Bitcoin-kryptovaluutta

Oulun yliopisto
Tietojenkäsittelytieteiden laitos
LuK-tutkielma
Juhani Karppinen
31.5.2015

Tiivistelmä

Tässä tutkimuksessa käsitellään, kuinka bitcoin-verkko toimii ja mitä eri käyttötarkoituksia sillä on. Tutkimus rajattiin bitcoiniin, koska se on ensimmäinen ja eniten käytetty kryptovaluutta. Tutkimus perustui kirjallisuustutkimukseen.

Tietotekniikan kehittyminen on vaikuttamassa myöskin maksuliikenteeseen. Transaktioita on suoritettu jo verkon kautta esimerkiksi pankkien toimesta ja kolmansien osapuolien tarjoamien palvelujen avulla. Kryptovaluutat ovat täysin uusi ilmiö maksutapahtumien näkökulmasta. Kryptovaluutat pyrkivät olemaan täysin omia valuuttojansa ja toimimaan ilman keskuspankkia.

Kryptovaluutat toimivat täysin verkossa eikä ne ole fyysisesti käsin kosketeltavissa. Toinen suuri ero traditionaalisiin pankkivaluutoihin on se, että kryptovaluutoilla ei ole omaa keskuspankkia.

Kryptovaluuttojen tapauksessa kaikki transaktiot on julkista tietoa, mitä ei tapahdu traditionaalisissa pankkivaluutoissa. Käytännössä kaikki kryptovaluutoilla suoritetut transaktiot näkyvät julkisina. Käyttäjien identiteetti suojataan niin, että henkilötietoja ei tallenneta järjestelmään. Tämä on ennenkuulumatonta traditionaalisessa pankkimallissa, sillä henkilötiedoilla rajoitetaan varoihin pääsyä esimerkiksi verkkopankissa tai pankin asiakaspalvelupisteellä asioidessa.

Generoiduilla kryptovaluutoilla ei näin ollen ole ollenkaan omistajia. Käyttäjillä on olemassa julkisia avaimia, joihin voidaan vastaanottaa varoja, sekä yksityisiä avaimia, joilla varat ovat käytettävissä. Transaktiot vahvistetaan erillisen louhijaverkon avulla. Louhijaverkon solmuksi voi liittyä kuka tahansa. Transaktioiden vahvistuksesta louhijat saavat palkkioksi generoitua kryptovaluuttaa, ja tällöin valuuttaa saadaan luotua lisää.

Avainsanat
bitcoin, kryptovaluutat

Ohjaaja
yliopistonlehtori Juha Kortelainen

Sisällys

1. Johdanto

Internet ja tietotekniikan kehittyminen tuovat uusia mahdollisuuksia monelle eri liiketoiminnan sektorille. Erilaiset verkkopalvelut ovat mahdollistaneet varojen siirron verkossa huomattavasti pienemmällä viiveellä kuin pankkisiirrot, mutta ongelmana on se, että nämä kyseiset palvelut eivät useinkaan tarjoa mahdollisuutta suorittaa maksutapahtumia esimerkiksi fyysisessä kaupassa asioidessa. Elektronisiin maksutapoihin on tosin erilaisia kolmannen osapuolen palveluita, kuten esimerkiksi VISA-korttimaksut.

Kryptovaluutat ovat tuoneet yllä mainittuihin haasteisiin ratkaisun. Kryptovaluutta vaihtoehtoisena maksutapana tukee hyvin pienen viiveen maksutapahtumat jopa toiselle puolelle maapalloa. Niitä voidaan käyttää myös maksutapahtuman suorittamiseen kivijalkamyymälöissä sekä verkkokaupoissa, mikäli myyjä tukee kyseistä maksutapaa.

Toisin kuin perinteiset pankkivaluutat, kryptovaluutat ovat desentralisoituja, eivätkä ne ole minkään keskuspankin hallittavissa. Bitcoin on kaikista kryptovaluutoista käytetyin, lisäksi suurin osa kryptovaluuttoihin liittyvistä tutkimuksista on tehty käyttäen bitcoinia esimerkkinä. Bitcoin on avoimen lähdekoodin projekti, joten sen toimintatapa on kaikille tiedossa. Edellä mainittujen huomioiden takia ja aiheen rajauksen vuoksi keskityn tässä tutkimuksessa käsittelemään bitcoinia.

Bitcoin julkaistiin ensimmäisenä kryptovaluuttana vuonna 2009. Koska kryptovaluutat ovat suhteellisen uusi käsite informaatioteknologian alalla, niistä ei kirjoitushetkellä ei ole löytynyt tieteellistä tutkimusta yhtä laajasti kuin muista informaatioteknologian osa-alueista. Kryptovaluutat on kuitenkin jo löytäneet paikkansa globaalissa ekonomiassa, sillä kirjoitushetkelläkin useita transaktioita on suoritettu eri kryptovaluuttojen avulla.

Tämän tutkimuksen tarkoituksena on tehdä kattava selonteko bitcoinista ja siihen liittyvistä aspekteista. Tarkemmin tutkimusongelmina ovat bitcoinin määritelmä, bitcoin-verkon toiminnan selittäminen, bitcoinin hyödyt ja haitat sekä sen tulevaisuuden näkymät.

Tutkimus perustuu kirjallisuustutkimukseen. Aluksi määrittelen työn laajuuden rajaamalla, mitkä bitcoiniin liittyvät elementit tässä tutkimuksessa esitellään. Sen jälkeen valikoin ja arvioin alkuperäistutkimukset, joihin tutkimus perustuu. Lopuksi yhdistelen alkuperäistutkimuksista saadun datan kokonaisuudeksi, joka vastaa tutkimusongelmaan.

Aloitan tutkimuksen esittelemällä lyhyesti tutkimuksen kannalta tärkeimmiksi osoittautuneet kirjallisuuslähteet ja niissä esitellyt näkökulmat aiheeseen liittyen. Sen jälkeen määrittelen kryptovaluutan ja bitcoinin. Sitä seuraavissa kappaleissa käsitellään bitcoin-verkon toimintaa transaktoiden ja louhinnan osalta, jonka jälkeen esitellään bitcoinin erilaisia käyttötarkoituksia hyötyineen ja haittoineen. Lopussa on yhteenveto johtopäätöksineen.

2. Tärkeimmät kirjallisuuslähteet

Tässä kappaleessa käyn läpi tärkeimmät tutkimuksessa käytettävät lähteet ja niiden näkökulmat tutkimusaiheeseen liittyen.

Vuonna 1998 Dai esitteli teorian anonyymistä, desentralisoidusta valuutasta Cypherpunks-sähköpostilistalla. Dai nimitti uutta vaihtoehtoista valuuttaa nimellä "b-money". Dai käsittelee tekstissään vaihtoehtoisen valuutanluontimenetelmän sekä transaktioiden verifioinnin. Dain teoriaa on hyödynnetty käytännössä Nakamoton (2008) kehittämässä bitcoinissa.

Vuonna 2008 Satoshi Nakamoto kehitti valuutan pohjautuen Dain ideaan. Anonyymi, desentralisoitu valuutta bitcoin pohjautuu hänen verkossa julkaisemaansa artikkeliin *Bitcoin: A Peer-to-Peer Electronic Cash System* (Kaplanov, 2012). Nakamotoa pidetään pseudonyyminä, sillä hänen identiteettiään ei tiedetä (Jacobs, 2011; Kaplanov, 2012; Plassaras, 2013). Nakamoton artikkelissa käsitellään bitcoinin transaktioihin ja louhintamenetelmään liittyvä logiikka teknisestä näkökulmasta. Nakamoton artikkeli on ainoa lähde, jossa bitcoinin toiminta selitetään kokonaisvaltaisesti. Tämä ilmenee jo siitä, että kaikki tutkimusta varten luetut lähteet viittaavat Nakamoton artikkeliin.

Kaplanovin (2012) artikkeli *Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation* käsittelee bitcoinin käyttöä ja sen vaikutusta talouteen Yhdysvaltain lakien ja erilaisten säännösten näkökulmasta. Bitcoin eroaa keskitetyistä pankkivaluutoista jo siten, että bitcoin-verkon hyväksymää maksutapahtumaa ei voida keskeyttää. Kaplanov käsittelee artikkelissaan sitä, voiko bitcoinia luokitella valuutaksi esimerkiksi Yhdysvaltain dollarin tavoin, ja mikä vaikutus sillä on maan ekonomiaan.

Christin käsittelee vuonna 2012 julkaistussa artikkelissaan *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace* verkossa olleen kauppapaikan Silk Roadin luonnetta anonyyminä alustana laillisten ja laittomien tavaroiden myynnissä. Christin käyttää kvantitatiivisia analysointimenetelmiä tutkiakseen kauppapaikassa tapahtuneita toimintoja, kuten tuotteiden esilläoloaikaa ja myyjien käyttäytymistä. Koska kauppapaikka keskittyi varsinkin laittomien tuotteiden myyntialustana toimimiseen, korosti se käyttäjien identiteetin suojausta rajaamalla pääsyn Silk Roadiin ainoastaan Tor-verkon kautta, sekä sallimalla ainoana maksuvaihtoehtona bitcoinit.

3. Kryptovaluutta ja bitcoin

Idea desentralisoidusta, täysin elektronistesta kryptovaluutasta on esitetty Cypherpunks-sähköpostilistalla vuonna 1998 (Dai, 1998). Dain (1998) mukaan pankit ovat tavallisesti valtion instituutioiden omistuksessa, ja hän esittääkin määritelmän protokollasta, jolla elektroninen maksujärjestelmä voitaisiin toteuttaa jäljittämättömien entiteettien välillä. Kryptovaluutta on elektroninen, vertaisverkossa toimiva verkkovaluutta. Kryptovaluutat ovat viime aikoina saaneet yhä enemmän medianäkyvyyttä, ja niiden käyttö vaihdannan välineenä yleistyy. Kryptovaluutta-sanan alkuosa krypto viittaa järjestelmässä käytettyyn kryptografiaan (Grinberg, 2012). Toinen kryptovaluutan yhtenäisyyttä tukeva elementti kryptografian lisäksi on vertaisverkko, joka vahvistaa transaktiot (Grinberg, 2012). Vaihtoehtoisia kryptovaluuttoja on olemassa kirjoitushetkellä 2990 kappaletta (Cryptocoincharts, 2015).

Bitcoin on yksi kryptovaluutoista. Yleisradio esitteli 15.4.2013 Aamu-tv -ohjelmassaan pääasiallisesti bitcoinia, mutta lisäksi ohjelmassa esiintyi helsinkiläinen ravintola Vegemesta. Vegemesta liittyi aiheeseen asiakkaille tarjoamien maksuvaihtoehtojensa puolesta. Vegemesta-ravintolassa tilaukset on Aamu-tv:n mukaan mahdollista maksaa - ei ainoastaan käteisellä, pankki- tai luottokortilla - vaan myöskin bitcoin on yksi maksuvaihtoehdoista. Voidaan siis ajatella, että bitcoin ja muut kryptovaluutat ovat yksi monista saatavilla olevista maksuvaihtoehdoista, siinä kuten perinteiset keskitetyt pankkivaluutat. Bitcoinin arvo perustuu ainoastaan kysyntään ja tarjontaan, eikä se ole yksittäisen keskuspankin hallittavissa. Ei ole olemassa myöskään tahoa, joka voisi kontrolloida bitcoinien käyttöä vaihdannan välineenä.

Bitcoin on kehitetty elektroniseksi vaihdannan välineeksi, jossa varojen siirtoon ei tarvita erillistä kolmatta osapuolta, joka voisi kontrolloida varoja. Bitcoinissa käyttäjien identiteettiä ei tallenneta mihinkään. Henkilötunnistautumisen sijaan bitcoinissa lompakkoon päästään generoidun yksityisen avaimen avulla, jolloin yksityisen avaimen haltijalla on oikeus bitcoin-lompakossa oleviin varoihin. Bitcoinin louhinta-algoritmi perustuu Hashcash-menetelmään (Nakamoto, 2008). Nakamoton (2008) määritelmästä seurasi avoimen lähdekoodin ohjelmiston julkaisu verkkoon. Ensimmäinen bitcoin-verkon lohko generoitiin 3. tammikuuta 2009 (Bitcoin.it, 2014), josta lähtien bitcoin-verkko on ollut saatavilla. Muiden kryptovaluuttojen ero bitcoiniin verrattuna voi olla nimessä ja/tai käytetyissä algoritmeissa.

4. Asiakasohjelmat

Asiakasohjelman avulla käyttäjä yhdistetään bitcoin-verkkoon. Ensimmäinen bitcoin-asiakasohjelma *bitcoind* toimii komentorivipohjaisena rajapintana bitcoin-verkkoon (Bitcoin.it, 2015a). Nykyisin loppukäyttäjille on tarjolla komentorivipohjaisen rajapinnan lisäksi vaihtoehtoisesti graafisella käyttöliittymällä varustettuja asiakasohjelmia. Bitcoin-ytimen mukana tarjotaan loppukäyttäjille tarkoitettua graafisen käyttöliittymän sisältävää Bitcoin-Qt -asiakasohjelmaa, mutta vaihtoehtoisiakin asiakasohjelmia on olemassa. (Bitcoin Project, 2015; Bitcoin.it, 2015b)

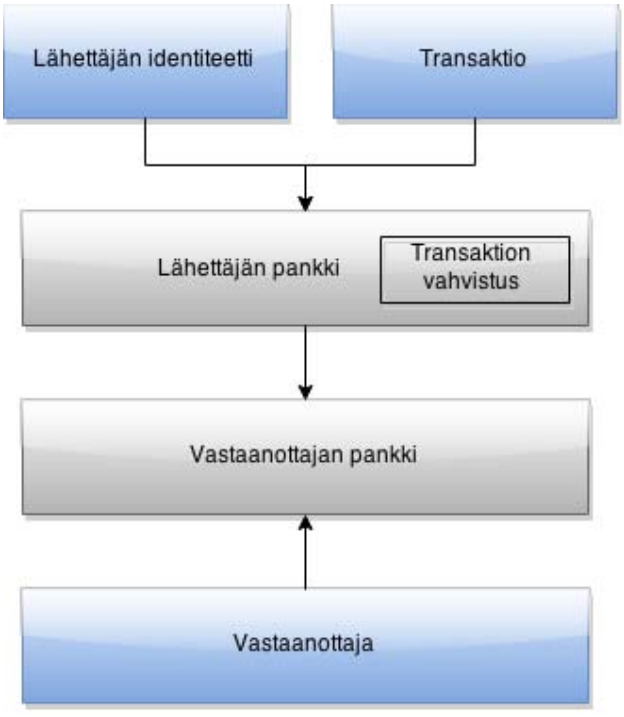
Asiakasohjelmassa voidaan generoida uusia julkisia avaimia jotka toimivat tilinumeroiden lailla – julkisen avaimen saatuaan toinen taho voi lähettää varoja kyseiseen bitcoin-osoitteeseen. Asiakasohjelmalla voi myös suorittaa varojen siirtotoimenpiteen. Asiakasohjelmalla pystytään myös avaamaan bitcoin-lompakko. Käyttäjän varat ovat bitcoin-lompakossa. Lompakolla on tiedoston muodossa oleva yksityinen avain, josta bitcoin-varoihin pääsee käsiksi. Lompakon julkinen avain esiintyy transaktioissa bitcoinien lähetys- ja vastaanottamisosoitteena.

5. Bitcoinien generointi ja transaktiot

Tässä osassa käsittelen sekä bitcoinien generoinnin, eli louhinnan, että transaktiot. Nämä kaksi asiaa käsitellään samassa yhteydessä, koska louhinta on myös transaktioiden suorittamiseen liittyvä toiminto. Tarkastelen ensin transaktioita ja siirryn sen jälkeen louhintaan.

5.1 Transaktiot

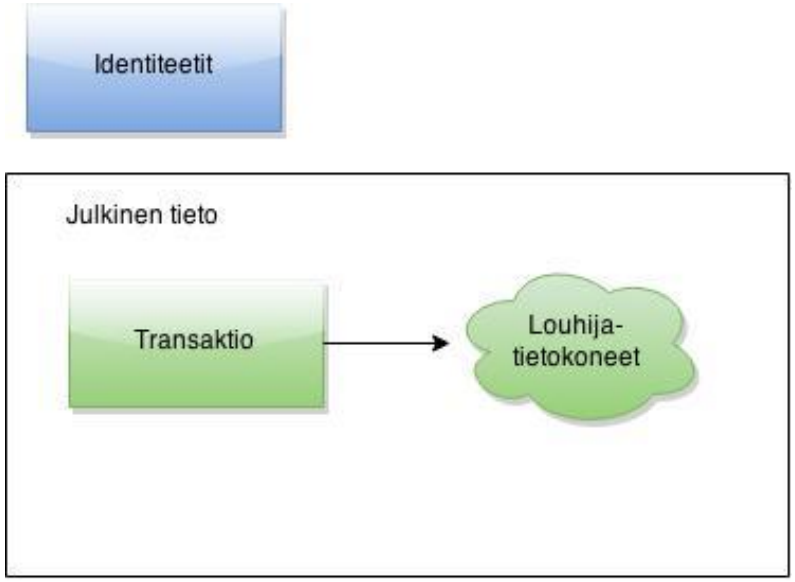
Transaktio on tapahtuma, jossa varoja lähetetään kahden osapuolen välillä. Bitcoin-järjestelmän kautta toteutetut transaktiot perustuvat kahteen bitcoin-osoitteeseen ja louhijatietokoneiden suorittamaan prosessointiin, kun taas traditionaalisessa pankkimallissa kolmantena osapuolena on pankki. Erona traditionaaliseen pankkimalliin bitcoin-järjestelmässä varoihin ei ole kontrollia kolmannella osapuolella (Nakamoto, 2008). Bitcoineja voidaan lähettää bitcoin-verkossa ilmaiseksi, mutta transaktioon voidaan sisältää vapaavalintainen transaktiomaksu, jolla transaktion vahvistusta voidaan nopeuttaa. (Grinberg, 2012)



Kuvio 1: Transaktion välitys traditionaalisessa pankkimallissa.

Kuvio 1 osoittaa transaktioiden välittymisen traditionaalisessa pankkimallissa. Pankin rooli transaktiossa on toimia kolmantena osapuolena varojen välittäjänä. Pankilla on yleensä myös tieto tilin omistajuudesta ja erillisistä käyttöoikeuksista, joka mahdollistaa

tilin käyttäjän identiteetin vahvistamisen ennen transaktion suorittamista. Pankki välittää transaktion toisen osapuolen tilille, ja hän saa varat käyttöönsä pankkinsa kautta.



Kuvio 2: Transaktio bitcoin-järjestelmässä

Toisin kuin traditionaalisessa pankkimallissa, bitcoin-järjestelmän kautta suoritetun transaktion tietoihin ei liity käyttäjää identifioivia tietoja. Tämän takia identiteetit on eriytetty pois julkisista tiedoista kuviossa 2. Bitcoin-lompakolla ei ole omistajatietoja, joten transaktion pystyy suorittamaan kuka tahansa, jolla on lompakon yksityinen avain hallussaan. Bitcoin-mallissa transaktion vahvistus tapahtuu louhijatietokoneiden avulla. Vastaanottaja saa varat käyttöönsä bitcoin-lompakon yksityisellä avaimella.

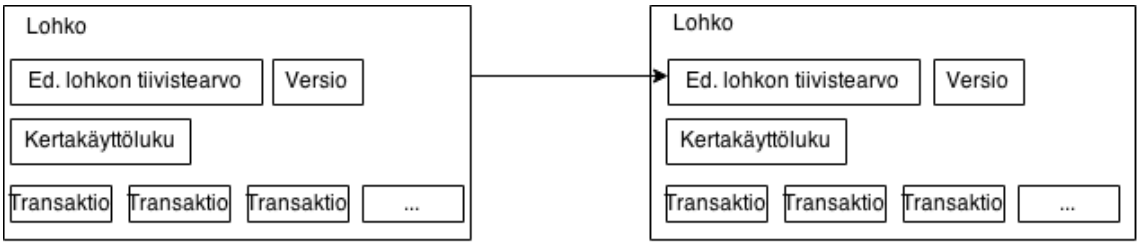
5.2 Louhinta

Louhinta on bitcoinien generointilogiikkaa, sekä bitcoin-verkon toiminto, jolla kaikki transaktiot suoritetaan. Jokainen transaktio vahvistetaan louhintaverkoston avulla. Bitcoinien louhintaan tarvitaan laitteiston lisäksi erillinen louhintaohjelma, jolla bitcoin-louhintaverkkoon liitytään louhinnan suorittamiseksi. Louhintaohjelmat voidaan jakaa alustaspesiifisti esimerkiksi ohjelmiin, joilla voidaan suorittaa louhintaa esimerkiksi näytönohjaimilla (Graphics Processing Unit, GPU) tai prosessoreilla (Central Processing Unit, CPU) (Bitcoinx.com, 2015).

Louhijatietokone toimii osana louhintaverkkoa. Louhintaverkkoon voidaan kytkeä tietokoneita, ja louhinta-algoritmia voidaan suorittaa prosessoria tai näytönohjainta hyödyntäen tai algoritmin suoritukselle suunniteltujen mikropiirien avulla. Tällaisia mikropiirejä ovat ASIC-piirit (Application-specific Integrated Circuit) tai FPGA-piirit (Field-programmable gate array) avulla (Bitcoin.it, 2015c). Mikä tahansa taho pystyy siis saamaan bitcoineja joko vaihdantatapahtuman (esimerkiksi tavaran myymisen) kautta tai louhimalla niitä louhintaan tarkoitetun laitteiston avulla. (Kaplanov, 2012).

Nakamoton (2008) artikkelista ilmenee, että lohko on datasäilö, joka sisältää transaktioita. Transaktioiden lisäksi lohkossa on lohkoketjun edellisen lohkon

tiivistearvo, bitcoin-protokollan versio sekä kertakäyttöluku. Lohkoketju alkaa verkon ensimmäisestä lohkosta eli Genesis-lohkosta. Kuviossa 3 on kuvattu kaksi lohkoa, jotka ovat muodostaneet lohkoketjun. Lohkoketju muodostetaan lisäämällä uuteen lohkoon edellisen vahvistetun lohkon tiivistearvo.



Kuvio 3: Bitcoin-lohkoketjun muodostus

Bitcoineja voidaan generoida maksimissaan 21 miljoonaa kappaletta. Pienin yksikkö, johon bitcoin voidaan jakaa, on 1 x 10^{-7} bitcoinia, jota kutsutaan satoshiksi (Stanković, Mihajlović, & Mihajlović, 2014). Bitcoin-verkon ensimmäinen lohko, niin kutsuttu Genesis-lohko on generoitu 3. tammikuuta 2009 (Barber, Boyen, Shi, & Uzun, 2012).

Louhijasolmu vahvistaa lohkon löytäessään sellaisen tiivistearvon, joka on pienempi tai yhtä suuri kuin kohdearvo. Kohdearvo (engl. target value) on 256-bittinen luku joka on tiedossa kaikilla verkon solmuilla. Kohdearvon tarkoitus on kontrolloida lohkojen vahvistamistahtia suhteessa bitcoin-verkon sen hetkiseen laskentatehoon, jotta lohkoja ei vahvistettaisi keskimäärin nopeammin tai hitaammin kuin 10 minuutin välein. Kohdearvo lasketaan uudelleen aina 2016 vahvistetun lohkon välein. (Bitcoin.it, 2012)

Lohko vahvistetaan iteroimalla kertakäyttöluvun arvon kasvattamista ja generoimalla lohkon tiivistearvo uudelleen. Kun louhija löytää sellaisen tiivistearvon, joka on pienempi kuin bitcoin-verkon kohdearvo, lohko on vahvistettu. Palkkiona lohkon vahvistamisesta louhijasolmu saa bitcoineja (Bryans, 2014). Palkkio, joka on saatu 210 000 ensimmäisen lohkon vahvistamisesta, on 50 bitcoinia. Louhinnasta saatu palkkio puolitetaan aina jokaisen 210 000 generoidun lohkon kohdalla. Noin kahdessa vuodessa ensimmäiset 210 000 lohkoa saatiin vahvistettua, jonka jälkeen palkkio puolittuu noin joka neljäs vuosi aina 210 000 lohkon vahvistamisen jälkeen. (Grinberg, 2012)

Bitcoin-louhintaverkko koostuu vertaisverkkoon kytketyistä solmuista, louhijatietokoneista, jotka suorittavat louhinta-algoritmia vahvistaakseen uusia transaktioita bitcoin-verkossa. Louhinta koostuu yhteensä kuudesta osasta (Nakamoto, 2008):

1. Uudet transaktiot lähetetään kaikille solmuille.

2. Jokainen solmu kerää uudet transaktiot lohkoon

3. Jokainen solmu suorittaa louhinta-algoritmia vahvistaakseen lohkon..

4. Kun solmu löytää sellaisen kertakäyttöluvun, jolla bitcoin-lohkon tiivistearvo on pienempi tai yhtä suuri kuin vaadittu kohdearvo, lähettää se lohkon kaikille solmuille.

5. Solmut hyväksyvät lohkon, mikäli kaikissa transaktion lähdeosoitteissa on tarpeeksi bitcoineja maksun suorittamista varten.

6. Solmut näyttävät vahvistuksen lohkon oikeellisuudesta siirtymällä työskentelemään lohkoketjun seuraavan lohkon kanssa käyttämällä hyväksytyn lohkon tiivistettä edellisenä tiivisteenä.

5.2.1 Keskitetty louhintakehä

Bitcoin-louhinnan haastavuus on noussut sitä mukaa, kun uusia louhijatietokoneita on liittynyt vertaisverkkoon. Koska haastavuustaso on noussut, niin louhintatietokoneen on yhä haastavampi löytää lohkon vahvistusta itsenäisesti. Louhinnan tehostamiseksi on perustettu keskitettyjä louhintakehiä (engl. mining pool), jonka tarkoituksena on hajauttaa useampi louhintatietokone laskemaan samaa louhintatapahtumaa.

Louhintakehä näkyy bitcoin-louhintaverkolle yhtenä louhijana, ja palkkio ratkaistusta lohkosta annetaan louhintakehälle. Louhintakehä lähettää jaetun osan palkkiosta kaikille niille louhijatietokoneille, jotka osallistuivat kyseisen lohkon ratkaisuun. Lisäksi louhintakehä saattaa ottaa louhinnan keskittämispalvelun ylläpitämisestä itse nimeämänsä osuuden.

5.2.2 Louhinta-algoritmi

Bitcoinin louhinta-algoritmi pohjautuu Hashcashiin (Nakamoto, 2008). Hashcash on alunperin esitelty vuonna 1997 mekanismina, jolla resurssien systemaattista väärinkäyttöä pyritään rajoittamaan. (Back, 2002). Back mainitsee myös, että rajoittamattomina internetin resursseina voidaan pitää esimerkiksi sähköpostien lähettämistä. Bitcoin-lohkon vahvistuslogiikka on variaatio Hashcashista (Nakamoto, 2008).

Lohkon vahvistus tapahtuu iteroimalla kertakäyttöluvun kasvattamista ja generoimalla lohkon tiivistearvoa niin pitkään, kunnes vahvistettavasta lohkosta laskettu tiivistearvo on pienempi tai yhtä suuri kuin bitcoin-verkon kohdearvo (Bitcoin.it, 2012). Lohko sisältää kertakäyttöluvun ja vahvistettavien transaktiotietojen lisäksi myös tiivisteen edellisestä hyväksytystä lohkosta. Tämä tarkoittaa sitä, että kaikki hyväksytyt lohkot ovat ketjutettu toisiinsa. Lohkoa ei tällöin voi muuttaa ilman, että laskentatyö ja ketjuttaminen tehtäisiin myöskin kaikille seuraaville lohkoille. (Nakamoto, 2008)

Louhintaan käytettävien alustojen tuottavuudessa voi olla huomattavia eroja, kuten nähdään kuviossa 4. Kuvion 4 otoksesta nähdään, että louhintatietokoneissa käytetty laitteisto vaikuttaa siihen, kuinka nopeasti louhinta-algoritmia voidaan suorittaa. Louhinta-algoritmin suoritusta mitataan tiivisteiden generoinneissa per sekunti (hash/s). Plassarasin (2013) mukaan on huomioitava myös laitteen sähkönkulutus ja sähkön hinta, mikäli bitcoin-louhinnasta on tarkoitus jäädä rahallisesti voitolle. Hän kirjoittaa myös, että tyypillisellä toimistotietokoneella bitcoin-louhintaa tulisi suorittaa keskimäärin viidestä kymmeneen vuoteen, jotta se yksin pystyisi tuottamaan bitcoineja. Tämän myötä sähköä on kulunut enemmän, kuin mitä saatujen bitcoinien arvo todellisuudessa on.

6. Louhinta-alustat ja niiden erot

Bitcoin on alunperin kehitetty louhittavaksi tietokoneiden prosessorien (CPU) avulla (Nakamoto, 2008). Louhinnan suorittamisesta myös muilla alustoilla on oltu tietoisia, sillä bitcoiniin keskitetyllä keskustelualueella Nakamoto on maininnut, että tasapuolisuuden nimissä näytönohjaimilla (GPU) louhimiseen ei tulisi siirtyä, sillä silloin CPU-louhijat saisivat pienemmän osuuden palkkioksi saatavista bitcoineista (Bitcointalk, 2009).

Syyskuussa 2010 nimimerkillä puddinpop esiintyvä taho julkaisi Windows-pohjaisen louhintaohjelman avoimen lähdekoodin ohjelmistona (Bitcointalk, 2010). Kyseinen louhintaohjelma mahdollisti louhintaan liittyvän logiikan laskennan siirtämisen prosessorilta näytönohjaimelle NVIDIAn kehittämän CUDA-alustan avulla. CUDA on näytönohjainvalmistaja NVIDIAn kehittämä alusta, joka mahdollistaa laskennan suorittamisen prosessorin sijaan näytönohjaimella (Nvidia, n.d.).

Tuote	Tyyppi	Esitetty suorituskyky (Mhash/s)	Sähkönkulutus (W)
Antminer S3	ASIC	441000	340
Hashcoins Apollo v3	ASIC	1100000	1000
ATI Radeon 4870	GPU	104,6	120
Nvidia GTX295	GPU	120,7	289
Intel Core i5 2600K	CPU	17,3	75
AMD Athlon II X4 630	CPU	10,7	95

Kuvio 4: Ote louhinta-alustoista, niiden suorituskyvystä ja sähkonkulutuksesta. (Bitcoin.it, 2015c)

Kuvion 4 taulukossa esitellään erilaisten louhinta-alustojen tehokkuus bitcoinin louhinta-algoritmia suoritettaessa. Kuten taulukon tuloksista huomataan, on ASIC-piireillä toteutetut alustat huomattavasti tehokkaampia louhinta-algoritmin suorituksessa verrattuna näytönohjaimiin ja tietokoneiden prosessoreihin.

7. Bitcoinin hyödyt ja haitat

Traditionaalisessa pankkimallissa yksityisyys rajataan varojen lähettäjän, vastaanottajan ja pankin välille. Kaikkien transaktioiden julkistaminen ei tue pankkimallin tapaista yksityisyyttä, mutta yksityisyys voidaan suojata poistamalla tietoa muualta kuin yllämainituin tavoin; poistamalla julkisten avainten omistajatiedot, jolloin kaikista transaktioista tulee näin ollen anonyymejä. Koska kaikki bitcoin-transaktiot ovat julkisia eli kenen tahansa tarkasteltavissa, voidaan nähdä ainoastaan julkisten avainten välinen transaktio ja sen suuruus. (Nakamoto, 2008)

Kryptovaluutoissa julkinen avain toimii samankaltaisin periaattein kuin pankkitili perinteisessä pankkimallissa; julkiselle avaimelle voidaan suorittaa transaktioita, ja yksityisen avaimen haltija saa pääsyn käsitellä varoja, jotka julkisella avaimella on mahdollista käyttää. Traditionaalisessa pankkimallissa pankkitilillä on aina omistaja, mutta koska kryptovaluutoissa julkista avainta ei omista kukaan, varoihin pääsee käsiksi kuka vain, joka omistaa vastaavan yksityisen avaimen.

Bitcoinin anonyymius tuo etuja myös rikollisissa aikeissa toimiville tahoille. Yhtenä esimerkkinä tästä on Tor-verkossa toiminut Silk Road -verkkosivusto, joka toimi laittomien ja laillisten tuotteiden kauppapaikkana (Christin, 2013). Silk Road keskittyi erityisesti toimimaan kauppa-alustana huumausaineiden myyjien ja ostajien välillä (Christin, 2013). Christin (2013) mainitsee, että Silk Road tuki maksuvälineenä ainoastaan bitcoinia siitä syystä, että bitcoinin tarjoama transaktioiden anonyymius suojaa parhaiten käyttäjien henkilöllisyyttä.

8. Pohdinta ja johtopäätökset

Tutkimusta tehdessä huomattiin, että bitcoinista löytyvä tieto on useissa eri lähteissä. Aiheesta on tehty tutkimusta jo jonkin verran, mutta määrittelevä, tekninen tieto koostui muun muassa Nakamoton itse julkaisemasta artikkelista sekä avoimen lähdekoodin projektin wiki-sivustosta. Tämän tutkimuksen tärkein kontribuutio oli koota useista lähteistä koostuva tieto yhteen dokumenttiin.

Kryptovaluutoista ei löytynyt kovin laajasti lähteitä. Tämä voi johtua siitä, että ensimmäisen kryptovaluutan, bitcoinin, määritelmä julkaistiin vuonna 2008 ja suurin osa aiheeseen liittyvistä lähteistä on julkaistu sen jälkeen. Aihetta ei ole siis ehditty tutkia vielä kovin pitkään, joten tämän takia esimerkiksi Julkaisufoorumin korkeimman tason lähteet jäivät kovin rajalliseksi. Suomenkielistä tutkimusta bitcoinista tai muista kryptovaluutoista ei ole vielä olemassa kovinkaan paljon, joten tutkimuksen aikana lähdekieleltään englanninkielisten termien määrittely oli jokseenkin haastavaa.

Lähteiden luotettavuutta oli joissakin tapauksissa vaikeaa arvioida. Pseudonyymi Satoshi Nakamoton artikkeli bitcoinista määritteli teknisestä näkökulmasta bitcoin-verkon toimintatavat. Artikkelia ei oltu kuitenkaan julkaistu missään vaiheessa esimerkiksi alan lehdissä, joten tästä syystä Julkaisufoorumi-tasoa ei ole. Kävi kuitenkin ilmi, että Nakamoton verkossa itse julkaisemaansa tutkimukseen oli viitattu hyvin paljon muissa aiheeseen liittyvissä artikkeleissa, joten lähdettä voitiin sanoa luotettavaksi. Tilanteen tekee harvinaislaatuiseksi se, että Nakamoto on pseudonyymi, joten ei ole tiedossa, onko kyseessä yksityishenkilö vai useammasta henkilöstä koostuva ryhmä.

Bitcoin-verkossa on kirjoitushetkelläkin paljon louhijatietokoneita vahvistamassa käyttäjien tekemiä transaktioita. Kyseiset laitteet kuluttavat paljon sähköä bitcoin-verkon laskentaa suorittaakseen. Kestävän kehityksen näkökulmasta bitcoin-järjestelmään käytetyn laskentakapasiteetin voisi muuttaa laskemaan jotain muuta. Tällaisella ajatuksella on kehitetty vaihtoehtoinen kryptovaluutta Primecoin, jossa Hashcash-variaatio on korvattu alkulukujen etsinnällä (Primecoin, 2014).

Kryptovaluutta ja bitcoin -kappaleessa mainittiin, että helsinkiläinen ravintola oli ottanut bitcoinin käyttöön yhdeksi maksutavaksi hoitaa ravintolalasku. Tästä voidaan tehdä johtopäätös, että bitcoinia voidaan mahdollisesti käyttää maksutapana myöskin muissa yrityksissä tulevaisuudessa. Kansainvälisesti katsottuna on jo nyt olemassa muutamia yrityksiä, jotka tarjoavat bitcoinin yhdeksi maksutavaksi. Coindesk (2013) uutisoi Sydenyssä sijaitsevasta pubista, joka otti käyttöön niin ikään bitcoinin yhdeksi maksuvaihtoehdoksi. Uutisen mukaan pubin omistaja Garry Pasfield oli ottanut bitcoinin testikäyttöön siitä syystä, ettei sen tarjoamisesta maksutapana koidu ollenkaan ylimääräisiä kustannuksia yritykselle.

Mielestäni bitcoinilla on potentiaalia kasvaa valtavirran maksutavaksi. Transaktioiden anonyymiys on kuitenkin haaste valtiollisille toimijoille, kuten verottajille, sillä se saattaa innostaa kansalaisia kiertämään maansa veropolitiikkaa suhteellisen helpolla tavalla. Toisaalta, jos kryptovaluutat eivät saavuta valtavirran suosimaa asemaa maksuvälineenä, voi kryptovaluuttojen käyttö jäädä marginaaliryhmän harrastukseksi. Esimerkiksi bitcoiniin siirtyminen traditionaalisten pankkivaluuttojen sijaan voi tuntua

hieman absurdilta, sillä likviditeetti eli markkinoiden volyymi on suhteellisen pieni. Tämä aiheuttaa muutosherkkyyttä bitcoinin arvossa.

Aihetta voisi tutkia edelleen useammastakin näkökulmasta. Syy siihen, että esimerkiksi myyjät eivät ota bitcoinia maksuvaihtoehdoksi, voi liittyä bitcoinin hinnan suureen vaihteluun. bitcoin ei ole vielä saavuttanut vaadittavaa likviditeettiä, vaan sen arvo saattaa vaihdella yhden vuorokauden aikana kymmeniä prosenttiyksiköitä. Taloustieteiden tutkimuksista hinnan vaihteluun voisi löytyä kirjallisuutta aikaisemmin tapahtuneisiin samankaltaisiin ilmiöihin, esimerkiksi kullan hintaan liittyen. Tietojenkäsittelyn näkökulmasta voitaisiin pohtia esimerkiksi sitä, muuttaisiko kvanttitietokoneiden yleistyminen kryptovaluuttojen louhintaa.

9. Yhteenveto

Tässä tutkimuksessa käytiin läpi bitcoin-verkon logiikka ja bitcoinin hyödyntämismahdollisuudet vaihdannan välineenä. Tutkimuksessa käy ilmi, että bitcoin voi olla maksuväline siinä missä käteinen raha tai esimerkiksi VISA-korttimaksut. Bitcoinin ja traditionaalisten pankkivaluuttojen väliset erot keskittyivät henkilötunnistautumiseen, varojen säilytykseen ja transaktiotapahtumiin. Toisin kuin perinteisissä pankkivaluutoissa, kaikki transaktiot ovat julkisia bitcoin-verkossa. Tässä erona on se, että tilien omistajatietoja bitcoin-verkossa ei ole, jolloin ainoaksi tiedoksi jää se, että kaksi anonyymiä tahoa siirtää tiedossa olevan määrän bitcoin-varoja tililtä toiselle.

Tutkimuksessa käytiin läpi myös bitcoinin transaktioiden vahvistuslogiikka ja bitcoinien generointi. Transaktiot perustuvat variaatioon Adam Backin Hashcashista. Bitcoinien generointia rajoitetaan muuttamalla louhijatietokoneiden selvitettävän tiivistesumman vaihtoehtoja suhteessa valmistuneisiin lohkoihin ja louhijatietokoneiden määrään. Keskitetyt louhintakehät mahdollistavat tehokkaamman louhinnan silloin, kun vaativuustaso kasvaa huomattavan suureksi suhteessa yksittäisen louhijatietokoneen laskentakapasiteettiin. Louhintakehissä laskenta jaetaan kaikille kehään liitetyille louhijoille.

Kirjallisuusviitteet

Back, A. (2002). Hashcash-a denial of service counter-measure. Retrieved from ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better: how to make bitcoin a better currency. In *Financial cryptography and data security* (pp. 399–414). Springer.

Bitcoin Project. (2015). Choose your wallet. Retrieved April 20, 2015, from https://bitcoin.org/en/choose-your-wallet

Bitcoin.it. (2012). Target - Bitcoin. Retrieved May 31, 2015, from https://en.bitcoin.it/wiki/Target

Bitcoin.it. (2014). Genesis block - Bitcoin. Retrieved May 2, 2015, from https://en.bitcoin.it/wiki/Genesis_block

Bitcoin.it. (2015a). Bitcoind - Bitcoin. Retrieved April 12, 2015, from https://en.bitcoin.it/wiki/Bitcoind

Bitcoin.it. (2015b). Clients - Bitcoin. Retrieved April 12, 2015, from https://en.bitcoin.it/wiki/Clients

Bitcoin.it. (2015c). Mining hardware comparison - Bitcoin. Retrieved April 24, 2015, from https://en.bitcoin.it/wiki/Mining_hardware_comparison

Bitcointalk. (2009). A few suggestions. Retrieved April 15, 2015, from https://bitcointalk.org/index.php?topic=12.msg54#msg54

Bitcointalk. (2010). Generating Bitcoins with your video card (OpenCL/CUDA). Retrieved April 15, 2015, from https://bitcointalk.org/index.php?topic=133.msg13135#msg13135

Bitcoinx.com. (2015). Bitcoin Mining Software. Retrieved May 24, 2015, from http://www.bitcoinx.com/bitcoin-mining-software/

Bryans, D. (2014). Bitcoin and money laundering: mining for an effective solution. *Indiana Law Journal*, *89*(1), 441–472.

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213–224). International World Wide Web Conferences Steering Committee.

Coindesk. (2013). Australians can now buy beer in bitcoin at Sydney pub. Retrieved May 3, 2015, from http://www.coindesk.com/australian-pub-accepts-bitcoin-sydney/

Cryptocoincharts. (2015). List of all traded alternative cryptocurrencies with blocks, difficulty, hashrate and marketcap. Retrieved April 15, 2015, from http://www.cryptocoincharts.info/coins/info

Dai, W. (1998). B-money, http://www.weidai.com/bmoney.txt. Retrieved from http://www.weidai.com/bmoney.txt

Grinberg, R. (2012). Bitcoin: an innovative alternative digital currency. *Hastings Science & Technology Law Journal*, *4*(1), 160–206.

Jacobs, E. (2011). Bitcoin: A Bit Too Far? *Journal of Internet Banking and Commerce*, *16*(2), 1–4.

Kaplanov, N. (2012). Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. *Loyola Consumer Law Review*, *25*(1), 111–174.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Nvidia. (n.d.). Parallel Programming and Computing Platform. Retrieved April 15, 2015, from http://www.nvidia.com/object/cuda_home_new.html

Plassaras, N. A. (2013). Regulating digital currencies: bringing bitcoin within the reach of IMF. *Chicago Journal of International Law*, *14*, 377.

Primecoin. (2014). Primecoin. Retrieved April 24, 2015, from http://primecoin.io/

Stanković, I., Mihajlović, R. A., & Mihajlović, A. (2014). Crypto-currency And E-financials. *International Journal of Economics and Law*, (10), 132–137.

Yleisradio. (2013). Ylen aamu-tv 15.4.2013 - Bitcoin. Retrieved from https://www.youtube.com/watch?v=OeqG4-G9IVo

Liitteet

Liite A. Tutkimussuunnitelma

Johdanto

Tämän tutkimuksen tarkoituksena on käsitellä kryptovaluutta Bitcoinin merkitystä vaihdannan välineenä sekä tehdä kattava selonteko kryptovaluuttaan liittyvistä aspekteista. Kryptovaluutat eroavat traditionaalisista pankkivaluutoista sillä, että kryptovaluutoilla ei ole olemassa omaa keskuspankkia.

Tutkimusongelma ja tutkimusmenetelmät

Tutkimusongelmana on tarkastella Bitcoinia desentralisoituna kryptovaluuttana määritelmänsä ja siihen liittyvän tutkimuksen kautta, avata Bitcoin-verkon toimintaperiaatteet sekä löytää hyödyt, haitat ja tulevaisuudennäkymät Bitcoiniin liittyen. Käytettävänä tutkimusmenetelmänä käytetään kirjallisuustutkimusta.

Rajoitteet

Tutkimus kohdistetaan bitcoiniin, sillä valtaosa alan tutkimuksista on tutkinut bitcoinia kryptovaluuttana. Haaste muiden kryptovaluuttojen käsittelemisessä LuK-työssä on siinä, että niistä ei löydy tarpeeksi tieteellistä tutkimusta LuK-työtä varten.

Aikaisempi tutkimus

Satoshi Nakamoton itse vuonna 2008 julkaisemansa artikkeli *Bitcoin: A Peer-to-Peer Electronic Cash System* antaa teknisen spesifikaation Bitcoin-järjestelmän toiminnasta. Artikkelissa käsitellään sekä louhintamenetelmä että transaktioihin liittyvä logiikka. Nakamoton artikkeli toimii määritelmiensä puolesta monen aiheeseen liittyvän tutkimuksen pohjana.

Christin (2013) on tutkinut verkossa toiminutta Silk Road -verkkosivustoa ja sen luonnetta verkon kauppapaikkana. Silk Road -verkkoalustan tarkoitus oli toimia alustana kaupankäynnille Bitcoinia vaihdannan välineenä käyttäen.

Kaplanovin (2012) artikkeli *Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation* käsittelee Bitcoinia ja sen määritelmää valuuttana Yhdysvaltain lakien ja säännösten näkökulmasta. Kaplanov käsittelee muun muassa sitä, voiko Bitcoinia määritellä valuutaksi.

Lähteet

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

Kaplanov, N. (2012). Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. *Loyola Consumer Law Review*, *25*(1), 111–174. http://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1920&context=lclr&sei-redir=1

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

Aikataulu

Maaliskuun 2015 loppuun mennessä tutkimusongelma on tarkennettu, sopiva tutkimusmenetelmä ja lähdemateriaalit on valittu. Aiheen pääasialliseen kirjallisuuteen liittyvä kappale on tässä vaiheessa kirjoitettu.

Maaliskuussa 2015 tutkin aiheeseen liittyviä teorioita ja aloitan määritelmän kirjoittamisen.

Maaliskuun 2015 toisella viikolla aloitan kirjoittamaan Bitcoin-verkon toimintamallista.

Maaliskuun 2015 viimeisellä viikolla kirjoitan Bitcoinin hyödyistä ja haitoista.

Huhtikuun 2015 ensimmäisellä ja toisella viikolla kirjoitan transaktioihin ja louhintaan liittyvät kappaleet.

Huhtikuun 2015 aikana kirjoitan tiivistelmän, johdannon, Bitcoinin tulevaisuudennäkymiin liittyvän kappaleen sekä yhteenvedon.

Huhtikuun 2015 loppuun mennessä tutkielma on lähetetty ohjaajalle tarkastettavaksi.

15.6.2015 mennessä tutkielma on ladattu Laturi-järjestelmään.

Sisällysluettelo

Tiivistelmä

Johdanto

Aiheen pääasiallinen kirjallisuus

Kryptovaluutta ja bitcoin

Transaktiot

Louhinta

Bitcoinin käyttötarkoitukset

Bitcoinin tulevaisuudennäkymät

Kirjallisuusviitteet

Liitteet