Roope Taipale

# KRYPTOVALUUTTOJEN TIETOTURVAUHAT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

# TIIVISTELMÄ

Taipale, Roope
Kryptovaluuttojen tietoturvauhat
Jyväskylä: Jyväskylän yliopisto, 2021, 25 s.
Tietojärjestelmätiede, Kandidaatintutkielman tutkimussuunnitelma
Ohjaaja(t): Seppänen, Ville

Lohkoketjuteknologia ja kryptovaluutat ovat saavuttaneet merkittävää huomiota viime aikoina. Kryptovaluuttojen määrä ja markkina-arvo on kasvanut merkittävästi siitä lähtien kun ensimmäinen kryptovaluutta Bitcoin kehitettiin. Lohkoketjuteknologiaa pidetään turvallisena, mutta kuitenkin käytännössä kryptovaluuttoihin kohdistuu useita erilaisia uhkia. Erilaiset uhat vähentävät kryptovaluuttojen omistamisen turvallisuutta, sekä vaikuttavat negatiivisesti kryptovaluuttojen uskottavuuteen, ja siten niiden arvoon markkinoilla. Tutkielmassa selvennetään kryptovaluuttojen toimintaa, kryptovaluuttoihin kohdistuvia uhkia ja niiden vaikutuksia kryptovaluuttoihin.

Asiasanat: kryptovaluutta, kryptovaluuttojen vaihtoalustat, kyberturvallisuus, tietoturva

# ABSTRACT

Taipale, Roope
Cybersecurity threats in cryptocurrency
Jyväskylä: University of Jyväskylä, 2021, 25 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Seppänen, Ville

Blockchain technology and cryptocurrencies have gathered attention lately. The amount of different cryptocurrencies and their market cap has increased significantly ever since the first cryptocurrency Bitcoin was developed. Blockchain technology in general is considered safe, but in practice certain threats still exist. The different kinds of threats reduce the safety of owning cryptocurrency and the credibility of cryptocurrency in general, thus the threats also affect the cryptocurrencies value in the market. In this literature review first the basics of cryptocurrency are explained, then the cyber threats concerning cryptocurrencies and their effect on cryptocurrencies are reviewed.

Keywords: cryptocurrency, cryptocurrency exchange platform, cybersecurity

# SISÄLLYS

# 1 JOHDANTO

Kryptovaluutat ovat ajankohtainen käsite, ja suhteellisen uusi sijoituskohde. Kryptovaluuttojen asema sijoituskohteena on ollut kiistanalainen, ja kryptovaluuttojen mahdollisuuksiin liittyy paljon epävarmuutta. Tutkimuksen tavoitteena on tarkastella kryptovaluuttoihin ja niiden käyttöön liittyviä uhkia erityisesti tietoturvanäkökulmasta.

Tutkielma on kirjallisuuskatsaus, jonka lähteet on etsitty pääosin Goole Scholarilla ja IEEE Xplorerilla. Tutkielmassa ensin selitetään kryptovaluuttojen käyttöön ja toimintaan liittyvät asiat, sekä lohkoketjuteknologian toimintaperiaatteet. Kryptovaluuttojen käyttöön liittyvien asioiden, sekä lohkoketjujen toiminnan ymmärtäminen on tarpeellista voidakseen ymmärtää niihin liittyvien tietoturvauhkien toimintaperiaatteita, ja siten kryptovaluuttojen tietoturvan heikkouksia ja tietoturvan parantamiseksi kehitettyjä ratkaisuja. Tutkielman tutkimuskysymykset ovat seuraavanlaiset:

- Mitä merkittäviä uhkia kryptovaluuttojen toimintaan liittyy, ja mitä keinoja niitä vastaan on kehitetty?
- Mitä merkittäviä hyökkäyksiä kryptovaluuttojen toimintaan liittyen on tapahtunut
- Miten uhat ovat vaikuttaneet kryptovaluuttoihin?

Tutkielma pyrkii tutkimaan informaatiota erilaisista kryptovaluuttojen uhista, niiden kehityksestä, ja pohtia niiden perusteella kryptovaluuttojen ja niiden riskien tulevaisuuden näkymiä.

Luku 2 käsittelee kryptovaluuttoja, ja niihin liittyviä ominaisuuksia ja peruskäsitteitä, kuten lohkoketjut, louhinta ja lompakot. Luku 3 käsittelee tarkemmin niihin liittyviä tietoturvauhkia, historiallisia tapahtumia ja ratkaisuja uhkia aiheuttaviin heikkouksiin. Kryptovaluuttojen ominaisuuksien käsittely on tarkoitettu selventämään erityisesti niitä ominaisuuksia, jotka liittyvät kryptovaluuttojen merkittävimpiin tietoturvauhkiin ja niiden toimintaan. Käsiteltyjen tietoturvauhkien valinta on perustunut historiallisten tapausten merkittävyyteen, ja artikkeleihin, joissa kartoitetaan kryptovaluuttojen tietoturvauhkia.

Lähteiden etsimiseen käytettyjä hakusanoja on käytetty useita erilaisia, kuten esimerkiksi: ”cryptocurrency threats”, ”cryptocurrency exchange breaches”, ”cryptocurrency security” ja ”bitcoin security”. Motiivit tutkielman aiheelle on lohkoketjuteknologian uutuus, sekä kryptovaluuttojen nopea arvonnousu, ja näiden ominaisuuksien johdosta tulleet suurikokoiset, ja vaikeasti ratkaistavat tietomurrot ja muut hyökkäykset. Tutkielmassa ei tarkennuta kryptovaluuttoihin liittyviin lakisääteisiin riskeihin, markkinariskiin tai muihin toimintaperiaatteiden ja käytännön ulkopuolisten tekijöiden aiheuttamiin riskeihin.

# 2 KRYPTOVALUUTAT

Tässä luvussa käsitellään mitä lohkoketjut ovat, lohkoketjuteknologian toimintaperiaatetta, sekä siihen pohjautuvien kryptovaluuttojen, kuten esimerkiksi ensimmäisen ja suurimman kryptovaluutta Bitcoinin toimintaperiaatteita. Luvussa käydään läpi myös kryptovaluuttojen käyttöön liittyviä aiheita, kuten louhintaa, lompakoita, sekä kryptovaluuttojen eri tyyppejä. Lisäksi luvussa käydään läpi tutkielman aihealueen tarpeellisia käsitteitä. Monet lohkoketjuteknologian toiminnan esimerkit perustuvat Bitcoinin lohkoketjuun, joka on toiminut pohjana tuleville lohkoketjuille ja kryptovaluutoille, ja täten sopii havainnollistamaan näiden asioiden perusteet, mutta muitakin merkittäviä lohkoketjumalleja käsitellään tässä luvussa.

## 2.1 Kryptovaluutta Bitcoin ja sen ominaisuudet

Finanssivalvonnan (2019) mukaan kryptovaluutta tarkoittaa salausalgoritmiikkaan perustuvaa virtuaalivaluuttaa, ja virtuaalivaluutoille on yhteistä, että:

- Ne eivät ole keskuspankin tai viranomaisen liikkeeseen laskemia tai takaamia
- Niitä ei välttämättä ole kytketty lailliseksi maksuvälineeksi vahvistettuun valuuttaan
- Niillä ei ole samaa oikeudellista asemaa kuin valuutalla tai rahalla
- Luonnolliset henkilöt tai oikeushenkilöt hyväksyvät niitä vaihdantavälineinä
- Niitä voidaan siirtää, varastoida ja myydä sähköisesti

Ensimmäinen kryptovaluutta on Bitcoin, jonka on kehittänyt Satoshi Nakamoto-nimimerkillä esiintynyt henkilö. Nakamoto julkaisi ideansa lohkoketjuteknologiaan perustuvasta valuutasta ja sen toimintaperiaatteesta vuonna 2008. (Nakamoto, 2008)

Nakamoto esitteli julkaisussaan lohkoketjuteknologian toiminnan, ja kuinka sen pohjalta kryptovaluutta bitcoin toimii. Artikkelissa kerrotaan, kuinka netin kaupankäynti on lähes täysin riippuvainen kolmannen osapuolen instituutioiden tarjoamista palveluista, ja Bitcoin esitetäänkin vaihtoehtoiseksi rahajärjestelmäksi, joka ei ole riippuvainen luottamuksesta kolmannen osapuolen instituutioihin. (Nakamoto, 2008) Bitcoinin markkina-arvo on tutkielman ajankohtana yli 1.2 biljoonaa, ja yksittäinen bitcoin maksaa yli 66 tuhatta Yhdysvaltain dollaria (*CoinMarketCap*, 2021).

Bitcoin on saanut paljon kritiikkiä kyvystään toimia arvon säilyttäjänä sen suuren volatiliteettinsa takia. Bitcoinia pidetäänkin enemmän korkean riskin sijoituskohteena kuin stabiilina arvonsäilyttäjänä. (Franco, 2015)

Franco (2015) on eritellyt Bitcoinin toimintaperiaatteen ja ominaisuuksien tuomia vahvuuksia ja heikkouksia, verrattuna perinteisempiin valuuttoihin ja arvon säilyttäjiin, kuten esimerkiksi kultaan. Bitcoinin vahvuuksia Franco (2015) luettelee muun muassa:

- Bitcoin välttää takavarikoinnin, valuutan hallinnan, ja kohtuuttoman verotuksen. Fiat-rahaa tai arvotavaraa voi takavarikoida tai varastaa. Käyttäjä, jolla on laite millä pääsee internetiin ja yksityisavain voi aina päästä käsiksi varantoihinsa.
- Bitcoinilla ei ole varsinaisia varastointikuluja, muuta kuin mahdolliset kustannukset lompakon hankinnasta.
- Bitcoin on niukka vara, eikä mikään keskushallinto voi päättää sen arvoa. Bitcoin on myös täten deflatorinen vara. Deflaatiota edistävät myös hävitetyt bitcoinit.
- Bitcoin on kryptograafisesti suojattu, toisin kuin arvoesineet, joita pitää suojella fyysisiltä uhilta, tai Fiat-raha, joka on jonkin instituution vastuulla.

Bitcoinin heikkouksista Franco (2015) luettelee esimerkiksi seuraavat:

- Bitcoin on volatiili, mikä johtuu esimerkiksi mahdollisten säännösten aiheuttamasta epävarmuudesta, matalasta likviditeetistä, vähäisestä käyttöönotosta ja muista vastaavista tekijöistä.
- Varan tuotanto ei ole kenenkään hallussa, ja täten voi muuttua valtaosan käyttäjistä niin halutessa.
- Kryptovaluutoilla ei ole samaa laillista asemaa kuin Fiat-valuutalla
- Jotkut valtiot voivat kieltää kryptovaluutan käytön kokonaan

## 2.2 Lohkoketjun ja kryptovaluutan toimintaperiaate

Lohkoketju koostuu tietoaineistoista, jotka koostuvat ketjusta dataa, joita kutsutaan lohkoiksi. Ketjussa yksi lohko käsittää useita transaktioita. Lohkoketju pitenee siihen lisättäessä uusia lohkoja ja täten käsittää koko tilikirjan kaikkien

transaktiotapahtumien historiasta (Nofer ym., 2017). Lohkot vahvistetaan oikeiksi kryptografisesti. Transaktiotapahtumien lisäksi lohkoihin tallennetaan aikaleima ja edellisen lohkon kryptografiset tiivisteet (engl. hash), jotka varmentavat lohkoketjun muuttumattomuuden, sekä satunnaisen muuttujan, jota kutsutaan nimellä nonce (number used once), joka todentaa hashin. Tämä toimenpide varmistaa lohkoketjun eheyden, sillä lohkon sisällön muokkaaminen muuttaisi myös lohkon yksilöllistä hashia (Nofer ym., 2017).

Lohkoketjun verkostossa olevat palvelimet (engl. node) toimivat validoijina lohkoketjun eheydelle. Tämä perustuu konsensusmekanismiin, jossa lohkoketjun verkostossa olevat palvelimet muodostavat konsensuksen lohkon validiudesta. Jos valtaosa palvelimista muodostavat konsensuksen kyseisestä lohkosta, se liitetään lohkoketjuun. Konsensusprosessi varmistaa, että transaktiot ovat lohkossa tietyn ajan verran ennen kuin ne sisältävä lohko liitetään ketjuun, jonka jälkeen lohkojen sisältöä ei voi enää muuttaa. (Nofer ym., 2017)

Lohkoketjuteknologiaan perustuvat kryptovaluutat pohjautuvat tallennettuihin tietoihin transaktioista. Esimerkiksi yksittäinen henkilö ei varsinaisesti omista mitään konkreettista omistaessaan bitcoinia, mutta transaktio on julkisesti todennettavissa, josta näkyy hänen omistavan transaktiossa tulleen määrän bitcoinia. Kyseiselle henkilölle voitiin vaihtaa, ja hän voi edelleen vaihtaa bitcoinia, sillä lohkoketjuun on tallennettu edellisen omistajan omistaneen transaktiossa annetun määrän bitcoinia, ja henkilön vastaanottaessa ne tämä transaktio tallentuu myös lohkoketjuun, jolloin voidaan todentaa hänen olevan näiden bitcoinien hallussapitäjä. (Böhme ym., 2015)

Kaikki bitcoinit voidaan jäljittää transaktiosta aiempaan, aina niiden lähteeseen saakka, ja kaikki bitcoinin vaihtotilanteet ovat julkisia kaikille. Transaktiot järjestetään rekursiivisesti, viittaamalla bitcoinin lähteeseen, eli aiempaan transaktioon. Esimerkiksi henkilö X lähettää henkilölle Y bitcoinia, jotka on saatu henkilöltä Z. (Böhme ym., 2015)

## 2.3 Lompakot

Kuten aiemmin mainittu kryptovaluutan toimintaperiaatteissa, ei kryptovaluutan sinänsä tarvitse olla mitään konkreettista. Bitcoinin lohkoketju ei tallenna tilejä tai tilin varoja, vaan bitcoinin transaktiotapahtumia (Franco, 2015). Kryptovaluuttojen säilyttämistä varten on olemassa lompakoita. Bitcoin lompakot ovat tiedostoja, joihin sisältyy Bitcoin käyttäjätili, tallennetut transaktiot ja yksityiset avaimet, joita tarvitaan valuutan käyttämiseen (Böhme ym., 2015).

Kryptovaluuttoja voidaan varastoida monilla eri tavoilla. Verkkoon kytkettyä lompakkoa kutsutaan kuumaksi lompakoksi. Varastointitapaa, joka ei ole yhteydessä internetiin kutsutaan puolestaan kylmävarastoinniksi. Varastointitapa vaikuttaa merkittävästi varastoinnin turvallisuuteen ja siihen minkälaisia riskejä kryptovaluutan hallussapidolla on.

Kylmien ja kuumien varastojen avaimia voi suojata monilla eri tavoilla. Internetiin kytkemättömiä varastointitapoja ovat lompakot, jotka ovat säilötty

esimerkiksi paperille tai USB-muistitikulle. Tällä tavoin säilöttynä lompakot ovat suojassa haittaohjelmilta, mutta avaimet niistä on ladattava laitteelle, kun lompakon sisältöä halutaan käyttää, jolloin niistä tulee taas alttiita haittaohjelmille (Bonneau ym., 2015). Tämän kaltaisilla varastointitavoilla on myös uhkana ulkoisen säilön hukkaaminen tai rikki meneminen. Esimerkiksi paperinen lompakko voi turmeltua helposti. Jos paperisella avaimella on esimerkiksi QR-koodi sen voi nähdessään hyväksikäyttää ja ottaa varat itselleen. Esimerkkinä tästä on tapaus vuonna 2013 jolloin TV-ohjelmassa näkyi QR-koodi yksityisestä avaimesta paperilompakkoon, jolloin varat otettiin välittömästi, mutta palautettiin myöhemmin omistajalleen (Franco, 2015).

Laitteelliset lompakot eli hardware-lompakot, ovat laitteita joihin tallennetaan yksityisavaimet ja joilla voi hyväksyä transaktioita. Yksityisavaimet eivät missään vaiheessa lähde laitteesta, joten tietokoneella olevat haittaohjelmat eivät pääse niihin käsiksi (Franco, 2015). Hardware-lompakko tarvitsee lompakko-ohjelmiston tietokoneella, joka toimii välikätenä hardware-lompakon ja lohkoketjun kanssa. Ohjelmistopohjainen lompakko vain lähettää hardware-lompakon hyväksymät transaktiot. Hardware-lompakkolaite näyttää yleensä ruudulla transaktion hyväksymistä varten varmistaakseen, että mikään haittaohjelma ei ole vaikuttanut siihen. Hardware-lompakot ovat yleensä myös suojattu PIN-koodilla tai salasanalla. (Franco, 2015)

Online-lompakot ovat kuuma varastointitapa kryptovaluutalle. Online-lompakot ovat ulkoisen palveluntarjoajan tarjoamia alustoja tileille, joihin tekemällä käyttäjän ja todentautumalla voi tallettaa ja nostaa varoja (Franco, 2015). Monissa online-lompakoissa on myös kryptovaluutanvaihtomahdollisuus ja toimivat kryptovaluuttapörssinä. Vaikkakin online-säilytys on usein ilmaista, ja mahdollistaa valuuttojen vaihtamisen. Ovat netissä olevat varastointimuodot mahdollisia hakkeroinnin tai palvelunestohyökkäyksien kohteita, ja esimerkiksi virukset tai keyloggerit voivat myös uhata käyttäjän itsensä kautta lompakon turvallisuutta. Kryptovaluuttapörssit ovat kryptovaluuttojen keskittymiä, ja täten verkkorikollisten ykköskohteita (Bitcoinkeskus, 2021). Joillakin kryptovaluutanvaihtoalustoilla voi olla vakuutus tietomurtoja vastaan. Esimerkiksi vuonna 2018 Binance julkisti Secure Asset Fund for Users (SAFU) vakuutusrahaston. 10% Binancen toimeksiantokuluista kylmävarastoidaan SAFU-rahastoon suojatakseen käyttäjien varoja tietomurron tapahtuessa (Binance Academy, ei pvm. a).

## 2.4 Louhinta

Bitcoin hyödyntää proof-of-work-mekanismia lohkoketjussaan. Tätä varten Bitcoin käyttää SHA256 (Secure Hashing Algorithm) hajautusfunktiota, joka antaa 256-bittisen numeron, jonka kaikki käyttäjät jakavat. Uuden lohkon ollakseen validi, tulee sen hashin arvon olla vähemmän kuin hajautusfunktion an-

taman kohdenumeron. Mitä matalampi algoritmin antama numero on, sitä vaikeampi ja täten aikaa kuluttavampi prosessi on saada matalampi arvo, ja siten validi lohko. (Pilkington, 2015)

Kryptovaluutan louhinnan tarkoitus on tuottaa turvallinen tilikirja kaikista valuutan transaktioista desentralisoidusti. Valuutan siirtyessä omistajalta toiselle kopio transaktiosta siirretään louhijoille todennusta varten, joita lähetetään jatkuvasti kaikille siinä verkossa oleville tietokoneille. Louhijat ovat yksilöitä tai ryhmiä, jotka ajavat louhintaohjelmaa verkossa. Louhijat koittavat muuttaa viimeisimmän transaktion lohkoksi. (Extance, 2015)

Transaktion kryptaaminen luo hashin, eli kryptografisen tiivisteen. Verkossa olevat louhijat kisaavat siitä, kuka ratkaisee hashin todentamiseen vaaditun numerosarjan, (engl. nonce) (number used once) (Extance, 2015; Nofer ym., 2017). Louhija, joka ratkaisee vaaditun numeron ensimmäisenä lähettää todennuksen (engl. proof-of-work) siitä, että on ratkaissut tehtävän. Tämä ”voittava” lohko siirretään lohkoketjuun. Tämä kryptografisten tehtävien ratkaisukisa periaatteessa ylläpitää lohkoketjun turvallisuutta, sillä oikean numeron ratkaiseminen on tehtävänä liian hankala, että yksittäinen louhija voisi itse ratkaista sen joka kerta, mikä tarkoittaa, että kukaan ei tule saamaan kryptattuja linkkejä lohkoketjussa käsiinsä, ja mahdollisuutta uudelleenkirjoittaa tilikirjaa. Louhinta myös lisää kryptovaluutan tarjontaa, sillä louhija, joka ratkaisee tehtävän saa palkinnoksi kryptovaluuttaa. Nakamoton suunnittelu rajoittaa valuutan tarjonnan vaikeuttamalla louhintatehtävää, sekä palkkio uuden lohkon liittämisestä aina puoliintuu noin neljän vuoden välein. Bitcoin on rajoitettu tällä tavalla 21 miljoonaan bitcoin-yksikköön. (Extance, 2015)

Jotkut yksittäiset louhijat ovat yhdistäneet resurssinsa ryhmittymäksi (engl. mining pool). Esimerkiksi GHash.IO ylitti hetkellisesti yli valtaosan Bitcoinin louhintatehosta omistaessaan 54 % laskentatehosta (Bastiaan, 2015). Tämä mahdollistaisi 51 % hyökkäyksen. Jos jollain yksittäisellä taholla on valtaosa louhintatehosta voi louhia niin tehokkaasti, että saa itse lisättyä kaikki lohkot lohkoketjuun. Tämä käytännössä tarkoittaa, että kyseisellä taholla on tilikirja hallussaan, ja se voi käyttää samat bitcoinit toistuvasti, eli toteuttaa tuplakulutushyökkäyksen (engl. double spending).

Monet kryptovaluutat toimivat proof-of-work-konsensusalgoritmilla, mutta vuonna 2012 King & Nadal (2012) esittivät ehdotuksen proof-of-stake-konsensusalgoritmista ja hybridi implementaation, kryptovaluutan nimeltä Peercoin. Myöhemmin proof-of-stake-mekanismi käyttöönotettiin Nxt-lohkoketjussa ja sittemmin useita eri valuuttoja, jotka käyttävät proof-of-stake-mekanismia on kehitetty (Saleh, 2021). Peercoin, joka tunnetaan myös nimellä PPCoin, projektina kehitettiin mahdollistaakseen peer-to-peer-desentralisoidut kryptovaluutat, jotka eivät kuluta yhtä paljoa energiaa kuin proof-of-work-mekanismilla toimivat (King & Nadal, 2012). Proof-of-stake ratkaisee louhinnan aiheuttaman energiakustannukset vaihtamalla proof-of-work-mekanismin kilpailun lohkon lisäämisestä ketjuun arvontaan siitä, mikä osallinen lisää seuraavan lohkon (Saleh, 2021). Yksinkertaisin implementaatio proof-of-stake-mekanismista on follow-the-Satoshi (FTS) -algoritmi. FTS-algoritmi valitsee sa-

tunnaisen yksikön valuuttaa se, jonka valuutta valitaan voi lisätä lohkon ketjuun, ja saa tästä palkkion niin kuin proof-of-work-periaatteellakin. Todennäköisyys sille, että lohkon lisäävän validoijan valuuttayksikkö valitaan riippuu siitä, kuinka paljon valuuttaa hänellä on hallussa (Saleh, 2021).

## 2.5 Erilaiset kryptovaluutat

Erilaisia kryptovaluuttoja on tutkielman ajankohtana yli 13 000 kappaletta, ja kryptovaluuttojen yhteinen markkina-arvo tutkielman ajankohtana on 2,88 biljoonaa dollaria (*CoinMarketCap*, 2021). Vaihtoehtoisetvaluutat (engl. alternative coin) on kehitetty Bitcoinin tulon jälkeen. Kaikki muita kryptovaluuttoja kuin Bitcoin kutsutaan yleisesti nimellä altcoin (Binance Academy , ei pvm. b). Raja coinin ja tokenin välillä on usein häilyvä (Kryptokansalainen, 2017). Monet altcoineista perustuvat Bitcoinin lähdekoodiin. Markkina-arvoltaan suurimpia, ja merkittäviä altcoineja ovat esimerkiksi Ethereum, Cardano ja XRP (Ripple) (*CoinMarketCap*, 2021.). Altcoinit usein koittavat usein parantaa joitain Bitcoinin ominaisuuksia, tai puutteita. Esimerkkinä tästä on aiemmin mainittu proof-of-stake-mekanismi. Esimerkiksi Cardano mainostaa itseään ensimmäisenä vertaisarvioidun tutkimuksen pohjalta rakennettuna lohkoketjualustana, ja käyttää Ouroboros-nimistä proof-of-stake-mekanismia (*Cardano.org,* ei pvm.). Myös markkina-arvoltaan toisiksi suurin kryptovaluutta Ethereum (*CoinMarketCap*, 2021) on siirtymässä proof-of-stake-mekanismiin, vaikka aloitti proof-of-work-mekanismilla. Tämän muutos toteutetaan Buterinin & Griffithin (2019) Casper projektissa, jonka tarkoituksena on tehdä tämä muutos proof-of-work- ja proof-of-stake-mekanismien hybridimallin kautta, ja myöhemmin siirtyä johonkin tehokkaampaan. Tämä uusi Ethereum tunnetaan myös nimellä Ethereum 2.0.

Tokenit ovat usein tiettyyn lohkoketjuun sidottu kryptovaluutan yksikkö, joka toimii vain tietyn rajatun toimintaympäristön sisällä. Tokenilla voidaan tarkoittaa myös muita vaihdon välineitä tietyn verkon tai lohkoketjun sisällä. Toisin kun Bitcoinilla tai altcoineilla, tokenilla voi vaihdon välineenä toimimisen lisäksi olla muita ominaisuuksia. (Kryptokansalainen, 2017)

# 3 KRYPTOVALUUTTOJEN TIETOTURVA

Tämä luku käsittelee erilaisia tietoturvauhkia, mitä kryptovaluuttoja vaihtaessa, louhiessa tai hallussa pitäessä voi olla. Luvussa käsitellään myös hyökkäysten historiallista kehitystä, kryptovaluuttojen luotettavuutta, sekä toimenpiteitä uhkatekijöiden ehkäisyksi ja ratkaisuksi.

## 3.1 Hyökkäykset

Toimintamallistaan johtuen kryptovaluuttoihin liittyy lukuisia tietoturvauhkia. Conti, Kumar, Lal & Ruj (2018) listaavat esimerkiksi seuraavat: tuplakulutus, yli 50 % laskentatehon, eli 51 % hyökkäys, itsekäs louhinta (engl. selfish mining), lohkon panttaaminen (engl. block withholding) ja mustalistaamisen. Näiden hyökkäysten toiminta perustuu Bitcoinin ja proof-of-work-mekanismin ominaisuuksiin. Artikkelissa listataan myös lompakon varastaminen ja palvelunestohyökkäykset, jotka hyökkäyksinä ovat puolestaan kohdistettu käyttäjiin tai valuutanvaihtokeskuksiin. Muitakin hyökkäystyyppejä on mainittu, mutta tutkielmissa ei syvennytä niistä kaikkiin. Tässä kappaleessa käydään läpi erilaisia esimerkkitapauksia hyökkäyksistä. Erilaisia tapauksia on lukuisia, mutta kappaleessa mainitaan vain joitain merkittävimmistä metodeista ja tapauksista.

### 3.1.1 Palvelunestohyökkäykset

Palvelunestohyökkäysten arvioidaan olevan yleisimpiä hyökkäyksiä Bitcoiniin liittyen. Vasek, Thornton & Moore (2014) artikkelissaan ovat laskeneet palvelunestohyökkäysten kohdistuvan useimmiten Bitcoin-vaihtoalustoihin ja Bitcoin-louhintaryhmittymiin. Melkein 80 % hajautetuista palvelunestohyökkäyksistä kohdistui näihin kahteen kohteeseen. Kolmannes ryhmittymistä ja vaihtoalustoista käyttivät anti-DDoS-palveluita suojautuakseen palvelunestohyökkäyksiltä. Palvelunestohyökkäykset voivat myös kohdistua esimerkiksi käyttäjien online-lompakoihin, tai kauppoihin, jotka hyväksyvät Bitcoinin mak-

suvälineenä. Palvelunestohyökkäyksillä voidaan koittaa esimerkiksi vaikuttaa markkinoiden hintatasoon, häiritä isompia louhintaryhmittymiä parantaakseen omia todennäköisyyksiä ratkaista proof-of-work tehtävä ensin, tai häiritäkseen kilpailevien vaihtoalustojen toimintaa.

### 3.1.2 The DAO hyökkäys

Distributed Autonomous Organization (DAO) eli hajautettu autonominen organisaatio on konsepti, jonka tarkoituksena on poistaa organisaation valvovat osat, ja korvata ne koodilla. Hajautetussa autonomisessa organisaatiossa ihmiset kirjoittavat älysopimukset, eli ohjelmat, jotka ohjaavat organisaatiota. Projektin alussa on joukkorahoitus, jossa myydään esimerkiksi tokeneita, jotka edustavat omistustaosaa. Rahoitusvaiheen jälkeen organisaatio aloittaa toimintansa, ja tokeneiden omistajat voivat tehdä ehdotuksia varojen käytöstä organisaation sisällä ja äänestää, mitkä ehdotukset hyväksytään. (Siegel, 2016)

Tunnetuin DAO on nimeltään ”The DAO”. The DAO hyödynsi lohkoketjuteknologiaa, sekä Ethereumin kryptovaluuttaa ja älysopimuksia, toteuttaakseen organisaation ilman esimiehiä, jotka ovat korvattu koodilla. Lohkoketju mahdollistaa läpinäkyvän ja luotettavan vaihtoehdon perinteiselle johdolle. (Mehar ym., 2017) The DAO:n koodista löydettiin heikkous 5.6.2016, ja sen löytänyt käyttäjä ilmoitti asiasta eteenpäin. Heikkoudesta julkaistiin sen jälkeen artikkeli. Virhe koodissa mahdollisti käyttäjää nostamaan varantonsa The DAO:sta toistuvasti, ennen kuin varojen nosto kirjattiin tilille (Mehar ym., 2017). Väliaikaista korjausta tehdessä tuntematon hyökkääjä hyödynsi tätä heikkoutta ja alkoi nostamaan etheriä, eli Ethereumin kryptovaluuttaa, jota oli aikaisemmin kerätty myymällä tokeneita (Siegel, 2016). Ethereumin ja The DAO:n desentralisoidun luonteensa vuoksi äänestys ja valtaosan konsensus oli vaadittu ennen kuin hyökkäyksen olisi voinut pysäyttää. Ryhmä käyttäjiä vastusti hyökkäystä nostamalla varoja The DAO:sta samalla tavalla kuin hyökkääjä, jotta mahdollisimman paljon varoista saataisiin pois ennen kuin hyökkääjä saa ne nostettua itselleen. 22.6.2016 The DAO oli tyhjennetty kaikista varoistaan. Hyökkäyksen ajankohtana The DAO sisälsi 15 % kaikesta etheristä, ja yksittäisen etherin arvo putosi 20:stä Yhdysvaltain dollarista kolmeentoista dollariin. (Mehar ym., 2017)

Päätös siitä, mitä hyökkäyksen suhteen tehtiin ei ollut yksimielinen. Osa käyttäjistä olivat sitä mieltä, että koska hyökkääjä oli käyttänyt älysopimusten mahdollistamia keinoja varojen nostamiseen, ja täten oikeutettu niihin. Useita päiviä kestäneen äänestyksen jälkeen Ethereum-yhteisö päätti haarauttaa lohkoketjun (engl. fork) uuteen lohkoketjuun siten, että hyökkääjän tekemät transaktiot palautuivat siihen tilaan, missä ne olivat ennen hyökkäystä. Osa käyttäjistä päätti kuitenkin louhia vanhaa lohkoketjua, ja tämä ketju tunnetaan nimellä Ethereum Classic. (Mehar ym., 2017) Matalasta laskentatehosta johtuen Ethereum Classic on ollut 51 % hyökkäyksen kohteena (Sayeed & Marco-Gisbert, 2019).

### 3.1.3 Tuplakulutuksen mahdollistavat hyökkäykset

Tuplakulutus on hyökkäys, jossa samat varat käytetään useaan eri transaktioon. Proof-of-work-mekanismi on suunniteltu estämään tuplakulutusta, mutta sen voi silti toteuttaa useilla eri tavoilla. Conti ym. (2018) luettelee seuraavat: Finney-hyökkäys, brute-force-hyökkäys, Vector 76-hyökkäys ja 51 % hyökkäys.

51 % hyökkäyksessä käyttäjä tai ryhmä, jolla on hallussaan valtaosa laskentatehosta, joka on proof-of-work-verkossa rakentamassa lohkoketjua, yksityisesti alkaa rakentamaan muiden ketjusta täysin erillistä ketjua, joka myöhemmin esitetään oikeana ketjuna. 51 % hyökkäys mahdollistaa tuplakulutuksen. Ketju hyväksytään oikeaksi ketjuksi lohkoketjun pisimmän ketjun säännön vuoksi. Ketju on pisin, sillä sitä on ollut rakentamassa suurin osa laskentatehosta, jolloin hyökkääjä saa myös lopuksi muutkin palvelimet yhtymään siihen. Tuplakulutus on mahdollista myös pienemmällä laskentateholla, mutta sen onnistumistodennäköisyys on pienempi. (Sayeed & Marco-Gisbert, 2019)

Sayeed & Marco-Gisbert (2019) artikkelissaan listaavat useita eri ratkaisuehdotuksia 51 % hyökkäystä vastaan. Hyökkäyksen kustannusvaatimuksia voidaan nostaa rangaistusjärjestelmällä, joka tekee yksityisestä louhimisesta vaativampaa. Kahden eri valuutan louhintojen yhdistäminen myös lisää 51 % hyökkäyksen toteutuksen vaativuutta, mutta ei kuitenkaan täysin estä sitä tapahtumasta. Viivästytetty proof-of-work on käytössä jo ainakin 20 lohkoketjussa, mutta sitä ei voi käyttää kaikissa lohkoketjumalleissa. Artikkelin mukaan kuitenkaan mikään mainituista metodeista ei täysin suojaa 51 % iskulta, ja uusia ratkaisuvaihtoehtoja tarvitaan ongelman täydelliseen ratkaisemiseen.

Finney-hyökkäyksessä hyökkääjä louhii yksityisesti lohkon, johon sisältyy hänen transaktionsa, jossa hän on siirtänyt varat itselleen. Samalla hän toteuttaa transaktion samoilla varoilla, jonkun toisen kanssa, esimerkiksi ostaakseen jonkin tuotteen. Kun hyökkääjä saa ostamansa tuotteen, se lähettää louhimansa lohkon verkostoon, jos verkosto jatkaa tätä ketjua, jossa ennalta louhittu transaktio on, siitä tulee virallinen, jolloin lohko, jossa samat varat siirtyivät toiselle osapuolelle, hylätään. Tämä hyökkäys kuitenkin edellyttää sen, että lohkoketjun haarasta, jossa varat siirtyvät hyökkääjältä takaisin itselleen tulee pisin lohkoketju. Finney Hyökkäykseltä voi puolustautua odottamalla useampaa varmistusta, ennen kuin tuote lähetetään ostajalle, jolloin hyökkäyksen tapahtuessa, tuotetta ei lähetetä hyökkääjälle liian aikaisin, tämä ei kuitenkaan täysin ehkäise tuplakulutuksen mahdollisuutta. Brute-force-hyökkäys on samankaltainen kuin Finney-hyökkäys, mutta siinä käytetään useita palvelimia louhimiseen, ja louhitaan useampia lohkoja, jolloin useiden lohkojen odottaminen varmistaakseen kaupan ei välttämättä enää toimi hyökkäystä vastaan yhtä todennäköisesti. (Conti ym., 2018)

Vector 76-hyökkäys on yhdistelmä tuplakulutusta ja Finney-hyökkäystä. Tämä hyökkäys kohdistetaan kryptovaluuttojen vaihtoalustaan. Tässä metodissa hyökkääjä lähettää lohkon, johon on tallennettu hänen transaktionsa, jossa hän on tallettanut varansa vaihtoalustalle. Seuraavaksi hyökkääjä nostaa rahat siinä toivossa, että toisesta haarasta, jossa tätä talletustransaktiota ei ole, tulee ensisijainen lohkoketju. Jos hyökkäys onnistuu, niin transaktio, jossa varat talle-

tettiin ei koskaan kirjaudu viralliseen lohkoketjuun, mutta hyökkääjä on kerennyt nostamaan varat vaihtoalustalta, jolloin vaihtoalusta menettää varojaan. (Conti ym., 2018)

Ennaltaehkäisevät ratkaisut tuplakulutusta vastaan ovat tuplakulutusten monitorointia tehokkaampia, sillä kryptovaluutat mahdollistavat pseudonymiteetin käyttäjilleen transaktioiden tallentuessa lohkoketjuun, ei niitä voi enää peruuttaa. Conti ym. (2018) toteavat useiden lohkojen tuoman varmistuksen olevan yksinkertaisin ja tehokkain tapa ennaltaehkäistä tuplakulutuksen mahdollisuutta. Esimerkiksi Bitcoinin lohkoketjussa kuuden peräkkäisen lohkon muodostumista transaktion jälkeen voidaan pitää varmana, tämä väite perustuu oletukseen siitä, että yksittäinen taho ei todennäköisesti omaa yli 10 % laskentatehosta, ja alle 0,1 % onnistumismahdollisuus on tarpeeksi pieni riski. Bitcoinin tapauksessa kuuden lohkon muodostuminen kestää noin tunnin ajan. Kaikkien toimijoiden palvelut eivät voi kuitenkaan odottaa varmistusta näin pitkään.

### 3.1.4 Muut lohkoketjuteknologiaan perustuvat hyökkäykset

Tuplakulutuksen lisäksi lohkoketjuteknologia mahdollistaa muita hyökkäystapoja, jotka voivat olla uhkana joillekin tahoille. Louhintaryhmittymät, jotka yleisesti palkitsevat osittaisesta työn todennuksesta kaikkia ryhmittymän osallisia jonkun osallisen saavuttaessa täyden työn todennuksen. Osallistuminen louhintaan ilman täyttä työn todennusta on käytännössä merkityksetöntä. Osallistumisesta palkitaan motivoidakseen käyttäjiä liittymään ryhmittymään, joka taas keskimääräisesti onnistuu yhdessä useammin kuin yksittäiset käyttäjät. Tämä toimintamalli kuitenkin mahdollistaa pahantahtoisen tai itsekkään toiminnan ryhmittymän sisällä (Conti ym., 2018).

Itsekäs louhinta voi mahdollistaa epäreilun suuret palkkiot suhteessa louhijan tarjoamaan laskentatehoon, tai häiritä muiden louhijoiden toimintaa ja tuhlata niiden resursseja. Itsekäs ryhmittymä voi koittaa louhia yksityisesti, ja saadessaan etumatkaa haarassaan ryhmittymä voi saada enemmän palkintovaluuttaa, ja samalla tuhlaa toista haaraa louhivien resursseja. Lohkon panttaaminen on hyökkäys, jossa yksilö ryhmittymän sisällä ei julkaise louhimaansa lohkoa, mutta saattaa kerätä palkkiot osallistumisesta ryhmittymään. (Conti ym., 2018)

Tarpeeksi suuren laskentatehon saavutettaessa, on muiden louhijoiden mustalistaaminen mahdollista. Käytännössä tämä toteutetaan kieltäytymällä louhimasta niitä lohkoja, joita mustalistattava taho louhii, tai joissa on mustalistattavan tahon transaktio. Suuremman laskentatehon omaavan tahon haarasta tulee pidempi, jolloin siitä tulee virallinen. Jos laskentateho on yli puolet, voidaan mustalistaaminen toteuttaa aina. Laskentatehon ollessa vähemmän, voi hyökkääjä yrittää toteuttaa erillistä haaraa, mutta tässä tapauksessa hyökkäys ei aina onnistu. Mustalistaamista voi käyttää esimerkiksi jonkun tietyn tahon kiristämiseen tai häirintään. (Conti ym., 2018)

## 3.2 Huijaukset

Bitcoinin ekosysteemissä on monenlaisia huijausmahdollisuuksia. Ympäristössä on paljon asioita mitä ei ole säännöstelty ja monet huijarit ovat huomanneet mahdollisuuden järjestää esimerkiksi pyramidihuijauksia, ja koska Bitcoin-transaktiot ovat peruuttamattomia, monet huijatut ovat jääneet ilman minkäänlaista korvausta (Vasek ym., 2014).

Vuonna 2012 pireateat40 nimimerkillä tunnettu e-raha-pankkiiri sulki Bitcoin Savings & Trust-nimisen hedgerahaston, joka lupasi suuria tuottoja sijoittajilleen, jotka sijoittivat sinne bitcoinia. Pirateat40 väitti rahastoaan sulkiessa siellä olleen 500 000 bitcoinia, ja lupasi palauttaa rahat sijoittajilleen, sekä maksavan korkoa viikon kuluttua (Jeffries, 2012). Badawi & Jourdan (2020) mainitsee tämän esimerkkinä pyramidihuijauksesta, joka oli kerännyt 700 000 bitcoinia sijoittajiltaan, kunnes Yhdysvaltain arvopaperi- ja pörssikomissio nosti syytteen 2013. Ethereumin vastaavia huijauksia arvioidaan olevan 0.03% - 0.15% kaikista älysopimuksista, ja näiden arvon olleen noin 500 000 dollaria (Badawi & Jourdan, 2020).

Useita huijausvaluuttoja on myös tehty uusien kryptovaluuttojen yleistyessä. Viimeisimpiä esimerkkejä tästä on SQUID-niminen kryptovaluutta. SQUID markkinoi itseään aikansa suosituimman Netflix sarjan Squid Gamen avulla, ja lupasi pääsyn online-peliin, joka oli inspiroitunut kyseisestä sarjasta. SQUID ei ollut yhteydessä Netflixiin, mutta ei ilmoittanut tätä. Yksittäinen SQUID-yksikkö oli arvoltaan aluksi 0,01 Yhdysvaltain dollaria, ja nousi korkeimmillaan 2861,80 dollariin asti, mutta 5 minuuttia myöhemmin arvo oli laskenut alle senttiin. SQUID-valuuttaa ei voinut myydä enää ollenkaan, ja aiemmin mainittu peli vaati 456 yksikköä, jotta sitä voisi pelata. Pelillä pystyi ansaitsemaan toista kryptovaluuttaa, jonka avulla investointinsa voisi myydä. Kuitenkin jos pelin hävisi, menetti kaikki 456 SQUID-yksikköään, ja alle 456 yksiköllä ei voinut pelata. Mahdollisuus pelistä antoi vaihtoehdon investoida lisää rahaa pelaamismahdollisuuden toivossa. Nykyisin kyseisen valuutan nettisivutkaan eivät ole enää käytössä. Kryptovaluutan kehittäjät hylkäsivät projektin, ja pitivät sijoittajien sijoittamat varat. (CoinMarketCap, 2021)

## 3.3 Tietomurtojen kehitys

Oosthoekin & Doerrin (2020) artikkelissa kerättiin tapauksia, jossa tietomurtoja bitcoinin vaihtoalustoille oli tapahtunut. Tapauksia löytyi 36, ja ne sijoittuivat aikavälille 2011–2019. Tapauksista käy ilmi, että valtaosassa hyökkäyksiä on käytetty yksinkertaisia menetelmiä. Ainoastaan 3 tapausta käytti monimutkai-

sempia hyökkäysmetodeja. Yksinkertainen hyökkäyksien taso osoittaa alustojen tietoturvan olleen heikkoa.

Toiminnallisten ominaisuuksien hyväksikäyttöön perustuvat hyökkäykset ovat ajan kuluessa vähentyneet. Tällaiset hyökkäykset yleensä kertovat heikosta valvonnan tasosta uhrin puolesta. Hyökkäykset, joissa jonkun alustan auktoriteetin pääsytiedot oli varastettu, ja tätä kautta siirretty varoja pois olivat aikavälin alkupuolella yleisiä, mutta vähentyneet ajan kuluessa, joka osoittaa turvallisuuskäytäntöjen kohenemista. (Oosthoek & Doerr, 2020)

Selvittämättömät hyökkäysmetodit ovat yleistyneet ajan kuluessa. Tämä osoittaa hyökkäystapahtumien ratkomisten vähentymistä ja alustojen vähentynyttä läpinäkyvyyttä hyökkäystapahtumien suhteen. Valtaosa varastetuista varannoista ja iskuista kohdistui kuumalompakoihin, ja ainoastaan kahdessa tapahtumassa varat eivät lähteneet kuumalompakosta. Varoja kylmävarastoidaankin nykyisin aiempaa enemmän, mikä osoittaa kehitystä alustoiden puolesta. (Oosthoek & Doerr, 2020)

Vietyjen bitcoinien kappalemäärä on vähentynyt ajan kuluessa, mutta murroissa vietyjen bitcoinmäärein rahallinen kokonaisarvo on kasvanut, mikä johtuu bitcoinin arvonnoususta. Tutkimuksen tapausten aikavälin alkupuolella monet alustat päätyivät lopettamaan toimintansa ja ne suljettiin. Vaihtoalustojen sulkeminen murrosta johtuen on kuitenkin vähentynyt, ja jotkut alustat ovat palauttaneet asiakkailleen menetetyt varat täysin. Toiset alustat taas ovat palauttaneet vain osan varannoista, perustuen johonkin päätettyyn prosenttiosuuteen. Jotkut alustat, kuten esimerkiksi Bitfinex ja Yapizon jakoivat tokeneita, jotka osoittivat velkaa, mutta eivät korvanneet menetettyjen varantojen todellista arvoa. Jotkut alustat ovat tarjonneet vain anteeksipyynnön. Alustojen vaihtokauppojen volyymi, on kuitenkin pysynyt vakaana, tietomurtotapahtumista huolimatta. (Oosthoek & Doerr, 2020) Pelkkä anteeksipyyntö ei kuitenkaan yleensä ole riittänyt palauttamaan asiakkaiden positiivista asennetta alustaa kohtaan. Esimerkiksi vuonna 2013 BitCash-niminen alusta hakkeroitiin, ja 4000 asiakkaan lompakot vaarantuivat. BitCash lähetti anteeksipyyntöilmoituksen tapahtumasta, ja totesi tehneensä kantelun tapahtuneesta rikoksesta, ja vain 33 % käyttäjistä osoitti tyytyväisiä asenteita alustaa kohtaan. Varastettujen varojen kompensoiminen tietomurron tapahtuessa on merkittävä osa luottamuksen jälleenrakentamista. Esimerkiksi Binancen tietomurron tapahtuessa 2019 Binanceen hyökättiin useilla eri metodeille, kuten tietojenkalastelulla ja viruksilla. 7000 bitcoinia vietiin useilta eri käyttäjiltä murron aikana. Binance korvasi kaikki vahingot SAFU-vakuutusrahastollaan, niin kuin oli luvannutkin. Asenteet Binancea kohtaan olivat murron jälkeen kuitenkin enimmäkseen positiiviset. (Marella ym., 2021)

McCorry, Möser & Ali (2018) artikkelissa todetaan, että vaihtoalustoilla on ollut historiallisesti heikot turvallisuussäännökset, ja on väitetty, että yli kolmannes vaihtoalustoista oli vaarantunut jo vuoteen 2015 mennessä. Eniten bitcoineja vienyt ryöstö tapahtui helmikuussa 2014, kun japanilainen alusta Mt. Gox menetti 850 000 bitcoinia, jotka Bitcoinverkosto hyväksyi, ja täten ovat mahdotonta palauttaa. Mt. Gox oli suurin vaihtoalusta, ja se käsitteli 70 % kai-

kista bitcoin-transaktioista. Vietyjen bitcoinien arvo oli tapahtuman aikaan 450 miljoonaa Yhdysvaltain dollaria. Oosthoek & Doerr (2020) ovat tutkimuksessaan merkanneet kyseisen murtotapahtuman toimikuvan ja hyökkäyksen laadun tunnistamattomiksi, mutta mainitsevat sisäpiirin toiminnan vaikuttaneen murtoon.

# 4 YHTEENVETO

Tutkielmassa tarkasteltiin kryptovaluuttoja ja niiden tietoturvauhkia pohjautuen akateemisiin lähteisiin, vertaisarvioimattomiin raportteihin ja kryptovaluuttojen hintaseurantasivustoihin. Suuri osa kryptovaluuttoihin liittyvästä informaatiosta on saatavilla vain raporteista, ja monia niihin liittyviä tapahtumia ei ole tarkasti käsitelty akateemisessa kirjallisuudessa. Tutkimukset käsittelevät usein potentiaalisia uhkia, tai ehdottavat potentiaalisia ratkaisuja uhkiin. Monien potentiaalisten hyökkäysten oikeaa tapahtumatodennäköisyyttä on vaikea arvioida, jolloin on myös vaikeaa arvioida niiden aiheuttamien uhkatilanteiden suuruutta käytännössä. Useat tutkimukset eivät kuitenkaan ehdottaneet selvää tai yleisesti käyttöönotettua ratkaisua, joten monet ehdotetuista ratkaisuista jäävät spekulatiivisiksi.

Ensimmäisessä luvussa selitettiin lohkoketjujen toimintaa, sekä yleisiä kryptovaluuttojen käyttöön, vaihtoon ja hallussapitoon liittyviä asioita. Kryptovaluuttojen omat ominaisuudet, vaihtoalustat ja lompakot omaavat erilaisia ominaisuuksia, ja täten vaikuttavat eri tavoin mahdollisiin tietoturvauhkiin. Toisessa luvussa käsiteltiin erilaisia hyökkäystapoja lohkoketjuteknologian, ja kryptovaluuttojen käytön omien heikkouksiin liittyen.

Kryptovaluutat käyttävät lohkoketjuteknologiaa transaktioiden tallentamiseen, ja lohkoketjuteknologia on robustista rakenteestaan huolimatta, desentralisoidun luonteensa puolesta vaikea toteuttaa käytännössä niin, että minkäänlaista hyökkäysmahdollisuutta ei ole. Tuplakulutus on mahdollista toteuttaa monella erilaisella metodilla, ja vaikka sitä ei voi täysin varmasti toteuttaa ilman valtaosaa laskentatehosta, voi se käytännössä onnistua jonkinlaisella todennäköisyydellä laskentatehosta riippuen. Monet käytännössä parhaaksi todetuista ratkaisuista ovat vain tuplakulutuksen onnistumisen todennäköisyyksien minimoimista, tapoja motivoida yksittäisiä tahoja omaamaan pienemmän laskentatehon kerrallaan tai rankaisumetodeja haitallisesta toiminnasta. Tuplakulutuksen lisäksi lohkoketjun louhintaprosessia voidaan manipuloida kiristämällä, tai häiritsemällä hyödyntäen omaa laskentatehoa tai esimerkiksi palvelunestohyökkäyksillä.

Kryptovaluuttojen lompakkoina ja pörsseinä toimivat vaihtoalustat ovat olleet useiden tietomurtojen uhreja. Hyökkäysten laatu on ollut suurelta osin samankaltaista, mutta ratkaisemattomiakin tapauksia on useampia. Hyökkäysten seurauksena pienempiä määriä kryptovaluuttaa on viety kerralla, mutta vietyjen varojen rahallinen arvo on usein vieläkin yhtä korkealla. Monien alustojen tietoturva on kehittynyt, ja isoja hyökkäyksiä ei voi toteuttaa yhtä helposti. Alustat myös harvemmin kaatuvat näiden hyökkäysten seurauksena, ja jotkut alustat omaavat vakuutusrahaston tietomurtojen seurauksien korvaamiseksi. Eri alustat ovat tietoturvatasoiltaan kuitenkin toisistaan poikkeavia, ja oikean alustan valinta on tietoturvan kannalta käyttäjälle merkittävää.

Hyökkäyksien lisäksi käyttäjän omaan toimintaan liittyviä uhkia on olemassa. Osa kryptovaluutoista ja rahastoista ovat huijauksia, jotka eivät käytännössä toimi luvatulla tavalla. Myös huijaukset ovat aiheuttaneet merkittäviä varojen menetyksiä, ja joissain tapauksissa huijauksien tekijöitä on vaikea saada kiinni tai rankaista. Käyttäjän valitseman lompakon tyyppi vaikuttaa siihen, kuinka merkittäviä ja millaisia uhkia kryptovaluutan säilyttämiseen liittyy. Kuumalompakot ovat usein käytännöllisyydestään ja suosiostaan huolimatta turvattomampia, ja täten myös usein hyökkäysten kohteina. Käyttäjä voi myös itse hukata tai turmella avaimensa omiin kryptovaluuttoihin, jolloin ne menetetään pysyvästi.

Hyökkäykset ovat aiheuttaneet kuluja käyttäjille, sekä vaikuttaneet vaihtoalustojen toimintaan, ja jopa joissain tapauksissa aiheuttanut alustan konkurssin. Myös lohkoketjujen käyttäjien muuhun toimintaan vaikuttaneita hyökkäyksiä on, kuten esimerkiksi The DAO-hyökkäys, joka aiheutti Ethereumin lohkoketjun haarautumisen, joka johti kahteen erilliseen kryptovaluuttaan, mikä herätti kysymyksiä kyseisen lohkoketjun luotettavuudesta.

Kryptovaluuttojen ympäristön kehittyneemmistä tietoturvakäytännöistä huolimatta, ovat useat merkittävät uhat vielä ratkaisemattomia, ja kryptovaluuttaympäristö monella tavalla ennalta-arvaamaton. Koska monet tutkielman käsittelemät uhat ovat vieläkin olemassa, ovat samat uhat varmasti myös tulevaisuuden tutkimusten aiheita, sillä uusia ratkaisuehdotuksia tarvitaan. Kryptovaluuttojen kehittyessä nopeasti myös uusia uhkamahdollisuuksia kehittyy, ja ympäristön muuttuessa voivat vanhat uhat myös vähentyä. Esimerkiksi Ethereum 2.0 ja sen tuoma proof-of-stake-mekanismi muuttaa eri lohkoketjupohjaisten hyökkäyksien todennäköisyyksiä. Proof-of-stake-mekanismin, muiden vastaavien ehdotusten, ja lohkoketjuratkaisujen yleistyessä käytäntöön, tulee uusien uhkakartoituksien tekeminen tarpeelliseksi uuden ympäristön uhkien selvittämistä varten. Myös huijausten aiheuttamien vahinkojen, ja vaihtoalustojen vastuuseen liittyvien lainsäädännöllisten aiheiden tutkimukset voivat olla merkittäviä tulevaisuuden tutkimuskohteita

# LÄHTEET

*Altcoin*. (ei pvm.). Binance Academy. Noudettu 8. marraskuuta 2021, osoitteesta https://academy.binance.com/en/glossary/altcoin

Badawi, E., & Jourdan, G.-V. (2020). Cryptocurrencies Emerging Threats and Defensive Mechanisms: A Systematic Literature Review. *IEEE Access*, *8*, 200021–200037. https://doi.org/10.1109/ACCESS.2020.3034816

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

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *2015 IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Buterin, V., & Griffith, V. (2019). Casper the Friendly Finality Gadget. *arXiv:1710.09437 [cs]*. http://arxiv.org/abs/1710.09437

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

*Cardano is a decentralized public blockchain and cryptocurrency project and is fully open source.* (ei pvm.). Cardano. Noudettu 9. marraskuuta 2021, osoitteesta https://cardano.org/

Conti, M., Sandeep Kumar, E., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys Tutorials*, *20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

*Cryptocurrency Prices, Charts And Market Capitalizations*. (ei pvm.). CoinMarketCap. Noudettu 4. lokakuuta 2021, osoitteesta https://coinmarketcap.com/

Erilaistet Bitcoin-lompakot—Talletusmuotojen vertailu. (2021, kesäkuuta 4). *Bitcoinkeskus.com*. https://bitcoinkeskus.com/kryptovaluutta-lompakko/

Extance, A. (2015). The future of cryptocurrencies: Bitcoin and beyond. *Nature*, *526*(7571), 21–23. https://doi.org/10.1038/526021a

Franco, P. (2015). *Understanding Bitcoin: Cryptography, Engineering and Economics*. John Wiley & Sons.

*"I Lost Everything": How Squid Game Token Collapsed | CoinMarketCap*. (ei pvm.). CoinMarketCap Alexandria. Noudettu 22. marraskuuta 2021, osoitteesta https://coinmarketcap.com/alexandria/article/i-lost-everything-how-squid-game-token-collapsed

Jeffries, A. (2012, elokuuta 27). *Suspected multi-million dollar Bitcoin pyramid scheme shuts down, investors revolt*. The Verge.

https://www.theverge.com/2012/8/27/3271637/bitcoin-savings-trust-pyramid-scheme-shuts-down

King, S., & Nadal, S. (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. 6.

Kryptokansalainen. (2017, joulukuuta 12). *Kryptokansalainen | Perustiedot: Kryptovaluutat*. Kryptokansalainen. https://kryptokansalainen.fi/muut-kryptovaluutat/

Marella, V., Roshan, M., Merikivi, J., & Tuunainen, V. (2021). *Rebuilding Trust in Cryptocurrency Exchanges after Cyber-attacks*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2021.684

Mehar, M., Shier, C., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. (2017). *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack* (SSRN Scholarly Paper ID 3014782). Social Science Research Network. https://doi.org/10.2139/ssrn.3014782

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Oosthoek, K., & Doerr, C. (2020). From Hodl to Heist: Analysis of Cyber Security Threats to Bitcoin Exchanges. *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 1–9. https://doi.org/10.1109/ICBC48266.2020.9169412

Pilkington, M. (2015). *Blockchain Technology: Principles and Applications* (SSRN Scholarly Paper ID 2662660). Social Science Research Network. https://papers.ssrn.com/abstract=2662660

Saleh, F. (2021). Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies*, *34*(3), 1156–1190. https://doi.org/10.1093/rfs/hhaa075

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*, *9*(9), 1788. https://doi.org/10.3390/app9091788

*Secure Asset Fund for Users (SAFU)*. (ei pvm.). Binance Academy. Noudettu 2. marraskuuta 2021, osoitteesta https://academy.binance.com/en/glossary/secure-asset-fund-for-users

Siegel, D. (2016, kesäkuuta 25). *Understanding The DAO Attack*. https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/

Vasek, M., Thornton, M., & Moore, T. (2014). Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. Teoksessa R. Böhme, M. Brenner,

T. Moore, & M. Smith (Toim.), *Financial Cryptography and Data Security* (ss. 57–71). Springer. https://doi.org/10.1007/978-3-662-44774-1_5