



LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

BITCOIN VERKKOKAUPAN MAKSUVÄLINEENÄ

Case: Lahden Datatronic Oy

LAHDEN
AMMATTIKORKEAKOULU
Liiketalouden ala
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Syksy 2013
Sanna Korhonen

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

KORHONEN, SANNA:

Bitcoin verkkokaupan maksuvälineenä
Case: Lahden Datatronic Oy

Tietojenkäsittelyn opinnäytetyö

42 sivua, 1 liitesivu

Syksy 2013

TIIVISTELMÄ

Tämän opinnäytetyön aiheena on bitcoinmaksujen vastaanottaminen verkkokaupassa. Työn tilaaja on Lahden Datatronic Oy ja työn tarkoituksena on selvittää sille sopivin ratkaisu bitcoinmaksujen vastaanottamiseen tietoturvan näkökulmasta. Työ on kartoittava tapaustudkimus.

Työn teoriaosuudessa tutustutaan bitcoiniin ja selvitetään sen keskeiset toimintaperiaatteet. Lisäksi esitellään erilaisia vaihtoehtoja bitcoinmaksujen vastaanottamiseen verkkokaupassa ja arvioidaan bitcoinmaksuliikenteen tietoturvallisuutta verkkokaupassa.

Tutkimus oli laadullinen ja siinä selvitettiin käyttäjäkokemuksia niiltä yrityksiltä, jotka jo hyväksyvät bitcoinmaksuja verkkokaupassaan. Tiedonkeruumenetelmänä käytettiin sähköpostikyselyä. Tutkimuksesta ilmeni, että bitcoinmaksujen hyväksyminen verkkokaupan maksuvälineenä käytetystä tavasta riippumatta koettiin erittäin helppona ja turvallisena.

Erilaisia vaihtoehtoja bitcoinmaksujen vastaanottamiseen on runsaasti ja tässä työssä tutustuttiin niistä sellaisiin, jotka ovat jollain tavoin soveltuvia toimeksiantajan tapaukseen. Työn johtopäätöksenä sopivin ratkaisu toimeksiantajalle on kolmannen osapuolen palveluntarjoajan käyttäminen, mikä vastaa parhaiten yrityksen tämän hetkisiin tarpeisiin ja toiveisiin.

Asiasanat: verkkokaupan maksuliikenne, bitcoin, virtuaalivaluutta

Lahti University of Applied Sciences
Degree Programme in Information Technology

KORHONEN, SANNA:

Bitcoin as Payment Method
for Online Store
Case:
Lahden Datatronic Oy

Bachelor's Thesis in Information Technology

42 pages, 1 appendix

Autumn 2013

ABSTRACT

This thesis deals with accepting bitcoin payments in an online store. The thesis was commissioned by Lahden Datatronic Oy. The purpose of this study was to find out the best method for handling bitcoin payments from the aspect of information security. This study is a case study survey.

The theoretical section of this thesis is about bitcoin and the main operational principles of it. In addition various different methods are presented for accepting bitcoin payments in an online store. The theoretical section also discusses the information security of bitcoin payment processing in an online store.

The research method was qualitative and a questionnaire survey was conducted with a goal to examine user experiences in companies that already accept bitcoins as a payment method for their online store. The survey was carried out as an e-mail survey. The results show that all respondents found accepting bitcoin payments very easy and safe, regardless of the method used.

There are various different methods for handling bitcoin payments and in this study only those somehow appropriate for the commissioner were examined. As a conclusion it was found that the best method for the commissioner to handle bitcoin payments was to use a third party service provider as it responded best to the current needs and hopes of the company.

Key words: online payments, bitcoin, virtual currency

SISÄLLYS

1	JOHDANTO	1
1.1	Tutkimusongelma	2
1.2	Viitekehys	3
1.3	Tutkimusmenetelmä	5
1.4	Lahden Datatronic Oy	6
2	BITCOIN	7
2.1	Yleistä bitcoinista	7
2.2	Bitcoinin historiaa	8
2.3	Bitcoinin toimintaperiaate	8
2.3.1	Lohkoketju	9
2.3.2	Lohko	9
2.3.3	Bitcoin-osoitteet	10
2.3.4	Transaktiot	11
2.3.5	Louhinta	13
3	BITCOINIEN SÄILYTTÄMINEN JA KÄYTTÄMINEN	14
3.1	Lompakot	14
3.2	Bitcoin-asiakasohjelma	14
3.3	Selainpohjaiset lompakot	14
3.4	Aivo- ja paperilompakot	15
3.5	Muut säilytysmenetelmät	16
3.6	Bitcoinien käyttäminen	17
4	VERKKOKAUPAN MAKSULIIKENTEN TIETOTURVALLISUUS	18
4.1	Tietoturvallisuus	18
4.2	Bitcoinmaksuliikenteen julkisuus	18
4.3	Käyttäjän vastuu	19
4.4	Säilytys	20
4.5	Maksujen vastaanottaminen	22
5	BITCOINMAKSUJEN HYVÄKSYMINEN VERKKOKAUPASSA	23
5.1	Verotus	23
5.2	Kirjanpito	24
5.3	Maksuliikenteen vaihtoehdot	24
5.3.1	Asiakasohjelman käyttö maksujen vastaanottamiseen	25

5.3.2	Osoitteiden etukäteisluonti	26
5.3.3	Ulkopuoliset palveluntarjoajat	26
6	TUTKIMUSTULOKSET	30
6.1	Tutkimusaineisto	30
6.2	Aineiston analyysiprosessi	30
6.3	Analyysi	31
6.3.1	Yleinen toimivuus	31
6.3.2	Maksutavan käyttöönotto	32
6.3.3	Maksutapahtumien käsittely	33
6.3.4	Turvallisuus	33
7	JOHTOPÄÄTÖKSET	35
8	YHTEENVETO	38
	LÄHTEET	40
	LIITTEET	42

SANASTO

Julkinen avain - Vapaasti jaettavissa oleva salaamiseen käytettävä luku.

Kryptografia - Salakirjoituksen tiede.

Proof-Of-Work - Menetelmä, jolla tehtävän suorittaminen (esimerkiksi salauksen purkaminen) on tehty vaikeaksi, mutta suoritettun tehtävän tarkistaminen helpoksi.

QR-koodi (Quick Responce) - Kaksiulotteinen kuviokoodi, jonka sisältö on luettavissa ja purettavissa helposti esimerkiksi älypuhelimella.

SEPA (Single Euro Payments Area) - Yhtenäinen euromaksualue.

Tiiviste - Tiedon tiivistäminen pienempään tilaan niin, että alkuperäistä tietoa voidaan vertailla vertailemalla tiivisteitä.

Vertaisverkko - Verkko, jossa jokainen taho toimii sekä palvelimena että asiakkaana verkon muille jäsenille.

Virtuaalivaluutta - Digitaalinen käytäntö, jolla rahaa voidaan siirtää käyttäjältä toiselle.

Yksityinen avain - Julkisesta avaimesta johdettu, salassa pidettävä, salauksen purkamiseen käytettävä luku.

1 JOHDANTO

Viime vuosien taloustilanteen heilahtelut ja epäluottamus pankkien toimintatapoihin ovat saaneet ihmiset etsimään ja luomaan uusia ratkaisuja vaihdannan välineiksi. Talouden epävakauden synnyttämät uhkakuvat ovat herättäneet tarvetta varautua myös siihen, että koko talousjärjestelmä romahtaa. Suurten keskuspankkien hallitseman rahatalouden koetaan olevan liian kaukana ihmisten arkipäiväisestä elämästä ja sen vaikutusten olevan suhteettoman suuria.

Nykyään halutaan enemmän vapautta, riippumattomuutta ja mahdollisuuksia vaikuttaa omaan elämään. Valvonnan, määräysten ja säännösten jatkuva lisääntyminen on herättänyt monella taholla vastustusta ja halua irtautua ”isoveljen” valvonnasta. Monimutkaisten järjestelmien sijaan on alettu etsiä uusia järkevämpiä, edullisempia ja ihmisläheisempiä ratkaisuja. Aikapankit, jakamistalous, vaihtopiirit ja erilaiset vertaisvaluutat ovat esimerkkejä uusista tai uudelleen käyttöön otetuista tavoista, jotka kaikki pyrkivät siirtämään edes osan talousjärjestelmästä takaisin ihmisten omaan hallintaan.

Virtuaalivaluutta bitcoin on osa tätä kehitystä ja siitä on muutamassa vuodessa tullut yksi merkittävimmistä uuden sukupolven virtuaalisista maksuvälineistä. Bitcoin on vapaa kaikesta byrokratiasta, eikä sitä omista tai hallinnoi mikään yksittäinen taho, vaan se on täysin käyttäjiensä määrittelemä ja valvoma. Kuka tahansa, missä päin maailmaa tahansa voi käyttää bitcoinia, käyttäminen vaatii vain verkkoyhteyden. Rahan siirto toiselle puolelle maapalloa tapahtuu hetkessä ja täysin ilmaiseksi. Bitcoinia ei voi väärentää, eikä sen arvoon voida vaikuttaa uutta rahaa luomalla, vaan sen arvo määräytyy suoraan kysynnän ja tarjonnan mukaan.

Tuotteiden ja palvelujen ostaminen verkkokaupasta lisääntyy koko ajan. Pankkien ja luottokorttiyhtiöiden kautta tehdyt rahansiirrot ovat kuitenkin kalliita ja erityisesti pienten maksuerien osalta kulut saattavat olla huomattavan suuri osa kaupan loppusummasta. Maksujen prosessointi on myös hidasta ja erityisesti kansainvälisten maksujen osalta rahan siirtyminen tililtä toiselle kestää useita päiviä. Bitcoin-siirrot tapahtuvat suoraan käyttäjältä toiselle ilman välikäsiä, nopeasti ja kuluttomasti.

Bitcoin on ollut viime aikoina paljon esillä mediassa myös Suomessa ja se on herättänyt runsaasti keskustelua ja ihmetystä sekä julkishallinnon, että yksityisten ihmisten keskuudessa. Joidenkin näkemysten mukaan bitcoin on vain pienen piirin keinotteluväline, tai utopistinen leikkiraha, mutta yhä useammat ovat alkaneet suhtautua siihen varteenotettavana maksuvälineenä virallisten valuuttojen rinnalla. Vaikka bitcoin on myös säästö- ja sijoituskohde, sen ensisijainen tarkoitus on kuitenkin toimia maksuvälineenä. Jotta bitcoin olisi varteenotettava maksuväline, on sitä voitava käyttää monenlaisten hyödykkeiden ja palveluiden hankkimiseen. Suomalainen Bitcoin-yhteisö tekee jatkuvasti työtä edistääkseen ja helpottaakseen bitcoinin käyttöä ja on esimerkiksi tätä opinnäytetyötä tehtäessä juuri tuomassa Suomeen ensimmäistä bitcoin-automaattia.

Bitcoinista on tehty tutkimuksia sen turvallisuudesta, taloustieteellisestä vaikutuksesta ja yksittäisten teknisten ominaisuuksien toimivuudesta. Vaikka bitcoinista on saatavilla runsaasti tietoa ja erilaisia oppaita, ei tutkimuksia tai selvityksiä sen hyväksymisestä verkkokaupan maksuvälineenä ole tehty. Tämä johtuu osaksi siitä, että bitcoin on vielä kovin tuore ilmiö ja sen käyttö marginaalista. Bitcoinin maksuvälineenä hyväksyvät yritykset ovat myös suurimmaksi osaksi olleet siitä jo aiemmin kiinnostuneita ja käyttäneet sitä maksuvälineenä muutenkin, jolloin tieto erilaisista tavoista on ollut helposti saatavilla ja omaksuttavissa.

Tämä opinnäytetyö on tehty sellaista yritystä varten, jolla ei vielä ole kovinkaan paljon tietoa bitcoinista tai sen käytöstä, mutta joka kuitenkin haluaa tietoa mahdollisuuksista vastaanottaa bitcoinmaksuja. Opinnäytetyön tarkoituksena ei ole olla yleistettävä opas maksujen vastaanottamisen aloittamiseen, mutta se antaa kokonaiskuvan siitä, mitä bitcoinmaksujen vastaanottaminen verkkokaupassa vaatii.

1.1 Tutkimusongelma

Tämän opinnäytetyön tarkoituksena on kartoittaa tarjolla olevia erilaisia tapoja bitcoinmaksujen vastaanottamiseen toimeksiantajan verkkokaupassa ja selvittää, mikä tapa olisi erityisesti tietoturvallisuuden näkökulmasta sopivin.

Tutkimuskysymys on: Minkälainen ratkaisu bitcoinin hyväksymiseen

verkkokaupan maksuvälineenä olisi yritykselle sopivin tietoturvallisuuden näkökulmasta? Kysymys on luonteeltaan tutkaileva ja kartoittava. Työssä tutkitaan ensin mitä toimia vaatii se, että verkkokauppa alkaa ottaa vastaan bitcoinmaksuja. Sen jälkeen selvitetään, mitä tietoturvariskejä bitcoinmaksujen vastaanottamiseen liittyy ja kuinka maksujen vastaanottaminen vaikuttaa yrityksen toimintaan. Lopuksi löydetyistä vaihtoehdoista pyritään löytämään sopivin juuri Datatronicin tapaukseen.

Tämän opinnäytetyön päätavoitteena on selvittää toimeksiantajalle sopivin ratkaisu bitcoinmaksujen vastaanottamiseen verkkokaupassa. Tavoitteena on antaa tietoa bitcoinista ja tutkia sen käyttöönottoa verkkokaupan maksuvälineenä. Työssä selvitetään, minkälaisia toimia bitcoinin käyttöönotto verkkokaupan maksuvälineenä vaatii, minkälaisia vaihtoehtoja on tarjolla ja mikä niistä olisi toimeksiantajalle sopivin ratkaisu. Työssä pohditaan yleisellä tasolla, minkälaisia tietoturvakysymyksiä maksujen vastaanottamiseen liittyy ja arvioidaan käytettävyyttä yrityksen kannalta tietoturvallisuuden osa-alueena, mutta myös valitun maksutavan käyttöönottoon liittyvien ratkaisujen helppouden suhteen. Opinnäytetyössä selvitetään käyttäjäkokemusten avulla, minkälaiseksi bitcoinia jo käyttävät yritykset kokevat sen käytön, kuinka turvalliseksi ja helppokäyttöiseksi he ovat kokeneet valitsemansa menetelmän käyttöönoton ja maksujen vastaanottamisen.

Työn tilaaja on Lahden Datatronic Oy, jonka tarkoituksena ei ole aivan lähiaikoina ottaa bitcoinia maksuvälineeksi, mutta joka on kiinnostunut aiheesta. Bitcoinmaksujen vastaanottaminen tulevaisuudessa ei ole ainakaan toistaiseksi poissuljettu vaihtoehto. Tämä opinnäytetyö hyödyttää myös muita bitcoinin hyväksymistä suunnittelevia yrityksiä antaen tietoa eri vaihtoehdoista.

1.2 Viitekehys

Tässä opinnäytetyössä bitcoinia tarkastellaan valuuttana ja sen käyttöä kuin mitä tahansa valuuttaa erotuksena ne ominaispiirteet, jotka vaikuttavat sen käyttöön. Työssä keskitytään bitcoinin verkkokaupan maksuliikenteen kannalta ja siksi teoriaosuudessa pyritään antamaan lukijalle kokonaiskuva bitcoinista käsittelemällä vain tämän työn kannalta olennaisia asioita.

Verkkokaupan maksuliikenteeseen kuuluu monia osa-alueita ja sitä voidaan tarkastella sekä myyjän, että ostajan näkökulmasta. Tässä työssä maksuliikennettä tarkastellaan ainoastaan verkkokaupparytyksen näkökulmasta ja maksuliikennettä käsitellään pääosin bitcoinin osalta. Myös muihin maksutapoihin viitataan niissä tilanteissa, jolloin se auttaa selvittämään bitcoinin ominaispiirteitä ja ymmärtämään niiden vaikutusta. Työn tarkoituksena on selvittää toimeksiantajalle sopivin ratkaisu bitcoinmaksujen vastaanottamiseen. Ratkaisulla tarkoitetaan niitä toimia ja valittuja palveluita, joita vaaditaan bitcoinmaksujen vastaanottamiseen. Tämän opinnäytetyön puitteissa ei toteuteta valittua ratkaisua, eikä kuvata yksityiskohtaisesti ratkaisun käyttöönoton vaatimia toimia. Sopivuutta arvioidaan helppouden, edullisuuden ja turvallisuuden ja muiden vertailtavissa olevien tekijöiden kannalta.

Tässä työssä käsitellään tietoturvallisuutta bitcoinin osalta käytettäessä sitä maksujen vastaanottamiseen verkkokaupassa, sekä sen käyttöön, säilyttämiseen ja maksuliikenteeseen liittyviä uhkia ja tarkastellaan keinoja niihin varautumiseen ja niiden ehkäisyyn. Työssä ei tutkita bitcoin-verkon tietoturvallisuutta, sen toimintaan tai toteutukseen liittyviä uhkia tai haavoittuvuuksia eikä arvioida siihen liittyviä riskejä. Verkkokaupankäynnin tietoturvallisuutta ei tarkastella laajemmin tai muiden maksutapojen osalta muutoin, kuin niissä tilanteissa, jolloin niihin vertaaminen auttaa ymmärtämään bitcoinin ominaispiirteitä.

Tässä opinnäytetyössä ei tutkita bitcoinin toimivuutta valuuttana, eikä sen merkitystä tai vaikutusta taloustieteelliseltä kannalta. Tutkimustuloksia arvioidaan yrityksen näkökulmasta ja esimerkiksi verkkokaupan asiakkaan osalta käytettävyyttä ja tietoturvaa tarkastellaan vain niiltä osin, kuin sen voi olettaa olevan yritykselle merkityksellistä asiakastytyväisyyden osalta. Tässä työssä ei oteta kantaa bitcoiniin yhdistettyihin lieveilmiöihin, eikä työn tarkoituksena ei ole estää tai edistää bitcoinin käyttöä. Bitcoinin toimintaperiaate esitetään teoriaosuudessa niin, että valuutan toiminta ja sen erityispiirteet ymmärretään. Toiminnan kuvauksessa ei syvennytä teknisiin yksityiskohtiin, ellei niillä ole tutkimuksen tavoitteen tai toiminnan ymmärtämisen kannalta oleellista merkitystä.

1.3 Tutkimusmenetelmä

Tutkimus on laadullinen kartoittava tapaustutkimus, lähestymistapa on pääosin induktiivinen. Käyttäjäkokemusten analyysissä lähestymistapa on kuitenkin deduktiivinen, sillä tuloksista pyritään etsimään teoriaosuudesta esiin nousseita asioita. Tutkimus on tapaustutkimus, sillä tutkimuksessa keskitytään tietyn yrityksen tiettyyn maksuvälineeseen ja sen käyttöönottoon. Työssä ei pyritä löytämään yleisesti parasta tapaa bitcoinien vastaanottamiseen, vaan keskitytään juuri Datatronicin tämänhetkiseen tilanteeseen.

Koska bitcoinin käyttö on vielä kovin vähäistä, eikä se ole suomalaisissa verkkokaupoissa kovinkaan yleinen maksuväline, ei aineistoa tällä hetkellä käytössä olevista tavoista ole juuri saatavilla. Tutkimusongelman luonne on kyselevä ja kartoittava, useita vaihtoehtoja vertaileva, joten sen ratkaisemiseksi on pyrittävä saamaan kokemukseräistä tietoa niiltä yrityksiltä, jotka bitcoinin maksuvälineenä jo hyväksyvät. Teoriaosuudessa esiin tulevia vaihtoehtoja vertailtaessa tuovat käyttäjien kokemukset lisäsyvyyttä ja konkreettisuutta ja antavat näkemystä valittaessa toimeksiantajalle sopivaa ratkaisua. Eskolan & Suorannan (1998) mukaan yksi laadullisen tutkimuksen tunnusmerkeistä on tutkimusaineiston yksityiskohtainen ja tarkka kuvailu, jolloin sen tieteellisyyden kriteeri on enemmän laatu, kuin määrä.

Tutkimuksen teoriaosuudessa selvitetään bitcoinin toimintaperiaate ja sen maksuvälineenä hyväksymiseen tarvittavat toimet ja erilaiset vaihtoehdot. Lisäksi käsitellään bitcoinin tietoturvallisuutta maksuliikenteen osalta. Varsinainen tutkimus toteutetaan suorittamalla kyselytutkimus sellaisille yrityksille, jotka jo hyväksyvät bitcoinmaksuja, sekä toimeksiantajan haastatteluilla. Bitcoinin tällä hetkellä maksuvälineenä hyväksyville yrityksille suoritettavalla kyselyllä pyritään selvittämään kuinka valitut ratkaisut vastaavat odotuksia, onko maksujen vastaanottamisessa ilmennyt ongelmia ja kuinka yritykset arvioivat oman ratkaisunsa tietoturvallisuutta ja käytön helppoutta. Toimeksiantajan edustajan haastattelulla pyritään selvittämään yrityksen valmiutta muutoksiin ja nykyisten toimintatapojen ja olemassa olevan tekniikan soveltuvuutta uuden maksutavan vastaanottamiseen.

Kokemusten keräämistä varten kyselyn vastaanottajiksi valittiin yrityksiä bittiraha.fi sivuston julkaiseman yrityslistan perusteella. Listalle on kerätty suomalaisia bitcoinin hyväksyviä yrityksiä, joista tähän tutkimukseen valittiin vain ne, joilla on Suomessa toimiva verkkokauppa. Täysin Datatroniciin verrattavia yrityksiä ei listalla ollut, eikä sellaisia, joissa bitcoinmaksujen hyväksyminen olisi otettu käyttöön jo aiemmin toiminnassa olleeseen verkkokauppaan. Haastatteluista saatua tietoa verrataan teoriaosuuden antamaan tietoon ja johtopäätöksenä pyritään löytämään vastaus tutkimuskysymykseen, eli löytämään toimeksiantajalle sopivin ratkaisu maksujen vastaanottamiseen.

1.4 Lahden Datatronic Oy

Lahden Datatronic Oy (myöh. Datatronic) on lahtelainen tietotekniikan tarvikkeita, komponentteja, varaosia ja lisävarusteita myyvä yritys. Datatronic tarjoaa myös monipuolisia tietokonepalveluja sekä tietokonehuoltoa. Datatronic myy tuotteitaan ja palveluitaan Lahden keskustassa toimivassa myymälässä ja verkkokaupassaan. Datatronic on perustettu syyskuussa vuonna 2000 ja se siirtyi Devnet Oy:n omistukseen vuonna 2011. Datatronicilla on tällä hetkellä viisi työntekijää ja sen liikevaihto oli noin 1,2 miljoonaa euroa vuonna 2012.

Datatronic käyttää tällä hetkellä tukkurin verkkokauppaa, joka sijaitsee tukkurin palvelimella. Vuoden 2014 aikana Datatronic on siirtymässä täysin oman, emoyhtiö DevNetin palvelimella sijaitsevan verkkokaupan käyttöön. Koska bitcoinmaksujen vastaanottaminen vaatii muutoksia verkkokauppaohjelmistoon, tulee muutos mahdolliseksi vasta tämän jälkeen. Ohjelmointiosaamista löytyy DevNet-konsernin sisällä, joten ohjelmointia vaativat ratkaisut ja muutokset verkkokauppaohjelmistoon ovat helposti toteutettavissa. (Heino 2013.)

Datatronicin myymien tuotteiden katteiden ollessa hyvin pieniä, on yrityksen myynnin kannalta tärkeää kiinnittää huomiota bitcoinin kurssin heilahteluihin. Esimerkiksi kevään 2013 tilanne, jossa bitcoin menetti yhden päivän aikana lähes puolet arvostaan, saattaisi tietyissä tilanteissa aiheuttaa yritykselle huomattavia tappioita. Datatronicin haastatteluissa selvisi, että yritys haluaisi ainakin alkuvaiheessa muuntaa maksuna saadut bitcoinit heti euroiksi. (Heino 2013.)

2 BITCOIN

2.1 Yleistä bitcoinista

Bitcoin on avoimen lähdekoodin kryptografiseen protokollaan perustuva kokeellinen kansainvälinen virtuaalivaluutta. Bitcoinin lyhenne on BTC. Bitcoinin kehitti Satoshi Nakamoto nimimerkkiä käyttänyt henkilö tai taho vuonna 2008 ja se otettiin ensimmäisen kerran käyttöön vuonna 2009. Bitcoinia ei hallinnoi mikään pankki, valtio tai organisaatio, vaan sen toiminta ja olemassaolo perustuu täysin käyttäjien ylläpitämään järjestelmään. Bitcoinin arvo määräytyy kysynnän ja tarjonnan mukaan, eikä siihen pysty ulkopuolinen taho vaikuttamaan. Bitcoinia ei pysty väärentämään. (Bitcoin.org 2013; Bitcoin Wiki 2013c.)

Bitcoin on käytännössä vertaisverkkoon hajautettu suuri, julkinen kirjanpito, jota ylläpitämällä valuutan olemassaoloa ja toimintaa valvovat sen käyttäjät. Verkon turvallisuus ja oikeanlainen toiminta varmistetaan säilyttämällä valuutan täydellinen siirtohistoria ja käyttämällä proof-of-work -menetelmää. Bitcoinia säilytetään bitcoin-osoitteissa, jotka ovat kryptografisia julkisia avaimia. Sekä siirrot osoitteiden välillä, että osoitteiden sisältämät bitcoinmäärät ovat julkisia, mutta täysin anonyymejä. (Bitcoin.org 2013; Bitcoin Wiki 2013c.) Bitcoinin toimintaperiaatteista kerrotaan lisää luvussa 3.3.

Yksi bitcoin jakautuu 100 miljoonaan pienempään yksikköön, satoshiin. Bitcoinin rahavarannon arvo lokakuussa 2013 oli noin 11,9 miljoonaa bitcoinia ja keskimääräinen vaihtokurssi noin 138 euroa. Näin ollen rahavarannon arvo euroissa oli yli 1,6 miljardia. Bitcoin-talouteen uutta rahaa syntyy verkon ylläpidon sivutuotteena louhinnaksi kutsutulla menetelmällä ennalta määrätyn mekanismin mukaan niin, että vuoden 2140 tietämällä uutta rahaa ei enää synny. Rahan luontimekanismin on haluttu jäljittelevän arvometallien louhintaa. (Bitcoin.org 2013; Bitcoin Wiki 2013c.)

2.2 Bitcoinin historiaa

Bitcoinin kuvaili ensimmäisen kerran marraskuussa 2008 nimimerkkiä Satoshi Nakamoto käyttävä henkilö tai taho kuvauspaperissaan ”Bitcoin: A Peer-to-Peer Electronic cash system” Cryptography -postituslistalla. Bitcoinin ensimmäinen prototyyppi Bitcoin v0.1 julkaistiin samalla postituslistalla tammikuussa 2009 ja ensimmäinen siirto käyttäjältä toiselle tehtiin pian sen jälkeen. Ensimmäinen bitcoinien myyntiin ja ostamiseen tarkoitettu sivusto, Bitcoin Market perustettiin helmikuussa 2010. Tiedettävästi ensimmäinen bitcoineilla ostettu hyödyke oli 10 000 bitcoinia maksanut pizza, joka tilattiin keskustelupalstan välityksellä keväällä 2010. Kyseisen pizzan hinta olisi syyskuun 2013 vaihtokurssin mukaan laskettuna yli miljoona euroa. Suurin bitcoinien vaihtoon erikoistunut pörssi MtGox perustettiin heinäkuussa 2010. Bitcoinin kurssi nousi ensimmäisen kerran yli dollarin vuoden 2011 aikana ja on siitä eteenpäin jatkanut nousuaan, ollen toistaiseksi korkeimmillaan huhtikuussa 2013 yli 160 euroa (Bitcoincharts 2013; Bitcoin Wiki 2013g.)

2.3 Bitcoinin toimintaperiaate

Bitcoin-verkon peruskäsite lohkoketju on vertaisverkossa toimiva suuri julkinen kirjanpito tietokanta. Lohkoketju sisältää koko bitcoinin olemassaoloajan siirtohistorian kaikkien aikojen ensimmäisestä siirrosta alkaen, tiedon kaikista bitcoin-osoitteista (myöh. myös osoite) ja tiedon niissä olevista rahamääristä. Koska siirtohistoria on julkinen, kuka tahansa voi tarkistella sitä ja näin varmistaa siirtojen oikeellisuuden tai tietyn osoitteen bitcoinmäärän. Käytännössä lohkoketju sisältää vain siirtoja osoitteesta toiseen ja osoitteen sisältämä bitcoinmäärä on vain verkossa olevien siirtojen yhteenlaskettu summa. (Nakamoto 2008.)

Siirtohistorian säilyttämisen ensisijainen tarkoitus on varmistaa se, ettei samaa rahaa voi käyttää kahteen kertaan. Tavallisesti digitaalisessa rahansiirrossa käytetään liikkeelle laskevaa tahoja, jonka kautta kaikki siirrot tapahtuvat. Tämä taho vastaa siirtojen oikeellisuudesta ja varmistaa, ettei samaa rahaa käytetä useita kertoja. Koska bitcoinilla ei ole keskushallintoa, eikä sen luotettavuuden ole

haluttu olevan riippuvainen ulkopuolisesta tahosta, on luotettavuus ja siirtojen eheys varmistettu kryptografisin menetelmin ja proof-of-work menetelmällä. Menetelmän tarkoituksena on tehdä ulkopuolisten hyökkäysten tekeminen niin vaikeaksi ja laskentatehoa vaativaksi, ettei se ole yhtä kannattavaa, kuin verkon rehellinen ylläpito. Verkkoa ylläpitävät käyttäjät saavat palkkioksi bitcoineja, mikä kannustaa yhteisöä pitämään yhdessä huolta verkon toimivuudesta ja luotettavuudesta. (Nakamoto 2008.)

2.3.1 Lohkoketju

Lohkoketjun, eli bitcoin-verkon perustan muodostavat toisiinsa tiivistein yhteen ketjutetut kronologisessa järjestyksessä olevat lohkot, jotka sisältävät itse siirrot. Lohko sisältää myös aina sitä edeltävän lohkon tiivisteen, jolloin lohkoista muodostuu yhtenäinen ketju aina ensimmäisestä viimeisimpään. Lohkoketjua ylläpitävät vertaisverkon solmut, eli käyttäjät yhdessä varmistavat, että vain verkon sääntöjen mukaiset lohkot liitetään ketjuun. Jos lohko on sääntöjen vastainen, se jätetään huomiotta ja näin vain hyväksytyistä lohkoista syntyy verkon pisin ketju. (Bitcoin Wiki 2013e.)

Kun uusi lohko luodaan ja se on ollut ketjussa jonkin aikaa, sille alkaa syntyä jatkoa. Näin lohkon jälkikäteen muokkaaminen on käytännössä mahdotonta, sillä se vaatisi myös kaikkien muokattavan lohkon jälkeen syntyneiden lohkojen muokkaamisen. Tämä vaatisi kuitenkin niin paljon aikaa ja laskentatehoa, että rikollisen tahon siitä mahdollisesti saamat hyödyt jäisivät vähäisemmiksi, kuin siihen käytetyt resurssit. (Bitcoin Wiki 2013e.)

2.3.2 Lohko

Lohko on tiedosto, joka sisältää kaikki ne viimeaikaiset siirrot, joita ei vielä ole tallennettu bitcoin-talouden kirjanpitoon, eli lohkoketjuun. Lohko sisältää myös aina sitä edeltävän lohkon tiivisteen, josta ilmenee sen sijainti lohkoketjussa. Aina, kun uusi lohko syntyy, syntyy myös uusia bitcoineja ja ne jaetaan palkkioksi lohkon luomiseen osallistuneille verkon jäsenille. Kun lohko on luotu ja liitetty lohkoketjuun, sitä ei enää voida muuttaa. Jotta lohko tulee pysyväksi

osaksi verkkoa, on sen sisältämien siirtojen oltava täysin verkon sääntöjen mukaisia. Vaikka samanaikaisesti syntyisi useita lohkoja, vain yksi niistä huomioidaan ja siitä tulee osa lohkoketjua. (Bitcoin Wiki 2013d.)

Uusia lohkoja luodaan laskemalla monimutkaisia matemaattisia ongelmia, joiden vaikeus kasvaa koko ajan ja vaatii näin verkkoon liitetystä tietokoneelta enemmän laskentatehoa. Näin bitcoinien luomisesta tulee aina vain hitaampaa ja vaikeampaa ja lopulta uutta rahaa ei enää synny. (Bitcoin Wiki 2013d.) Kuvassa 1 on eräs lohko, jossa näkyvät lohkon tiedot, sekä lista sen sisältämistä siirroista. Listalla ensimmäisenä näkyvät siirtopalkkiot uuden lohkon luomiseen osallistuneille.

Block 260591²

Short link: <http://blockexplorer.com/b/260591>
 Hash²: 000000000000003d43671546559283d11e2c17f628e9a1015058e7955a36e8d
 Previous block²: 000000000000001a134244fa7d9c976f1ca209008128c7c995406cbe81b6b954
 Time²: 2013-09-28 15:13:17
 Difficulty²: 148 819 199.805092 ("Bits"²: 191 cdc20)
 Transactions²: 391
 Total BTC²: 5427.44140322
 Size²: 158.334 kilobytes
 Merkle root²: 14e8f630a6a7f3e719a778b437bd2ae7f3ab724109dee3e56faaebc662b241dd
 Nonce²: 2455308830
[Raw block²](#)

Transactions

Transaction ²	Fee ²	Size (kB) ²	From (amount) ²	To (amount) ²
73e497e49f...	0	0.102	Generation: 25 + 0.17386521 total fees	1BxD2VLE95n7ZeVJSy3uoU5WdR72jWj5F 25.17386521 1Amrgseym9qTYhkZCGqos2EU4hAFN4X9 : 12.96 13hwBHhLbN9pPACe2lUsoF45q7rkhwmj5 : 5.056 1PLESZaBfKR2F6P6boUrsj5mwY7uWwmyP : 1.296 1De7KaFyRHUVJCup7Ap88xYbu2Z4q1F63 : 2.53 14kMFWZRsAxU64YEPymHE6rYtRzeMNA : 2.592 1Lcgv74xH5JeVrscFyztgawJeNp3ZmUx4 : 1.296 15craUyHkKfObWER65Z3LZGUW4zUwem8m : 25.92 1UVfngaFgaqa3BqBseP7RfdPwr2eD514y3 : 22.032 161718ZHpCSLdmk7sbyVL9ahyRUBpmLn7 : 2.592

Kuva 1: Lohko 260591 (blockchain.info)

2.3.3 Bitcoin-osoitteet

Bitcoineja säilytetään bitcoin-osoitteissa. Osoite on julkinen avain, joka on näkyvässä kaikille lohkoketjua tarkasteleville, mutta osoitteen omistaja ei ole tiedossa. Osoite on numerolla 1 tai 3 alkava 27–34 merkkinen satunnainen numeroista ja kirjaimista koostuva merkkijono. Osoite voi olla esimerkiksi *31uEbMgunupShBVTewXjtqtBv5MndrfXhb*. Osoitteita voi luoda myös itse siihen tarkoitetuilla ohjelmilla. Bitcoin-verkko alkaa seurata osoitetta, kun siihen

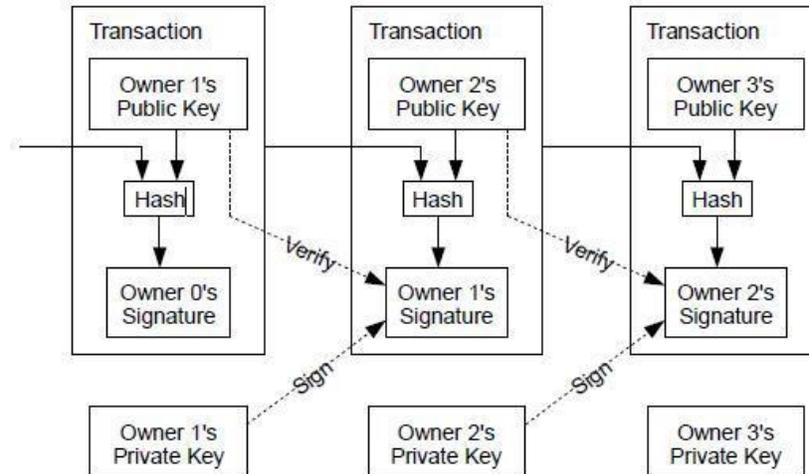
ensimmäisen kerran siirretään varoja. Osa osoitteen merkeistä muodostaa tarkistussummia, jotka takaavat osoitteen aitouden ja poistavat kirjoitusvirheiden aiheuttamat sekaannukset. (Bitcoin Wiki 2013a.)

Bitcoin-osoitteet ovat anonyymeja, eli niitä ei voi liittää kehenkään henkilöön. Maksuliikennettä seuraamalla voi kuitenkin päättelemällä saada osoitteen omistajan tietoonsa, jos sama henkilö käyttää aina samaa osoitetta. Henkilöllä voi olla useita osoitteita ja jotta osoitteen anonymiteetti säilyisi ja jotta maksutapahtumat pystyy erittelemään, on suositeltavaa käyttää eri osoitetta jokaiselle siirtotapahtumalle. Useimmat bitcoin-lompakot luovatkin käyttäjälleen uuden osoitteen jokaista siirtotapahtumaa varten. (Bitcoin Wiki 2013a.)

Koska bitcoin-osoite on kryptografinen julkinen avain, siihen liittyy myös yksityinen avain. Yksityinen avain on ainoa tapa päästä käsiksi siihen liittyvään julkiseen avaimeen, eli bitcoin-osoitteeseen. Jos osoitteeseen liittyvä yksityinen avain katoaa, ovat osoitteessa olevat bitcoinit käytännössä ikuisesti menetetty. Kukaan ei pysty niitä hankkimaan takaisin, sillä yksityisen avaimen selvittäminen on käytännössä mahdotonta. (Bitcoin Wiki 2013a.)

2.3.4 Transaktiot

Bitcoin-siirtoa, eli rahan siirtämistä osoitteesta toiseen kutsutaan transaktioksi. Bitcoin-kolikko on digitaalisten allekirjoitusten ketju (Kuvio 1). Transaktiossa kolikon omistaja siirtää kolikon seuraavalle omistajalle allekirjoittamalla digitaalisesti kolikon edellisen transaktion tiivisteen ja vastaanottajan julkisen avaimen, eli bitcoin-osoitteen ja liittää ne kolikon loppuun. Allekirjoitukset tarkistamalla maksunsaaja voi varmistua omistusoikeuksien siirtymisestä. (Nakamoto 2008.)



Kuvio 1: Kolikon siirtyminen omistajalta toiselle transaktioissa (Nakamoto, S. 2008)

Jokainen transaktio sisältää siis tiedon kaikista sen mahdollistavista aiemmista lähettäjän osoitteeseen liittyvistä transaktioista. Koska osoitteiden ”kate” ei ole missään tiedossa, se tarkistetaan osoitteeseen tulleista transaktioista. Jotta samaa rahaa ei voi käyttää moneen kertaan, vain ensimmäinen tapahtunut transaktio otetaan huomioon. Tämä on mahdollista vain säilyttämällä tieto kaikista transaktioista lohkoketjussa. (Nakamoto 2008.)

Transaktiot julkaistaan bitcoin-verkkoon, jossa ne kerätään lohkoihin. Kun transaktion sisältämä lohko liitetään lohkoketjuun ja siitä on tullut pysyvä osa ketjua, on siirto sen jälkeen peruuttamaton. Kun siirron sisältämä lohko on luotu, on siirto ensimmäisen kerran varmistettu. Tähän kuluu noin kymmenen minuuttia. Koska siirto voidaan kuitenkin ensin kerätä sellaiseen lohkoon, joka ei jostain syystä pääsekään pysyväksi osaksi lohkoketjua (ks. luku 3.3.2), on olemassa mahdollisuus, että siirto peruutetaan. Tästä syystä erityisesti suuria rahasummia siirrettäessä odotetaan kuusi varmistusta (Bitcoin Wiki 2013m), jotta voidaan olla täysin varmoja siirron onnistumisesta. Tämän jälkeen maksun vastaanottaja voi olla varma, että siirto on peruuttamaton.

Siirtoihin sisältyy vapaaehtoinen siirtopalkkio, joka on lohkojen luojille tarkoitettu kannustin. Kun uusi lohko syntyy, sen luoja saa itselleen lohkon sisältämien transaktioiden siirtopalkkiot. Uuden lohkon löytäjän ei ole mikään pakko sisällyttää tiettyjä transaktioita lohkoonsa ja transaktio saattaa näin jäädä varmistumatta. Siirtopalkkio kannustaa louhijaa sisällyttämään transaktion lohkoon. Monet lompakkopalvelut ja muut palveluntarjoajat lisäävät siirtopalkkiot maksuihin automaattisesti. On arvioitu, että kun tulevaisuudessa louhimalla syntyvien bitcoinien määrä vähenee, nousevat siirtopalkkiot ensisijaiseksi kannustimeksi verkon ylläpitämiseen. (Bitcoin Wiki 2013l.)

2.3.5 Louhinta

Uutta rahaa bitcoin-talouteen syntyy louhinnaksi kutsutulla menetelmällä. Louhinta tarkoittaa bitcoin-verkon ylläpitoa uusia lohkoja luomalla ja sen turvallisuudesta ja toiminnan rehellisyydestä huolehtimista. Uutta rahaa bitcoin-talouteen syntyy käytännössä verkon ylläpidon sivutuotteena. Verkkoon liitetyn tietokoneen laskentatehoa käytetään ratkaisemaan lohkojen matemaattisia tehtäviä ja näin pyritään löytämään uusi lohko. Kun uusi lohko löytyy, saa löytäjä tästä palkinnoksi bitcoineja.

Uusia bitcoineja syntyy tällä hetkellä 25 aina kymmenen minuutin välein, eli aina kun uusi lohko luodaan. Jotta bitcoineja ei pystytä luomaan loputtomasti, puolittuu uusien bitcoinien syntymisen määrä aina neljän vuoden välein. Lopulta uutta rahaa ei enää synny ja koko bitcoin-talouteen tulee syntymään yhteensä 21 miljoonaa bitcoinia. Louhinta vaatii tietokoneelta suuren laskentatehon, jotta se olisi kannattavaa, minkä vuoksi louhintaan käytetyt laitteistot ovat usein vain kyseistä tarkoitusta varten kokoonpantuja. Käyttäjä voi myös liittyä niin kutsuttuun pooliin, jonka tarkoituksena on yhdistää useiden käyttäjien laskentateho ja jakaa ansaitut bitcoinit poolin jäsenten kesken. (Bitcoin Wiki 2013i.)

3 BITCOINIEN SÄILYTTÄMINEN JA KÄYTTÄMINEN

3.1 Lompakot

Bitcoineja säilytetään bitcoin-lompakoissa. Lompakko on tiedosto, joka sisältää avainpareja; julkisia (bitcoin-osoitteita) ja yksityisiä avaimia. Lompakon avulla voi luoda uusia osoitteita, jolloin niihin voi vastaanottaa bitcoineja. Nämä osoitteet kuka tahansa voi nähdä bitcoin-verkossa ja siirtää niihin varoja, mutta vain yksityisen avaimen haltija voi osoitteessa olevia varoja käyttää. Osoite kerrotaan vastaanottajalle, kun halutaan vastaanottaa maksu. Lompakko sisältää myös osoitteisiin liittyvät yksityiset avaimet, joiden kautta osoitteen sisältämiä varoja voi käyttää. Lompakoita voi säilyttää ja käyttää useilla eri tavoilla, joista kerrotaan tarkemmin seuraavissa kappaleissa.

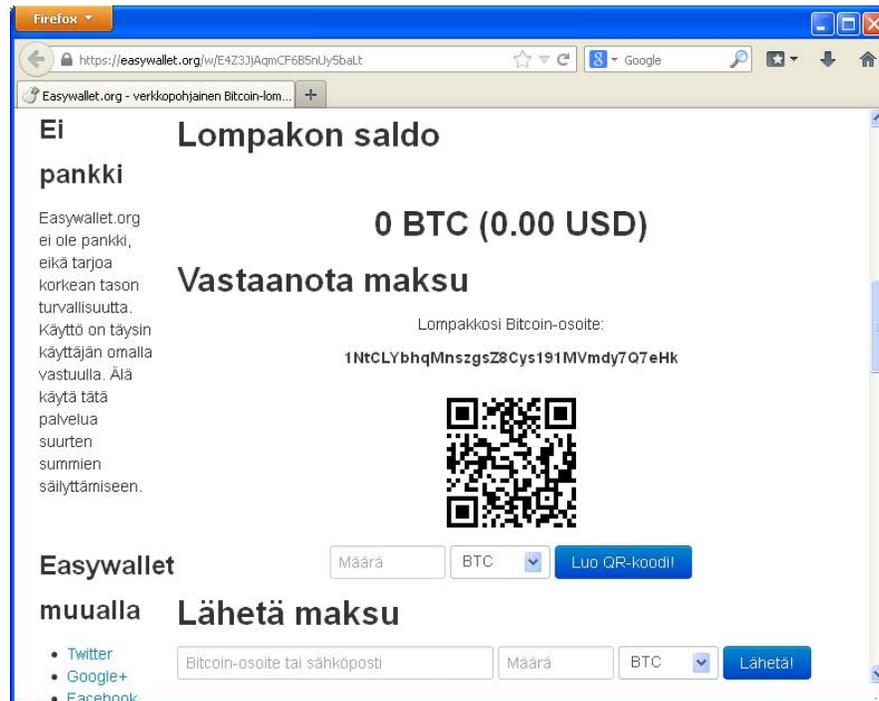
3.2 Bitcoin-asiakasohjelma

Bitcoin-asiakasohjelma on käyttäjän omalla tietokoneella oleva ohjelmisto, joka toimii osana bitcoin-verkkoa. Ohjelma sisältää yhden tai useamman lompakon. Asiakasohjelmilla voi säilyttää, lähettää ja vastaanottaa bitcoineja. Asiakasohjelmia on saatavilla useita erilaisia ja niiden toiminnot eroavat jonkin verran toisistaan. Alkuperäinen asiakasohjelma Bitcoin-qt lataa käynnistettäessä koko lohkoketjun siirtohistorian ja tarkistaa sen ja toimii sen jälkeen verkon yhtenä täysimääräisenä jäsenenä (Bitcoin.org 2013). Ohjelmaa pyörittäessä pitää siis samalla huolta verkon toiminnasta ja turvallisuudesta. Asiakasohjelmista on saatavilla myös kevyempiä versioita, kuten MultiBit, joka lataa vain osan lohkoketjusta (MultiBit 2013).

3.3 Selainpohjaiset lompakot

Ehkä helpoin tapa säilyttää bitcoineja on käyttää selainpohjaista lompakkoa. Selainpohjainen lompakko on verkossa sijaitseva selaimella käytettävä lompakko, jonka käyttöön tarvitaan joko salasana tai kuten Eaywallet-palvelussa (Kuva 1) salassa pidettävä lompakon URL-osoite. Selainpohjaiset lompakot luovat käyttäjälleen automaattisesti uusia osoitteita, joten maksujen vastaanottamiseen

voi käyttää joka kerta eri osoitetta. Monet lompakkopalvelut tarjoavat käyttäjilleen monipuolisia turvallisuutta lisääviä ominaisuuksia, kuten varmuuskopioinnin tai paperi- ja aivolompakon luonnin.



Kuva 2: Easywallet-lompakko. Lompakon URL-osoite on salainen avain lompakkoon. (easywallet.org)

3.4 Aivo- ja paperilompakot

Aivolompakko tarkoittaa bitcoin-osoitteen muuntamista ulkoa opeteltavaksi lauseeksi. Jos lause on tallessa ainoastaan omistajan muistissa, voidaan ajatella bitcoinien olevan tallessa ainoastaan omistajan aivoissa ja siksi menetelmää kutsutaankin aivolompakoksi. Jos lompakon omistaja unohtaa lompakkonsa, eli salaisen lauseen tai hän kuolee, katoavat kaikki lompakossa olevat bitcoinit ikuisesti. Valitun lauseen tulee olla ainutlaatuinen, sekä tarpeeksi pitkä ja monimutkainen. Kirjallisuudesta tai muusta julkisesti saatavilla olevasta lähteestä otettu lause on rikollisen tahon helppo selvittää. Aivolompakko luodaan

muuntamalla lause 256 bittiseksi yksityiseksi avaimeksi ja laskemalla sille julkinen avain, eli bitcoin-osoite. Bitcoinit siirretään tähän osoitteeseen ja ne saa käyttöönsä lauseesta syntyvällä yksityisellä avaimella. Aivolompakoiden luontiin on saatavilla useita ohjelmia ja palveluita. (Bitcoin Wiki 2013f.)

Paperilompakko luodaan tulostamalla tai kirjoittamalla paperille tarkoitusta varten luotu uusi bitcoin-osoite sekä siihen liittyvä yksityinen avain. Osoitteeseen siirretyt bitcoinit ovat näin kyseisen paperin haltijan käytössä. Käytännössä paperilompakko on siis eräänlainen seteli. Paperilompakkoon bitcoin-osoitteen voi tulostaa myös älypuhelimella helposti luettavaksi QR-koodiksi. Paperilompakkoa luodessa on erityisen tärkeää pitää yksityinen avain salassa niin, ettei sitä pystytä kopioimaan, vaan se on käytössä ainoastaan paperilompakon yhteydessä. Suositeltavaa on piilottaa yksityinen avain esimerkiksi taittelemalla paperi niin, ettei yksityinen avain näy. Paperilompakoiden luontiin ja tulostamiseen on tarjolla erilaisia ohjelmia ja monien lompakkopalveluiden avulla voi luoda myös paperilompakoita. (Bitcoin Wiki 2013j.)

3.5 Muut säilytysmenetelmät

Bitcoinin käyttäjälle vaivaton vaihtoehto käyttövarojen säilyttämiseen on älypuhelimeen ladattava lompakkosovellus, jossa bitcoinit kulkevat käyttäjän mukana. Maksujen vastaanottaminen tapahtuu puhelimesta olevan lompakon QR-koodia näyttämällä ja maksaminen vastaavasti lukemalla puhelimesta maksun vastaanottajan antaman QR-koodin. Bitcoineja voi säilyttää myös yhteydettömässä tietokoneessa tai USB-muistilla sijaitsevassa lompakossa. Näin estetään verkon kautta tapahtuvat varkaudet ja tämä tapa onkin suositeltava säilytettäessä suuria summia, joita ei tarvita päivittäisessä käytössä. Bitcoineja on mahdollista säilyttää myös bitcoin-kolikkona, joka on fyysiseen kolikkoon sijoitettu bitcoin-lompakko. Bitcoinien säilyttämiseen on lisäksi useita muita tapoja ja käytännössä vain mielikuvitus on rajana, sillä osoitteen ja siihen liittyvän yksityisen avaimen voi säilyttää lukuisin eri tavoin.

3.6 Bitcoinien käyttäminen

Bitcoineilla voi maksaa ostoksia bitcoinit hyväksyvissä kaupoissa ympäri maailman. Suomessa bitcoinin hyväksyviä eri alojen tuotteita ja palveluja tarjoavia fyysisiä liikkeitä oli lokakuussa 2013 bittiraha.fi sivuston karttapalvelun mukaan 21 (Bittiraha 2013, Bitcoin-karttapalvelu). Erilaisia verkkokauppoja ja verkossa toimivia palveluntarjoajia on huomattavasti enemmän kuin fyysisiä liikkeitä. Maailmanlaajuisesti kattavaa listaa bitcoinin hyväksyvistä yrityksistä ei ole saatavilla, mutta tutkijan oman erilaisiin listoihin perustuvan arvion mukaan niitä on tuhansia. Bitcoin on erityisen kätevä tippien ja lahjoitusten antamiseen, sillä sen käyttö on nopeaa, yksinkertaista ja yleensä ilmaista. Maksujen ilmaisuus korostuu erityisesti niin kutsutuissa mikromaksuissa, jotka ovat yleensä verkkopalveluissa tehtyjä hyvin pieniä maksusuorituksia.

4 VERKKOKAUPAN MAKSULIIKENTEN TIETOTURVALLISUUS

Tässä luvussa perehdytään bitcoinin tietoturvallisuuteen liittyviin asioihin erityisesti verkkokaupan maksuliikenteen osalta. Bitcoin eroaa perinteisistä valuutoista toimintansa ja myös tietoturvallisuuden osalta. Bitcoinien säilyttämiseen ja käyttämiseen on monia eri tapoja ja tavat vaihtelevat myös tietoturvallisuuden osalta. Mitä helpommin ja nopeammin bitcoinit ovat saatavilla, sen kevyempää on tietoturva ja vastaavasti tarkoin turvattujen bitcoinien käyttäminen vaatii enemmän vaivaa. Tärkeintä onkin noudattaa annettuja ohjeita ja arvioida turvallisuuden ja käytön helppouden suhde tilanteen ja kyseessä olevan rahasumman mukaan.

4.1 Tietoturvallisuus

Tietoturvallisuus määritellään perinteisesti tiedon arvoon perustuen luottamuksellisuudesta, käytettävyydestä ja eheydestä koostuvaksi kokonaisuudeksi. Nykyisin määritelmään sisältyvät usein myös kiistämättömyys ja pääsynvalvonta. Luottamuksellisuudella taataan tiedon käytettävissä oleminen vain tietoon oikeutetuille henkilöille ja käytettävyydellä sitä, että oikea tieto on saatavilla oikeassa muodossa riittävän nopeasti. Eheydellä tarkoitetaan tietojen paikkansapitävyyttä ja virheettömyyttä. Kiistämättömyys tietoturvallisuuden osalta tarkoittaa käyttäjän tunnistamista ja tunnistetietojen tallentamista niin, että myös jälkikäteen voi kiistatta selvittää järjestelmää käyttäneen henkilön. Pääsynvalvonnalla ehkäistään ulkopuolisten pääsyä järjestelmään. (Hakala, Vainio & Vuorinen, 4-6.)

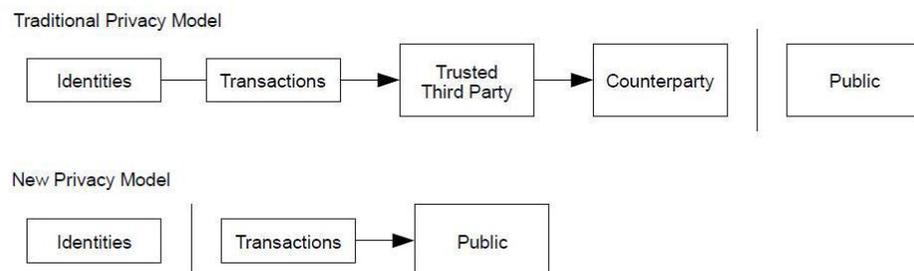
4.2 Bitcoinmaksuliikenteen julkisuus

Tavanomaisessa digitaalisessa maksuliikenteessä on totuttu varmistamaan suuri osa tietoturvallisuudesta kolmannen osapuolen avulla. Tilisiirron tekeminen pankkitililtä toiselle tarkoittaa siihen luottamista, että oma tilipankki vähentää siirron verran saldoa omalta tililtä ja vastaavasti lisää saman verran saldoa vastaanottajan tilille. Pankki pitää huolen siitä, että sekä maksaja, että maksun saaja ovat tilien käyttöön oikeutettuja. Henkilöiden tunnistaminen on toteutettu erilaisin tunnistusmenetelmin ja sekä maksaja, että maksun saaja voivat olla

varmoja toistensa henkilöllisyydestä lukuun ottamatta tilannetta, jolloin esimerkiksi pankkitunnukset ja salaiset avainluvut ovat päässeet väärin käsiin. Koko maksuprosessi on ulkopuoliselta taholta tarkoin salattu ja näkyvissä pankin lisäksi ainoastaan maksajan ja vastaanottajan tiliotteilla.

Bitcoineja osoitteesta toiseen siirrettäessä koko siirtoprosessi näkyy julkisena verkossa. Jokainen maksutapahtuma koko bitcoinin historian ajalta on jäljitettävissä ja minkä tahansa bitcoin-osoitteen saldo on tarkasteltavissa, kukaan ei vain tiedä osoitteiden omistajia. Siirtoa tehdessä ei myöskään maksajan tai maksun vastaanottajan tarvitse tietää toistensa henkilöllisyyttä. Riittää, että maksajalla on tiedossaan maksun saajan bitcoin-osoite ja maksun yksilöimiseksi ja varmistamiseksi riittää julkisesti tarkisteltavissa oleva vahvistettu siirtotapahtuma bitcoin-verkossa. Halutessaan osapuolet voivat tietenkin tarkistaa toistensa henkilöllisyyden, mutta tämä ei itse maksun onnistumisen tai sen luotettavuuden kannalta ole tarpeen.

Käytännössä bitcoinin käyttöä voi verrata käteisen rahan käyttöön. Käteisellä maksettaessa riittää itse maksuvälineen aitouden tarkistaminen, eikä maksajan tai vastaanottajan henkilöllisyydellä ole merkitystä. Kuvassa 4 on havainnollistettu bitcoinin ja perinteisen rahaliikenteen eroa julkisuuden kannalta.



Kuva 3: Bitcoin-siirtojen julkisuus (Nakamoto 2008)

4.3 Käyttäjän vastuu

Bitcoinia käytettäessä käyttäjän osuus tietoturvallisuudesta huolehtimisesta on olennainen. Osoitteiden ja niihin liittyvien yksityisten avainten tallessa ja salassa pitäminen on koko turvallisuuden perusta. Jos käyttäjä unohtaa tai kadottaa

bitcoin-osoitteensa tai siihen liittyvän yksityisen avaimen, ovat osoitteen sisältämät varat käytännössä ikuisesti menetetty. Jos taas ulkopuolinen henkilö saa tietoonsa osoitteen ja sen yksityisen avaimen, voi hän käyttää osoitteen sisältämiä bitcoineja kuin omiaan.

Koska bitcoin-verkossa kaikki siirrot ja osoitteet ovat julkisia, on myös henkilöllisyyden salassa pitäminen käyttäjän vastuulla. Verkkokaupan maksuliikenteen osalta tämä tarkoittaa ensisijaisesti huolehtimista siitä, että jokaista maksutapahtumaa varten käytetään uutta osoitetta, jolloin mitään käytettyä osoitetta ei voida yhdistää tiettyyn verkkokauppaan. Bitcoinin käyttö vaatii huolellista tutustumista turvallisuusohjeisiin, jotka ovatkin vastuuntuntoisten palveluntarjoajien sivustoilla hyvin esillä. Bitcoineja vastaanottavan verkkokaupan on hyvä ohjeistaa myös asiakkaitaan bitcoinin turvallisesta käytöstä.

4.4 Säilytys

Kuten edellä on mainittu, on bitcoinien käytössä ensisijaisen tärkeää säilyttää osoitteet ja niihin viittaavat yksityiset avaimet huolellisesti. Jos käyttäjä kadottaa lompakkonsa, tai sen käyttöön oikeuttavan yksityisen avaimensa, ovat lompakossa olevat varat ikuisesti kadotettuja. Lompakkoon liittyvät bitcoineja sisältävät osoitteet jäävät toki olemaan bitcoin-verkkoon, mutta kukaan ei voi koskaan niitä käyttää. Bitcoin-maailmassa siis rahaa pursuavan lompakon löytämisestä tai omistamisesta ei ole mitään hyötyä, jos sen käytön mahdollistavaa yksityistä avainta ei ole saatavilla.

Yksityisten avaimien joutuminen väärin käsiin antaa rikolliselle vapaan pääsyn niihin liittyviin osoitteisiin. Varasta ei myöskään pystytä jäljittämään, sillä hän voi täysin anonymisti siirtää varat osoitteesta toiseen ja rikoksen uhri voi vain seurata rahojensa liikkeitä ilman, että mitään muuta on tehtävissä. Tästä johtuen erityistä huolellisuutta on noudatettava yksityisten avainten säilytyksen ja salauksen suhteen. Tietomurto voi tapahtua sekä verkon kautta, että fyysisesti ja molempiin mahdollisuuksiin on varauduttava suojaamalla yksityiset avaimet vahvoin salausmenetelmin ja säilytettävä salasanat ja mahdolliset kopiot turvassa.

Lompakon suojaaminen mahdolliselta katoamiselta tapahtuu varmuuskopioimalla lompakko ja säilyttämällä varmuuskopio turvallisessa paikassa salasanalla suojattuna. Salasanan muistaminen on hyvin tärkeää, sillä bitcoinin suhteen salasanojen palauttamisen mahdollisuudet ovat hyvin vähäisiä ja jos salasana unohtuu, ovat sen takana olevat rahat menetettyjä. Varmuuskopioita voi säilyttää verkossa, omalla tietokoneella, matkapuhelimessa tai vaikkapa USB muistilla ja suositeltavaa onkin luoda useita varmuuskopioita eri paikoissa säilytettäväksi. (Bitcoin Wiki 2013k.)

Bitcoinien säilyttämiseen lompakossa tulisi suhtautua kuin tavalliseen käteistä sisältävään lompakkoon. Päivittäiseen asiointiin tarkoitettuja varoja voi hyvin säilyttää helposti saatavilla tietokoneella tai matkapuhelimessa, mutta suurempia summia tulisi säilyttää turvallisemmassa paikassa. Monet virtuaalilompakoita tarjoavat palvelut ovat käteviä ja turvallisia jokapäiväiseen käyttöön, mutta pankkien tasoista turvallisuutta niiltä ei voi odottaa.

Jos verkkokauppa vastaanottaa säännöllisesti bitcoinmaksuja ja haluaa säilyttää varat bitcoineina, tulee säilytysratkaisu valita huolella. Pitkäaikaiseen ja suurien summien säilyttämiseen sopiva ratkaisu on esimerkiksi verkkoyhteydettömällä tietokoneella sijaitseva lompakko, josta on luotu salasanalla suojattuja varmuuskopioita useaan paikkaan. Lompakkoon ja varmuuskopioihin liittyvät salasanat tulisi säilyttää niin, että ulkopuolisen ei ole niihin mahdollista päästä käsiksi, mutta niin, että ne ovat tarvittaessa saatavilla. Verkkokaupan osalta on huolehdittava myös henkilöturvallisuudesta ja varmistettava, että kaikki bitcoinien käsittelyyn osallistuvat ovat tietoisia oikeista käytänteistä ja osaavat toimia niin, että turvallisuus säilyy.

Erilaisten säilytysmenetelmien osalta on aina otettava huomioon myös bitcoinien kohtalo kuoleman tai muun omistajan toimintakykyä olennaisesti heikentävän tapahtuman sattuessa. Liian turvallisessa säilytystavassa, kuten aivolompakoissa on mahdollisuus siihen, että jos omistaja ei pääse käsiksi bitcoineihin, ne katoavat kokonaan. Kaikkien säilytystapojen osalta on siis varmistettava, että jollakin luotetulla henkilöllä on tieto tai mahdollisuus tarvittaessa saada tieto olemassa olevista osoitteista ja keino päästä niihin käsiksi.

4.5 Maksujen vastaanottaminen

Bitcoin-siirroissa osoitteeseen ei liity tunnistetietoja osoitteen omistajasta, niin kuin tavanomaisissa tilisiirroissa. Tästä johtuen ei ole olemassa mitään varmistusmekanismia siitä, että kyseinen osoite on varmasti juuri oikea. Bitcoin-verkko tunnistaa kirjoitusvirheiden aiheuttamat virheelliset osoitteet, eikä siirtoja voi niihin tehdä, mutta jos osoite vain on kelvollinen, on siihen tehty siirto peruuttamaton. Käyttäjän on siksi itse huolehdittava ja varmistettava, että käytettävä osoite on oikea. Vahingossa väärään osoitteeseen tehtyä siirtoa ei voi peruuttaa, eikä siirrettyjen bitcoinien vastaanottajaa voi tietää, ellei osoitteen omistaja ole tiedossa. Virheellisten maksujen korjaaminen onnistuu ainoastaan, jos maksun vastaanottaja palauttaa rahat tekemällä puolestaan siirron alkuperäisen maksajan antamaan bitcoin-osoitteeseen.

Bitcoin-siirto tapahtuu nopeimmillaan muutamassa sekunnissa ja ensimmäinen vahvistus tapahtuu noin kymmenessä minuutissa. Tänä aikana epärehellinen maksaja saattaa kuitenkin onnistua peruuttamaan siirron ja näin pyrkiä huijaamaan maksun saajaa. Jos maksun peruuttamattomuudesta haluaa saada täyden varmuuden, tulee odottaa vähintään kuusi vahvistusta, mikä tarkoittaa noin tuntia. Tämän jälkeen siirto on täysin vahvistunut, eikä sitä pysty enää peruuttamaan. Verkkokaupankäynnin osalta tämä tarkoittaa, että maksun vastaanottajan on arvioitava odotusaika sopivaksi asiakastyytyvyyden ja tietoturvallisuuden suhteen. Bitcoinmaksut ovat hitaimmillaankin huomattavasti nopeampia, kuin perinteiset maksutavat, joten käytännössä kauppiaan ei tarvitse odotusajoissa juurikaan tinkiä turvallisuudesta.

5 BITCOINMAKSUJEN HYVÄKSYMINEEN VERKKOKAUPASSA

5.1 Verotus

Verohallinnon (2013) mukaan virtuaalivaluutta ei ole tuloverolain tarkoittamaa rahaa tai arvopapereita, vaan muu erikseen määrittelemätön käyttäjien välinen sopimus. Veronalaista tuloa ovat verovelvollisen rahana tai rahanarvoisena etuutena saamat tulot, ellei niitä ole erikseen säädetty verovapaaksi.

Virtuaalivaluutta realisoituu verotettavaksi kun sitä käytetään vaihdantatilanteessa. Riippumatta siitä, missä valuutassa tulo on syntynyt, on vaihtotilanteessa verovelvollisen osapuolen ilmoitettava tulo itse Verohallinnolle.

Virtuaalivaluutan arvoksi Verohallinto (2013) katsoo Kirjanpitolautakunnan ohjeistusta vastaavalla tavalla sen käyvän arvon maksupäivänä. Jos maksupäivän mukainen kurssi on saatavilla, Verohallinnon mukaan virtuaalivaluutta muunnetaan vastaanottaessa sen mukaisesti Suomen rahaksi kirjanpitoon merkitsemistä varten. Jos maksupäivän kurssia ei ole saatavilla, käytetään osapuolten sopimaa arvoa. Virtuaalivaluutta, joka on saatu suoritemyynnistä, on Verohallinnon mukaan lähtökohtaisesti elinkeinotoiminnan rahoitusomaisuutta.

Virtuaalivaluuttojen realisoitunut arvonnousu on Verohallinnon (2013) mukaan veronalaista pääomatuloa. Virtuaalivaluutan arvonnousun verotus realisoituu, kun sitä käytetään missä tahansa vaihdantatilanteessa tai kun se muunnetaan oikeaksi valuutaksi. Positiivisen arvonnousun Verohallinto katsoo olevan varallisuuden kerryttämää tuloa, jolloin verotus tapahtuu muun pääomatulon verotuksen mukaisesti. Verotuksessa virtuaalivaluutan arvonnousun suhteen valuuttakurssivoittoja koskevaa verovapaussääntöä ei sovelleta, vaan sen katsotaan olevan kokonaan veronalaista pääomatuloa. Koska virtuaalivaluutta ei ole verohallinnon mukaan arvopaperi, ei sen vaihtamisen yhteydessä mahdollisesti syntyvää arvonalaskua tai muita siihen liittyviä menetyksiä voida kuitenkaan vähentää tuloverotuksessa.

5.2 Kirjanpito

Kirjanpitolautakunnan antaman selvityksen (KILA 1895) mukaan kaikki liiketapahtumat, myös ne, joihin liittyy vertaisvaluutan (virtuaalivaluutan) käyttäminen, kuuluvat yleisen kirjanpitovelvoitteen piiriin ja on sen vuoksi merkittävä kirjanpitoon. Selvityksessä huomautetaan, että kirjanpitoon perustuvat viranomaisille tehtävät ilmoitukset tulee kuitenkin tehdä euromääräisinä.

Kun maksu otetaan vastaan vertaisvaluutassa, sen arvo tulee Kirjanpitolautakunnan selvityksen (KILA 1895) mukaan kirjanpitoon merkitsemistä varten muuntaa Suomen rahaksi maksupäivän kurssiin silloin kun kurssi on saatavilla. Muussa tapauksessa käytetään osapuolten sopimaa arvoa. Kirjanpitolautakunta suosittelee seuraamaan vastaanotettujen vertaisvaluuttaerien hankintamenoja verotuksen toimittamista varten joko pääkirjanpidossa tai erillisessä osakirjanpidossa. Samalla on huolehdittava siitä, ettei vertaisvaluuttasalkun arvo tilinpäätöksessä ylitä sen hankintamenoa tai todennäköistä luovutushintaa.

Kirjanpitolautakunnan selvityksen (KILA 1895) mukaan tarvittavat tiedot vertaisvaluuttavälineiden arvostusperiaatteista ja -menetelmistä on esitettävä tilinpäätöksen liitetietona oikean ja riittävän kuvan antamiseksi. Joissain tilanteissa myös liitetieto vertaisvaluuttavälineiden kokonaismäärästä on syytä antaa.

5.3 Maksuliikenteen vaihtoehdot

Yksinkertaisimmillaan bitcoinmaksujen vastaanottamisen voi aloittaa lisäämällä verkkokauppaan Bitcoin-logolla varustetun ”Täällä voit maksaa bitcoineilla” -viestin ja ohjata halukas maksaja ottamaan yhteyttä maksun suorittamiseksi. On kuitenkin useita eri tapoja vastaanottaa maksuja, joista tässä tarkastellaan vain sellaisia, joiden voidaan olettaa soveltuvan toimeksiantajan tapaukseen.

5.3.1 Asiakasohjelman käyttö maksujen vastaanottamiseen

Yksi tapa vastaanottaa bitcoinmaksuja on asentaa yrityksen palvelimelle Bitcoin-asiakasohjelma. Asiakasohjelma sisältää lompakon bitcoinien säilyttämiseen ja toiminnot maksujen vastaanottamiseen ja maksamiseen. Samalla asiakasohjelma ylläpitää bitcoin-verkon toimintaa ja yritys voi näin osallistua verkon turvallisuuden parantamiseen. Asiakasohjelman asentamisen lisäksi tulee verkkokaupan ohjelmakoodiin tehdä tarvittavat muutokset, jotta maksujen vastaanottamiseen tarvittava toiminnallisuus näkyy asiakkaalle ja maksuliikenteen seuraaminen on sujuvaa. Tähän on saatavilla erilaisia avoimella lähdekoodilla toteutettuja valmiita moduuleja, mutta mikään ei estä myöskään luomasta omaa tapaa.

Kun asiakas ilmaisee verkkokaupassa haluavansa maksaa bitcoineilla, maksutapahtumaa varten luodaan asiakasohjelmassa uusi bitcoin-osoite ja se lähetetään asiakkaalle. Kun asiakas on maksanut ostoksensa, voi myyjä odottaa maksulle haluamansa määrän vahvistuksia ennen kuin lähettää tuotteet. Maksu on kuitenkin viimeistään tunnin kuluessa vahvistunut peruuttamattomaksi. Asiakkaalta voi olla tarpeen myös pyytää hänen bitcoin-osoitteensa mahdollisia palautuksia varten. (Bitcoin Wiki 2013h.)

Asiakasohjelmaa käytettäessä on sen ja verkkokaupan välisten prosessien hallitseminen mahdollista toteuttaa erilaisin tavoin riippuen verkkokauppaohjelmiston ja asiakasohjelman sijainnista ja palvelinten välisistä yhteyksistä. Asiakasohjelman käyttö pitää maksujen vastaanottamisen täysin yrityksen omassa hallinnassa, jolloin tietoturvallisuuden kannalta yrityksen sisäinen osaaminen, ratkaisun toteutus ja käytetyt menetelmät ovat avainasemassa.

Asiakasohjelmaa käytettäessä on myös päätettävä lähde, josta maksutapahtuman aikainen valuuttakurssi haetaan. Nopean kurssivaihtelun varalle on maksutapahtumille asetettava aikaraja, jonka sisällä maksun on tapahduttava, jotta mahdollisista kurssiheilahteluista ei aiheudu epäselvyyksiä. Jos yritys haluaa vaihtaa vastaanottamansa bitcoinin euroiksi, on se tehtävä joltain bitcoinien vaihtoa tarjoavaa palvelua käyttämällä.

5.3.2 Osoitteiden etukäteisluonti

On mahdollista myös luoda etukäteen suuri määrä osoitteita, jotka tallennetaan palvelimelle ja luovutetaan yksitellen asiakkaalle kutakin maksutapahtumaa varten. Kun jokaiselle maksutapahtumalle on oma osoitteensa, pystytään maksut osoittamaan kullekin ostotapahtumalle erikseen. Osoitteita voi luoda niihin tarkoitetuilla sivustoilla, joilla luodaan osoitteet ja niihin liittyvät yksityiset avaimet. Yksityisiä avaimia ei tule tallentaa palvelimelle, vaan ne tulee säilyttää erillään.

Lompakko, jossa osoitteet sijaitsevat voi olla ulkopuolinen webblompakko tai omalla palvelimella oleva asiakasohjelma. Maksutapahtumien seuraaminen tapahtuu joko lompakon vastaanotettuja maksuja seuraamalla tai seuraamalla annettua osoitetta lohkoketjussa. Jos maksuja tulee paljon, vaatii tämä tapa verkkokauppaohjelmiston muokkaamista niin, että maksujen seuraaminen on sujuvaa. Tietoturvallisuudesta ja vaihtokurssien määrittämisestä tulee huolehtia kuten asiakasohjelmaa käytettäessä.

5.3.3 Ulkopuoliset palveluntarjoajat

Edellä on esitetty kaksi erilaista tapaa vastaanottaa bitcoineja hallitsemalla osoitteita ja maksutapahtumia itse. On olemassa useita palveluja, jotka tekevät maksujen vastaanottamisesta yritykselle vaivattomampaa. Erilaiset ulkopuoliset palveluntarjoajat tarjoavat eritasoisia vaihtoehtoja maksujen vastaanottamisen avuksi aina yksinkertaisesta maksuliikenteen hoidosta kokonaisesti verkkokauppasovelluksiin ja valuutanmuunto-ominaisuuksiin. Palveluntarjoajia voidaankin huoletta verrata perinteisiin verkkomaksupalveluihin ja esimerkiksi PayPalin kaltaisiin maksujenvälitysjärjestelmiin.

Koska erilaisia palveluja tarjoavia tahoja on lukematon määrä, tarkasteluun valittiin ensin ne palveluntarjoajat, jotka löytyivät Bitcoin Wikistä, jolloin niillä voitiin olettaa olevan Bitcoin-yhteisön antama hyväksyntä. Niistä valittiin edelleen sellaiset, jotka tarjoavat mahdollisimman monipuolisia palveluja ja jotka vaikuttivat luotettavilta ja eniten käytetyiltä. Näistä valittiin vielä lopuksi vain sellaiset palvelut, jotka mahdollistavat asiakkaalleen mahdollisuuden vastaanottaa

maksut suoraan euromääräisinä SEPA-maksuina, mistä Datatronicin tapauksessa voisi olla hyötyä varsinkin alkuvaiheessa. Laaja-alaista tai virallista tutkimusta eri palveluiden luotettavuudesta ei ole saatavilla, joten sitä on arvioitu kunkin palveluntarjoajan osalta eri tavoin esimerkiksi internetsivustojen ulkoasun, tietosisällön ja yleisvaikutelman perusteella. Ei ole myöskään saatavilla tarkkaa tietoa eri palveluntarjoajien käyttäjämääristä, mikä johtuu osaksi bitcoinin anonyymiydestä ja osaksi siitä, että kaikki palveluntarjoajat ovat vielä suhteellisen uusia. Tästä johtuen valinta oli tehtävä lähinnä bitcoin-aiheisten keskustelupalstojen, blogimerkintöjen ja artikkelien perusteella. Lopulliseen tarkasteluun päätyi kaksi eri palveluntarjoajaa, jotka on esitelty tässä lyhyesti ja lopuksi vertailtu toisiinsa eri ominaisuuksien osalta.

BIPS

BIPS on eurooppalainen maksupalvelun tarjoaja, joka on perustettu vuonna 2013. Yhtiön toimitilat sijaitsevat Tanskassa ja sillä on verkkosivujensa mukaan yli 15000 asiakasta ympäri maailman. BIPS tarjoaa asiakkailleen valmiita maksumoduuleja yleisimmin käytössä oleville verkkokauppa-alustoille, sekä laajan tarjonnan ostoskoriliitännäisiä ja ohjelmointirajapinnan bitcoinmaksujen vastaanottamiseksi verkkokaupassa. BIPS tarjoaa myös mahdollisuuden muuntaa maksut suoraan euroiksi SEPA-maksuna, josta veloitetaan 2,25 euroa. Palvelun sivustolta ei kuitenkaan selviä suorittaako se euromääräisen maksun jokaista maksutapahtumaa kohden vai tietyin välein. Pelkkä bitcoinmääräisten maksujen prosessointi palvelun kautta on ilmaista. BIPS käyttää dataliikenteensä salaamiseen SSL-salaustekniikkaa ja vakuuttaa noudattavansa samoja turvallisuusstandardeja kuin useimmat pankit. Palvelun sivusto on toteutettu huolella ja tietoa palvelusta on tarjolla kohtalaisesti. BIPS tarjoaa asiakkailleen ilmaisen teknisen tuen. BIPS:n käyttöönotto vaatii palveluun rekisteröitymisen, sekä tarvittavien ohjelmointirajapintaa hyödyntävien ohjelmakoodien lisäämisen verkkokauppaan.



Kuva 4: Esimerkki näkymästä asiakkaan maksaessa verkkokaupassa käytettäessä BIPS-palvelua (bips.me)

BitPay

BitPay on vuonna 2013 perustettu, yli 10 000 asiakkaan käyttämä kansainvälinen maksupalvelujen tarjoaja. BitPay tarjoaa asiakkaille valmiita ostoskoriliitännäisiä monille verkkokauppa-alustoille, monipuolisen PHP-kirjaston, maksuyhdyskäytävä-ohjelmointirajapinnan, sekä valmiit Osta nyt -painikkeet ja BitPay ostoskorin. BitPayta käytettäessä on myös mahdollisuus näyttää verkkokaupan asiakkaalle maksuohjeet suomenkielisinä. BitPay tilittää asiakkaalle tulleet maksut kerran päivässä asiakkaan bitcoin-osoitteeseen, jolloin minimisiirto on 0,1 bitcoinia. Asiakkaan niin halutessa, BitPay muuntaa maksut euroiksi ja tilittää ne SEPA-maksuna asiakkaan pankkitilille joka pankkipäivä ilman lisämaksua. Minimisiirto on tällöin 20 euroa. BitPayn käyttö on ilmaista, jokaista maksutapahtumaa kohden veloitetaan 1 % siirtopalkkio. Palvelun sivulla mainostettiin tätä työtä tehdessä myös marraskuussa 2013 tulossa olevista maksullisista palvelupaketeista, joihin sisältyy lisäpalveluita valitusta paketista riippuen. Ainoana maksupalvelun tarjoajana BitPay antaa asiakkailleen vaihtokurssitakuun, joten BitPay tilittää prosessoimansa maksut asiakkaan tilille verkkokaupan maksutapahtumahetken kurssin mukaan riippumatta tilityshetken kurssista. BitPayn verkkosivusto on huolellisesti toteutettu ja sieltä löytyy kiitettävästi tietoa palvelusta. BitPayn käyttöönotto vaatii palveluun rekisteröitymisen, sekä tarvittavien liitännäisten asentamisen verkkokauppaan tai maksuyhdyskäytävän rakentamisen ohjelmointirajapintaa hyödyntäen verkkokaupan ohjelmakoodiin.



Kuva 5: Esimerkki maksutapahtumasta BitPayta käyttävässä verkkokaupassa. (kauppa.bittiraha.fi)

Seuraavassa taulukossa on vertailtu palveluntarjoajien ominaisuuksia, jotka vaikuttavat niiden sopivuuteen tässä työssä etsityksi ratkaisuksi.

Taulukko 1: Palveluntarjoajien vertailu

	BIPS	BitPay
Palvelun hinta	0,00 €	0,00 €
Siirtopalkkio	0,00 %	1,00 %
Euromääräisen tilityksen hinta	2,25 €	0,00 €
Valuuttakurssitakuu	Ei	Kyllä
Ostoskoriliitännäiset	Kyllä	Kyllä
API	Kyllä	Kyllä
Tekninen tuki	Kyllä	Kyllä
Suomenkielen tuki	Ei	Kyllä

6 TUTKIMUSTULOKSET

6.1 Tutkimusaineisto

Tämän työn tavoitteena oli löytää toimeksiantajalle sopiva ratkaisu bitcoinmaksujen vastaanottamiseen verkkokaupassa. Jotta tarjolla olevia vaihtoehtoja voitiin verrata syvällisesti, haluttiin käyttäjäkokemusten kautta saada tietoa myös muiden kokemuksista. Sähköpostitse suoritettulla kyselyllä (Liite 1.) kerättiin kokemuksia niiltä yrityksiltä, jotka jo hyväksyvät bitcoinin verkkokaupansa maksuvälineenä. Kysely lähetettiin yhdeksälle suomalaiselle yritykselle, joilla on Suomessa toimiva verkkokauppa ja jotka hyväksyvät bitcoinin maksutapana. Yritykset valittiin bittiraha.fi palvelun tarjoamasta listasta, jossa on lueteltu Suomessa bitcoinin hyväksyviä yrityksiä. Näistä valittiin kyselyyn sellaiset yritykset, joilla on verkkokauppa. Kyselyyn vastasi viisi yritystä, vastausprosentin ollessa näin 55 %. Yrityksistä yksi esitti vain bitcoin-osoitteensa asiakkaalle maksutilanteessa, kaksi käytti omalla palvelimella sijaitsevaa asiakasohjelmaa ja kaksi BitPay maksupalvelun tarjoajaa. Yritysten verkkokaupan valikoima vaihteli aina rintamerkeistä elintarvikkeisiin.

6.2 Aineiston analyysiprosessi

Koska kysely toteutettiin sähköpostitse, oli aineisto jo valmiiksi helposti käsiteltävässä sähköisessä muodossa ja sen esivalmisteluksi riitti vastausten kerääminen yhteen asiakirjaan.

Aineiston analyysi aloitettiin koodaamalla, eli jäsentelemällä vastauksia merkitsemällä värikoodein vastauksista löytyneitä merkityksiä ja aiheita. Laadullisessa tutkimuksessa koodaamiseksi kutsutaan aineiston pilkkomista helpommin tulkittaviin osiin liittämällä merkkejä tekstin määriteltyihin tekstijaksoihin (Eskola & Suoranta 1998, 155). Aineistoa lähestyttiin deduktiivisesti etsimällä vastauksista tutkimuskysymyksen kannalta olennaisiin käsitteisiin viittaavia ilmaisuja. Näitä olivat esimerkiksi käytetty ratkaisu, turvallisuus ja helppous.

Koodaamisen jälkeen aineisto teemoiteltiin tutkimusongelman mukaisiin teemoihin. Eskolan ja Suorannan (1998, 175) mukaan teemoittelu on suositeltava tapa erityisesti käytännöllisen ongelman ratkaisemisessa, sillä teemojen avulla aineistosta voidaan poimia tutkimusongelman kannalta olennaisia asioita. Teemoittelulla aineistosta nostetaan esiin sellaisia teemoja, jotka valaisevat tutkimusongelmaa.

Vaikka teemoittelun lähtökohtana olivat deduktiivisesti tutkimuskysymyksen antamat suuntaviivat, annettiin aineistosta nousta esiin myös muita teemoja, jotka omalta osaltaan lisäsivät tutkimuksen antia. Koska tämän työn tutkimusongelmana oli löytää toimeksiantajalle sopiva ratkaisu, pyrittiin aineistosta löytämään sellaisia teemoja, jotka valaisivat kyselyyn vastanneiden yritysten kokemuksia omien ratkaisuidensa sopivuudesta. Sopivuus käsitteenä saatiin teemoittelun avulla jaettua tarkempiin käsitteisiin, kuten ”käyttöönoton helppous” tai ”turvallisuuden kokeminen”.

6.3 Analyysi

6.3.1 Yleinen toimivuus

Kyselyvastausten selvästi näkyvimmit aiheet olivat käytön helppous ja ratkaisujen toimivuus. Bitcoinmaksut käytetystä ratkaisusta riippumatta koettiin helpoiksi ja hyvin toimiviksi. Kaiken kaikkiaan aineistosta saatu mielikuva oli, ettei bitcoinin käyttöön ja maksujen vastaanottamiseen muutamaa poikkeusta lukuun ottamatta koettu yleisellä tasolla liittyvän juuri minkäänlaisia ongelmia tai riskejä.

Erialaisten palveluiden ja sovellusten toimimattomuuteen, ongelmatilanteisiin ja monimutkaisuuteen tottuneen tarkastelijan näkökulmasta vastaukset saattavat ensisilmäyksellä antaa jopa epäilyttävän huolettoman vaikutelman. On kuitenkin pidettävä mielessä, että yritysten vertailukohtana ovat muut verkkokaupan maksutavat ja bitcoinin olennaisin ero näihin on nimenomaan helppous ja yksinkertaisuus. Osaksi vastaukset kuvastavat myös yleisellä tasolla bitcoinin käytön ja maksujen vastaanottamisen helppoutta ja turvallisuuteen luottamista.

No toimii hyvin kaikinpuolin

Maksujen vastaanottaminen toimii todella hyvin

Helppoa ja miellyttävää.

6.3.2 Maksutavan käyttöönotto

Yrityksen käyttämän ratkaisun käyttöönoton osalta kokemukset poikkesivat toisistaan erityisesti työmäärän osalta. BitPay-palvelua käyttävät yritykset eivät maininneet käyttöönottoon liittyviä ongelmia tai vaikeutta, vaan kokivat sen helpoksi ja yksinkertaiseksi.

Bitpay-maksupalveluun rekisteröityminen ja siihen liittyvän laajennuksen asennus verkkokauppaohjelmistoon, helppoa oli

Ne yritykset, joiden toteutukseen liittyi omalla palvelimella toimiva asiakasohjelma, kokivat toteutuksen jonkin verran vaikeaksi tai todella helpoksi mutta molemmissa tapauksissa melko työlääksi. Kokemukseen on osaltaan vaikuttanut yrityksen sisäinen ohjelmointiosaaminen, jonka koettiin helpottaneen toteutusta. Tästä voidaan päätellä, että ilman ohjelmointiosaamista toteutus olisi ollut huomattavasti vaikeampaa ja työläämpää.

Toki tämä on hankalampi tapa kuin moni muu, mutta siihen aikaan ei vielä ollut valmiita ratkaisuja tarjolla. Toisaalta ohjelmointiosaaminen löytyi talostamme sisältä, joten itse toteuttaminen ei ollut ongelma.

Toteutus oli todella helppoa.

Maksumoduuli oli englanninkielinen, käänsimme sen itse suomeksi

6.3.3 Maksutapahtumien käsittely

Itse maksutapahtumien käsittely oli käytettävästä tavasta riippumatta kaikkien tutkittavien mielestä helppoa ja vaivatonta ja vastaajat arvioivat maksamisen olevan helppoa myös verkkokaupan asiakkaille. Positiivisiksi puoliksi omaa asiakasohjelmaa käyttävät kokivat sen, että bitcoinmaksujen vastaanottaminen on ilmaista ja varat ovat käytettävissä välittömästi. BitPay-palvelun käyttäjät kokivat sen käytön helpommaksi ja kevyemmäksi verrattuna asiakasohjelman käyttöön. Yksi asiakasohjelmaa käyttävistä yrityksistä arveli bitcoinmääräisten maksujen vastaanottamisen mahdollisesti työlääksi, mutta vain oletuksena, sillä yrityksen mukaan maksutapaa ei ole juuri käytetty. Yritys, joka hoitaa maksutilanteen näyttämällä vain asiakkaalle bitcoin-osoitteen maksutilanteessa arveli, että rajapinta maksupalveluntarjoajaan saattaisi olla hyödyllinen jos maksuja tulisi enemmän.

Erittäin kevyt ja helppo, ei tarvitse omaa Bitcoin-asiakasohjelmaa

Erittäin helppoa, ei eroa oikein muistakaan maksutavoista

Bitcoinin vastaanottaminen on todella edullista. Meidän toteutuksella maksujen vastaanottaminen on kulutonta.

Pystymme tarkistamaan sekunnin tarkkuudella milloinka maksu on rekisteröitynyt verkkoon.

6.3.4 Turvallisuus

Bitcoinin käyttö koettiin turvalliseksi sekä BitPay-palvelua käyttävien, että asiakasohjelmaa käyttävien yritysten keskuudessa. Turvallisuuteen vaikuttavia seikkoja olivat erityisesti maksutapahtumien nopeus ja asiakasohjelmaa käyttävien yritysten osalta oman palvelimen hallinta, jolloin turvallisuuteen voitiin itse vaikuttaa. Vaikka BitPay-palvelun käyttäjät mainitsivatkin huonona puolena ulkopuolisen palveluntarjoajan varassa olemisen, kokivat he palveluntarjoajan kuitenkin luotettavaksi ja turvalliseksi. Turvallisuutta tuovana tekijänä koettiin se, että maksujen tilitys tapahtuu nopeasti.

Kyselyyn osallistuneista yrityksistä yksikään ei kokenut erityisiä turvallisuushkia bitcoinin käytön suhteen, eikä ollut kokenut tarvetta varautua niihin. Vastaajat ovat kuitenkin luultavasti jättäneet mainitsematta uhkiin varautumisena sellaisia toimia, jotka koetaan itsestäänselvyyksinä. Tällaisina voidaan pitää esimerkiksi uuden osoitteen luomista jokaista maksutapahtumaa varten anonymiteetin säilyttämiseksi. Luultavaa on, että vastaajat ovat ymmärtäneet kysymyksen tietoturvahkista kysymyksenä tietoturvariskeistä ja vastauksista ilmeneekin nimenomaan riskien ja haavoittuvuuksien kokeminen. Tämä oletus lähtökohtana voidaan tuloksista päätellä, että tietoturvariskejä ei maksujen vastaanottamiseen liittyen koettu.

Eipä ole tullut koettua [tietoturva]ongelmia tai sellaisia mielessä.

Koemme sen erittäin turvalliseksi. Emme ole kokeneet tietoturvahkia itse maksujen vastaanottamisessa, sillä Bitcoin-osoite haetaan omalta palvelimelta.

BitPay oli jonkun aikaa palvelunestohyökkäyksen kohteena, mutta tämä asia on otettu hoitoon, joten emme pidä sitä enää uhkana. Riskejä tässä ei muuten ole. Emme ole nähneet tarpeelliseksi varautua uhkiin BitPayn osalta, vaan luotamme yhteistyökumppaniimme.

Vastaanottamisessa ei ole tietoturvaongelmia, koska kaikki maksut tarkistetaan manuaalisesti. Bitcoinien säilytyksessä ja käytössä normaalit tietoturvaohjeistukset pätevät

7 JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tarkoituksena oli selvittää erilaisia vaihtoehtoja bitcoinin hyväksymiseen verkkokaupan maksuvälineenä ja etsiä Datatronicille sopivin vaihtoehto tietoturvallisuuden näkökulmasta. Tutkimuskysymys oli: Mikä ratkaisu bitcoinin hyväksymiseen verkkokaupan maksuvälineenä olisi yritykselle sopivin tietoturvallisuuden näkökulmasta? Työn teoriaosuudessa käsiteltiin bitcoinia yleisesti, kerrottiin sen toimintaperiaatteista ja arvioitiin maksujen vastaanottamisen tietoturvallisuutta. Lisäksi esiteltiin erilaisia vaihtoehtoja maksujen vastaanottamiseen ja kerrottiin Datatronicin tämänhetkisestä tilanteesta. Tutkimuksessa selvitettiin käyttäjäkokemusten kautta, kuinka bitcoinmaksuja jo vastaanottavat yritykset kokevat käyttämänsä ratkaisun.

Jos ratkaisu valitaan puhtaasti tietoturvallisuuden näkökulmasta, on sopivia käytäntöjä noudattaen rakennettu omaan asiakasohjelmaan perustuva ratkaisu kaikkein varmin. Asiakasohjelmaa käytettäessä kaikki maksuliikenteeseen liittyvä on yrityksen omassa hallinnassa ja näin tietoturvallisuudesta voidaan varmistua yrityksen sisäisillä toiminta- ja tietoturvallisuusmenetelmillä. Bitcoinien muuntaminen euroiksi täytyisi tehdä jotain vaihtopalvelua käyttämällä.

Käyttäjäkokemuksista selvisi, että asiakasohjelmaa käyttävät yritykset ovat erittäin tyytyväisiä ratkaisuunsa ja kokevat sen turvalliseksi. Ratkaisun toteutus ja käyttö vaativat kuitenkin jonkin verran vaivannäköä, mutta koska Datatronicin emoyhtiön DevNetin sisältä löytyy hyvin ohjelmointiosaamista, olisi toteutus kuitenkin mahdollinen. Datatronicin tapauksessa asiakasohjelman käyttö maksujen vastaanottamiseen vaatisi yrityksen sisällä kiinnostusta itse bitcoiniin ja halua olla osallisena verkon toiminnan ylläpitämisessä. Asiakasohjelman käyttö olisi paras ratkaisu siinä tapauksessa, että Datatronic haluaisi maksujen vastaanottamisen lisäksi tukea verkon toimintaa ja samalla bitcoinin tulevaisuutta.

Koska tietoturvallisuus ei ole pelkästään teknistä turvallisuutta ja verkkokaupan toiminnassa maksuliikenne on vain yksi monesta osa-alueesta, on otettava huomioon myös valitun ratkaisun vaivattomuus. Ulkopuolisen palveluntarjoajan käyttäminen maksujen prosessointiin olisi Datatronicin tapauksessa helpoin ja vaivattomin ratkaisu maksujen vastaanottamiseen. Käyttöönotto oli

käyttäjäkokemusten mukaan ainakin BitPayn osalta helppoa ja maksujen vastaanottaminen sujuvaa. Koska Datatronic haluaisi ainakin alkuun muuntaa bitcoinit suoraan euroiksi, tekisi palveluntarjoajan käyttö sen helpoksi, eikä erillistä vaihtopalvelua tarvitsisi käyttää.

Maksupalvelun käyttöönotto vaatii palveluun rekisteröitymisen ja lisäosien asentamisen verkkokauppaohjelmistoon tai räätälöityjen muutosten tekemisen ohjelmakoodiin ohjelmointirajapintaa hyödyntäen. Jos Datatronicin uusi verkkokauppa tulee olemaan sellaisella alustalla, johon jommalla kummalla tässä työssä esitellyllä palveluntarjoajalla on tarjolla valmiita moduuleja, helpottaisi se käyttöönottoa vielä entisestään. Koska DevNet-konsernin sisällä on kuitenkin runsaasti ohjelmointiosaamista, olisi käyttöönotto joka tapauksessa helposti ja varsin nopeasti toteutettavissa myös räätälöitynä ratkaisuna.

Tässä työssä esiteltiin kaksi palveluntarjoajaa, jotka oli valittu esittelyn yhteydessä mainituin perustein. Palveluntarjoajat ovat hyvin samankaltaisia ja vaikuttavat molemmat helppokäyttöisiltä ja luotettavilta. Olennaisia eroja BIPS:n ja BitPayn välillä olivat siirtopalkkiot, SEPA-maksujen hinta sekä valuuttakurssitakuu. Vaikka BitPay periikin siirroista pienen siirtopalkkion, on se silti kokonaiskustannuksiltaan edullisempi, sillä euromääräisistä tilityksistä ei peritä erillistä maksua. Käytännössä palveluiden hinnoittelu ei kuitenkaan ole olennaista valinnan kannalta, sillä maksujen vastaanottaminen on joka tapauksessa perinteisiin maksutapoihin verrattuna lähes ilmaista. Ainoaksi merkittäväksi eroksi maksupalveluiden vertailussa nousee BitPayn tarjoama vaihtokurssitakuu. Koska Datatronicin haastatteluissa (Heino 2013) selvisi, että yrityksen myymien tuotteiden katteet ovat pieniä, voisi valuuttakurssin äkillinen laskeminen aiheuttaa tappioita. Tästä johtuen valuuttakurssitakuu on merkittävä tekijä sopivaa ratkaisua valittaessa.

Tietoturvallisuuden kannalta palveluntarjoajan käyttö siirtäisi toimintatapoihin liittyvistä riskeistä suuren osan pois yritykseltä. Erityisesti, jos maksut muunnetaan suoraan euroiksi, ei tietoturvallisuuden kannalta palveluntarjoajan käyttö eroa juurikaan perinteisten maksupalveluiden käytöstä. Ainoa ero bitcoinin tapauksessa on palveluntarjoajan yleinen luotettavuus. Tämän opinnäytetyön tarkoituksena ei ole ollut tehdä syvällistä luotettavuusanalyysiä yksittäisestä palveluntarjoajasta, joten lopullinen luotettavuuden arviointi jää Datatronicin tehtäväksi.

Johtopäätöksenä voidaan siis todeta, että tämän opinnäytetyön myötä saatujen tietojen valossa paras ratkaisu Datatronicille bitcoinmaksujen vastaanottamiseen olisi ainakin alkuvaiheessa BitPay-palvelun käyttö. BitPay tarjoaa sopivimmat ominaisuudet Datatronicin tämänhetkiseen tilanteeseen ja käyttäjäkokemusten perusteella sen toiminta on luotettavaa ja sujuvaa. Käytön aloittaminen vaatii rekisteröitymisen palveluun ja sivustolta löytyvien ohjeiden ja oppaiden mukaisten ohjelmakoodien lisäämisen tulevaan verkkokauppaohjelmistoon. Lisäksi palveluun rekisteröityessä tulee valita maksujen muuntaminen suoraan euroiksi.

Ratkaisun lopullinen toimivuus ja sopivuus selviävät luonnollisesti vasta sitä käytettäessä, mutta tässä työssä esille tulleiden käyttäjäkokemusten perusteella voidaan odottaa hyviä tuloksia. Tulevaisuudessa Datatronicin tarpeiden tai toimintatapojen muuttuessa, tulee ratkaisua arvioida aina uudelleen sen hetkisen tilanteen mukaan. Koska bitcoin on vielä uusi, nähtäväksi jää myös, minkälaisia uusia palveluita ja tapoja tulee tarjolle. Kun käytössä on jo jokin ratkaisu ja maksujen vastaanottamisesta kertyy kokemusta, myös uusien tapojen arviointi on helpompaa.

8 YHTEENVETO

Tämän opinnäytetyön yhtenä lähtökohtana oli henkilökohtainen kiinnostukseni bitcoinista ja sen tuomista mahdollisuuksista innovatiivisena uuden ajan maksuvälineenä. Hankin ensimmäiset bitcoinini vuonna 2012, mutta en ole juurikaan päässyt käyttämään niitä missään tilanteessa. Bitcoinit hyväksyviä kauppia on kovin vähän, eikä minulle tarpeellisia tuotteita ole juurikaan ollut tarjolla. Tuotteita voisi tietenkin ostella pelkästään sen vuoksi, että saisi bitcoinejaan käyttää, mutta se ei ole tuntunut järkevältä vaihtoehdolta. Osasy bitcoinit hyväksyvien kauppajien vähyyteen saattaa olla tiedon puute ja erityisesti se, ettei oikein tiedetä, mitä kaikkia toimia bitcoinien vastaanottamiseen liittyy ja minkälainen ratkaisu olisi valittava.

Bitcoineja tällä hetkellä hyväksyvät yritykset ovat lähes kaikki sellaisia, joiden johdossa tai henkilöstössä on bitcoinista kiinnostuneita henkilöitä. Kuten tämänkin opinnäytetyön tutkimusosuudessa tuli ilmi, on moni verkkokauppa myös perustettu siitä lähtökohdasta, että se vastaanottaa bitcoinmaksuja. Halusin kuitenkin etsiä sellaisen yrityksen, jonka verkkokaupan tuotevalikoima luultavasti kiinnostaisi bitcoinia käyttäviä asiakkaita, mutta joka ei niitä vielä vastaanota. Lahden Datatronic Oy paikallisena tietotekniikan tarvikkeita myyvänä yrityksenä vaikutti juuri sopivalta tämän opinnäytetyön toimeksiantajaksi ja he olivatkin saman tien erittäin kiinnostuneita yhteistyöstä. Yhteistyö heidän kanssaan oli erittäin miellyttävää ja olen ainakin henkilökohtaisesti tyytyväinen työn lopputulokseen, sillä heille sopiva ratkaisu löytyi.

Toivon, että lähitulevaisuudessa yhä useampi sellainenkin yritys, joka ei bitcoinista paljoa tiedä, kiinnostuisi bitcoinmaksujen vastaanottamisesta. Tämä opinnäyte toimii toivottavasti myös esimerkkinä muille yrityksille ja erityisesti maksujen vastaanottamisen tavan valinnan osalta toimia vertailun apuna omaa ratkaisua valitessa. Vaikka tässä työssä bitcoinista ja sen käyttämisestä kerrotaankin Datatronicin tapaukseen keskittyen, voi työtä käyttää erityisesti teoriaosuuden osalta myös oppaana bitcoinin käyttöön.

Tulevaisuudessa bitcoinin käytön mahdollisesti lisääntyessä olisi tärkeää tutkia tarkemmin sen vaikutuksia yritysten liiketoimintaan. Koska maksutapojen monipuolisuus on erityisesti verkkokaupankäynnissä suuri etu, on bitcoinin osalta mielenkiintoista nähdä, kuinka suuri vaikutus sillä tulee tulevaisuudessa olemaan verkkokauppojen asiakasvirtojen osalta. Vaikka bitcoinin käyttäjien osuus on vielä kovin marginaalinen, antaisi käyttäjien mieltymysten ja ostokäyttäytymisen tutkimus arvokasta tietoa siitä, minkälaisien yritysten kannattaisi alkaa vastaanottaa bitcoinmaksuja. Bitcoinin käyttäjien kannalta olisi myös aiheellista tehdä vertailuja ja käytettävyydetutkimuksia erilaisista maksutavoista, lompakkopalveluista ja muista säilytysmenetelmistä. Käytön lisääntyessä myös tarjolla olevien palveluiden ja ohjelmistojen tarjonta lisääntyy jatkuvasti ja laadukkaasti toteutetut ratkaisut tuovat etua kaikille bitcoinin käyttäjille.

Bitcoinin tarina on vasta alussa. Kukaan ei tiedä varmuudella kuinka sen tulee käymään. Bitcoin on kuitenkin esimerkki siitä, kuinka pienestäkin voi kasvaa suurta, kun tarpeeksi moni uskoo siihen ja yhdessä toimii yhteisen asian eteen. Teknologiat eivät koskaan ole itsessään hyviä tai pahoja, vaan niiden merkitys ja vaikutukset muodostuvat niitä käyttävien ihmisten valintojen ja päämäärien perusteella.

LÄHTEET

Elektroniset lähteet:

Bitcoin Charts 2013. Charts. [viitattu 20.9.2013]. Bitcoincharts.com. Saatavissa: <http://bitcoincharts.com/charts/mtgoxEUR#tgMzm1g10zm2g25zv>

Bitcoin.org 2013a. Bitcoin – Open source p2p money. [viitattu 20.9.2013]. Bitcoin Project. Saatavissa: <http://bitcoin.org/en/>

Bitcoin Wiki 2013b. Adresses. [viitattu 23.9.2013]. Saatavissa: <https://en.bitcoin.it/wiki/adresses>

Bitcoin Wiki 2013c. Bitcoin. [viitattu 20.9.2013]. Saatavissa: <https://en.bitcoin.it/wiki/bitcoin>

Bitcoin Wiki 2013d. Blocks. [viitattu 20.9.2013]. Saatavissa: <https://en.bitcoin.it/wiki/block>

Bitcoin Wiki 2013.e Blockchain. [viitattu 20.9.2013]. Saatavissa: <https://en.bitcoin.it/wiki/blockchain>

Bitcoin Wiki 2013f. Brain wallet. [viitattu 10.10.2013]. Saatavissa <https://en.bitcoin.it/wiki/brainwallet>

Bitcoin Wiki 2013g. History. [viitattu 20.9.2013]. Saatavissa: <https://en.bitcoin.it/wiki/history>

Bitcoin Wiki 2013h. Merchant How to. [viitattu 15.10.2013]. Saatavissa: https://en.bitcoin.it/wiki/merchant_howto

Bitcoin Wiki 2013i. Mining. [viitattu 10.10.2013]. Saatavissa: <https://en.bitcoin.it/wiki/mining>

Bitcoin Wiki 2013j. Paper wallet. [viitattu 10.10.2013]. Saatavissa https://en.bitcoin.it/wiki/paper_wallet

Bitcoin Wiki 2013k. Secure your wallet. [viitattu 15.10.2013]. Saatavissa: https://en.bitcoin.it/wiki/secure_your_wallet

Bitcoin Wiki 2013l. Transaction fees. [viitattu 10.10.2013].

Saatavissa: https://en.bitcoin.it/wiki/transaction_fee

Bitcoin Wiki . Transactions. [viitattu 10.10.2013].

Saatavissa: <https://en.bitcoin.it/wiki/transactions>

Bittiraha 2013. Bitcoin-karttapalvelu. [viitattu 29.9.2013]. Prasos Oy. Saatavilla:

<https://bittiraha.fi/content/bitcoin-karttapalvelu>

Kila 1895/23.10.2012. Lausunto digitaalisen vertaisvaluutan käsittelystä

kirjanpidossa. Saatavissa: <http://www.edilex.fi/kila/1895>

Multibit 2013. Secure lightweight international Bitcoin wallet. [viitattu

10.10.2013]. Multibit. Saatavissa: <https://multibit.org/index.html>

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

10.9.2013]. White Paper. Saatavissa: <http://bitcoin.org/bitcoin.pdf>

Verohallinto 2013. Virtuaalivaluuttojen tuloverotus. [viitattu 23.10.2013].

Verohallinnon ohjeet. Saatavissa: <http://vero.fi/fi->

[FI/Syventavat_veroohjeet/Verohallinnon_ohjeet/Virtuaalivaluuttojen_tuloverotus%2828450%29](http://vero.fi/fi-FI/Syventavat_veroohjeet/Verohallinnon_ohjeet/Virtuaalivaluuttojen_tuloverotus%2828450%29)

Painetut lähteet:

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere:

Vastapaino

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja.

Porvoo: WS Bookwell.

Haastattelu:

Heino, J. 2013. Toimitusjohtaja. Lahden Datatronic Oy. Haastattelu 12.9.2013.

LIITTEET

Liite 1. Kyselylomake

Kokemuksia bitcoinmaksujen vastaanottamisesta

- 1. Milloin ja minkä vuoksi aloitte vastaanottaa bitcoinmaksuja?**
- 2. Minkälainen ratkaisu yrityksellänne on bitcoinmaksujen vastaanottamiseen?**
Kertokaa ratkaisustanne ja siihen vaikuttaneista tekijöistä mahdollisimman seikkaperäisesti. Kuvailkaa myös kuinka helpoksi/vaikeaksi koitte toteutuksen.
- 3. Valitsemanne toteutuksen hyvät ja huonot puolet?**
Mikä toimii, mikä ei? Minkälaisia muutoksia kaipaisitte tai olette jälkeenkään tehneet?
- 4. Kuinka turvalliseksi koette bitcoinmaksujen vastaanottamisen?**
Minkälaisia tietoturvaohjeita olette mahdollisesti kokeneet ja minkälaiset uhkakuvat koette aiheelliseksi? Kuinka olette niihin varautuneet?
- 5. Minkälaiseksi koette bitcoinmaksujen vastaanottamisen käytännössä?**
Kuvailkaa asiaa maksun vastaanottajan, eli yrityksenne näkökulmasta. Helppous, miellyttävyys jne.
- 6. Kuinka bitcoinien käsittely yrityksessänne on hoidettu?**
Verotus, kirjanpito, säilytys jne.
- 7. Jos verkkokauppanne on ollut toiminnassa jo ennen bitcoinin hyväksymistä maksutapana, kuinka uusi maksutapa on vaikuttanut yrityksenne toimintaan ja liiketoimintaprosesseihin?**
- 8. Jäikö jotain mielestänne olennaista kysymättä?**
Muuta bitcoinmaksujen vastaanottamiseen ja sen aloittamiseen liittyvää, mistä haluaisitte kertoa.