Tämä ei kuitenkaan takaa tutkimusten mukaan täydellistä murtamattomuutta.

Yksi pelätty tietoturvariski onkin se, että jokin osapuoli onnistuu saamaan haltuunsa yli 50 % vertaisverkosta, jolloin transaktiohistorian väärentäminen olisi mahdollista (Böhme ym., 2016). Tämä kuitenkin vaatisi valtavat määrät laskentatehoa. Näin on kuitenkin jo päässyt käymään muutamaan otteeseen: esimerkiksi vuoden 2014 aikana louhintayhtymä Ghash.IO onnistui pariin otteeseen saavuttamaan valtaosan koko verkon laskentatehosta (Tasca, 2015: 75). Lisäksi tutkimukset ovat osoittaneet (Eyal & Sirer, 2014), että verkon haltuun saamiseen ei välttämättä edes tarvita valtaosaa verkon laskentatehosta. Transaktioita pimittämällä louhintayhtymien on mahdollista niin sanottua itsekästä louhintaa (engl. *selfish mining*) hyödyntäen saada verkon haltuunsa, eikä Bitcoin-protokollassa itsessään ole keinoja tämän estämiseksi.

Myös yksittäisiin käyttäjiin kohdistuu tietoturvariskejä. Androulaki ym. (2013) selvittivät tutkimuksessaan, että jopa 40 % Bitcoinin käyttäjistä on yksilöitävissä suositeltavista suojamekanismeista (mm. usean Bitcoin-osoitteen käyttö) huolimatta. Samaa tulosta osoittaa myös Meiklejohnin ym. (2013) tutkimus, jossa tutkijat onnistuivat jäljittämään käyttäjiä seuraamalla yksittäisiä bitcoineja. Riskinä on se, että jokin rikollinen taho voi transaktioita seuraamalla

jäljittää käyttäjiä. Ongelmaa tehostaa vielä se, että useat käyttäjät uskovat Bitcoinin olevan täysin anonyymi järjestelmä, jolloin tietoturvariskien mahdollisuus tehostuu entisestään (Brezo & Bringas, 2012).

4.2.4 Kaupankäynnin riskit

Nykyisellään Bitcoinin käyttö elektronisessa liiketoiminnassa on riippuvaista kolmansien osapuolten palveluista (Yermack, 2013). Monet Bitcoinin käyttöön liittyvät riskit elektronisessa liiketoiminnassa liittyvätkin vertaisverkon ja maksujärjestelmän ulkopuolisiin tekijöihin. Koska edelleen suurin osa kaupankäynnistä käydään vertaisverkon ulkopuolella maksupalveluita ja vaihdantapaikkoja käyttäen, on selvää, että Bitcoinin ominaiset hyödyt menetetään.

Yksi Bitcoinin perusajatuksista on olla vapaa kolmansista osapuolista maksutapahtumissa. Mutta kun kaupankäyntiin tarvitaan esimerkiksi maksupalvelu, ei tämä ehto toteudu, vaan maksutapahtumista tulee taas keskitettyjä. Bitcoinin ympärille muodostunut kolmansien osapuolten palveluntarjoajien ekosysteemi on siis paradoksaalisesti suurin riski kaupankäynnissä, vaikka samalla se onkin suurin kasvualusta Bitcoinille.

Kaupankäynnissä suurin riski aiheutuu bitcoinien varastamisesta tai katoamisesta eri palveluista, kuten aiemmin mainittu vaihdantapaikka MtGoxin kaatuminen osoittaa (Moore & Christin, 2013). Bitcoinin oma maksujärjestelmä on hyvin suojattu murtoyrityksiltä sen hajautetun luonteen vuoksi. Tämä ei kuitenkaan päde kolmannen osapuolten sovelluksissa. Tietomurrot ja palvelunestohyökkäykset vaihdantapaikkoihin ja Bitcoin-lompakoihin ovat olleet yleisiä, ja bitcoineja on ryöstetty paljon, jolloin voidaan puhua digitaalisesta taskuvarkaudesta (Brezo & Bringas, 2012). Vaikka blockchainia ei pysty murtamaan, ellei hallitse valtaosaa vertaisverkosta, on vaihdantapaikoilla aivan samat riskit kuin muillakin verkkopalveluilla.

Kaupankäynnin riskeihin on vaikeaa löytää ratkaisua Bitcoinia kehittämällä, sillä ne riippuvat kolmannen osapuolen toimijoista. Yhtenä ratkaisuna pidetään kolmannen osapuolen toiminnan säätelyä, mihin otetaan kantaa tämän tutkielman seuraavassa pääluvussa.

5 BITCOININ KEHITTÄMISMAHDOLLISUUDET

Tässä luvussa kuvaillaan, minkälaisia kehitysehdotuksia on tehty, jotta Bitcoinista tai sen teknologioiden pohjalta saisi luotettavamman ja siten helpommin hyväksyttävän maksuvälineen elektroniseen liiketoimintaan. Edellisen luvun haasteiden pohjalta muodostetaan tässä luvussa kehitysmahdollisuudet.

Bitcoinin kehittämismahdollisuudet käydään läpi kategorioittain. Joidenkin kehitysmenetelmien laajuuden takia niihin perehdytään vain pintapuolisesti. Ensin tarkastellaan, miten tietoturvaa on ehdotettu parannettavaksi. Sitten keskitytään maksujärjestelmän keskeisten teknologioiden, eli blockchainin ja louhinnan kehittämiseen. Seuraavaksi tarkastellaan, miten bitcoinin volatiliteettiä voisi hallita. Lopuksi kuvaillaan, miten Bitcoinin säätelyllä kaupankäynnissä voisi parantaa sen käyttöä ja toisaalta myös, miksi joidenkin lähteiden mukaan Bitcoinia ei pitäisi säädellä.

5.1 Tietoturvan parantaminen

Eräs jo käyttöön otettu menetelmä käyttäjien yksityisyyden suojaamiseksi on niin kutsuttujen transaktioiden sekoittimien (engl. *Bitcoin mixers*) käyttö. Menetelmä perustuu siihen, että usean maksajan maksut yhdistetään keskenään kolmannen osapuolen palveluntarjoajan toimesta ja sekoitetaan, jolloin yksittäisten käyttäjien jäljittäminen vaikeutuu (Böhme ym., 2016). Ongelmiksi tässä vain muodostuvat palveluntarjoajan luotettavuus ja se, että transaktioiden käsittelyaika pitenee entisestään.

Barber ym. (2012) ehdottavat niin sanottua *fair exchange* -protokollaa maksujen anonymiteetin parantamiseksi. Protokollassa maksutapahtuma jaetaan kolmeen erilliseen transaktioon: sitoutumis-, hyvitys- ja saamismaksuihin. Käyttäjä tekee silti vain yhden maksun, mutta protokolla tekee jaottelun automaattisesti. Ajatuksena on se, että maksun tapahtuessa kryptografiaa hyödyntäen tehdään eräänlainen maksusopimus osapuolten välillä. Tämän protokollan

etu on se, ettei kolmannen osapuolen käsittelijöitä tarvita ja transaktioajat lyhenevät.

Yksi kokonaisvaltaisempi ehdotus yksityisyyden suojaamiseksi maksuissa on Zerocash-protokolla. Sen ajatuksena on salata niin osoitteet kuin maksujen suuruus blockchainiin tallennetusta transaktiohistoriasta. Tämä tekee käyttäjien jäljittämisestä hankalampaa, ellei peräti mahdotonta. Toiminta perustuu siihen, että käyttäjät voivat muuttaa tavallisia bitcoineja erikoisiksi zerocoineiksi, joita ei voi jäljittää. Suunnitteilla onkin Zerocashia käyttävä Bitcoinista erillinen kryptovaluutta Zcash[3]. (Ben-Sasson, Chiesa, Garman, Green, Miers, Tromer & Virza, 2014.)

5.2 Blockchainin ja louhinnan kehittäminen

Blockchainin keskeisimmäksi ongelmaksi määriteltiin viime luvussa heikko skaalautuvuus. Barber ym. (2012) ideoivat ratkaisuksi palvelua, joka suodattaisi transaktiot siten, että käyttäjät saisivat tiedon vain itselleen relevanteista transaktioista. Kaikki transaktiot olisivat julkisina edelleen blockchainissa, mutta niitä ei tarvitsisi lähettää jokaiselle vertaisverkon käyttäjälle. Ajatuksen vievät pitemmälle Poon & Dryja (2016) vielä suunnitteilla olevassa *Bitcoin lightning network* -protokollassaan[4], jonka tarkoituksena on mahdollistaa nopeat transaktiot ja toimiva skaalautuvuus. Toiminta perustuu siihen, että käyttäjien välille muodostetaan mikromaksukanavien verkko, joka toimii blockchainin ulkopuolella.

Louhinnan suurimmiksi ongelmiksi kartoitettiin kestämätön kannustinmalli ja siitä johtuva louhinnan keskittyminen vain muutaman louhintayhtymän vastuulle. Babaioff ym. (2012) ehdottavat parempaa kannustinmallia, joka perustuu siihen, että louhijoita palkitaan transaktioiden välittämisestä muille louhijoille ja vertaisverkon avoimuuden tukemisesta. Näin transaktiomaksuista saa taas kannattavia.

Jos yksittäinen taho, esimerkiksi louhintayhtymä, onnistuu saamaan Bitcoin-verkon haltuunsa, se voi muokata verkon transaktiohistoriaa ja siten esimerkiksi varastaa bitcoineja. Barber ym. (2012) esittävät menetelmän, joilla tämän riskin todennäköisyyttä voisi vähentää. Vertaisverkon noodit voisivat tallentaa tilannekatsauksia blockchainista aina tietyin väliajoin. Näin jokainen noodi voisi varmentaa transaktiohistorian oikeellisuuden vertaamalla sitä tilannekatsauksiinsa.

[3] http://z.cash/
[4] http://lightning.network/

5.3 Volatiliteetin ja deflaation parantaminen

Bitcoinin valuuttana keskeiseksi ongelmaksi määriteltiin aiemmin sen deflaatio, mistä pohjimmiltaan juontuu myös korkea volatiliteetti ja se, että bitcoineja mieluummin säästetään kuin käytetään. Ongelmaan on vastattu muissa kryptovaluutoissa, kuten Primecoinissa ja Peercoinissa, tekemällä ehtymätön määrä rahaa louhittavaksi, mikä tekee niistä inflatorisia valuuttoja (Böhme ym., 2016:234). Barber ym. (2012) ehdottavat myös inflatorisen säätelymekanismin rakentamista rahojen louhintaan: rahamäärä kasvaisi esimerkiksi transaktiomäärien mukaan. Näin mittavaa muutosta kuitenkaan Bitcoinin protokolla voi tukea, joten ainoa ratkaisu olisi uuden kryptovaluutan kehittäminen.

Ametrano (2014) esittelee artikkelissaan Hayek Money -protokollan, joka tarjoaa ratkaisun deflaatioon ja siten myös volatiliteettiin. Tarkoituksena on löytää ratkaisu Bitcoinin rahantuotannon joustamattomuuteen. Ratkaisuna tähän pidetään, että jokaisen käyttäjän bitcoin-määrää voisi säädellä sen sijaan, että valuutan arvo muuttuisi. Säätely perustuisi vertaisverkossa muodostettavaan konsensukseen. Järjestelmän toimivuudesta ei tosin ole todistusaineistoa, sillä sitä ei ole käytetty vielä missään kryptovaluutassa.

5.4 Bitcoinin säätely kaupankäynnissä

Kysymys siitä, missä määrin jonkin virallisen tahon pitäisi säädellä Bitcoinia, on aiheuttanut paljon keskustelua niin puolesta kuin vastaan. Erityisesti bitcoinien ryöstäminen ja katoaminen vaihdantapaikoilta sekä transaktioiden peruuttamattomuus ovat herättäneet kysymyksiä kuluttajansuojasta Bitcoinin käytössä (Böhme ym., 2016; Papp, 2014). Lisäksi esimerkiksi aiemmin mainitun verkkokauppa SilkRoadin tapaus ovat luoneet säätelylle kysyntää rikollisen toiminnan hillitsemiseksi (Böhme ym., 2016).

Koska itse Bitcoinia on vaikea lähteä säätelemään sen hajautetun luonteen vuoksi, säätelypyrkimykset kohdistuvatkin kolmannen osapuolen palveluntarjoajiin (Böhme ym., 2016). Erityisesti vaihdantapaikoissa tarvitaan säätelyä: on esitetty, että mikäli vaihdantapaikkojen käyttäjämäärät lisääntyvät, kansainvälinen valuutanvaihto vaarantuu (Plassaras, 2013). Ilman vaihdantapaikkojen säätelyä bitcoinien käyttö sijoituskohteena maksuvälineen sijaan todennäköisesti jatkuu, mikä heikentää kaupankäyntiä (Papp, 2014).

Toisaalta on myös katsottu, ettei Bitcoinin kaupankäyntiä pitäisi säädellä. White (2014) perustelee säätelemättömyyden siten, että Bitcoinin markkinat ovat vielä nuoret, ja niiden pitäisi antaa vielä kehittyä vapaina markkinoina. Samaa mieltä on Kaplanov (2012), jonka mukaan Bitcoinin säätelemättömyys tuottaa lisää talouskasvua ja liiketoimintamahdollisuuksia, kuten Bitcoinin kasvava ekosysteemi on osoittanut.

6 YHTEENVETO

Tässä tutkielmassa tutkittiin Bitcoinia ja sen käyttöä elektronisessa liiketoiminnassa haasteisiin ja mahdollisuuksiin keskittyen. Tutkimusmenetelmänä käytettiin kirjallisuuskatsausta eri tutkimusartikkeleita hyödyntäen. Tutkimuskysymyksiä oli kaksi: mitkä ovat Bitcoinin hyödyt ja haitat elektronisessa liiketoiminnassa, sekä miten Bitcoinista voisi kehittää paremman maksuvälineen.

Aluksi esiteltiin lyhyesti, mikä Bitcoin on ja miten se toimii, sitten esiteltiin elektronisen liiketoiminnan maksujärjestelmät ja markkinat, joilla Bitcoin voisi menestyä. Samalla tunnistettiin jo alustavasti keskeisiä ongelmia niin Bitcoinin käytössä valuuttana kuin maksujärjestelmänä. Sitten syvennyttiin tarkemmin Bitcoinin hyötyihin ja haittoihin, joiden pohjalta kartoitettiin kehittämismahdollisuudet.

Keskeisenä tuloksena havaittiin, että Bitcoinin haitat elektronisessa liiketoiminnassa jättävät suurilta osin varjoonsa sen tarjoamat hyödyt. Tästä syystä valtavirran toimijoiden on vaikea hyväksyä Bitcoinia, jolloin sen käyttö todennäköisesti pysyy vielä marginaalisena. Kehittämiselle on siis paljon tarvetta, jotta Bitcoinista saisi toimivan valuutan.

Bitcoinin ekosysteemi on jo nykyisellään kehittynyt varsin monipuoliseksi kokonaisuudeksi. Mielenkiintoinen havainto tätä tutkielmaa tehdessä oli huomata, että kolmannen osapuolen palveluntarjoajista koostuva ekosysteemi tarjoaa Bitcoinille sekä parhaat kasvumahdollisuudet, mutta samalla suurimmat liiketoiminnalliset riskit. Markkinoiden hurjat käänteet ovat tosin selitettävissä sillä, että Bitcoin on vielä verrattain nuori maksujärjestelmä ja valuutta, joten sen ekosysteemi ei ole vielä kovin vakiintunut. Tietomurrot, rikolliset verkkokaupat ja käyttäjien yksityisyyteen liittyvät ongelmat todennäköisesti vähenevät, mikäli Bitcoin jatkaa kasvuaan vielä seuraavat vuodet.

Selvää on kuitenkin, että Bitcoin ja sen jälkeen kehittyneet kryptovaluutat ovat tuoneet tullessaan muutoksen ihmisten välisiin maksutapahtumiin, ja sen vaikutuksia on alettu huomata vasta viime aikoina. Olemme siirtymässä uuteen Internet-aikakauteen, jolle on ominaista käyttäjien välinen yhteistyö, kuten joukkorahoitukset, yhteisöllisyys ja suorat maksutapahtumat vertaisten välillä (Tasca, 2015: 8).

Vain aika näyttää, voiko Bitcoin vielä kehittyä varteenotettavaksi maksujärjestelmäksi vai onko sen kohtalona jäädä suunnannäyttäjäksi. Monet nuoremmat kryptovaluutat ovat korvanneet Bitcoinin puutteita ja vieneet sen ideaa vielä pidemmälle. Toisaalta Bitcoin on tällä hetkellä ylivoimaisesti tunnetuin, joten nuoremmilla kryptovaluutoilla on suuri kynnys päästä suurempaan julkisuuteen.

Tärkeä havainto oli myös se, että blockchain on todennäköisesti Bitcoinin tärkein yksittäinen ominaisuus ja sen suurin innovaatio. Blockchain on jo nykyisellään mahdollistanut monenlaisia uusia palveluita, ja sitä tullaan todennäköisesti soveltamaan ennennäkemättömillä tavoilla. Jatkotutkimusaihetta ajatelleen blockchain voisikin olla mielenkiintoinen tutkimuskohde, sillä mitään sen kaltaista ei ole ennen ollut. Lisäksi blockchainin tarjoamat mahdollisuudet ovat vielä kartoittamatta.

LÄHTEET

Ali R., Barrdear J., Clews R. & Southgate J. (2014a). The economics of digital currencies. *Bank of England Quarterly Bulletin* , Q3.

Ali R., Barrdear J., Clews R. & Southgate J. (2014b). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin* , Q3.

Ametrano F. M. (2014). Hayek money: The cryptocurrency price stability solution. *Available at SSRN 2425270*

Androulaki E., Karame G. O., Roeschlin M., Scherer T. & Capkun S. (2013). Evaluating user privacy in Bitcoin. *Financial cryptography and data security* (s. 34-51) Springer.

Babaioff M., Dobzinski S., Oren S. & Zohar A. (2012). On Bitcoin and Red Balloons. *Proceedings of the 13th ACM Conference on Electronic Commerce,* 56-73.

Back A. (2002). Hashcash – a Denial of Service Counter-Measure

Baddeley M. (2004). Using e-cash in the new economy: An economic analysis of micro-payment systems. *Journal of Electronic Commerce Research 5*(4), 239-253.

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. 399-414) Springer.

Ben-Sasson E., Chiesa A., Garman C., Green M., Miers I., Tromer E. & Virza M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *Security and Privacy (SP), 2014 IEEE Symposium on,* 459-474.

Bhatla T. P., Prabhu V. & Dua A. (2003). Understanding credit card frauds. *Cards Business Review 1(6)*

Brezo F. & Bringas P. G. (2012). Issues and risks associated with cryptocurrencies such as bitcoin. *The Second International Conference on Social Eco-Informatics*

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives 29*(2), 213-238.

Chaum D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology,* 199-203.

Christin N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. *Proceedings of the 22nd International Conference on World Wide Web,* 213-224.

Dwyer G. P. (2015). The economics of bitcoin and similar private digital currencies. *Journal of Financial Stability 17*, 81-91.

Eyal I. & Sirer E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. *Financial cryptography and data security* (s. 436-454) Springer.

Glaser F., Zimmermann K., Haferkorn M., Weber M. C. & Siering M. (2014). Bitcoin-asset or currency? revealing users' hidden intentions. *Revealing Users' Hidden Intentions (April 15, 2014).ECIS*

Grinberg R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal 4*, 160.

Kaplanov N. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loy.Consumer L.Rev. 25*, 111.

Karame G. O., Androulaki E. & Capkun S. (2012). Double-spending fast payments in bitcoin. *Proceedings of the 2012 ACM Conference on Computer and Communications Security,* 906-917.

Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G. M. & Savage S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. *Proceedings of the 2013 Conference on Internet Measurement Conference,* 127-140.

Moore T. & Christin N. (2013). Beware the middleman: Empirical analysis of bitcoin-exchange risk. *Financial cryptography and data security* (s. 25-33) Springer.

Nakamoto S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted 1*(2012), 28.

Papp, J. (2015). A Medium of Exchange for an Internet Age: How to Regulate Bitcoin for the Growth of E-Commerce. *Pittsburgh Journal of Technology Law and Policy, 15(1)*, 33-56.

Plassaras N. A. (2013). Regulating digital currencies: Bringing bitcoin within the reach of IMF. *Chi.J.Int'l L. 14*, 377.

Poon, J., & Dryja, T. (2015). The bitcoin lightning network: Scalable off-chain instant payments. Technical Report (draft). https://lightning.network

Sumanjeet S. (2009). Emergence of payment systems in the age of electronic commerce: The state of art. *Global Journal of International Business Research 2*(2)

Tasca P. (2015). Digital currencies: Principles, trends, opportunities, and risks. *ECUREX (September 7, 2015)*

Velde F. (2013). Bitcoin: A primer. *Chicago Fed Letter,* Dec.

White, L. H. (2015). The Market for Cryptocurrencies. *Cato Journal*, 35(2).

Woo, D., Gordon, I., & Iaralov, V. (2013). Bitcoin: a first assessment. *Bank of America Merrill Lynch*, Dec.

Yermack, D. (2013). Is Bitcoin a Real Currency? An economic appraisal. *NBER Working Paper Series*, 19747.

Zwass V. (1996). Electronic commerce: Structures and issues. *International Journal of Electronic Commerce 1*(1), 3-23.