Tomislav Kukulj

Anonymiteetin haasteet Bitcoinin käytössä

Tietotekniikan kandidaatintutkielma

23. kesäkuuta 2019

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Tomislav Kukulj

Yhteystiedot: tomislav.t.kukulj@student.jyu.fi

Työn nimi: Anonymiteetin haasteet Bitcoinin käytössä

Title in English: Challenges of anonymity in using Bitcoin

Työ: Kandidaatintutkielma

Sivumäärä: 31+0

Tiivistelmä: Tutkielman tavoitteena on selvittää, tarjoaako viimeisen vuosikymmenen aikana suosioon noussut kryptovaluutta Bitcoin käyttäjilleen anonymiteettiä. Kryptovaluuttojen anonymiteetin tarkasteluun eivät perinteiseen tiedonsiirtoon liitetyt anonymiteetin teoreemat täysin sovellu ja tästä johtuen on muodostettu kryptovaluuttoja koskeva uusi anonymiteetin määritelmä. Tämän uuden määritelmän mukaisesti anonymiteettia tarkastellessa on selvää, että Bitcoin ei oletusarvoisesti tarjoa käyttäjilleen anonymiteettia. Myös vaihtoehtoisia kryptovaluuttoja on Bitcoinin suosion myötä luotu ja useita Bitcoinin sisällä toimivia palveluja on kehitetty anonymiteettiä silmällä pitäen. Tutkielmassa tarkastellaan myös näiden vaihtoehtojen käyttäjille tarjoamaa mahdollisuutta toimia anonyymisti. Tutkielma toteutetaan kirjallisuuskartoituksena.

Avainsanat: Bitcoin, kryptovaluutta, anonymiteetti, pseudonymiteetti

Abstract: The aim of this thesis is to find out whether the popular cryptocurrency Bitcoin offers anonymity to its users. To examine the anonymity of cryptocurrencies, the anonymity theories attached to traditional data transmission are not fully applicable and, consequently, a new definition of anonymity for cryptocurrencies has been formed. In accordance with this new definition, it is clear that by default, Bitcoin does not provide its users with anonymity. However, with the popularity of Bitcoin, alternative cryptocurrencies have also been created and several services within Bitcoin have been developed with anonymity in mind. The thesis also explores the possibility of anonymity for users of these alternatives. The thesis is carried out as a literature survey.

Keywords: Bitcoin, cryptocurrency, anonymity, pseudonymity

Kuviot

Sisältö

1 Johdanto

Virtuaalivaluutat ja erityisesti kryptografiaan perustuvat kryptovaluutat ovat nostaneet suosiotaan vaihtoehtoisina maksuvälineinä viime vuosina. Suosituimmaksi niistä on noussut vuonna 2008 julkaistu ja 2009 käyttöönotettu, ensimmäinen hajautetussa vertaisverkossa toimiva kryptovaluutta *Bitcoin*[1]. Bitcoin sai alkunsa tiedeyhteisön ulkopuolella, kryptografiaan keskittyneellä keskustelufoorumilla, jossa ”Satoshi Nakamoto” -nimimerkillä toiminut taho julkaisi vuonna 2008 kirjoituksen, jossa esiteltiin julkisen avaimen salaukseen perustuva hajautetussa vertaisverkossa toimiva virtuaalivaluutta Bitcoin (Nakamoto 2008). Tutkijayhteisön tarkempi huomio kiinnittyi Bitcoiniin vasta vuoden 2011 lopulla, jolloin ensimmäiset aihetta käsittelevät tutkimukset julkaistiin arXiv-arkistossa (Herrera-Joancomartí 2015, s.3). Yksi ensimmäisistä tutkimuksista oli Reidin ja Harriganin ensin vuonna 2011 arXiv-arkistossa ja myöhemmin Springerin kautta julkaistu analyysi Bitcoinin anonymiteetistä (Reid ja Harrigan 2013).

Vuosina 2012–2015 toteutettiin joukko tutkimuksia, jotka osoittivat Bitcoin-protokollaan liittyviä yksityisyyden suojaa koskevia heikkouksia (Conti ym. 2018, s.3442). Nämä tutkimukset käynnistivät tietosuojaa parantavien tekniikoiden kehitysaallon, jolla pyrittiin vahvistamaan yksityisyyttä ja parantamaan anonyymiyttä rikkomatta Bitcoinin perustavanlaatuisia suunnitteluperiaatteita (Conti ym. 2018, s.3442). Joitakin ehdotettuja ratkaisuja on toteutettu parannuksina olemassa olevaan Bitcoin-protokollaan, toiset taas ovat johtaneet täysin uusien kryptovaluuttojen syntymiseen (Amarasinghe, Boyen ja McKague 2019, luku 3.3). Useat näistä uusista valuutoista pohjautuvat Bitcoinin avoimeen lähdekoodiin, kun taas toisissa on käytetty täysin uudenlaisia ratkaisuja. Bitcoinin johtavan aseman vuoksi muut kryptovaluutat ovat saaneet kutsumanimen *vaihtoehtovaluutat* (engl. *Altcoins*). Monet vaihtoehtovaluutoista ovat kehittäneet ratkaisujaan yhä kryptografisempaan, eli raskaita salausmenetelmiä hyödyntävään suuntaan ja siten pyrkineet tarjoamaan käyttäjilleen anonyymimpiä tapoja toimia. Kryptovaluutat yleisesti ovatkin saaneet maineen erityisesti anonyymiyttä varjelevina

1. Vakiintuneeseen tapaan pohjautuen tässä tutkielmassa käytetään isolla alkukirjaimella kirjoitettua termiä *Bitcoin*, kun viitataan maksujärjestelmään ja sen vertaisverkkoon ja pienaakkosin kirjoitettua termiä *bitcoin* (lyhennetty *BTC*), kun viitataan valuutan yksikköön (Meiklejohn ym. 2013, s.128).

valuuttoina. Täydellinen anonyymiys varsinkin Bitcoinia käytettäessä on kuitenkin osoittautunut tutkimusten mukaan monimutkaiseksi kysymykseksi (Reid ja Harrigan 2013, s.197, Conti ym. 2018, s.3440).

Keskityn tutkielmassani suosituimmaksi nousseen kryptovaluutan, Bitcoinin, käytön haasteisiin anonyymiyden näkökulmasta. Tarkastelen olemassa olevan tutkimustiedon perusteella tarjoaako Bitcoin käyttäjilleen täyttä anonymiteettiä. Tutkimuskysymykseni ovat seuraavat: 1) Tarjoaako Bitcoin käyttäjilleen täyden anonyymiyden? 2) Jos ei, mitä vaihtoehtoja on olemassa, jos käyttäjä pyrkii toimimaan anonyymisti? Toteutan tutkielman kirjallisuuskartoituksena.

Johdantoluvun jälkeen luvussa 2 esitellään tarvittavat taustatiedot Bitcoinin protokollasta, transaktioista sekä lohkoketjuun, louhintaan ja vertaisverkkoon liittyvistä käsitteistä. Luvussa 3 avataan anonymiteetin ja pseudonymiteetin käsitteitä sekä anonymiteettiin liittyviä erityispiirteitä ja ominaisuuksia kryptovaluuttojen viitekehyksessä. Luvussa 4 selvitetään toteutuvatko luvussa 3 esitellyt anonymiteetin ominaisuudet bitcoinia käytettäessä ja käydään läpi eri menetelmiä ja teknologioita, jotka tarjoavat mahdollisuuden anonyyminpään kryptovaluuttojen käyttöön. Luvussa 5 esitellään tutkielman johtopäätökset.

2 Bitcoin

Tämän luvun tarkoituksena on kuvata Bitcoinin peruskäsitteistöä. Aluksi kerrotaan lyhyesti kryptografian ja elektronista viestintää koskevan tutkimuksen taustaa, jonka myötä edetään lopulta Bitcoinin toteutukseen.

David Chaum julkaisi vuonna 1981 artikkelin *"Untraceable electronic mail, return addresses, and digital pseudonyms"*, jonka katsotaan aloittaneen anonyymiä elektronista viestintää koskevan tutkimuksen (Ren ja Wu 2010, s.420). Artikkelissaan Chaum esitteli julkisen avaimen kryptografiseen salaukseen perustuvan tekniikan ja osapuolten välillä toimivan sekoitusprotokollan, joka mahdollistaisi anonyymin sähköpostiviestinnän (D. L. Chaum 1981). Vuonna 1983 Chaum julkaisi artikkelin *"Blind Signatures for Untraceable Payments"*, jossa kuvattiin kryptografinen menetelmä, joka Chaumin mukaan mahdollistaisi jäljittämättömien elektronisten maksujärjestelmien toteuttamisen ja tarjoaisi silloisiin järjestelmiin verrattuna tehostettua tarkastettavuutta ja valvontaa sekä vahvempaa yksityisyyttä (D. Chaum 1983, s.203). Kus Khalilovin ja Levin (2018, s.2543) mukaan Chaumin menetelmä oli ensimmäinen kryptografiaan perustuva digitaalisen rahan konsepti. Chaum kehitti tulevina vuosina konseptiaan ja julkaisi vuonna 1988 yhdessä Amos Fiatin ja Moni Naorin kanssa artikkelin *"Untraceable Electronic Cash"*, jossa esiteltiin *"eCash"* - mikromaksamisjärjestelmän toteutus (Chaum, Fiat ja Naor 1990). Androulakin ym. (2013, s.47) mukaan eCash oli anonyymien luottokorttien lisäksi ensimmäinen yritys määritellä yksityisyyttä suojaavia maksutapahtumia. Chaumin ym. (1990, s.319–320) toteutus tukeutui pankkeihin, jotka varmistivat, ettei kukaan pysty käyttämään rahaa kahteen kertaan. Kus Khalilovin ja Levin (2018, s.2543) mukaan Chaumin menetelmää kehitettiin tulevina vuosikymmeninä alunperin osapuolten välillä toimivien kolmansien osapuolten tarjoamasta keskitetystä luottamuksesta kohti hajautettuja verkkoja.

Vuonna 2008 Nakamoto yhdisteli muun muassa Chaumin alunperin esittämiä menetelmiä ja esitti julkaisussaan systeemin, joka tarjoaisi mahdollisuuden elektronisiin maksutapahtumiin ilman, että se nojautuisi osapuolten väliseen luottamukseen tai mihinkään kolmanteen tahoon osapuolten välillä. Nakamoton julkaisun mukaan luottamus perustuisi maksutapahtumista (*transaktioista*) taltioituihin toisiinsa linkittyviin kryptografisiin todisteisiin, jotka kir-

jattaisiin vertaisverkossa ylläpidettävään jatkuvaan avoimeen elektroniseen tilikirjaan (*lohkoketju*, engl. *blockchain*). Kyseistä tilikirjaa olisi laskennallisesti epäkäytännöllistä väärentää, ellei toistaisi jo tehtyä työtä alusta alkaen uudestaan (Nakamoto 2008, s.1).

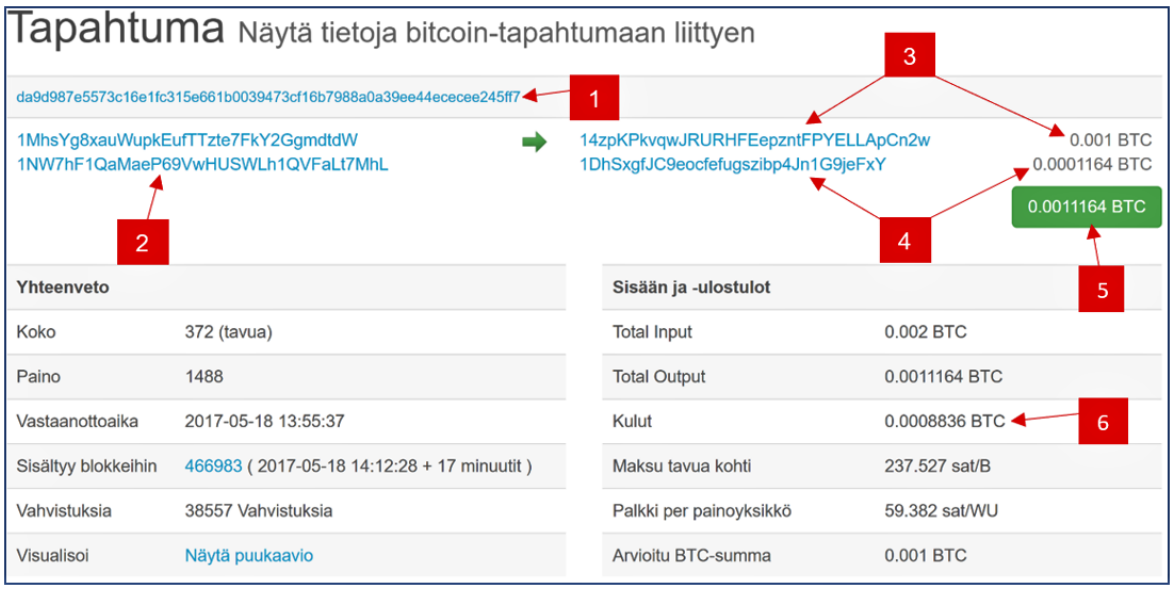
2.1 Transaktiot

Bitcoinin valuuttayksikkö on *bitcoin* ja sen lyhennös on *BTC*. Valuuttayksikön pienintä alayksikköä kutsutaan *satoshiksi* ja yksi bitcoin koostuu sadasta miljoonasta satoshista (0,00000001 BTC). Bitcoinien siirtoa yhdestä osoitteesta toiseen kutsutaan transaktioksi. Transaktiossa voidaan siirtää sekä bitcoineja että satosheja tai molempia.(Kus Khalilov ja Levi 2018, s.2546)

Bitcoinissa käytetään julkisen avaimen kryptografista salausta (Antonopoulos 2014, s.61). Tällä menetelmällä luodaan *yksityinen avain* ja siitä yksisuuntaisella kryptografisella menetelmällä (*elliptic curve multiplication*) johdettu *julkinen avain*, jotka yhdessä muodostavat avainparin, joilla hallinnoidaan bitcoineja (Antonopoulos 2014, s.62–63). Julkista avainta käytetään bitcoinien vastaanottamiseen ja yksityistä avainta bitcoineja lähetettäessä tapahtuvan transaktion varmentamiseen (Antonopoulos 2014, s.62). Antonopouloksen (2014, s.61) mukaan julkinen avain voitaisiin mieltää ikäänkuin perinteiseksi pankkitilin tilinumeroksi ja yksityinen avain olisi tämän tilin salainen tunnusluku. Käytännössä julkisesta avaimesta jalostetaan vielä varsinainen julkisesti näkyvä *bitcoinosoite* käyttämällä yksisuuntaisia kryptografisia SHA-256 (*Secure Hash Algorithm*) ja RIPEMD160 (*RACE Integrity Primitives Evaluation Message Digest*) algoritmeja sekä enkoodaamalla heksaluvuista koostuva lopputulos ihmiselle helpommin luettavaan muotoon Base58 -menetelmällä (Antonopoulos 2014, s.70–75). Käyttäjät voivat hyödyntää erilaisia *lompakkosovelluksia* bitcoinosoitteiden ja yksityisten avainten hallintaan (Kus Khalilov ja Levi 2018, s.2549, Antonopoulos 2014, s.61).

Kus Khalilovin ja Levin (2018, s.2546) mukaan jokainen transaktio sisältää vähintään lähettäjän ja vastaanottajan osoitetiedot sekä tiedot siirrettävästä bitcoinien määrästä. Käyttäjän saldo muodostuu käyttäjän hallussa olevien käyttämättömien bitcoinosoitteiden yhteisarvosta (Kus Khalilov ja Levi 2018, s.2546). Toisin kuin perinteisillä valuutoilla tehtävissä tilisiirroissa, Bitcoinissa käyttäjän lähettäessä bitcoineja toiselle käyttäjälle yksittäisestä

osoitteestaan, hänen täytyy käyttää kaikki osoitteessa olevat varat (Conti ym. 2018, s.3418, Kus Khalilov ja Levi 2018, s.2546). Jos käyttäjällä ei yksittäisessä osoitteessa ole riittävästi bitcoineja, voi hän käyttää useamman hallussaan olevan osoitteen varoja samaan transaktioon. Jos käyttäjällä on yksittäisessä osoitteessa suurempi määrä bitcoineja, kuin mitä hän haluaa käyttää, tulee hänen valita kohde ylijääville bitcoineille. Bitcoinit voidaan osoittaa joko välityspalkkioksi tai siirtää toiselle käyttäjän hallussa olevalle tai varta vasten luodulle uudelle bitcoinosoitteelle (Kus Khalilov ja Levi 2018, s.2546). Androulakin ym. (2013, s.36) ja Herrera-Joancomartin (2015, s.6) julkaisuissa tästä osoitteesta käytettiin vielä nimeä *shadow address*, mutta sittemmin on yleistynyt nimitys *change address* (suom. *vaihto-osoite*) (Meiklejohn ym. 2013, s.131, Conti ym. 2018, s.3441, Kus Khalilov ja Levi 2018, s.3546). Kaikki lohkoketjuun kirjatut transaktiot ovat avoimesti selattavissa sivustoilla kuten *www.blockchain.com*. Kuviossa 1 esitellään sivustolla näkyvään yksittäiseen esimerkkitransaktioon sisältyvät tiedot (S.A. 2019).



Kuvio 1. Yksittäisen esimerkkitransaktion tapahtumatiedot www.blockchain.com -sivustolla: 1. Tapahtuman tunnistenumero, 2. Lähettäjän transaktioon käyttämät bitcoinosoitteet (tässä tapauksessa kaksi kappaletta), 3. Vastaanottajan bitcoinosoite ja vastaanotettujen bitcoinien määrä, 4.Vaihto-osoite ja lähettäjälle palautettujen bitcoinien määrä, 5. Transaktiossa siirrettyjen bitcoinien yhteenlaskettu summa (sisältää vastaanottajalle ja vaihto-osoitteeseen siirretyt määrät), 6. Välityspalkkion summa.

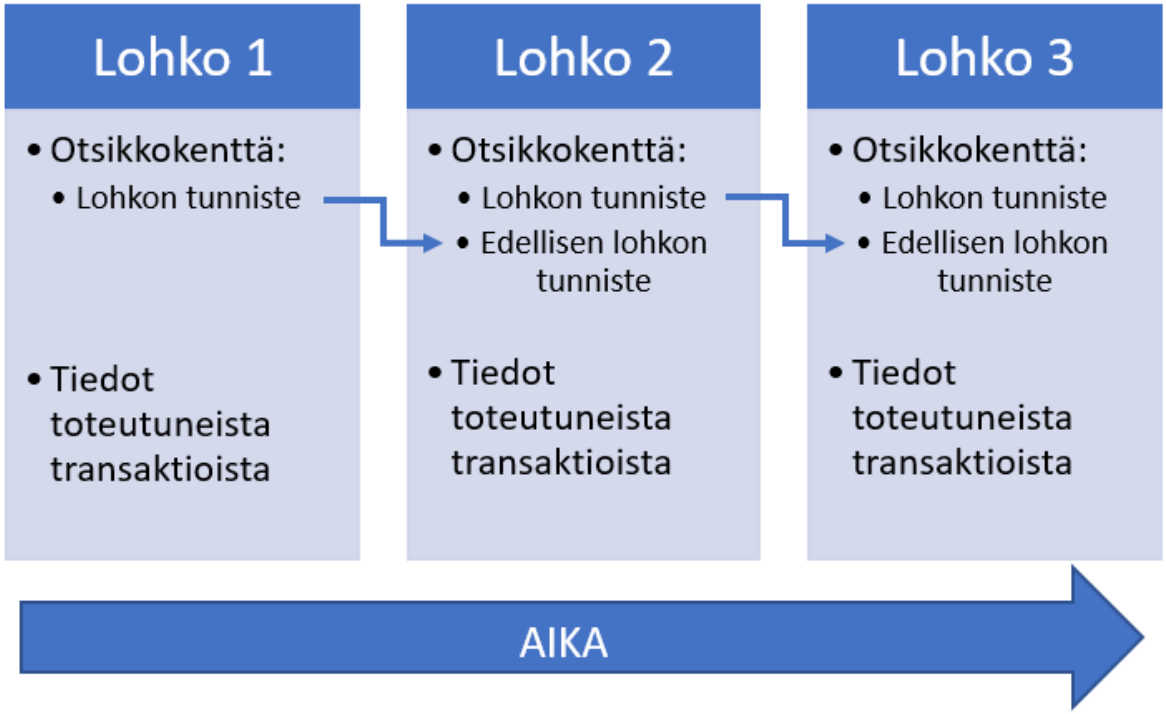
Useiden lähteiden mukaan on suositeltavaa, että jokaisessa transaktiossa luotaisiin uusi vaihto-osoite jäljittämisen heikentämiseksi ja anonymiteetin parantamiseksi (Nakamoto 2008, s.6, Ron ja Shamir 2013, s.9, Kus Khalilov ja Levi 2018, s.2546). Lisäksi asiantuntijoiden mukaan käyttäjälle suositeltavampaa olisi käyttää useita eri lompakkosovelluksia eri käyttötarkoituksiin, sillä eri lompakoiden kautta tehtyjä transaktioita ei pystytä linkittämään toisiinsa (Kus Khalilov ja Levi 2018, s.2549).

2.2 Lohkoketju ja louhinta

Lohkoketju on julkinen, vertaisverkon ylläpitämä tilikirja, johon kirjataan kaikki transaktiot Bitcoinissa. Transaktioiden kirjaaminen lohkoketjuun tapahtuu matemaattisen laskentaprosessin kautta, jota kutsutaan *louhinnaksi* (engl. *mining*). *Louhijoiksi* (engl. *miner*) kutsutaan Bitcoin-verkon käyttäjiä, jotka tarjoavat tietokoneidensa laskentatehoja transaktioiden tarkistamiseen ja lohkoketjuun kirjaamiseen. Vastineeksi tästä työstä he ansaitsevat louhintaprosessin tuloksena järjestelmään luotuja uusia bitcoineja sekä lohkoketjuun lisättyjen transaktioiden välityspalkkioita.(Kus Khalilov ja Levi 2018, s.2544)

Lohkoketju koostuu lohkoista ja lohkot edelleen toteutuneista transaktioista. Jokaisesta transaktiosta lasketaan kryptografinen *tiiviste* (engl. *hash*), eli transaktion tiedot tiivistetään yksilölliseksi hajautusarvoksi, joka toimii transaktion tunnisteena. Transaktiot liitetään pareiksi joista lasketaan taas uusi tiiviste, kunnes lopulta jäljelle jää ainoastaan yksi tiiviste, joka toimii koko lohkon yksilöllisenä tunnisteena (Antonopoulos 2014, s.168 ja Kus Khalilov ja Levi 2018, s.2546). Tätä tunnistetta kutsutaan Ralph Merklen kehittämän kryptografisista tiivisteistä koostuvan tietorakenteen mukaan *Merkle-juureksi* (Merkle 1988). Jokainen lohko sisältää otsikkotiedoissaan sekä edellisen lohkon tunnisteen että oman tunnisteen, joka linkitetään seuraavaan lohkoon luoden näin ajan myötä lohkojen ketjumaisen rakenteen (Kus Khalilov ja Levi 2018, s.2546 ja Antonopoulos 2014, s.189). Kuviossa 2 havainnollistetaan lohkoketjun ketjumaisen rakenteen muodostumista.

Näiden tunnisteiden lisäksi jokaisen lohkon otsikkotietoihin lisätään matemaattisesti helposti todistettavissa oleva sattumanvarainen arvo, joka toimii tositteena siitä, että lohko on todella luotu louhijan toimesta (engl. *nonce value*) (Kus Khalilov ja Levi 2018, s.2547). Louhinta-



Kuvio 2. Lohkoketjussa lohkot muodostavat ketjumaisen rakenteen tunnisteiden avulla.

prosessia käytetään *työtodisteena* (engl. *proof-of-work, PoW*), joka Kus Khalilovin ja Levin (2018, s.2548) mukaan luo käyttäjien kesken yhteisymmärryksen tapahtuneista transaktioista ja siten estää bitcoinien käytön kahteen kertaan. Prosessi voidaan kuvata palapeliksi, jonka ratkaisemiseksi louhijoiden täytyy nähdä aikaa ja vaivaa, mutta lopputulos voidaan todentaa helposti (Kus Khalilov ja Levi 2018, s.2547).

Bitcoin käyttää työtodistealgoritmina Adam Backin alunperin vuonna 1997 esittelemää palvelunestohyökkäysten (engl. *Denial of Service, DoS*) ja roskapostiviestien (engl. *spam*) torjumiseksi luotua työtodistealgoritmia nimeltä *Hashcash* (Back 2002). Louhintaprosessissa louhijat laskevat algoritmin mukaista laskentakaavaa löytääkseen louhittavan lohkon otsikkotiedoille hyväksyttävän tiivistearvon (engl. *hash value*), jolla he pääsevät liittämään lohkon lohkoketjuun (Antonopoulos 2014, s.189–191). Oikean tiivistearvon laskenut louhija lisää lohkon ensimmäiseksi transaktioksi (engl. *generation transaction / coinbase transaction*) itselleen maksettavan palkkion, johon sisältyy järjestelmään uusina bitcoineina syntyneet sekä lohkoon sisältyvien transaktioiden välityspalkkioina olevat bitcoinit (Antonopoulos 2014, s.184).

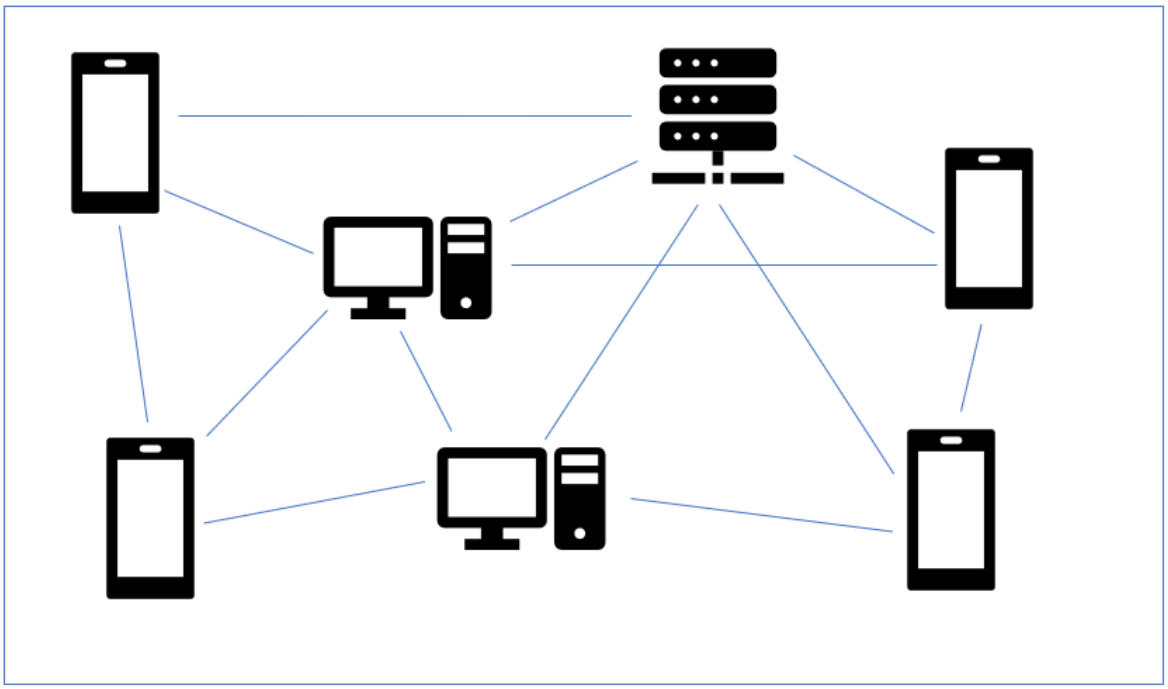
Bitcoin-verkko pyrkii automaattisesti tasapainottamaan lohkoketjuun lisättävien lohkojen määrän siten, että yksi uusi lohko lisätään lohkoketjuun noin joka kymmenes minuutti (Antonopoulos 2014, s.197). Laskentatehon ja käyttäjämäärien muuttuessa tämä tahti saattaa vaihdella, joten jokaisen lohkon otsikkotietoihin asetetaan *vaikeustavoite* (engl. *difficulty target*), joka määrittää hyväksyttävän tiivistearvon ja Bitcoin-verkko säätää automaattisesti tätä vaikeustavoitetta 2016 lohkon välein joko lisäämällä tai vähentämällä sitä riippuen ajasta, joka kyseisten lohkojen louhintaan on kulunut (Antonopoulos 2014, s.189–191 ja 197–198). Käytännössä louhijat laskevat lohkon otsikkotiedoille sopivaa tiivistettä yksi tiivistearvo kerrallaan, muuttamalla aina vähitellen sattumanvaraista arvoa (*nonce value*), kunnes onnistuvat laskemaan vaikeustavoitetta pienemmän tiivisteen lohkolle ja näin liittämään uuden lohkon lohkoketjuun (Antonopoulos 2014, s.189–191). Antonopouloksen (2014, s.193) mukaan oikean tiivistearvon laskeminen on paljon onnesta kiinni ja hän kuvaakin prosessia noppapeliksi, jossa pelaaja heittää kahta noppaa ja yrittää saada noppien yhteisen silmäluvun alle tietyn tavoitearvon. Aluksi tavoitearvoksi asetetaan 12, jolloin tavoitteeseen pääsy on helppoa (kaikki muut heitot pääsevät tavoitteeseen, paitsi heittämällä molemmilla nopilla luvut 6). Pelin jatkuessa tavoitearvoa voidaan laskea, jolloin tavoitearvon alle päästäkseen on pelaajan käytettävä yhä useampia heittoja ja yhä enemmän aikaa onnistuakseen tavoitteessa.

Bitcoinin käyttöönoton aikaan tammikuussa 2009 jokaisen lohkoketjuun liitetyn lohkon louhija sai 50 uutta bitcoinia ja sen jälkeen syntyvien uusien bitcoinien määrä on puolittunut joka 210 000:s lohko. Loppuvuodesta 2012 lukumäärä oli 25 bitcoinia ja vuonna 2016 lukumäärä puolittui taas, asettuen tämänhetkiseen 12,5 bitcoiniin. Järjestelmään on asetettu lopulliseksi bitcoinien määräksi 21 miljoonaa, jonka jälkeen yhtään uutta bitcoinia ei enää synny. Tämän on laskettu toteutuvan noin vuoteen 2140 mennessä, jolloin louhijat tulevat ansaitsemaan työstään palkkaa ainoastaan välityspalkkioiden muodossa. (Antonopoulos 2014, s.175–176 ja 184–186)

2.3 Vertaisverkko

Bitcoin-vertaisverkko muodostuu solmuiksi (engl. *node*) kutsutuista käyttäjien tietokoneista tai palvelimista, joissa on käytössä bitcoin-P2P (*peer-to-peer*) -protokollan mukainen ohjelmisto ja jotka ovat yhteydessä toisiinsa salaamattoman TCP-IP-väylän kautta (Antono-

poulos 2014, s.139–141 ja Kus Khalilov ja Levi 2018, s.2548). Antonopouloksen (2014, s.140–142) mukaan vaikka kaikki solmut todentavat transaktioita ja lohkoja, eroavat ne toisistaan toiminnallisuuksiltaan, kuten esimerkiksi käyttäjän tietokone, joka suorittaa louhintaa, käyttäjän matkapuhelimeen asennettu lompakkosovellus tai koko lohkoketjua ylläpitävä tietokanta. Yksittäinen solmu saattaa sisältää kaikki nämä toiminnallisuudet, mutta yhä yleisempiä käyttäjien keskuudessa ovat matkapuhelimiin asennettavat lompakkosovellukset, jotka eivät sisällä kopiota koko lohkoketjusta ja todentaakseen transaktioita ja lohkoja joutuvat pyytämään viitteitä tarvittaviin lohkoketjun tietoihin muilta solmuilta (Antonopoulos 2014, s.140–141 ja 149–152). Kuviossa 3 havainnollistetaan Bitcoin-vertaisverkon rakennetta.



Kuvio 3. Bitcoin-vertaisverkon rakenne muodostuu solmuiksi kutsutuista laitteista, jotka ovat yhteydessä toisiinsa.

Kus Khalilovin ja Levin (2018, s.2548–2549) mukaan yksittäisellä solmulla voi olla yhteensä enintään 125 samanaikaista yhteyttä ja jokainen solmu tallentaa yhteyksiensä IP-osoitteet luetteloksi itselleen. Näistä yhteyksistä enintään 8 yhteyttä on ulospäin lähtevää ja enintään 117 saapuvia yhteyksiä (Kus Khalilov ja Levi 2018, s.2549). Jos solmu toimii osoitteenmuunnoksen (engl. *Network Address Translation, NAT*) takaa, ei se kykene vastaanottamaan lainkaan saapuvia yhteyksiä vaan ainoastaan muodostamaan enintään 8 ulospäin lähtevää

yhteyttä (Kus Khalilov ja Levi 2018, s.2549).

Kun yksittäinen solmu (tässä tapauksessa louhintaa suorittava) tuottaa uuden lohkon lohkoketjuun, siitä lähetetään ilmoitus kaikille solmun yhteysluettelossa oleville yhteyksille, jotka todentavat lohkon muun muassa sen otsikkorivin tiedoista lasketun tiivisteen, lohkon koon ja aikaleiman sekä lohkon louhijalle maksetun palkkion ja lohkoon sisältyvien transaktioiden oikeellisuuden perusteella (Antonopoulos 2014, s.200–201 ja Kus Khalilov ja Levi 2018, s.2549). Todennuksen tehneet solmut välittävät tiedon uudesta lohkosta kaikille omille yhteyksilleen, kunnes tieto on levinnyt kaikille verkossa oleville solmuille ja samaan aikaan louhintaa jatketaan seuraavan lohkon parissa (Kus Khalilov ja Levi 2018, s.2548–2549). Samoin, kun käyttäjä suorittaa transaktion, häneltä lähtee tieto siitä kaikille hänen yhteyksilleen, jotka todentavat transaktion oikeellisuuden ja välittävät tiedon uudesta transaktiosta omille yhteyksilleen (Kus Khalilov ja Levi 2018, s.2549).

Jokainen solmu ylläpitää jokaista yhteyttään kohden *rangaistuspistelukua*, joka mittaa saapuneiden viallisten yhteysviestien (esimerkiksi TCP-IP tai bitcoin-P2P-protokollaa rikkovat viestit) määrää ja luvun kasvaessa tietyn raja-arvon yli, asetetaan viallisia viestejä lähettäneelle yhteydelle yhteyskielto 24 tunniksi (Kus Khalilov ja Levi 2018, s.2549). Biryukovin ym. (2014, s.18–19 ja 26–27) mukaan tällä mekanismilla pyritään estämään Bitcoin-verkkoon kohdistuvia palvelunestohyökkäyksiä, mutta tutkijat ovat myös osoittaneet, että mekanismia hyödyntämällä voidaan heikentää Bitcoin-verkon käyttäjien anonymiteettiä.

3 Anonymiteetin määritteleminen

Tässä luvussa käydään läpi anonymiteetin ja pseudonymiteetin ero ja esitellään kryptovaluuttoja koskeva anonymiteetin määritelmä. Ensimmäisessä alaluvussa 3.1 kerrataan anonymiteetin klassinen määritelmä ja sen erot pseudonymiteettiin. Alaluvussa 3.2 käydään läpi Amarasinghen, Boyen ja McKaguen (2019, luku 3.1) julkaisussa esitelty kooste anonymiteetin ominaisuuksista kryptovaluuttoja koskien.

3.1 Anonymiteetti ja pseudonymiteetti

Klassisen määritelmän mukaan anonymiteetti koostuu kahdesta ominaisuudesta, tunnistamattomuudesta (engl. *unidentifiability*) ja linkittymättömyydestä (engl. *unlinkability*) (Kelly ym. 2012, s.581). Pfitzmann ja Köhntopp julkaisivat vuonna 2001 artikkelin ”*Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology*”, joka ehdotti näiden termien osalta täsmennystä tietotekniselle tutkimusalalle. Julkaisun mukaan saavuttaakseen anonyymiyden, toimijan täytyy kuulua joukkoon muita toimijoita, joilla on mahdollisesti samoja ominaisuuksia (Pfitzmann ja Köhntopp 2001, s.1). Pfitzmann ja Köhntopp (2001, s.2) määrittelevät anonyymiyden tilaksi, jossa toimija ei ole tunnistettavissa muiden toimijoiden joukosta ja kutsuvat tätä joukkoa *anonymiteettijoukoksi* (engl. *anonymity set*). Heidän mukaansa toimijat voidaan jakaa erillisiin kokonaisuuksiin, kuten lähettäjiin ja vastaanottajiin, jotka muodostavat kaikki oman anonymiteettijoukkonsa (Pfitzmann ja Köhntopp 2001, s.2).

Pfitzmannin ja Köhntoppin (2001, s.2) mukaan anonyymisyys voimistuu sitä myöden, mitä suuremmaksi vastaava anonymiteettijoukko kasvaa ja mitä tasaisemmin tapahtumat anonymiteettijoukon sisällä jakautuvat (esimerkiksi viestien tai maksujen lähettäminen ja vastaanottaminen). Ren ja Wun (2010, s.421) mukaan anonymiteetin aste voidaan laskea jakamalla yksittäisen toimijan osuus koko anonymiteettijoukkoon kuuluvien toimijoiden määrällä (1 / n, missä n on anonymiteettijoukon jäsenten määrä).

Ren ja Wun (2010, s.421) mukaan pseudonymiteetti tarkoittaa salanimien käyttöä tunnisteina. Heidän mukaan toimija on pseudonyymi, jos hän käyttää oman oikean nimensä sijasta pseudonyymiä tunnistetta, kuten nimimerkkiä (Ren ja Wu 2010, s.421). Pseudonyymit tun-

nisteet voivat olla vaihtuvia, toisin kuin toimijan todellinen nimi, joka on oletusarvoisesti muuttumaton (Ren ja Wu 2010, s.421). Pfitzmannin ja Köhntoppin (2001, s.6) mukaan transaktioiden yhteydessä käytettäessä pseudonyymejä tunnisteita, voitaisiin mahdollisimman vahva anonymiteetti saavuttaa käyttämällä jokaista transaktiota kohden eri tunnistetta. Samoin, mikäli samaa tunnistetta käytettäisiin useammassa eri transaktiossa, voitaisiin kaikki nämä transaktiot linkittää kyseiseen tunnisteeseen (Pfitzmann ja Köhntopp 2001, s.5–7).

3.2 Anonymiteetin määritelmä kryptovaluutoissa

Amarasinghe, Boyen ja McKague havaitsivat kirjallisuuskatsauksessaan, että vaikka tieteellisessä tutkimuksessa on mallinnettu kryptovaluuttoja varten uusia anonymiteetin eri puolia käsittäviä ominaisuuksia, tuntuu kryptovaluuttoja koskeva yhtenäinen anonymiteetin viitekehys puuttuvan tieteellisestä tutkimuksesta ja anonymiteetin eri puolia kuvaavia ominaisuuksia on käytetty toisistaan irrallisina eri tutkimuksissa (Amarasinghe, Boyen ja McKague 2019, luku 3.1). Amarasinghe, Boyen ja McKague kokosivat tieteellisissä julkaisuissa esiintyvät kryptovaluuttojen anonymiteetin tarkasteluun käytetyt anonymiteetin ominaisuudet määritelläkseen viitekehyksen kryptovaluuttojen anonymiteetin tarkasteluun. Tässä tutkielmassa käytetään heidän kokoamiaan anonymiteetin ominaisuuksia Bitcoinin anonymiteetin havainnollistamiseen.

Amarasinghen, Boyen ja McKaguen (2019, luku 3.1, ominaisuuksien suomennokset minun) määritelmä anonymiteetistä kryptovaluuttojen viitekehyksessä koostuu seitsemästä anonymiteetin eri puolia kuvaavasta ominaisuudesta: linkittymättömyys (engl. *unlinkability*), vastaanottajan anonymiteetti (engl. *recipient anonymity*), jäljittämättömyys (engl. *untraceability*) tai lähettäjän anonymiteetti (engl. *sender anonymity*), valuutan korvattavuus[1] (engl. *fungibility of a currency*), piilotetut transaktiomäärät (engl. *hidden transaction values*), metadatan linkittymättömyys (engl. *metadata unlinkability*) ja kiellettävyys (engl. *deniability*).

1. MOT Englanti sanakirjan suomennosta englanninkielen termistä ”fungible” (”korvattava”) käytetään tässä yhteydessä puhuttaessa valuutoista (*MOT Englanti* 2019). Jyväskylän Yliopistolla tehdyssä selvitystyössä termin ”fungible” merkitys on määritelty ”Korvattava/vaihdettava/lajiesine. Esimerkiksi valuutat ovat korvattavia, koska kaksi kahdenkymmen euron seteliä ovat yhtä arvokkaita maksuvälineitä keskenään, vaikka niillä on eri sarjanumero.” (Mahlberg ja Hyytiäinen 2019, s.2).

Kuviossa 4 esitellään nämä ominaisuudet tarkemmin.

Anonymiteetin ominaisuuksien lisäksi Amarasinghen, Boyen ja McKague katsovat, että anonymiteetin astetta voitaisiin mitata kolmella eri arvolla. Nämä arvot ovat anonymiteettijoukon koko, transaktion prosessoimiseen kuluva aika ja transaktiolohkon koko (Amarasinghe, Boyen ja McKague 2019, luku 3.2).

Kus Khalilov ja Levi (2018, s.2545) toteavat julkaisussaan, että täyden anonymiteetin saavuttaminen on vaikeaa. Useat julkaisut pitävät lohkoketjun julkisen luonteen vuoksi Bitcoinia pseudonyyminä järjestelmänä (Androulaki ym. 2013, s.34, Meiklejohn ym. 2013, s.127, Conti ym. 2018, s.3418, Kus Khalilov ja Levi 2018, s.2549, Amarasinghe, Boyen ja McKague 2019, luku 2.1). Androulakin ym. (2013, s.34) mukaan lohkoketjun avoimuus ja sen myötä transaktioiden julkisuus aikaleimoineen sekä arvoineen on herättänyt huolta käyttäjien yksityisyydestä ja Conti ym. (2018, s.3446, suomennos minun) toteavatkin laajassa kirjallisuuskartoituksessaan, että ”...Bitcoin on kaikkea muuta kuin yksityinen”. Herrera-Joancomartín (2015, s.8) mukaan internetin ei-anonyymi infrastruktuuri yhdistettynä lohkoketjun avoimuuteen on osoittautunut uhkaksi anonyymiydelle ja Kus Khalilov ja Levi (2018, s.2545) pitävätkin metadataa, kuten IP-osoitteita ja transaktiotapahtumien lokitietoja yhtenä suurimmista todellisen anonymiteetin estävistä tekijöistä. Kus Khalilovin ja Levin (2018, s.2545) mukaan metadatan analyyttinen ja kokonaisvaltaisella lähestymistavalla tehty käsittely saattaa johtaa bitcoinosoitteiden takana olevien todellisten identiteettien jäljille.

Kuvio 4. Anonymiteetin ominaisuudet kryptovaluuttojen viitekehyksessä.

4 Bitcoinin käyttö anonyymisti

Tässä luvussa tarkastellaan tarjoaako Bitcoin käyttäjilleen edellisessä luvussa esiteltyjä anonymiteetin ominaisuuksia sekä tulevissa alaluvuissa käydään läpi anonymiteetin parantamiseen ehdotettuja ratkaisuja sekoitusprotokollien (alaluku 4.1), kryptografisten vaihtoehtojen (alaluku 4.2) ja näitä yhdistelevien tekniikoiden (alaluku 4.3) muodossa. Anonymiteetin ominaisuudet käydään seuraavaksi läpi yksitellen ja ominaisuuksien toteutumista arvioidaan olemassa olevan tutkimustiedon perusteella. Linkittymättömyys sekä vastaanottajan ja lähettäjän anonymiteetti käsitellään yhtenä kokonaisuutena, koska ne nivoutuvat toisiinsa läheisesti ja lisäksi tutkimukset, joissa niiden ilmentyvyyttä käsitellään, koskettavat usein kaikkia kolmea ominaisuutta.

Linkittymättömyys, **vastaanottajan anonymiteetti** ja **lähettäjän anonymiteetti**: Reid ja Harrigan (2013, s.204–210) muodostivat vuonna 2013 julkaistussa tutkimuksessaan lohkoketjusta kaksi verkkorakennetta: *transaktioverkon* ja *käyttäjäverkon*. Molemmat verkkorakenteet kuvastavat bitcoinien maksuvirtaa suhteessa aikaan; transaktioverkko transaktioiden välillä ja käyttäjäverkko käyttäjien välillä (Reid ja Harrigan 2013 s.204–210). Reid ja Harrigan (2013, s.206) jalostivat käyttäjäverkon soveltamalla transaktioverkon tietoihin menetelmää, jonka mukaan jokaisen transaktion lähettävänä osapuolena olevat bitcoinosoitteet kuuluvat samalle taholle. Alunperin tämän toiminnon huomioi jo Nakamoto omassa julkaisussaan (Nakamoto 2008, s.6). Reid ja Harrigan (2013, s.212 ja 221) osoittivat myös, että yhdistelemällä käyttäjäverkkoon avoimista lähteistä saatavia tietoja, voidaan käyttäjiä tunnistaa ja heidän aktiivisuuttaan tutkia tarkasti.

Dorit Ron ja Adi Shamir julkaisivat vuonna 2013 kvantitatiivisen analyysin koko silloisesta Bitcoinin lohkoketjusta. Osoittaakseen kuinka lohkoketjua voidaan käyttää yksilöiden tai organisaatioiden rahavirtojen analysointiin, he linkittivät WikiLeaksin lahjoituksia varten mainostamaan bitcoinosoitteeseen joukon muita WikiLeaksin omistuksessa olevia bitcoinosoitteita (Ron ja Shamir 2013, s.10). Analyysissään he osoittivat, että WikiLeaksille kuuluu vähintään 83 bitcoinosoitetta, jotka ovat olleet osallisina yhteensä 1088 transaktiossa ja muodostavat kokonaisuudessaan 2605,25 bitcoinin omaisuuden (Ron ja Shamir 2013, s.10).

Meiklejohn ym. (2013, s.131–133) käyttivät vuonna 2013 ilmestyneessä julkaisussaan *uudelleentunnistushyökkäystä* (engl. *re-identification attack*) ja *vaihto-osoiteanalyysiä* linkittääkseen bitcoinosoitteita samoille tahoille. Heidän mukaansa tiettyjen arvojen perusteella voidaan transaktiossa näkyvistä vastaanottavista osoitteista todeta yhden olevan lähettäjälle kuuluva vaihto-osoite (Meiklejohn ym. 2013, s.131–133). Uudelleentunnistushyökkäyksessä Meiklejoh ym. asioivat tunnettujen vaihdantapalvelujen ja palveluntuottajien kanssa ja saivat näin varmistettua tietyt osoitteet kuuluviksi näille palveluille (Meiklejohn ym. 2013, s.130). Käyttämällä vaihto-osoiteanalyysiä näihin todennettuihin osoitteisiin, he pystyivät nimeämään samoille tahoille 1600-kertaisesti suuremman määrän uusia osoitteita jo tunnettujen osoitteiden lisäksi (Meiklejohn ym. 2013, s.133–134).

Androulaki ym. (2013) toteuttivat ensimmäisinä käyttäytymiseen perustuvilla KMC (*K-Means*) ja HAC (*Hierarchical Agglomerative Clustering*) -algoritmeilla toteutetun bitcoinosoitteiden ryhmittelyanalyysin (Kus Khalilov ja Levi 2018, s.2558). Androulaki ym. (2013, s.42–43) toteuttivat tutkittavan datan keruuta varten yliopistoympäristössä toimivan Bitcoinin päivittäiskäyttöä kuvaavan simulaation. Analyysin tuloksena he onnistuivat kokoamaan 40 prosenttia käyttäjäprofiileista ryhmittelemällä bitcoinosoitteita perustuen transaktioiden ajankohtaan, siirrettyjen bitcoinien määrään sekä erittelemällä lähettäjät ja vastaanottajat (Androulaki ym. 2013, s.42 ja 47).

Valuutan korvattavuus: Contin ym. (2018, s.3440) laajassa kirjallisuuskatsauksessa todetaan, että Bitcoinin transaktiohistorian läpinäkyvyys ja jäljitettävyys asettavat riskin valuutan korvattavuudelle. Böhmen ym. (2015, s.228) mukaan lohkoketjun julkisuuden vuoksi jokaisen bitcoinin transaktiohistoria voitaisiin jäljittää ja esimerkiksi anastettujen tai rikollista alkuperää olevien bitcoinien jälleenmyynti voitaisiin yrittää estää asettamalla yleisesti saataville ”mustalista”, jota muu yhteisö seuraisi ja kieltäytyisi vastaanottamasta maksuja listalle lisätyistä bitcoinosoitteista. Böhmen ym. mukaan ”mustienlistojen” laaja käyttö voisi heikentää bitcoinien korvattavuutta ja listojen käyttöönotto jakaakin mielipiteitä Bitcoin-yhteisössä (Böhme ym. 2015, s.228).

Piilotetut transaktiomäärät: Lohkoketjun julkisuuden myötä kaikki transaktiot Bitcoinissa ovat näkyvillä ja transaktiot sisältävät siirrettyjen bitcoinien määrät (Kus Khalilov ja Levi 2018, s.2578). Transaktiomääriä on käytetty esimerkiksi käyttäytymismalleihin perustu-

vien ryhmittelyalgoritmien muuttujina (Androulaki ym. 2013, s.42). Kus Khalilovin ja Levin (2018, s.2578) mukaan piilotetut transaktiomäärät saattaisivat johtaa tilanteeseen, jossa systeemin sisällä olevien varojen kokonaismäärää ei pystyttäisi laskemaan eikä valvomaan ja siten koko systeemin eheys olisi vaarassa.

Metadatan linkittymättömyys: Koshy ym. (2014) toteuttivat ensimmäisinä tutkimuksen, jossa linkitettiin bitcoinosoitteita IP-osoitteisiin (Kus Khalilov ja Levi 2018, s.2552). Koshy ym. (2014, s.473) kehittivät tutkittavan datan keruuseen Bitcoin-asiakasohjelman nimeltä *CoinSeer*, joka keräsi dataa oikeasta Bitcoin-verkosta heinäkuusta 2012 vuoden 2013 tammikuulle saakka muodostamalla yhteyksiä mahdollisimman moniin Bitcoin-käyttäjiin ja havainnoimalla transaktioverkon liikennettä. Koshy ym. (2014, luku 6) havaitsivat saadussa datassa selviä transaktioiden välittämiseen liittyviä kaavoja ja kehittivät menetelmiä näiden kaavojen tulkitsemiseen. Lopuksi Koshy ym. (2014, s.481 ja 483) pystyivät linkittämään jopa yli tuhat bitcoinosoitetta niitä vastaaviin IP-osoitteisiin yli 99 prosentin todennäköisyydellä. Tutkijat tiedostivat, että heidän käyttämissään menetelmissä on myös rajoituksia. Esimerkiksi verkkoliikennettä anonymisoivia TOR- (*The Onion Router*) tai I2P- (*The Invisible Internet Project*) välityspalvelimia käyttävät käyttäjät tai erilaisten lompakko-sovellusten kautta toimivat käyttäjät olisi heidän menetelmillään yhdistetty väärin, sillä näiden palveluiden kautta toimiviin käyttäjiin ei pystytty muodostamaan suoraa yhteyttä (Koshy, Koshy ja McDaniel 2014, s.483).

Biryukov ym. (2014, s.26) toteuttivat simuloidun *deanonymisointihyökkäyksen* osoittaakseen, että käyttäjien IP-osoitteita voidaan linkittää heidän hallitsemiinsa bitcoinosoitteisiin. Myös he kehittivät tutkimustaan varten oman Bitcoin-asiakasohjelman, joka loi TCP-IP-väylän kautta yhteyksiä muihin verkossa oleviin käyttäjiin ja tämän jälkeen havainnoi verkon liikennettä ja kartoitti muiden käyttäjien julkaisemia transaktioita heidän IP-osoitteisiinsa (Biryukov, Khovratovich ja Pustogarov 2014, s.26). Toisin kuin Koshyn ym. tutkimuksessa, Biryukov ym. (2014, s.21) eivät toteuttaneet hyökkäystään oikeassa Bitcoin-verkossa, eettisiin syihin vedoten. Biryukovin ym. (2014, s.16 ja 22) mukaan ratkaiseva havainto tutkimuksessa oli se, että käyttäjä voidaan yksilöidä NAT-IP osoitteen takaa hänen muodostamiensa ulospäin lähtevien yhteyksien (maksimissaan 8 kappaletta) kautta. He osoittivat tutkimuksessaan myös sen, että Bitcoin-verkon sisäänrakennettua palvelunestohyökkäystor-

juntamekanismia voidaan käyttää estämään anonymisoivien välityspalvelinten (esimerkiksi TOR tai I2P) käyttö koko verkon laajuisesti (Biryukov, Khovratovich ja Pustogarov 2014, s.18–19 ja 26–27). Useamman kuukauden simuloidun deanonymisointihyökkäyksen tuloksena Biryukov ym. (2014, s.20 ja 28) totesivat, että vuokraamalla 50 palvelinta käyttääkseen eri IP-osoitteita, hyökkääjä pystyisi halutessaan pitäytyä huomaamattomana ja kykenisi silti tunnistamaan oikeassa Bitcoin-verkossa vähintään 11 prosenttia kaikkien tapahtuvien transaktioiden IP-osoitteista. Kustannukset tämän hyökkäyksen jatkuvaan toteutukseen olisivat maksimissaan 1500 euroa kuukaudessa (Biryukov, Khovratovich ja Pustogarov 2014, s.28).

Kiellettävyys: Saxenan, Misran ja Dharin mukaan transaktiotapahtuma toimii pysyvänä linkkinä lähettävän ja vastaanottavan osoitteen välillä ja kryptografisena tositteena lähetetyistä varoista, joten lähettäjä ei voi myöhemmin kieltää lähettäneensä varoja vastaanottajalle (Saxena, Misra ja Dhar 2014, s.133).

Tutkimustiedon perusteella vaikuttaisi siltä, ettei Bitcoin oletusarvoisesti tarjoa käyttäjilleen yhtäkään yllä läpikäydyistä anonymiteetin ominaisuuksista. Amarasinghen, Boyen ja McKaguen (2019, luku 3.3) mukaan Bitcoinin ja muiden kryptovaluuttojen anonymiteetin parantamiseen on tehty monia ratkaisuehdotuksia, joista osa perustuu raskaisiin salaustekniikoihin ja toiset keskittyvät enimmäkseen maksutapahtumien sekoittamiseen jäljittämisen vaikeuttamiseksi. Osa ratkaisuista on toteutettu hajautetulla rakenteella, toiset taas toimivat keskitetysti ja osa on käyttöönotettu suoraan parannuksina Bitcoinin protokollaan ja toiset taas ovat johtaneet täysin uusien kryptovaluuttojen syntyyn (Amarasinghe, Boyen ja McKague 2019, luku 3.3). Kus Khalilovin ja Levin (2018, s.2578) mukaan anonymiteettiä ja yksityisyyttä lisäävien menetelmien myötä myös vaatimus luottaa itse systeemiin kasvaa. Haasteeksi heidän mukaan muodostuukin, että käyttäjät toivovat systeemin tarjoavan yksityisyyttä ja anonyymiyttä, mutta kokevat vaikeaksi luottaa sellaiseen systeemiin (Kus Khalilov ja Levi 2018, s.2578).

Seuraavissa kolmessa alaluvussa käydään läpi näiden ratkaisuiden tarjoamia mahdollisuuksia käyttää kryptovaluuttoja anonyymimmin. Tutkielman rajauksen vuoksi yksittäisiä ratkaisuja ei esitellä yksityiskohtaisesti, vaan ratkaisutekniikat ja teknologiat esitellään pääpiirteissään sekä niiden tarjoamia vahvuuksia ja heikkouksia käydään läpi siten, että voidaan muodostaa yleiskuva kyseisen vaihtoehdon tarjoamista eduista ja riskeistä.

4.1 Sekoitusprotokollat

Amarasinghen, Boyen ja McKaguen (2019, luku 3.4) mukaan yksinkertaisin ratkaisu anonymiteetin ongelmaan on sekoittaa käyttäjien bitcoineja tai transaktioita muiden käyttäjien bitcoineihin tai transaktioihin. Kus Khalilovin ja Levin (2018, s.2565) mukaan vuonna 2013 bitcointalk -keskustelufoorumilla julkaistu ”*CoinJoin: Bitcoin privacy for the real world*” -kirjoitus oli ensimmäinen, joka kuvasi tämän tyyppistä ratkaisua anonymiteetin parantamiseen. Sittemmin CoinJoin-protokolla on yleisesti hyväksytty ja sitä voidaan hyödyntää joko hajautetulla tai keskitetyllä tavalla (Kus Khalilov ja Levi 2018, s.2565).

Hajautetussa toteutuksessa ainoastaan maksutapahtumaan osallistuvat käyttäjät tietävät toistensa transaktiossa olevat lähtö- ja tulo-osoitteet, eikä ulkopuolisia osapuolia osallistu transaktiotapahtuman toteuttamiseen. Käyttäjät sopivat itsenäisesti toisten käyttäjien kanssa maksutapahtumiensa yhdistämisestä CoinJoin-protokollaa hyödyntäen. Asiantuntijoiden mukaan sekoitustapahtumassa on tärkeää käyttää yhdenmukaisia siirrettäviä summia anonymiteetin parantamiseksi, sillä toisistaan poikkeavia summia voitaisiin helposti poimia maksuvirrasta ja yhdistellä lähtö- ja tulo-osoitteisiin. (Kus Khalilov ja Levi 2018, s.2565)

Keskitetyssä sekoitustapahtumassa käyttäjä lähettää halutun määrän bitcoineja kolmannen osapuolen tarjoamalle palvelulle ja palvelu sekoittaa bitcoinit muiden käyttäjien bitcoineihin ja lopuksi palauttaa tuoreesta bitcoinosoitteesta varat takaisin käyttäjälle. Käytännössä käyttäjä lähettää siirrettävän summan palvelulle sekoitustapahtuman ajaksi, joten käyttäjien täytyy pystyä luottamaan palvelua tarjoavan tahon rehellisyyteen. Lisäksi palvelut saattavat pitää lokikirjaa sekoitustapahtumiin osallistuvista käyttäjistä, joten heidän on mahdollista linkittää käyttäjät lähtö- ja tulo-osoitteisiin. (Kus Khalilov ja Levi 2018, s.2550 ja 2565)

Osassa tapauksista, joissa tutkijat ovat käyttäneet sekoituspalveluja, ovat sekoituspalvelua tarjoavat tahot osoittautuneet huijauksiksi. Meiklejohn ym. (2013, s.130) lähettivät tutkimuksensa aikana bitcoineja sekoitettavaksi muun muassa *BitMix* -sekoituspalveluun, joka varastikin heidän lähettämänsä bitcoinit. Lisäksi *Bitcoin Laundry* -palvelu lähetti heidän lähettämänsä samat bitcoinit kaksi kertaa takaisin, menettäen sekoituspalvelun käytön merkityksen (Meiklejohn ym. 2013, s.130).

Anonyymiyden taso sekoitustapahtumassa nousee sitä mukaa, mitä enemmän käyttäjiä ja sa-

mansuuruisia summia tapahtumaan liitetään (Amarasinghe, Boyen ja McKague 2019, luku 3.4). Amarasinghen, Boyen ja McKaguen (2019, luku 3.4) mukaan vaikka sekoitusprotokollien käyttö lisääkin hiukan anonyymiyttä vaikeamman jäljitettävyyden ja linkitettävyyden myötä, niiden käytöllä on useita riskejä sekä rajoituksia anonyymiyden suhteen. Tällaisia ovat esimerkiksi usein keskitetysti tehty toteutus ja tarve luottaa siihen, että palvelua tarjoava taho palauttaa lähetetyt bitcoinit takaisin käyttäjälle sekoitustapahtuman jälkeen (Amarasinghe, Boyen ja McKague 2019, luku 3.4). Asiantuntijoiden mukaan sekoituspalvelut tarjoavat sekoitustapahtumia usein ainoastaan tietyn nimellisarvon summille ja ovatkin tehokkaita ainoastaan pienten summien jälkien peittämiseen (Amarasinghe, Boyen ja McKague 2019, luku 3.4 ja Kus Khalilov ja Levi 2018, s.2550). Sekoitusviiveiden vuoksi myös transaktioajat pitenevät ja suurten summien siirtäminen on tehotonta ja helposti jäljitettävissä (Amarasinghe, Boyen ja McKague 2019, luku 3.4 ja Kus Khalilov ja Levi 2018, s.2550).

4.2 Kryptografiset vaihtoehdot

Sekoitusprotokollien rajoitukset anonyymiyden suhteen sekä epärehellisten sekoituspalveluiden riskit ovat johtaneet anonyymiyteen pyrkivien toteutusten suunnittelua ja alaan liittyvää tutkimusta kryptografisten vaihtoehtojen suuntaan (Amarasinghe, Boyen ja McKague 2019, luku 3.5).

Kryptovaluutat kuten Zerocoin, ZeroCash ja Zcash tarjoavat vahvaan kryptografiaan, kuten ZKP- (*zero-knowledge proof*), zk-SNARK- (*zero-knowledge Succinct Non-interactive Arguments of Knowledge*) ja DAP- (*Decentralised Anonymous Payment*) protokolliin perustuvaa salausta liittyen transaktioiden varmistamiseen paljastamatta kyseistä transaktiota muille (ZKP ja zk-SNARK) sekä mahdollisuutta suorittaa maksuja suoraan käyttäjien välillä paljastamatta lähettäjää, vastaanottajaa tai siirrettyä summaa (DAP). Näiden raskasta kryptografiaa hyödyntävien kryptovaluuttojen toteutuksissa ei kuitenkaan ole toteutettu käyttäjien IP-osoitteiden piilottamista ja lisäksi laskennallisesti raskaan salauksen toteutus hidastaa järjestelmän suorituskykyä. (Amarasinghe, Boyen ja McKague 2019, luku 3.5)

Vuonna 2013 julkaistu CryptoNote-protokolla mahdollistaa Bitcoin-protokollaan verrattuna joustavasti useiden eri ominaisuuksien lisäämisen (Amarasinghe, Boyen ja McKague 2019,

luku 3.5). CryptoNoten joustavuutta ollaan hyödynnetty monissa anonyymiyteen pyrkivissä kryptovaluutoissa, kuten ByteCoin, DigitalNote, DarknetCoin, Aeon ja Monero (Amarasinghe, Boyen ja McKague 2019, luku 3.5). Amarasinghen, Boyen ja McKaguen (2019, luku 3.5) mukaan näistä vahvimman anonymiteetin omaava kryptovaluutta on Monero, joka piilottaa lähettäjän tiedot transaktioista käyttämällä *ring signatures* -salausta ja kertakäyttöisiä vaihto-osoitteita (tunnetaan Monerossa nimellä *stealth address*) piilottaakseen vastaanottajan sekä *Ring Confidential Transactions (Ring CT)* -salausta piilottaakseen siirrettävät summat. Kumar ym. (2017, s.156) julkaisivat Moneron jäljitettävyyttä analysoivan tutkimuksen, joka käytti aineistona Moneron koko silloista lohkoketjua (huhtikuulta 2014 helmikuulle 2017). Julkaisun mukaan ensimmäiset Ring CT -salausta hyödyntävät transaktiot löytyivät lohkoketjusta tammikuulta 2017 ja niiden käyttö oli vielä vuonna 2017 käyttäjille vapaaehtoista (Kumar ym. 2017, s.155-156). Tutkimuksessa kehitettiin kolme eri hyökkäysvektoria ja tutkijat onnistuivat jäljittämään 88 % tutkittavista Moneron transaktioista, jotka eivät hyödyntäneet Ring CT -salausta (Kumar ym. 2017, s.155-156, 160-161 ja 171).

4.3 Yhdistelmätekniikat

On tiedossa, että sekoitusprotokollissa sekä kryptografisissa vaihtoehdoissa on molemmissa omat rajoituksensa täyden anonyymiyden saavuttamisessa. Viimeaikaisissa julkaisuissa ollaankin ehdotettu näiden kahden lähestymistavan parhaita puolia yhdisteleviä ratkaisuja (Amarasinghe, Boyen ja McKague 2019, luku 3.6).

Kus Khalilovin ja Levin (2018, s.2574) mukaan puhtaasti osoitteiden sekoittamiseen keskittyvät CoinJoin -tyyppiset sekoitusprotokollat eivät sisällä minkäänlaista kryptografista salausta, joten ne ovat usein vasteajaltaan nopeimpia menetelmiä. Näihin sekoitusprotokolliin yhdistettäessä myös kryptografisia salausmenetelmiä, kuten Chaumin vuonna 1983 esittelemä ”*blind signature*”, voidaan sekoitustapahtumaan osallistuvien käyttäjien lähtö- ja tulo-osoitteet peittää myös sekoituspalvelua tarjoavalta taholta (Kus Khalilov ja Levi 2018, s.2565). Kyseistä salausta voidaan käyttää yhdessä sekoitusprotokollien kanssa myös ilman käyttäjien välillä toimivaa kolmatta osapuolta, jolloin sekoitustapahtumaan osallistuvien käyttäjien lähtö- ja tulo-osoitteet eivät paljastu edes tapahtumaan osallistuville käyttäjille (Kus Khalilov ja Levi 2018, s.2567).

Useat yhdistelmätekniikat, kuten CoinJoin sekoitusprotokollaa ja transaktioiden summat piilottavaa *CT* (*Confidential Transactions*) -salausta hyödyntävä *ValueShuffle* ovat saavuttaneet asiantuntijoiden mukaan hyväksyttävän tason linkittymättömyyden ja jäljittämättömyyden suhteen, mutta esimerkiksi IP-osoitteiden linkittymättömyyttä ei ole täysin saavutettu ja useat tutkimukset ovatkin ehdottaneet verkkoliikennettä anonymisoivien viestintäkanavien, kuten TOR:in käyttöä (Amarasinghe, Boyen ja McKague 2019, luku 3.6). Kryptovaluutat kuten Stealthcoin ja Anoncoin tarjoavat käyttäjilleen sisäänrakennettuna ominaisuutena TOR -palvelun kautta kulkevan anonymisoidun verkkoliikenteen ja Anoncoin tarjoaa lisäksi tuen myös verkkoliikenteen salaavalle I2P -palvelulle (Kus Khalilov ja Levi 2018, s.2564). TOR-palvelun kautta verkkoliikennettään ohjaavat käyttäjät eivät kuitenkaan ole täysin turvassa, kuten Biryukov ym. (2014, s.18–19 ja 26–27) tutkimuksessaan osoittivat ja Amarasinghen, Boyen ja McKaguen (2019, luku 3.5) mukaan myös Moneron transaktioissa olevia osoitteita saattaisi olla mahdollista linkittää käyttäjien IP-osoitteisiin.

Myös IP-osoitteiden linkittymättömyyttä ja transaktioiden jäljittämättömyyttä tarjoavia ratkaisuja ollaan kehitetty, kuten vuonna 2017 ehdotettu *salamaverkko* (engl. *Lightning Network*) sekä Moneron omaa verkkoliikennettä anonymisoiva maksukanava nimeltä *Kovri*. Salamaverkon taustalla toimii menetelmä nimeltä *BOLT* (*Blind Offchain Light-weight Transactions*), joka tarjoaa osittain lohkoketjun ulkopuolelle tallennettavia transaktioita anonymisoivia maksukanavia käyttäjien välille ja Moneron Kovri peittäisi käyttäjän IP-osoitteen transaktioissa. (Amarasinghe, Boyen ja McKague 2019, luvut 3.5 ja 3.6)

Suurin osa kryptovaluutoista on keskittynyt parantamaan linkittymättömyyttä, vastaanottajan anonymiteettiä ja jäljittämättömyyttä (Amarasinghe, Boyen ja McKague 2019, luku 4.1). Hyvin harvat toteutukset tarjoavat kuitenkaan ratkaisuja metadatan linkittymättömyyden, valuuttojen korvattavuuden ja käyttäjien kiellettävyyden parantamiseksi (Amarasinghe, Boyen ja McKague 2019, luku 4.1). Amarasinghen, Boyen ja McKague (2019,luvut 3.6 ja 5) toteavat kirjallisuuskatsauksensa tuloksena, että kokonaisuudessaan yhtä ainoaa toteutusta, joka tarjoaisi kaikkiin anonymiteetin ominaisuuksiin ratkaisun, ei vielä näytä olevan.

5 Yhteenveto

Tutkielmassa toteutettiin kirjallisuuskartoitus kryptovaluuttojen anonymiteetin haasteita käsitteleviin julkaisuihin. Tutkielma keskittyi ensimmäisen ja suosituimmaksi nousseen kryptovaluutan, Bitcoinin, käyttäjilleen tarjoaman anonymiteetin tarkasteluun. Tutkielman alussa asetetut tutkimuskysymykset olivat seuraavat: Tarjoaako Bitcoin käyttäjilleen täyden anonyymiyden? Jos ei, mitä vaihtoehtoja on olemassa, jos käyttäjä pyrkii toimimaan anonyymisti? Aihetta työstäessä kävi selväksi, että kryptovaluuttojen anonyymiyttä koskevien tutkimusten käyttämät näkökulmat kokonaisvaltaisesta anonyymiydestä ovat vaihtelevia ja niiden kattavuus eroaa tutkimuksesta toiseen. Selkeän lähtökohdan asettamiseksi tutkielmassa käytettiin anonymiteetin määritelmää, jonka ollaan yleisesti katsottu kattavan kryptovaluuttoja koskevan anonymiteetin eri osa-alueet. Näiden seitsemän ominaisuuden kautta tarkastellessa on selvää, että tutkimusten mukaan Bitcoin ei tarjoa käyttäjilleen anonymiteettiä. Tutkielmassa käytiin läpi myös eri menetelmien, kuten sekoitusprotokollien, raskasta kryptografiaa hyödyntävien salausmenetelmien sekä näitä yhdistelevien tekniikoiden tarjoamia vaihtoehtoja käyttää kryptovaluuttoja anonyymimmin. Useat menetelmät tarjoavat ainoastaan muutamiin eri anonymiteetin ominaisuuksiin ratkaisuja, mutta yhtä toteutusta, joka tarjoaisi kaikkiin seitsemään ominaisuuteen ratkaisun, ei vaikuta tulosten perusteella vielä olevan.

Tutkimuksista suurin osa vaikuttaa pitävän pyrkimystä anonyymiyteen jonkinlaisena itseisarvoisena tavoitteena. Jään mielenkiinnolla seuraamaan lisäpohdintaa, mitä hyviä ja huonoja seurauksia kokonaisvaltainen anonymiteetti kryptovaluuttojen maailmassa saattaisi aiheuttaa ja minkälaisia maailmanlaajuisia vaikutuksia tästä voisi seurata.

Lähteet

Amarasinghe, Niluka, Xavier Boyen ja Matthew McKague. 2019. “A Survey of Anonymity of Cryptocurrencies”. Teoksessa *Proceedings of the Australasian Computer Science Week Multiconference,* 2:1–2:10. ACSW 2019. Sydney, NSW, Australia: ACM. ISBN: 978-1-4503-6603-8. doi:10.1145/3290688.3290693.

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer ja Srdjan Capkun. 2013. “Evaluating User Privacy in Bitcoin”. Teoksessa *Financial Cryptography and Data Security,* toimittanut Ahmad-Reza Sadeghi, 34–51. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-39884-1.

Antonopoulos, Andreas M. 2014. *Mastering Bitcoin: unlocking digital cryptocurrencies.* "O’Reilly".

Back, Adam. 2002. “Hashcash — A Denial of Service CounterMeasure”. http://www.hashcash.org/hashcash.pdf. (Haettu: 12.06.2019).

Böhme, Rainer, Nicolas Christin, Benjamin Edelman ja Tyler Moore. 2015. “Bitcoin: Economics, Technology, and Governance”. *Journal of Economic Perspectives* 29, numero 2 (toukokuu): 213–38. doi:10.1257/jep.29.2.213.

Biryukov, Alex, Dmitry Khovratovich ja Ivan Pustogarov. 2014. “Deanonymisation of Clients in Bitcoin P2P Network”. Teoksessa *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* 15–29. CCS ’14. Scottsdale, Arizona, USA: ACM. ISBN: 978-1-4503-2957-6. doi:10.1145/2660267.2660379.

Chaum, David. 1983. “Blind Signatures for Untraceable Payments”. Teoksessa *Advances in Cryptology,* toimittanut David Chaum, Ronald L. Rivest ja Alan T. Sherman, 199–203. Boston, MA: Springer US. ISBN: 978-1-4757-0602-4. doi:10.1007/978-1-4757-0602-4_18.

Chaum, David L. 1981. “Untraceable electronic mail, return addresses, and digital pseudonyms”. *Communications of the ACM* 24 (2): 84–90.

Chaum, David, Amos Fiat ja Moni Naor. 1990. “Untraceable Electronic Cash”. Teoksessa *Advances in Cryptology — CRYPTO’ 88,* toimittanut Shafi Goldwasser, 319–327. New York, NY: Springer New York. ISBN: 978-0-387-34799-8.

Conti, M., E. Sandeep Kumar, C. Lal ja S. Ruj. 2018. “A Survey on Security and Privacy Issues of Bitcoin”. *IEEE Communications Surveys Tutorials* 20, numero 4 (Fourthquarter-Fourthquarter): 3416–3452. ISSN: 1553-877X. doi:10.1109/COMST.2018.2842460.

Herrera-Joancomartí, Jordi. 2015. “Research and Challenges on Bitcoin Anonymity”. Teoksessa *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance,* toimittanut Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Emil Lupu, Joachim Posegga, Alessandro Aldini, Fabio Martinelli ja Neeraj Suri, 3–16. Cham: Springer International Publishing. ISBN: 978-3-319-17016-9. doi:10.1007/978-3-319-17016-9_1.

Kelly, D., R. Raines, R. Baldwin, M. Grimaila ja B. Mullins. 2012. “Exploring Extant and Emerging Issues in Anonymous Networks: A Taxonomy and Survey of Protocols and Metrics”. *IEEE Communications Surveys Tutorials* 14, numero 2 (SecondSecond): 579–606. ISSN: 1553-877X. doi:10.1109/SURV.2011.042011.00080.

Koshy, Philip, Diana Koshy ja Patrick McDaniel. 2014. “An Analysis of Anonymity in Bitcoin Using P2P Network Traffic”. Teoksessa *Financial Cryptography and Data Security,* toimittanut Nicolas Christin ja Reihaneh Safavi-Naini, 469–485. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-662-45472-5.

Kumar, Amrit, Clément Fischer, Shruti Tople ja Prateek Saxena. 2017. “A Traceability Analysis of Monero’s Blockchain”. Teoksessa *Computer Security – ESORICS 2017,* toimittanut Simon N. Foley, Dieter Gollmann ja Einar Snekkenes, 153–173. Cham: Springer International Publishing. ISBN: 978-3-319-66399-9.

Kus Khalilov, M. C., ja A. Levi. 2018. “A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems”. *IEEE Communications Surveys Tutorials* 20, numero 3 (thirdquarterthirdquarter): 2543–2585. ISSN: 1553-877X. doi:10.1109/COMST.2018.2818623.

Mahlberg, Alvar, ja Teemu Hyytiäinen. 2019. *AuroraAI ja uudenlaiset token-taloudet.* (Haettu: 04.04.2019), http://blockchain.it.jyu.fi/assets/pdf/aurora-ai.pdf.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker ja Stefan Savage. 2013. “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names”. Teoksessa *Proceedings of the 2013 Conference on Internet Measurement Conference,* 127–140. IMC ’13. Barcelona, Spain: ACM. ISBN: 978-1-4503-1953-9. doi:10.1145/2504730.2504747.

Merkle, Ralph C. 1988. “A Digital Signature Based on a Conventional Encryption Function”. Teoksessa *Advances in Cryptology — CRYPTO ’87,* toimittanut Carl Pomerance, 369–378. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-48184-3.

MOT Englanti. 2019. Kielikone Ltd. (Katsottu: 23.03.2019), https://mot-kielikone-fi.ezproxy.jyu.fi/mot/jyu/netmot.exe.

Nakamoto, Satoshi. 2008. “Bitcoin: A peer-to-peer electronic cash system.” https://bitcoin.org/bitcoin.pdf. (Haettu: 05.02.2019).

Pfitzmann, Andreas, ja Marit Köhntopp. 2001. “Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology”. Teoksessa *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability Berkeley, CA, USA, July 25–26, 2000 Proceedings,* toimittanut Hannes Federrath, 1–9. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-44702-3. doi:10.1007/3-540-44702-4_1.

Reid, Fergal, ja Martin Harrigan. 2013. “An Analysis of Anonymity in the Bitcoin System”. Teoksessa *Security and Privacy in Social Networks,* toimittanut Yaniv Altshuler, Yuval Elovici, Armin B. Cremers, Nadav Aharony ja Alex Pentland, 197–223. New York, NY: Springer New York. ISBN: 978-1-4614-4139-7. doi:10.1007/978-1-4614-4139-7_10.

Ren, Jian, ja Jie Wu. 2010. “Survey on anonymous communications in computer networks”. *Computer Communications* 33 (4): 420–431. ISSN: 0140-3664.

Ron, Dorit, ja Adi Shamir. 2013. “Quantitative Analysis of the Full Bitcoin Transaction Graph”. Teoksessa *Financial Cryptography and Data Security,* toimittanut Ahmad-Reza Sadeghi, 6–24. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-39884-1.

S.A., Blockchain Luxembourg. 2019. “www.blockchain.com”. https://www.blockchain.com/btc/tx/da9d987e5573c16e1fc315e661b0039473cf16b7988a0a39ee44ecececee245ff7. (Katsottu: 20.06.2019).

Saxena, Amitabh, Janardan Misra ja Aritra Dhar. 2014. “Increasing Anonymity in Bitcoin”. Teoksessa *Financial Cryptography and Data Security,* toimittanut Rainer Böhme, Michael Brenner, Tyler Moore ja Matthew Smith, 122–139. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-662-44774-1.