



**Juho Toratti**

**KRYPTOVALUUTTOJEN PSEUDONYMITEETIN LUOMAT UHKAT – RAHANPESU JA  
TERRORISMIN RAHOITUS**

Kandidaatintutkielma

Kauppatieteet

Toukokuu 2021

## SISÄLLYS

<b>1</b>	<b>JOHDANTO</b> .....	<b>3</b>
<b>2</b>	<b>KRYPTOVALUUTTOJEN RIKOLLINEN POTENTIAALI</b> .....	<b>7</b>
<b>2.1</b>	<b>Kryptovaluutat</b> .....	<b>7</b>
<b>2.2</b>	<b>Lohkoketjuteknologia kryptovaluuttojen takana</b> .....	<b>8</b>
<b>2.3</b>	<b>Kryptovaluuttoihin liittyvät rikolliset mahdollisuudet</b> .....	<b>11</b>
2.3.1	Kryptovaluutat pimeän verkon maksuvälineenä.....	12
2.3.2	Moderni rahanpesu.....	13
2.3.3	Terrorismin rahoittaminen kryptovaluutoilla.....	15
<b>3</b>	<b>KRYPTOVALUUTTOIHIN LIITTYVÄN RIKOLLISUUDEN TODELLINEN UHKA</b> .....	<b>18</b>
<b>3.1</b>	<b>Kryptovaluuttojen rikollinen käyttö</b> .....	<b>18</b>
<b>3.2</b>	<b>Kryptovaluuttarikollisuuden luoma uhka</b> .....	<b>20</b>
<b>3.3</b>	<b>Kryptovaluuttarikollisuuteen puuttuminen</b> .....	<b>23</b>
<b>4</b>	<b>JOHTOPÄÄTÖKSET</b> .....	<b>26</b>
	<b>LÄHTEET</b> .....	<b>29</b>

## 1 JOHDANTO

Maaliskuussa 2021 muun muassa Reuters uutisoi Intian tekevän lakiesityksen, joka kriminalisoisi kryptovaluuttojen, kuten bitcoinin käytön ja omistamisen. Huhtikuussa Wall Street Journal julkaisi pitkän artikkelin, joka kertoi Kiinan luovan ensimmäisenä valtiona oman digitaalisen valuuttansa. Bitcoinin luoman megatrendin myötä tavalliselle sijoittajalle on voinut helposti tulla käsitys kryptovaluutoista ainoastaan mahdollisuutena nopeaan rikastumiseen, joten yllä mainitut uutiset ovat saattaneet ihmetyttää monia.

Menneenä talvena 2020–2021 bitcoin on ylittänyt useasti valtamedian uutiskynnyksen, mutta sitä käsittelevät uutisartikkelit keskittyvät enimmäkseen virtuaalivaluutan arvon volatiilisuuteen ja sen alttiuteen spekulatiivisille kuplille. Kryptovaluuttojen, kuten bitcoinin, muihin merkittäviin ominaisuuksiin media kiinnittää huomiota harvoin, eikä yksityissijoittaja välttämättä tiedosta muita virtuaalivaluuttoihin liittyviä piirteitä. Taloudellisen heilahtelun lisäksi virtuaalivaluuttoihin liittyy yhteiskunnallista riskiä niiden pseudonyymien, eli peitenimiin perustuvan luonteen takia. Koska kryptovaluutat ovat täysin kaiken viranomais sääntelyn ulottumattomissa ja ne salaavat käyttäjänsä todellisen identiteetin, houkuttelevat ne väistämättä osakseen globaalia rikollisuutta, kuten rahanpesua ja terrorismin rahoittamista. (Casey, Crane, Gensler, Johnson & Narula, 2018.) Foley, Karlsein ja Putninšin (2019) mukaan jopa 26 prosenttia bitcoinin käyttäjistä ja 46 prosenttia sen vaihdannasta liittyy rikollisuuteen.

Tutkielman aiheena on kryptovaluuttojen pseudonyymiin luonteeseen liittyvien riskien tutkiminen ja arvioiminen. Tarkastelun kohteena on virtuaalivaluuttojen käyttö rikollisen toiminnan, erityisesti terrorismin rahoittamisen ja modernin rahanpesun työkaluna. Virtuaalivaluutoista käsitellään pääsääntöisesti bitcoinia, sillä sen osuus kaikkien kryptovaluuttojen yhdistetystä markkina-arvosta on noin 62,3 prosenttia (Coin.dance, 2021). Koska bitcoin on suurin ja tunnetuin kryptovaluutta, on siitä kertynyt eniten tietoa, ja valtaosa tutkielman aihetta käsittelevistä tutkimuksista lähestyy yleisellä tasolla kryptovaluuttoja bitcoinin kautta.

Kryptovaluutat ovat nousseet selvästi sijoittamisen megatrendien joukkoon, ja niillä käydyssä kaupassa liikkuu paljon varallisuutta, minkä takia kryptovaluuttoihin liittyvä aihe on todella ajankohtainen. Huomioitavaa on myös se, että kryptovaluutoilla tapahtuvasta rikollisuudesta on kirjoitettu suhteellisen vähän tieteellistä tutkimusta, minkä takia aihetta käsittelevää kirjallisuutta tarvitaan. Tutkielma suoritetaan kirjallisuuskatsauksena, eli aiheeseen perehdytään ja pyritään vastaamaan tutkimuskysymyksiin aikaisemmin tehtyjen, vertaisarvioitujen tutkimusten perusteella.

Tutkielman tavoitteena on selvittää, kuinka paljon kryptovaluuttoja käytetään terrorismin rahoittamiseen ja rahanpesuun tällä hetkellä sekä kuinka paljon määrän odotetaan muuttuvan ajan kuluessa. Tutkielman tarkoituksena on myös kartoittaa kryptovaluuttarikollisuuden esittämää uhkaa globaalille yhteiskunnalle, sekä löytää keinoja kyseisen rikollisuuden estämiseen ja ennaltaehkäisemiseen. Tutkielman päätutkimuskysymyksiä ovat:

*Miten kryptovaluutat mahdollistavat rikollisuutta?*

*Kuinka suuri uhka kryptovaluuttarikollisuuteen liittyy?*

Lisäksi esitetään seuraavat apututkimuskysymykset, joilla pyritään rajaamaan päätutkimuskysymystä ja havainnollistamaan ratkaisuja ongelmaan:

*Kuinka merkittävä uhka kryptovaluutoilla tapahtuva rahanpesu on?*

*Kuinka merkittävä uhka kryptovaluutoilla tapahtuva terrorismin rahoittaminen on?*

*Kuinka paljon rikollisorganisaatiot voivat käytännössä hyödyntää kryptovaluuttoja?*

*Miten kryptovaluuttojen mahdollistamaa rikollisuutta voidaan estää?*

Kryptovaluuttojen käyttäminen ei vaadi käyttäjältään minkään henkilökohtaisen informaation luovuttamista ja valuutan omistajuus todennetaan virtuaalisen avainparin avulla. Tämä pseudoanonymiteetti luonnollisesti houkuttelee rikollisia, jotka haluavat salata kryptovaluutoilla tekemänsä transaktiot. Tunnistamattomuuden lisäksi kryptovaluuttoihin liittyy muita rikollisia hyödyttäviä piirteitä, kuten kansalliset rajat ylittävä liikkuvuus sekä verohyöty.

Yleistä mielipidettä kryptovaluuttojen rikolliseen soveltuvuuteen ei ole, vaan tutkijoiden mielipiteet ja arviot kryptovaluuttarahoitteisesta rikollisuuden uhasta vaihtelevat paljon. Kuitenkin on tullut esiin näyttöä kryptovaluutoilla tapahtuvasta rahanpesusta ja joidenkin terroristijärjestöjen tiedetään pyytävän lahjoituksia bitcoineina. Konkreettisesta näytöstä huolimatta tutkijat suhtautuvat eri tavoin kryptovaluuttojen merkitykseen globaalissa rikollisuudessa. Esimerkiksi kryptovaluuttarahoitteisen rikollisuuden vaikutus on joidenkin tutkijoiden mukaan suhteellinen verrattuna käteisellä rahalla tehtyihin rikoksiin.

Lähdemateriaalin perusteella tutkijoiden esittämät ratkaisukeinot kryptovaluuttarikollisuudelle ovat pitkälti samat; Kryptovaluutoilla tapahtuvaan rikollisuuteen voidaan puuttua parhaiten luomalla kansainväliset sääntelyraamit lohkoketjupohjaisille teknologioille. Tutkijat korostavat myös valtioiden keskinäisen yhteistyön sekä virkavallan yhteistoiminnan merkitystä kryptovaluuttarikollisuuden tutkimisessa ja rikoksista syyttämässä.

Tutkielma on jaettavissa pääpiirteittäin kahteen osaan. Ensimmäisessä osassa (luku 2) esitellään tiiviisti kryptovaluutat, lohkoketjuteknologia sekä rikollisesta näkökulmasta houkuttelevat piirteet kryptovaluutoissa. Ensimmäisen osan tarkoituksena on avata lukijalle tutkielmassa käytetyt termit, sekä luoda yleiskäsitys kryptovaluuttojen rikollisesta potentiaalista.

Toisen osan (luku 3) alussa käydään läpi, miten ja kuinka paljon kryptovaluuttoja käytetään rikollisten toimesta. Tämän jälkeen tutkielma käy läpi tutkijoiden arvioita kryptovaluuttarikollisuuden muodostamasta uhasta globaalille taloudelle ja turvallisuudelle sekä esittelee, miten tulevaisuuden kryptovaluutat voivat muuttaa tilannetta. Toisen osan lopussa kuvaillaan jo käytössä olevia ratkaisuja ja avataan tutkijoiden esittämiä ehdotuksia kryptovaluutoilla tehtävään rikollisuuteen puuttumiseen.

Tutkielman päätteeksi, neljännessä luvussa koostetaan tärkein sisältö ja tehdään johtopäätökset. Luvussa pyritään löytämään vartenotettavat vastaukset pää- ja apututkimuskysymyksiin. Luvun lopussa esitellään myös tutkielman pohjalta tulleita jatkotutkimuskysymyksiä ja -kohteita.

## 2 KRYPTOVALUUTTOJEN RIKOLLINEN POTENTIAALI

Tässä luvussa esitellään kryptovaluuttoihin liittyviä riskejä, erityisesti niiden pseudonyymien luonteen houkuttelemaa rikollisuutta. Luvun alussa kerrotaan tiivistetysti kryptovaluutoista ja niiden perustana olevasta lohkoketjuteknologiasta sekä avataan tarkemmin kryptovaluuttojen piirteitä, jotka mahdollistavat laittoman toiminnan. Luvun loppuosassa tarkastellaan kryptovaluutoilla tapahtuvaa rikollisuutta, erityisesti terrorismin rahoittamista ja rahanpesua.

### 2.1 Kryptovaluutat

Kryptovaluutta on kryptografiaan perustuva virtuaalinen valuutta. Yksinkertaisin määritelmä kryptografialle saadaan sen antiikin kreikankielisistä sanoista *kryptos* ja *graphein*, jotka suoraan käännettyinä tarkoittavat salakirjoitusta. Maailman ensimmäinen kryptovaluutta julkaistiin vuonna 2009, kun Satoshi Nakamoto<sup>1</sup> kehitti lohkoketjukonseptiin pohjautuvan bitcoinin. (Furieux, 2018.) Kryptovaluutoista tilastoja keräävän Coinmarketcap-internetsivun (2021) mukaan tällä hetkellä samaan lohkoketjuteknologiaan pohjautuu noin yhdeksän tuhatta eri kryptovaluuttaa, jotka eroavat toisistaan eri tavoin.

Kryptovaluutta luotiin finanssikriisin puhjettua vaihtoehtoiseksi maksutavaksi perinteisen elektronisen maksamisen rinnalle. Globaalin kriisin myötä luotto pankkisektoria kohtaan laski, minkä takia Nakamoton uskotaan innostuneen hajautettuun luottoon perustuvan valuutan kehittämistä (Kuo Chuen, Guo & Wang, 2018). Kryptovaluutat eroavat muista virtuaalivaluutoista siten, että kryptovaluutta ei tarvitse niin sanottua luotettua kolmatta osapuolta (trusted third party), kuten esimerkiksi pankkia tai välittäjää. Tämä on edelleen kaikkia kryptovaluuttoja yhdistävä piirre. Kolmannen osapuolen toiminnan sijasta kryptovaluutoilla maksaminen pohjautuu kryptografiseen todisteeseen. (Nakamoto, 2008.)

---

<sup>1</sup> Myös Satoshi Nakamoton epäillään olevan pseudonyymi. Bitcoinin luoja on pysynyt paria julkaisua lukuun ottamatta poissa suuren yleisön tietoisuudesta, eikä hänestä tiedetä sukupuolta, tai edes onko kyseessä vain yksi henkilö. (Kuo Chuen ym., 2018.)

Valtaosa internetin maksutapahtumista nojautuu perinteiseen elektroniseen maksamiseen ja luotettuina kolmansina osapuolina toimiviin rahoituslaitoksiin (Nakamoto, 2008). Luotetun kolmannen osapuolen tehtävänä on muun muassa toimia välikätenä ja varmistaa vaihdon osapuolten keskinäinen luotto sekä huolehtia, että käytetty valuutta on niin sanotusti käypää (Casey ym., 2018). Välikätenä toimimisesta rahoituslaitos perii palkkion, mikä kasvattaa maksutapahtuman kustannusta. Mitä suurempi maksutapahtuman transaktiokustannus on, sitä epäkannattavammaksi pienten ostojen tekeminen muodostuu. Kryptovaluuttojen tarvetta perustellaan sillä, että lohkoketjuun perustuvalla virtuaalivaluutalla on mahdollista tehdä pieniä käytännön ostoksia ilman transaktiokustannuksia. (Nakamoto, 2008.)

## **2.2 Lohkoketjuteknologia kryptovaluuttojen takana**

Virtuaalivaluutoille ainutlaatuinen haaste on digitaalisen rahan kahdesti käyttämisen ongelma (double spending problem). Koska virtuaalivaluutan transaktio ei tarvitse kolmatta osapuolta, syntyy riski siihen, että transaktiossa vaihtuva virtuaalivaluutan yksikkö, eli kolikko on jo käytetty. Tilanne on verrattavissa lunastettuun sekkiin, joka näyttää maksunsaajalle käypäisenä vaihdon välineenä, mutta todellisuudessa se on menettänyt arvonsa. (Pérez-Solà, Delgado-Segura, Navarro-Arribas & Herrera-Joancomartí, 2019.) Luodessaan bitcoinin Nakamoto ratkaisi kahdesti käyttämisen ongelman vertaisverkkoon (peer-to-peer network) hajautetulla julkisella tilikirjalla (distributed ledger), eli lohkoketjulla (block chain). Lohkoketjussa näkyvät kaikki bitcoinilla tehdyt transaktiot kronologisessa järjestyksessä. (Nakamoto, 2008; Antonopoulos, 2014, s. 15.)

Jokainen kryptovaluutan kolikko koostuu ketjusta digitaalisia allekirjoituksia. Kolikoiden hallinta perustuu käyttäjälleen annettuun digitaaliseen avainpariin, jonka perusteella kolikon omistajuus voidaan todentaa ja maksutapahtumat hyväksyä. Julkinen avain on kolikon osoite, joka on johdettu omistajan lompakossa, eli kryptovaluuttatilillä olevasta yksityisestä avaimesta. Julkista avainta käytetään kolikoiden lähettämiseen ja vastaanottamiseen. Yksityisellä avaimella kolikon salaus voidaan avata ja näin todistaa kolikon omistajuus sekä päästä käsiksi siitä johdettujen julkisten avainten takana oleviin varoihin. Transaktiossa, eli kryptovaluutan

maksutapahtumassa, edellinen omistaja allekirjoittaa omalla yksityisellä avaimellaan edellisen transaktion tiivisteeseen (hash), sekä seuraavan omistajan julkisen avaimen ja liittää nämä transaktioketjun perään. (Furieux, 2018; Nakamoto, 2008.)

Jotta maksunsaaja voi olla varma, ettei yksikään aikaisempi kolikon omistaja ole käyttänyt kolikkoa useasti, on maksutapahtumien oltava vertaisverkossa julkisia ja suurimman osan vertaisverkon solmujen (node) oikeaksi toteamia. Nakamoto (2008) ehdottaa ratkaisuksi aikaleimapalvelinta, jossa tietynä ajanjaksona tehdyistä transaktioista luotujen lohkojen (block) tiivisteet aikaleimataan ja julkaistaan. Jokainen aikaleima osoittaa aikaisemman datan verifioiduksi kyseisenä ajanhetkenä. Aikaleimatut lohkot muodostavat ketjun, jossa jokainen aikaleima vahvistaa edeltävien leimojen todenmukaisuuden.

Jotta aikaleimapalvelin toimisi vertaisverkossa, Nakamoto kehitti luonteeltaan ainutlaatuisen työntodistejärjestelmän (proof-of-work system), jolla lohkot suljetaan. Työntodistejärjestelmässä vertaisverkon solmujen tietokoneet ratkaisevat matemaattista yhtälöä etsien arvoa, joka tiivistettäessä antaa tietyn kirjain- ja numeroyhdisteen. Kun tietyn lohkon tiivistettä vastaava yhdistelmä löytyy, ensimmäisenä yhtälön ratkaissut vertaisverkon solmu julkaisee oikean yhdistelmän ja siihen liittyvän lohkon koko vertaisverkolle. Muut solmut hyväksyvät lohkon, mikäli kaikki siinä olevat transaktiot ovat päteviä, eikä niitä ole käytetty aikaisemmin. Solmut ilmaisevat hyväksyntänsä aloittamalla ketjun seuraavan lohkon työstämisen ja käyttävät siinä hyväksytyyn lohkon tiivistettä osana uutta lohkoa. Järjestelmän nopeuden tasaamiseksi työntodisteiden vaikeustaso kasvaa, mitä enemmän valmiita lohkoja luodaan. Tätä transaktioiden niputtamista ja verifiointia kutsutaan louhimiseksi (mining). (Furieux, 2018; Nakamoto, 2008.)

Insentiivinä louhimiselle ja työntodistejärjestelmälle on niin sanottu lohkopalkkio (block reward). Bitcoinin lohkoketjussa palkkiona ratkaistusta työntodisteesta ja siihen käytetyistä kustannuksista louhija saa uusia bitcoineja. Bitcoinjärjestelmässä lohkopalkkio puolittuu jokaisen 210 000 louhitun kolikon jälkeen, kunnes bitcoineja on kiertäessä ennalta määritetty 21 miljoonaa kappaletta ja lohkopalkkion suuruus on nolla. Bitcoinjärjestelmän aloittaessa toimintansa vuonna 2009, lohkopalkkio oli 50

bitcoinia. Tämä alkuperäinen lohkopalkkio määrittä vauhdin, jolla 21 miljoonan rajapyykin on arvioitu saavutettavan vuonna 2140. Kun lohkopalkkio on nolla, louhijat eivät saa louhinnasta uusia kolikoita, vaan louhimisprosessin ainoaksi tarkoitukseksi jää transaktioiden verifioiminen. Tällöin palkkiona louhimisesta louhijat saavat vain kolikoilla tehdyistä transaktiosta vähennetyt transaktiomaksut, joiden on arvioitu olevan liian pienet pitääkseen louhimisprosessin kannattavana. (Furieux, 2018.)

Työntodistejärjestelmän turvallisuutta kasvattaa se, ettei valmiiksi louhittua lohkoa voi enää muuttaa ilman, että vaadittu työ tehdään uudestaan. Seuraavien lohkojen ketjuuntuessa edellisiin, yhden lohkon muuttamiseksi tulee tehdä uudestaan myös kaikkiin muihin lohkoihin vaadittu työ. Mitä pidemmäksi valmiiden lohkojen ketju kasvaa, sitä vaikeampi järjestelmää on manipuloida. Toinen turvallisuutta kasvattava tekijä työntodistejärjestelmässä on tapa, jolla uudet lohkot hyväksytään. Jokainen vertaisverkon solmu on käytännössä tietokone, joka voi äänestää lohkon hyväksymisestä yhden kerran yhtä suoritinta kohti. Kun valtaosa suoritintehosta on niin sanotusti rehellistä, ainoastaan rehellisesti ja oikein suoritettut työntodisteet hyväksytään. Jotta epärehellinen tai laitton toimija voisi hyväksikäyttää tai manipuloida työntodistejärjestelmää, tarvitsisi se niin suuren suoritintehon ja energiatarpeen, että se on käytännössä mahdotonta. (Furieux, 2018; Nakamoto, 2008.)

Työntodistejärjestelmään perustuvan kryptovaluutan louhimiseen vaadittu valtava energiatarve on herättänyt kysymyksiä kyseisen louhinnan vaikutuksista ilmastoon ja pitkäaikaiseen kestävyteen (Casey ym., 2018). Kryptovaluutat ovat kehitymässä tällä sektorilla ja esimerkiksi markkina-arvoltaan toiseksi suurin kryptovaluutta Ethereum on siirtymässä ympäristöystävällisempään varantodistejärjestelmään (proof-of-stake system). Varantodistejärjestelmässä louhinta vaatii omistuosuuden louhittavasta kryptovaluutasta. Järjestelmän louhinnassa ei vaadita monimutkaisten laskutehtävien ratkaisua, vaan louhijan tulee todistaa omistuksensa, minkä jälkeen hänellä on oikeus louhia oman osuutensa verran kaikista transaktioista. Esimerkiksi omistamalla 40 prosenttia kaikesta Ethereum varallisuudesta, louhijalla on oikeus louhia noin 40 prosenttia transaktioista. Koska lohkojen sulkeminen ei varantodistejärjestelmässä vaadi matemaattisten yhtälöiden ratkaisua eikä yhtä

korkeaa suoritintehoa kuin työntodistejärjestelmässä, on varantodistejärjestelmän energiatarve huomattavasti pienempi. Toisin kuin työntodistejärjestelmässä, varantodistejärjestelmän louhimisesta ei saa palkkioksi uusia kryptovaluuttakolikoita, vaan ainoastaan transaktiomaksun. Varantodistejärjestelmässä louhijoita kutsutaan validaattoreiksi (validator). (Furieux, 2018.)

Yksi kryptovaluutan merkittävimmistä ominaisuuksista on sen käyttöön liittyvä yksityisyys. Perinteisessä elektronisessa maksamisessa maksutapahtuman osapuolet tuntevat toistensa ja luotetun kolmannen osapuolen todelliset identiteetit. Tässä mallissa yksityisyys suojataan pitämällä koko transaktio poissa julkisuudesta. Kryptovaluutat käyttävät mallia, jossa yksityisyys suojataan pitämällä maksutapahtuman osapuolien identiteetit täysin salassa ja sen sijaan itse transaktio on julkisessa tiedossa. (Nakamoto, 2008.) Albrechtin (2018) mukaan kryptovaluuttatiliä, eli lompakkoa avatessa käyttäjän ei tarvitse luovuttaa mitään henkilökohtaista informaatiota, mitä vaaditaan esimerkiksi pankkitilin käyttöönottamisessa. Kryptovaluutat eivät kuitenkaan ole täysin anonyymejä, vaan niitä voisi kutsua mieluummin pseudonyymeiksi, sillä käyttäjät jättävät lohkoketjuun oman tunnisteensa, joka ei kuitenkaan paljasta heidän todellista identiteettiään (O'Sullivan, 2018).

### **2.3 Kryptovaluuttoihin liittyvät rikolliset mahdollisuudet**

Puhuttaessa kryptovaluuttoihin liittyvistä riskeistä, tarkoitetaan yleensä kryptovaluuttojen voimakkaaseen volatiilisuuteen liittyviä, jo yleisesti tiedostettuja taloudellisia riskejä (Delikanli & Vogiazas, 2018). Harvemmin keskusteluissa nousee esiin kryptovaluuttojen pseudonyymien luonteen mahdollistama rikollinen potentiaali, mitä tämän tutkielman on tarkoitus käsitellä.

Ihmiskunnan historian läpi on aina ollut olemassa rikollisuutta jossain muodossa. Uusien teknologisten sovelluksien kehittyessä rikolliset ovat sopeutuneet kehitykseen ja pyrkineet löytämään uusia keinoja hyväksikäyttää teknologiaa. Näin on käynyt myös kryptovaluutoille, joiden identiteetin salaava käyttö on houkuttanut osakseen rikollisia toimijoita. Erityisesti niin sanotun pimeän verkon (darknet) markkinat ovat

omaksuneet anonymiteettia mahdollistavat kryptovaluutat yhdeksi tai jopa ainoaksi käyttökelpoiseksi vaihdannanvälineeksi (Kethineni, Cao & Dodge, 2018)

### 2.3.1 Kryptovaluutat pimeän verkon maksuvälineenä

Internet on jaettu nimellisesti kolmeen luokkaan: pintaverkkoon, syvään verkkoon ja pimeään verkkoon. Pintaverkko koostuu tavallisista, kaikille julkisista ja kaikilla selaimilla saatavilla olevista internetsivuista. Syvä verkko on pintaverkon vastakohta, eli sen sisältämiä verkkosivuja ei löydä tavallisilla hakukoneilla, mutta niille on mahdollista päästä tavallisilla selaimilla. Pimeä verkko on internetsivujen luokka, jotka vaativat IP-osoitteen piilottavan internetselaimen päästäkseen sisälle. Anonymiteetin antava ja tietojen urkinnalta suojaava pimeä verkko on suosittu henkilöiden keskuudessa, jotka haluavat pitää todellisen identiteettinsä ja selaushistoriansa salassa. Vaikka osa käyttäjistä toimii täysin laillisesti ja hakee pimeästä verkosta vain yksityisyyden suojaaja, on valtaosa verkon toiminnasta ja materiaalista laitonta. Pimeä verkko toimii alustana esimerkiksi terroristijärjestöjen kommunikaatiolle ja monille kauppapaikoille, joissa myydään muun muassa huumeita, aseita, laitonta pornografiaa ja palkkamurhia. (Kethineni ym., 2018; Moore & Rid, 2016.)

Mahdollisesti tunnetuin pimeän verkon markkinapaikka on Silkkitie (Silk Road), joka toimi kohtaamispaikkana monille rikollisille toimijoille, erityisesti huumekaupan parissa. Kahden vuoden toimintansa aikana Silkkitie ehti tuottaa voittoa arviolta yli 1,2 miljardia dollaria, kunnes Yhdysvaltain keskusrikospoliisi FBI sulki sivuston vuonna 2013. (Kethineni ym., 2018.) Bitcoin oli Silkkitien ainoa hyväksytty valuutta ja sivuston sulkemisen yhteydessä FBI takavarikoi yli neljän miljoonan dollarin arvosta bitcoineja (Foley ym., 2019; Kethineni ym., 2018). Lohkoketjuteknologian mahdollistamaa itsenäisyyttä luotetuista kolmansista osapuolista hyödynnetään siis aktiivisesti internetissä operoivien rikollisten toimesta. Anonymiteetin kasvattamiseksi on luotu myös muita kryptovaluutoita, kuten Zcash ja Dash, joiden on tarkoitus salata valuutalla tehdyt transaktiot ja niiden takana olevat identiteetit bitcoinia paremmin (Furieux, 2018).

### 2.3.2 Moderni rahanpesu

Rahanpesu on määritelmän mukaan toimintaa, jossa ohjataan laittomista lähteistä saatuja rahavirtoja ulkopuolisten rahoituskanavien kautta, jotta varat näyttäisivät laillisilta (Buchanan, 2004). Rahanpesu on usein yhdistettävissä järjestäytyneeseen rikollisuuteen ja sen tarkoituksena on häivyttää laittomasti saatujen varojen yhteyttä niiden takana oleviin rikollisiin toimiin, eli niin sanottuihin alkurikoksiin (Gilmour, 2016; Mabunda, 2018). Käytännössä rahanpesua harjoittavat toimijat haluavat sulauttaa laittomin keinoin saadut varat yleiseen rahoitusjärjestelmään, jotta ne näyttäytyisivät ulkopuolisille rehellisesti ansaittuina ja käyttökelpoisina kassavirtoina. Näin rahanpesijat voivat käyttää varat tavallisen rahan tavoin joko uusien rikoksien rahoittamiseen tai oman elintasonsa ylläpitämiseen. (Levi, 2002 via Albrecht, Duffin Hawkins & Morales Rocha, 2019; Buchanan, 2004.) Ilman rahanpesua alkurikoksista saadut tuotot eivät olisi rikollisille täysin käytettävissä (Gilmour, 2016).

Rahanpesu on monimutkainen prosessi, jonka ajatellaan tapahtuvan yleensä kolmiosaisena tapahtumasarjana (Gilmour, 2016). Ensimmäinen osa on sijoittaminen (placement), jossa laittomasti ansaitut varat vaihdetaan helpommin liikuteltavaan ja vähemmän epäilyttävään muotoon sijoittamalla ne suoraan yleiseen rahoitusjärjestelmään, esimerkiksi tallettamalla ne yhdelle tai usealle pankkitilille. Sijoittaminen on rikollisen kannalta rahanpesun haavoittuvin vaihe, sillä useimmat rikolliset aktiviteetit tuottavat käteistä, jota on vaikea piilottaa ja liikuttaa hallintoalueiden välillä. (Buchanan, 2004.) Lisäksi sijoittamisvaiheessa rikolliset varat tulevat ensikertaa esille, jolloin viranomaiset voivat jäljittää varoja (Albrecht ym., 2019). Toisessa vaiheessa, eli kerrostamisessa (layering) varoja käytetään laillisissa maksutapahtumissa, jotta niiden alkuperä hämärtyisi. Maksutapahtumien verkko pyritään kerrostamisessa pitää mahdollisimman luonnollisen näköisenä ja usein tässä vaiheessa käytetään ulkomaisia rahoituskanavia. Kun kassavirrat kulkevat usean eri maan ja hallintoalueen läpi, varojen jäljittäminen vaikeutuu entisestään. (Albrecht ym., 2019; Buchanan, 2004.) Viimeisessä vaiheessa, integraatiossa (integration) laittomin keinoin syntyneet kassavarat integroituvat rahoitusjärjestelmään tavallisten taloudellisten toimien, kuten sijoittamisen ja arvopapereiden ostamisen kautta. Näiden

kolmen portaan kautta kuljettuaan laittomista rahoista tulee niin sanotusti pestyjä. (Buchanan, 2004.)

Ennen internetiä rahanpesu tehtiin tyypillisesti perustamalla pieniä, erillisiä yrityksiä tai kätkemällä kassavirrat suurten yritysten rahoituskanaviin. Internetin myötä myös rahanpesu on alkanut siirtymään entistä enemmän digitaaliseen ympäristöön. Kryptovaluuttojen suosion kasvaessa järjestäytynyt rikollisuus on kiinnostunut kryptovaluutoista rahanpesun välineenä. (Albrecht ym., 2019.) Lähes kaikki bitcoineilla tehty rahanpesu tapahtuu pimeän verkon alustoilla, kuten Silkkitiellä. Yleisimmät vaihdantapalvelut laittomien bitcoinien pesemiseen ovat uhkapelisivuodot, sekä kryptovaluuttamixerit (cryptocurrency mixer), joissa identifioitavia kryptovaluuttavaroja kootaan yhteen niiden alkuperän ja maksuliikenteen salaamiseksi. (Fanusie & Robinson, 2018.)

Moderni kryptovaluutoilla tapahtuva rahanpesu noudattaa pitkälti samaa kolmiosaista prosessia kuin perinteinen rahanpesu, vaikkakin kaikki vaiheet tapahtuvat suurimmaksi osaksi kryptovaluuttojen omassa ekosysteemissä (Fanusie & Robinson, 2018). Kryptovaluuttoihin liittyy kuitenkin useita piirteitä, jotka houkuttelevat rikollisia suosimaan esimerkiksi bitcoinia rahanpesussa. Ennen kryptovaluuttojen kehittämistä järjestäytynyt rikollisuus joutui siirtämään ja piilottamaan laittomin keinoin ansaittuja varoja yleiseen keskuspankkijärjestelmään. Tämä antoi julkiselle vallalle, kuten valtioille mahdollisuuden puuttua rahanpesuun sääntelemällä pankkitoimintaa raskaammin, mikä vaikeutti rahanpesuprosessia. Kryptovaluutoilla tapahtuvassa rahanpesussa ei ole tällaista mahdollisuutta, sillä kryptovaluutat ovat täysin valtioiden sääntelyn ulottamattomissa. (Albrecht ym., 2019.)

Toinen rahanpesun kannalta hyödyllinen piirre liittyy kryptovaluuttojen mahdollistamaan veronkiertoon. Koska kryptovaluutat ovat pseudonyymejä ja niillä tapahtuva maksuliikenne on täysin digitaalista, ei kryptovaluutoilla saatuja voittoja voida yhdistää yhteenkään yksityishenkilöön, ellei henkilö realisoi voittojaan vaihtamalla kolikkonsa perinteiseksi lainvoimaiseksi valuutaksi, eli fiat-rahaksi. Näin ollen kryptovaluutoista saatuja tuottoja ei voida verottaa, mikäli varat pidetään

kryptovaluuttana. Kryptovaluuttojen voidaan ajatella olevan täydellinen veroparatiisi, jonka toimintaan valtiot eivät voi puuttua. (Albrecht ym., 2019.)

Kerrostusvaiheessa kryptovaluuttojen ehdoton etu liittyy niiden siirtämiseen. Perinteisellä tilisiirrolla varojen siirtäminen toisen valtion hallintoalueelle voi herättää viranomaisten huomion ja maksuliikenteeseen voidaan puuttua. Kryptovaluutoilla varojen siirtäminen onnistuu mistä vain, kunhan internetyhteys on saatavilla, sillä kolikkojen käytön mahdollistavat avaimet voidaan lähettää vaikka sähköpostitse. (Albrecht ym., 2019; Fanusie & Robinson, 2018.)

### 2.3.3 Terrorismin rahoittaminen kryptovaluutoilla

Irwin ja Milad (2016) määrittelevät terrorismin rahoittamisen olevan sananmukaisesti prosessi, jossa terroristijärjestöt saavat varoja terroritekojensa toteuttamiseen. Kuten mitkä tahansa organisaatiot, myös järjestäytyneet rikollisuus ja terroristijärjestöt tarvitsevat toimivan taloudellisen infrastruktuurin toimiakseen. Dion-Schwartzin, Manheimin ja Johnstonin (2019, s.7) mukaan tämä rahankäyttöllinen järjestelmä on jaettu kolmeen osaan: rahoitukseen (receipt), hallintaan ja kuljetukseen (management and transfer) sekä kulutukseen (spending).

Terroristijärjestön rahankäytön ensimmäinen luokka on rahoitus, eli kanavat, joilla terroristijärjestö kerää toimintaansa tarvitsemansa varat. Yleisimmät terroristijärjestön rahoitustavat ovat yksityiset lahjoitukset, valtiovaltojen antama suora rahoitus<sup>2</sup>, laiton toiminta, kuten huumekauppa ja kiristyksset, sekä lailliset tulonlähteet, kuten järjestön jäsenten lailliset palkkatulot (Oftedal, 2015). Toinen luokka on hallinta ja kuljetus.

---

<sup>2</sup> Valtiovaltojen antama suora rahoitus tai sponsorointi tarkoittaa nimensä mukaan valtioiden terroristiorganisaatioille antamaa suoraa taloudellista tukea. Taloudellinen tuki voi olla suoraa rahoitusta tai aseiden välittämistä organisaatioille. Valtioiden insentiivinä tukea terroristijärjestöjä on usein järjestöjen ajama, valtiolle suotuisa aate. Kylmän sodan aikana terrorismin tukeminen valtioiden suoralla rahoituksella oli yleistä, esimerkiksi Neuvostoliiton esitetään tukeneen Marxistisia aatteita ajaneita organisaatioita ja Yhdysvallat puolestaan tukivat samaa aatetta vastustaneita järjestöjä. Tänä päivänä mahdollisesti aktiivisin terroristijärjestöjä tukeva valtio väitetään olevan Iran, jonka arvioidaan antavan taloudellista apua terroristijärjestö Hizbollahille. (Freeman, 2011.)

Ajan saatossa valtioiden antama suora rahoitus on vähentynyt huomattavasti ja muiden rahoituskanavien merkitys on vahvistunut terroristijärjestöille (Oftedal, 2015).

Luokka pitää sisällään menetelmät, joilla järjestö hallinnoi ja kätkee varojaan sekä myöhemmin siirtää rahaa sitä tarvitseville tahoille, kuten iskuja valmistelevalle terroristisolulle. Mikäli järjestö ei suoraan hallitse keräämiään varoja tai turvallisuussyistä niitä ei voi kuljettaa järjestön hallitsemalle alueelle, voi terroristiorganisaatio käyttää rahanpesua työkaluna varojen haltuun ottamisessa. Muita varojen siirrossa käytettäviä menetelmiä ovat muun muassa käteiskuriirit, epäviralliset siirtojärjestelmät, kuten hawala<sup>3</sup>, korruptoituneiden työntekijöiden mahdollistamat tilisiirrot julkisissa pankeissa, valelaskuttaminen ja kalliiden hyödykkeiden, kuten kullan salakuljettaminen. (Freeman & Ruehsen, 2013.) Viimeinen luokka on kulutus, eli terroristijärjestölle kertyvät kustannukset. Jokaiselle eri terroristiorganisaatiolle kertyy eri tavalla kustannuksia riippuen järjestön toiminnasta ja tavoitteista, mutta yleisesti kulutusluokka jaetaan organisaation toiminnallisiin kuluihin ja väkivaltaan liittyviin kustannuksiin. Toiminnallisia kuluja ovat muun muassa järjestön sisäiset palkat sekä koulutuskustannukset, ja väkivaltaan liittyviä kustannuksia ovat esimerkiksi aseostot. (Dion-Schwarz ym., 2019, s. 8–14.)

Rahoituksen kerääminen ja hallinta vaatii terroristijärjestöiltä kykyä sopeutua uusiin rahoituskanaviin, ja järjestöt hakevat jatkuvasti uusia vaihtoehtoisia kanavia entisten keinojen tullessa riskialttiimmiksi (Freeman & Ruehsen, 2013). Kuten moni muukin rikollisorganisaatio, myös terroristijärjestöt ovat kiinnostuneet kryptovaluutoista niiden identiteettiä piilottavan luonteen takia. Dion-Schwartzin ym. (2019, s. 8–14) arvioivat terroristijärjestöjen hyötyvän kryptovaluutoista taloudellisen infrastruktuurin kahdessa ensimmäisessä luokassa, eli rahoituksessa ja hallinnassa.

---

<sup>3</sup> Hawala -järjestelmä on vanha, intialaisissa ja kiinalaisissa sivilisaatioissa syntynyt varojen siirtojärjestelmä, joka toimii edelleen vaihtoehtoisena varojensiirtoväylänä modernia pankkijärjestelmää kaihtaville henkilöille. Järjestelmässä kauppiat käyttävät pientä korvausta vastaan kauppasuhteitaan kolmannen osapuolen varojen siirtämiseen. (Irwin & Milad, 2016.) Käytännössä hawala toimii niin, että varoja siirtävä henkilö ottaa yhteyttä hawalakauppiaseen (hawaladar) ja antaa hänelle siirrettävän rahasumman. Hawalakauppias välittää tiedon siirrosta toiselle kauppiaille halutussa maassa ja antaa varoja lähettävälle henkilölle sekä kohdemaan hawalakauppiaille yhteisen koodin. Tällä koodilla kohdemaassa varat vastaanottava henkilö voi lunastaa paikalliselta kauppialta siirrettävän summan, josta on vähennetty välityspalkkio. Tilit tasatakseen hawalakauppiat odottavat vastaavan suuruista, toisin päin suuntautunutta siirtotapahtumaa tai he tekevät siirrety summan kokoisena valemaksutapahtuman. On tärkeä huomata, etteivät hawala-järjestelmässä siirretyt varat todellisuudessa ylitä valtioiden tai alueiden välisiä rajoja. (Freeman & Ruehsen, 2013.)

Rahoituksessa kryptovaluutoilla arvellaan olevan suurin rooli liittyen yksityisiin lahjoituksiin ja huumekauppaan. Kryptovaluuttojen ja niiden pseudonyymien luonteen arvellaan madaltavan kynnystä ja helpottavan ulkomailla asuvien, terroristijärjestön aatteita ihannoivien yksityisten henkilöiden mahdollisuutta tukea järjestöjä. Brantleyn (2014) mukaan tästä on jo näyttöä, sillä joidenkin terroristijärjestöjen tiedetään suosittavan kannattajille suunnatuillaan propagandasivustoilla bitcoinin käyttöä lahjoitusten tekemisessä. Merkittävässä roolissa terroristijärjestöjen rahoituksessa on huumekauppa ja laittoman materiaalin myyminen, mitä tapahtuu pimeässä verkossa pitkälti kryptovaluuttojen välityksellä. Luonnollisesti terroristijärjestöt hyötyvät samoista kryptovaluuttojen piirteistä kuin muut pimeän verkon käyttäjät. (Dion-Schwarz ym., 2019, s. 8–10.)

Hallinnallisissa toimissa terroristijärjestöt voivat hyödyntää kryptovaluuttoja varojen siirrossa. Kryptovaluutat mahdollistavat rahan siirron todella nopeasti ja vaivattomasti verrattuna esimerkiksi perinteiseen hawala-siirtojärjestelmään. Vaikka hawalalla siirrettyjä varoja on todella vaikea jäljittää, on järjestelmällä epäkäytännöllistä lähettää varoja laajalta alueelta ja toimittaa niitä useaan kohteeseen. Lisäksi hawala-järjestelmällä varojen siirtäminen voi olla todella hidasta. (Irwin & Milad, 2016.)

### **3 KRYPTOVALUUTTOIHIN LIITTYVÄN RIKOLLISUUDEN TODELLINEN UHKA**

Luvun tarkoituksena on käydä läpi kryptovaluuttojen mahdollistaman rikollisuuden merkitystä globaaliin talouteen ja turvallisuuteen. Luvun alussa tuodaan esiin tutkijoiden näkemyksiä siitä, kuinka mahdolliseksi tai todennäköiseksi kryptovaluuttojen rikollinen käyttö käytännössä koetaan. Tämän jälkeen esitellään tutkijoiden ajatuksia kryptovaluuttojen luomasta todellisesta uhkasta ja luvun lopussa annetaan mahdollisia ratkaisuehdotuksia kryptovaluutoilla tapahtuvan rikollisuuden ehkäisemiseksi.

#### **3.1 Kryptovaluuttojen rikollinen käyttö**

Foleyn ym. (2019) tutkimuksen mukaan merkittävä osa, jopa 46 prosenttia kaikesta bitcoinilla tapahtuvista transaktioista liittyy rikollisuuteen, joten rikollisuuden merkitystä kryptovaluuttojen vaihdannassa ei ainakaan voida kieltää. Vaikka kryptovaluutoilla on potentiaalia helpottaa rikollista toimintaa, on tutkijoilla erilaisia näkemyksiä siitä, kuinka hyvin kryptovaluutat käytännössä soveltuvat rikollisten käyttöön.

Yhteinen mielipide monilla tutkijoilla on se, että kryptovaluuttojen pseudonyymi luonne houkuttelee rikollisuutta puoleensa. Teichmannin ja Falkerin (2020) haastatteleminen rikollisten mukaan perinteiseen pankkijärjestelmään verrattuna lohkoketjuteknologian mahdollistama salatumpi identiteetti on rikollisesta näkökulmasta suuri etu kryptovaluutoissa. Myös Albrecht ym. (2019) mainitsevat kryptovaluuttojen käyttäjien vaikean jäljittämisen houkuttelevan mustassa pörssissä operoivia rikollisia.

Ongelmana kryptovaluuttojen rikolliselle käytölle tutkijat näkevät sen sopimattomuuden jokapäiväisiin maksutapahtumiin. Tällä hetkellä hyvin harva kauppa vastaanottaa kryptovaluuttoja, mikä rajaa rikollisorganisaatioiden mahdollisuutta käyttää kryptovaluuttoja täysimittaisesti (Albrecht, 2018; Teichmann & Maximilian, 2018). Kuitenkin Albrecht ym. (2019) huomauttavat, että

kryptovaluuttojen alati kasvattaessa suositaan, rikolliset hyötyvät niistä entistä enemmän. Varsinkin bitcoinin käytön yleistymisen ja yleisen hyväksynnän kasvamisen myötä, Kethineni ym. (2018) arvioivat rikollisorganisaatioiden kiinnostuneen kryptovaluuttojen rikollisesta potentiaalista yhä enemmän ja käyttävän esimerkiksi bitcoineja luovemmin operaatioissaan.

Terrorismin rahoittamisen kannalta tutkijoiden mielipiteet kryptovaluuttojen sopivuudesta poikkeavat hieman. Teichmann (2018) pitää kryptovaluuttoja sopivana välineenä terroristiorganisaatioille ja painottaa, kuinka kryptovaluutoilla organisaatiot voivat kerryttää merkittäviä summia pieninä, hajautettuina lahjoituksina anonyymeinä pysytteleviltä kannattajilta sekä hyödyntää kryptovaluuttoja pimeän verkon maksutapahtumissa. Dion-Schwarz ym. (2019, s. 21) kuitenkin toteavat, että vaikka kryptovaluutoilla on mahdollista edistää tiettyjä terrorismin rahoituksen osa-alueita, eivät kryptovaluutat sovellu terroristijärjestöjen yleisiin tarpeisiin. Tutkijaryhmä näkee vain vähän todistusaineistoa sille, että terroristiorganisaatiot olisivat ottaneet tai niillä olisi motivaatiota ottaa käyttöön kryptovaluuttoja laajasti tai systemaattisesti. Dion-Schwarz ym. arvioivat kryptovaluuttojen soveltuvuutta järjestöjen käyttöön kuuden piirteen; anonyymiteetin, käytettävyyden, turvallisuuden, hyväksynnän, luotettavuuden ja volyymin perusteella. Tutkijoiden mukaan mikään olemassa oleva kryptovaluutta ei täyttänyt täysin kyseisiä tarpeita.

Osa tutkijoista on kuitenkin sitä mieltä, että terrorismin rahoittamisesta kryptovaluutoilla on jo nyt vahvaa näyttöä. Esimerkiksi Brantly (2014) tuo ilmi, että muutamat terroristijärjestöihin liitetyt nettisivut ovat alkaneet mainostaa lahjoitusten vastaanottamista bitcoineilla. Tämän lisäksi kerrotaan löytyneen merkkejä siitä, että terroristijärjestö ISISin omistamissa lompakoissa olisi miljoonien arvosta bitcoineja. Terroristijärjestöjen kryptovaluuttoihin liittyvän tietotaidon kasvamisesta kertoo osakseen myös ISISin ulkomaisille kannattajille suunnattu ohjekirja, jossa on erillinen kappale siitä, kuinka järjestön hallinnoimille alueille voi päästä huomaamattomasti käyttämällä bitcoineja. (Irwin & Milad, 2016.) Dion-Schwartz ym. (2019, s. 10) mainitsevat kryptovaluuttojen mahdollisuudesta helpottaa pimeässä verkossa käytävää laitonta kauppaa, johon liittyen Kfir (2020) nostaa esiin arvion, että Pariisissa vuonna 2016 tehdyissä terrori-iskuissa olisi käytetty pimeästä verkosta ostettuja aseita. Myös

Irwin ja Milad (2016) tuovat ilmi, että Ranskassa vuonna 2015 koordinoitusti toteutettujen terrori-iskujen epäillään olleen rahoitettu bitcoineilla.

Siinä missä kryptovaluuttojen soveltumisesta ja tämänhetkisestä käytöstä terroristijärjestöissä on hieman erilaisia näkemyksiä tutkijoiden kesken, rahanpesun suhteen kryptovaluutoilla nähdään vähemmän esteitä. Brenigin, Accorsin ja Müllerin (2015) analyysin perusteella suurin osa kryptovaluuttojen taloudellisista piirteistä, kuten pseudonyymi luonne, voidaan katsoa insentiiveiksi rahanpesussa hyödyntämiseen. Van Wegbergin, Oerlemansin ja van Deventerin (2018) mukaan kryptovaluuttojen käytöllä rahanpesuprosessissa on kasvaneen anonymiteetin lisäksi mahdollisuus jopa laskea prosessin kustannuksia rikollisorganisaatiolle, minkä takia tutkijat pitävät kryptovaluuttojen integroimista tämän päivän sekä tulevaisuuden rahanpesuun erittäin todennäköisenä.

Rikollisesta näkökulmasta negatiivisia puolia kryptovaluutoissa ovat vain rajoittunut hyväksyntä ja hinnan merkittävä volatiilisuus (Brenig ym., 2015). Albrecht ym. (2019) toteavat kryptovaluuttojen suosion sekä yleisen hyväksynnän kuitenkin kasvavan jatkuvasti, ja Mabunda (2018) huomauttaa, että kryptovaluuttojen käyttö rahanpesussa ei lakkaa tapahtumasta, vaikka niiden markkinat romahtaisivat. Van Wegberg ym. (2018) mukaan EU-maiden poliisiorganisaatioiden yhteenliittymä Europolin raporttien perusteella rikollisorganisaatiot käyttävät jo nyt bitcoineja rahanpesun välineenä. Myös Fanusien ja Robinsonin (2018) tutkimus antaa vahvaa näyttöä bitcoineilla tapahtuvasta rahanpesusta.

### **3.2 Kryptovaluuttarikollisuuden luoma uhka**

Kryptovaluutat ovat herättäneet rikollisten kiinnostuksen, ja rikollisorganisaatioiden tiedetään soveltavan niitä laittomissa toimissaan. Kryptovaluutoilla tapahtuvan rikollisen toiminnan uhasta kansainväliselle taloudelle ja turvallisuudelle on kuitenkin eriäviä mielipiteitä. Kryptovaluuttojen uniikit piirteet, kuten hajautettu luotto sekä pseudonymiteetti mahdollistavat niiden käytön terrorismin rahoituksessa ja modernin rahanpesun välineenä. Piirteet ovat niin merkittäviä, että ne voivat jopa kannustaa rikollisia käyttämään kryptovaluuttoja toiminnassaan. Tämä takia tutkijat näkevät

kryptovaluuttojen muodostavan akuutin uhkan kansalliselle turvallisuudelle (Fletcher, Larkin & Corbetin, 2021). Vastakkaisen näkemyksen antaa O’Sullivan (2018), jonka mukaan kryptovaluutat eivät luo juuri minkäänlaista uutta uhkaa, jota säännellyt fiat-valuutat eivät jo mahdollistaisi. Sen sijaan O’Sullivanin mukaan kryptovaluuttojen voidaan nähdä ajavan säänneltyjä valuuttoja paremmin länsimaisia arvoja, kuten yksityistä omistamista ja sopimuksille lojaaliutta (contractual fidelity).

Merkittävä huomautus, jonka O’Sullivan (2018) tuo ilmi on se, että vaikka kryptovaluuttoja on mahdollista hyödyntää rikollisuudessa ja niiden avulla voidaan toteuttaa hirveitä asioita, eivät kryptovaluutat ole ainoa ehto rikollisille. Kyseisiä rikoksia on tehty jo ennen kuin Satoshi Nakamoton julkaisi artikkelin lohkoketjuun pohjautuvasta virtuaalivaluutasta, ja niitä tullaan jatkossakin tekemään käteisellä rahalla. Yhdysvaltojen dollari on mahdollisesti maailman luotetuin valuutta ja sen käyttö sekä hyväksyntä on levinnyt ympäri maailman, toisin kuin kryptovaluutat, joiden hyväksyntä on vielä hyvin rajattua. (O’Sullivan, 2018.) Europolin raportin (2015) mukaan käteinen on edelleen vallitsevin valuutan muoto rikollisten keskuudessa ja esimerkiksi rahanpesustrategioissa ja terrorismin rahoittamisessa perinteisen käteisen käyttö on hallitsevin menetelmä. Vaikka raportin mukaan kryptovaluutat, kuten bitcoin mahdollistavat uudenlaisen rahanpesun, tarvitaan tällä hetkellä vielä käteistä rahaa tämän modernin rahanpesuprosessin aloittamiseen ja lopulta hyödyntämiseen (Europol, 2015).

Käteisessä valuutassa, kuten sadan euron setelissä, ei ole nähtävissä kenen omistuksessa kyseinen raha on ollut aikaisemmin. Koska kryptovaluutan yksittäinen kolikko koostuu sen omistajien ’nimikirjoituksista’ ja kolikolla tehdyt transaktiot ovat tallennettu kaikille avoimeen lohkoketjuun, on jokaisessa kolikossa nähtävissä sen koko omistushistoria (Nakamoto, 2008). Tämä kryptovaluuttojen piirre on ratkaiseva tekijä kryptovaluutoilla tehtyjen rikosten tutkinnassa. Vaikka kryptovaluutat antavat henkilöllisyydensuojaa niiden käyttäjille, voidaan kaikki transaktioketjun osapuolet yhdistää rikolliseen toimintaan, mikäli yhdenkin ketjun käyttäjän identiteetti paljastuu rikosta tutkivalle organisaatiolle. Rikollisen transaktioketjun paljastuttua muiden ketjun osallisten henkilöllisyydet pysyvät yhä salassa, mutta virkavalta pystyy seuraamaan ja etsimään heidän tekemiään transaktioita sekä mahdollisesti tekemään

päätelmiä rikollisorganisaatioiden laajuudesta tai jopa yksittäisten toimijoiden henkilöllisyydestä. (Foley ym., 2019.)

Reynolds ja Irwin (2017) esittävät, että lohkoketjun transaktioita seuraamalla rikollisessa toiminnassa käytetyt bitcoinit voidaan jäljittää kryptovaluutanvaihtajaan, eli kryptovaluuttapörssiin (crypto exchange), joka on vaihtanut kyseiset kolikot fiat-valuuttaan. Jos bitcoinin ostaja on luovuttanut pörssille jotain henkilökohtaista informaatiota, voidaan rikollinen toiminta yhdistää tiettyyn henkilöön. Kuitenkin kryptovaluuttapörssien identifikaatiota ja vaihdannassa käytettävää rahamuotoa, kuten käteismaksua koskevat säännöt voivat vaihdella, minkä takia lompakon omistajan identifioimiseen tarvittavia tietoja ei ole välttämättä saatavilla. Tutkijoiden mukaan valtaosaan kryptovaluuttapörssien keräämistä henkilökohtaisista tiedoista voidaan luottaa esimerkiksi rikoksesta syyttämisen yhteydessä, mutta toistaiseksi kyseiseen informaation tulee suhtautua varauksella. Tietoteknisesti taitava rikollinen voi onnistua vaihtamaan perinteistä valuuttaa kryptovaluutaksi salanimen turvin. (Reynolds & Irwin, 2017.)

Vaikka kryptovaluutat tarjoavat rikollisille toimijoille ylimääräistä anonymiteettiä, ovat ne tietyiltä osin käteistä rahaa helpommin yhdistettävissä niiden alkurikoksiin. Lisäksi kryptovaluuttoihin liittyy muita rikollisesta näkökulmasta negatiivisia piirteitä ja niillä operoiminen vaatii selvästi käteistä enemmän vaivaa ja tietotaitoa. Käteisen hyödyntäminen on kuulunut vuosien ajan rikollisorganisaatioiden toimintaan, minkä takia sen käyttö ei vaadi rikollisilta sopeutumista tai uuden opettelua. Tämän perusteella kryptovaluuttojen mahdollistaman rikollisuuden todellinen uhka verrattuna käteisellä rahalla tapahtuvaan rikollisuuteen on suhteellinen.

Kryptovaluutat eivät välttämättä luo merkittävää uhkaa kansainväliselle turvallisuudelle tällä hetkellä, mutta muun muassa Dion-Schwarz ym. (2019, s. 47–56) näkevät kryptovaluutoilla pitkän aikavälin vaikutuksia esimerkiksi vasta-terrorisminrahoittamiseen. Kryptovaluuttojen alati kehittyessä tutkijaryhmä kokee mahdolliseksi, että syntyy uusi kryptovaluutta, joka ominaisuuksiltaan sopii kehittyneiden terroristijärjestöjen käyttöön ja mahdollistaa entistä helpommin terrorismiskut länsimaita vastaan. Albrecht ym. (2019) mukaan kryptovaluutoilla tehtävällä

rahanpesulla on jo nyt potentiaalia vaikuttaa laajasti talouteen ympäri maailman, mitä uudet kehittyneemmät kryptovaluutat voivat Fanusien ja Robinsonin (2018) mukaan vain helpottaa. Irwin ja Milad (2016) sekä Albrecht ym. (2019) toteavat, että kryptovaluutoilla tapahtuvaan rikollisuuteen tulee puuttua mahdollisimman nopeasti vielä, kun kyseinen rikollisuus on suhteellisen vähäistä.

### 3.3 Kryptovaluuttarikollisuuteen puuttuminen

Keväällä 2021 kryptovaluuttojen käyttöön puuttuminen nousi median otsikoihin, kun Intia julkisti esittävänsä lakia, joka kriminalisoi kryptovaluuttojen käytön. Laki olisi yksi maailman tiukimmista kryptovaluuttoihin liittyvistä rajoituksista, ja sen myötä muun muassa valuuttojen omistus, vaihdanta ja louhiminen olisi laitonta. Kryptovaluuttojen käytön totaalinen kieltäminen on kuitenkin keino, jota Teichmann (2018) pitää epärealistisena.

Kryptovaluuttojen käytön kriminalisointi on sääntelyn keinona todella äärimmäinen ja käytännössä vaativa toteuttaa. Kryptovaluuttojen käyttö on kielletty aikaisemmin muun muassa Saudi-Arabiassa ja Vietnamissa, mutta kriminalisoinnista huolimatta tutkimustulokset osoittavat kansalaisten jatkaneen kryptovaluutoilla kaupankäyntiä (Teichmann & Falker, 2020). Useiden tutkijoiden mukaan huomattavasti toimivampi tapa estää ja ennaltaehkäistä kryptovaluutoilla tapahtuvaa rikollisuutta on lisätä kryptovaluuttojen sääntelyä. Huangin (2015) mukaan sääntelyä tulisi lisätä valtiollisella tasolla ja hän näkee varteenotettavimmaksi vaihtoehdoksi parantaa valtiovallan kryptovaluuttoihin keskittyvää syyttämisoimaa (subpoena power). Syyttämisoimalla Huang tarkoittaa virkavallan toimintaoikeuksien kasvattamista, jotta valtion toimijat voisivat paljastaa kryptovaluuttojen käyttäjien todellisen henkilöllisyyden ja viedä kryptovaluuttarikoksista epäillyt oikeuden eteen.

Kansallisen sääntelyn kehittäminen ainoana ratkaisukeinona on kyseenalainen. Hajautettuun luottoon perustuvia kryptovaluuttoja ei hallita yhdestä pisteestä, eivätkä ne tunne valtioiden tai talousalueiden rajoja, minkä takia Teichmann ja Falker (2020) pitävät paikallisen sääntelyn vaikutusta kryptovaluutoilla operoidun rikollisuuden estämisessä hyvin vähäisenä. Covolo (2020) arvioi kryptovaluutoilla tapahtuvaan

rikollisuuteen puuttumisen lepäävän pitkälti rajojen ylittävän sääntelijöiden, säännösten valvojien sekä virkavallan keskinäisen vahvan koordinaation ja yhteistyön varassa. Kryptovaroja koskevat regulatiiviset lähestymistavat eroavat Covolon mukaan paljon eri maiden, ja jopa Euroopan sisämarkkinoiden kesken. Kansallisten sääntelyiden erot voivat hankaloittaa kansainvälistä yhteistyötä, minkä takia Piazza (2017) ehdottaakin kansallisen sääntelyn lisäksi luotavan kansainvälisesti hyväksytyt standardit bitcoiniin ja sen kaltaisiin kryptovaluuttoihin liittyen.

Kryptovaluuttojen ja niillä toteutetun rikollisuuden sääntelyssä ongelmaksi muodostuu kryptovarojen jatkuva kehitys. Konkreettisen esimerkin antaa Covolo (2020), joka toteaa Euroopan Unionin tuoreen, vuonna 2018 säädetyin viidennen vastarahanpesudirektiivin olevan jo tietyiltä osin vanhentunut. Ratkaisu kryptovaluuttojen nopeaan kehitykseen löytyy Teichmannin ja Falkerin (2020) mukaan Liechtensteinista, jossa hallitus on luonut uuden laajakäsitteisen oikeudellisen kehyksen, jonka tulisi pysyä relevanttina kryptovaluuttojen kehityksestä huolimatta. Liechtensteinin TVTG-lain (Token- und VT-Dienstleister-Gesetz) suurimpana vahvuutena on se, ettei se keskity ainoastaan kryptovaluuttoihin, kuten valtaosa kryptovaroja koskevista laeista. Sen sijaan TVTG-laissa käytetään abstrakteja termejä viittaamaan lohkoketjupohjaisiin teknologioihin, jotka pitävät sisällään kryptovaluutat, kuitenkin rajoittumatta niihin. Näin toimimalla Liechtensteinin hallitus on onnistunut pitämään TVTG-lain ajankohtaisena ja luomaan pitkäkestoisen ratkaisun kryptovaluutoilla tapahtuvaan rikollisuuteen. Liechtensteinin lakia pidetään sopivana esimerkkinä standardoidun kansainvälisen sääntelyn pohjalle. (Teichmann & Falker, 2020.)

Hieman erilaisen lähestymistavan kryptovaluuttojen sääntelylle antavat Fletcher, Corbet ja Larkin (2021), jotka ehdottavat, että bitcoin klassifioitaisiin rahoituksellisia komponentteja omaavana teknologiana. Tämän pohjalta bitcoinia pitää säännellä osana kasvavaa rahoitusteknologian (financial technology; FinTech) toimialaa ja sääntely tulee tehdä pääsääntöisesti yksityisen sektorin yhtiöiden toimesta. Fletcher ym. ehdottavat sääntelijän rooliin World Wide Web Consortiumia (W3C), joka osapuoliltaan ja tehtävältään on tutkijoiden mukaan valmis sääntelijäksi. W3C on kansainvälinen monialayhtiö, jonka tehtävänä on luoda standardeja internetin

kehittämiseksi. Itse sääntely tapahtuu kolmiportaisen raamin mukaan, joka noudattaa yhteisiä standardeja ja parhaita toimintamalleja. Raamin alimmassa, ensimmäisessä luokassa ovat yksittäiset kryptovaluutan käyttäjät, joita säätelee raamin toinen luokka. Toinen luokka koostuu yhtiöistä, jotka tarjoavat bitcoinpalveluita, kuten bitcoinien myymistä, vaihtamista fiat-valuuttaan tai kolikoiden säilyttämistä. Loogisesti raamin toista luokkaa sääntelee puolestaan kolmas luokka. W3C edustaa kolmatta luokkaa, mikä toimii läheisessä yhteistyössä eri valtioiden sekä bitcoinyhtiöiden kanssa. Yhdessä W3C, valtiot ja bitcoinyhtiöt luovat tietyt standardit kryptovaluuttojen käyttäjien keskuuteen. Todellinen ratkaisu kryptovaluutoilla tapahtuvan rahanpesun ja terrorismin rahoittamisen estämiseksi esitetään olevan tämän raamin mukainen, alhaalta ylös suuntautunut monikansallinen sääntely. (Fletcher ym., 2021.)

Vaikka kansainvälinen sääntely kuulostaa ratkaisuna melko yksinkertaiselta, on todennäköisesti mahdotonta luoda sääntelyä, joka vastaa kaikkien maailman valtioiden intressejä. Ongelmaa kasvattavat entisestään valtiot, jotka ovat kriminalisoineet kryptovaluutat, kuten Saudi-Arabia ja nyt mahdollisesti Intia. Globaalia päätöksentekoa vaikeuttaa varmasti myös Kiina, joka yrittää luoda oman digitaalisen valuuttaansa (Teichmann & Fletcher, 2020). Kun valtiot kasvattavat viranomaisten toimintaoikeuksia ja kehittävät omia virtuaalivaluuttoja, herää huoli siitä, kuinka paljon kyseisellä toiminnalla ja teknologialla voidaan rajoittaa kansalaisten yksityisyyttä.

#### 4 JOHTOPÄÄTÖKSET

Tutkielman tavoitteena on selvittää kryptovaluuttojen rikollinen potentiaali ja miten mahdollinen kryptovaluuttarikollisuus uhkaa globaalia yhteiskuntaa. Tavoitteen havainnollistamiseksi tutkielmalle asetetaan päätutkimuskysymykset: *Miten kryptovaluutat mahdollistavat rikollisuutta ja kuinka suuri uhka siihen liittyy, sekä päätutkimuskysymystä tukevat apututkimuskysymykset: Kuinka merkittävä uhka kryptovaluutoilla tapahtuva rahanpesu on? Kuinka merkittävä uhka kryptovaluutoilla tapahtuva terrorismin rahoittaminen on? Kuinka paljon rikollisorganisaatiot voivat käytännössä hyödyntää kryptovaluuttoja? Miten kryptovaluuttojen mahdollistamaa rikollisuutta voidaan estää?*

Kryptovaluutat pohjautuvat lohkoketjuteknologiaan, mikä mahdollistaa käyttäjälleen pseudoanonymiteetin, eli salanimen luoman anonymiteetin. Käytännössä tämä tarkoittaa sitä, ettei kryptovaluuttalompakoiden omistajien tarvitse luovuttaa henkilökohtaista informaatiota saadakseen käyttää kryptovaluuttoja. Pseudonymiteetin lisäksi kryptovaluuttoja, kuten bitcoinia ei säädellä minkään virallisen tahon puolesta, joten niillä voi tehdä kauppaa yli valtioiden rajojen ilman verokustannuksia. Käyttäminen puolestaan vaatii vain digitaalisen avainparin, jolla saadaan kryptokolikon varat käyttöön, sekä toimivan internetyhteyden. Kaikki nämä piirteet yhdistettynä tekevät kryptovaluutoista houkuttelevan työkalun rikollisorganisaatioille.

Koska kryptovaluuttarikollisuutta ja yleisesti kyberrikollisuutta esiintyy todella useassa muodossa, tämä tutkielma käsittelee vain kahta merkittävintä kryptovaluuttoihin liitettyä rikollista toimintaa: modernia rahanpesua ja terrorismin rahoittamista. Rahanpesu on menetelmänä todella vanha ja se tarkoittaa rikollisin toimin hankittujen varojen integroimista yleiseen talousjärjestelmään siten, että ne näyttäisivät täysin laillisin keinoin ansaituilta. Perinteinen rahanpesuprosessi jaetaan yleensä kolmeen vaiheeseen: sijoittamiseen, kerrostamiseen ja integroimiseen. Modernissa rahanpesussa käytetään kryptovaluuttoja osana kahta ensimmäistä prosessin vaihetta. Niin sanotusta alkurikoksesta saadut rahat vaihdetaan kryptovaluutaksi, minkä jälkeen kryptovaroilla tehdään useita ostoksia ja vaihtoja.

Varat säilytetään joko kryptovaluuttoina, tai ne vaihdetaan sopivan ajan kuluttua takaisin fiat-valuutaksi.

Terrorismin rahoittaminen on toimintaa, jossa terroristijärjestöksi luokiteltu rikollisorganisaatio kerää varoja toimintansa edistämiseen ja ylläpitämiseen. Suurin kryptovaluuttojen suoma etu terroristiorganisaatioille liittyy järjestön saamiin lahjoituksiin. Useilla terroristijärjestöillä on paljon ulkomaisia, organisaation aatteita tukevia tai terroritekoja ihannoivia kannattajia, jotka tukevat taloudellisesti järjestöä. Kryptovaluuttojen takaaman pseudoanonymiteetin suojin tukijat voivat lähettää lahjoituksia pienemmällä kiinnijäämisen riskillä. Lisäksi kryptovaluuttojen vapaa liikkuvuus mahdollistaa varojen suoran ja todella nopean siirron.

Tutkijoilla ei ole yhteistä mielipidettä kryptovaluuttarikollisuuden uhasta. Koska kryptovaluutoilla tapahtuvasta rahanpesusta on jo näyttöä ja osan kehittyneimmistä terroristijärjestöistä tiedetään pyytävän tukijoiltaan lahjoituksia bitcoineina, osa tutkijoista kokee kryptovaluuttojen luovan akuutin uhan globaalille taloudelle ja kansalliselle turvallisuudelle. Toiset tutkijat puolestaan näkevät virtuaalivaluuttojen käytössä rikollisesta näkökulmasta liian monta heikkoutta, minkä takia kryptovaluuttarikollisuuden ajatellaan jäävän marginaaliseksi.

Lohkoketju kryptovaluuttojen takana luo monta rikolliselta kannalta positiivista piirrettä, mutta lohkoketjuteknologiaan liittyy myös rikollisille negatiivinen puoli. Kaikki kryptovaluutalla tehdyt transaktiot tallennetaan lohkoketjuun, minkä takia rikollisten tekemiksi epäiltyjä transaktioketjuja voidaan jäljittää aina kryptovaluutan fiat-valuutaksi vaihtaneeseen kryptovaluuttapörssiin asti. Vaikka virtuaalivaluutan käyttäjät voivat piiloutua salanimen taakse, on kryptovaluuttarikollisuutta tutkivalla virkavallalla mahdollisuus seurata transaktioketjua ja mahdollisesti yhdistää lompakon omistaja tapahtuneeseen rikokseen. Tämän kaltaista mahdollisuutta ei esiinny käteisessä valuutassa. Käteisellä on aina tehty, ja tullaan varmasti aina tekemään rikoksia, joten se käsittely ei vaadi rikollisorganisaatioilta tietoteknistä osaamista tai uuden oppimista. Verrattaessa käteisen mahdollistamaan rikollisuuteen, on kryptovaluuttarikollisuuden uhka varsin suhteellinen.

Vaikka tutkijoilla ei ole yhtenäistä mielipidettä kryptovaluuttarikollisuuden merkittävyydestä tällä hetkellä, yhdistää tutkijoiden ajatuksia mahdollisuus uudesta kryptovaluutasta. Uusia kryptovaluuttoja syntyy jatkuvasti lisää ja ne pyrkivät kehittymään aina edellistä paremmiksi. On siis mahdollista, että kehitetään uusi kryptovaluutta, joka sopii täydellisesti rikollisten käyttötarkoituksiin ja välillisesti uhkaa globaalia taloutta ja turvallisuutta. Tutkijat ovat samaa mieltä siitä, että kryptovaluuttojen käyttöön tulee puuttua vielä, kun se on mahdollista.

Kryptovaluuttarikollisuuteen puuttumiseen nähdään parhaana keinona kansainväliset standardit, jotka keskittyvät lohkoketjuteknologiaa käyttävien sovellusten rajoittamiseen. Kohdistamalla sääntely juuri lohkoketjuteknologiaan, vältetään luomasta uusia lakeja tai regulaatioita, jotka vanhentuvat heti uuden kryptovaluutan julkaisemishetkellä. Lisäksi uutena ratkaisuehdotuksena on annettu kolmiportainen malli, jossa kryptovaluuttojen yksityisiä käyttäjiä sääntelevät kryptovaluuttayhtiöt, kuten kryptovaluuttapörssit, ja yhtiöitä puolestaan sääntelee kansainvälinen internetyhtiöiden yhteenliittymä W3C (World Wide Web Consortium) läheisessä yhteistyössä valtioiden kanssa. Kryptovaluuttarikollisuuden tutkimisessa, syyttämisessä ja ennaltaehkäisemisessä tärkeimmät tekijät ovat eri valtioiden sekä valtion alaisten toimijoiden välinen tiivis yhteistyö.

Vaikka tutkielma onnistuu vastaamaan asetettuihin tutkimuskysymyksiin tutkielman tavoitteiden mukaisesti, on kryptovaluuttarikollisuuden saralla vielä paljon mahdollisuuksia jatkotutkimukselle. Mielenkiintoista on esimerkiksi nähdä, saako Intia asetettua kryptovaluutat kriminalisoivan lain ja miten tämä laki vaikuttaisi kryptovaluuttojen käyttöön Intiassa. Toinen jatkotutkimuskohde voisi liittyä Kiinan julkaisemaan digitaaliseen Yuaniin. On huolestuttavaa ajatella tilannetta, jossa Kiinan kaltaisessa valtiossa yleiseksi valuutaksi otettaisiin lohkoketjuteknologiaan perustuva digitaalinen raha, mikä käytännössä mahdollistaisi valtiolla jokaisen kansalaisen tekemien transaktioiden seuraamisen. Tutkimus voisi käsitellä juuri kryptovaluuttojen yleistymisen vaikutuksia ihmisten yksityisyyteen.

## LÄHTEET

- Albrecht, C., Duffin, K. M., Hawkins, S. & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, 22(2), 210–216. Doi:10.1108/JMLC-12-2017-0074
- Albrecht, M. (2018). Bitcoinin perusteet. *Haaste: Asiantuntevasti Rikoksentsorjunnasta ja Kriminaalipolitiikasta*, 18(2), 46–47. Haettu osoitteesta <https://www.haaste.om.fi/fi/index/lehtiarkisto/haaste22018/bitcoininperusteet.html>
- Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. Sebastopol, CA: O'Reilly Media, Inc.
- Brantly, A. (2014). Financing terror bit by bit. *CTC Sentinel*, 7(10), 1–5. Haettu osoitteesta <https://ctc.usma.edu/wp-content/uploads/2014/10/CTCSentinel-Vol7Iss105.pdf>
- Brenig, C., Accorsi, R. & Müller, G. Economic analysis of cryptocurrency backed money laundering. Esitetty konferenssissa 23rd European Conference on Information Systems, ECIS 2015. Doi: 10.18151/7217279
- Buchanan, B. (2004). Money laundering - A global obstacle. *Research in International Business and Finance*, 18(1), 115–127. Doi:10.1016/j.ribaf.2004.02.001
- Casey, M., Crane, J., Gensler, G., Johnson, S. & Narula, N. (2018). The impact of blockchain technology on finance: A catalyst for change. *Geneva Reports on the World Economy*, 21. Haettu osoitteesta <https://www.sipotra.it/old/wp-content/uploads/2018/07/The-Impact-of-Blockchain-Technology-on-Finance-A-Catalyst-for-Change.pdf>
- Coin.dance. (2021). *Cryptocurrencies by Market Cap Summary*. Haettu osoitteesta <https://coin.dance/stats/marketcaptoday>
- Coinmarketcap.com. (2021). *All Cryptocurrencies*. Haettu osoitteesta <https://coinmarketcap.com/all/views/all/>
- Covolo, V. (2020). The EU response to criminal misuse of cryptocurrencies: The young, already outdated 5th anti-money laundering directive. *European Journal of Crime, Criminal Law & Criminal Justice*, 28(3), 217–251. Doi:10.1163/15718174-bja10003

- Delikanli, İ. U., & Vogiazas, S. (2018). Testing for the presence of speculative price bubbles in bitcoin. *Istanbul Commerce University Journal of Social Sciences*, 17(33), 511–523. Haettu osoitteesta <https://www-proquest-com.pc124152.oulu.fi:9443/docview/2068437967/fulltextPDF/510F1B5C7F8A449BPQ/1?accountid=13031>
- Dion-Schwarz, C., Manheim, D. & Johnston, P. B. (2019). *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Santa Monica, CA: Rand Corporation.
- Europol (2015). *Why is cash still a king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*. Haettu osoitteesta <https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering>
- Fanusie, Y. J. & Robinson, T. (2018). Bitcoin laundering: An analysis of illicit flows into digital currency services. *Center on Sanctions and Illicit Finance memorandum, January*. Haettu osoitteesta [https://www.fdd.org/wp-content/uploads/2018/01/MEMO\\_Bitcoin\\_Laundering.pdf](https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf)
- Fletcher, E., Larkin, C. & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, 56. Doi: 10.1016/j.ribaf.2021.101387
- Foley, S., Karlsen, J. R. & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies*, 32(5), 1798–1853. Doi:10.1093/rfs/hhz015
- Freeman, M. & Ruehsen, M. (2013). Terrorism financing methods: An overview. *Perspectives on Terrorism*, 7(4), 5–26. Haettu osoitteesta <http://www.jstor.org/stable/26296981>
- Furneaux, N. (2018). *Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence*. Indianapolis, IN: John Wiley & Sons.
- Gilmour, N. (2016). Understanding the practices behind money laundering - A rational choice interpretation. *International Journal of Law, Crime and Justice*, 44, 1–13. Doi:10.1016/j.ijlcj.2015.03.002
- Irwin, A. S. M. & Milad, G. (2016). The Use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*, 19(4), 407–425. Doi:10.1108/JMLC-01-2016-0003

- Kethineni, S., Cao, Y. & Dodge, C. (2018). Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes. *American Journal of Criminal Justice: AJCJ*, 43(2), 141–157. Doi:10.1007/s12103-017-9394-6
- Kfir, I. (2020). Cryptocurrencies, national security, crime and terrorism. *Comparative Strategy*, 39(2), 113–127. Doi:10.1080/01495933.2020.1718983
- Kuo Chuen, D. L., Guo, L. & Wang, Y. (2018). Cryptocurrency: A new investment opportunity? *The Journal of Alternative Investments*, 20(3), 16–40. Doi:10.3905/jai.2018.20.3.016
- Levi, M. (2002). Money laundering and its regulation. *The Annals of the American Academy of Political and Social Science*, 582(1), 181–194. Doi:10.1177/000271620258200113
- Mabunda, S. (2018). (2018). Cryptocurrency: The new face of cyber money laundering. Esitetty konferenssissa 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, icABCD 2018, Doi:10.1109/ICABCD.2018.8465467
- Moore, D. & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival*, 58(1), 7–38. Doi:10.1080/00396338.2016.1142085
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Haettu osoitteesta <https://bitcoin.org/bitcoin.pdf>
- Oftedal, E. (2015). The financing of jihadi terrorist cells in Europe. Norwegian Defence Research Establishment (FFI). Haettu osoitteesta <https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/1103/14-02234.pdf?sequence=1&isAllowed=y>
- O'Sullivan, A. (2018). Ungoverned or anti-governance? How bitcoin threatens the future of western institutions. *Journal of International Affairs*, 71(2), 90–102. Haettu osoitteesta <https://www.jstor.org/stable/26552331>
- Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G. & Herrera-Joancomartí, J. (2019). Double-spending prevention for bitcoin zero-confirmation transactions. *International Journal of Information Security*, 18(4), 451–463. Doi:10.1007/s10207-018-0422-4

- Piazza, F. (2017). Bitcoin in the dark web: A shadow over banking secrecy and a call for global response. *Southern California Interdisciplinary Law Journal*, 26(3), 521–546. Haettu osoitteesta <http://web.a.ebscohost.com/pc124152.oulu.fi:8080/ehost/detail/detail?vid=0&sid=23208116-c255-4011-84eb-b350b1d8722d%40sessionmgr4008&bdata=JnNpdGU9ZWZWhvc3QtbGl2ZQ%3d%3d#db=asn&AN=123824519>
- Reynolds, P. & Irwin, A. S. M. (2017). Tracking digital footprints: anonymity within the bitcoin system. *Journal of Money Laundering Control*, 20(2), 172–189. Doi:10.1108/JMLC-07-2016-0027
- Teichmann, F. M. J. & Falker, M. (2020). Cryptocurrencies and financial crime: Solutions from Liechtenstein. *Journal of Money Laundering Control*, painossa. Doi:10.1108/JMLC-05-2020-0060
- Teichmann, F. M. J. (2018). Financing terrorism through cryptocurrencies – a danger for Europe? *Journal of Money Laundering Control*, 21(4), 513–519. Doi:10.1108/JMLC-06-2017-0024
- van Wegberg, R., Oerlemans, J. & van Deventer, O. (2018). Bitcoin money laundering: Mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419–435. Doi:10.1108/JFC-11-2016-0067