HAAGA-HELIA
ammattikorkeakoulu

P2P-kryptovaluutta Bitcoin

Jesse Lindroos

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2012

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

Raportin palautuksen tai esityksen päivämäärä

Koulutusohjelma

Tekijä tai tekijät Jesse Lindroos	**Ryhmätunnus tai aloitusvuosi** 2012
Raportin nimi P2P-kryptovaluutta Bitcoin	**Sivu- ja liitesivumäärä** 49 + 15
Opettajat tai ohjaajat Jyri Partanen	

Tämä opinnäytetyö tarkastelee suhteellisen tuoreen, vertaisverkko-periaatteella toimivan elektronisen rahajärjestelmän, Bitcoinin, roolia sen käyttäjien elämässä. Siinä myös vertaillaan Bitcoinin ja perinteisten valuuttojen ominaisuuksia toisiinsa. Opinnäytetyön päätavoite oli tutkia, miksi Bitcoinin käyttäjät ovat valinneet tämän valuutan ja millä tavoin he hyödyntävät sitä. Toinen tärkeä näkökulma on tutkia Bitcoinin taloudellista potentiaa: minkälaista liiketoimintaa sen ympärille on kasvanut, ja onko mahdollista käyttää Bitcoinia perinteisten valuuttojen rinnalla.

Tutkimusosiota edelsi teoriaosuus. Siinä esiteltiin perinteisen valuutan transaktioprosessi ja turvaominaisuuksia, Bitcoinia teoriassa ja käytännössä ja Bitcoin-verkon keskeisintä toimintaa: Louhintaa, joka luo uudet bitcoinit louhijoille ja pitää samalla huolen verkon turvallisuudesta.

Tutkimusosio toteutettiin käyttämällä kyselyä. Kysely koostui 15-20 kysymyksestä, riippuen siitä, miten vastaaja vastasi niihin. Tulokset osoittivat, että kaikki vastaajat olivat melko nuoria ja koulutettuja miehiä, eikä kukaan heistä ollut nainen. Suurin osa vastaajista valitsi Bitcoinin suosiakseen yksinkertaista ratkaisua byrokratian sijaan, ja moni myönsi myös haluavansa protestoida fiat-valuuttoja vastaan. Vastaajat hyödynsivät Bitcoinia pääasiassa vaihtoehtoisena sijoituksena ja valuuttana erilaisten hyödykkeiden ostamisessa. Bitcoin-verkoston perustoimintaa ja turvallisuutta pidettiin enimmäkseen erinomaisena.

Opinnäytetyössä tultiin siihen johtopäätökseen, että toisin kuin fiat-rahan transaktioprosessi, Bitcoinin vastaava on yhtenäinen ja jämäkkä, mutta vaikka Bitcoinia on helppo käyttää, jää sen käytöstä vastuu pelkästään käyttäjälle itselleen. Kauppiaat ovat potentiaalisesti valmiita hyväksymään bitcoinit maksuvälineenä joko nyt tai tulevaisuudessa, ainakin teknisellä tasolla, mutta jää nähtäväksi kuinka moni on henkisesti valmis tarttumaan tilaisuuteen. Edellinen toteamus ja se fakta, että louhintametodeista täytyy tulla energiatehokkaampia, määräävät Bitcoinin menestymisen valtavirtamarkkinoilla.

Asiasanat
Hajautus, maksaminen, turvallisuus, arvo, kätevyys

HAAGA-HELIA
University of Applied Sciences

Abstract

Date of presentation

Degree programme

Authors Jesse Lindroos	**Group or year of entry** 2012
The title of thesis P2P CRYPTOGRAPHIC CURRENCY BITCOIN	**Number of pages and appendices** 49+15
Supervisor(s) Jyri Partanen	

This thesis examines the role of a relatively new Peer-To-Peer electronic currency system, Bitcoin, in its users' lives. It also compares Bitcoin's features with conventional currencies. The main goal of this thesis was to investigate why Bitcoin's users have chosen this currency and in which ways do they utilize it. Another important aspect of this thesis is to exmine Bitcoin's economic potential; what kinds of businesses have arisen around it and is it feasible to use Bitcoin beside conventional currencies.

Before the research part of the thesis, a background theory was composed. The theory part introduced conventional currency's transaction process and safety features, the theory and practice of Bitcoin and the key part of the Bitcoin network: Mining, which creates new bitcoins for the miners and at the same time, ensures the safety of the network.

The research was conducted by using a questionnaire. The questionnaire consisted of 15-20 questions, depending on how the respondent answered. The results showed that all the respondents were quite young and educated men, no female was involved. Most of them chose Bitcoin to favor simplicity over bureaucracy and many admitted that they wanted to protest against fiat currencies. The respondents utilized Bitcoin mainly as an alternative investment and as a currency to buy goods and services. The security and basic functionality of Bitcoin network was considered mostly excellent.

First of all, this study concluded that unlike the security of fiat money's transaction process, Bitcoin's equivalent is uniform and rigid but also, although Bitcoin is easy to use, it also leaves the responsibility fully to its user. Merchants are potentially ready to accept bitcoins as a payment method either now or in the future, at least technically, but it remains to be seen how many are psychically ready to seize the opportunity. The previous statement and the fact that mining methods must become more energy efficient, will dictate if Bitcoin is to become more popular in the mainstream market.

Key words
Decentralization, payment, security, value, convenience

Sisällys

Sanasto

Avoimen lähdekoodin ohjelma = Tietokoneohjelma, jonka lähdekoodi on avointa tarkastelua ja muokkaamista varten. Avoimen lähdekoodin ohjelmaa saa käyttää mihin tarkoitukseen tahansa ja kopioida ja jakaa ohjelman alkuperäistä ja muokattua versiota.
BTC = Bitcoinin rahayksikön lyhenne, vrt. EUR (euro) ja USD (Yhdysvaltojen dollari).
Credit = Velka, joka luvataan maksaa myöhemmin heti vastaanotetuista hyödykkeistä. Credit-sanalla tarkoitetaan myös maksukortin ominaisuutta, jolla näin pystyy tekemään.
Debit = Summa rahaa, joka otetaan pois tililtä myöhempää käyttöä tai välitöntä maksua varten. Debit-sanalla tarkoitetaan myös maksukortin ominaisuutta, jolla näin pystyy tekemään.
Deflaatio = Deflaatio voi tarkoittaa joko kuluttajahintojen yleistä laskua, rahan arvon nousua suhteessa hyödykkeiden arvoon tai rahamäärän vähenemistä. Deflaation vastakohta on inflaatio. Deflaatiota ei kannata sekoittaa devalvaatio-sanan kanssa.
Digitaalinen allekirjoitus = Sähköinen allekirjoitus, jonka tarkoitus on varmentaa lähetetyn datan sisältö ja lähettäjän/allekirjoittajan henkilöllisyys.
Double spending = Termi, jolla kuvataan digitaalisen rahan laitonta uudelleenkäyttöä kopioinnin avulla. Vastaava termi fyysisen rahan suhteen on väärentäminen tai petos.
ECDSA = Elliptic Curve Digital Signature Algorithm. ECDSA on digitaalisen DSA-avaimen variantti, joka hyödyntää elliptisen käyrän kryptografiaa.
EMV = Europay, MasterCard and Visa. Maailmanlaatuinen standardi, joka mahdollistaa siruilla varustettujen debit- ja credit-korttien toiminnan korttimaksupäätteissä ja raha-automaateissa.
Fiat-raha = Raha, jolla ei ole luontaista arvoa, ja jonka perustana ei käytetä esimerkiksi kulta- tai hopeakantaa. Fiat-rahan arvo perustuu hallinnon luomiin lakeihin ja säännöksiin ja yleiseen luottamukseen.
IP-osoite = Internetin Protokolla-osoite. Jokaisella internet-verkkoon kytketyllä tietokoneella on yksilöity IP-osoite, joka erottaa ja yksilöi tietokoneen muista. IP-osoitteen alkuosa kuuluu yksilöidylle verkolle ja loppuosa verkon sisäpuolelle yksilöidylle tietokoneelle.
Julkinen avain = Kaikille julkinen sähköinen avain (merkkijono), jonka vastaparina toimii yksityinen avain, jonka vain sen omistaja tietää. Toimii avainparina yksityisen avaimen kanssa datan salaamisessa.

Rootkit = Haittaohjelma/-ohjelmisto, joka antaa järjestelmänvalvojan oikeudet hyökkääjälle saastuneeseen tietokoneeseen.

RPC = Remote procedure call. Etäproseduurikutsu, joka mahdollistaa tietokoneohjelman suorittavan jaetun verkon toisen tietokoneen toisessa muistiavaruudessa toiminnon tai aliohjelman ilman ohjelmoijan tarvetta ohjelmoida erillisiä yksityiskohtia etätoimenpiteen suhteen. Ohjelmoija ei siis RPC:tä hyödyntäessään joudu ohjelmoidessaan välittämään, suoritetaanko toiminto tai aliohjelma paikallisesti tai etäkohteessa.

SEPA = Single Euro Payments Area. Yhtenäinen euromaksualue, johon kuuluu 32 (määrä voi muuttua) Euroopan maata. SEPA-maiden välillä tehdyt euromääräiset tilisiirrot eivät eroa kotimaisista tilisiirroista.

Solmu = Tietue, joka sisältää tietoja ja linkkejä muihin solmuihin. Vertaisverkossa solmulla tarkoitetaan hajautetun verkon yhtä osaa, tietokonetta, joka on verkon välityksellä yhteydessä vertaisverkon muihin tietokoneisiin.

Tiiviste / Hash = Hajautusarvo, jonka avulla tieto tiivistetään pienempään osaan, jotta alkuperäistä tietoa voidaan verrata esimerkiksi kopioidun tiedon tiivisteeseen, jotta voidaan varmistaa kopion validiteetti suhteessa alkuperäiseen.

Yksityinen avain = Datan salaamisessa käytetty, ainoastaan sen omistajan tuntema avain, jonka parina toimii julkinen avain. Yksityisen avaimen avulla voidaan purkaa sen julkisella avainparilla allekirjoitettua ja salattua dataa

1 Johdanto

Bitcoin on avoimen lähdekoodin periaatteella toteutettu digitaalinen valuutta, jonka BTC-rahayksiköitä ihmiset voivat lähettää toisilleen ilman keskitettyä tahoa. Tähän se kykenee hyödyntämällä vertaisverkkoperiaatetta, kuten nykyaikaiset tiedostonjako-ohjelmatkin.

Bitcoin on ilmiönä melko uusi. Sen kehitti mies, joka kutsuu itseään nimellä ”Satoshi Nakamoto” vuonna 2008. Nyt tämä ilmiö on kehittynyt moniulotteiseksi valuutaksi, jonka ympärille on kehitetty muun muuassa valuutanvaihtopalveluita, lehti, uutispalveluita, internet-kauppoja ja mainospalveluita, joiden avulla saa pienen määrä bitcoineja per päivä. Varjopuolena rikolliset tahot voivat anonyymisti käydä kauppaa esim. huumeilla ja aseilla erilaisten anonyymien internet-sivujen välityksellä, käyttäen bitcoineja vaihdannan välineenä.

Bitcoin on tutkimisen arvoinen, koska se on ensimmäinen hajautetusti toimiva digitaalinen valuutta, jolla ei, sisäänrakennettua deflaatiota lukuun ottamatta, ole keskitettyä, keskuspankin lailla toimivaa ohjaajaa. Tutkimisen arvoa lisää sekin fakta, että Bitcoinista käydään ja on käyty paljon keskustelua siitä, onko se kehitetty moraalisesti kestävälle pohjalle ja ylipäänsä siitä, miten pitkälle valuutta tulee selviytymään ja kehittymään pitkällä aikavälillä. Ja koska Bitcoin omalla tavallaan kilpailee keskitettyjen valuuttojen kanssa, niin vertailemme tutkimuksessa näiden kummankin ominaisuuksia.

Aloitan tutkielman selvittämällä ensin keskitettyjen, perinteisten valuuttojen sähköisen pankkitoiminnan, tilisiirtojen prosessin ja tietoturvan teoriaa. Tämän jälkeen tutkielmassa kootaan lähteiden avulla teoriatausta Bitcoinin olemuksesta, perustoiminnasta, käyttämisestä ja bitcoinien louhimisesta. Teoriaosuuden jälkeen on vuorossa tutkimus, jossa suoritetaan Webropol-sovelluksen avulla kysely, jonka tarkoitus on selvittää Bitcoinin käyttäjien suhdetta Bitcoiniin ja sitä, minkälaisia taloudellisia edellytyksiä Bitcoinilla on. Tutkielman lopussa teoriataustasta ja tutkimusosuudesta vedetään yhteinen johtopäätös, jossa pohditaan Bitcoinin käytettävyyttä ja taloudellista potentiaalia.

1.1 Sähköinen pankkitoiminta

Bitcoin on täysin elektroninen rahayksikkö. Se kuitenkin poikkeaa perinteisestä pankkitoiminnasta täysin. Kerromme tässä luvussa alustavasti perinteisen fiat-rahan käytöstä elektronisessa pankkitoiminnassa, jotta tulisi selville, minkälainen suhde sähköistämisellä on perinteiseen rahaan ja kuinka suurta roolia se näyttelee kokonaisuudessa.

Elektroniseen pankkitoimintaan kuuluu internet-, puhelin-, TV-, mobiili- sekä PC-pohjainen pankkitoiminta. Elektroninen pankkitoiminta mahdollistaa 24-tuntisen asioinnin tiliotteen tarkistukseen, laskujen maksamiseen, lainan hakemiseen, arvopapereiden kauppaamisen sekä muihin mahdollisiin toimiin. (Parker M & T 2008, 1)

1.1.1 Tilisiirrot

Suomi kuuluu Euroopan yhtenäiseen euromaksualueeseen, SEPAan. Kun tilisiirto suoritetaan SEPA-alueella euroilla, täytyy tilinumerosta käyttää kansainvälistä IBAN-muotoa sekä pankin BIC-koodia. (Finanssialan Keskusliitto 2011). 1.1.2012 tuli voimaan EU:n maksupalvelulain kohta, jonka mukaan SEPA-alueen maksujenvälityksen tulee kestää enintään toimeksiantopäivän sekä yhden pankkipäivän (Finanssialan Keskusliitto 2009). Tilisiirto ulkomaille vaatii kaikki nämä kohdat:

- Maksajan tiedot: tilinumero, nimi, jakeluosoite ja osoitetoimipaikka
- Saajan tiedot: tilinumero, nimi, lähiosoite, kaupunki ja postinumero sekä maa
- Valuutta ja määrä
- Eräpäivä
- Maksutapa: maksumääräys tai pikamaksu
- Saajan pankin tiedot: BIC- ja Clearing-koodi, pankin nimi, katuosoite, kaupunki, postinumero ja maa

Tilisiirrosta saatetaan myös periä palvelupalkkio sekä oman pankin että ulkomaisen, vastaanottavan rahalaitoksen puolesta. On mahdollista valita pelkästään oman pankin kulut tai kummatkin. (Nordea 2011) Kulut voivat vaihdella sen mukaan, onko kyseessä

esimerkiksi SEPA-maksu tai maksu EU-alueen ulkopuolelle. Hinnoittelu vaihtelee tapauskohtaisesti, joten emme käy sitä läpi sen tarkemmin.

”Nykyään raha on suurimmaksi osaksi vain elektronisia merkintöjä liike-, säästö- ja osuuspankkien tietojärjestelmissä. Pankkijärjestelmässä näitä merkintöjä voidaan tuottaa hyvin vähäisellä työmäärällä ilman merkittäviä raaka-aine- tai energiakustannuksia.” (Kauko 2011, 4) Koska fiat-raha on nykyään suurimmaksi osin aineetonta ja kuitenkin laajalti ja oletusarvoisesti hyväksytty maksuväline, jonka arvo perustuu luottamukseen, niin voidaan olettaa, että myös täysin elektronisessa muodossa olevan valuutan olemassaolo on lähtökohtaisesti uskottavaa, jos sille annetaan tarpeeksi luottamusta.

1.1.2 Tilisiirtojen tietoturva

Ovatko perinteiset tilisiirrot turvallisia verrattuna esimerkiksi Bitcoinin vastaaviin? Tätä on vaikea arvioida, koska tilisiirtojen turvallisuus riippuu niin monesta tekijästä; käyttäjän tietokoneen ja verkkopankin tietoturvatasosta, käyttäjän tietotekniikan ymmärtämisestä ja monesta muusta asiasta. Näiden kartoitus veisi tutkimusta liikaa sivuraiteille, joten emme käy niitä läpi. Voimme kuitenkin selvittää, miten turvallisia universaalisti maksuissa käytetyt todennusjärjestelmät ovat, jotta voisimme vertailla niitä luvuissa 2.1 ja 2.2 selitettyihin Bitcoinin transaktioiden turvamekanismeihin.

Ihmiset käyttävät nykyään monesti erilaisia debit- ja credit-kortteja hoitaessaan maksujaan internetin kautta tai paikan päällä maksaessaan. Toisin sanoen, maksavalla asiakkaalla on luottokorttiyhtiön kortti, joka siirtää asiakkaan pankkitililtä rahaa yrittäjän pankkitilille. Luottokorttiyhtiöt toimivat siis välittäjinä pankin, maksajan ja vastaanottajan välillä. Eniten luottokortteja jakaneet yhtiöt Yhdysvalloissa ovat MasterCard ja Visa, joten keskitymme niiden käyttämään todennusjärjestelmään (Schulz & Woolsey 2012).

”Verified by Visa”- ja ”MasterCard SecureCode”-todennuspalvelut käyttävät kummatkin samaa ”3-D Secure”-protokollaa, jonka heikkouksista on tehty tieteellinen julkaisu Cambridgen yliopistossa vuonna 2010. Jo pelkkä sirujen tuleminen maksukortteihin on tehnyt hävinneiden ja varastettujen korttien väärinkäytöstä ja kopioimisesta vaikeampaa, mutta väärinkäytökset tapauksissa, joissa kortti ei ole läsnä (internet), ovat lisään-

tyneet huomattavasti. 3D Securen (josta lyhenne 3DS) tarkoitus on ollut parantaa EMV-sirukorttien tietoturvaa nimenomaan internetissä, mutta tutkimuksen mukaan tavoitetta ei ole saavutettu. (Anderson & Murdoch 2010, 1-2)

3DS:n päätarkoitus on varmistaa, että kauppias voi tunnistaa käyttäjän olevan tietyllä sarjanumerolla varustetun kortin oikea omistaja. Tutkimus väittää järjestelmän olevan kuitenkin hankala asiakkaille, koska 3DS:n kaavake esitetään kauppiaan internet-sivuilla iframessa. (Anderson & Murdoch 2010, 2-3) Iframe on html-tagi, joka mahdollistaa toisen HTML-dokumentin tuomisen sen hetkisen HTML-dokumentin sisälle omaan kehykseensä (W3Schools). Tämä kehys sisältää normaalissa kauppatilanteessa 3DS:n varmennuslomakkeen sen omalta varmennuspalvelimelta. Peruskäyttäjän on kuitenkin vaikea tietää, onko lomake aito vai phishing-yritys, koska hänen on myös vaikeaa ymmärtää, että lomake on kehyksen sisällä, jonka lähdekoodi saattaa tulla 3. osapuolen palvelimelta. (Anderson & Murdoch 2010, 3)

Toinen kohta tutkimuksessa käsittelee activation during shopping-ominaisuutta (ADS), jossa asiakkaalta kysytään usein esimerkiksi hänen henkilökohtaisia tietojaan ostotilanteessa, jotta hänen henkilöllisyys voidaan todentaa. Ongelma on siinä, että pankki saa itse päättää, miten ominaisuutta hyödynnetään, joka tekee käytännöstä epäyhtenäisen. Ja koska asiakkaan pitää syöttää lomakkeeseen kortin tiedot, on tämä otollinen tilaisuus rikollisille, jotka ovat erikoistuneet phishing-sivustojen tekemiseen. Tällöin rikollinen voi mahdollisesti saada kalastettua käyttäjältä sekä kortin numeron että identiteetin (Anderson & Murdoch 2010, 3)

2 Bitcoin teoriassa ja käytännössä

Bitcoin ei yksittäisenä sanana kerro itsestään vielä mitään muuta, kuin että se on biteistä koostuva kolikko. Sen vuoksi avaamme tässä kappaleessa Bitcoinin metafyysistä olemusta ja tapaa, jolla Bitcoin-verkko ja -asiakasohjelma toimii. Bitcoin keksittiin vuonna 2008, eikä sen perustoiminnassa ole ainakaan tätä tutkimusta kirjoitettaessa vielä ehtinyt tapahtua kovin suuria muutoksia. Tämän voi kuka tahansa tarkistaa Satoshi Nakamoton ”Bitcoin: A Peer-to-Peer Electronic Cash System”-julkaisusta, joka on Bitcoinin virallinen white paper, ja jota tässä luvussa hyödynnetään paljon lähteenä.

2.1 Bitcoinin filosofinen perusta

Suurin osa internetissä tapahtuvasta transaktioliikenteestä perustuu 3. osapuolen luotettuihin, taloudellisten tahojen maksuvälityspalveluihin, esimerkiksi Visan ”Verified by Visa”-palveluun. Näiden palveluiden tarkoitus on varmistaa, että kaupan kumpikin osapuoli voi luottaa toiseensa, ja ettei varojen väärinkäytöksiä tapahdu. Välityspalveluista joutuu kuitenkin maksamaan, joten maksujen hinnat nousevat, joka on haitallista etenkin pienempien maksujen yhteydessä. Ja koska välityspalvelut maksavat, niin täytyy kauppiaiden tietenkin kerätä asiakkaista paljon yksityiskohtaista tietoa varmistaakseen, että asiakas on kuka hän väittää olevansa, maksukykyinen ja muutenkin validi transaktioon. Tämä, kuten mikään muukaan järjestelmä, ei ole 100 % vilppivapaa, mutta se vaatii tietynlaista byrokratiaa ja teknisiä turvatoimia toimiakseen. Ja se maksaa. (Nakamoto 2008, 1)

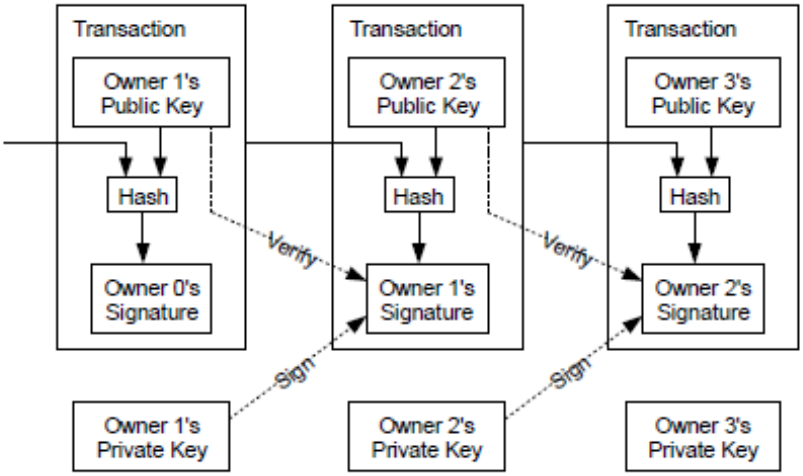
Bitcoin toimii eri tavalla. Se perustuu kryptografiseen todisteeseen, joten 3. osapuolen välittäjäpalveluita ei tarvita kaupan transaktioon. Bitcoinin tekninen rakenne pyrkii estämään double spending -ongelman, jossa digitaalisessa muodossa oleva raha on peilikopioitu/väärennetty, ja tällöin sen voi käyttää niin monta kertaa kuin sitä on kopioitu. Normaalisti 3. osapuoli (esim. pankki) pitää huolen tästä asiasta, joka on Bitcoinissa sisäänrakennettu ominaisuus. Järjestelmä toimii oikein niin kauan kuin enemmistö Bitcoin-verkosta, yli puolet, on hyväksi todetun laskentatehon takana. (Nakamoto 2008, 1)

2.2 Bitcoin-verkon toimintamalli

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

2.2.1 Transaktiot

Bitcoin-kolikko koostuu digitaalisten allekirjoitusten ketjusta. Kuten kuvasta 1 näkyy, kolikon 1. omistaja lähettää kolikon 2. omistajalle allekirjoittamalla edellisen transaktion tiivisteen ja 2. omistajan julkisen avaimen kolikon perään. Ja koska tämän uuden transaktion tiiviste on allekirjoitettu 2. (eli nykyisen) omistajan julkisella avaimella, voi 2. omistaja varmistaa ko. kolikon transaktioketjun omalla yksityisellä avaimellaan. Näin toimitaan aina uuden transaktion yhteydessä. (Nakamoto 2008, 2)



Kuva 1. Transaktio (Nakamoto 2009.)

Kolikon omistajan julkisena avaimena käytetään ECDSA (Elliptic Curve DSA) -avainta. Kun kolikko vaihtaa omistajaa, niin jokainen solmu saa tietoonsa tämän uuden omistajan julkisen avaimen. Toisin sanoen, jokainen solmu tietää jokaisen kolikon transaktioketjun, eli block chainin. (Bitcoin Wiki 2011.) Tietoa mm. transaktioista voi tarkistaa esim. osoitteesta http://blockchain.info ja http://blockexplorer.com/.

2.2.2 Transaktiomaksut

Bitcoinin transaktio saattaa sisältää transaktiomaksun. Transaktiomaksu menee bitcoinien louhijoille louhimisesta saatavan palkkion lisäkannustimena. Bitcoinin transaktiomaksuja voidaan verrata perinteisen fiat-rahan pankkien lainoista perimään korkoon; kun pankki perii korkoa ihmisille ja yrityksille antamistaan lainoista rahoittaakseen toimintaansa, veloittaa Bitcoinin vertaisverkko tarvittaessa automaattisesti transaktiomaksun suoritetusta transaktiosta bitcoinien louhijoille, jotta louhinta olisi kannattavaa esi-

merkiksi siitä syntyviin sähkölaskuihin nähden. Luvussa 2.2.4 ja 3 on lisätietoa louhijoista, louhimisesta ja eri louhinta-alustojen hyötysuhteesta. Transaktiomaksuilla yritetään myös tehdä Bitcoin-verkon tahallinen ruuhkauttaminen pienien ja monien transaktioiden avulla kannattamattomaksi; ruuhkauttajalle tulee erittäin kalliiksi tehdä monta pientä transaktiota peräkkäin.

10.6.2012 lähtien virallinen Bitcoin-asiakasohjelma vaatii minimissään 0,0005 bitcoinin transaktiomaksun transaktion sisällyttämisestä blokkiin sekä transaktion välittämisestä käyttäjältä toiselle 0,0001 bitcoinin transaktiomaksun. Mitä suuremman määrän transaktio vaatii dataa, sitä suurempi on myös transaktiomaksu. Jos yksittäisen transaktion koko on vähemmän kuin 10 kilotavua ja sen suuruus on enemmän kuin 0,01 bitcoinia, niin transaktiomaksua ei peritä. Muussa tapauksessa transaktiomaksut ovat pakollisia, eikä asiakasohjelma toteuta transaktiota, jos käyttäjä ei niitä hyväksy. Käyttäjä voi kuitenkin halutessaan valita asiakasohjelman asetuksista minimimaksun, jonka hän voi halutessaan maksaa jokaisesta tekemästään transaktiosta. Mitä isomman transaktiomaksun käyttäjä maksaa transaktiostaan, sitä nopeammin transaktio tulee voimaan Bitcoin-verkon teknisten rajoitusten puitteissa. Transaktiomaksut voivat muuttua ajan kanssa ja voi hyvin olla, että jo puolen vuoden päästä eri tekijöiden vuoksi maksujen määrä ja laskulogiikka voivat olla hyvin erilaisia kuin tätä tekstiä kirjoittaessa. (Bitcoin Wiki 2012)

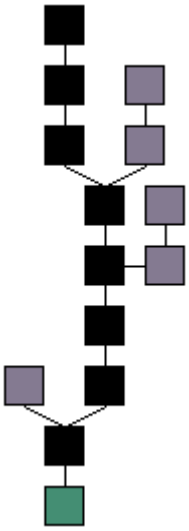
2.2.3 Block chain

Kaikki transaktiotietueet säilytetään jokaiselle solmulle jaetussa block chain -tietokannassa, joka koostuu blokeiksi (block) kutsutuista tietuesarjoista. Jokaisen blokin sisällä on edellisen blokin tiiviste, joka jatkuu aina ensimmäisenä, 3.1.2009, luotuun genesis-blokkiin saakka. (Bitcoin Wiki 2011.)

Jokaisen transaktion yhteydessä blokin uusi tiiviste aikaleimataan kronologisesti, jonka jälkeen tiiviste julkaistaan muille solmuille. Jokainen tiiviste myös sisältää edellisen aikaleiman, joka siten muodostaa luotettavan ketjun. (Nakamoto 2008, 2)

Blokin luotettavuus varmistetaan sen ”pituudella”, eli laskentatehon vaativuuden mukaan. Ja kuten kuva 2 osoittaa, niin Bitcoin-verkko pitää pisimpiä blokkeja kaikista luo-

tetuimpina. Blokin pitää olla myös viimeisimpänä ketjussa. Pisin ja viimeisin ketju on kaikista luotettavin, joten jos block chain haarautuu jossain vaiheessa, niin jatkossa uudet blokit luodaan sen perään. Ja koska verkossa on kaikki em. turvatoimet, jotka pakottavat luodut blokit juontamaan juurensa genesis-blokista, niin double spending/väärentäminen on erittäin vaikeaa, koska kaikki edellisetkin blokit pitäisi väärentää. Lyhyempiä blokkeja kutsutaan orvoiksi blokeiksi, ja vaikka ne säilytetään block chainissä, niin niiden perään ei kuitenkaan luoda enää uusia blokkeja, eikä niitä käytetä enää mihinkään. Jos orvossa blokissa sattuu kuitenkin olemaan verkon sääntöjen mukaisia transaktioita, niin ne siirretään lopuksi pitkän ja luotettavan blokin jatkoksi. (Bitcoin Wiki 2012.)



Kuva 2. Block chain, jossa mustat blokit valideja ja vihreä Genesis-blokki (Bitcoin Wiki 2010.)

2.2.4 Proof-of-Work ja uusien blokkien luonti

Luotettavuus on ehkä Bitcoin-verkon tärkein tekijä. Verkon perustoiminta ei vaadi 3. osapuolen varmennusta, jonka vuoksi varmennus täytyy integroida sovellukseen. Proof-of-Work:n tarkoitus on hallita uusien blokkien luontia luotettavasti ja hallitusti. Se onkin nimensä mukaisesti menetelmä, joka varmentaa uuden blokin tulleen luoduksi laskentateholla, eikä väärentämällä.

Jotta uusi blokki hyväksyttäisiin/luotaisiin block chainiin, täytyy sen tiivisteen arvon olla pienempi tai yhtä suuri kuin nykyinen kohde. Kohde on 256 bitin (2 ^ 256 -1 on

suurin 256-bittinen luku) SHA-256 -tiiviste, jonka jokainen Bitcoin-solmu tietää. Tiivistettä voi etsiä louhimalla, johon alun perin käytettiin prosessorin laskentatehoa, mutta jota nykyään toteutetaan enimmäkseen näytönohjainta hyödyntäen. Jos arvattu tiiviste on yhtä suuri tai pienempi kuin kohdeluku, niin uusi blokki luodaan ja liitetään block chainiin, jonka lisäksi kierroksen voittaja palkitaan X määrällä uusia bitcoineja, josta lisätietoa luvussa 3. Jos ei, niin tiivisteen arvaaminen jatkuu siten, etteivät edelliset arvaamiset vaikuta seuraavien vaikeustasoon. (Bitcoin Wiki 2011.)

Epäonnistuneet arvaukset eivät ole turhia, koska ne kasvattavat blokin nonce-arvoa inkrementaalisesti, jolloin kyseistä blokkia ei voi väärentää ilman, että edellä mainittu laskentatyö tehtäisiin uudelleen alusta asti. (Nakamoto 2008, 3)
Sen sijaan verkko säätää vaikeustasoa jokaisen 2016 uuden, löydetyn/louhitun blokin välein siten, että uusi blokki syntyisi jokaisen 10 minuutin välein. Syy tähän on se, että jos blokkeja luodaan liian lyhyin väliajoin, niin valuutasta tulee epävakaa. Jos taas liian harvoin, niin transaktioihin tulee liikaa viivettä, koska uudet transaktiot varmistuvat vasta kun solmut ovat hyväksyneet uuden blokin, johon uudet transaktiot tallennetaan. Kohdelukua muuttamalla vaikeustaso joko lisääntyy tai vähenee. Pienempi kohdeluku lisää vaikeustasoa, isompi vähentää. Vaikeustasoa ei kuitenkaan muuteta kerralla kerroinlukua 4 enempää. (Bitcoin Wiki 2011.)

2.2.5 Bitcoin-verkon vaiheet askeleittain

Tässä kappaleessa kootaan yhteen edellä mainitut Bitcoin-verkon vaiheet ja esitetään lyhyesti järjestys, jolla saadaan aikaiseksi kokonainen, toimiva Bitcoin-verkko.

1. Uudet transaktiot tuodaan julki verkon jokaiselle solmulle.
2. Jokainen solmu kerää uusia transaktioita ja pyrkii yhdistämään ne blokkiin.
3. Jokainen solmu, ts. jokainen louhiva solmu, koittaa laskentatehon avulla löytää Proof-of-Work:in mukaisesti kohdelukua pienemmän tai yhtä suuren SHA-256 -tiivisteen luodakseen uuden blokin.
4. Solmun löytäessä oikean tiivisten, se tuo sen julki kaikille muillekin solmuille.
5. Muut solmut hyväksyvät kollektiivisesti löydetyn/louhitun blokin, jos kaikki sen sisältämät transaktiot ovat valideja, eivätkä jo käytettyjä, estäen double spending -/väärennys-ongelman.

6. Solmujen hyväksyttyä uuden blokin, ne tallentavat sen tiivisteen block chainin uusimmaksi ja alkavat luomaan seuraavaa blokkia sen perään. (Nakamoto 2008, 3)

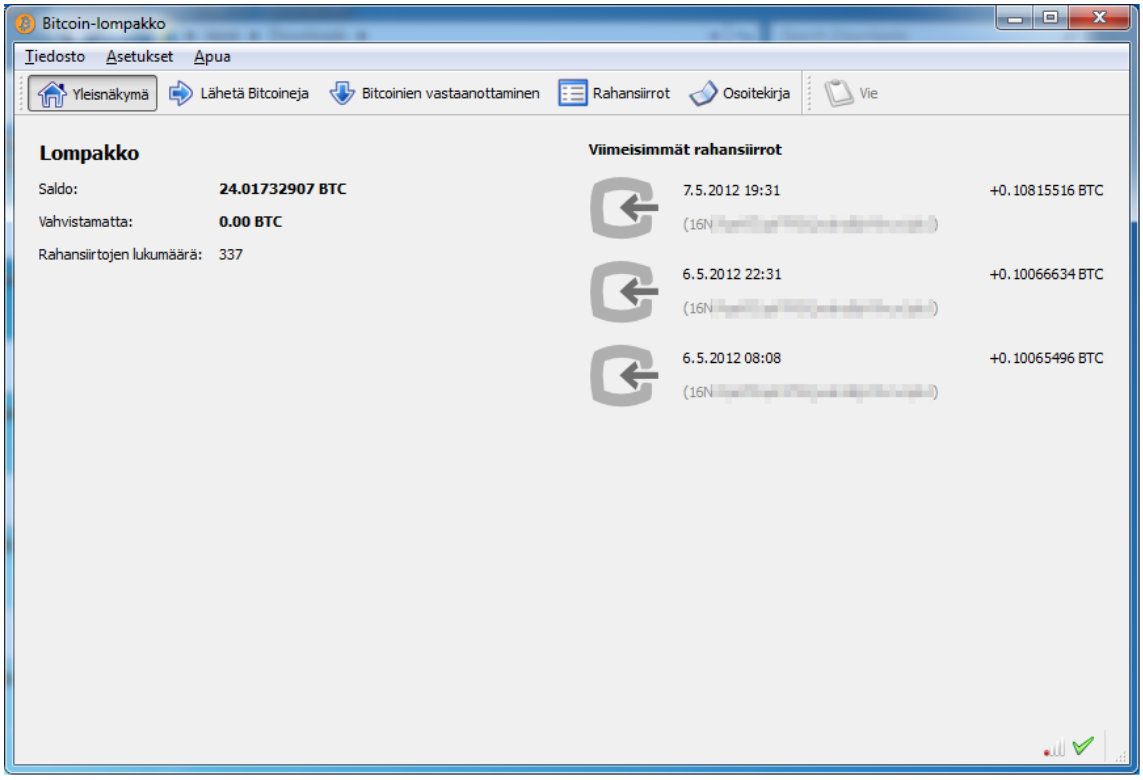
2.3 Bitcoin-asiakasohjelma

Käyttäjä tarvitsee avoimeen lähdekoodiin perustuvan Bitcoin-asiakasohjelman liittyessään Bitcoinin P2P-verkostoon. Yksi asiakasohjelma vastaa verkon yhtä solmua. Louhimista lukuunottamatta kaikki luvussa 2.2 tapahtuvat toiminnot tehdään Bitcoin-asiakasohjelmalla. Näistä toiminnoista kaikki paitsi Bitcoinien lähettäminen tapahtuvat automaattisesti. Pystyäksemme selittämään tutkimuksen lukijalle Bitcoin-asiakasohjelman toimintaa selkeästi, esittelemme nopeasti graafisella käyttöliittymällä varustetun, Windows 7:lle asennetun version ja muutaman siihen liittyvän oleellisen yksityiskohdan.

2.3.1 Windows-version graafinen käyttöliittymä

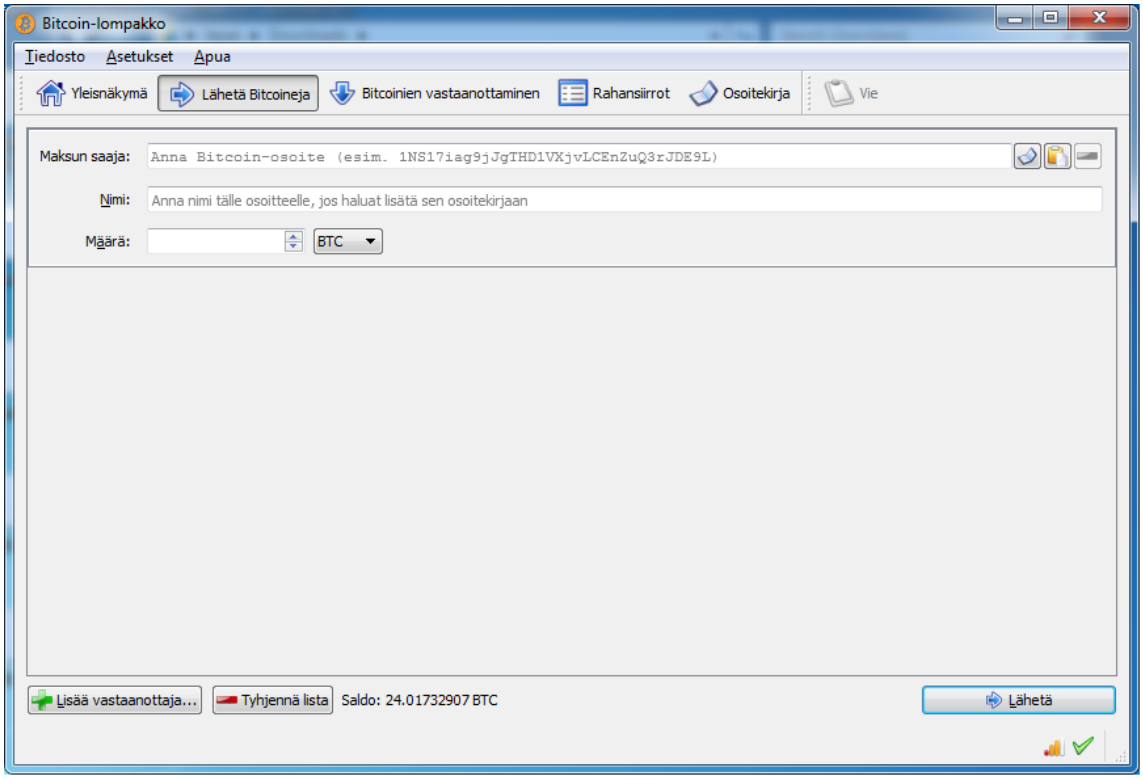
Bitcoinin käynnistyttyä se lataa aluksi luvussa 2.2.2 mainitun block chain -transaktiotietokannan käyttäjän koneelle ja luo käyttäjälle yhden Bitcoin-osoitteen, joka koostuu julkinen/yksityinen ECDSA-avainparin julkisen avaimen 160-bittisestä tiivisteestä (Bitcoin Wiki 2012). Tämä osoite on varsinainen bitcoineja vastaanottava osoite.

Kuten kuvasta 3 ilmenee, on ohjelma nimetty Bitcoin-lompakoksi. Kuvassa on ohjelman yleisnäkymä, jossa näkyy käyttäjän saldo, eli määrä, jonka verran hän omistaa bitcoineja. Näkymässä on myös jo saapuneiden bitcoinien määrä, jota asiakasohjelma ei ole vielä vahvistanut. Ohjelma pitää näitä transaktioita vahvistettuina vasta, kun transaktion jälkeen on luotu 6 uutta blokkia, eli jotakuinkin tunnin päästä (Bitcoin Wiki 2011). Mitä enemmän muiden solmujen hyväksymiä blokkeja on transaktion jälkeen luotu block chainiin, sitä suuremmalla varmuudella tehty transaktio ei ole väärennös tai muulla tavalla epävalidi. Yleisnäkymässä on myös tilin transaktioiden lukumäärä sekä viimeisimmät transaktiot.

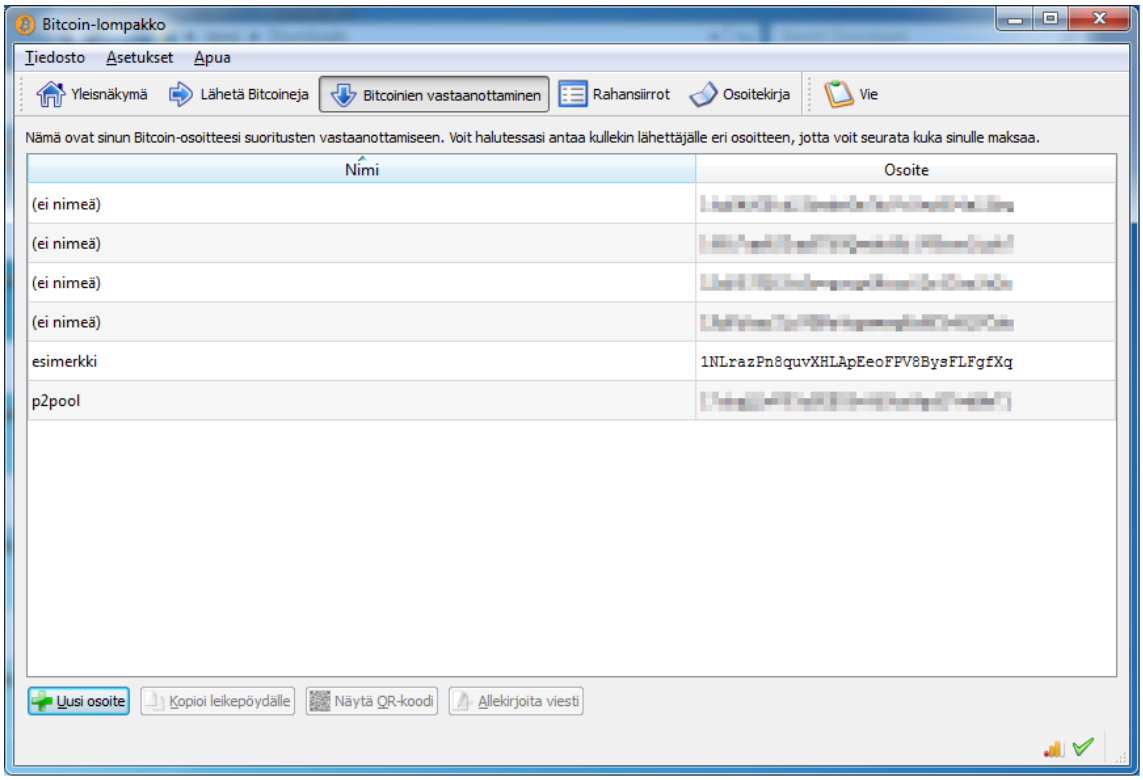


Kuva 3. Bitcoinin yleisnäkymä

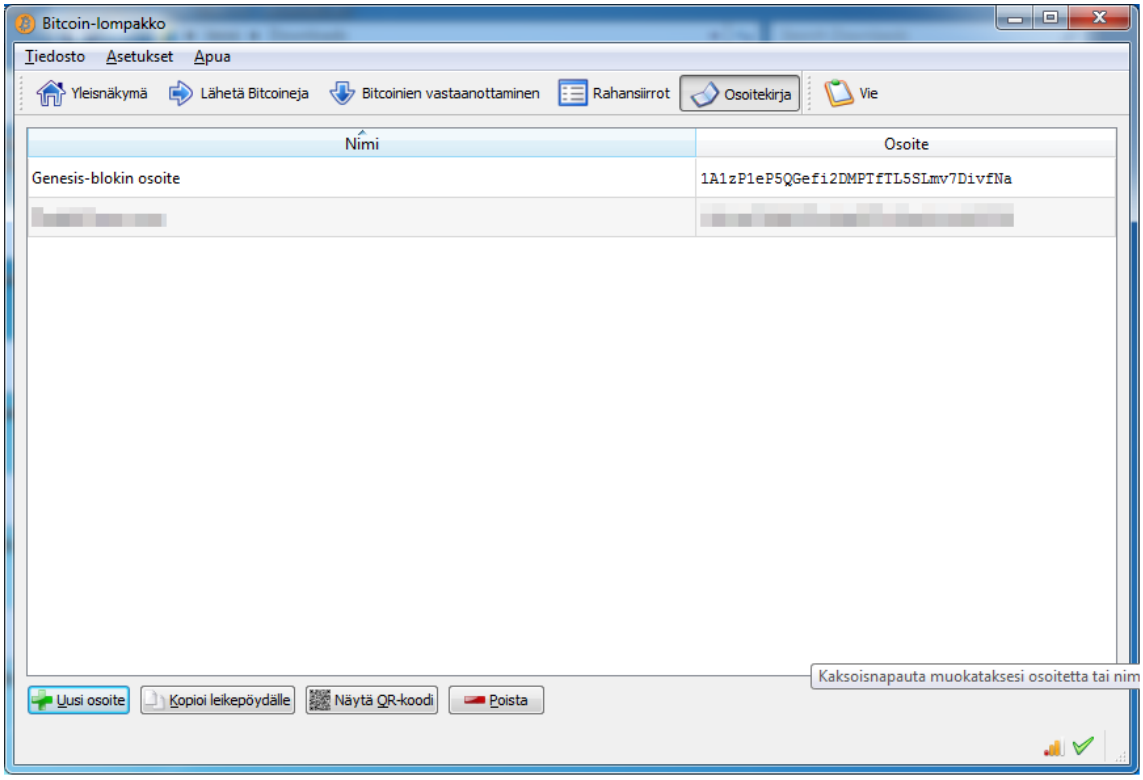
Kuvassa 4 näkyy ohjelman sivu, jossa voi lähettää bitcoineja eri osoitteisiin. Transaktioita voi tehdä monta kerrallaan, jos haluaa. Asiakasohjelmalla on myös kuvan 6 mukaisesti mahdollista pitää osoitekirjaa, josta nimetyn osoitteen voi pikavalita maksun saajaksi. Kuvasta 5 huomaa, että yksi Bitcoin-tili voi sisältää monta vastaanottavaa osoitetta. Osoitteet toimivat suppilomaisesti, eli kaikki vastaanotetut transaktiot menevät samaan tiliin, joten osoitteet eivät toimi erillisinä tileinä. Eri osoitteet mahdollistavat teoreettisen anonymiteetin, koska käyttäjän ei tarvitse antaa samaa osoitetta eri tahoille. Käyttäjän on myös helpompi seurata eri lähettäjiä antamalla heille yksilöllisen osoitteen.



Kuva 4. Bitcoinien lähettäminen

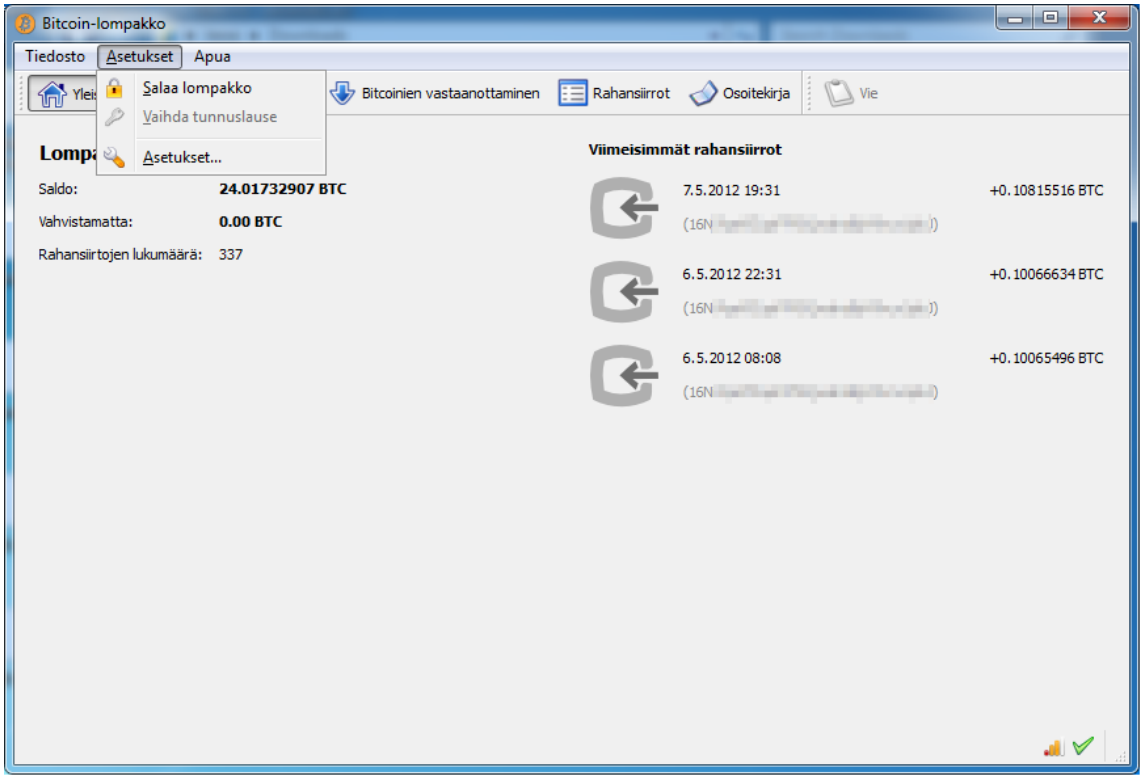


Kuva 5. Bitcoineja vastaanottavat osoitteet



Kuva 6. Osoitekirja

Alun perin Bitcoinissa ei ollut mahdollista salata lompakkoa salasanalla, mutta kuva 7:n mukainen ”Salaa lompakko”-asetus tuli mukaan uudemmissa versioissa. Salasanalla suojattu lompakko estää luvatonta käyttäjää varastamasta lompakon/tilin sisältöä esimerkiksi tilanteessa, jossa käyttäjän tietokone on kaapattu rootkitillä, tai jos luvaton käyttäjä pääsee siihen käsiksi paikan päällä. Salasanaa voi muuttaa, mutta ainakaan tätä tutkimusta kirjoittaessa ei ole olemassa vaihtoehtoa jo salatun lompakon salauksen poistamiseen.



Kuva 7. Bitcoinin asetukset ja lompakon salaus

2.3.2 Lompakko

Bitcoin-asiakasohjelman varsinainen lompakko on sen data-kansiossa sijaitseva wallet.dat. Wallet.dat sisältää seuraavat asiat:

- Käyttäjän bitcoinien vastaanotto-osoitteiden julkinen/yksityinen-avainparit
    - Luvun 2.3.1 kuvassa 5 ja sen selitteessä tarkempaa tietoa
- Käyttäjän osoitteisiin ja osoitteista muihin osoitteisiin tehdyt transaktiot
- Käyttäjän asetukset
- Oletusarvoinen vastaanotto-osoitteen avain
    - Tämä on sama avain, joka on selitetty luvun 2.3.1 alussa
- Bitcoin-tilit, joista jokainen voi sisältää useita vastaanotto-osoitteita
- Bitcoin-asiakasohjelman versionumero
- Avainpooli, joka sisältää valmiita julkisia ja yksityisiä avaimia transaktioita varten
- Tietoa uusimmasta ja luotetuimmasta block chainistä

(Bitcoin Wiki 2011)

Yksi Bitcoin-lompakko voi sisältää monia tilejä. Bitcoin tukee useita RPC-etäproseduurikutsun metodeja, joiden avulla tämä voidaan toteuttaa. Tämän tarkoitus on helpottaa web-palveluiden luomista, jossa yhdellä lompakolla voidaan hallita monen eri käyttäjän tiliä. (Bitcoin Wiki 2012)

3 Louhinta

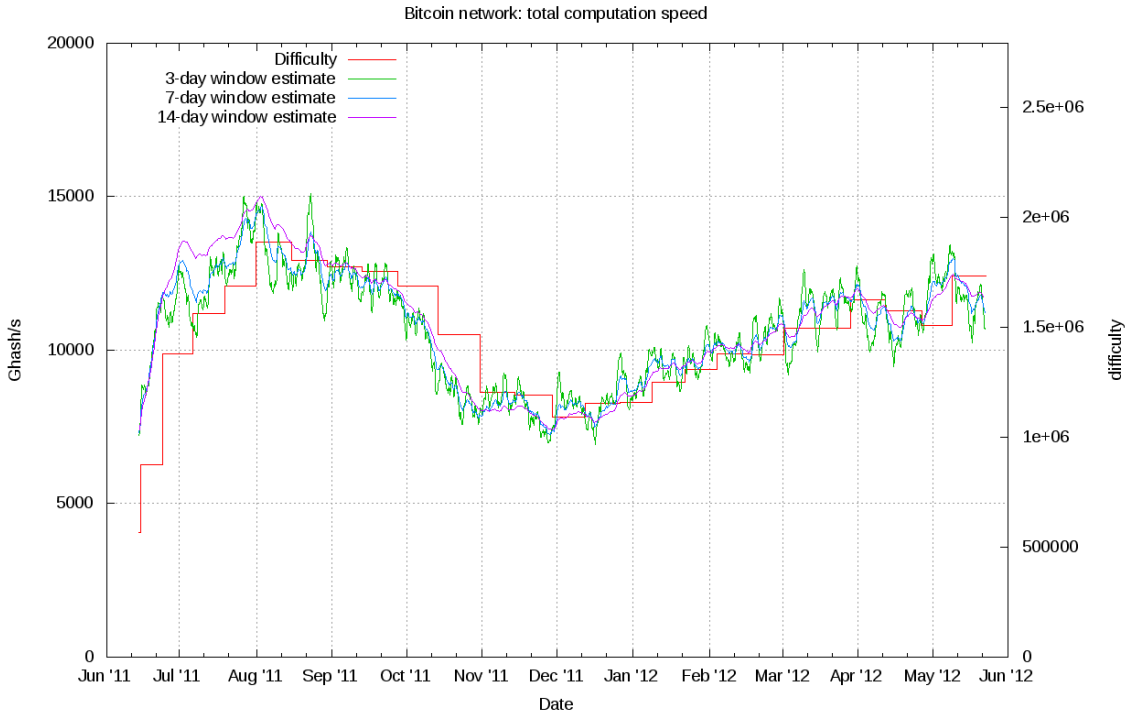
Louhinta on luvun 2.2.3, Proof-of-Work:n mukaista, SHA-256 -tiivisteen arvaamista uuden blokin luomista varten. Louhinta vaatii paljon laskentatehoa ja mitä enemmän kollektiivista laskentatehoa on, sitä vaikeammaksi se muuttuu. Vastaavasti, kollektiivisen laskentatehon laskiessa, helpottuu louhinta. Louhintaa harrastetaan, koska siitä saa palkinnoksi bitcoineja, joita voi esimerkiksi vaihtaa fiat-rahaksi erilaisissa internetissä toimivissa valuutanvaihtopalveluissa tai käyttää valuuttana kaupoissa, joissa bitcoinit hyväksytään maksuvälineenä. Tätä kirjoittaessa jokaista luotua blokkia kohden vapautuu 50 bitcoinia. Palkkio kuitenkin puoliintuu jokaisen 210 000 luodun blokin välein (Bitcoin Wiki 2012).

3.1 Louhinnan nopeus, vaikeustaso ja bitcoinien määrä

Kuten luvussa 2.2.3 mainitaan, Bitcoin-verkko säätää louhinnan vaikeustasoa siten, että uusi blokki syntyy keskimäärin jokaisen 10 minuutin välein. Laskulla ”210 000 * 10 min / 60 min / 24 h / 365 d = 3,9954 a = 4 a” voidaan ennustaa yhden blokin luomisesta saadun palkkion puoliintuvan jokaisen 4 vuoden välein. Bitcoinin rahayksikössä on kahdeksan desimaalia, joten kun louhintapalkkio tarpeeksi monen puolittumisen jälkeen pienenee 9. desimaalin puolelle, ei louhinta enää generoi uusia bitcoineja, jolloin bitcoinien määrä jää ~21 miljoonaan (Bitcoin Wiki 2012). Louhinnan ympärille syntynyt hajautettu ja kollektiivinen, erittäin suuri laskentatehon määrä, pyrkii palkkion lisäksi myös varmistamaan sen, ettei väärintekijä pysty ilman mittavia investointeja vääristämään block chainiä ja täten myöskään transaktioita.

Louhinnan nopeutta mitataan miljoonissa sekunnin aikana lasketuissa tiivisteissä, koska tällä hetkellä suurin osa louhimiskokoonpanoista laskee selvästi enemmän kuin miljoona, mutta vähemmän kuin miljardi tiivistettä sekunnissa. Siksi käytämme tästä lähtien

tutkimuksessa englanninkielistä lyhennettä Mhash/s, Mega/Million hashes per second, koska se on Bitcoin-yhteisön vakiintunut termi louhimisen nopeuden kuvaamisessa. Jos louhijoiden kollektiivinen laskentateho täytyy laskea yhteen, niin silloin pitää käyttää astetta isompaa etuliitettä, gigaa. Kuten kuvasta 8 näkee, louhinnan kollektiivinen laskentateho oli vuoden 2011 ja 2012 kesäkuiden välisenä aikana ~ 7500 – 15 000 Ghash/s.



Kuva 8. Louhinnan kokonaislaskentateho ja vaikeus kesäkuiden 2011 ja 2012 välillä (Bitcoin network graphs)

3.2 Louhimisalustat

Louhimisalustoilla viitataan tässä tutkimuksessa erilaisiin teknisiin välineisiin, joilla louhintaa toteutetaan. Louhinta vaatii paljon laskentatehoa, joka puolestaan kuluttaa sähköä. Kaikki erilaiset tekniset välineet kuluttavat eri määrän sähköä ja laskevat tietyn määrän SHA-256 -tiivisteitä sekunnissa. Vertailemme tutkimuksessa kolmea louhintaan soveltuvaa välinettä: tietokoneen prosessori, näytönohjain ja erillinen FPGA-mikropiiri.

3.2.1 Prosessori ja näytönohjain louhinnassa

Tutkimme ensin prosessorin ja näytönohjaimen eroavaisuuksia. Nykyaikainen moniydinprosessori sisältää usein alle 32 ALU-yksikköä, monta tasoa välimuistia sekä komponentteja logiikan hallintaan. Tämän monipuolisen kokonaisuuden avulla prosessori on optimoitu minimoimaan moniajossa tarvittavien säikeiden vasteajan, jotta käyttäjä pystyy hallitsemaan rinnakkain montaa eri sovellusta ilman suurempia viiveitä. Näytönohjain sisältää vähemmän välimuistia ja komponentteja logiikan hallintaan, mutta enemmän ALU-yksiköitä ydintä kohden sekä tiedonsiirron nopeuteen optimoidun muistiväylän, joka mahdollistaa tarvittavan kaistan lukuisille ALU-yksiköille. Tämä mahdollistaa näytönohjaimen suorittavan yksinkertaisia, aritmeettisia laskutoimituksia ja 32-bittisiä operaatioita erittäin nopeasti. (AMD 2011, 39-45)

Edinburghin yliopistossa vuonna 2010 tehty tutkimus paljastaa, että SHA-1 -version tiivisteiden laskemisessa näytönohjain, jossa on >=32 stream-prosessoria, ylittää tietokoneen prosessorin laskentatehon (Xouris 2010, 27-28). Stream-prosessorit ovat käytännössä ALU-yksiköitä. Tutkimuksessa käytetyt näytönohjaimet ovat kuitenkin näytönohjainvalmistaja Nvidian malleja ja Bitcoinin käyttämä SHA-256 -algoritmi kuuluu versioon SHA-2. Nvidian ja AMD:n näytönohjainten stream-prosessorien arkkitehtuuri eroaa toisistaan siten, että Nvidian CUDA-ytimet ovat monimutkaisempia ja tehokkaampia monipuolisissa tehtävissä, kun AMD:n vastaavat Stream-ytimet ovat puolestaan yksinkertaisempia ja tehokkaampia yhden, itseään toistavan tehtävän suorittamisessa. Tämä näkyy myös siinä, että AMD:n Stream-ytimet vievät vähemmän tilaa ja näin ollen niitä mahtuu piirilevylle enemmän. Siksi AMD:n näytönohjaimet kykenevät tekemään sekunnissa enemmän 32-bittisiä operaatioita kuin Nvidian. Bitcoinin SHA-256 -tiivisteitä laskeva louhinta-algoritmi on sattumoisin myös sillä tavalla toteutettu, että AMD:n näytönohjaimesta saa 1,7-kertaisen edun Nvidiaan. Louhinnassa etu on AMD:n näytönohjaimille yhteensä noin 3-5 -kertainen, joten käytännössä Nvidian näytönohjaimia ei käytetä tähän tarkoitukseen. (Bitcoin Wiki 2012) AMD:n tämän hetken nopeimmassa 6000-sarjan näytönohjaimessa, Radeon HD 6990:ssä on 3072 stream-prosessoria (AMD 2012). Vertailun vuoksi AMD:n heikoimmassa 6000-sarjan Radeon-näytönohjaimessa, Radeon HD 6450:ssä, stream-prosessoreita on 160 kappaletta

(AMD 2012). On siis selvää, että näytönohjaimessa on malliin katsomatta huomattavasti tietokoneen prosessoria enemmän laskentatehoa bitcoinien louhimista varten.

3.2.2 FPGA louhinnassa

Ohjelmoitava FPGA-mikropiiri, eli Field Programmable Gate Array, on hieman työläämpi ja harvinaisempi ratkaisu bitcoinien louhintaan. FPGA koostuu digitaalisista, integroiduista IC-piiristä, joissa on ohjelmoitavia logiikkablokkeja sekä konfiguroitavia liitoksia näiden välissä (Maxwell 2004, 1). FPGA-mikropiirejä on erilaisia, eivätkä kaikki niistä sovellu bitcoinien louhintaan. Yhteistä niissä on kuitenkin se, että ne kaikki ovat muokattavissa käyttäjän tarpeita varten. Tämän ansiosta niissä ei tarvitse ajaa taustalla laskentatehoa vievää ja sähkönkulutusta lisäävää, raskasta käyttöjärjestelmää, joten ne ovat hyötysuhteeltaan parhaita louhintaan, mutta hankintakustannuksiltaan suuria. FPGA:n suurimmiksi haittapuoliksi muodostuvat hinta ja ohjelmointitaitojen tarve.

3.2.3 Yhteenveto louhinta-alustojen hyötysuhteesta

Käymme tässä luvussa läpi hieman bitcoinien louhinnan hyötysuhdetta. Tämä on tärkeää, koska louhinta kuluttaa sähköä, mutta on välttämätöntä uusien bitcoinien luomista ja Bitcoin-verkon tietoturvan ylläpitämistä varten. Bitcoinin wiki-sivuille on koottu taulukoita, joissa lukee tietoa eri louhinta-alustojen louhintanopeudesta, sähkönkulutuksesta ja hankintahinnasta sekä näiden yhdistelmiä. Ne ovat suuntaa-antavia, mutta tarpeeksi informatiivisia, jotta voimme luotettavasti vertailla pöytätietokoneen prosessoria, näytönohjainta ja FPGA-mikropiiriä keskenään laskentatehon ja kulutuksen suhteen. Otamme kustakin ryhmästä parhaaseen hyötysuhteeseen optimoidun yksilön, jotta saamme käsityksen siitä, miten eri louhinta-alustat eroavat toisistaan. Kuten kuvasta 9 huomaa, paras hyötysuhde louhintaan on FPGA-mikropiirillä, sitten näytönohjaimella ja viimeiseksi vasta prosessorilla luvuin 25/3,06/0,176 Mhash/J, jossa siis 1 W = 1 J/s, eli yksi joule käytetään yhdeksi watiksi sekunnissa. (Bitcoin Wiki 2012)

FPGA:

Board	Cores	Mhash/s	Mhash/J	Mhash/s/$	Power [W]	Board price	Clock	Version	FPGA Model
Avnet Spartan-6 LX150T Development Kit	1	100	~25		~4.0	$995 [5]	100 MHz	fpgaminer makomk Xilinx port	Xilinx XC6SLX150T-3FGG676

Näytönohjain:

Model	Mhash/s	Mhash/J	Mhash / $[1]	Watts	Clock	SP	SDK	Slot
5850	282.75	3.06	-	92.25	666 (UC)	1440	2.1	PCI-E 2.1 x16

Prosessori:

Model	nprocs	Mhash/s	Mhash/J	TDP [W]	CPU Clock	Mhash/s CPU
Phenom II X6 1100T	6	22	0.176	125W	3.82 GHz	22

Kuva 9. Yhteen koottu kuva louhinta-alustojen hyötysuhteesta (Bitcoin Wiki 2012)

Vertaillessamme edellä kuvattua FPGA-mikropiiriä, näytönohjainta sekä prosessoria, huomaamme, että Avnet Spartan-6 LX-150T Development Kit kustantaa 793 euroa (Avnet Electronics Marketing 2012). AMD:n näytönohjain Radeon HD 5850 kustansi julkaisuhetkellä 280 euroa ja AMD:n prosessori Phenom II 1100T 275 euroa (MBnet 2009; MBnet 2011). Vaikka hinnat elävät ja ovat esimerkissämme suuntaa-antavia, niin voidaan niistä kuitenkin todeta se, että hyötysuhteeltaan paras louhinta-alusta, FPGA-mikropiiri, saattaa parhaimmillaan maksaa jopa kolme kertaa enemmän kuin omassa luokassaan parhaan hyötysuhteen näytönohjain tai prosessori. Louhinnassa FPGA jää silti määrälliseltä tuotoltaan monen näytönohjaimen taakse, kuten kuvasta 9 voidaan todeta. Tämän vuoksi, selvästi parhaasta hyötysuhteesta huolimatta, FPGA-mikropiirin hankintahinnan kuoletusaika louhinnalla on sen verran pitkä, että sijoitusajastakin muodostuu pitkä. Bitcoin on myös sen verran tuore ja vakiintumaton elektroninen valuutta, että näytönohjaimeen verrattuna FPGA on riskisijoitus.

3.3 Louhinta yksin ja yhteisöissä

Kun Bitcoin oli vielä alkutekijöissään, eikä käyttäjiä ollut olemassa paljon, niin myös louhijoiden määrä oli pieni. Siksi louhinnan vaikeustaso oli matala, jolloin sitä harrastavat saivat louhittua suurella todennäköisyydellä uusia blokkeja 50 bitcoinin palkkioineen melko pienellä odotusajalla. Tämän tietää jo siitä, että tammikuun 3. ja heinäkuun 25. päivän välillä 2009 koko Bitcoin-verkon louhinnan keskimääräinen laskentateho oli vain 5 Mhash/s, kun se tänä päivänä on yli 10 000 Ghash/s (Bitcoin Wiki 2011). Kun ajan kuluessa louhijoita tuli lisää, niin samalla louhinnan vaikeus mukautui, jotta uusi blokki syntyisi edelleen 10 minuutin välein. Lopulta yksittäisen louhijan mahdollisuus

löytää uutta blokkia ja saada täten palkkion, vaikeutui huomattavasti. Tämä ongelma ratkaistiin joulukuussa 2010, kun ensimmäinen keskitetty louhintapooli aloitti toimintansa, jota seurasi monen muun vastaavanlaisen poolin perustaminen (BITCOINCZ Mining 2012). Keskitettyjen louhintapoolien vastapainoksi kesäkuun 17. päivä 2011 julkaistiin vertaisverkkoperiaatteella toimiva P2Pool-pooli (Bitcoin Wiki 2012). Koska suurin osa louhinnasta tapahtuu nykyään näissä ympäristöissä, niin selitämme niiden toimintatapaa tässä luvussa.

3.3.1 Keskitetyt louhintapoolit

Bitcoinin ympärille rakentuneet keskitetyt louhintapoolit ovat seurausta ilmiölle, jossa yksin toimiva louhija ei enää kyennyt luomaan uutta blokkia tarpeeksi suurella todennäköisyydellä ja tasaisin väliajoin isoksi kasvaneen louhinnan vaikeustason vuoksi. Pooleja voisi verrata isoihin yrityksiin, joihin moni ihminen menee ennemmin töihin kuin perustaa yksityisyrityksen, jonka menestyminen on epävarmaa, vaikka kaikki tulot saisikin pitää itsellään. Poolien tapauksessa sellaiseen liittyvä louhija lainaa tietokoneensa laskentatehoa sen muiden käyttäjien tavoin poolin keskitettyyn louhimistoimintaan. Kun monta louhijaa toimii yhdessä, niin saadaan uusi blokki luotua kommuunin sisällä suuremmalla todennäköisyydellä kuin yksin louhiessa. Mitä enemmän yksi louhija pystyy antamaan laskentatehoa poolin käyttöön, sitä isomman siivun hän saa palkkiosta, jonka pooli on ansainnut louhittuaan kollektiivisesti uuden blokin. Tällöin käyttäjä ei saa yhtä suurta palkkiota kuin yksin louhiessaan, mutta todennäköisyys ansaita bitcoineja tasaisin väliajoin, tai ylipäänsä, kasvaa huomattavasti.

Keskitetyt poolit ottavat louhintapalveluistaan maksuksi korkeintaan muutaman prosentin louhituista bitcoineista sekä lähes aina pitävät kaikki transaktiomaksut itsellään (Bitcoin Wiki 2012). Käyttäjä tarvitsee keskitetyssä poolissa louhiakseen erillisen louhinta-asiakasohjelman, joka ottaa yhteyden pooliin. Ohjelma käyttää OpenCL-viitekehystä, joka siis mahdollistaa näytönohjaimen käytön tiivisteiden laskemisessa (Bitcoin Wiki 2012). Bitcoineja poolissa louhiva tietokone ei kuitenkaan tarvitse itse Bitcoin-asiakasohjelmaa, vaan riittää, että yksi bitcoinit vastaanottava tietokone ajaa ohjelmaa.

Keskitetyn louhintapoolin keskittyneisyys on sen hyödyllisyyden lisäksi myös sen isoin uhka, koska toteuttamalla palvelunestohyökkäys yhteen isoon pooliin, saadaan iso osa louhinnan kokonaislaskentatehosta pois, jolloin Bitcoinin tietoturva heikkenee. Jos esimerkiksi yksittäisen poolin laskentateho nousee yli 50 prosenttiin kokonaislaskentatehosta, niin se on vaara jo sinänsä, koska tällöin poolin pitäjällä on mahdollisuus peruuttaa kaikki tekemänsä transaktiot, estää ainakin osasta tehdyistä transaktioista varmistukset sekä estää ainakin osaa louhijoista louhimasta yhtään valideja blokkeja. Tätä kutsutaan 51 prosentin hyökkäykseksi (Bitcoin Wiki 2012). Ja vaikkei poolin omistaja näin tahtoisi tehdä, niin palvelimen kaappaus on aina mahdollista.

Poolien virka Bitcoinin maailmassa on loppupeleissä hyvinkin verrattavissa suurien pankkien merkitykseen fiat-rahan puolella: Luottamus näihin tahoihin kertoo siitä, että myös käytettävissä olevaan valuuttaan luotetaan. Jos luottamus instituutioon poistuu esimerkiksi väärinkäytösten tai huonosti hoidettujen asioiden takia, niin saattaa valuutan arvo laskea käyttäjien siitä luopuessa, tai kuten fiat-rahan suhteen voi käydä, voi yhdenkin suuren rahoitusmekanismi-instanssin kaatuminen vaikuttaa koko maailmantalouteen negatiivisesti fiat-rahan monopolimaisen aseman ja globaalien markkinoiden vuoksi. Bitcoinissa on kuitenkin vaihtoehto isojen poolien käyttämiselle, P2Pool. Tästä lisää seuraavassa luvussa.

3.3.2 P2Pool

P2Pool on epäkeskitetty louhintapooli, jonka jokainen solmu samaan aikaa sekä ylläpitää poolin toimintaa että toimii siinä myös louhijana. P2Pool-verkossa toimii Bitcoinin sääntöjen mukainen, hajautettu share chain, joka poikkeaa Bitcoinin omasta block chainistä vain siten, että siinä syntyy uusi blokki aina 10 sekunnin, eikä 10 minuutin, välein. Vaikeustaso on siis säädetty helpommalle kuin Bitcoin-verkossa. 10 sekunnin välein syntyvä blokki mahdollistaa useammalle solmulle mahdollisuuden vaikuttaa share chainin kasvamiseen, jonka avulla voidaan samalla mitata, kuinka suuren laskentatehon solmu on antanut P2Poolin toimintaan. Mitä enemmän solmu on löytänyt uusia blokkeja share chainiin muihin solmuihin verrattuna, sitä isomman provision se saa palkkiosta, kun P2Pool löytää uuden blokin Bitcoin-verkon vaikeustason mukaisesti. P2Pool toimii siis samaan aikaan automatisoituna palkkionjakajana sekä Bitcoin-verkon louhi-

jana, koska ennen pitkään se löytää myös itse Bitcoin-verkon vaatiman, 10 minuutin välein löydettävän blokin block chainiin. (Bitcoin Wiki 2012)

P2Pool vaatii toimiakseen solmulta kyvyn toimia sekä palvelimena että asiakkaana, koska tässä tapauksessa solmu ei ota yhteyttä poolin palvelimeen, vaan toiseen solmuun. Toisen solmun täytyy myös saada yhteys tähän solmuun, jolloin P2Pool toimii puhtaana vertaisverkkona. Käytännössä tämä tarkoittaa sitä, että Bitcoin-asiakasohjelma pitää ajaa RPC-rajapinta ja palvelin-asetus päälle kytkettynä, jonka lisäksi block chain pitää olla ajan tasalla. Tietokoneella täytyy tällöin olla myös erillinen P2Pool-ohjelmisto käynnissä, joka liittää tietokoneen P2Pool-vertaisverkkoon. Tämän jälkeen otetaan louhinta-asiakasohjelmalla yhteys localhostin portti 9332:een ja aloitetaan louhiminen. On kuitenkin mahdollista pitää P2Pool-palvelinta käynnissä toisella ja louhinta-asiakasohjelmaa toisella tietokoneella, jolloin yhteys otetaan palvelinkoneen IP-osoitteen, jolloin se toimii ikään kuin ”alipoolina” louhintakoneelle. Toisin kuin poolissa louhiessa, vaaditaan P2Pooliin liitetyssä tietokoneessa näytönohjaimen suorituskyvyn lisäksi myös enemmän muistin ja prosessorin käyttöä, joka hidastaa tietokonetta ja lisää sen sähkönkulutusta. P2Pool vie myös lähiverkon kaistaa paljon enemmän, koska solmun täytyy vastaanottaa ja ylläpitää muiden solmujen siihen ottamia yhteyksiä. (Bitcoin Wiki 2012) Näiden vuoksi P2Poolissa louhiva tietokone ei louhiessaan toimi muussa käytössä läheskään yhtä tehokkaasti kuin tietokone, joka louhii erillisessä poolissa. Oman tietokoneen konfigurointi P2Poolia varten on myös paljon vaikeampaa kuin normaaliin pooliin liittyminen, joten Bitcoin-amatööriä tämä vaihtoehto ei ehkä kiinnosta.

3.3.3 Yhteenveto luvusta 3

Bitcoinien louhinta jatkaa kehitystään. Alussa mukana oli vain muutamia ihmisiä, jotka harrastivat louhintaa Bitcoin-asiakasohjelman sisäänrakennetulla prosessori-louhinnalla. Louhijoiden siirtyessä tehokkaampaan näytönohjain-louhintaan pooleihin erillisine louhinta-asiakasohjelmineen, poistettiin Bitcoin-asiakasohjelmasta louhinnan mahdollisuus, koska kukaan ei enää käyttänyt sitä. Tämän jälkeen markkinoille tulivat FPGA-mikropiirit, jotka vastasivat hankintahinnaltaan edullisia ja hieman kalliimpia tietokoneita, ja joiden laskentateho vastasi erilaisten näytönohjainten laskentatehoa, mutta joiden

sähkönkulutus oli aika pitkälti 1/10 näytönohjaimen kulutuksesta. Louhimisalustojen tulevaisuus saattaa kuitenkin löytyä ASIC-piiristä.

ASIC on lyhenne sanoista application-specific integrated circuit ja Bitcoinin yhteydessä sillä tarkoitetaan louhintaan suunniteltua mikropiiriä. Johonkin tiettyyn tehtävään suunniteltu mikropiiri on tehokas lähinnä tehtävässä, johon se on suunniteltu, mutta on vastaavasti huonompi muissa tehtävissä, eikä sitä voi FPGA:n tavoin ohjelmoida uudelleen. (Smith 1997) Bitcoinien louhimiseen soveltuvat ASIC-mikropiirit ovat tätä tekstiä kirjoittaessa vasta tuotannon jälkeisessä esitilaus-vaiheessa, eli kaupallisessa ja laajamittaisessa käytössä niitä ei olla vielä nähty. Puutteellisten tietojen ja kokemusten vuoksi emme tutki sitä sen tarkemmin. Spesifikaatiot ovat kuitenkin lupaavia: Esimerkiksi Butterfly Labsin halvimman ASIC:n, 150 dollaria maksavan BitForce Jalapenon luvataan tuottavan 4,5 Ghash/s, joka on nopeudeltaan moninkertainen verrattuna mihin tahansa näytönohjaimeen tai FPGA-mikropiiriin, ja hintakin vastaa keskitehoisen näytönohjaimen hintaa (Butterfly Labs Inc. 2012).

4 Tutkimus

Opinnäytetyöni tutkimusosa käsittelee käyttäjien kokemuksia Bitcoinista. Tähän sisältyy myös Bitcoinin taloudellisia puolia, eli minkälaista liiketoimintaa sen ympärille on muodostunut ja minkälainen sen suhde on fiat-rahaan. Tutkimuksesta on tarkoitus saada selville myös käyttäjien suhde Bitcoinin talouteen sekä heidän syynsä Bitcoinin käyttämiseen.

4.1 Tutkimuksen tavoitteet

Koetan tutkimuksessani saada selvitettyä nämä kaksi tutkimusongelmaa, joissa on vielä tarkentavia pohdintoja:

1.) Miten Bitcoin vaikuttaa sen käyttäjän elämässä?
   - Mikä on käyttäjien syy Bitcoinin käyttämiseen?
   - Mitä mieltä käyttäjät ovat Bitcoin-verkon perustoiminnasta?
   - Miten eri tavoin käyttäjät hyödyntävät Bitcoin-verkkoa?
   - Pystyvätkö käyttäjät luottamaan Bitcoinin tietoturvaan?

2.) Miten Bitcoinia hyödynnetään talouden puolella?
   - Minkälaista liiketoimintaa Bitcoinin ympärille on muodostunut?
   - Miten Bitcoinia hyödynnetään valuuttana?
   - Onko bitcoineja mahdollista käyttää jotenkin fiat-rahan rinnalla, vai onko Bitcoinin talous enemmän sisäänpäin kääntynyttä?

4.2 Tutkimusmenetelmät

Bitcoinista löytyy paljon hajallaan olevaa tietoa internetistä, mutta melko vähän tieteellisiä julkaisuja, eikä tietääkseni yhtään kirjaa. Koska Bitcoin on vielä uusi ilmiö, niin sen käyttäjien mielipiteet ovat tutkimuksessa tärkeitä. Tarkoitus on ensin koostaa lähteitä hyödyntäen tietoa siitä, mikä Bitcoin on, miten sen eri prosessit toimivat ja miten sitä voisi verrata yleisesti käytössä olevaan fiat-rahaan. Tätä teoriataustaa hyödynnetään sitten tutkimusongelmiin yleistasolla sen verran kuin se on mahdollista. Jäljelle jäävät

tutkimusongelmat selvitetään syvällisemmin ja yksityiskohtaisemmin kvalitatiivisella kyselyllä Bitcoinin käyttäjille. Kysely on kvalitatiivinen, koska sen kohderyhmä on tarkoin rajattu pelkkiin Bitcoinin käyttäjiin, joka oletusarvoisesti on siltä osin homogeeninen ryhmä, että se kertoo oman yhtenäisen näkökulmansa tutkittavasta aiheesta. Kvalitatiivisen luonteensa vuoksi yksittäisen vastaajan sanaa pidetään painoarvoltaan tärkeämpänä kuin kvantitatiivisessa tutkimuksessa.

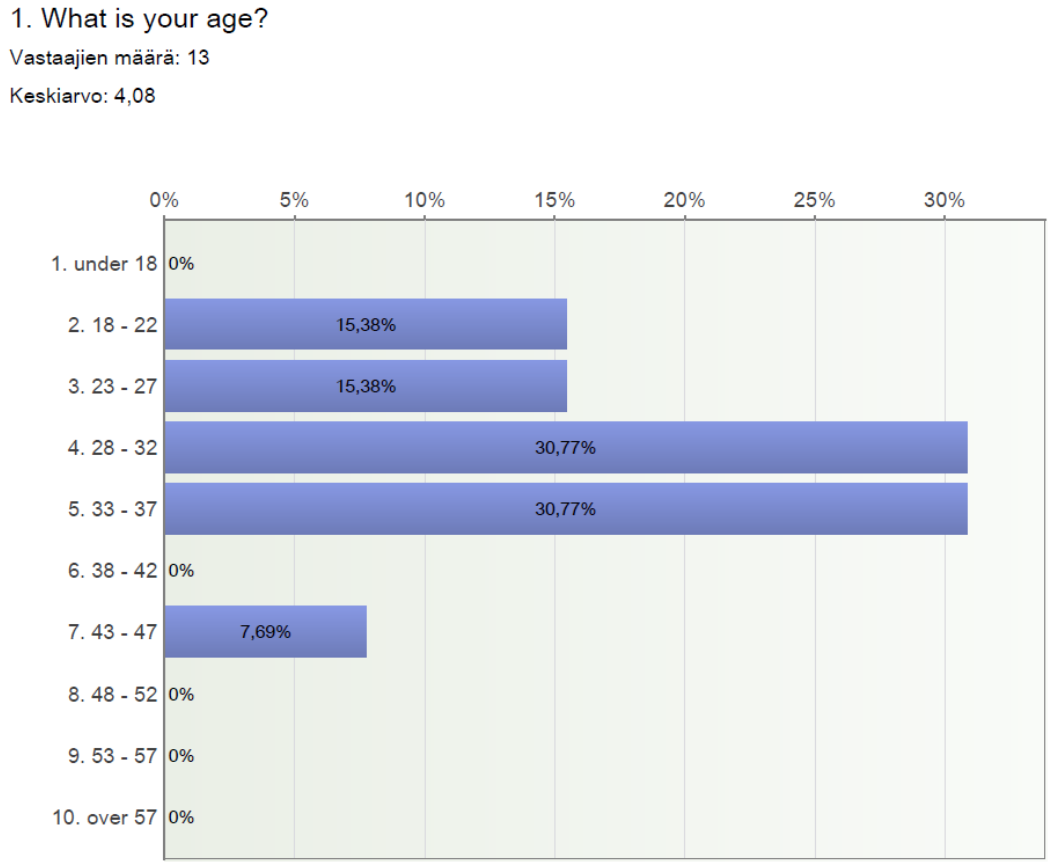
5 Tutkimuksen tulokset

Hain kvalitatiiviseen kyselyyn vastaajia kansainväliseltä bitcointalk.org-keskustelufoorumilta, koska se on yksi suurimmista ja tunnetuimmista Bitcoiniin liittyvistä foorumeista. Tutkimusalustana käytin Webropol -internet-sovellusta, koska se sisältää valmiiksi kaikki tarvittavat työkalut vastausten keräämisestä analyysiin asti. Teknisesti kysely toteutettiin lähettämällä jokaiselle vapaaehtoiselle henkilökohtainen, kyselyyn johtanut linkki sähköpostiin, jonka avaamalla ja kyselyn loppuun suorittamalla näin, ketkä kaikki ovat vastanneet kyselyyn.

5.1 Kvalitatiivinen kysely

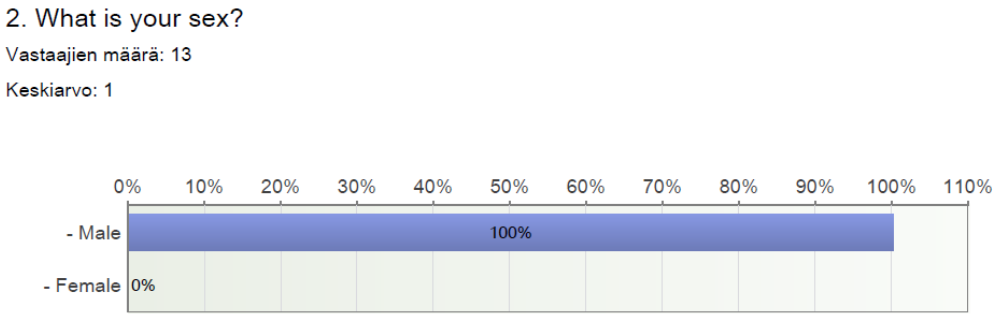
Avasin kyselyn 23.12.2012 ja suljin sen 29.3.2013. Vapaaehtoisia ehti tässä ajassa kertyä 15, joista kyselyyn vastasi 13 henkilöä. Kyselyssä oli 15-20 kysymystä, koska osa kysymyksistä toi tietyllä tavalla vastattaessa esiin lisäkysymyksen tai -kysymyksiä. Kysyjän oli pakko vastata jokaiseen hänelle esitettyyn kysymykseen. Joitakin vastauksia pystyi täydentämään sen viereen sijoitetun kommentti-kentän avulla. Tämän lisäksi kysymykset oli jaoteltu moneen eri sivuun kysymysten aiheiden mukaisesti. Jokaisen, paitsi ensimmäisen kysymyssivun lopussa, oli tekstikenttä sivun kysymyksiin kommentoimista varten. Käyn tässä luvussa läpi kyselyn tuloksia. Yksityisyyden vuoksi en julkaise kyselyn avoimia vastauksia tutkimuksessa suoraan, vaan kerron niistä omin sanoin, jos on tarpeen.

Kyselyyn vastanneiden ikäjakauma oli aika pitkälti sitä, mitä voisi odottaakin Bitcoinin kaltaiselta projektilta. 62 %, suurin osa vastaajista, oli 28-37-vuotiaita. Toisena tulivat 18-27-vuotiaat, joita oli 31 %. Yksi vastaaja, eli 8 % vastaajista, kuului 43-47-vuotiaiden ikäjoukkoon.



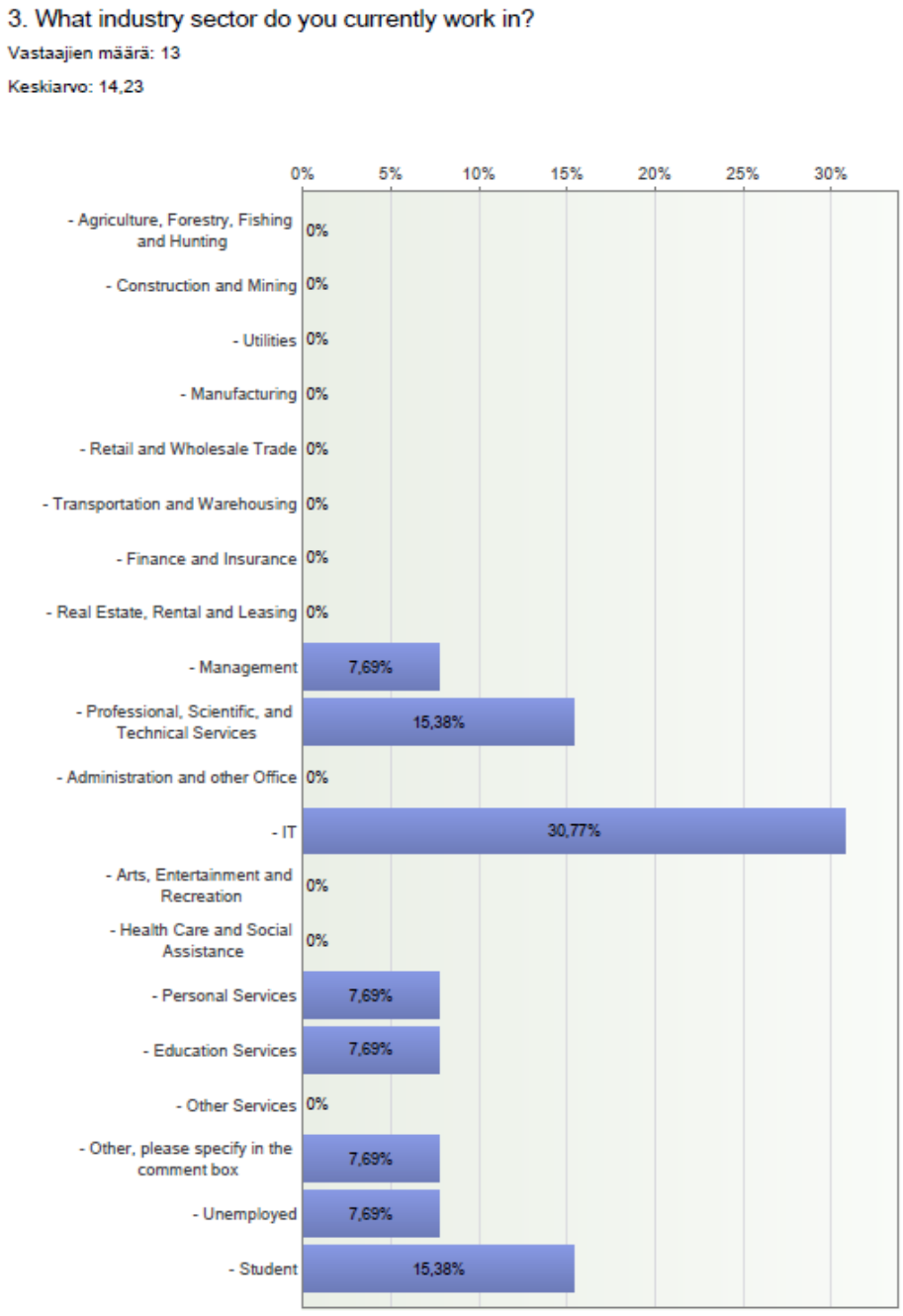
Kuva 10. Vastaajien ikä

Sukupuolijakauma oli selkeä: 100 % vastaajista oli miehiä. Tämä vastaa mielestäni sitä todellisuutta, johon olen Bitcoin-yhteisössä törmännyt; naiset eivät vaikuta ainakaan toistaiseksi olevan lähellekään yhtä kiinnostuneita projektista kuin miehet.



Kuva 11. Vastaajien sukupuoli

Noin kolmasosa vastaajista, 31 %, tekee töitä IT-alalla. Toisen sijan jakavat opiskelijat ja ammattilais-, tieteellisten ja teknisten palvelualojen työntekijät 15 % osuuksillaan. 8 %, eli yksi kappale kutakin vastaajaa tekee töitä johdon, palvelualan ja opiskelualan töitä. Viimeisestä kahdesta vastaajasta toinen on työtön ja toinen aktivisti. Vastaukset osoittavat sen, että kyselyä luettaessa tulee ottaa huomioon, että kyselyn vastaajat edustavat enimmäkseen vähintään 2. asteen koulutuksen käyneitä henkilöitä. Avoimista vastauksista kävi ilmi, että yksi vastaaja suorittaa tällä hetkellä insinöörin tohtorin arvoon johtavaa tutkintoa, ja että eräs toinen vastaaja on kokenut sovelluskehittäjä.



Kuva 12. Vastaajien toimiala

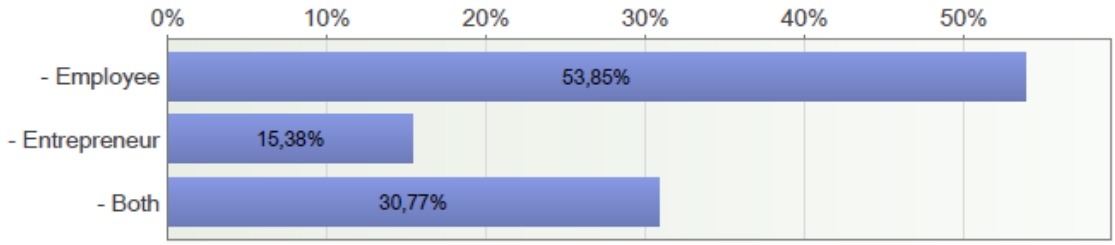
54 %, eli yli puolet vastaajista, ovat työntekijöitä. 31 % sanoi olevansa sekä työntekijä että työnantaja. Vain 15 % vastaajista sanoi olevansa yksinään työnantaja. Jos vastaaja kertoi olevansa työntekijä, niin 5. kysymys jätettiin väliin.

4. Are you an employee or an entrepreneur?

If Employee, the next question will be skipped.

Vastaajien määrä: 13

Keskiarvo: 1,77



Kuva 13. Työntekijä vai yrittäjä

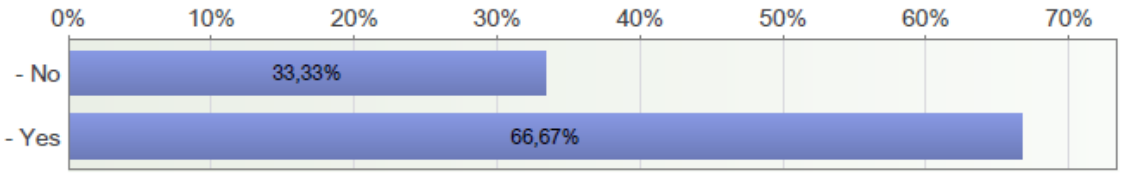
Viides kysymys esitettiin vain niille, jotka vastasivat edellisessä kysymyksessä olevansa yrittäjiä tai yrittäjiä ja työntekijöitä. Tasan kaksi kolmasosaa vastasi Bitcoinin liittyvän heidän liiketoimintaansa. Avoimista vastauksista kävi selkeästi ilmi, että bitcoinit käyvät usealla yrittäjällä joko vaihtoehtoisena maksutapana, tai sitten ne tulevat käymään maksutapana tulevaisuudessa. Kysymyssivun lopun vapaaehtoisissa kommenteissa yksi vastaaja mielsi Bitcoinin voivan mahdollisesti toimivan siirtymäteknologiana pois ”viallisesta järjestelmästä, joka perustuu väärään auktoriteettiin”.

5. If an entrepreneur, does Bitcoin involve your business?

If Yes, please specify your answer (not necessary but recommended):

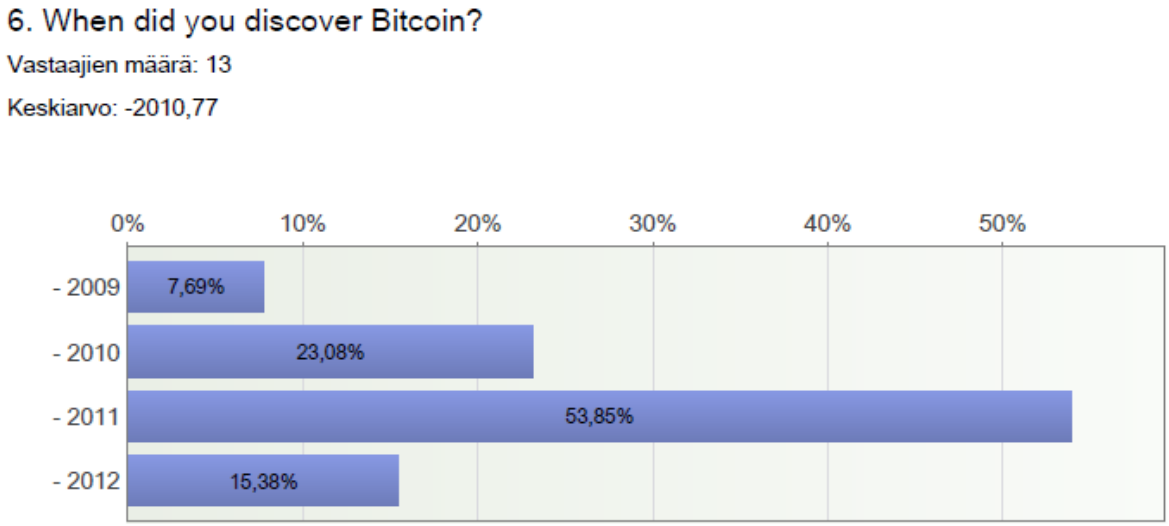
Vastaajien määrä: 6

Keskiarvo: 1,67



Kuva 14. Bitcoin ja yrittäjyys

Yli puolet vastaajista kuuli Bitcoinista ensimmäisen kerran vuonna 2011, kuten itsellänikin kävi. Toiseksi eniten kuultiin vuonna 2010 ja kolmanneksi vuonna 2012. Vain yksi vastaaja oli löytänyt Bitcoinin sen aloitusvuotena, vuonna 2009.

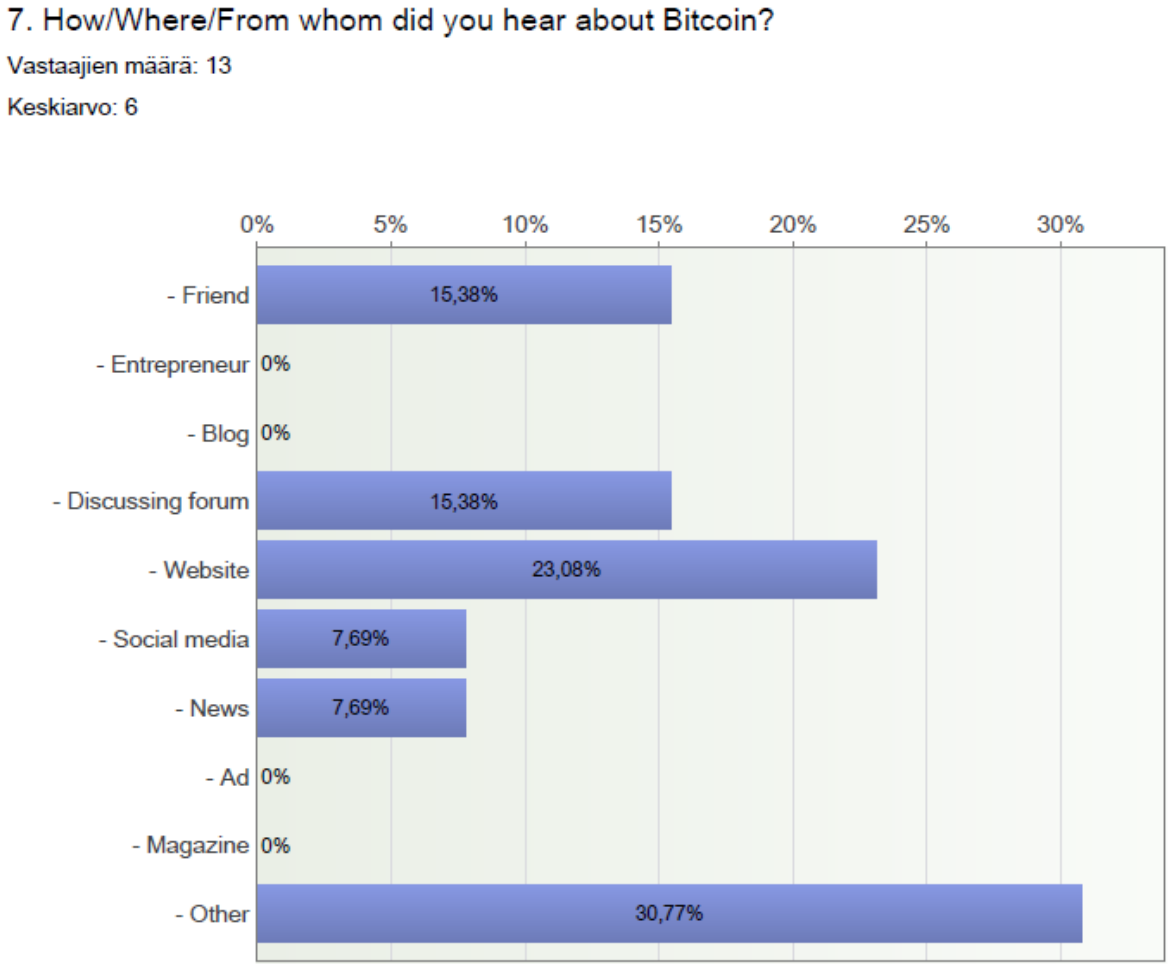


Kuva 15. Bitcoinin löytövuosi

Seitsemännessä kysymyksessä selvitettiin, mistä vastaajat olivat ensimmäisen kerran kuulleet Bitcoinista. Eniten, 31 %, vastasi ”Other”, eli ”Muu”, jonka vuoksi poikkeuksellisesti julkaisen ”Other”-kohdan avoimet vastaukset tässä suoraan ja sellaisenaan:

- Max Keiser Report
- Hidden wiki on tor
- Security Now Podcast
- debates in the open source developers scene

Toiseksi eniten Bitcoiniin oli tutustuttu sellaisten internet-sivujen kautta, joita ei voida luokitella muiden vastausvaihtoehtojen mukaan. Kolmanneksi eniten vastaajat kuulivat Bitcoinista joko kaverin tai keskutelufoorumin kautta. Sosiaalinen media ja uutiset jäivät häntäpäähän, vain yksi vastaaja oli valinnut jommankumman. Kukaan ei ollut kuullut Bitcoinista yrittäjän, blogin, mainoksen tai lehden kautta.



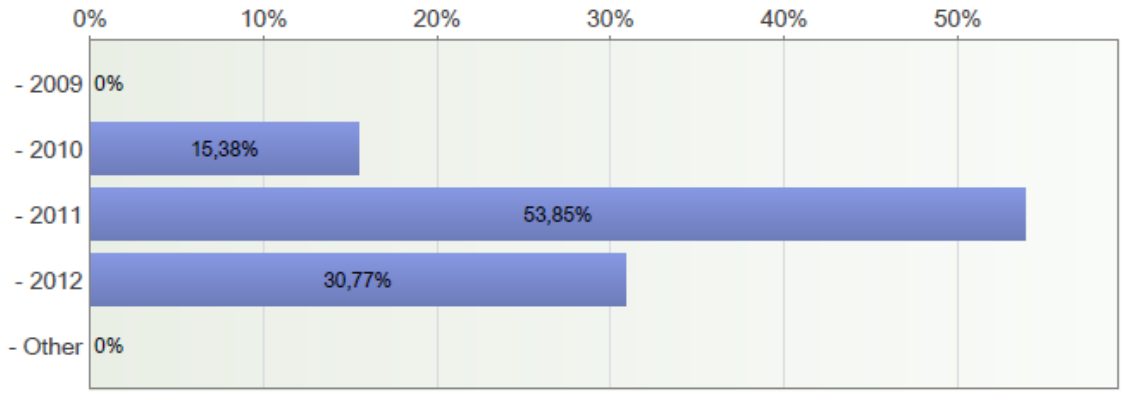
Kuva 16. Mitä kautta Bitcoiniin tutustuttiin

Kahdeksas kysymys oli melko samanlainen kuin kuudes. Sen tarkoituksena oli selvittää, ovatko vastaajat aloittaneet Bitcoinin käytön samana vuonna kuin milloin he olivat löytäneet sen. Sama määrä, 54 %, oli vastannut kumpaankin kysymykseen ”2011”, eli suurin osa aloitti käyttämisen samana vuonna, tilastollisesti. Tilastollisesti vain pieni osa, 15 %, näyttäisi alkaneen käytön myöhemmin kuin löytövuonna. Tämä näkyy siinä, että vaikka vain 15 % vastaajista löysi Bitcoinin vuonna 2012, niin kuitenkin 31 % aloitti käytön samana vuonna. Toisin sanoen, pari vastaajaa on aloittanut käytön myöhemmin kuin löytövuonna, toisin kuin suurin osa.

8. When did you start using Bitcoin?

Vastaajien määrä: 13

Keskiarvo: 3,15



Kuva 17. Bitcoinin käytön aloitusvuosi

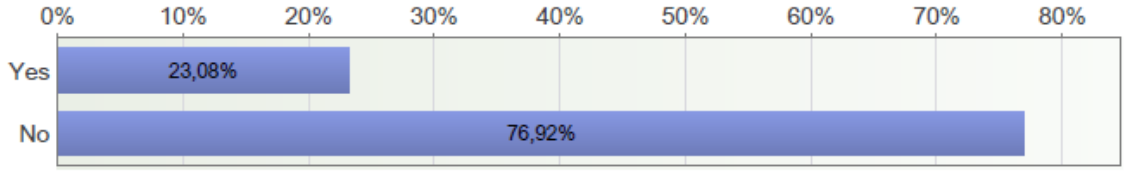
Seuraavassa kysymyksessä kävi ilmi, että 77 % vastaajista ei ole Bitcoinin lisäksi käyttänyt mitään muuta elektronista/digitaalista rahajärjestelmää. Jos kysmykseen vastasi ”No”, niin seuraava kysymys ohitettiin automaattisesti.

9. Have you used any other digital money system(s) than Bitcoin?

If No, the next question will be skipped.

Vastaajien määrä: 13

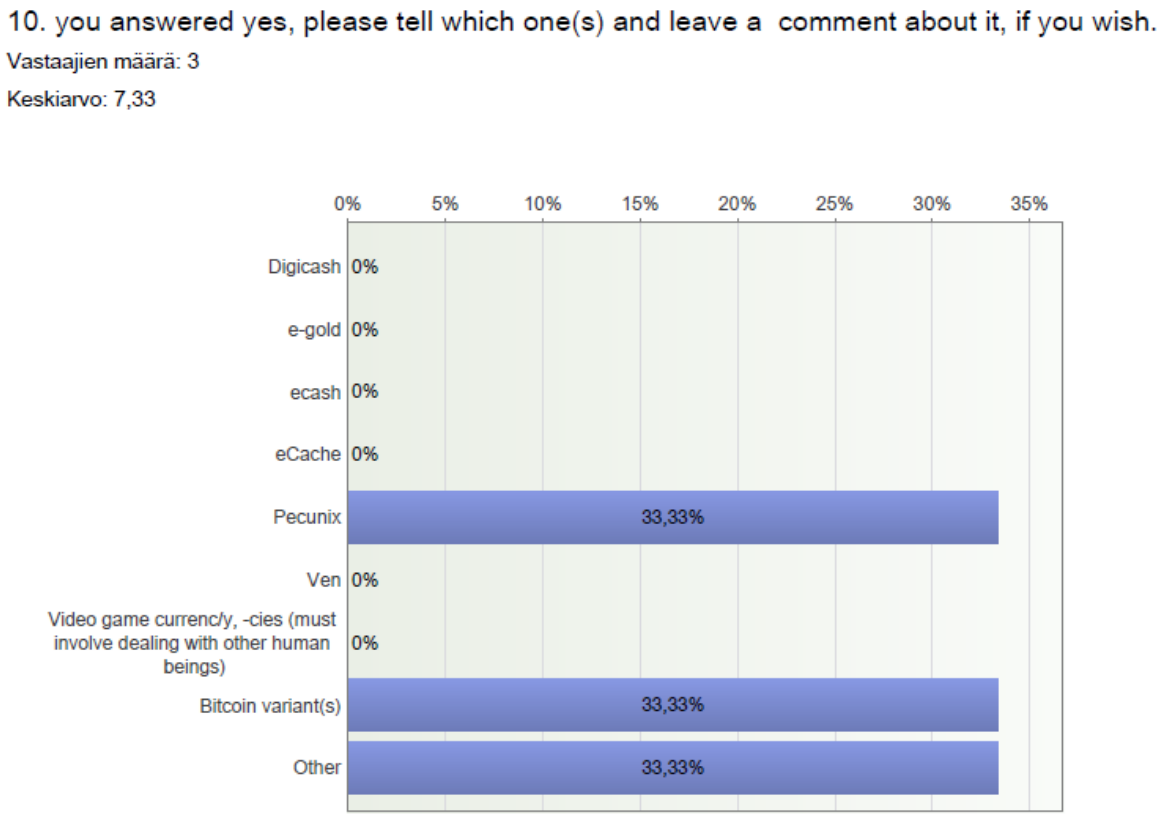
Keskiarvo: 1,77



Kuva 18. Muiden digitaalisten/elektronisten rahajärjestelmien käyttö

Kymmenenteen kysymykseen vastasi vain kolme vastaajaa, sillä loput eivät olleet käyttäneet muita elektronisia/digitaalisia rahajärjestelmiä Bitcoinin lisäksi. Jokainen näistä kolmesta vastaajasta oli käyttänyt eri rahajärjestelmiä: Pecunix, Bitcoin-variaatiot ja ”Muu” oli vastattu kyselyyn. ”Muu”-vaihtoehtoa oli tarkennettu Paypalilla ja Moneybookersilla, jotka kummatkin ovat yrityksiä, jotka välittävät maksuja internetin välityksellä, käyttäen vaihdannan välineenä fiat-rahaa. Pecunix on digitaalinen, internetin

välityksellä toimiva valuutta, jonka arvon perustana käytetään kultaa, jonka yritys omistaa (Pecunix Inc 2001-2013).



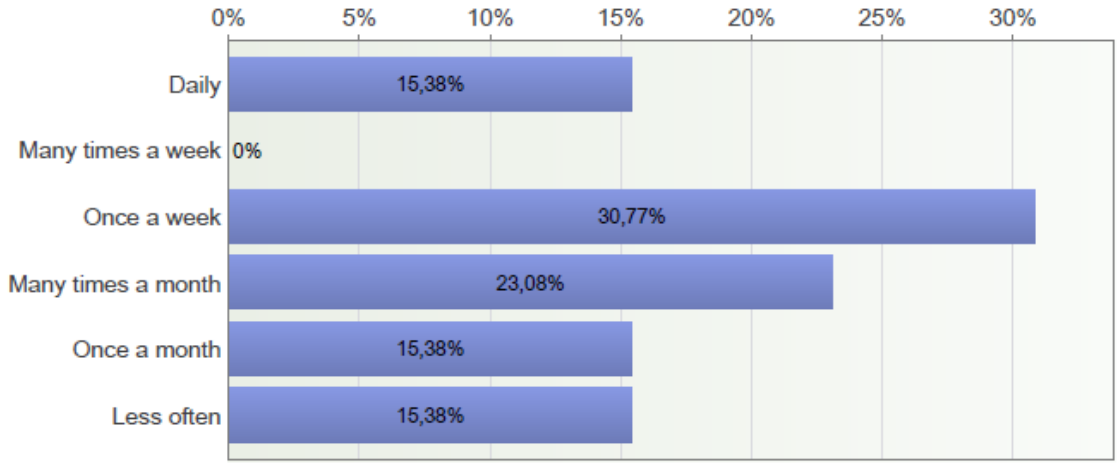
Kuva 19. Vastaajien käyttämät digitaaliset/elektroniset rahajärjestelmät

Kyselyssä kysyttiin tietenkin myös, kuinka usein sen käyttäjät käyttävät Bitcoinia keskimäärin, pois lukien louhinta. Eniten, 31 %, vastasi käyttävänsä sitä kerran viikossa. Seuraavaksi eniten, 23 %, vastasi käyttävänsä Bitcoinia monta kertaa kuukaudessa. Yhtä suurella 15 % osuudella oli vastattu kolmeen viimeiseen vaihtoehtoon, ”päivittäin”, ”kerran kuukaudessa” ja ”harvemmin”. Kukaan ei vastannut ”monta kertaa viikossa”.

11. How often do you use Bitcoin (mining doesn't count)?

Vastaajien määrä: 13

Keskiarvo: 3,69



Kuva 20. Bitcoinin käytön määrä

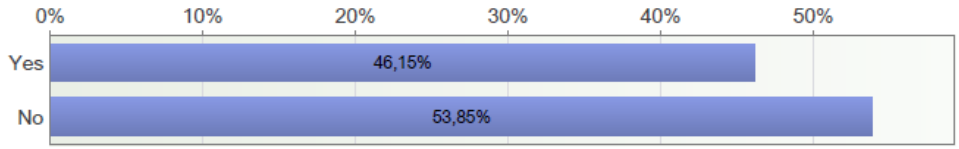
12. kysymyksessä selvitettiin, louhivatko vastaajat bitcoineja vai eivät. Vastaukset menivät aika tasan, sillä 54 % vastasi, ettei louhi ja 46 % vastasi, että louhii. Jos osallistuja vastasi kielteisesti, ei hän joutunut vastaamaan kolmeen seuraavaan kysymykseen.

12. Do you mine bitcoins?

If No, the next three questions will be skipped. Keep in mind that even if you have somehow outsourced your mining, it is considered that you ARE mining bitcoins. Buying bitcoins from an exchange service etc. is not counted as mining.

Vastaajien määrä: 13

Keskiarvo: 1,54



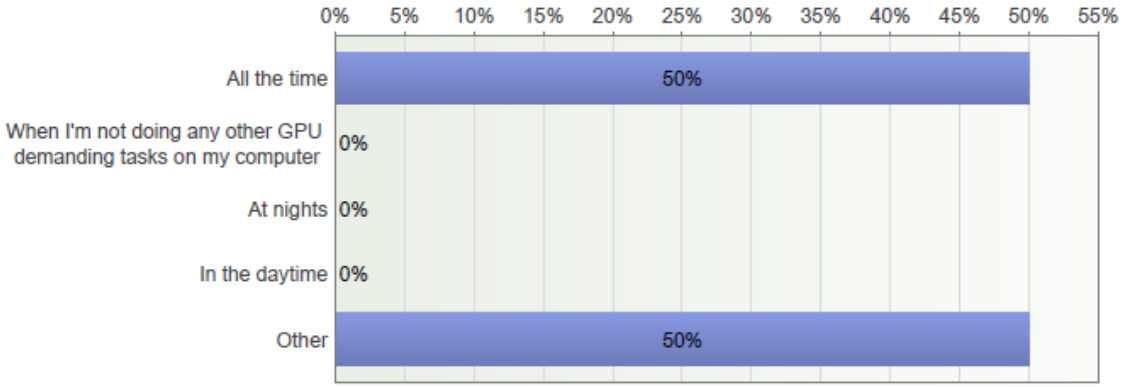
Kuva 21. Louhitaanko bitcoineja vai ei

Louhintaosion ensimmäisessä kysymyksessä 50 % vastasi louhivansa koko ajan ja 50 % vastasi ”Other”, eli jotain muuta. Näistä ”Other” vastanneista yksi vastasi, että koska 2013 vaiheilla tapahtui louhimispalkkion puolittuminen, loppui kiinnostus louhintaan. Toinen vastasi, että louhii melko harvoin.

13. If you answered yes to the previous question, how often do you mine?

Vastaajien määrä: 6

Keskiarvo: 3



Kuva 22. Kuinka usein vastaajat louhivat

Seuraavassa louhintaosion kysymyksessä kysyttiin, minkälaista louhimisalustaa vastaajat käyttivät. Vaihtoehtoina oli CPU (prosessori), GPU (näytönohjain), FPGA-mikropiiri ja Combination (yhdistelmä). 50 %, 3 vastaajaa, vastasi ”yhdistelmä”, jota he tarkensivat seuraavanlaisesti:

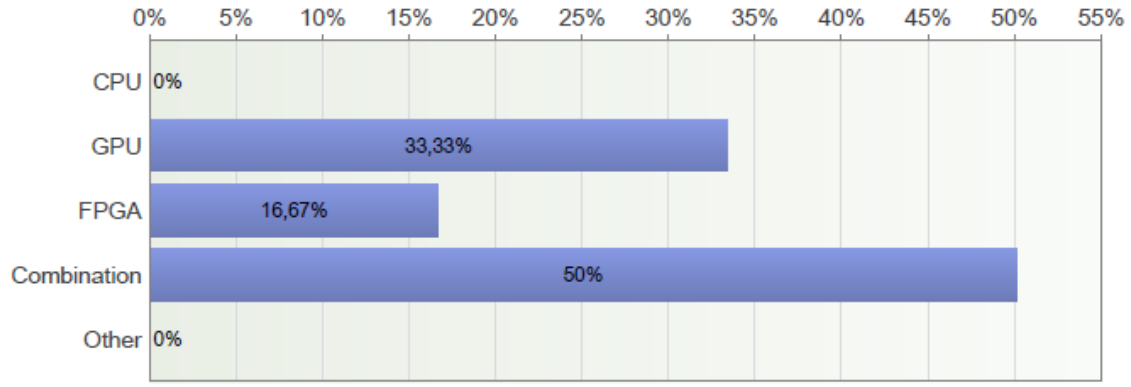
- GPUs and FPGAs
- CPU, GPU
- GPU and FPGA

Tasan kolmasosa kysymykseen vastanneista vastasi käyttävänsä pelkästään näytönohjainta ja kuudesosa FPGA-mikropiiriä. Kaikki vastaukset yhteenlaskettuna näytönohjainta käytti 4, FPGA-mikropiiriä 3 ja prosessoria 1 vastaaja. Näytönohjain oli hieman FPGA-mikropiiriä suositumpi, mutta ainoastaan yksi vastaaja hyödynsi louhinnassa prosessoria, mutta ei yksin, vaan näytönohjaimen kanssa.

14. What mining hardware do you use?

Vastaajien määrä: 6

Keskiarvo: 3,17



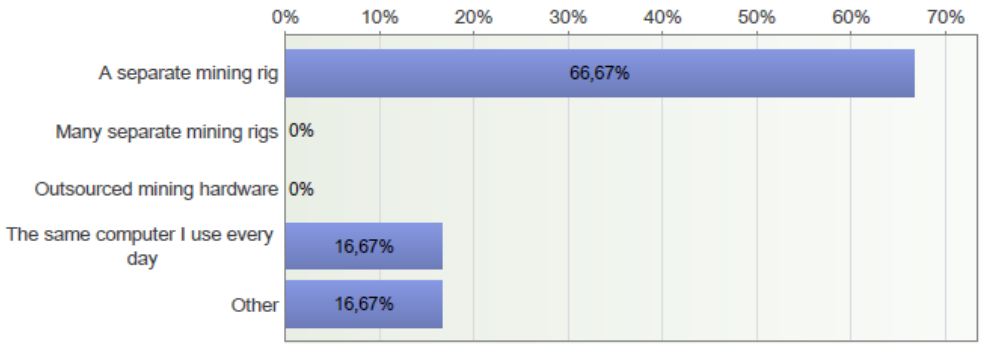
Kuva 23. Eri louhimisalustojen käyttöaste

Viimeisessä louhintaan liittyvässä kysymyksessä kysyttiin, miten paljon vastaajat ovat sijoittaneet louhimiseen. Vastaajilta kysyttiin, käyttävätkö he louhimiseen erillistä louhimiseen tarkoitettua konetta tai koneita, vai samaa konetta, jota he käyttävät päivittäin. 67 % vastasi käyttävänsä erillistä louhintakonetta, ja vain 17 %, eli yksi vastaaja sanoi käyttävänsä pelkästään tietokonetta, jota hän käyttää päivittäin. Yksi vastaaja valitsi ”Other”-vaihtoehdon ja sanoi käyttävänsä montaa erillistä louhintakonetta koko ajan ja päivittäin käyttämäänsä tietokonetta louhimiseen silloin, jos hän oli tietokoneella.

15. Do you have separate mining rig(s) or do you mine with the same computer you use every day?

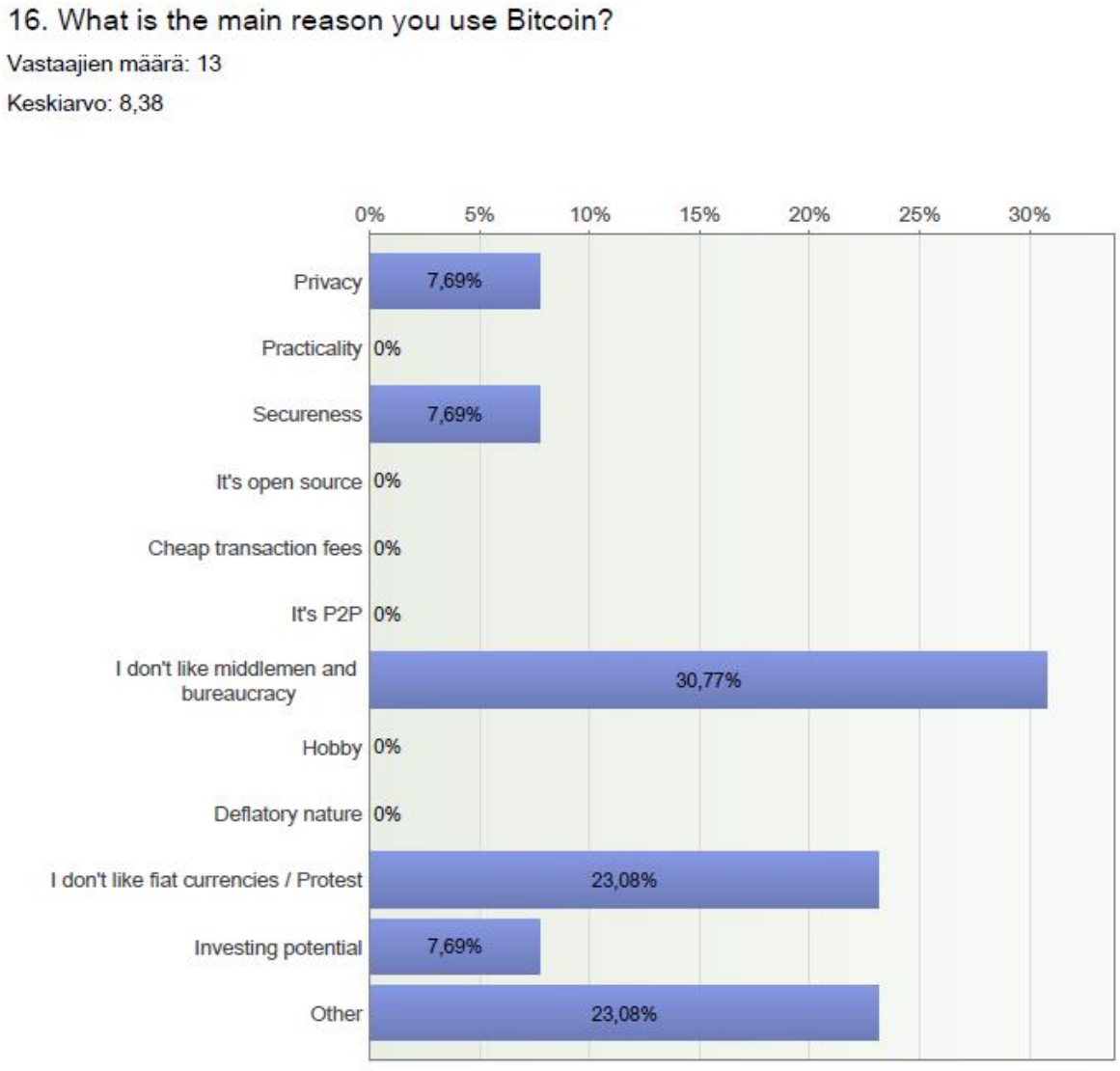
Vastaajien määrä: 6

Keskiarvo: 2,17



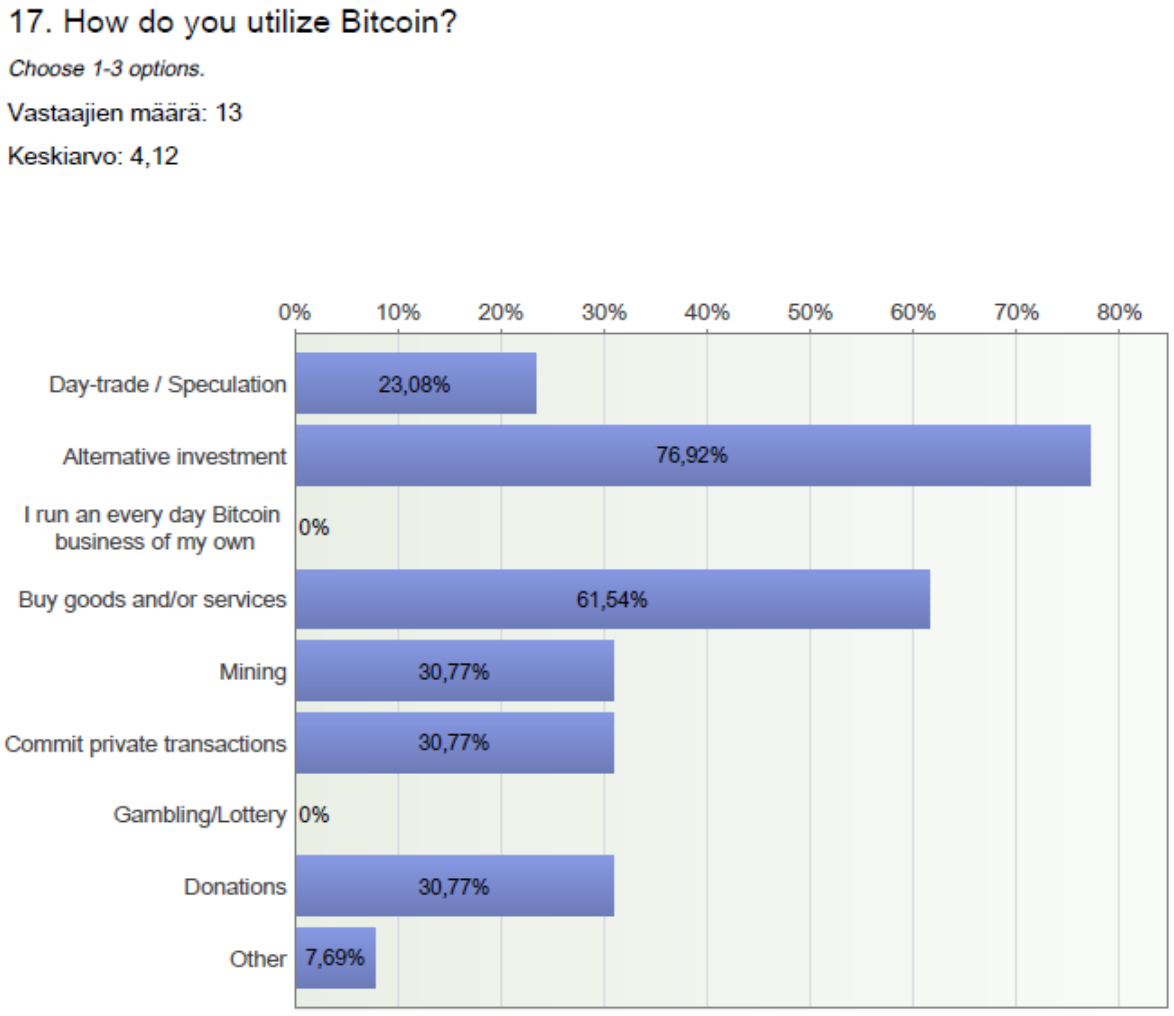
Kuva 24. Millä vastaajat louhivat

Kaksi seuraavaa kysymystä liittyivät Bitcoinin käyttäjien mielipiteisiin ja syihin käyttää Bitcoinia. 16. kysymyksessä vastaajilta kysyttiin, mikä heidän pääasiallinen syynsä oli käyttää Bitcoinia. Melkein kolmasosa, 31 % vastasi, ettei pidä byrokratiasta ja välikäsistä. 23 % käytti Bitcoinia protestoidakseen fiat-rahaa vastaan, ja saman verran vastasi ”Other”, jossa vastauksen sai määritellä itse. ”Sotien vastustus”, ”kaikki yllä olevat vaihtoehdot” ja ”kiinnostus vaihtoehtoisiin taloussektorin organisaatiomalleihin” kuuluivat näihin määritelmiin. Yhden vastauksen ääniä saivat yksityisyys, turvallisuus ja sijoituspotentiaali 8 % osuuksillaan.



Kuva 25. Pääsyy Bitcoinin käyttämiseen

Seuraavassa kysymyksessä vastaajat saivat valita 1-3 vastausta siitä, miten he hyödyntävät Bitcoinia. Reilusti suosituin vastaus, 77 %, oli käyttää sitä vaihtoehtoisena sijoituskohteena. Toisena, 62 % osuudellaan, oli käyttää sitä hyödykkeiden ja palveluiden ostamiseen. Kolmanneksi suosituin vastaus oli jaetuilla 31 % osuuksillaan louhinta, yksityisten transaktioiden suoritus ja lahjoitukset. Päivittäiseen sijoittamiseen ja muuhun toimintaan eivät vastaajat juurikaan Bitcoinia käyttäneet.



Kuva 26. Bitcoinin käyttötavat

Kyselyn kolmessa viimeisessä kysymyksessä selvitettiin asteikolla 1-5, mitä mieltä vastaajat olivat Bitcoinin eri ominaisuuksista. 1 tarkoitti heikkoa ja 5 erinomaista. Näistä ensimmäisessä kysyttiin, miten helppona ja/tai kätevänä vastaajat pitivät bitcoinien käyttämistä fiat-rahan tapaan ja esimerkiksi bitcoinien vaihtamista fiat-rahaan ja toisin päin. Erittäin kätevänä tai epäkätevänä tätä valuuttaa pitivät vain kaksi ihmistä, eli ääripäitä ei hirveästi esiintynyt. Melkein puolet vastaajista, 46 %, vastasi 4. Kuitenkin, 23 %

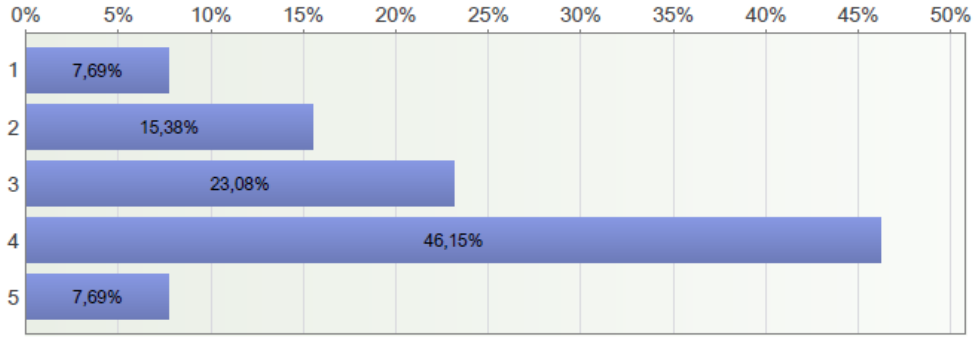
vastasi 3 ja 15 % vastasi 2, keskiarvon jäädessä 3,31:een, joten on melko selvää, että vastaajat pitivät valuuttaa kätevänä käyttää, mutta parantamisen varaa voisi kuitenkin olla.

18. How easy/convenient do you think it's to use bitcoins beside fiat currencies, i.e. to exchange them to fiat currencies and vice versa, use them like fiat currencies etc.?

Very inconvenient 1 | 2 | 3 | 4 | 5 Very convenient

Vastaajien määrä: 13

Keskiarvo: 3,31



Kuva 27. Käyttämisen kätevyys

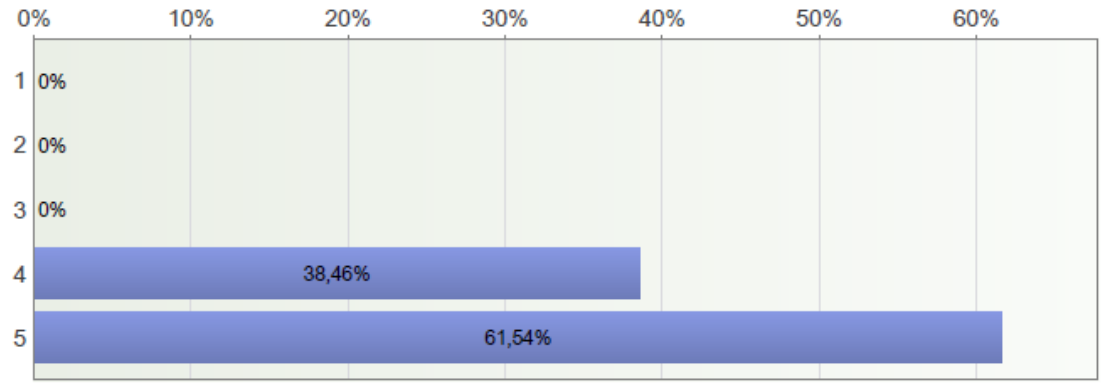
19. kysymyksessä kysyttiin, miten hyvänä vastaajat pitävät Bitcoin-verkon perustoimintaa. Vastaus oli melko yksiselitteinen, koska 62 % piti perustoimintaa erinomaisena ja 39 % kiitettävänä. Kukaan ei antanut arvosanaa 1-3, epäluottamusta ei ollut.

19. How do you rate the basic functionality of the Bitcoin network in the scale of 1-5?

Very poor 1 | 2 | 3 | 4 | 5 Very good

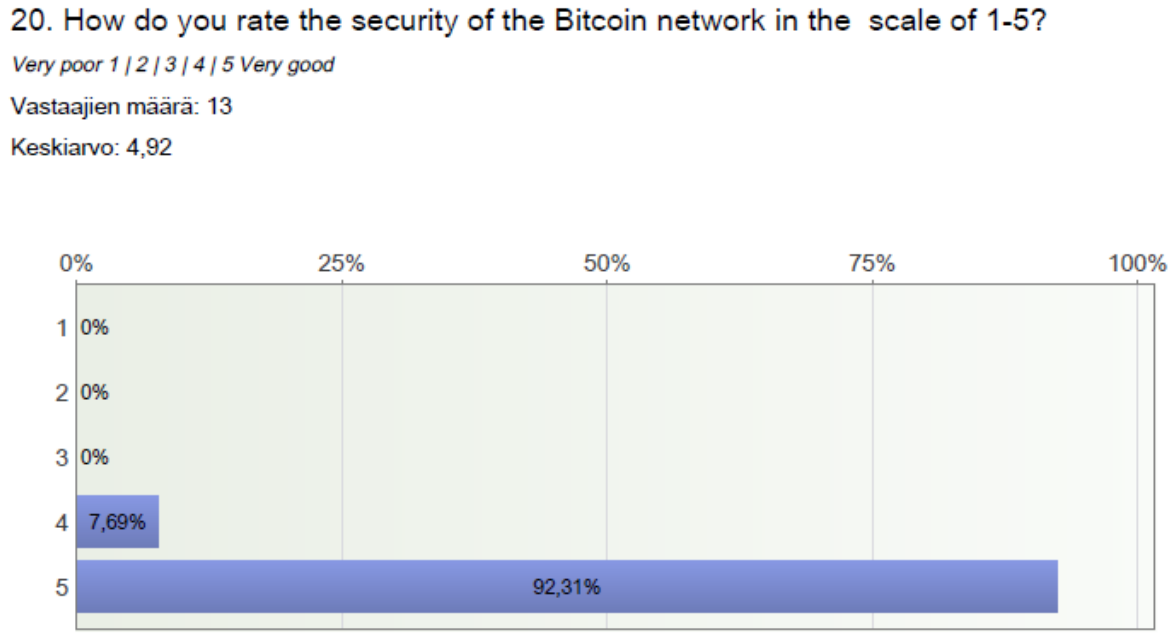
Vastaajien määrä: 13

Keskiarvo: 4,62



Kuva 28. Bitcoin-verkon perustoiminnan arvostelu

Kyselyn viimeisessä kysymyksessä kysyttiin, mitä mieltä vastaajat olivat Bitcoin-verkon tietoturvan tasosta. Vastaus oli vielä yksiselitteisempi kuin edellisessä kysymyksessä: 92 %, eli lähes kaikki vastaajat pitivät tietoturvan tasoa erinomaisena. Vain yksi vastaaja piti tietoturvaa kiitettävänä, eli vain hieman erinomaista huonompana. Yksi vastaaja myös hieman täydensi vastaustansa mainitsemalla, että pitää 51 % hyökkäystä ainoana heikkoutena.



Kuva 29. Mielipiteet Bitcoinin tietoturvan tasosta

6 Johtopäätökset

Suorittamani kysely Bitcoinista paljasti vastaajista sen, että suuri osa heistä on nuoria ja hyvin kouluttautuneita mieshenkilöitä. Melkein kolmasosa vastaajista työskentelee IT-alalla, joka kuulostaa luontaiselta henkilöltä, joka on kiinnostunut bittirahasta. Moni vastaaja työskentelee myös muilla erikoisammattitaitoa vaativalla alalla, tai on opiskelemassa itselleen ammattia. Kukaan vastaajista ei kuitenkaan vaikuttaisi työskentelevän perinteisemmissä työpaikoissa, esimerkiksi kaupan, logistiikan, tuotannon tai terveydenhoidon puolella. Tämän valossa vaikuttaisi siltä, että käyttäjät ovat keskimääräistä koulutetumpia ja enemmänkin miesvaltaisilla, teknisillä aloilla työskenteleviä henkilöitä.

Yli puolet kyselyyn vastanneista henkilöistä sanoivat olevansa työntekijöitä, mutta myös lähes puolet vastanneista sanoi olevansa joko yrittäjiä tai yrittäjiä sekä työntekijöitä. Kaksi kolmasosaa näistä vastaajista sanoi Bitcoinin liittyvän heidän liiketoimintaansa, ja vielä tarkennettuna, moni sanoi, että he hyväksyvät myös bitcoinit maksun välineenä, tai sitten ovat ottamassa bitcoinit mukaan tulevaisuudessa perinteisen valuutan rinnalle maksamisen yhteydessä. Tutkimuksessa kävi siis ilmi, että bitcoineja on mahdollista käyttää ostojen maksamiseen normaalisti, jos vain kauppias hyväksyy niillä maksamisen ja varautuu tähän hieman teknisesti. On vain ajan kysymys nähdä, tuleeko bitcoineilla maksamisen mahdollisuus yleistymään vai ei.

Tutkimuksen kyselyssä kävi toteen suurella todennäköisyydellä, että yli puolet kyselyyn vastanneista henkilöistä löysi Bitcoinin vuonna 2011 ja alkoi myös käyttää sitä samana vuonna. Yli puolet sanoi myös käyttävänsä Bitcoinia kerran viikossa tai monta kertaa kuukaudessa, joten käyttökokemusta ja käytännön testaamista vastaajille on ehtinyt kertyä paljon ennen heille teetettyä kyselyä. Kokemus huomioon ottaen voidaan varmuudella olla vakuuttuneita Bitcoin-verkon perustoiminnan ja tietoturvan puolesta, koska kaikki vastaajat pitivät kummankin tasoa joko kiitettävänä tai erinomaisena.

Kysely osoitti vastaajista myös sen, etteivät he vaikuttaneet olevan puolueellisia elektronista rahaa kohtaan, sillä yli kolme neljäsosaa vastaajista ei ollut käyttänyt Bitcoinin lisäksi mitään muuta vastaavanlaista valuuttaa. Heillä, jotka olivat käyttäneet, oli lähin Bitcoinia vastaava valuutta jokin sen varianteista ja Pecunix, elektroninen raha, joka on taattu kullalla. Loput vastasivat käyttäneensä Paypalia ja Moneybookersia, jotka välittävät normaalilla fiat-rahalla tehtyjä kauppoja elektronisesti, eivätkä siis täten edusta mitään omaa elektronista rahayksikköä. Elektronisen rahan käyttö ei siis ollut vastaajille itseisarvo tai ennakkosyy alkaa käyttää Bitcoinia.

Pääsyy Bitcoinin käyttämiseen lähes kolmasosalle vastaajista oli byrokratian ja välikäsien karsastus. Moni ei myöskään pitänyt fiat-rahasta ja piti Bitcoinin käyttöään protestina sitä vastaan. Näistä voisi vetää sen johtopäätöksen, että Bitcoinin käyttäjät ovat kyllästyneet esimerkiksi ostotapahtumissa tarvittaviin 3. osapuolen välittäjiin ynnä muuhun byrokraattiseen koneistoon, jota ei vaadita Bitcoin-verkon ylläpitoon ja sen yksityisyyttä kunnioittavien transaktioiden toteuttamiseen. Tätä johtopäätöstä tukee se

fakta, että vastaajien toiseksi suosituin käyttötapa Bitcoinille oli hyödykkeiden ja palveluiden ostaminen. Bitcoinien hyödyntäminen vaihtoehtoisena sijoituskohteena oli selkeästi suosituin käyttötapa, mutta koska vain alle neljäsosa vastasi käyvänsä bitcoineilla päiväkauppaa, eikä kukaan sanonut käyttävänsä sitä uhkapeleihin, voidaan olettaa, että suurinta osaa käyttäjistä kiinnostaa bitcoinien arvo pitkällä aikavälillä. Tähän suuntaan viittaa myös se, että päiväkauppaa suositumpaa oli bitcoinien louhinta, yksityiset transaktiot ja lahjoitukset, joista ensimmäinen on yksi Bitcoinin perustoiminnoista ja loput perustuvat perustoimintojen hyödyntämiseen ilman tarpeettomia välikäsiä. Toisaalta, moni ei pitänyt bitcoinien louhimiseen vaadittavan sähkön ja sitä kautta rahan kuluttamisesta, eikä siitä, että vuoden 2013 tienoilla louhimisesta saatu palkkio puolittui. Muun muuassa tämä on syynä sille, että vain puolet vastaajista sanoi louhivansa bitcoineja, ja moni odottaakin hyvin optimoitujen ASIC-piirien laajamittaista tuloa markkinoille, jotta louhimisesta tulisi kannattavampaa.

7 Yhteenveto

Teoriastaustaksi ammennetut lähdetiedot yhdessä kyselytutkimuksen kanssa paljastavat Bitcoinista monta asiaa. Yksi näistä on se lähdemateriaalista koostuva fakta, että kun perinteisillä fiat-valuutoilla tehdyissä transaktioissa maksun vastaanottaja ja pankki mahdollisesti kolmannen osapuolen kanssa huolehtivat transaktioiden turvallisuudesta, jää Bitcoinin transaktioissa vastuu maksavalle osapuolelle ja maksun vastaanottajalle: Bitcoineilla tehdyt transaktiot ovat pysyviä, eli niitä ei voi peruuttaa. Tämä johtuu järjestelmän luonteesta, jossa kaikki toteutuneet transaktiot kirjataan lopullisesti julkiseen tietokantaan, jonka jokainen Bitcoinin käyttäjä joutuu lataamaan tietokoneelleen, ennen kuin hän pystyy itse suorittamaan transaktioita. Bitcoinissa jokaista transaktiota siis turvaa itse järjestelmän yhtenäinen rakenne, kun, ainakin vielä toistaiseksi, on fiat-rahalla tehtyjen transaktioiden tietoturvan toteutus epäyhtenäistä ja tapauskohtaista. Bitcoinin tietoturvan ja perustoiminnallisuuden toimivuutta puoltaa myös kyselyyn vastanneiden henkilöiden lähes täysi niitä kohtaan osoittama luottamus.

Luottamuksen lisäksi tutkimuksessa pyrittiin selvittämään käyttäjien syytä Bitcoinin käyttämiseen ja tapaa, jolla he sitä hyödyntävät. Teoriataustasta käy ilmi, että tehdessä perinteisellä rahalla tilisiirron ulkomaille, tulee siirron yhteydessä täyttää kuusi eri koh-

taa pelkästään pankin järjestelmässä. Bitcoinin transaktiossa tarvitaan kaksi kohtaa, eli kolmasosa: Bitcoinien määrä ja vastaanottajan osoite. Tutkimus osoittaa, että juuri tämä simppeli käyttötapa viehättää käyttäjiä Bitcoinin ympärillä. Bitcoinin käyttäjät myös jollain tapaa kokevat sen automaattisen arvonsäätelymekanismin olevan puolueettomampi kuin keskuspankkien mekanismit, jotka ovat harvojen ihmisten käsissä.

Bitcoin on helppokäyttöinen ja nopea, elektroninen valuutta, joka toimii hajautetusti P2P-periaatteen mukaisesti. Käyttäjiltä löytyy suuri luottamus sen perustoimintaan ja tietoturvaan. Löytyy myös yrittäjiä, jotka vastaanottavat bitcoineja heidän myymiään hyödykkeitä vastaan, jonka lisäksi on olemassa yrittäjiä, jotka voisivat laajentaa asiakaskuntaansa ottamalla bitcoinit vaihtoehtoiseksi maksutavaksi. Bitcoinista löytyy myös ominaisuuksia, jotka saattavat jakaa ihmisten mielipiteitä:

Bitcoinin sisäänrakennettu, deflatorinen luonne takaa sen, että valuutan arvo kasvaa ajan myötä, päinvastoin kuin fiat-valuutoissa. Aikaiset käyttäjät hyötyvät tästä, kun taas tuoreet käyttäjät joutuvat maksamaan kalliimman hinnan yhdestä bittikolikosta. Toisaalta, tällä kalliimmalla kolikolla pystyy kuitenkin ostamaan enemmän hyödykkeitä. Tämä ominaisuus kannustaa ihmisiä säästämään heidän bitcoinejaan. Miten tämä vaikuttaa Bitcoinin käyttäjien kulutukseen pitkällä aikavälillä, ja onko se hyvä vai huono asia? Bitcoin on myös osittain anonyymi valuutta sen käyttäjälle, koska sen transaktiot tai muu käyttäminen ei vaadi käyttäjän nimeä eikä muita henkilötietoja. Bitcoin antaa sen käyttäjälleen yksityisyyttä, mutta vaatii käyttäjäänsä myös ottamaan täyden vastuun Bitcoinin käytöstä, eli ilman mahdollista 3. osapuolta, suojaa ei ole sille, jos bittirahat syystä tai toisesta katoavat käyttäjän Bitcoin-lompakosta, tai jos maksaa kauppiaalle, joka ei toimita luvattua hyödykettä. Edellisten lisäksi Bitcoin on täysin elektroninen valuutta, joten sitä ei löydy käteisenä. Tämä saattaa olla ongelma ihmisille, jotka ovat tottuneet pitämään rahaa aina käden ulottuvilla, ja jotka eivät ole itsevarmoja tietoteknisten laitteiden käyttämisessä, mutta ainakin väärennetyn rahan painaminen saadaan estettyä. Jos edellä mainitut asiat eivät tuota ongelmaa, ja jos bitcoinien louhinnasta saadaan tehtyä kustannustehokkaampaa, niin bitcoineilla saattaa olla tulevaisuus markkinoilla, jos yhä useampi yrittäjä ottaa myös Bitcoinin maksutavaksi.

8 Pohdinta

Opinnäytetyö Bitcoinista oli mielenkiintoinen idea ainakin parista eri syystä: Ensinnä, aloin itse harrastamaan Bitcoinin käyttämistä ja bitcoinien louhimista 2011 syksyllä. Tällöin yhden bitcoinin hinta oli vain 2-3 euron luokkaa, eikä varmaan kenelläkään ollut aavistusta siitä, että hinta tulisi vuonna 2013 pomppaamaan hetkeksi lähes 200 euron tuntumaan ja vakiintumaan lähelle sataa euroa. Toiseksi, Bitcoin jakoi jo vuonna 2011 mielipiteitä ja jakaa yhä. Kun toiset pitivät sitä pyramidihuijauksena, saattoivat toiset pitää sitä täysin keskuspankeista vapautuneena, byrokratiavapaana ja liberaalina valuuttana, josta ei löydy heikkouksia. Näin suuri vastakkainasettelu ja ylipäänsä teknologian ja liiketalouden yhdistävä aihe vaati mielestäni tutkimusta, jonka vuoksi aloin työstämään aiheesta opinnäytetyötä 2012 kesällä.

Aloittaessani opinnäytetyöni huomasin heti, ettei Bitcoinista löydy kovinkaan paljon valmista tieteellistä materiaalia, jonka vuoksi lähteinä oli pakko käyttää suurimmaksi osaksi sen omaa wiki-sivustoa. Kannatti siis hyödyntää Bitcoinista kertovaa materiaalia lähinnä sen perustoiminnan kuvaamisen yhteydessä. Siksi painotin työssä Bitcoinin vertaamista fiat-rahaan ja Bitcoin-käyttäjien kokemuksiin, koska fiat-rahasta löytyy paljon lähteitä ja kokemukset ovat näin uudessa aiheessa faktalukuja tärkeämpiä. Tutkimuksen tulokset olivat aika pitkälti sitä mitä luulin, eli käyttäjät olivat tyytyväisiä Bitcoinin tietoturvaan ja perustoimintaan. Selkeää oli myös nykyisen talouslaman yhteydessä se, että moni vastaaja käytti Bitcoinia protestina fiat-rahaa vastaan. Tutkimisosio sujui aika lailla tutkimusten tavoitteiden mukaisesti, vaikka Bitcoinin liiketoiminnallisen puolen selvitys jäi vähän vajaammaksi.

Kaiken kaikkiaan, opinnäytetyön prosessi sujui itse tekovaiheessa sopivan verkkaisesti. Itselleni oli kuitenkin hankalaa opinnäytetyön aloituksen ja lopetuksen byrokratia ja tutkimusosion aloitus kyselyineen. Koska sain oman alan työtä melkein heti opinnäytetyön aloitettuani, en pystynyt hyödyntämään aikaani sen tekemiseen enää kovin tehokkaasti, tai en ainakaan jaksanut. Kun työhön yhdisti vielä auto- ja asuntoprojektin ja säännölliset illalliset kuntosalikäynnit, piti jäljelle jäävä lyhyt aika käyttää joko lepäämiseen tai opinnäytetyön tekemiseen. Projektinhallinta kärsi tämän vuoksi, jonka takia opinnäytetyö valmistui puoli vuotta itse itselleni asetetun maksimi-deadlinen jälkeen.

Opinnäytetyö ehti ASIC-piirien tulemisen myötä kesällä 2013 jo hieman vanhentua. Positiivisiakin asioita toki löytyy: Tämä opinnäytetyö toimii mielestäni hyvänä ja helppolukuisena Bitcoinin perusselvityksenä monelle vaativammalle projektille ja ylipäänsä kaikille Bitcoinista kiinnostuneille ihmisille. Tämän lisäksi voidaan tästä opinnäytetyöstä jatkaa tutkimusta esimerkiksi aiheella, joissa selvitettäisiin, onko nykyisen sukupolven ASIC-louhintalaitteilla jotain virkaa tehokkaampien laitteiden saapumisen jälkeen, vai tuleeko niistä romurautaa. Voitaisiin myös tutkia, tuleeko louhinta olemaan enää mielekästä toimintaa, kun louhijoita tulee olemaan niin paljon, ettei bitcoineja riitä enää jaettavaksi. Vai nouseeko silloin bitcoinien arvo yhä enemmän, jotta sähkökulujen jälkeen jäädään vielä voitolle? Aiheita riittää ja uskon ja toivon, että tämä opinnäytetyö herättää kysymyksiä kaikissa sitä lukevissa ihmisissä.

Lähteet

Accounts explained. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Accounts_explained Luettu: 10.5.2012

AES-S6DEV-LX150T-G. Avnet Electronics Marketing 2012. Verkkokauppa. Luettavissa: http://avnetexpress.avnet.com/store/em/EMController/Development-Kits/Avnet-Electronics-Marketing/AES-S6DEV-LX150T-G/_/R-10548846/A-10548846/An-0?listIndex=-1&catalogId=500201&action=part&langId=-1&currency=USD&displayCurrency=EUR&updateTransactionCurrency=false&storeId=500201 Luettu: 6.6.2012

AMD Fusion11 Developer Summit: Face Detection: Performance Opportunities for CPU-GPU Kernel Migration in Fusion Architecture. AMD 2011. Esittelymateriaali. Luettavissa: developer.amd.com/afds/assets/presentations/1724_final.pdf Luettu: 17.5.2012

AMD Phenom II X6 1100T. MBnet 2011. Tuote-esittely. Luettavissa: http://www.mbnet.fi/tuotteet/tuote/prosessoripaivitys_amd_phenom_ii_x6_1100t Luettu: 6.6.2012

AMD Radeon™ HD 6450 Graphics. AMD 2012. Tuote-esittely. Luettavissa: http://www.amd.com/us/products/desktop/graphics/amd-radeon-hd-6000/hd-6450/Pages/amd-radeon-hd-6450-overview.aspx#2 Luettu: 20.5.2012

AMD Radeon™ HD 6990 Graphics. AMD 2012. Tuote-esittely. Luettavissa: http://www.amd.com/us/products/desktop/graphics/amd-radeon-hd-6000/hd-6990/Pages/amd-radeon-hd-6990-overview.aspx#3 Luettu: 20.5.2012

Anderson, R & Murdoch, S 2010. Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication. Tieteellinen julkaisu. Luettavissa: http://www.cl.cam.ac.uk/~sjm217/papers/fc10vbvsecurecode.pdf Luettu: 24.4.2012

ASIC Products. Butterfly Labs Inc. 2012. Verkkokauppa. Luettavissa: http://www.butterflylabs.com/products/ Luettu: 13.1.2013

ATI Radeon HD 5850. MBnet 2009. Tuote-esittely. Luettavissa: http://www.mbnet.fi/tuotteet/tuote/radeonin_uusi_sukupolvi_ati_radeon_hd_5850 Luettu: 6.6.2012

Block chain. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Block_chain Luettu: 12.4.2012

Comparison of mining pools. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Comparison_of_mining_pools Luettu: 9.6.2012

Confirmation. Bitcoin Wiki 2011. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Confirmation Luettu: 8.5.2012

Controlled Currency Supply. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Controlled_Currency_Supply Luettu: 14.5.2012

FAQ. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/FAQ Luettu: 30.5.2012

How Bitcoin works. Bitcoin Wiki 2011. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/How_bitcoin_works Luettu: 11.4.2012

HTML <iframe> Tag. W3Schools. Ohje. Luettavissa: http://www.w3schools.com/tags/tag_iframe.asp Luettu: 24.5.2012

Kauko, K. 2011. BoF Online 5 / 2011: Lyhyt johdatus rahaan. Suomen Pankin verkko-julkaisu. Luettavissa: http://www.suomenpankki.fi/fi/julkaisut/selvitykset_ja_raportit/bof_online/Documents/BoF_Online_05_2011.pdf Luettu: 22.5.2012

Maksu ulkomaille - valuuttamaksut. Nordea 2011. Maksuohje. Luettavissa: http://www1.nordea.fi/solo/1/help/VAL-1payments_abroad.ASP Luettu: 22.5.2012

Maxfield, Clive 2004. The Design Warrior's Guide to FPGAs: Devices, Tools and Flows, Nide 1. Elsevier. E-kirja. Luettavissa: http://books.google.fi/books?id=dnuwr2xOFpUC&pg=PA1&dq=What+are+FPGAs?&hl=fi&sa=X&ei=JTe6T7jOHKPP4QTAstjpCQ&ved=0CEsQ6AEwAg#v=onepage&q=What%20are%20FPGAs%3F&f=false Luettu: 21.5.2012

Mining hardware comparison. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Mining_hardware_comparison Luettu: 24.5.2012

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. White paper. Luettavissa: http://bitcoin.org/bitcoin.pdf. Luettu: 10.4.2012

OpenCL miner. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/OpenCL_miner Luettu: 14.6.2012

P2Pool. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/P2Pool Luettu: 10.1.2013

Parker M. & T. 2008. Electronic Banking in Finland and the Effect on Money Velocity. Tutkielma. Luettavissa: http://www.eurojournals.com/Pages from jmib 4-2_parker.pdf Luettu: 22.5.2012

Proof-of-Work. Bitcoin Wiki 2011. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Proof_of_work Luettu: 17.4.2012

Schulz, M & Woolsey, B. Credit card statistics, industry facts, debt statistics. Credit-Cards.com 2012. Tilastotietoa. Luettavissa: http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php#Circulation-issuer Luettu: 23.5.2012

Smith, M. Application-Specific Integrated Circuits. 1997. VLSI Design Series. Ote kirjasta. Luettavissa: http://iroi.seu.edu.cn/books/asics/Book2/CH01/CH01.1.htm#pgfId=1331 Luettu: 18.1.2013

Technical background of version 1 Bitcoin addresses. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Technical_background_of_Bitcoin_addresses Luettu: 8.5.2012

Tilisiirto-opas. Finanssialan Keskusliitto 2011. Ohje. Luettavissa: http://www.fkl.fi/materiaalipankki/oppaat/Dokumentit/Tilisiirto-opas_2011.pdf Luettu: 22.5.2012

Tour - what is Pecunix? Pecunix Inc 2001-2013. Tuote-esittely. Luettavissa: http://www.pecunix.com/money.cfm...tur.pecunix Luettu: 14.4.2013

Transaction fees. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Transaction_Fee Luettu: 12.6.2012

Wallet. Bitcoin Wiki 2011. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Wallet Luettu: 10.5.2012

Weaknesses. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Weaknesses Luettu: 14.6.2012

What is Pooled Mining?. BITCOINCZ Mining 2012. Luettavissa: http://mining.bitcoin.cz/ Luettu: 11.6.2012

Why a GPU mines faster than a CPU. Bitcoin Wiki 2012. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU Luettu: 21.5.2012

Why pooled mining. Bitcoin Wiki 2011. Avoin tietosanakirja. Luettavissa: https://en.bitcoin.it/wiki/Why_pooled_mining Luettu: 09.6.2012

Xouris, V. 2010. Parallel Hashing,Compression and Encryptionwith OpenCL under OS X. Maisterin tutkinto. Luettavissa: http://www.scribd.com/doc/91548770/Parallel-Hashing Luettu: 17.5.2012

Yhtenäinen euromaksualue yrityksille. Finanssialan Keskusliitto 2009. Tiedote. Luettavissa: http://www.fkl.fi/teemasivut/sepa/vaikutukset_yritystoimintaan/Dokumentit/Sepa_yrityksille.pdf Luettu: 22.5.2012

Liitteet

Liite 1. Kvalitatiivisen kyselytutkimuksen kysymykset

Personal info

Basic information about you.

1. What is your age? *

- ◯ 1. under 18
- ◯ 2. 18 - 22
- ◯ 3. 23 - 27
- ◯ 4. 28 - 32
- ◯ 5. 33 - 37
- ◯ 6. 38 - 42
- ◯ 7. 43 - 47
- ◯ 8. 48 - 52
- ◯ 9. 53 - 57
- ◯ 10. over 57

2. What is your sex? *

- ◯ - Male
- ◯ - Female

Work

Information about your employment.

3. What industry sector do you currently work in? *

- ◯ - Agriculture, Forestry, Fishing and Hunting
- ◯ - Construction and Mining
- ◯ - Utilities
- ◯ - Manufacturing
- ◯ - Retail and Wholesale Trade
- ◯ - Transportation and Warehousing
- ◯ - Finance and Insurance
- ◯ - Real Estate, Rental and Leasing
- ◯ - Management
- ◯ - Professional, Scientific, and Technical Services
- ◯ - Administration and other Office
- ◯ - IT
- ◯ - Arts, Entertainment and Recreation
- ◯ - Health Care and Social Assistance
- ◯ - Personal Services
- ◯ - Education Services
- ◯ - Other Services
- ◯ - Other, please specify in the comment box

_____

- ◯ - Unemployed
- ◯ - Student

4. Are you an employee or an entrepreneur? *

If Employee, the next question will be skipped.

- ◯ - Employee

◯ - Entrepreneur

◯ - Both

Voluntary comments about this page's questions

_____

_____

_____

Entrepreneur

Finding out more about your entrepreneurship.

5. If an entrepreneur, does Bitcoin involve your business? *

If Yes, please specify your answer (not necessary but recommended):

◯ - No

◯ - Yes

_____

Voluntary comments about this page's question

_____

_____

_____

Bitcoin and you

Your first relation to Bitcoin.

6. When did you discover Bitcoin? *

◯ - 2009
◯ - 2010
◯ - 2011
◯ - 2012

7. How/Where/From whom did you hear about Bitcoin? *

◯ - Friend
◯ - Entrepreneur
◯ - Blog
◯ - Discussing forum
◯ - Website
◯ - Social media
◯ - News
◯ - Ad
◯ - Magazine
◯ - Other

_____

8. When did you start using Bitcoin? *

◯ - 2009
◯ - 2010
◯ - 2011
◯ - 2012

◯ - Other

_____

9. Have you used any other digital money system(s) than Bitcoin? *

If No, the next question will be skipped.

◯ Yes

◯ No

Voluntary comments about this page's questions

_____

_____

_____

Other digital currencies

Your relation to other digital currencies.

10. you answered yes, please tell which one(s) and leave a comment about it, if you wish. *

- [ ] Digicash _____
- [ ] e-gold _____
- [ ] ecash _____
- [ ] eCache _____
- [ ] Pecunix _____
- [ ] Ven _____
- [ ] Video game currenc/y, -cies (must involve dealing with other human beings) _____
- [ ] Bitcoin variant(s) _____
- [ ] Other _____

Voluntary comments about this page's question

_____

_____

_____

Bitcoin usage

How much do you spend your time around Bitcoin.

11. How often do you use Bitcoin (mining doesn't count)? *

- ◯ Daily
- ◯ Many times a week
- ◯ Once a week
- ◯ Many times a month
- ◯ Once a month
- ◯ Less often

Voluntary comments about this page's question

_____

_____

_____

Mining

Using the combination of hardware and software to mine bitcoins.

12. Do you mine bitcoins? *

If No, the next three questions will be skipped. Keep in mind that even if you have somehow outsourced your mining, it is considered that you ARE mining bitcoins. Buying bitcoins from an exchange service etc. is not counted as mining.

- ◯ Yes
- ◯ No

Voluntary comments about this page's question

_____

_____

_____

Mining (page 2)

More specific information about you mining bitcoins.

13. If you answered yes to the previous question, how often do you mine? *

- ◯ All the time
- ◯ When I'm not doing any other GPU demanding tasks on my computer
- ◯ At nights
- ◯ In the daytime
- ◯ Other

_____

14. What mining hardware do you use? *

- ◯ CPU
- ◯ GPU
- ◯ FPGA
- ◯ Combination

_____

- ◯ Other

_____

15. Do you have separate mining rig(s) or do you mine with the same computer you use every day? *

- ◯ A separate mining rig
- ◯ Many separate mining rigs
- ◯ Outsourced mining hardware

○ The same computer I use every day

○ Other

_____

Voluntary comments about this page's questions

_____

_____

_____

Using Bitcoin

16. What is the main reason you use Bitcoin? *

- ◯ Privacy
- ◯ Practicality
- ◯ Secureness
- ◯ It's open source
- ◯ Cheap transaction fees
- ◯ It's P2P
- ◯ I don't like middlemen and bureaucracy
- ◯ Hobby
- ◯ Deflatory nature
- ◯ I don't like fiat currencies / Protest
- ◯ Investing potential
- ◯ Other

_____

17. How do you utilize Bitcoin? *

Choose 1-3 options.

- ☐ Day-trade / Speculation
- ☐ Alternative investment
- ☐ I run an every day Bitcoin business of my own
- ☐ Buy goods and/or services
- ☐ Mining
- ☐ Commit private transactions
- ☐ Gambling/Lottery
- ☐ Donations

Other

☐ _____

Voluntary comments about this page's questions

_____

_____

_____

18. How easy/convenient do you think it's to use bitcoins beside fiat currencies, i.e. to exchange them to fiat currencies and vice versa, use them like fiat currencies etc.? *

Very inconvenient 1 | 2 | 3 | 4 | 5 Very convenient

◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

19. How do you rate the basic functionality of the Bitcoin network in the scale of 1-5? *

Very poor 1 | 2 | 3 | 4 | 5 Very good

◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

20. How do you rate the security of the Bitcoin network in the scale of 1-5? *

Very poor 1 | 2 | 3 | 4 | 5 Very good

◯ 1 ◯ 2 ◯ 3 ◯ 4 ◯ 5

Voluntary comments about this page's questions / Comments about this questionnaire.

The questionnaire will be finished after this page.

_____

_____

_____