Viljami Kaasalainen

LOHKOKETJUTEKNOLOGIAN HAAVOITTUVUUDET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Kaasalainen, Viljami
Lohkoketjuteknologian haavoittuvuudet
Jyväskylä: Jyväskylän yliopisto, 2018, 32 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Halttunen, Veikko

Lohkoketjut ovat teknologiana uusi ilmiö ja ainakin toistaiseksi useimmille täysin tuntematon termi. Lohkoketjuista puhutaan usein hyvin positiiviseen sävyyn maailmaa mullistavana teknologiana. Käsitteen ympärille on muodostunut erittäin paljon keskustelua, josta seurauksena usein on se, ettei asiaa muisteta tarkastella tarpeeksi kriittisesti. Siksi tässä kandidaatin tutkielmassa käsitellään lohkoketjuteknologiaan liittyviä haavoittuvuuksia, erityisesti lohkoketjuihin kohdistuvia hyökkäyksiä. Tutkielma on toteutettu kirjallisuuskatsauksena. Ensin tutkielmassa käydään läpi lohkoketjuteknologian ominaisuudet ja toiminta periaatteet, minkä jälkeen siirrytään käsittelemään kolmea erilaista haavoittuvuutta ja mahdollisia ratkaisuja niihin. Kyseisiä haavoittuvuuksia ovat 51 prosentin hyökkäys, tuplakulutus ja hyökkäys kolmannen osapuolen palveluun. Tutkielma avaa erilaiset haavoittuvuudet ja niihin liittyvät hyökkäykset yksityiskohtaisesti, mutta varmasti toimivia ratkaisuja kyseisiin ongelmiin ei löydetty. Lohkoketjuteknologia on vielä uusi asia ja sen merkittävimmät haavoittuvuudet perustuvat niin syvälle sen perimmäisiin toimintaperiaatteisiin, että niihin tarjotut ratkaisut ovat pääasiassa vielä vain ehdotuksia.

Asiasanat: lohkoketjuteknologia, bitcoin, haavoittuvuus, hyökkäys, tuplakulutus

ABSTRACT

Kaasalainen, Viljami
Vulnerabilities of blockchain technology
Jyväskylä: University of Jyväskylä, 2018, 32 pp.
Information systems, Bachelor's thesis
Supervisor(s): Halttunen, Veikko

As a technology, blockchain is a new phenomenon and an unknown term for the most. Discussion about blockchains often has a positive tone and it has been called as a groundbreaking technology. This has caused a vast amount of discussion around the subject, which often leads to a lack of critical examination. That is why this thesis focuses on blockchain technology's vulnerabilities and especially various attacks concerning it. The thesis was implemented as a systematic literature review. First, it will review the features of blockchain technology comprehensively and after that, three different vulnerabilities and their possible solutions will be addressed. The three vulnerabilities in question are 51 percent attack, doublespending and attack on third-party service. The vulnerabilities are explained in a detailed way, but solutions are lacking practical and working answers. The blockchain technology is still emerging technology and its vulnerabilities are based deep into its core features. That is why the solutions to the vulnerabilities concerned are primarily only suggestions.

Keywords: blockchain, bitcoin, vulnerability, attack, doublespenging

KUVIOT

SISÄLLYS

1 JOHDANTO

Lohkoketjut ovat suhteellisen uusi teknologia ja tänä päivänä keskeinen puheenaihe. Idean vuonna 2008 esitteli Satoshi Nakamoto -nimeä käyttävä anonyymi henkilö. Hän julkaisi kirjoituksen, jossa esiteltiin Bitcoinin tekniset toimintaperiaatteet. Siitä lähtien aihe on saanut lisää julkisuutta ja uusien tutkimusten määrä lohkoketjuista on moninkertaistunut vuosi vuodelta (Google Scholar Plot, 2017). Monet uskovat lohkoketjuteknologian mullistavan maailman ja sen olevan mullistavin keksintö sitten internetin (Tapscott & Tapscott, 2016). Lohkoketjuista puhutaan useimmiten mahdollisuutena ja idean ympärillä oleva ilmapiiri on erittäin positiivinen. Yleisestä innostuneisuudesta johtuen kriittinen tarkastelu on ollut vähäistä (Morini, 2016). Sen vuoksi tässä tutkielmassa analysoidaan lohkoketjuteknologian haavoittuvuuksia.

Lohkoketjuteknologiaan liittyy erilaisia varjopuolia tai haavoittuvuuksia, jotka täytyy ratkaista ennen kuin lohkoketjuja voidaan käyttää tehokkaasti ja turvallisesti. Lisäksi on olemassa suuri määrä erilaisia asioita ja merkkipaaluja, joihin on ennemmin tai myöhemmin päästävä, jotta lohkoketjut vakiinnuttaisivat paikkansa. Kyseisiä haasteita tiedetään jo useita, osa suurempia, toiset pienempiä. Johtuen teknologian nuoruudesta erilaisia epäkohtia tiedetään jo niin monia, ettei niitä kaikkia voi käsitellä tässä tutkimuksessa yksityiskohtaisesti. Tämän vuoksi tutkimusaihe on rajattu vain merkittävimpiin haavoittuvuuksiin. Tässä tutkielmassa haavoittuvuuksilla tarkoitetaan erityisesti hyökkäyksiä, joita jokin entiteetti, eli ryhmä tai jokin kokonaisuus toimijoita, voisi kohdistaa lohkoketjua tai sen käyttäjiä kohtaan.

Tutkielma on suoritettu kirjallisuuskatsauksena, jonka suurin osa lähteistä on etsitty Google Scholarista. Sen ensimmäisenä tavoitteena on avata lohkoketjujen toimintaa ja määritellä käsite hyvin tarkkaan. Käsitteen ja idean ymmärtäminen on erityisen tärkeää, koska ilman perinpohjaista ymmärrystä lohkoketjuista, ei voi myöskään ymmärtää niiden heikkouksia. Toinen motiivi aiheen laajaan pohjustukseen on sen uutuus ja tuntemattomuus. Määrittelyn jälkeen tutkielma käsittelee lyhyesti lohkoketjujen hyötyjä ja vahvuuksia eli syitä miksi sellaista teknologiaa ylipäätänsä käytettäisiin. Toimintaperiaatteiden ja hyöty-

jen lisäksi lohkoketjujen käytöstä annetaan käytännön esimerkkejä. Tutkielman tutkimuskysymykset, joihin se pyrkii ensisijaisesti vastaamaan ovat:

- Mihin lohkoketjuteknologiaan liittyvät merkittävimmät haavoittuvuudet perustuvat?
- Miten kyseiset haavoittuvuudet ovat ratkaistavissa?

Ensimmäisten peruskäsitteitä määrittelevien lukujen jälkeen päästään tutkielman tärkeimpään asiaan, eli lohkoketjujen haavoittuvuuksiin. Luvut 3, 4 ja 5, käsittelevät kolmea erilaista lohkoketjun haavoittuvuutta. Kandidaatin tutkielman luonteen ja sen ohjeellisen laajuuden perusteella merkittäviä hyökkäyksiä tai haavoittuvuuksia on valittu kolme. Haavoittuvuuksia ovat 51 prosentin hyökkäys, tuplakulutus ja hyökkäys kolmannen osapuolen palveluun. Jokaisen haavoittuvuuden yhteydessä käsitellään sen määritelmä ja yleinen kuvaus, hypoteettisen hyökkäyksen suorittaminen ja onnistumisen todennäköisyys, sekä jo valmiita ratkaisuja tai ratkaisuehdotuksia.

Prosessi merkittävimpien lohkoketjuteknologian haavoittuvuuksien löytämiseksi alkoi erilaisten haavoittuvuuksien listaamisella. Niiden löytämiseksi käytettiin useita hakusanoja, kuten: ”blockchain vulnerabilities”, ”attacks on blockchain”, ”blockchain threats”. Monia muita synonyymejä ja samankaltaisia hakusanoja myös käytettiin haavoittuvuuksien listaamisessa. Haavoittuvuuksista ”merkittävimmät”, eli tässä tapauksessa useimmiten esiintyvät, vakavimmat ja eniten tutkitut, ovat mukana tutkielmassa. Tiivistettynä tutkielma pyrkii selittämään lohkoketjuteknologian ja sen erilaiset haavoittuvuudet yksityiskohtaisesti, sekä lyhyesti pohtia sen tulevaisuuden näkymiä.

2 LOHKOKETJUTEKNOLOGIA

Elinkaarensa alussa lohkoketjuteknologian tarkoitus oli toimia kryptovaluutta Bitcoinin pohjana. Nykyään lohkoketjuun perustuvia ratkaisuja käytetään myös Bitcoinin ulkopuolella, mutta kyseisen teknologian esi-isänä Bitcoin toimii erinomaisesti esimerkkinä lohkoketjuteknologiasta yleisesti. Sen vuoksi tutkielma käyttää Bitcoinin lohkoketjua usein havainnollistamaan asiaa käytännössä. Toisessa luvussa käsitellään lohkoketjuja yleisesti. Luvun jälkeen lukijalla on kuva lohkoketjujen toimintaperiaatteista, hyödyistä ja käyttökohteista. Lisäksi luku sisältää tutkielman kannalta merkittävien käsitteiden selittämistä.

2.1 Ominaispiirteet ja toiminta

Kaikki Bitcoinin oleellinen tieto liikkuu lohkoketjuverkoston sisällä ja se mahdollistaa kolikoiden lähettämisen, vastaanottamisen ja säilömisen. Lyhyesti sanottuna jokainen bitcoineilla tehty tapahtuma siirtyy verkostoon odottamaan varmistusta ja kyseinen tapahtuma tulee voimaan vasta silloin, kun se oli saanut hyväksynnän useilta eri lähteiltä. Selvennyksenä Bitcoin kirjoitettuna isolla alkukirjaimella tarkoittaa koko maksujärjestelmää ja yleistä ideaa, kun taas pienellä kirjoitettuna pelkästään valuuttaa (Brenig, Schwarz & Rückeshäuser, 2016). Bitcoin ja monet muut kryptovaluutat omaavat potentiaalin toimia valuuttana ja muuttaa maailmaa, mutta se on vain pieni osa siitä, mihin lohkoketjuja on mahdollista käyttää (Jacobs, 2011).

Jotta voidaan puhua lohkoketjujen haavoittuvuuksista, on sen toiminta ja periaatteet ymmärrettävä melko perinpohjaisesti. Kyseessä on siis aikaisemmista käytännöistä poikkeava tapa tallentaa, vastaanottaa ja lähettää tietoa. Kuvainnollisesti se on kuin tilikirja, jonka voivat halutessaan nähdä kaikki, mutta sieltä ei voi poistaa mitään. (Pilkington, 2016)

Lohkoketjuverkosto koostuu sitä ylläpitävistä prosessoreista tai käyttäjistä, joista puhutaan solmuina. Näistä yksittäisistä verkon osista käytetään englannin kielessä termiä ”node”. Verkosto on hajautettu ympäri maailmaa ja se toimii

vertaisverkkona (engl. peer-to-peer), jota ei suoranaisesti valvo kukaan viranomainen. Mitä useampi tietokone pyörittää lohkoketjua ylläpitävää sovellusta, sitä tehokkaampi verkosto on, koska jokainen käyttäjä antaa osan laitteensa suorituskyvystä lohkoketjun käyttöön. Kaikkien käyttäjien ei tarvitse ladata koko lohkoketjun sisältävää ”full node”- sovellusta käyttääkseen sitä tai ollakseen osana yhteisöä. Tällainen sovellus sisältää koko lohkoketjun informaation sen synnystä nykyhetkeen, ja se myös monitoroi ja hyväksyy uusia tapahtumia. Bitcoinin tapauksessa full node- sovellus vaatii tietokoneelta noin 145 gigatavua tallennustilaa ja 2 gigatavua lähimuistia (Bitcoin Project, 2009). Lompakot eli sovellukset, joiden avulla lähetään, vastaanotetaan ja säilötään kryptovaluuttoja, useimmiten pitävät sisällään vain lohkoketjun uusimmat tapahtumat ja ovat sovelluksina paljon kevyempiä. Kolmas erilainen sovellustyyppi on louhimiseen tarkoitetut sovellukset, jotka esitellään seuraavaksi.

Lohkoketjujen sisältö koostuu nimensä mukaisesti lohkoista, jotka sisältävät erilaista tietoa. Esimerkiksi Bitcoinissa lohkot sisältävät tiedon erilaisista maksutapahtumista, edellisen lohkon tiivisteen (engl. hash), sekä yleisen tiivisteen. Louhiminen lohkoketjujen yhteydessä tarkoittaa sitä, että tietokoneet ajavat sovellusta, jonka tarkoituksena ratkaista erittäin vaativia algoritmeja, jotka ovat vaikeusasteeltaan ennalta määrättyjä. Kun ratkaisu ongelmaan löytyy, syntyy ketjuun uusi lohko lisää. Tätä periaatetta kutsutaan todisteeksi työstä (engl. proof of work), jonka avulla lohkoketjun skaalautuvuutta ja käyttöä rajataan. (Pilkington, 2016)

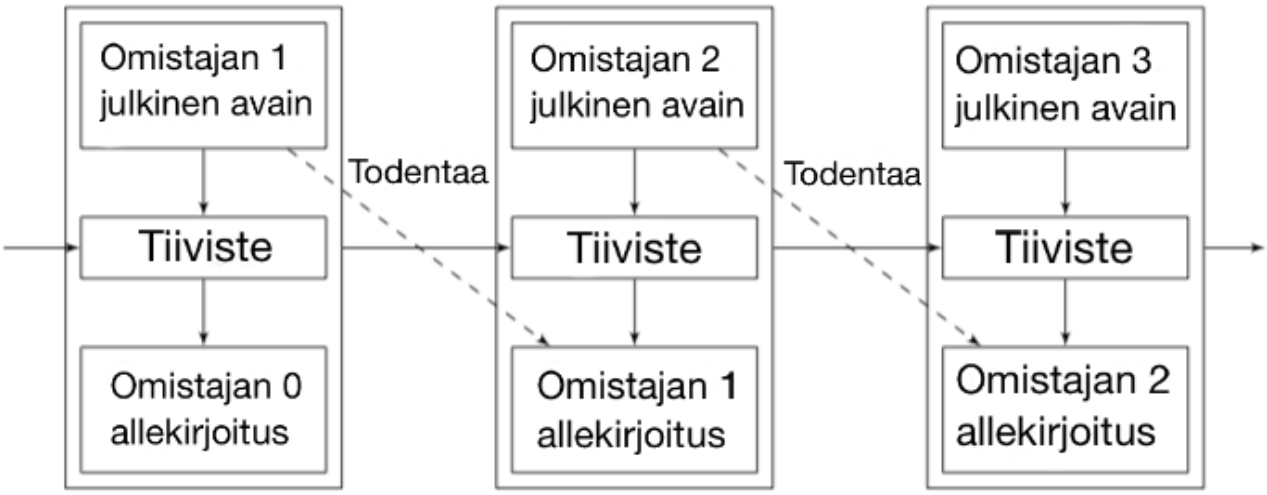
Proof of workia voidaan ajatella tapahtumana tuottaa dataa, jota on vaikeaa generoida, mutta helppo todistaa oikeaksi (Nakamoto, 2008). Käytännössä Bitcoinin vertaisverkkoa ylläpitämät solmut ratkovat SHA-256 (Secure Hash Algorithm) nimistä algoritmia, jonka ratkaisulla ei ole periaatteessa ole mitään järkevää käyttökohdetta. Toisin sanoen solmut ratkovat generoituja matemaattisia ongelmia, joiden ratkaisulla ei ole minkäänlaista käyttökohdetta. Poikkeuksena tai vastakohtaisena esimerkkinä tästä toimii kryptovaluutta Primecoin, jonka louhinnasta on potentiaalisesti tieteellistä hyötyä. Kyseisen kryptovaluutan louhinnassa etsitään uusia alkulukuja, eli vain yhdellä tai itsellään jaollisia lukuja (King, 2013). Jos Primecoin luetaan pois, ei louhimisella ole muuta käytännön tarkoitusta kuin varmistaa solmujen työnteko.

Kun oikea ratkaisu tai tiiviste, joka on muodoltaan sarja numeroita ja kirjaimia löydetään, voidaan lohkoketjuun lisätä uusi lohko. Solmuja, jotka ylläpitävät verkostoa eli ratkovat kyseisiä algoritmeja, kutsutaan louhijoiksi (engl. miner). Kun louhija ratkaisee algoritmin, saa hän siitä vastineeksi hetkellisen oikeuden toimia lohkon hallitsijana, ja täten oikeuden lohkoon tallentuvien maksutapahtumien siirtokuluihin, sekä tietyn määrän bitcoineja. Siirtokulut ovat lohkoketjua käyttävien henkilöiden maksuja louhijoille vastineeksi heidän tekemästään työstä. Transaktion suorittava henkilö voi itse päättää siirtokulujen suuruudesta, mutta louhijat yleensä hyväksyvät ensin ne transaktion, jotka antavat heille suurimmat voitot. Siksi transaktio vähäisillä siirtokuluilla tai ilman niitä voi jäädä hyväksymättä. (Easley, O'Hara & Basu, 2017)

Uusia lohkoja syntyy noin 10 minuutin välein, joka on keskimääräinen aika kyseisen algoritmin ratkaisemiseen. Teknologian kehittyessä ja verkoston laskentatehon kasvaessa myös algoritmia itsessään muutetaan haasteellisemmaksi, jotta noin 10 minuutin aikahaarukka pysyisi. Samalla myös algoritmin ratkaisevan louhijan palkinto puolitetaan. Ajassa eteenpäin mentäessä louhijan saamasta kokonaispalkkiosta aina pienempi osa tulee olemaan kiinteää ratkaisupalkkiota, koska siirtokulujen voidaan olettaa pysyvän ennallaan. (Nakamoto, 2008) Yhden lohkon louhiminen vaatii kuitenkin niin paljon laskentatehoa, että esimerkiksi tehokkaalta kuluttajakäyttöön tarkoitetulta tietokoneelta se veisi todennäköisesti vuosia. Siksi monet yksityiset louhijat ovat liittyneet louhintaryhmiin (engl. mining pool), jossa useat solmut yhdistävät voimansa saman algoritmin ratkaisemiseen ja lopulta jakavat palkinnon jäseniensä kesken työpanoksen mukaan. (Eyal & Sirer, 2014) Louhintaryhmien ymmärtäminen on oleellinen tieto tämän tutkielman kannalta.

Proof of work toimii ratkaisuna kahteen ongelmaan, joita aikaisemmilla vertaisverkoilla, kuten uTorrentilla on ollut. Vertaisverkkojen yksi ongelma on ollut puute järjestelmästä, joka jollain tavalla palkitsisi verkon ylläpitämisestä. Esimerkiksi torrenttipalveluissa moni käyttäjistä ainoastaan lataa haluamansa tiedostot itselleen, jonka jälkeen he sulkevat palvelun. Verkoston on tarjottava käyttäjilleen korvausta ylläpidosta tai torrenttien tapauksessa tiedostojen jakamisesta (engl. seeding), koska vapaaehtoisten määrä ei riitä ylläpitämään tehokasta verkostoa. (Wu, Dhungel, Hei, Zhang & Ross, 2010) Lohkoketjuteknologiassa solmut saavat verkoston ylläpitämisestä palkinnoksi rahakkeita (engl. token), eli Bitcoinin tapauksessa bitcoineja. Proof of workin toinen merkittävä hyöty lohkoketjulle on sen tarjoama suoja hyökkäyksiä vastaan. Se rajoittaa toimintoja, joita lohkoketjun verkostolle voidaan suorittaa, eli näin ollen suojaa sitä esimerkiksi DoS-hyökkäyksiltä. Lisäksi tällainen protokolla takaa sen, ettei päätöksiä tee henkilö, jolla on eniten pääomaa tilillään, vaan henkilö joka omaa eniten laskentatehoa. (Nakamoto, 2008) Tämä asia käsitellään vielä tarkemmin luvussa 3.

Kun uutta tietoa halutaan tallentaa lohkoketjuun, sinne luodaan uusia lohkoja, jotka taas sisältävät uudet maksutapahtumat, edellisen lohkon tiivisteen ja uuden yleisen tiivisteen. Tiiviste tarkoittaa koodia, joka generoidaan suuremmasta määrästä tietoa luettavampaan muotoon. Esimerkiksi jos lohkon sisällä oleva data koostuisi jokaisen Suomen kaupungin nimistä, siitä tiedosta voitaisiin luoda suhteellisen lyhyt tiiviste. Kaikki lohkot ja tiivisteet ovat yhteydessä toisiinsa aivan kuten ketjussa, eli uusi lohko linkittyy sitä edeltävään (Kuvio 1). Jos lohkon sisällä olevasta tiedosta muutettaisiin edes hyvin pieni asia, esim. jonkun kaupungin nimestä vaihdettaisiin yksi kirjain, muuttuisi lohkon tiivisteen arvo täysin erilaiseksi. Lohkon tiivisteen lisäksi on olemassa koko lohkoketjun yleinen tiiviste, joka generoidaan jokaisen lohkon tiivisteistä. Tämä tarkoittaa sitä, että jos lohkon sisällä muutetaan edes yhtä kirjainta tai numeroa, muuttuu samalla niin kyseisen lohkon tiiviste että koko lohkoketjun yleinen tiiviste. (Jacobs, 2011)



KUVIO 1 Bitcoinissa käytetyn lohkoketjun transaktion havainnollistus (Drainville, 2012)

Tiivisteiden vertailu mahdollistaa sen, että lohkoketjujen sisältöä on erittäin vaikeaa manipuloida. Jotta tietoa tai maksutapahtumia voidaan lisätä lohkoketjuun, on uuden tiedon saatava hyväksyntä useilta eri käyttäjiltä eli solmuilta. Käytännössä tämä tarkoittaa sitä, että jos jokin käyttäjä yrittäisi muuttaa lohkoketjussa olevaa tietoa, muuttuisi myös koko lohkoketjun tiiviste. Tällöin uuden tiedon lisääminen tai vanhan tiedon muokkaaminen ei läpäise solmujen tarkistusta. Käyttäjä ei voi siis tehdä lisäyksiä lohkoketjuun ilman täysin identtistä versiota yleisesti hyväksytystä lohkoketjusta. (Pilkington, 2016) Luvussa 3 käsitellään 51 % hyökkäystä, jonka avulla lohkoketjuun voidaan puolestaan tehdä virheellisiä muutoksia.

2.2 Hyödyt

Edellä mainittiin lohkoketjuteknologian toimintaperiaatteita, joiden mukaan tämä aikaisimmista tietorakenteista poikkeava ratkaisu toimii. Ne mahdollistavat useita merkittäviä hyötyjä niin tiedon siirtämiseen kuin tallentamiseen liittyen. Suurimmat hyödyt lohkoketjujen käytöstä ovat tietokannan hajautus, tietojen pysyvyys ja anonyymiys, sekä turvallisuus (Pilkington, 2016).

Lohkoketjuilla on potentiaalia vähentää tarvetta kaikenlaisille välikäsille, puhuttiinpa sitten valuutasta tai informaatiosta. Välikädet kuten pankit tai kolmannen osapuolen palvelut tavaroiden myynnissä, ovat arkipäivää, koska ne ovat luotettavia ja varmoja. Huono puoli niissä on kuitenkin se, että ne yleensä maksavat ja lisäksi rajoittavat yksilön mahdollisuuksia toimia haluamallaan tavalla. Jos yksilö voisi itse säilöä vaikkapa rahojaan järkevistä ja turvallisesti, ei hänen tarvitsisi maksaa pankkitilin avausmaksuja tai huolehtia

nostorajoituksista. Lohkoketjujen avulla edellä kuvattu välikäsi on mahdollista poistaa monissa tapauksissa. (Underwood, 2016)

Yksi suurin epävarmuuden lähteistä kahden yksityishenkilön vaihdannassa on luottamuksen puute. Tämä ongelma voidaan ratkaista monin eri tavoin lohkoketjujen avulla. Esimerkiksi lohkoketjuissa käytettävät älysopimukset (engl. smart contracts) omaavat potentiaalin mullistaa C2C kaupankäynnin. Älysopimukset ovat ikään kuin tiedostoja tai ohjelmia, jotka suorittavat toimintoja vasta sitten, kun sovittu tapahtuma on käynyt toteen. Esimerkiksi jos henkilö A haluaa myydä tavaran henkilölle B, mutta B ei suostu maksamaan tuotetta etukäteen, voi hän suorittaa maksun älysopimukselle. Sopimukseen voidaan luoda ehto, että jos paketti saapuu ajoissa ostajalle niin samalla myös rahat siirtyvät myyjälle. Jos taas paketti ei täytä kaikkia sopimuksella luotuja ehtoja, saa ostaja rahansa takaisin. Älysopimuksia ei voi jälkikäteen muokata, eli ne ovat pysyviä. Tämä mahdollistaa sen, ettei kukaan voi yrittää muokata sopimusta itselleen mieleiseksi ja loukata vastapuolen oikeuksia. Sopimukset ovat myös kaikkien nähtävillä, joten sinne ei myöskään voi piilottaa ehtoja. (Luu, Chu, Olickel, Saxena, & Hobor, 2016)

2.3 Käyttötarkoitukset

Lohkoketjuteknologiaa käytetään jo nyt hyödyksi useissa eri tapauksissa, mutta sen suurimmat mahdollisuudet eivät ole vielä realisoituneet. Lohkoketjuteknologiasta voidaan tänä päivänä puhua jopa muoti-ilmiönä, joten halukkuutta teettää erilaisia ratkaisuja sen avulla on varmasti paljon. Potentiaalisia käyttökohteita pohtiessa on hyvä pitää mielessä teknologiaan liittyvät vahvuudet ja heikkoudet. Jos kysymyksiin: ”Tarvitaanko tietokannan sisällön säilömistä?” ja ”Kirjoittaako tietokantaan useita henkilöitä?” voidaan vastata kyllä, sekä ”Onko luotettavan kolmannen osapuolen käyttö mahdollista?” vastataan ei, voivat lohkoketjut tällöin olla järkevä ratkaisu (Wüst & Gervais, 2017). Lohkoketjut nähdään mahdollisena ratkaisuna sellaisiin ongelmiin, joissa tiedon validiteetti, pysyvyys, muuttumattomuus ovat tärkeitä tekijöitä, sekä tapauksissa, joissa kolmannen osapuolen palveluita tai valvontaa halutaan välttää. Kaikista parhaiten lohkoketju ratkaisee tilanteen, jossa tiedonsiirtoa suoritetaan kahden tai useamman toiselleen tuntemattoman henkilön välillä.

Tällä hetkellä ylivoimaisesti merkittävin käyttökohde on kryptovaluutat, lähinnä siksi, että koko idea on sieltä lähtöisin. Kryptovaluutat, joita kutsutaan myös virtuaaliseksi valuutaksi, ovat kuin digitaalista rahaa. Niiden käyttö pohjautuu kokonaan lohkoketjujen tarjoamaan teknologiaan. Vaikka tämä tutkielma keskittyy nimenomaan lohkoketjuihin, niin kryptovaluuttojen käsite kulkee hyvin lähellä jokaisessa luvussa. Siksi se määritelläänkin lyhyesti tässä luvussa. Tällä hetkellä tunnetuin kryptovaluutta on jo aikaisemmin mainittu Bitcoin, ja se toimii varsin hyvänä esimerkkinä siitä, mitä kryptovaluutat yleensä ovat. Bitcoinin oma lohkoketju on ensimmäinen hyvin tunnettu lohkoketjuun pohjautuva ratkaisu, josta johtuen siitä on tehty huomattavasti enemmän tutkimuksia

verrattuna muihin lohkoketjuihin. Erilaisia kryptovaluuttoja on kuitenkin jo satoja, ehkä tuhansia (Coinmarketcap, 2018). Niistä lähes kaikki pohjautuvat toisistaan erilaisiin, lohkoketjuteknologiaan perustuviin ratkaisuihin.

Yleensä kryptovaluuttoja eivät ohjaa pankit tai muut välikädet, eikä niihin liity mitään fyysistä vaihdonkohdetta. Eroavaisuuksia ja poikkeuksia kuitenkin löytyy, mutta kryptovaluutoista useimmat ovat teknologialtaan hyvin samankaltaisia (Narayanan, 2016). Siksi yleinen kuva tyypillisestä kryptovaluutasta on mahdollista muodostaa. Aikaisemmin vertaisverkoista todettiin niiden tarvitsevan jonkinlaisen palkitsemisjärjestelmän verkoston ylläpitämisestä. Lohkoketjuissa tällaista palkintoa kutsutaan rahakkeeksi (engl. token), eli kryptovaluutaksi, jota on mahdollista ansaita ylläpitämällä verkostoa. Vaikkakin jo useilla kryptovaluutoilla on hintansa ja kurssinsa suhteessa perinteisiin Fiat-rahoihin (valtioiden säätelemät valuutat), toimivat jotkut niistä muissakin käyttötarkoituksissa, kuten vaihdannan välineenä organisaation sisällä (Pilkington, 2016).

Toisessa luvussa käsiteltiin lohkoketjujen välttämättömät perusteet haavoittuvuuksien ymmärtämisen kannalta. Luvun jälkeen lukijalla olisi tarkoitus olla yleinen käsitys lohkoketjun toiminnasta ja siihen liittyvästä sanastosta. Seuraavat kolme lukua käsittelevät lohkoketjun erilaisia haavoittuvuuksia ja niiden ratkaisuja. Haavoittuvuudet ja niihin liittyvät ratkaisut käsitellään haavoittuvuus kerrallaan järjestyksessä 51 prosentin hyökkäys, tuplakulutus ja hyökkäys kolmannen osapuolen palveluihin.

3 51 PROSENTIN HYÖKKÄYS

Bitcoinin lohkoketjua voidaan tavallaan ajatella demokratiana, jossa valta on sellaisella entiteetillä, joka hallitsee yli 50 prosenttia lohkoketjun kokonaisesta laskentatehosta. On hyvin epätodennäköistä, että yksi toimija voisi päästä tällaiseen tilanteeseen, koska se vaatisi erittäin suurta panosta niin työn kuin hinnan puolesta, mutta se on teoriassa mahdollista. Kun tietokone tai solmu louhii kryptovaluuttaa, se tekee sitä tietyllä laskentateholla laitteen tehokkuuden rajoissa. Kun puhutaan yli 50 prosentin laskentatehon ylittämisestä, sillä tarkoitetaan kaikkien solmujen yhteenlasketun laskentatehon ylittämistä. Tässä luvussa käsitellään miten juuri mainittu 50 prosentin raja on mahdollista ylittää ja minkälaisia seurauksia tällaisesta hyökkäyksestä voi johtua. Luvun lopussa pohditaan ratkaisua kyseiseen haavoittuvuuteen.

3.1 Hyökkäyksen suorittaminen

Yli puolet Bitcoin lohkoketjun laskentatehosta maaliskuussa 2018 tarkoittaa noin 13 miljoonaa ”hashia” sekunnissa (engl. trillion hashes per second TH/s) (Blockchain.info, 2018) Yksi tehokkaimmista verkkokaupoissa myytävistä, ellei tehokkain bitcoinien louhimistietokone Dragonmint 16T pystyy suorituskyvyltään 16.0 TH/s nopeuteen. Laite maksaa Yhdysvalloissa noin 2700 dollaria eikä siihen ei ole otettu huomioon mitään asennukseen tai kuljettamiseen liittyviä kuluja. (Halongmining.com, 2018) Kyseisiä laitteita tarvittaisiin yli 800 000 tarvittavan tehon saavuttamiseksi, eli pelkän laitteiston hinta nousisi muutamaan miljardiin. Jos laskelmiin huomioitaisiin vielä työvoima-, energia- ja säilytyskulut, nousisi summa vielä huomattavasti. Tällaisten resurssien hankkiminen on erittäin vaikeaa.

Lohkoketjulle on hankala määritellä hintaa tai rahallista arvoa, mutta hyökkääjän kannalta sen tarvitsisi olla suurempi kuin hyökkäyksestä aiheutuvat kulut, jotta hyökkäys olisi kannattava suorittaa. On myös huomioita vaikutukset lohkoketjun arvoon, joita hyökkäyksellä todennäköisesti olisi. Jos jokin

ryhmä valtaisi Bitcoinin lohkoketjun, laskisi sen käyttäjämäärä ja arvo luultavasti heti kun tapahtuma selviäisi sen käyttäjille, koska hyökkäystä ole käytännössä mahdollista suorittaa huomaamatta. Lohkoketjun valloitus vaatii siis huomattavan määrän resursseja, jotka todennäköisesti ylittävät hyökkäyksestä saadut hyödyt. Teoriassa yksi toimija voi hankkia itselleen lähes miljoona tehokasta tietokonetta manipuloidakseen lohkoketjua, mutta käytännössä se on hyvin haasteellista ja tappiollista taloudellisesta näkökulmasta.

Lohkoketjun valloitus on mahdollista tehdä myös muilla tavoin, kuin suurilla hyökkääjän investoinneilla laitteistoon. Hajautetut ryhmät ja yhteisöt voivat jopa huomaamattaan saavuttaa riittävän laskentatehon. Heinäkuussa 2014 louhimisyhtymä Ghash.io piti hallussaan yli puolet Bitcoinin lohkoketjun laskentatehosta (Bastiaan, 2015). Luvussa 2 esitelty louhimisyhtymä tarkoitti siis yhteisöä, jossa useat louhijat yhdistävät voimansa saavuttaakseen itselleen tasaisemmat tulot. Tapahtumahetkellä Ghash.io palvelu oli niin suosittu, että kyseinen entiteetti piti halussaan jopa mahdottomaksi kutsuttua 51 prosenttia laskentatehosta. Varsinkin lohkoketjuteknologian elinkaaren alkupäässä tällaista tapahtumaa ei osattu varoa etukäteen, koska useimpien mielestä se tuntui niin mahdottomalta. Kun tapahtunut tuli yleiseen tietoisuuteen, lähtivät useat louhijat palvelusta pois estääkseen mahdollisen väärinkäytön, jota palvelun ylläpitäjät olisivat voineet toteuttaa (Bastiaan, 2015). Toistaiseksi tällaisen tapahtuman estäminen on täysin louhimisryhmän ylläpidon ja sen jäsenten vastuulla. Tapahtuneessa on kuitenkin muistettava kyseisen ajankohdan kokonainen laskentateho, joka oli reilut 120 000 TH/s verrattuna nykyiseen 26 miljoonaan.

Lohkoketjun teknologiassa on olemassa yksi virallinen tai oikeana pidetty ketju, jonka mukaan toimitaan. Ketju alkaa ensimmäisestä lohkosta, jota kutsutaan alkulohkoksi (engl. genesis-block) ja se päättyy uusimpaan lisättyyn lohkoon. (Eyal & Sirer, 2014) Kun uusia transaktioita ja lohkoja hyväksytään lohkoketjuun, niin samalla virallinen ketju kasvaa kuvainnollisesti pituutta. Jos joku yrittää lisätä virheellistä tietoa lohkoketjuun, syntyy silloin kopio virallisesta lohkoketjusta tiedon lisänneen henkilön ja sen varmistaneiden laitteille. Tämä uusi ketju on täsmälleen samanlainen kuin virallinen ketju, mutta sen uusin transaktio on erilainen. Kuten aikaisemmassa luvussa jo todettiin, niin hyvinkin minimaalinen muutos lohkoketjun tiedoissa muokkaa tiivisteen aivan erilaiseksi. Kun oikeasta lohkoketjusta syntyy kopio, joka sisältää virheellistä tietoa, huomaavat verkoston ylläpitäjät sen muuttuneesta tiivisteestä ja osaavat välttää sitä. Näin virallisen lohkoketjun kopioon ei kukaan lisää tai hyväksy uusia transaktioita, eikä se myöskään kuvainnollisesti kasva pituutta. Näin ollen virallinen lohkoketju pysyy oikeana. (Drainville, 2012)

Kuvitellaan edellinen tilanne, jossa jokin entiteetti haluaa lisätä lohkoketjuun virheellistä tietoa. Silloin oikeasta lohkoketjusta muodostuu kaksi versioita, joiden historia on täysin samanlainen, mutta uusimmat tiedot eroavat. Kaikki oikeaa versiota kannattavat jatkavat normaaliin tapaan virallisen lohkoketjun käyttämistä ja samalla ”kasvattavat” sitä. Virheellistä tietoa viljelleet henkilöt voivat jatkaa oman lohkoketjunsa käyttöä, mutta se on oletettavasti ”lyhyempi” kuin virallinen versio, koska siihen ei lisätä läheskään niin useita lohkoja kuin

viralliseen lohkoketjuun. Näin ollen sitä ei hyväksytä oikeana. Jos nämä kyseiset toimijat kuitenkin omaavat yli puolet lohkoketjun laskentatehosta, voivat he teoriassa käyttää ja samalla kasvattaa omaa lohkoketjuaan nopeammin kuin virallisen lohkoketjun käyttäjät. Tällöin virheellisestä lohkoketjun versiosta tulee uusi virallinen versio, joka sisältää kyseenalaista tietoa. Täytyy kuitenkin huomioida, että termi ”virallinen”, on tässä kontekstissa hieman harhaan johtava, koska Bitcoinia ei valvo kukaan virallinen toimija, vaan sen käyttö perustuu täysin sen käyttäjien kannattamaan versioon. (Bahack, 2013)

3.2 Ongelman ratkaiseminen

Monet tutkijat ja harrastajat ovat pohtineet ja tutkineet ratkaisua 51 prosentin hyökkäykseen. Koska kyseinen haavoittuvuus perustuu lohkoketjun perusluonteisiin ominaisuuksiin, vaatii ratkaisu todennäköisesti toimintaperiaatteiden muokkaamista. Eyal ja Sirer (2014) mainitsevat paljon keskustelua herättäneessä kirjoituksessaan kolme tärkeää kriteeriä liittyen lohkoketjun muokkaamiseen. Ensimmäinen ja ehkä tärkein säännöistä on se, että lohkoketjun on pysyttävä sisällöllisesti ennallaan muutoksesta huolimatta. Jos lohkoketjua muutetaan, on tärkeää tehdä muutokset juuri tiettyyn ja samaan lohkoketjuun, eikä vain luoda uutta ja paranneltua versiota. Varsinkin lohkoketjuissa, jotka sisältävät tietoa kryptovaluutoista ja maksutapahtumista, tiedon muuttumattomuus on erittäin tärkeä elementti. Toinen sääntö koskee louhijoiden ja verkoston ylläpitäjien investointeja. Muutoksen jälkeen olisi tärkeää, että solmut pystyisivät toimimaan mahdollisimman samalla laitteistokokoonpanolla. Tämä on tärkeää siksi, että jos jokaisen lohkoketjun käyttäjän laitteisto yhtäkkiä muuttuisi käyttökelvottomaksi tai tehottomaksi, ei verkostoa ylläpitäisi tarpeeksi suuri määrä solmuja. Tarve investoida erilaiseen laitteistoon ole motivoivaa käyttäjien kannalta. Viimeiseksi muutoksen ohjeistetaan olemaan mahdollisimman saumaton. Lisäksi olisi toivottua, jos muutokseen liittyviä muuttujia voitaisiin vaivattomasti säädellä ilman tarvetta uudelle suurelle muutokselle. Edellä mainitut ”säännöt” ovat pikemmin ohjeita tai toiveita, jotka on hyvä muistaa suunnitellessaan muutoksia lohkoketjuun. Ne ovat hyvin yleisluonteisia ja päteviä moneen eri teknologiaan, mutta tutkielma mainitsee ne lohkoketjujen poikkeuksellisuuden vuoksi. Lohkoketjuihin ei voida tehdä muutoksia aivan niin helposti ja huolettomasti kuin tavalliseen sovellukseen, koska jo sen teknologian yksi periaatteista on muuttumattomuus (Eyal & Sirer, 2014).

Hyökkäykseen, jossa entiteetti luvun alussa mainitsemalla tavalla hankkii itselleen valtavan laitteiston ja sillä tavoin saavuttaa yli puolet lohkoketjun laskentatehosta, ei ole vielä toistaiseksi ratkaisua. Kuten jo aikaisemmin mainittiin, on tällaisen hyökkäyksen toteuttaminen erittäin hankalaa ja samalla epätodennäköistä. On kuitenkin virheellistä puhua 51 prosentin hyökkäyksestä mahdottomana tapauksena, koska jo kerran louhimisyhtymä on jo pitänyt tarvittavaa osuutta laskentatehosta hallussaan (Bastiaan, 2015). Tällainen tilanne on myös todennäköisemmin tapahtuva, koska suuri laskentateho on loogisesti helpom-

paa saavuttaa tuhansien solmujen kanssa, kuin yksin tai pienessä ryhmässä. Jotta louhimisryhmät eivät tulevaisuudessa ajautuisi samanlaiseen tilanteeseen kuin Ghash.io, on esitetty ratkaisu kaksivaiheisesta työn todisteesta (engl. 2-phase proof of work). Ratkaisun tavoitteena on pienentää hyötyä ja etuja, joita suurilla louhimisyhtymillä on. Koska lohkon ratkaiseminen on periaatteessa arvonta kaikkia sitä yrittävien solmujen kesken, tarkoittaa suurempi yhtymä suurempaa mahdollisuutta voittaa. Tietysti suurempi yhtymä tarkoittaa myös pienempää palkkiota siinä kuuluville solmuille, mutta silloin louhimisesta saadut tulot ovat todennäköisempiä ja tasaisempia. Louhijoilla on siis hyviä syitä liittyä suuriin yhtymiin, jonka seurauksena yksi yhtymä voi ylittää laskentatehossa 51 prosentin rajan. (Bastiaan, 2015).

Uusien lohkojen luominen lohkoketjuun vaatii tietynlaisen algoritmin ratkaisemista, josta palkinnoksi ensimmäinen ratkaisija saa itselleen kryptovaluuttaa ja lohkon sisällä tapahtuvat transaktiokustannukset. Tällaista menetelmää kutsutaan siis nimellä todiste työstä (engl. proof of work). Kaksivaiheisessa työn todistuksessa louhijan tehtävä on puolestaan ratkaista kaksi erilaista algoritmia. Ensimmäinen algoritmeista, jota kutsutaan vaikka nimellä ”X”, on täysin sama, kuin tavallisesti lohkoketjuteknologiassa. Kun X on ratkaistu, täytyy louhijoiden ratkaista algoritmi ”Y”, joka ratkaistaan samalla periaatteella kuin X, mutta käyttäen erilaisia algoritmeja. Lisäksi Y:n algoritmeissa käytetään hyväksi louhimisyhtymän omistamaa yksityisavainta, jolla louhitut varat voidaan siirtää kolmannen osapuolen pörssiin, joka tässä esimerkissä on palvelu nimeltä Coinbase. Kaksi erillistä algoritmia mahdollistavat tasapainottelun niiden vaikeusasteiden välillä. Sen molemmat algoritmit voivat olla helpompia kuin jos niitä olisi vain yksi. Tämä mahdollistaa paremman todennäköisyyden yksittäiselle solmulle tai pienelle yhtymälle voittaa kilpailu lohkon ratkaisemisessa. Toinen syy siihen, miksi kyseinen ratkaisu pienentäisi yhtymien kokoa, on sen vaatimus luottamuksesta. Koska algoritmissa Y käytetään Coinbase-palveluun liittyvää yksityisavainta, voisi yksi käyttäjä halutessaan suorittaa väärinkäyttöä tai varastaa avaimen. Ratkaisun esittelevä tutkimus (Bastiaan, 2015) uskoo louhimisyhtymien tarpeen luottaa sen jäseniin vähentävän yhtymien kokoa huomattavasti. Ratkaisuun liittyy muutama negatiivinen puoli tai ongelma, joiden takia sitä ei todennäköisesti ole ainakaan toistaiseksi otettu käyttöön. Ensinnäkään sen avulla ei voida estää tilannetta, jossa yksi hyökkääjä suorittaa iskun lohkoketjuun omalla laitteistollaan, vaan se ainoastaan ehkäisee yhtymiä saavuttamasta 51 prosenttia laskentatehosta. Toinen haaste ratkaisuun liittyen on algoritmien vaikeuden säätely. Koska louhimiseen lisätään yksi ylimääräinen algoritmi, ei ensimmäinen ja alkuperäinen voi pysyä täysin ennallaan, koska silloin louhiminen muuttuisi entistä vaikeammaksi. Sopivan vaikeusasteen löytäminen molemmille algoritmeille on tärkeää muun muassa jo siksi, että kymmenen minuutin aikaväli lohkojen louhinnassa säilyisi. (Eyal & Sirer, 2014).

4 TUPLAKULUTUS

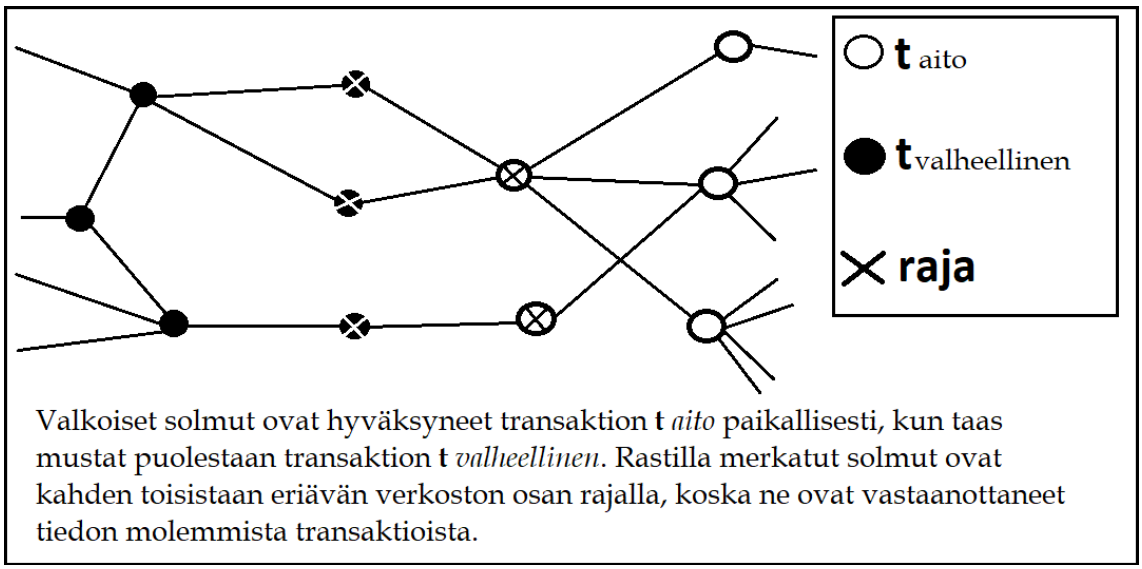
Tuplakulutus (engl. doublespending) lohkoketjuissa tarkoittaa tiedon lähettämistä tai siirtämistä lohkoketjuun useammin kuin oikeasti kuuluisi. Esimerkiksi Bitcoinin tapauksessa tämä tarkoittaisi saman kolikon käyttämistä kahteen kertaan. Tällöin rahan molemmat vastaanottajat uskovat saavansa samalla yksityisavaimella varustetun bitcoinin, mutta todellisuudessa toinen heistä jää ilman korvausta. Tuplakulutus on mahdollista suorittaa ainakin kahdella tavalla, joista ensimmäinen liittyy jo aikaisemmin käsiteltyyn 51 prosentin hyökkäykseen ja toinen todennäköisyyksiin ja puutteellisuuksiin lohkoketjun ominaisuuksissa. (Herrmann, 2012) Tässä luvussa käsitellään tuplakuluttamisen suorittamista ja siihen vaikuttavia tekijöitä. Luku kuvailee hyökkäykseen liittyvät vaiheet aluksi pääpiirteittäin, mutta myöhemmin suhteellisen yksityiskohtaisesti. Lopuksi luvussa käsitellään erilaisia ratkaisuja kyseiseen haavoittuvuuteen.

4.1 Hyökkäyksen suorittaminen

Kuten jo luvussa 3 todettiin, 51 prosentin hyökkäyksen avulla voidaan lohkoketjuun tallentaa tietoa, joka ei ole paikkaansa pitävää. Tämä pitää sisällään myös mahdollisuuden suorittaa tuplakulutusta. Kuvitellaan, että henkilöllä A on esimerkiksi 1 bitcoin, jonka hän lähettää maksuksi henkilöille B ja C, joista vain toinen oikeasti vastaanottaa kolikon. Jotta esimerkistä tulisi käytännönläheisempi, sovitaan A:n yrittävän ostaa autoa molemmilta kauppiailta, eli B:ltä ja C:ltä. A maksaa molemmat autot samaan aikaan, jolloin maksutapahtumat siirtyvät odottamaan hyväksyntää ja pääsyä viralliseen lohkoketjuun. Nyt lohkoketjusta on syntynyt kaksi versiota: oikeana pidetty ja virheellinen. Ilman erityistä manipulointia on kyse vain silkasta tuurista kumpi kauppiaista vastaanottaa maksun. Sovitaan, että kauppias B vastaanottaa A:n maksun, jonka jälkeen hän lähettää maksetun auton A:lle. Virallisessa lohkoketjussa lukee nyt kyseinen maksutapahtuma, jossa lähettiin yksi bitcoin A:n ja B:n välillä, mutta virheellinen lähetys C:lle on toisessa lohkoketjussa. Jos A omaisi tässä tapauk-

sessa resurssit suorittamaan 51 prosentin hyökkäyksen, voisi hän myös tehdä tuplakulutuksen samalle yhdelle bitcoinille. Niin kuin aikaisemmin jo todettiin, virallinen lohkoketju on se, joka on kuvainnollisesti pisin, eli siinä on eniten hyväksyttyjä maksutapahtumia. Nyt A voi toiminnallaan kohdistaa hallitsemansa laitteiston käyttämään virheellistä lohkoketjua, jonka uusin maksutapahtuma on A:n maksu C:lle. Kun aikaisemmin virheellinen lohkoketju muuttuu viralliseksi, on myös virheellinen maksu muuttunut oikeaksi, jolloin A on onnistunut käyttämään saman bitcoinin kahdesti. (Bahack, 2013)

Toinen tapa suorittaa tuplakulutus on lähettää kaksi lähes identtistä maksutapahtumaa, joista vain toinen oikeasti jää lohkoketjuun (Herrmann, 2012). Tällaisessa tapahtumassa hyökkääjän tavoitteena on lähettää sama bitcoin omasta osoitteestaan uhrille ja itselleen toiseen osoitteeseen. Lähes samalla tavoin kuin aikaisemmassa esimerkissä, kyseessä on kilpailu siitä, kumpi maksutapahtumista päätyy oikeaan lohkoketjuun. Toisin kuin edellisessä esimerkissä, jossa oletettiin virheellisen lähetyksen päätyvän omaan virheelliseen lohkoketjuunsa, yritetään tällaisessa hyökkäyksessä lisätä virheellinen lähetys suoraan oikeana pidettyyn lohkoketjuun. Nyt kyse on vain siitä, kumpi kahdesta transaktiosta hyväksytään ensin. (Karame, Androulaki, & Capkun, 2012). Tällaisessa hyökkäyksessä suoritetaan siis kaksi transaktiota; transaktio t_{aito} ja $t_{valheellinen}$. Hyökkääjän kannalta optimaalinen tilanne vaatii kahden ehdon täyttymistä, eli että transaktio t_{aito} saapuu uhrille ensimmäisenä, mutta $t_{valheellinen}$ hyväksytään ensimmäisenä lohkoketjuun. Se, kumpi transaktio saa ensin hyväksynnän, riippuu pääosin tuurista. Hyökkääjän on kuitenkin mahdollista manipuloida todennäköisyyksiä hyväkseen, josta hyvänä esimerkkinä toimii kuvion 2 hahmotus lohkoketjuverkoston vaikutuksesta. (Herrmann, 2012).



Valkoiset solmut ovat hyväksyneet transaktion **t** *aito* paikallisesti, kun taas mustat puolestaan transaktion **t** *valheellinen*. Rastilla merkatut solmut ovat kahden toisistaan eriävän verkoston osan rajalla, koska ne ovat vastaanottaneet tiedon molemmista transaktioista.

KUVIO 2 Verkoston vaikutukset hyökkäykseen (Herrmann, 2012)

4.1.1 Verkoston solmujen vaikutus

Kun kaksi transaktiota lähetetään lähes samaan aikaan lohkoketjun verkostoon, ei niiden hyväksymisen järjestykseen voida vaikuttaa kovinkaan merkittävästi. Hyväksymisen nopeuteen ja tuplakulutuksen tunnistamiseen vaikuttaa sen sijainti solmujen muodostamassa verkostossa. Tällaisessa tapauksessa lohkoketju sisältää kolmenlaisia solmuja; vain transaktion t_{aito} nähneet, vain transaktion $t_{valheellinen}$ nähneet, ja molemmat transaktion nähneet solmut. Vain yhdestä transaktiosta tietoiset solmut lähettävät vastaanottamansa transaktion naapureilleen, kun taas rajalla olevat solmut hylkäävät toisena saapuneen transaktion. Tällaisessa hyökkäyksessä optimaalinen lähestymistapa olisi lähettää t_{aito} uhrille ja $t_{valheellinen}$ hyökkääjän kontrolloimalle solmulle. Jotta hyökkäys pysyisi huomaamattomana uhrille, eivät uhri ja hyökkääjän kontrolloima solmu saa olla yhteydessä toisiinsa. Verkoston muodostelmalle hyökkääjä ei voi mitään, koska yhteydet muodostuvat sattumalta, mutta on keinoja, joilla se pystyy vaikuttamaan lopputulokseen. Jos hyökkääjän ja hänen kontrolloiman solmun sijainti on epäedullinen hyökkäyksen kannalta, voi hän käyttää apuna algoritmia, jonka tarkoituksena on keskeyttää transaktiot havaittuaan mahdolliset epäedullisuudet. Tällaisesta algoritmista annetaan esimerkki kuviossa 3, joka kirjoitettu pseudokoodilla. Koodin toiminta ja hyökkäyksen kulku selitetään seuraavaksi.

4.1.2 Hyökkäyksen tekninen toteutus

Suorittaakseen pseudokoodin mukaisen hyökkäyksen, tarvitsee hyökkääjän käyttää muunneltua lohkoketjusovellusta transaktioiden lähettämiseen. Algoritmin tavoite on tarkastella muuttujaa ”viive” (engl. delay), joka on erotus ajoista, joina aito ja valheellinen transaktio viestitetään eteenpäin uusille solmuille. Koska hyökkääjä ei voi varmasti onnistua valheellisen transaktion lisäämisessä lohkoketjuun, voi hän parantaa todennäköisyyttä peruuttamalla transaktion ja tekemällä sen uudestaan niin monta kertaa, kunnes viive on mahdollisimman edullinen hyökkäyksen kannalta. Jos viive on suurempi

```
error ← CHECK(parameters)
if error then
    return "Error"
end if
disconnect and prevent new connections   ▷ virheen tai ongleman sattuessa yhteys katkaistaan
error ← BITCOINCONNECT(victim)
if error then
    return "Error"
end if
(t_genuine, t_rogue) ← CREATETRANSACTIONS(addresses, amount)
if delay ≥ 0 then                                   ▷ viive tarkistetaan
    error ← ADDTOLOCALPOOL(t_genuine)
    BITCOINRELAY(t_genuine)
    if error then
        return "Error"
    end if
    time_start ← GETTIMEOFDAY()
    for all helper ∈ helpers do
        TCPCONNECT(helper)
        time_now ← GETTIMEOFDAY()
        delay_adjusted ← delay − (time_now − time_start)
        delay_adjusted ← max(0, delay_adjusted)      ▷ viive >= 0
        TCPSEND(t_rogue, delay_adjusted)
        TCPDISCONNECT(helper)
    end for
else                                                ▷ viive < 0
    for all helper ∈ helpers do
        TCPCONNECT(helper)
        TCPSEND(t_rogue, 0)
        TCPDISCONNECT(helper)
    end for
    SLEEP(−delay)
    error ← ADDTOLOCALPOOL(t_genuine)
    BITCOINRELAY(t_genuine)
    if error then
        return "Error"                              ▷ hyökkäys on jo matkalla
    end if
end if
```

KUVIO 3 Tuplakulutushyökkäyksen pseudokoodi (Herrmann, 2012)

kuin nolla, tarkoittaa se sitä, että transaktio t_{aito} viestitetään nopeammin seuraaville solmuille ja päätyy se myös todennäköisemmin osaksi lohkoketjua. Jos viive on siis suurempi kuin nolla, keskeytetään transaktioiden lähettäminen. Jos viive on puolestaan negatiivinen, voidaan hyökkäystä jatkaa. (Herrmann, 2012). Vaikka hyökkäysalgoritmin avulla hyökkääjä voi parantaa onnistumisen to-

dennäköisyyttä, on onnistumisprosentti silti hyvin pieni, jopa alle prosentti (Bamert & muut, 2013).

4.2 Ongelman ratkaiseminen

Tuplakulutuksen mahdollisuus on yleisesti tiedostettu ongelma ja sitä varten on jo tehty toimenpiteitä. Yleisesti ottaen jo Bitcoinin teknisessä esittelyssä todetaan, että lohkoketjuteknologia ja aikaisemmin mainittu proof-of-work ratkaisee tuplakuluttamisen (Nakamoto, 2008). Tämä ei tietenkään täysin pidä paikkaansa, koska vaikkakin kyseinen ratkaisu tekee tuplakuluttamisesta erittäin vaikeaa, on se kuitenkin mahdollista. Bitcoinin lohkoketju ei tällä hetkellä pysty ratkaisemaan tätä ongelmaa millään tavalla, joten se vaatii parantelua. Erilaisia vaihtoehtoja ovat muun muassa lohkoketjun toimintaperiaatteiden muokkaaminen tai erilaisten sovellusten käyttöönotto. Ratkaisu, jolla pystytään osittain ehkäisemään tuplakuluttamista, on aikalukon luominen transaktioiden käsittelyyn. (Yu, Shiwen, Li & Huijie, 2017).

Aikalukot ovat eräänlaisia älysopimuksia, joita lohkoketjun sisällä voidaan käyttää kaupankäynnin monipuolistamiseen (Poon & Dryja, 2016). Bitcoinin virallisessa lohkoketjussa on mahdollista käyttää älysopimuksia, mutta hyvin kankeasti. Ongelmana Bitcoinin tapauksessa on erilaisten sovellusten tarve liittää ne lohkoketjuun, joka puolestaan vaatii yhteistyötä louhijoilta. Erilaisia aikalukkoja on tällä hetkellä Bitcoinin lohkoketjussa neljä, joista ensimmäinen oli kiinnitetty jo valmiiksi lohkoketjun protokollaan, mutta kolme jälkimmäistä ovat myöhemmin liitettyjä (Bitcoin.org, 2018). Aikalukoissa on paljon yksityiskohtaisia eroja, mutta ne kaikki nimensä mukaisesti viivyttävät maksutapahtuman siirtymistä tai lähettämistä lohkoketjuun. Viivästyttämällä voidaan estää tuplakuluttamista siten, että kun viiveeksi laitetaan tarpeeksi pitkä aika, on sen oikeellisuus ehditty tarkistaa perinpohjaisesti (Todd, 2014). Koska lohkoketjut eivät tavallisesti tunne päivämäärän käsitettä, voidaan lukoille antaa parametreina joko sekunteja tai louhittuja lohkoja. Kyseisten muuttujien avulla voidaan valita sopiva viive, mutta haasteena tässä on tiettyjen liiketoimintamallien ominaispiirteet. Esimerkiksi ravintola-alalla ja varsinkin pikaruokaravintoloissa, asiakkaat eivät ole valmiita odottamaan pitkää varmistusviivettä maksamisen yhteydessä. Täysin vedenkestävää ratkaisua ei ole ainakaan Bitcoinin lohkoketjua koskien vielä keksitty. (Yu ym., 2017)

5 HYÖKKÄYS KOLMANNEN OSAPUOLEN PALVELUUN

Kolmannen osapuolen palveluilla tässä tutkielmassa tarkoitetaan erilaisia sivustoja ja yrityksiä, jotka tarjoavat lohkoketjuteknologiaa tukevia tai hyväksikäyttäviä ratkaisuja. Mainio esimerkki tällaisista palveluista ovat kryptovaluuttoja välittävät ja säilövät sivustot, jotka viime vuosina saaneet runsaasti lisää käyttäjiä aiheen suosion kasvun myötä. Viides luku käsittelee hyökkäyksiä ja haavoittuvuuksia, joita tällaisiin palveluihin kohdistuu. Luku sisältää tietoa hyökkäyksien yleisyydestä, syistä niiden tapahtumiselle, sekä ratkaisuehdotuksia ongelmiin.

5.1 Välittäjäpalveluiden haavoittuvuudet

Aikaisemmin mainitut ”kryptopörssit” tarjoavat suosituimpien kryptovaluuttojen myyntiä vaihdossa Fiat-rahaan tai toisiin kryptovaluuttoihin. (Heid, 2014) Vaihdannan lisäksi pörssit useimmiten tarjoavat käyttäjilleen myös lompakon, johon he voivat vaivatta säilöä hankkimansa valuutat. Pörssit pystyvät käyttäjäystävällisesti ja nopeasti liikuttamaan asiakkaidensa varoja merkittävän varjopuolen ansiosta, joka on heidän täysi hallinta käyttäjien kryptovaluutoista. Pörssit pitävät hallussaan kryptovaluuttojen yksityiset avaimet, jotka toimivat salasanana valuutan hallitsemiseen ja turvaavat sen omistamisen. Kryptovaluuttojen yksi hyödyistä on se, ettei välikäsiin tarvitse luottaa. Silti monet riskeeraavat varansa säilyttämällä niitä kolmannen osapuolen palveluissa, jotka eivät pysty takaamaan niiden turvallisuutta (McCorry ym., 2017). Ideaalitilanne turvallisuuden kannalta olisi sellainen, jossa jokainen digitaalisen valuutan omistaja ainoastaan itse tietäisi varojensa yksityisavaimen.

Pörssien alttius erilaisille hyökkäyksille on tilastojen varjolla keskimääräisesti erittäin huomattava. Vuosien varrella monet pörssit ovat joutuneet onnistuneiden iskujen kohteeksi ja menetettyjen kryptovaluuttojen arvo arvioidaan olevan jopa useita miljardeja dollareita (McCorry ym., 2017). Erittäin huolestut-

tavaa on onnistuneiden hyökkäyksien yleisyys. Jopa noin kolmas osa pörsseistä on ollut murtautumisen kohteena vuosien 2009 ja 2015 välillä. Yksi suurimmista hyökkäyksistä kohdistui japanilaiseen Mt. Gox pörssiin vuonna 2013, jolloin menetettiin noin 850 tuhatta bitcoinia. Onnistuneet hyökkäykset voivat luonnollisesti olla erittäin kalliita pörssien käyttäjille, jotka menettävät varansa, mutta myös pörssit itse joutuvat vastuuseen tehdyistä murroista. Suuren tietomurron jälkeen pörssin mahdollisuus jatkaa toimintaansa uskottavasti on pieni ja lähes puolet kaikista markkinapaikoista ovat vain kadonneet johtuen erilaisista ongelmista. (Chavez-Dreyfuss, 2016) Aineellisten vahinkojen lisäksi hyökkäykset aiheuttavat paljon aineettomia vahinkoja. Luottamus järjestelmän toimivuuteen kärsii jokaisen iskun myötä. Lohkoketjuteknologian ja erityisesti kryptovaluuttojen läpimurto osaksi arkipäiväistä käyttöä vaatii ensisijaisesti luottoa sen käyttäjiltä ja massoilta, jota tietomurrot tehokkaasti horjuttavat (Raymaekers, 2015).

5.2 Haavoittuvuuden syyt

Turvallisuuteen liittyvissä asioissa järjestelmä on sanonnan mukaan usein yhtä vahva kuin sen heikoin lenkki, joka puolestaan on lähes poikkeuksetta järjestelmän käyttäjä eli ihminen. Huonot ja useaan kertaan kierrätetyt salasanat voivat pahimmassa tapauksessa johtaa käyttäjän kaikkien varojen menetykseen, koska monet pörssit eivät vaadi esimerkiksi kaksiosaista todennusta. Hypoteettisesti on täysin mahdollista, että huolimattoman käyttäjän tilille voidaan kirjautua ja suorittaa siellä mitä tahansa transaktioita hänen varoillaan. Tämä osoittaa, että vaikka lohkoketjuteknologiaa itsessään pidetään erittäin turvallisena ratkaisuna, on siihen pohjautuvien käyttökohteiden heikkoudet silti olemassa.

Käyttäjien oman toiminnan lisäksi kolmannen osapuolen palveluissa turvallisuutta heikentää niiden oma tietoturva. Kun hyökkääjä tietää käyttäjän pääsytiedot, on mahdollisesti vain yksi käyttäjä uhattuna, mutta jos hyökkääjä onnistuu murtautumaan esimerkiksi kryptovaluuttoja välittävän pörssin palvelimille, on uhattuna sen koko käyttäjäkunta. Pörsseillä ja samalla käyttäjällä on karkeasti jaoteltuna kaksi tapaa varastoida kryptovaluuttaa: kylmät ja kuumat lompakot (engl. cold and hot wallets). Yleisesti lompakolla tarkoitetaan kokoelmaa kryptovaluuttoihin liittyvistä osoitteista ja avaimista. Kuumalla lompakolla tarkoitetaan tapaa säilöä tietoa verkossa tai laitteella, joka on kytkettynä verkkoon. Tämä mahdollistaa sen, että kryptovaluuttoja voidaan käyttää välittömästi ilman niiden kaivamista arkistosta tai vastaavanlaisesta säilöstä. Kylmässä lompakossa tieto puolestaan säilötään poiskytkettynä verkosta, josta varat tai tieto on siirrettävä kuumaan lompakkoon silloin, kun sitä halutaan käyttää. (McCorry ym., 2017)

Molemmissa tavoissa säilyttää tietoa on omat hyvät ja huonot puolensa, mutta turvallisuudessa kylmäsäilöntä on huomattavasti riskittömämpää. Kylmä lompakko voi kaikessa yksinkertaisuudessaan olla paperi, johon kryptova-

luutan yksityisavain on kirjoitettu ylös. Oikeastaan ainut heikkous tällaisessa säilöntätavassa on se, ettei säilöttyä kryptovaluuttaa ole mahdollista käyttää välittömästi. Kylmäsäilönnän hyvä puoli on sen erinomainen turvallisuus ja varmuus, jos säilöntä on tehty järkevästi. Jos yksityisavaimia ei pidetä yhteydessä verkkoon, on sen ainoat uhat fyysisiä, eli käytännössä muita ihmisiä, onnettomuuksia tai vastaavia tapahtumia. Kuuman lompakon sisältävät tiedot ovat puolestaan koko ajan yhteydessä verkkoon, joten silloin ne ovat haavoittuvia internetissä tapahtuville hyökkäyksille. (Goldfeder, Bonneau, Kroll & Felten, 2014)

Kryptovaluuttojen säilönnässä on myös riskejä, joita Fiat-rahan yhteydessä ei tavanomaisesti ole. Tähän vaikuttaa kryptovaluuttojen ja lohkoketjun anonyymiys, johon liittyy paljon hyviä ja huonoja ominaisuuksia. Eräs negatiivinen puoli on, että anonyymiys antaa paremman mahdollisuuden suorittaa sisältäpäin kohdistettuja hyökkäyksiä. Esimerkiksi perinteisessä pankkien maailmassa työntekijä ei voi tehokkaasti siirtää pankin varoja omalle tililleen jäämättä kiinni teoistaan, koska tavalliset pankkitilit ovat aina yhteydessä henkilöihin (McCorry ym., 2017). Hypoteettisesti on täysin mahdollista, että kryptovaluuttapörssissä työskentelevä henkilö voisi siirtää varojaan anonyymiin kylmälompakkoon. Tällöin kaikki lohkoketjua ylläpitävät solmut tietävät kyseisestä transaktiosta ja varmistavat sen aivan kuten muutkin transaktion tietämättä sen laittomuudesta ja osapuolista. Tämä on hyvä esimerkki lohkoketjuihin liittyvän valvonnan ja sääntöjen puutteellisuudesta, eli välillä on hyvin vaikeaa, ellei mahdotonta erotella normeja tai oikeudenmukaisuutta.

5.3 Ongelman ratkaiseminen

Kuten jo edellisessä alaluvussa useasti todettiin, on kylmä lompakko useimmiten huomattavasti turvallisempi tapa säilöä kryptovaluuttaa tai mitä tahansa informaatiota. Siksi tavallisen käyttäjän onkin turvallisuuden kannalta suositeltavaa säilöä varansa esimerkiksi omalle kovalevylle tai jopa paperille. Yksinkertaisin paperilompakko voi olla esimerkiksi vihko, johon kryptovaluutan julkiset ja yksityisavaimet ovat kirjoitettu kynällä muistiin. Pörssien on myös mahdollista hyödyntää kylmäsäilöntää ja osa niistä sitä jo tekeekin. Tämä tuo varoille lisää turvallisuutta, mutta teettää lisää töitä ja rasitteita. Pörssi voi halutessaan varastoida osan käyttäjien varoista verkosta poiskytkettyyn arkistoon, josta ne vasta tarpeen tullen siirrettäisiin kuumaan lompakkoon. Etu tällaisessa ratkaisussa on vahingon minimoiminen mahdollisen tietomurron tapahtuessa. Jos hyökkääjä murtautuu pörssin palvelimeen ja tietokantaan, ovat kaikki kuumassa säilössä olevat varat silloin uhattuna. Pahimmassa tapauksessa pörssin suurin osa tai jopa kaikki yksityisavaimet voidaan menettää, kuten Mt. Goxin tapauksessa kävi. Jos vain osa varoista säilytetään verkossa, mutta suurin osa kylmässä ja samalla turvassa digitaalisilta hyökkäyksiltä, on huonoin mahdollinen tilanne huomattavasti parempi. Ratkaisussa on myös rasitteensa. Silloin kun tieto on varastoitu pois verkosta, ei sitä myöskään ole mahdollista käyttää

välittömästi. Viivästykset ja pitkät odotusajat tiedonsiirrossa, erityisesti valuuttojen yhteydessä, eivät kuitenkaan ole käyttäjien mieleen. Osittainen kylmäsäilöntä on keino vähentää riskejä, mutta suoranainen ratkaisu se ei ole. (McCorry ym., 2017)

Ennaltaehkäiseviä parannuksia verkkosivujen ja palvelimien turvallisuuden takaamiseksi on jo tietenkin olemassa, mutta pörssien yhteydessä reaktiivisia metodeja ei vielä ole juurikaan hyväksikäytetty. McCorry ja kumppanien (2017) ratkaisuehdotus kolmannen osapuolen palveluiden turvallisuuden lisäämiseksi käyttää hyväkseen jo aikaisemmin esiteltyä aikalukkoa, jonka avulla transaktioiden toimeenpanoa voidaan viivyttää. Ehdotuksessa valtaosa pörssin hallitsemista varoista säilytetään kylmäsäilössä, josta ne tuodaan vain tarvittaessa alttiiksi verkkoyhteydelle. Ratkaisun kulmakivenä ovat kolme erilaista avainta, joiden avulla erilaisia siirtoja tai toimintoja voidaan hyväksyä. Avaimet eivät suoranaisesti liity millään tavalla itse lohkoketjuun, vaan niitä käytettäisiin ainoastaan kolmannen osapuolen palvelun sisällä. Avaimia on seuraavanlaisia:

1. Kuumat avaimet: Aina yhteydessä verkkoon
2. Kylmät avaimet: Tarvittaessa yhteydessä verkkoon
3. Holviavain: Käytetään tarvittaessa avainten palauttamiseen

Asiakas voi suorittaa kahdenlaisia siirtoja pörssin sisällä, joita ovat yksityisavaimien siirtäminen kylmäsäilöön ja niiden nostaminen hetkellisesti takaisin kuumaan lompakkoon. Varojen siirtäminen kylmään voidaan toteuttaa aina välittömästi, koska sellaisen siirron avulla mahdollinen hyökkääjä ei voi varastaa yksityisavaimia. Varojen siirtäminen kylmästä kuumaan riippuu kuitenkin avaimesta, jolla siirto on allekirjoitettu tai hyväksytty. Kylmä avain on ainoastaan käyttäjän tiedossa, eikä sitä säilytetä yhteydessä verkkoon. Tällaisen avaimen haltijan oletetaan aina olevan asianomainen henkilö, koska hyökkääjällä ei pitäisi olla mahdollisuutta saada sitä tietoonsa. Jos varojen nostamisella pois kylmästä on kiire, voidaan allekirjoittamisessa käyttää kylmää avainta, jolloin siirto toteutuu välittömästi. Asiakkaalla on myös mahdollisuus käyttää kuumaa avainta, joka voi olla uhattuna tietomurron sattuessa. Varojen nosto, joka on allekirjoitettu kuumalla avaimella, ei toteudu välittömästi, koska silloin käyttäjän on odotettava aikalukkoon asetetun ajan verran. Aikalukitus auttaa palvelun ylläpitäjiä hyökkäyksen sattuessa palauttamaan tilanteen ennalleen. Kuvitellaan hypoteettinen hyökkäys palveluun, jonka suurin osa varoista sijaitsee kylmässä varastossa. Kun hyökkääjä on murtautunut palvelun sisälle, on vain pieni osa varoista, eli kuumassa varastossa olevat varat vaarassa. (Möser, Eyal & Sirer, 2016) Myös kuumat avaimet, joiden avulla kylmässä varastossa sijaitsevat varat voidaan nostaa, ovat uhattuna tai jo menetetty hyökkääjän haltuun. Hyökkääjä ei kuitenkaan pysty siirtämään varoja välittömästi johtuen aikalukon viivästyksestä, jonka aikana ylläpidon oletetaan huomaavan poikkeava käytös. Hyökkäyksen havaittua palveluntarjoajan hallussa olevan holviavaimen (engl. vault key) avulla voidaan jäädyttää kaikki varojen siirrot kylmästä kuu-

maan lompakkoon. Konsepti tarjoaa holviavaimelle myös toisen toiminnon, jonka toimivuudelle esitetään kritiikkiä jo sen keksijöiltä. Jos hyökkäys havaittaisiin liian myöhään tai siihen reagoinnissa epäonnistuttaisiin, voitaisiin holviavaimen avulla tuhota kaikki vaarassa olevat varat. (McCorry ym., 2017) Vaikka ratkaisu teoriassa toimiikin, liittyy siihen useita kyseenalaisia ja pohdintaa vaativia asioita. Esimerkiksi juuri mainitsema varojen tuhoaminen uhkan käydessä toteen jakaa varmasti mielipiteitä useisiin suuntiin ja saattaisi aiheuttaa ongelmia oikeudellisissa asioissa. Ratkaisu on ainakin toistaiseksi vielä ehdotus.

6 YHTEENVETO

Tutkielmassa käsiteltiin lohkoketjuteknologiaa yleisesti ja siihen liittyviä haavoittuvuuksia. Lohkoketjut ovat teknologiana tuore ilmiö, mikä vaikuttaa siihen kohdistuvien tutkimusten määrään ja usein myös laatuun. Useat tutkimukset myöntelevät muutamia toistuvasti samoja tutkimuksia, mistä johtuen sisällöltään kattavia ja uutta informaatiota tuovia lähteitä ei löytynyt paljoa. Lisäksi useimmat teokset aiheesta ovat pohtivia ja spekulatiivisia, johtuen teknologian nuoruudesta.

Tutkielma alkaa kohtuullisen yksityiskohtaisella lohkoketjuteknologian ominaisuuksien käsittelyllä. Johtuen jo useaan kertaan mainitusta teknologian nuoruudesta ja sen vieraudesta useimmille, pyrkii tutkielma avaamaan käsitteen kattavasti. Lohkoketjuista esiteltiin sen toimintaperiaatteet, ominaisuudet, hyödyt ja käyttökohteet. Lisäksi tarkentavaa tietoa yleiseen toimintaan tulee koko tutkielman ajan.

Erilaisia haavoittuvuuksia tutkielmassa käsiteltiin kolme: 51 prosentin hyökkäys, tuplakuluttaminen ja hyökkäys kolmannen osapuolen palveluihin. Muita vähemmän vakavia haavoittuvuuksia tai ongelmia on olemassa, mutta tutkielma keskittyi vain niistä merkittävimpiin. Haavoittuvuudet valikoituivat tutkielmaan jokainen hieman eri syistä. 51 prosentin hyökkäystä ja tuplakuluttamista voitaisiin jopa kutsua klassisiksi ongelmiksi lohkoketjuissa. Nämä haavoittuvuudet vakavia, mutta niiden suorittaminen on erittäin vaikeaa. Esimerkiksi 51 prosentin hyökkäystä ei ole vielä koskaan onnistuttu suorittamaan, vaikkakin entiteetti on kerran pitänyt hallussaan yli puolta laskentatehosta (Li, 2017). Syy siihen, miksi nämä haavoittuvuudet ovat olemassa, johtuu lohkoketjuteknologian yleisesti toimintaperiaatteista. Juuri siksi nämä ongelmat ovat paljon puhetta herättäviä, eikä niihin ole helppoja ratkaisuja. Erilaisia, mutta pääosin samoihin periaatteisiin perustuvia ratkaisuja kyseisiin haavoittuvuuksiin on ehdotettu. Osa ehdotetuista ratkaisuista ei ole edennyt paperia pidemmälle, kun taas jo käyttöönotetut ratkaisut ovat ainoastaan hyökkäyksiä ehkäiseviä ratkaisuja.

Hyökkäys kolmannen osapuolen palveluihin valikoitui tutkielmaan pääosin sen yleisyyden vuoksi, mutta myös sen vakavuuden takia. Tutkielmassa selvisi, että kolmannen osapuolen palveluihin kohdistuvat iskut johtuvat lähes kokonaan internetverkkoon liittyvistä ominaisuuksista. Lohkoketjuverkosto on itsessään suhteellisen turvallinen, mutta internetpalveluiden kautta lohkoketjun sisältöön voi päästä käsiksi, jos siihen liittyviä avaimia säilyttää kolmannen osapuolen palveluissa tai muualla verkossa. Tutkielma löysi potentiaalisia ehkäisykeinoja kolmannen osapuolen palveluihin kohdistuviin hyökkäyksiin, mutta täysin mullistavia ratkaisuja ei löytynyt, joka puolestaan oli odotettavaa.

Kaikki tutkielmassa käsitellyt haavoittuvuudet ovat erilaisia ja omalla tavallaan vakavia. Tutkimustyötä ratkaisujen löytämiseksi on tehty, mutta ongelmien ratkaiseminen todennäköisesti vaatii merkittäviä muutoksia perinteiseen lohkoketjuteknologiaan. On kuitenkin tärkeä muistaa, että erilaisia lohkoketjuratkaisuja on useita, eivätkä kaikki haavoittuvuudet välttämättä esiinny niissä samalla tavoin.

Käsitellyt haavoittuvuudet ovat toistaiseksi vielä olemassa. Lohkoketjut ovat teknologiana todennäköisimmin elinkaarensa alkumetreillä, joten on mahdollista, että haavoittuvuuksiin löydetään ratkaisuja. Vaikka haavoittuvuuksia lohkoketjuista löytyy, voidaan sitä silti pitää turvallisena ratkaisuna säilyttää ja siirtää tietoa. Tämä johtuu siitä, että tutkielmassa analysoidut hyökkäykset ovat joko epätodennäköisiä ja hankalia toteuttaa, tai eivät perustu itse lohkoketjuteknologiaan. Täydellinen läpäisemättömyys ja turvallisuus ei tietoturvaasioihin liittyen useimmiten edes ole realistista. Haavoittuvuudet vaativat kuitenkin edes osittaisen ratkaisun, jotta lohkoketjuteknologia onnistuisi murtamaan tiensä arkipäivän teknologiaksi. Kehitystä kuitenkin tapahtuu koko ajan, joten näkymät ovat positiiviset. On silti muistettava, että teknologian ja maailman kehittyessä uusia uhkakuvia voi ilmestyä kuin tyhjästä. Lohkoketjut ovat laaja käsite, jota voidaan tutkia monella tapaa. Jatkotutkimuksia olisi mahdollista toteuttaa esimerkiksi lohkoketjuteknologian ominaisuuksien kehittämisestä, sen potentiaalisista käyttökohteista ja niihin liittyvistä haasteista. Lisäksi ongelmat liittyen etiikkaan ja lainsäädäntöön sisältävät paljon potentiaalisia tutkimuskohteita.

LÄHTEET

Bahack, L. (2013). Theoretical Bitcoin Attacks with less then Half of the Computational Power.

Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., & Welten, S. (2013). Have a snack, pay with Bitcoins. In Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on (1-5). IEEE.

Bastiaan, M. (2015). Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin.

Bitcoin Project (2009-2018). Haettu 10.5.2018 osoitteesta https://bitcoin.org/en/release/v0.11.0

Brenig, C., Schwarz, J. & Rückeshäuser, N. (2016). Value of Decentralized consensus Systems-Evaluation Framework. ECIS.

Chavez-Dreyfuss, G. (2016). Cyber threat grows for bitcoin exchanges. Reuters.

Coinmarketcap. (2018). Haettu 1.4.2018 osoitteesta https://coinmarketcap.com/all/views/all/

Drainville, D. (2012). An analysis of the Bitcoin electronic cash system.

Easley, D., O'Hara, M., & Basu, S. (2017). From mining to markets: The evolution of bitcoin transaction fees.

Eyal, I. & Sirer, E. G. (2017). How to disincentivize large bitcoin mining pools.

Goldfeder, S., Bonneau, J., Kroll, J. A., & Felten, E. W. (2014). Securing bitcoin wallets via threshold signatures.

Google Scholar Plotr. - Blockchain (2018). Haettu 20.4.2018 osoitteesta https://csullender.com/scholar/

Halongmining. (2018). Haettu 1.4.2018 osoitteesta https://halongmining.com/shop/dragonmint-16t-miner/

Heid, A. (2013). Analysis of the Cryptocurrency Marketplace.

Herrmann, M. (2012). Implementation, evaluation and detection of a doublespend-attack on Bitcoin (Master's thesis, ETH Zürich, Department of Computer Science).

Iansiti, Marco, & Lakhani. (2017). The truth about blockchain. Harvard Business Review 95.1, 118-127.

Jacobs, Edwin. (2011). Bitcoin: A Bit Too Far?. Journal of Internet Banking and Commerce 16.2.

Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 906-917). ACM.

King, S. (2013). Primecoin: Cryptocurrency with prime number proof-of-work.

Li, Z. (2013). Will Blockchain Change the Audit?

Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (254-269). ACM.

McCorry, P., Möser, M., & Ali, S. T. (2017). Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough.

Morini, M. (2016). From'Blockchain Hype'to a Real Business Case for Financial Markets.

Möser, M., Eyal, I. & Sirer, E. G. (2016). Bitcoin covenants. In International Conference on Financial Cryptography and Data Security, pages 126–141. Springer

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

Pilkington, M. (2016). 11 Blockchain technology: principles and applications. Research handbook on digital transformations.

Poon, J., & Dryja, T. (2016). The bitcoin lightning network: Scalable off-chain instant payments.

Raymaekers, W. (2015). Cryptocurrency Bitcoin: Disruption, challenges and opportunities. Journal of Payments Strategy & Systems, 9(1), 30-46.

Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.

Todd, P. (2014). OP_CHECKLOCKTIMEVERIFY Haettu 1.6.2014 osoitteesta https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki

Underwood, S. (2016). Blockchain beyond bitcoin. Communications of the ACM 59

Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia.

Wu, D., Dhungel, P., Hei, X., Zhang, C., & Ross, K. W. (2010). Understanding peer exchange in bittorrent systems. In Peer-to-Peer Computing (P2P), 2010 IEEE Tenth International Conference on (1-8). IEEE.

Wüst, K., & Gervais, A. (2017). Do you need a Blockchain?. IACR Cryptology ePrint Archive, 2017, 375.

Yu, X., Shiwen, M. T., Li, Y., & Huijie, R. D. (2017). Fair deposits against double-spending for Bitcoin transactions. In Dependable and Secure Computing, 2017 IEEE Conference on (44-51). IEEE.