

Timothy Korhonen

**LOHKOKETJUTEKNOLOGIAAN PERUSTUVIEN VA-
LUUTTOJEN MUODOSTAMAT SISÄISET JA ULKOI-
SET UHAT**



JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Korhonen, Timothy

Lohkoketjuteknologiaan perustuvien valuuttojen muodostamat sisäiset ja ulkoiset uhat

Jyväskylä: Jyväskylän yliopisto, 2022, 32 s.

Tietojärjestelmätiede, Kandidaatintutkielma

Ohjaaja(t): Kyppö, Jorma

Lohkoketjuteknologioihin perustuvat valuutat, kuten Bitcoin ovat viimeisten vuosien aikana kasvattaneet medianäkyvyyttä ja olleet esillä usein esillä. Tämän kirjallisuuskatsauksen tarkoituksena on käydä läpi kryptovaluuttojen negatiivisia piirteitä ja niiden ominaisuuksista johtuvia sisäisiä ja ulkoisia uhkia yhteiskunnalle. Tutkielmassa selvitetään lähdekirjallisuuden avulla eri syitä, miksi kryptovaluutat houkuttelevat rikollista ja terroristista toimijoita ottamaan käyttöön näitä valuuttoja. Tutkielmassa käy ilmi, että kryptovaluuttojen anonymitetin mahdollistava, välikäsiä tarvitsematon ja paikka- ja aikariippumaton järjestelmä on suosinut sen käyttöönottoa järjestäytyneen rikollisuuden maksuvälineenä toimimisena pimeässä verkossa. Kryptovaluuttoja on myös käytetty rahanpesussa ja terroristisen toiminnan rahoittamisessa. Tutkielmassa käy ilmi, että kryptovaluutat eivät ole ohittaneet perinteistä käteistä rikollisessa toiminnassa mutta tilanne on nopeasti muuttuva ja tulevaisuudessa tilanne todennäköisesti muuttuu ja monet asiantuntijat ovat sitä mieltä, että kryptovaluuttojen rooli rahanpesussa, ja terrorismin rahoituksessa tulee kasvamaan. Tämän vuoksi aihe vaatii lisätutkimusta, jotta eri organisaatiot, ihmiset ja viranomaiset pystyvät kehittämään keinoja, joilla tämän muodon rikollisuutta voidaan torjua. Alan asiantuntijat ajattelevat, että viranomaisten täytyy kehittää eri mekanismeja tiedonjaolle ja yhteistyölle, sekä valtioiden täytyisi yhtenäistää kryptovaluuttoihin liittyvää lainsäädäntöä, jotta rajoja ylittävää rikollisuutta, rahanpesua ja terrorismia voidaan ennaltaehkäistä.

Asiasanat: Lohkoketjut, kryptovaluutat, rikollisuus, terrorismi, Bitcoin.

ABSTRACT

Korhonen, Timothy

Internal and external threats created to society by currencies based on blockchain technology

Jyväskylä: University of Jyväskylä, 2022, 32 pp.

Information systems, Bachelor's Thesis)

Supervisor(s): Kyppö, Jorma

Currencies based on blockchain technology, such as Bitcoin, have in recent years been a topic of a lot of conversation in the media. The purpose of this literature review is to bring forth the negative sides of cryptocurrencies, and the reasons why they might create threats to society. In this literature review, with the help of prior studies, we search for reasons, why qualities of cryptocurrencies attract organized crime and terrorism. In the literature review, we found out, that the system, which favours anonymity, does not require intermediaries, such as banks and is independent of place and time, has been the key reasons why organized crime has implemented cryptocurrencies as a means of payment in the dark web. Cryptocurrencies have also been used in money laundering and financing terrorism. At this point in time "Cash is still king" when it comes to organized crime and terrorism, but the situation is ever evolving and there is a consensus that the role of cryptocurrencies will grow among the different elements of crime. Therefore, the topic requires more research, so that different organizations, people, and authorities can develop means of preventing this form of crime. The sources used in the literature review agree that authorities need to develop different mechanisms for information sharing and cooperation and governments need to unify their legislation regarding cryptocurrencies, in order to prevent organized cross-border crime, money laundering and terrorism.

Keywords: Blockchain, Cryptocurrencies, Crime, Terrorism, Bitcoin.

KUVIOT

Kuva 1 Lohkoketjun arkitehtuuri esitettynä pelkistetyksi	10
Kuva 2 Bitcoin maksutapahtumat vuodesta 2009-2021	11
Kuva 3 Pankkien toiminta välikätenä.....	12
Kuva 4 Swift-järjestelmä pelkistettynä	12
Kuva 5 Rahanpesun prosessi	17

TAULUKOT

Taulukko 1 Tunnetuimpia terroristisia järjestöjä.....	19
---	----

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

KUVIOT JA TAULUKOT

1	JOHDANTO.....	6
2	KRYPTOVALUUTAT JA LOHKOKETJUT SELITETTYNÄ	8
	2.1 Lohkoketjut.....	8
	2.2 Kryptovaluutat.....	10
3	KRYPTOVALUUTTOJEN MAHDOLLINEN KÄYTTÖ RIKOLLISESSA JA TERRORISTISESSA TOIMINNASSA	15
	3.1 Kryptovaluutat erilaisessa rikollisuudessa	15
	3.2 Kryptovaluutat ja terrorismi	18
4	LOHKOKETJUTEKNOLOGIAAN PERUSTUVIEN VALUUTTOJEN KÄYTTÖ NYKYPÄIVÄNÄ RIKOLLISESSA JA TERRORISTISESSA TOIMINNASSA, SEKÄ UHKIEN ESTÄMINEN	21
	4.1 Kryptovaluuttojen käyttö erilaisissa rikollisuuden muodoissa nykypäivänä	21
	4.2 Kryptovaluuttojen käyttö terroristisessa toiminnassa	23
	4.3 Tekijät, jotka heikentävät kryptovaluuttojen omaksumista	24
	4.4 Kryptovaluuttauhkien torjuminen ja ennaltaehkäiseminen	24
5	JOHTOPÄÄTÖKSET	27
	LÄHTEET	30

1 JOHDANTO

Viimeisten vuosien aikana lohkoketjuteknologiaan perustuvat valuutat, kuten Bitcoin ja Ethereum ovat olleet sekä suursijoittajien, että piensijoittajien kiinnostuksen kohteena, sekä valuutat ovat myös herättäneet kiinnostusta tavallisissa ihmisissä. Nämä lohkoketjuteknologiaan perustuvat valuutat ovat usein ylittäneet uutiskynnyksen, mutta näistä teknologioista usein puhutaan artikkeleissa vain positiiviseen sävyyn ja niiden tuomasta mahdollisuudesta rikastua nopeasti. Uutisissa kerrotaan usein virtuaalivaluuttojen suuresta arvon noususta tai laskusta eli volatilitteetistä. Tämän takia tavallinen piensijoittaja tai muuten valuutasta kiinnostunut ei välttämättä tunnistaakaan kryptovaluuttojen muita piirteitä ja käyttömahdollisuuksia, sekä mahdollisia riskejä ja uhkia.

Kryptovaluuttoihin liittyy kuitenkin riskejä ja uhkia, sillä kyseiset valuutat mahdollistavat käyttäjien identiteetin salaamisen ja viranomais sääntely ei ole ulottunut näihin vielä. Tämä mahdollistaa erilaista rikollista toimintaa, joka ylittää helposti valtioiden rajoja, joka taas houkuttelee siirtämään rikollista toimintaa, kuten rahanpesua ja terrorismin rahoitusta kryptomaailmaan.

Tutkielmassa tarkastellaan lohkoketjuteknologiaan perustuvien valuuttojen luomia sisäisiä ja ulkoisia uhkia yhteiskunnalle ja tutkielmassa keskitytään etenkin erilaisen rikollisuuden ja terrorismin rahoituksen näkökulmaan, sekä tutkitaan miten lohkoketjuteknologiaan perustuvat valuutat mahdollistavat ja helpottavat erilaista rikollista toimintaa. Tutkielmassa käydään läpi yleisesti kryptovaluuttoja mutta keskitytään etenkin Bitcoinin, sekä sen vaikutusta erilaisiin rikollisuuden muotoihin ja terrorismin rahoitukseen, sillä kyseinen valuutta on tunnetuin ja markkina-arvoltaan suurin. Tämän takia kyseisestä valuutasta on kertynyt myös eniten tietoa ja tutkimusta, jota voidaan tässä tutkielmassa käyttää hyväksi.

Johtuen kryptovaluuttojen suuresta suosiosta, jatkuvasta medianäkyvyydestä, sekä suuresta varallisuudesta, joka liikkuu kryptomaailmassa, on aihe erittäin ajankohtainen. Aiheesta riittää verran tutkimusta, josta on

kirjoitettu positiiviseen sävyyn mutta tämän vuoksi tämän tutkielman tarkoituksena on tuoda esille näiden teknologioiden muodostamia sisäisiä ja ulkoisia uhkia yhteiskunnalle ja tarkastella aihetta hieman erilaisesta näkökulmasta.

Tutkielmassa tavoitteena on tutustuttaa lukija lohkoketjuihin ja niihin perustuviin valuuttoihin ja tämän jälkeen auttaa lukijaa ymmärtämään, miksi kyseiset valuutat saattavat aiheuttaa erilaisia riskejä ja uhkia yhteiskunnalle. Tämän jälkeen avataan syitä, jotka kryptovaluuttojen ominaisuuksista johtuen saattavat houkutella erilaista järjestäytyntä rikollisuutta ja terroristista toimintaa ottamaan näitä valuuttoja käyttöön. Tutkielmassa käydään myös läpi, miten mahdollisesti näitä uhkia voidaan torjua kansallisella ja kansainvälisellä näkökulmalla.

Tutkimuskysymykset, joihin tässä pyrin vastaamaan ovat:

- Minkälaisia sisäisiä ja ulkoisia uhkia lohkoketjuteknologiaan perustuvat valuutat muodostavat yhteiskunnalle?
- Miten Kryptovaluuttoihin perustuvaa rikollisuutta ja terrorismia voidaan torjua?

Tutkielma tehdään kirjallisuuskatsauksena, jossa tarkastellaan olemassa olevaa kirjallisuutta ja pyritään niiden avulla vastaamaan tässä mainittuihin tutkimuskysymyksiin. Lähteitä pyritään käyttämään laajasti eri tietokannoista, kuten Google Scholar, JYKDOK ja Scopus. Tutkielma on jaettu kolmeen pääosaan, jossa ensimmäisessä osassa avataan yleisesti lohkoketjuteknologiaa ja tähän teknologiaan perustuvia valuuttoja. Ensimmäisessä kappaleessa käydään läpi määritelmät; kryptovaluutat ja lohkoketjuteknologia. Tässä lukijalle selviää, miksi valuutat mahdollisesti pystyvät vaikuttamaan rikolliseen ja terroristiseen toimintaan.

Toisessa osiossa käydään läpi tekijät, jotka houkuttelevat rikollisia ja terroristisia toimijoita käyttämään näitä teknologioita. Tarkoituksena on muodostaa lukijalle yleinen käsitys lohkoketjuista ja niiden mahdollisista riskeistä yhteiskunnalle. Kappaleessa avataan myös mitä erilaisia käyttökohteita, kuten eri rikollisuuden muotoja on, joihin lohkoketjuteknologiaan perustuvat valuutat pystyvät vaikuttamaan.

Kolmannessa pääluvussa käydään läpi tilannetta nykypäivänä ja tarkastellaan, miten kryptovaluuttojen käyttö on ilmennyt eri rikollisuuden muodoissa, kuten järjestäytyneessä rikollisuudessa, rahanpesussa ja terrorismin rahoituksessa. aihetta, miten tulevaisuudessa tilanne saattaa muuttua ja minkälaisilla kansallisilla ja kansainvälisillä keinoilla viranomaiset ja valtiot voivat puuttua kryptovaluutoilla tehtävään rikollistoimintaan. Viimeisessä osiossa tarkastellaan, miten tutkimuskysymyksiin on vastattu, sekä mitä tutkielmassa on käyty läpi. Viimeisenä tuodaan esille mahdollisia jatkotutkimusaiheita.

2 KRYPTOVALUUTAT JA LOHKOKETJUT SELITETTYNÄ

Tämän luvun tarkoitus on esitellä lohkoketjuteknologioihin perustuvia valuuttoja, ja tässä tutkielmassa pääteemana käsitellään Bitcoinia mutta sivutaan välillä muita myös valuuttoja. Tässä aukaistaan käsite lohkoketjut, joiden ymmärtäminen on tärkeää, jotta lukija saa käsityksen syistä, jotka vaikuttavat niiden omaksumiseen rikollisessa ja terroristisessa toiminnassa.

2.1 Lohkoketjut

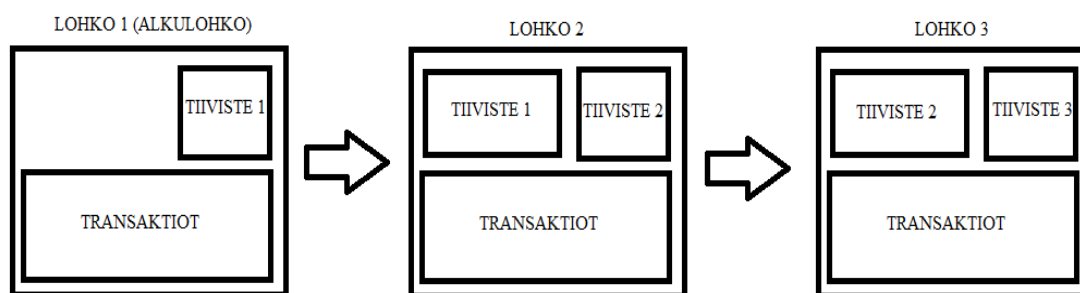
Lohkoketjut ovat kehitetty Satoshi Nakamoton toimesta Bitcoinia varten. Nakamoto (2008). Nakamoton luoma vertaisverkkoon perustuva tilikirja (distributed ledger) eli lohkoketju perustuu peräkkäisiin lohkoihin, jotka ovat sidottu toisiinsa ja uusin louhittu lohko siirretään ketjun pätyyn. Tällä Nakamoto ratkaisi haasteen, joka vaivaa virtuaalivaluuttoja, eli kahdesti käyttämisen ongelma (double spending problem). Tämä johtuu siitä, että virtuaalivaihdanta ei tarvitse kolmatta osapuolta, kuten pankkia, joka varmistaa vaihdannanvälineen käypäisyyden ja tästä voi syntyä riski, että vaihdetun valuutan yksikkö on jo käytetty. (Pérez-Solà, Delgado-Segura, Navarro-Arribas. 2019). On hyvä huomioida, että Satoshi Nakamotosta ei tiedetä juuri mitään, edes sitä, onko kyseessä yksi henkilö vai useampia. Nakamoto on pysynyt poissa julkisuudesta suurimmaksi osin. (Kuo Chuen ym, 2018).

Lohkoketjuihin kohdistuu paljon odotuksia tällä hetkellä, ja nämä ovatkin julkisuudessa usein esillä. Keskustelu kryptovaluutoista nousee ensimmäiseksi mieleen puhuttaessa lohkoketjuista mutta yleistyvässä määrin on alettu puhua itse teknologiasta kryptovaluuttojen takana. Lohkoketjut tarjoavat useita käyttömahdollisuuksia, sekä potentiaalista hyötyä eri aloille johtuen sen ominaispiirteistä. Näistä piirteistä tärkein on se, että toimijat voivat tuottaa ja ylläpitää tietokantoja hajautetusti. (Leible, S. Schlager, S. Schubotz, M. Gipp, B. 2019).

Nämä teknologiat tunnetaan parhaiten siitä, että ne mahdollistavat rahan vaihdon ilman välikäsiä. (Sasson, B, et al. 2014). Tunnetuimmat esimerkit ovat kryptovaluutat mutta suurenevissa määrin on julkisuudessa puhuttu lohkoketjujen käyttämisestä muillakin aloilla. Koska lohkoketjut poistavat tarpeen välikäsille, on mahdollista, että useat alat hyötyisivät ja pystyisivät lisäämään tehokkuutta omassa toiminnassa. (Smith & Castonguay, 2020). Aloja, joista on puhuttu pystyvän hyödyntämään lohkoketjuja, ovat esimerkiksi lääketiede, finanssiala, sekä julkinen sektori.

Lohkoketjuista puhuessa on hyvä ymmärtää käsite lohko. Tällä tarkoitetaan datapakettia, jonka sisällä on jonkun tapahtuman tieto. Tapahtuman ei tarvitse olla rahallinen transaktio vaan, vaan se voi sisältää esimerkiksi jonkun yrityksen muuta dataa. (Dai & Vahary, 2017, 9). Lohkossa tärkeimpinä tietoina pidetään tapahtumien tietoja, lohkon tiivistettä, ja aikaisemman lohkon tiivisteitä. (Zheng, Xie, Dai, Chen & Wang, 2017). Kun verkoston enemmistö solmuista (node) on varmentanut lohkon, hyväksytetään se lopulle verkostolle, jonka jälkeen lohko liitetään ketjuun ja näin muodostaen lohkoketjun. (Nakamoto, 2008). Tätä prosessia kutsutaan työntodistejärjestelmäksi (proof-of-work-system) ja verkoston enemmistöllä tarkoitetaan vertaisverkossa sijaitsevaa tietokonetta, joka pystyy äänestämään lohkon hyväksymisestä kerran yhtä suoritinta kohti. Turvallisuutta lisää se, että, mitä pidempi lohkojono on, sen vaikeampaa järjestelmää on manipuloida, sillä tämä vaatisi niin suuren suorituskehon, sekä energiatarpeen, jonka vuoksi se on melkein mahdotonta. Nakamoto. (2008). Tätä prosessia, jossa transaktioita niputetaan yhteen ja varmistetaan todeksi, kutsutaan louhimiseksi. (mining) (Nakamoto, 2008.)

Lohkoketjujen turvallisuuteen liittyen toinen tärkeä käsite tiiviste, eli hajautusarvo on olennainen osa lohkon todentamista. B. Scheier (1994) määrittelee hajautusfunktion seuraavasti; Hajautusfunktio on matemaattinen tai muu funktio, jonka syöte on vaihtuvamerkkinen merkkijono ja jonka tarkoituksena on tuottaa kiinteämittaisen tiiviste. Jotta hajautusfunktio olisi hyvä, tulisi tilanteen, jossa kaksi syötettä tuottaa saman tiiviste. Olla erittäin epätodennäköinen. Hajautusfunktion hyödyllisyyteen vaikuttaa myös, että se on yksisuuntainen. Tällä tarkoitetaan sitä, että syötteestä on helppo laskea tiiviste mutta tiivisteestä on erittäin vaikea laskea syöte. Hajautusfunktiolla varmistetaan tiedon eheys ja sillä voidaan tarkastaa dataa siten, että lasketaan tiiviste käsillä olevasta tiedosta ja verrataan sitä aiemmin tallennettuun tiivisteeseen. Jos nämä eroavat toisistaan, on varmaa, että dataa on muokattu tai alkuperäistä tiivistettä on muutettu. Jos taas tiivisteet ovat hyvin samankaltaiset, on todennäköistä, että alkuperäinen tiiviste ja uusi tieto on yhteneväistä. (Scheier, B. 1994)



Kuva 1 Lohkoketjun arkkitehtuuri esitettynä pelkistetyksi. (Nakamoto 2008, 3) ja (Zheng ym. 2017, 558)

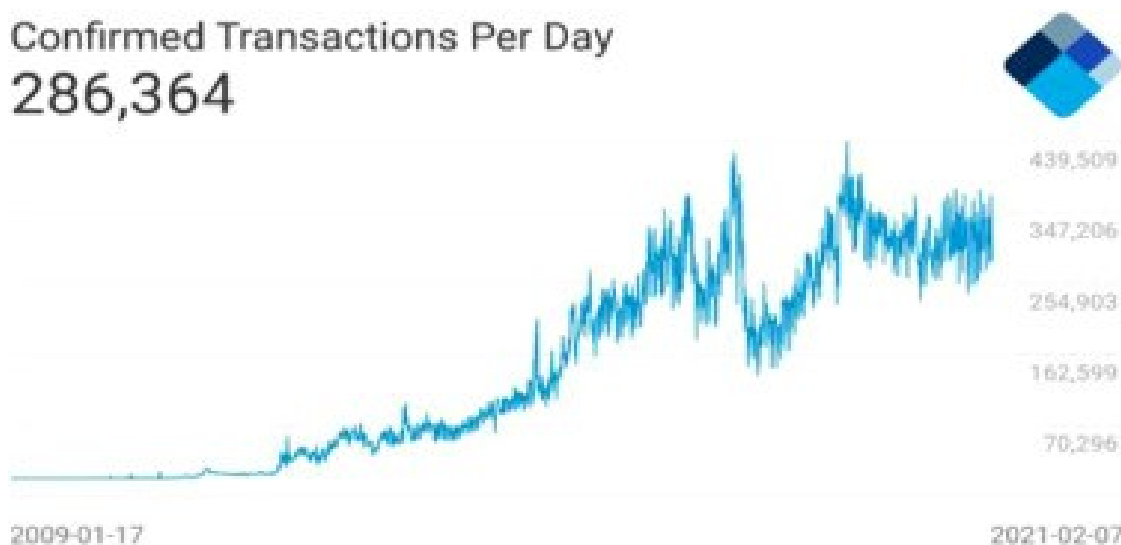
Kuviossa 1 kuvataan lohkoketju pelkistetyksi. Kuviossa on kolme kohtaa, joista jokaisessa löytyy tieto transaktiosta, sekä aikaisempien lohkojen tiivistetiedot. Teoriassa tiivisteiden avulla voidaan seurata transaktioiden ketjua alkulohkoon saakka.

2.2 Kryptovaluutat

Kryptovaluutat ovat hajautettuja virtuaalisia valuuttoja, jotka perustuvat kryptografiaan. Kryptografia suoraan suomennettuna antiikin kreikasta; Kryptós ”salainen” ja graphein ”kirjoitus” tai salakirjoitus. Tähän mennessä jokaisen kryptovaluutan on kehittänyt yksityinen henkilö, organisaatio tai yritys ja kryptovaluutat eivät ole lunastettavissa tavallisiin valuuttoihin, tai arvomineraaleihin, kuten kultaan tai hopeaan, samoin kuin perinteiset valuutat. White, L, W. (2015). Ensimmäinen kryptovaluutta on kehitetty Satoshi Nakamoton toimesta vuonna 2009. Vijayalakshmi, J & Murugan, A. (2017). Tällä hetkellä markkinoilla on yli 10 000 lohkoketjuteknologiaan perustuvaa kryptovaluutta coinmarketcap-nimisen internetsivun mukaan.

Vuonna 2008 tapahtuneen finanssikriisin takia luottamus laski merkittävästi finanssi- ja pankkisektoria kohtaan ja tämän on uskottu vaikuttaneen Satoshi Nakamoton innostukseen kehittää valuutta, jota ei valvo valtio, tai pankit ja joka perustuu lohkoketjuihin. (Kuo Chuen, Guo & Wang, 2018). On hyvä huomioda, että kryptovaluutat ja virtuaalivaluutat eivät ole sama asia, sillä kryptovaluutat eivät tarvitse kolmatta osapuolta, joka on näitä valuuttoja yhdistävä tekijä. Kolmas osapuoli on korvattu kryptografisella todisteella. (Nakamoto. 2008). Tällä hetkellä suurin osa internetissä tapahtuvista maksutapahtumista toimivat perinteisellä elektronisella maksamisella, jossa on kolmas osapuoli välikätenä.

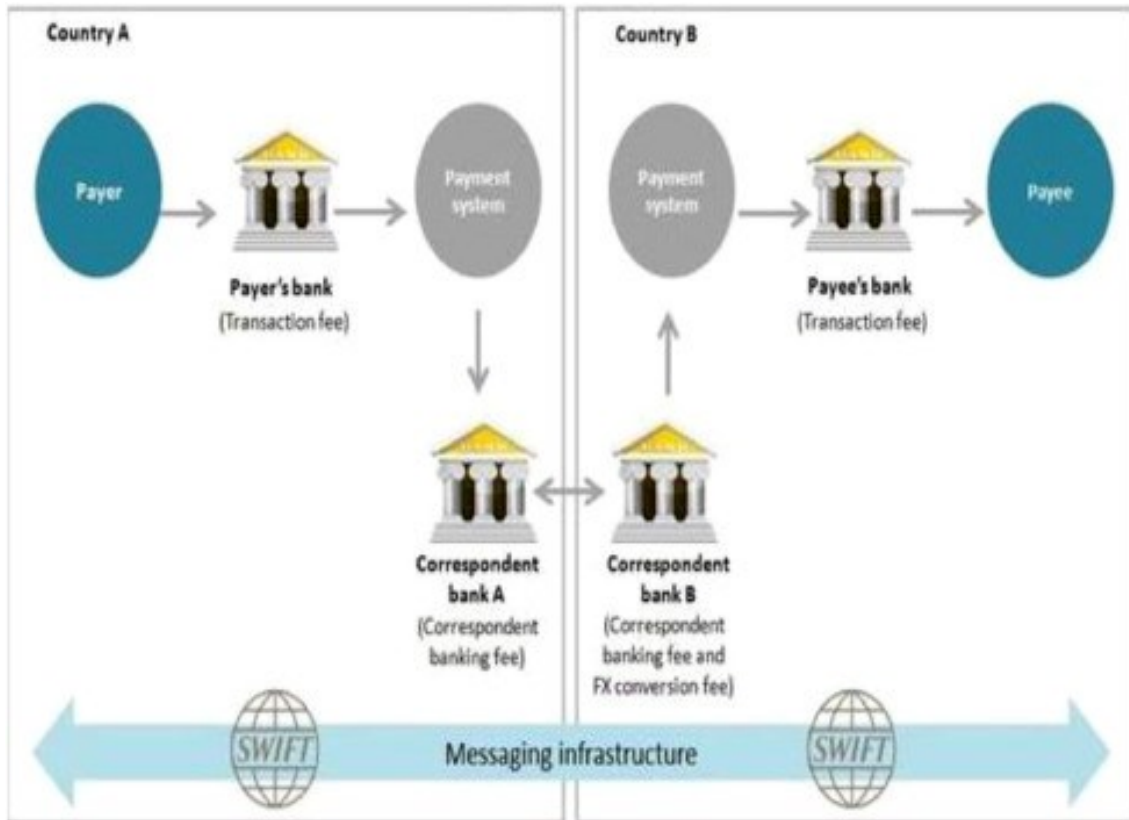
Confirmed Transactions Per Day 286,364



Kuva 2 Bitcoin maksutapahtumat vuodesta 2009–2021

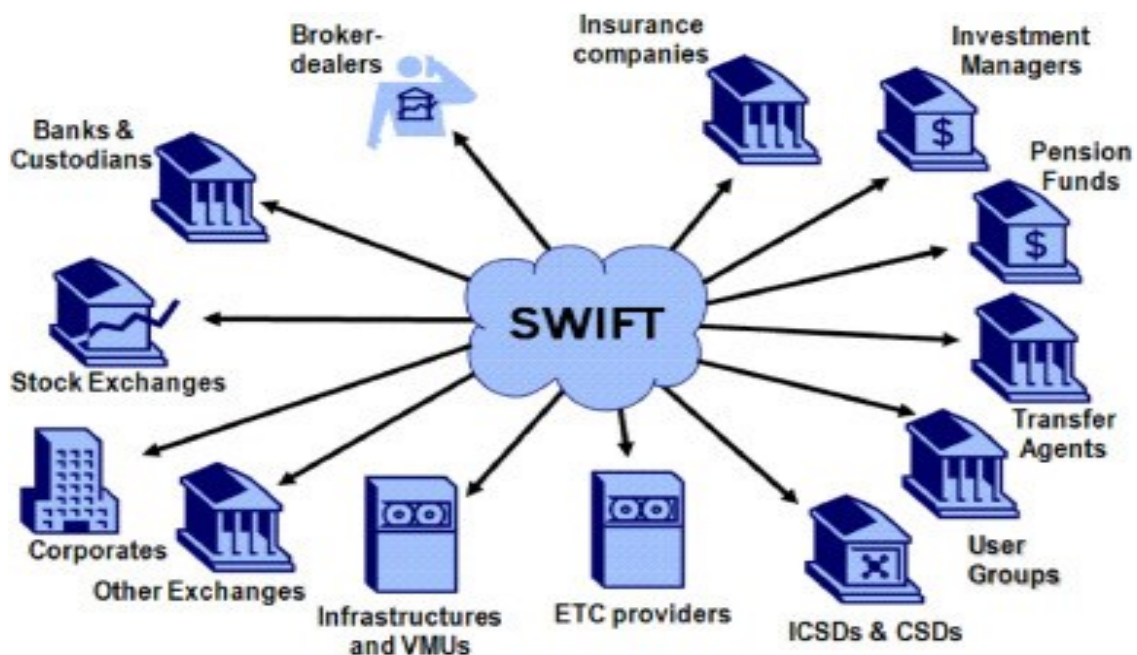
Kuviossa osoitetaan varmistetut päivittäiset Bitcoinin maksutapahtumat vuodesta 2009, vuoteen 2021. Vuodesta 2014 vuoteen 2021 Bitcoinin maksutapahtumat yli kuusinkertaistuivat. On hyvä huomioda, että kuvassa näytetään vain varmistetut tapahtumat. Todellisuudessa niitä on todennäköisesti huomattavasti enemmän. Gowda, N & Chakravorty, C. (2021).

Nämä välikädet ovat yleisesti luottamusta nauttivia rahoituslaitoksia ja näiden kolmansien osapuolien tehtävinä on varmistaa osapuolten luotot, sekä valuutan käypäisyys. (Casey, Crane, Gensler, Johnson & Narula, 2018). Tästä toiminnasta kolmannet osapuolet perivät palkkion, joka kasvattaa maksutapahtumien kustannuksia. Tämä taas pienentää pienien maksutapahtumien kannattavuutta. Nakamoto (2008) mukaan lohkoketjuihin perustuvilla kryptovaluutoilla on tässä hyvä mahdollisuus korvata perinteiset elektroniset maksutapahtumat, sillä näissä ei ole vastaavan kaltaisia palkkiokustannuksia, jotka nostavat etenkin pienten maksutapahtumien kustannuksia merkittävästi. Seuraavissa kuvioissa näytetään, pelkistetysti, miten Swift-järjestelmässä olevat rahoituslaitokset toimivat maksutapahtumissa välikäsinä, ja perivät näistä maksuista palkkioita.



Kuva 3 Pankkien toiminta välikätenä

Kuviossa nähdään kuinka välikätenä toimiva pankki ottaa välityspalkkion. Kuviossa kuvastetaan, kansainvälistä pankkien välistä transaktiota. (Gowda, N & Chakravorty, C. 2021).



Kuva 4 Swift-järjestelmä pelkistettynä

Yllä oleva kuva kuvastaa yksinkertaistetusti, kuinka Swift-järjestelmän kuuluisi ideaalitulanteessa toimia. (Gowda, N & Chakravorty, C. 2021). Swift järjestelmä on kansainvälinen pankkien omistama yhteisö, joka on perustettu vuonna 1973. Järjestelmän avulla välitetään turvattuja ja salattuja kansainväliseen rahaliikenteeseen liittyviä sanomia, kuten maksutoimeksiantoja. (Paavoseppä 2022).

Kryptovaluuttakolikot perustuvat digitaalisiin allekirjoituksiin ja niiden hallinta voidaan todeta siten, että käyttäjälle annetaan digitaalinen avainpari, jonka avulla kolikon omistajuus voidaan varmistaa, sekä maksutapahtumat hyväksyä. Kryptovaluuttamaksutapahtumat toimivat julkisten ja yksityisten avainten yhteistoiminnalla. Julkisella avaimella suoritetaan maksutapahtumia ja yksityisellä taas varmistetaan, että kryptolompakko on oikean käyttäjän omistama ja sisältää tarvittavat varat, jotta maksutapahtuma onnistuu. (Nakamoto, 2008). Nakamoton (2008) mukaan aikaleimapalvelimen, jonka tehtävänä on aiemmin tehtyjen lohkojen tiivisteiden aikaleimaaminen. Näin aikaleimatut lohkot muodostavat lohkon ja aikaleima vahvistaa edellisten lohkojen leimojen todennäköisyyden. (Nakamoto, 2008).

Kryptovaluuttoja lasketaan liikkeelle usein palkintona siitä, että tietokone on käyttänyt sen prosessointikykyä laskeakseen monimutkaisia matemaattisia ongelmia ja näillä matemaattisilla laskuilla varmistetaan uudet tapahtumat lohkoissa (Lansky, J. 2018). Vauhti, jolla uusia kryptovaluuttoja muodostetaan, on kryptovaluuttakohtaista. Kryptovaluutat ovat ainoita valuuttoja, jotka mahdollistavat anonymiteetin, eli nimettömänä pysymisen kaupankäynnin aikana, sekä itsenäisyyden valtiotilasta ja täten ovat suurimmaksi osin sääntelyn ulkopuolella. (Lansky. 2018). Bitcoinin louhimisesta saadaan niin sanottu lohkopalkkio (block reward). Bitcoinin lohkoketjun työtodisteen ratkaisemisesta louhija saa yhden Bitcoinin palkkiokseen. Bitcoinissa, jokaisen 210 000 louhitun kolikon jälkeen tai noin joka neljäs vuosi palkkio puolittuu, ja tämä prosessi jatkuu niin pitkään, kunnes 21 miljoonaa Bitcoinia on kierrossa ja tällöin louhintapalkkio on nolla. Tämän arvioidaan tapahtuvan vuonna 2140. (Hayes, Adam. 2022).

Kryptovaluuttojen tärkeimpiä ja tunnetuimpia ominaisuuksia on yksityisyyden suojaaminen maksuprosessissa. Tavallisilla keskuspankin laskevilla valuutoilla maksaminen on julkisessa tiedossa. Tämä eroaa kryptovaluutoista siten, että maksutapahtuman osapuolten identiteetti voi olla täysin salassa. (Nakamoto. 2008). Kryptovaluuttatiliä aukaistaessa henkilötietoja ei tarvitse luovuttaa, joka taas on vaatimus tavallisen pankkitilin avaamisessa. (Albrecht. 2018). Kryptovaluutoilla maksaminen ei kuitenkaan ole täysin salattua, ja vaikka kryptovaluutat väittäisivät olevan täysin salattuja, niiden vaihtaminen perinteiseen valuuttaan ei ole. (Dosset, J. 2022). Nämä kryptovaluutan vaihto yritykset ovat toimivat periaatteella 'tunne asiakkaasi' ja näin vaativat asiakkaan tietoja, joka anonymiteetin hyödyn useassa tilanteessa pois. (Dosset, J. 2022).

Bitcoin on vanhin, sekä yleisin kryptovaluutta, joka on markkinoilla tällä hetkellä vuodesta 2009 lähtien mutta nykyään se ei ole ainoa vaihtoehto kuluttajille ja kyseisistä valuutoista kiinnostuneille. Markkinoilla on tarjolla useita erittäin suosittuja valuuttoja, vaikkakin ei yhtä suuria kuin Bitcoin. Valuuttoja, jotka eivät ole Bitcoin, kutsutaan usein Altcoineiksi eli vaihtoehtoisiksi valuutoiksi. Toiseksi tunnetuin ja suurin kryptovaluutta markkinoilla on Ethereum, noin \$1500 yksikköhinnalla. Tämä on arvoltaan lähimpänä Bitcoinin markkina-arvoa, vaikka onkin noin 20 kertaa pienempi kuin \$23 000 arvoinen Bitcoin tällä hetkellä 20.07.2022. (Royal & Beers. 6.2022.). Muita tunnettuja valuuttoja ovat Tether, Solana, sekä Dogecoin, joka on ollut esillä sosiaalisessa mediassa, sekä uutisissa huomattavasti viimeisten vuosien aikana. (Royal, Beers. 2022).

3 KRYPTOVALUUTTOJEN MAHDOLLINEN KÄYTTÖ RIKOLLISESSA JA TERRORISTISESSA TOIMINNASSA

Tässä kolmannessa pääluvussa kerrotaan minkälaisiin eri rikollisuuden muotoihin, kuten järjestäytyneeseen rikollisuuteen, rahanpesuun ja terroristiseen toimintaan kryptovaluuttoja voidaan käyttää, sekä käydään läpi, miten kryptovaluuttojen ominaisuudet hyödyttävät tätä toimintaa. Luvussa vertaillaan, miten kryptovaluutoilla tapahtuva rikollisuus eroaa perinteisin keinoin tapahtuvasta rikollisuudesta.

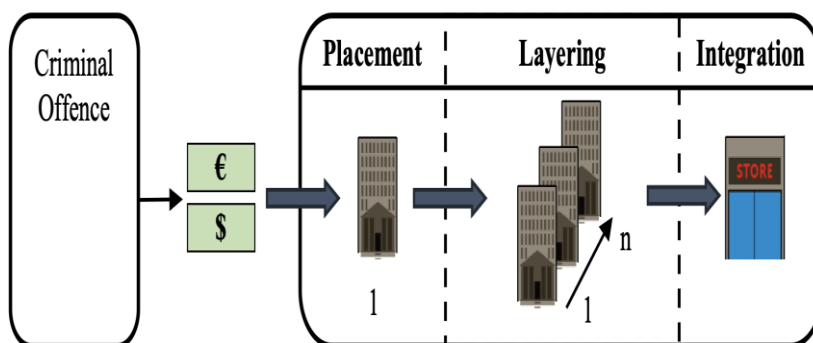
3.1 Kryptovaluutat erilaisessa rikollisuudessa

Kryptovaluutoista puhuttaessa nousee esille usein kryptovaluuttojen kaikki positiiviset mahdollisuudet ja hyvien tuottojen saamisen mahdollisuudet. Riskeihin liittyvät keskustelut liittyvät suurimmaksi osaksi kyseisten valuuttojen volatiliisuuteen, jolla tarkoitetaan hintavaihtelun voimakkuutta. Cowen, T. (2022).

Tässä tutkielmassa on tarkoitus käsitellä harvemmin puhutusta kryptovaluuttojen muodostamisista erilaisista uhista yhteiskunnalle, joka tässä osiossa käsittelee erilaista rikollista potentiaalia, kuten rahanpesua ja järjestynyttä rikollisuutta pimeässä verkossa, sekä sivuaa muita mahdollisia käyttökohteita. Rikollisella toiminnalla on usein tapana sopeutua uuden teknologian kehitykseen nopealla tahdilla ja näin on myös käynyt kryptovaluuttojen kanssa. Kryptovaluuttojen mahdollistama henkilöllisyyden suoja houkuttelee rikollista toimintaa ja tämän takia kryptovaluuttoja on omaksuttu ja suositaan vaihdannanvälineenä. Braaten, N, C. Vaughn, M. (2019). Tässä osiossa käydään läpi erilaisia käyttötapoja, mihin kryptovaluuttoja voidaan käyttää erilaisissa rikollisuuden muodoissa.

Ensimmäisenä käsitellään rahanpesua ja suuri osa rikollisesta toiminnasta pyrkiikin saavuttamaan mahdollisimman suuria taloudellisia voittoja rikollista toimintaa tekeville yksilöille tai organisaatioille. Rahanpesun tarkoituksena on taas peittää saatujen rahojen rikollinen tausta, jotta ”voitoista” voi nauttia ilman, että tuottojen lähde paljastuu. (FATF. 1999). Erilaista toimintaa, josta on mahdollista saada suuriakin voittoja, on esimerkiksi huume- ja ihmiskauppa, aseiden salakuljetukset, sekä muu järjestäytynyt rikollisuus. Rahanpesulla pyritään siirtämään tämän kaltaisesta toiminnasta varat yleiseen rahoitusjärjestelmään, jonka jälkeen varat ovat käyttökelpoisia. Ilman tätä prosessia rikoksista saadut tuotot eivät olisi kokonaisuudessaan käyttökelpoisia ilman suurta kiinnijäämisen riskiä. (CFI, 2021). Suomessa rahanpesusta tuli rangaistavaksi vuonna 1994 mutta se erotettiin kätkemispykälästä vasta vuonna 2003, jolloin se sai erillisen tunnusmerkkistön rikollislakiin. (Perämaa, N & Vasara 2003). Vuonna 2009 on arvioitu, että 1.6 triljoonaa dollaria pestiin, joka vastaisi 2,6 % maailman bruttokansantulosta. Tämä kuvastaa hyvin, kuinka laajaa tämä toiminta on ja kuinka erilaisia ratkaisuja ongelmaan vaaditaan. (Brenig, C. Accorsi, R, Müller, G. 2015)

Rahanpesu on prosessina erittäin pitkä ja monimutkainen ja se usein kuvataan kolmiosaisena prosessina, joita ovat sijoitus, kerrostamis- ja palauttamisvaiheet. (Brenig, et al, 2015). Ensimmäinen vaihe rahanpesussa on kaikkein riskialttiin, jossa tarkoituksena on siirtää varat helposti liikutettavaan muotoon, kuten esimerkiksi pankkitilille tallettamalla. Tässä vaiheessa rikollisesta toiminnasta saadut tuotot tulevat ensimmäistä kertaa muotoon, jota niitä on kohtuullisen helppo jäljittää viranomaisten toimesta. (Buchanan, 2004). Toisessa vaiheessa, joka on kerrostamisvaihe, pyritään hämärtämään rahojen alkuperää, joka tehdään laillisilla maksutapahtumilla. Usein näissä maksutapahtumissa käytetään ulkomaalaisia kanavia. Kun varat kulkevat useiden maiden läpi, vaikeutuu niiden jäljittäminen huomattavasti. (Buchanan, 2004). Kolmannessa ja viimeisessä vaiheessa rahanpesijöiden tarkoituksena on saada integroitua varat yleiseen rahoitusjärjestelmään esimerkiksi sijoittamalla arvopapereihin tai kiinteistöihin. Kun nämä kolme vaihetta on suoritettu menestyneesti, on raha pesty ja sijoitettu yleiseen rahoitusjärjestelmään. Nämä varat ovat tämän jälkeen käytettävissä. (Buchanan. 2004).



Kuva 5 Rahanpesun prosessi

Tässä kuvastetaan rahanpesun prosessia yksinkertaistetusti. (Brenig, et al. 2015).

Rahanpesu usein ajatellaan tapahtuvan perustamalla erilaisia yrityksiä, kuten ravintoloita, pesuloita, sekä muita liiketoimintoja, jossa käteinen liikkuu suurella volyymillä tai piilottamalla rahat suuren rahamäärän sekaan, kuten suuriin yrityksiin. Tätä tapahtuu edelleen mutta yhä suurenevissa määrin rahanpesu on digitalisoitunut tai on digitalisoitumassa. Mukaan on tullut kryptovaluutat ja niiden ominaisuuksien hyödyntäminen rahanpesussa. (Albrecht, Duffin, Hawkins & Morales. 2019). Suurin osa kryptovaluutoilla tehdystä rahanpesusta tapahtuu pimeässä verkossa sijaitsevilla sivuilla. Rahanpesu kryptovaluutoilla käyttää samaa prosessia pääasiassa kuin rahanpesu perinteisin menetelmin mutta kryptovaluuttojen ominaisuudet houkuttelevat siirtymään perinteisestä rahanpesusta lohkoketjuteknologiaan perustuvaan rahanpesuun. Kryptovaluutat ovatkin valtioiden sääntelyn ulkopuolella vielä tällä hetkellä, ja tämä helpottaa rikollisesta toiminnasta saatujen varojen rahanpesua. (Albrecht. 2019). Ennen kryptovaluutoilla mahdollistettua rahanpesua, varat jouduttiin piilottamaan keskuspankkijärjestelmään, johon oli mahdollista puuttua rajoittamalla ja vaikeuttamalla pankkijärjestelmässä tapahtuvaa rahanpesuprosessia ja rikollista toimintaa. (Albrecht. 2019).

Kryptovaluutoilla tapahtuvan rahanpesun kriittinen etu on siinä, että rahan pesun kolmannessa vaiheessa tapahtuva varojen integraatio rahoitusjärjestelmään voidaan tehdä paikka- ja aika riippumattomasti, esimerkiksi tekijän omasta huoneesta kannettavalla tietokoneella tai mobiililaitteella. Rahanpesussa ennen kryptovaluuttoja, varoja jouduttiin siirtämään toisten valtioiden alueille perinteisin keinoin ja tämä saattoi usein herättää viranomaisten huomion ja täten toimintaan voitiin puuttua helpommin. (Albrecht.2019). Varojen helppo liikuteltavuus rajojen yli on yksi suurimmista hyödyistä ja syistä ottaa kryptovaluutat tässä toiminnassa käyttöön.

Seuraavaksi käydään läpi pimeää verkkoa ja siellä tapahtuvaa laitonta toimintaa. Internet tyypillisesti jaetaan kolmeen osaan. Nämä ovat

pintaverkko, joka on kaikilla hakukoneilla saatavissa ja on julkinen kaikille. Toinen osa on syvä verkko, joka ei ole samalla tavalla julkinen, mutta niille on kohtuullisen helppo päästä perinteisillä selaimilla, kuten Google ja Safari. Kolmatta luokkaa kutsutaan pimeäksi verkoksi, joka vaatii selaimen, jonka avulla käyttäjä piilottaa IP-osoitteensa. Tällaisia selaimia ovat esimerkiksi Tor-selain. (Finklea, K. 2017). Pimeässä verkossa toimiminen mahdollistaa oman identiteetin salaamisen ja viranomaisilta piilossa pysymisen. Pimeässä verkossa toimii niin laillisia toimijoita, kuten toimittajia maista, jossa on suuri sensuuri ja sen myötä sananvapaus suuresti rajoitettua sekä myös huomattava määrä laittomia toimijoita. Laittomat toimijat keskittyvät usein eri alustoille, jossa valuuttana käytetään erilaisia kryptovaluuttoja. Nämä alustat toimivat esimerkiksi terroristisen toiminnan keskustelu, suunnittelu- ja toteutuspalstoina tai laittoman materiaalin, kuten aseiden ja huumeiden kauppalustoina. Johtuen. Finklean (2017) mukaan on epäselvää, kuinka paljon liikennettä näillä alustoilla on, sillä nämä palvelut, kuten Tor-selain mahdollistavat anonymiteetin. (Finklea.2017). Tunnetuin pimeän verkon alusta on Silkkitie, joka oli suosittu alusta huumekauppiain parissa, sekä muiden laittomien materiaalien kauppiaille, kuten ase, ja pornographian kauppiaille. Alustalla ainoa hyväksytty valuutta oli Bitcoin mutta vuonna 2013 kyseinen alusta suljettiin. Minnaar, A (2017). Nykypäivänä Bitcoinia on korvattu myös muilla kryptovaluutoilla ja Bitcoinin suosion kasvaessa ja valuutan tullessa tunnetuksi myös eri viranomaisten parissa, muut valuutat kasvattavat suosiotaan rikollisessa käytössä. (Möser, M, Soska, K. Et Al. (2018). Esimerkkinä voisi pitää valuuttaa, Monero, josta on tullut suosittu valuutta pimeän verkon uusilla alustoilla, jotka ovat korvanneet Silkkitien. Nämä uudet valuutat, kuten Monero parantavat edelleen käyttäjiensä yksityisyyttä. (Möser. et al. 2018).

3.2 Kryptovaluutat ja terrorismi

Ennen paneutumista terrorismin rahoitukseen, tarvitsee meidän määritellä käsite terrorismi. Terrorismia on vaikea määritellä ja sille ei ole kansainvälisesti hyväksyttyä määritelmää laissa ja Greene (2017) kertoo tähän olevan kaksi syytä. Ensimmäisenä syynä on kysymys, pystyykö valtio harjoittamaan terrorismia ja toisena syynä on kysymys, pystymmekö erottamaan vapaustaistelijan terroristista. (Greene, 2017, 413). Terrorismia on kuitenkin määritelty pitkään eri tavoin ja Laurila (2017) kertoo terrorismin olevan väkivaltaa, jonka tarkoituksena on ajaa erilaisia uskonnollisia tai poliittisia tavoitteita. 2004 julkaistussa Yhdistyneiden kansakuntien (YK) raportissa terrorismi määriteltiin toiminnaksi, jonka tarkoituksena on väkivallan avulla eri ihmisiä, organisaatioita tai valtioita kohtaan, saada halutut organisaatiot tai valtiot toimimaan halutulla tavalla. (Laurila, 2017, 5). Tässä tutkielmassa keskitytään enimmäkseen terrorismin rahoittamiseen,

sekä miten järjestöt mahdollisesti hyötyvät, sekä miksi kryptovaluuttojen käyttöönotto tällä toiminnassa olisi näille järjestöille suotuisaa.

Terrorismin rahoitus Suomessa on määritelty teoksi, jossa varoja kerätään, joko suoraan tai välillisesti tai tiedetään, että niiden tarkoituksena rahoitetaan tai tuetaan terrorismia. (Rikoslaki 1889/39. 5§). Terrorismin rahoitukseen osallistuvat yksityishenkilöt, organisaatiot, sekä valtiot. Terrorismin rahankäytön järjestelmä jaetaan kolmeen luokkaan, joita ovat rahoitus, hallinta, sekä. Kuljetus ja kulutus. (Dion-Schwarz, Manheim & Johnston. 2019). Ensimmäiseen luokkaan kuuluu rahoitus, jolla tarkoitetaan tapoja, joilla terroristinen järjestö saa kerättyä varoja. Näitä keinoja voivat esimerkiksi olla valtioiden suorat rahoitukset tai erilaiset kiristykset, joiden avulla järjestöt keräävät varoja. Toinen luokka taas käsittää tavat, joilla järjestö kätkee ja käyttää varoja, sekä siirtää varoja eri tahoille, joka tässä tapauksessa voisi olla taho, joka järjesteleekin iskua. Varoja saadakseen järjestön alueille, voidaan myös käyttää rahanpesua apuna. Perinteinen tapa siirtää varoja, on esimerkiksi salakuljettaminen. Kolmannessa vaiheessa on kulutus luokka, jolla tarkoitetaan kustannuksia, jotka kertyvät organisaatiolle. Terroristisen järjestön kustannuksia ovat riippuvaisia järjestön toiminnasta, mutta kulut voidaan usein jakaa kahteen osaan. Toiminnalliset kulut, kuten palkat ja toinen osa on erilaiset iskuihin tehtävät kulut, kuten aseiden ostaminen. (Schwarz. 2019).

Tässä lista kahdeksasta järjestöstä, jotka Yhdysvallat luokittelee terroristijärjestöksi. (U.S. DEPARTMENT of STATE). Organisaatiot ovat Yhdysvaltojen ulkopuolella sijaitsevia järjestöjä. On hyvä huomioida, että kaikki valtiot eivät pidä jokaista listalla olevaa maata terroristisena järjestönä. Lista on huomattavasti kattavampi mutta listaan tähän kahdeksan tunnetuimpana pidettyä järjestöä.

Taulukko 1 Tunnetuimpia terroristisia järjestöjä

• Al Qa'ida
• Ansaru
• Boko Haram
• ISIS-järjestöt eri alueilla
• Hizbul Mujahideen
• Hizballah
• Hamas
• Filippiinien kommunistinen puolue (CPP)

Rahoituksen saaminen vaatii terroristijärjestöiltä kykyä oppia käyttämään uusia keinoja toteuttaakseen omia tavoitteita. Vanhat keinot muuttuvat usein ajan myötä riskialttiimmiksi. (Freeman & Ruehsen. 2013). Kryptovaluutat houkuttelevatkin toimijoita ottamaan käyttöön lohkoketjuvaluuttoihin perustuvia menetelmiä hankkia rahoitusta, kuten monet muutkin rikollisorganisaatiot ovat tehneet, sillä niiden ominaisuudet mahdollistavat identiteetin salaamisen paremmin kuin perinteiset menetelmät. (Dion-Schwarz. 2019). Eniten hyötyä terroristijärjestöille on arvioitu koituvan rahankäytön järjestelmien kahdessa ensimmäisessä luokassa, kryptovaluuttojen käyttämisestä. Tämä johtuu siitä, että kryptovaluuttojen mahdollistava identiteetin salaaminen madaltaa kynnystä ulkomailla asuvien terroristijärjestöjen tukijoiden, sekä ihailijoiden lähettää rahaa kyseisille järjestöille. Rahoituksessa kryptovaluuttojen käyttö on tärkeässä asemassa ja on todettu monta näyttöä, siitä että terroristijärjestöt suosivat Bitcoinin käyttöä lahjoitusten vastaanottamisessa. (Bratley.2014). Laittomien materiaalien myyminen, huumekauppa, sekä muu pimeässä verkossa tapahtuva rikollinen toiminta on merkittävässä roolissa näiden järjestöjen rahoittamisessa. Terroristisessa toiminnassa kryptovaluuttojen ominaisuudet hyödyttävät näitä organisaatioita samoin tavoin kuin muita rikollisia organisaatioita ja toimijoita. (Dion-Schwaz. 2010). Toinen suuri hyöty näille järjestöille koituu kryptovaluuttojen, kuten Bitcoinin käytöstä siinä, että rahan siirto on erittäin nopeaa verrattuna perinteisiin rahoituskanaviin ja näiden rahasiirtojen jäljittäminen on tehty vaikeaksi. (Schwarz.2018). Tässä myös korostuu paikka- ja aikariippumattomuus, sekä valtioiden rajojen yli siirtämisen helppous.

4 LOHKOKETJUTEKNOLOGIAAN PERUSTUVIEN VALUUTTOJEN KÄYTTÖ NYKYPÄIVÄNÄ RIKOLLISESSA JA TERRORISTISESSA TOIMINNASSA, SEKÄ UHKIEN ESTÄMINEN

Seuraavassa pääluvussa tarkastellaan kryptovaluuttojen todellista käyttöä nykypäivän rikollisessa toiminnassa ja terrorismin rahoituksessa. Edellisissä kappaleissa määriteltiin käsitteet ja käytiin läpi mahdolliset käyttömahdollisuudet näille valuutoille. Tässä kappaleessa käydään myös läpi, miten käyttö on ilmennyt eri toiminnassa. Luvussa käydään lyhyesti läpi mahdollista tulevaisuuden tilannetta. Luvun loppupuolella tarkastellaan keinoja puuttua ja ennaltaehkäistä kryptovaluuttarikollisuutta ja terrorismin rahoitusta kansallisin ja kansainvälisin keinoin. Kappaleessa sivutaan hieman, miksi kryptovaluuttoja rikollis- ja terroristiset järjestöt eivät omaksuisi. Kappaleessa käsitellään niin sisäisiä ja ulkoisia uhkia, joista pääpiirteittäin rikollisuus voidaan jakaa valtion sisäisiin uhkiin, kun taas rahan pesu ja terrorismin rahoitus ulkoisiin uhkiin. On kuitenkin hyvä huomioida, että ulkoiset ja sisäiset uhat ovat melkein aina sidoksissa toisiinsa.

4.1 Kryptovaluuttojen käyttö erilaisissa rikollisuuden muodoissa nykypäivänä

Nykyään voidaan sanoa, että lohkoketjuteknologiaan perustuvat valuutat ominaisuuksillaan muodostavat valtioille ja kansainväliselle lainsäädännölle haasteen, johtuen näiden anonymiteetin mahdollistavista ominaisuuksista, sekä niiden itsenäisestä ja hajautetusta rakenteesta. (Breu, S. Seitz, T. 2018). Kappaleen ensimmäisessä osiossa käydään läpi kryptovaluuttojen vaikutusta erilaisiin rikollisuuden muotoihin.

Russon (2018) mukaan vuonna 2013 90 % Bitcoinin käytöstä oli laittomiin tarkoituksiin. Tämä luku on laskenut nykypäivänä, sillä sijoittaminen ja kryptovaluuttojen omistaminen on kasvattanut suosiotaan. Rahallisesti mitattuna, kryptovaluuttarikollisuus on kuitenkin kasvanut huomattavasti. Seuraavaksi käsitellään lyhyesti erilaisia rikollisuuden muotoja, joihin kryptovaluutat ovat vaikuttaneet ja miten niitä käytetään tänä päivänä eri rikollisuuden muodoissa.

Ensimmäisenä käsittelen huumekauppaa ja muuta järjestäytyneen rikollisuuden toimintaa pimeässä verkossa. Ennen kryptovaluuttoja, huumeita myytiin ja ostettiin vaihtamalla perinteistä valuuttaa ja käyttäen yleistä rahoitusjärjestelmää. Useimmiten, ostotilanteet toteutettiin kasvatusten. Nykyään ostotilanteet tapahtuvat pääosin pimeässä verkossa, käyttäen siihen soveltuvia selaimia, kuten Tor- Selainta. Tämä nykyinen malli antaa parempaa yksityisyyden suojaa niin myyjille, kuin ostajille. (Groysman, Igor. 2018). Hyvänä esimerkkinä pimeässä verkossa tapahtuvasta kaupankäynnistä voidaan pitää vuonna 2011 perustettua Silkkitietä. Tämä alusta lienee tunnetuin pimeässä verkossa toimivista alustoista. Alustalla myytiin melkein jokaista tunnettua huumeainetta mahdollistaen nimettömänä pysymisen ostajilla, sekä myyjillä ja vaihdonvälineenä käytettiin valuuttaa, jota on vaikea jäljittää. (Groysman.2018). Silkkitieltä lähetettyjen pakettien kohdepaikat eivät kuitenkaan olleet nimettömiä ja tämä vaikutti vuonna 2013 alustan sulkemiseen viranomaisten toimesta. Sivun perustajana toimi Ross William Ulbricht. Sivuston sulkemisen jälkeen tilalle on tullut useita vastaavia sivustoja, jotka ovat viranomaisilta paremmin piilossa. Greenbergin (2018) mukaan tulevaisuudessa Bitcoinin käyttö vähenee merkittävästi ja poistuu vähemmän tunnettujen valuuttojen tieltä. Bitcoinin ongelmana rikollisesta näkökulmasta on, että se jättää maksatapahtumasta jälkiä. Valuutat, kuten Monero ovat korjanneet nämä ongelmat. (Groysman.2018). Monerosta on tullutkin uusien alustojen pääasiallinen valuutta. Samalla periaatteella toimivat myös muiden laittomien materiaalien kauppa, kuten asekauppa. Useilla alustoilla, joissa kaupataan huumeita, niin on myös muuta laitonta materiaalia tarjolla. Groysmanin (2018) mukaan uusia alustoja syntyy nopealla tahdilla ja aina kun yksi alusta saadaan estettyä, toinen tulee tilalle.

Rahanpesu toimii merkittävässä roolissa rikollisesta toiminnasta saatujen varojen "nauttimisessa". Perinteiset rahanpesu menetelmät ovat yhä käytössä, mutta viranomaisten kyky jäljittää tätä toimintaa on parantunut. Tämän vuoksi kryptovaluutoilla tehtävä rahanpesu on muuttunut varteenotettavaksi vaihtoehdoksi eri rikollisille ja terroristisille toimijoille. (Groysman.2018). Kryptovaluutat mahdollistavatkin rahanpesun eri osapuolien pysymisen nimettömänä ja ilman yhteneväistä säännöstelyä ja yhteistyön parantamista viranomaisten välillä liittyen kryptovaluuttoihin, järjestäytyneeseen rikollisuuteen ja rahanpesuun, on tämän toiminnan estäminen käytännössä mahdotonta. (Dyntu, V. Dykyi, O. 2018).

Yleisesti yhteiskuntaa haittaava tekijä on harmaa talous ja merkittävä yhteiskuntaa haittaava toiminta on verojenkierto ja kryptovaluutat mahdollistavat tätä toimintaa. On mahdollista, että tulevaisuudessa kryptovaluutat korvaavat perinteiset veroparatiisit (Marian, Omri. 2013). Kryptovaluuttojen omaisuudet muistuttavatkin veroparatiisien piirteitä: Henkilöiden henkilöllisyys on piilossa ja tulot eivät ole verojen alaisia, olleessaan ”kryptolompakoissa”. Kryptovaluuttojen etuna on myös riippumattomuus rahoituslaitoksista. Yhä useamman perinteisen ”veroparatiisin” kiristäessä verotuspolitiikkaa, on virtuaaliset veroparatiisit muodostumassa houkuttelevaksi vaihtoehdoksi. Kryptovaluutoista saatujen hyötyjen verottaminen usein perustuu vapaaehtoiseen ilmoittamiseen ja kansalaisten ”luottamiseen”. (Jafari, S et al. 2018).

4.2 Kryptovaluuttojen käyttö terroristisessa toiminnassa

On näyttöä, että viime vuosina terroristiset järjestöt ovat alkaneet käyttämään kryptovaluuttoja rahoittaakseen omaa toimintaansa erilaisilla lahjoitus ja keräysmenetelmillä. (Wang, S. Zhu, X. 2022). Wang & Zhu (2022) kertovat, että erilaiset vastatoimenpiteet ja toiminnan estäminen on hankalaa, sillä nämä terroristien käyttämät menetelmät ovat verrattain uusia ja tutkimusta aiheesta on tehty vähän. Teollisuusmaissa terrorismin rahoitukseen on alettu kiinnittämään enemmän huomiota viime vuosina mutta Kehittyvissä valtioissa toimintaa ei valvota samalla tavalla. Tässä osiossa käydään läpi minkälaista toimintaa terroristiset järjestöt rahoittavat kryptovaluutoilla ja minkälaisia keinoja tähän käytetään.

Yksi terrorististen järjestöjen tärkeimpänä tulonlähteenä ovat erilaiset lahjukset ja järjestöt ovatkin kirjottaneet kirjan nimeltä Bitcoin wa Sadagat al jihad, jossa opastetaan eurooppalaisia, sekä pohjoisAmerikkalaisia lähettämään Bitcoineja Järjestöille. (Weimann, 2016). Kryptovaluuttoja käytetään myös huume, ase ja muiden laittomien materiaalien kaupassa, jonka avulla järjestöt keräävät itselleen voittoa. Tässä erilaiset pimeän verkon alustat toimivat tärkeässä roolissa. (Wang & Chu. 2022). Vuoden 2016 Jakartan terroristi-iskussa on arvioitu, että Bitcoinilla rahoitettiin iskun suunnittelua ja itse iskua. (Wang & Chu. 2022). ISIS-järjestö taas kidnappasi eurooppalaisia Syyriassa ja näiden avulla pyrki saamaan lunnaita Bitcoinin muodossa. Näiden lunnaiden avulla toteutettiin iskuja Euroopassa. (Wang & Chu. 2022). Kryptovaluuttoja pyritään myös saamaan kirstämällä yksityishenkilöitä ja eri organisaatioita. (Wang & Chu. 2022).

Vuodesta 2014 eteenpäin terrorismin rahoitus on osittain siirtynyt kryptomaailmaan mutta niistä ei ole muodostunut pääasiallinen keino hankkia rahoitusta. Eri järjestöt kuten Al Qaeda, ISIS ja Hezbollah. Tulevaisuudessa on mahdollista, että kryptovaluuttojen kehittyessä ja mahdollistaessa yhä paremman anonymiteetin, järjestöjen halu lisätä kryptovaluuttojen käyttöä ja korvata perinteisiä menetelmiä kasvaa. Tällä hetkellä perinteisiäkään menetelmiä ei olla

viranomaisien toimesta saatu estettyä ja tämän takia siirtyminen vaihtoehtoisiin valuuttoihin ei näillä järjestöillä ole ollut pakollista. (Wang & Chu. 2022). Teknologinen kehittyminen tällä alueella on kuitenkin nopeaa ja tätä on vaikeaa ennustaa, jonka vuoksi on tärkeää, että aiheesta tehdään lisätutkimuksia ja eri valtiot, sekä viranomaiset kehittävät uusia keinoja jäljittää ja torjua kryptovaluuttojen avulla suoritettua terroristista ja rikollista toimintaa.

4.3 Tekijät, jotka heikentävät kryptovaluuttojen omaksumista

Kryptovaluuttojen ominaisuudet tällä hetkellä ovat sellaisia, jotka saattavat myös vähentää terrorististen- ja rikollisjärjestöjen halua ottaa näitä valuuttoja käyttöön. Usein puhutaan ainoastaan ominaisuuksista, jonka vuoksi nämä houkuttelevat tätä toimintaa mutta on myös useita syitä, mitkä saattavat hidastaa näiden valuuttojen käyttöönottoa tai estää tämä kokonaan. Käydään läpi erilaisia syitä, miksi näitä ei välttämättä oteta käyttöön.

Näiden valuuttojen volatilitteetti on yksi kryptovaluuttojen tunnetuimmista haitoista, jotka vaikuttavat kaikkiin kryptovaluuttoista kiinnostuneihin. Tämä on usein myös mediassa esillä ja samalla vaikuttaa ihmisten sijoitushaluihin. Tämä äkillinen heilahtelu on tuonut välillä mahdollisuuden rikastua nopeasti. Rikollisilla ja terroristisilla järjestöillä tämän uskotaan vaikuttavan negatiivisesti halun ottaa kyseisiä valuuttoja käyttöön. (Wang & Chu. 2022). Kryptovaluuttoilla hinnan vaihtelu on niin suurta, että sitä on vaikeaa ennustaa ja on samalla erittäin epävakaa, sillä päivittäinen arvo saattaa heilahdella useilla kymmenillä prosenteilla. Järjestelmä, jossa kryptovaluuttakauppaa käydään, on myös epävakaa ja markkinoille saapuu jatkuvalla syötöllä uusia valuuttoja. Nämä ovat esimerkkejä syistä, jotka hidastavat kyseisen teknologian omaksumista terroristisessa- ja rikollisessa toiminassa. (Wang & Chu. 2022).

4.4 Kryptovaluuttauhkien torjuminen ja ennaltaehkäiseminen

Kryptovaluutat ja pimeä verkko ovat alkaneet kiinnostamaan päätöksentekijöitä, eri viranomaisia, sekä tutkijoita johtuen kryptovaluuttojen mahdollistamasta pimeän verkon maksuvälineenä toimimisen, rahanpesun ja terrorismin rahoittamisen edistämisen. Tutkimusta ei tällä hetkellä ole tarpeeksi ja päättäjät eri maissa pohtivat parhaita ratkaisuja, miten kryptovaluuttojen negatiivisia puolia voidaan estää ja säännellä. (Alkadri.2019). Tässä tutkielmassa käsiteltyjen kryptovaluuttojen käyttömahdollisuudet, kuten rahanpesu, erilainen järjestäytyneen rikollisuuden toiminta, sekä terrorismin rahoitus kuuluvat kansainvälisen lain

piiriin niin perinteisessä mielessä, kuin kryptovaluuttojen kanssa. (Juntunen, HM.2022).

Das (2018) väittää, että kryptovaluuttojen säännöstely ei ole riittävällä tasolla suurimmassa osassa maissa. Jotkut valtiot ovat omaksuneet virtuaaliset valuutat vastaan mielellään ja pyrkivät mahdollistamaan niiden käyttöä yhteiskunnissa, kun taas jotkut valtiot ovat ottaneet täysin vastakkaisen toimintamallin ja parhaimpina esimerkkeinä voidaan pitää joidenkin valtioiden pyrkimyksiä kieltää kryptovaluutat täysin. (Das, C, A. 2018). Reitman (2019) ei usko tämän olevan järkevää tai mahdollista suuressa mittakaavassa ja väittää, että kieltäminen saattaa hidastaa yhteiskunnan innovatiivisuutta, eikä myöskään estäisi rikollisuuden elementtejä käyttämästä kryptovaluuttoja.

Maailmassa on kuitenkin valtioita, jotka ovat kieltäneet täysin kryptovaluuttojen käytön johtuen niiden suuresta käytöstä rikollisten parissa. Vuonna 2021 Kiina yllätti maailman, kun sen keskuspankki kertoi, että kaikki kryptovaluuttatoiminta maassa on kiellettyä. Viranomaiset maassa ottivat tiukan otteen esimerkiksi kryptovaluutta louhijoita kohtaan. (Adebajo, M. 2022). Muita maita, jotka ovat ottaneet vastaavanlaisen käytänteen ovat esimerkiksi Bolivia, Vietnam ja Egypti. Haums, M. (2021) väittää, että Kryptovaluuttojen kieltämiset eivät estä niiden avulla suoritettua rikollisuutta. Tämä johtuu siitä, että näiden valuuttojen käyttöä ei voida estää suoraan, sillä ne eivät olet minkään yksittäisen valtion ulottuvissa. (Haums, M. 2021).

FATF järjestö, joka on taloudellisen yhteistyön ja kehityksen järjestö on viime vuosina tutkinut, sekä arvioinut kryptovaluuttojen luomia uhkia ja riskejä taloudellisten organisaatioiden näkökulmasta (Wang & Chu. 2021). Vuonna 2020 FATF julkaisi raportin, jossa eri riskitasoja arvioitiin, sekä pyrittiin avustamaan organisaatioita tunnistamaan terrorismin rahoitusta ja rahanpesua. (Wang & Chu. 2021). Wang & Chu väittävät, että kansainvälisillä organisaatioilla, kuten FATF on merkittävä rooli luodessaan erilaisia viitekehyksiä, jonka avulla valtiot sääntelevät kryptovaluuttoihin liittyvää toimintaa.

Toinen merkittävä keino, jolla kryptovaluuttoja ja niiden avulla suoritettua toimintaa voidaan säädellä, on valtioiden keskuspankkien avulla. Keskuspankit voisivat esimerkiksi tehostaa finanssipolitiikkaansa ja tuoda markkinoille omia digitaalisia valuuttoja muiden perinteisen käteisen ja kortin rinnalle. Tarkoituksena olisi muuttaa nykyiset valuutat paremmin sopiviksi nykymaailmaan. (Wang & Chu.2021). Tämä tapa voisi tuoda myös vakautta nykyisiin epävakaisiin kryptovaluuttamarkkinoihin.

Johtuen kryptovaluuttojen kansainvälisestä luonteesta, sekä mahdollisuudesta nopeasti ja helposti rajojen ylittävien maksutoimenpiteiden suorittamiseen, yksittäisten valtioiden on hankala selvittää ja estää tätä toimintaa. Tämän vuoksi on tärkeää maiden välille kehittää yhteistoimintaa. (Wang & Chu. 2021).

Esimerkkeinä voisi pitää eri viranomaisten tietojen jakamisen, sekä yhteistyön kehittämistä. Wang & Chu kertovat, että viranomaisille olisi tärkeää kehittää mekanismeja informaation jakamista varten, jonka avulla rahanpesua ja terrorismin rahoitusta rajojen yli voitaisiin estää. Kansainvälisiä sopimuksia ja raameja täytyisi myös luoda, joiden avulla voitaisiin yhtenäistää valtioiden lainsäädäntöä liittyen kryptovaluuttoihin. Tämä mahdollistaisi taas yhtenäisiä toimintamalleja viranomaisille.

5 JOHTOPÄÄTÖKSET

Kirjallisuuskatsauksen tarkoituksena oli selvittää, kuinka lohkoketkuteknologiaan perustuvat valuutat, kuten Bitcoin toimivat ja avata lukijalle käsitettä lohkoketjut. Näiden jälkeen oli tarkoitus tutkia, miten kryptovaluutat ominaisuuksillaan muodostavat tänä päivänä ja mahdollisesti tulevaisuudessa uhkia yhteiskunnalla. Tutkielman tarkoituksena oli myös selvittää, mitä erilaisia rikollisuuden muotoja kryptovaluutat voivat ominaisuuksillaan tukea, ja missä niiden käyttöönotosta olisi huomattavaa etua. Viimeisenä käydään läpi, miten näitä uhkia voidaan torjua kansallisin ja kansainvälisin keinoin. Tutkielman pääkysymykset, joihin tässä pyrin vastaamaan ovat; ”Minkälaisia sisäisiä ja ulkoisia uhkia lohkoketjuteknologiaan perustuvat valuutat muodostavat yhteiskunnalle?”, sekä ”Miten kryptovaluutoilla toteutettua rikollisuutta ja terrorismia voidaan torjua?”

Kryptovaluutat ovat lohkoketjuihin perustuvia, hajautettuja virtuaalisia valuuttoja, joista ensimmäisen on kehittänyt Satoshi Nakamoto vuonna 2008. Nykyään markkinoilla on tuhansia kryptovaluuttoja ja suurin näistä on Bitcoin, jonka vuoksi tässä tutkielmassa puhutaan pääasiassa tästä valuutasta ja vaikutuksista rikollisuuteen. Vuoden 2008 finanssikriisin on uskottu vaikuttaneen Nakamoton haluun kehittää maksutapa, jota ei valvo kolmannet osapuolet, eikä pankit peri palkkioita transaktioista. Kryptovaluuttojen tärkeimpiä ominaisuuksia, jonka vuoksi tämäkin tutkielma on tehty näiden valuuttojen mahdollistama anonymiteetin säilyttäminen erilaisten maksutapahtumien aikana. On hyvä huomioda, että transaktiot eivät ole täysin salassa ja näistä jää jälkiä, joka taas on vaikuttanut uusien kryptovaluuttojen kehittämisille, kuten Monero, jonka avulla maksutapahtumia voidaan suorittaa säilyttäen anonymiteettiä paremmin.

Vastatessani yhteen pääkysymyksistä ” minkälaisia sisäisiä ja ulkoisia uhkia kryptovaluutat muodostavat yhteiskunnalle?”, tuli lähdekirjallisuuden perusteella seuraavia rikollisuuden ja terrorismin muotoja, jotka kryptovaluuttojen ominaisuuksien takia houkuttelee rikollisia ja terroristisia toimijoita näiden valuuttojen käyttöönottamiseen erilaisessa rikollisessa toiminnassa. Tutkielmassa on käyty läpi muutamia rikollisuuden muotoja, joissa kryptovaluuttojen

käyttöön otosta olisi eniten hyötyä. Yksi näistä muodoista on rahanpesu, jossa kryptovaluutoilla rahanpesua voidaan tehdä aika- ja paikkariippumattomasti ja välittämättä valtioiden rajoista. Kryptovaluuttojen helppo liikuteltavuus onkin yksi suurimmista hyödyistä rahanpesussa kiinnijäämisen riskin pienentämiseksi. Rahanpesussa pyritään rikollisesta toiminasta saatujen tuottojen saamiseen käytökelpoiseksi yleisessä rahajärjestelmässä, jotta rikollisesta toiminnasta voidaan hyötyä.

Tässä tutkielmassa käsiteltiin myös, kryptovaluuttojen käyttöä muussa järjestäytyneen rikollisuuden toiminnassa, kuten huume- ja ihmiskaupassa. Tässä merkittävässä roolissa toimii pimeä verkko ja sen sisällä olevat erilaiset kauppialustat, kuten vuonna 2013 suljettu silkkitie ja nykyään sen korvanneet vastaavan kaltaiset alustat. vaihtoehtoiset valuutat, kuten Monero ovat kasvattaneet suosiotaan pimeän verkon alustoilla, sillä nämä ovat tuoneet entistä enemmän yksityisyyttä mahdollistavia ominaisuuksia. Tässä on hyvä huomioida, osto- ja maksutapahtumissa ovat hyötyneet niin ostajat, kuin myyjät. Suomessakin noin joka toinen huumeiden ostaja on hankkinut aineet pimeästä verkosta. Natri, S. (2018). Kolmas tässä tutkielmassa käsitelty kryptovaluuttojen käyttökohde on erilainen terroristinen toiminta ja sen rahoittaminen. Kryptovaluuttojen ominaisuudet hyödyttävät terroristisia organisaatioita samoin tavoin, kuin muita rikollisia organisaatioita. Tärkeimpinä hyötyinä on varojen nopea siirtäminen valtioiden rajojen yli, sekä aika- ja paikka riippumattomuus, sekä tietenkin varojen lahjoittajien ja vastaanottajien vahvempi kiinnijäämisen suoja.

Tutkielmassa käytiin myös läpi, minkälaisessa mittakaavassa nykypäivänä eri rikolliset ja terroristiset toimijat ovat ottaneet käyttöönsä kryptovaluuttoja ja kuinka suuria riskejä yhteiskunnalle näiden käyttöönotto on tuonut. Nykyään voidaan sanoa, että kryptovaluutat muodostavat haasteita ja riskejä eri organisaatioille ja kansainväliselle lainsäädännölle, johtuen kryptovaluuttojen anonyymiteetin mahdollistavista, sekä valtioiden rajoja helposti ylittävistä ominaisuuksista. Lähdekirjallisuuden perusteella voidaan sanoa, että kryptovaluutat ovat muodostaneet varteenotettavan vaihtoehdon nykypäivän rikollisuudelle ja terrorismille, vaikka eivät vielä olekaan syrjäyttäneet perinteisiä yleisessä rahajärjestelmässä tapahtuvaa varojen siirtoa ja rahanpesua. Viime aikoina terroristisen toiminnan rahoittaminen on osittain siirtynyt kryptomaailmaan, ja tapauksia, jossa iskuja on rahoitettu kryptovaluutoilla, on ilmennyt. Tämä ei kuitenkaan ole muodostunut pääasialliseksi tavaksi hankkia rahoitusta näille järjestöille. lohkoketjuteknologiaan perustuvat valuutat kehittyvät jatkuvasti ja nopealla tahdilla, joten näiden käyttämisen ennustaminen on vaikeaa. tämän vuoksi aihe vaatii jatkuvasti lisätutkimusta ja yhteistyön kehittämistä, jotta kyseistä toimintaa pystytään estämään.

Toinen tutkielman pääkysymys oli ”Miten kryptovaluutoilla toteutettua rikollisuutta ja terrorismia voidaan torjua?” Tähän pyrittiin vastaamaan käymällä läpi laajasti eri lähdekirjallisuutta ja voidaan todeta, että tutkimusta tarvitaan

aiheesta lisää. Monet valtiot ovat ottaneet erilaisia kantoja kryptovaluuttoihin, jotka eroavat toisistaan huomattavasti. Esimerkiksi Kiina on kieltänyt kryptovaluuttatoiminnan maassa, kun taas toiset maat ovat pyrkineet olemaan avoimia erilaiselle kryptovaluuttatoiminnalle. Tässä käytetyt lähteet toteavat, että kryptovaluuttojen kieltäminen ei estä näillä teknologioilla toteutettua rikollisuutta. Tässä tutkielmassa voidaan todeta, että yhtä selvää ratkaisua asialle ei ole, mutta tämän rikollisuuden muodon torjumiseen tarvitaan eri organisaatioiden, valtioiden ja viranomaisten välistä tiivistä yhteistyötä ja tiedonjakoa, sekä erilaisten mekanismien kehittämistä joiden avulla viranomaiset voivat seurata varojen liikkumista rajojen yli. Useat lähteet mainitsevat, että nykyinen tilanne saattaa tulevaisuudessa muuttua huomattavasti ja kryptovaluuttojen käyttö tulee suurella todennäköisyydellä yleistymään rikollisessa ja terroristisessa toiminnassa.

Aihe vaatii jatkotutkimuksia ja jatkossa voitaisiin tehdä tutkimusta tarkemmin yksittäisistä osa-alueista, tämän tutkielman ollessa yleinen ja kuvaava kirjallisuuskatsaus aiheesta. Tarkempia tutkimuskohteita voisi olla esimerkiksi rahanpesu tai terrorismi ja kryptovaluuttojen käyttöönottamisen käytännön seuraukset näissä toiminnoissa. Toinen mielenkiintoinen aihe, josta voisi tehdä tutkimusta, on miten valtioissa, joissa kryptovaluutat ovat kiellettyjä, on kryptovaluutoilla toteutettu rikollisuus kehittynyt verrattuna valtioihin, joissa on avoin suhtautuminen lohkoketjuteknologiaan perustuviin valuuttoihin. Aiheesta on tehty lopulta kohtuullisen vähän tutkimusta ajatellen, kuinka suosittu kryptovaluutta aiheet ovat mediassa ja tämän vuoksi tutkimusta tarvitaan lisää, jotta yleistämys ihmisillä, organisaatioilla ja valtion viranomaisilla kasvaisi.

LÄHTEET

- Adebajo, M (2022). Top-5 countries with strictest crypto regulations. Coinspeaker. Haettu kohteesta <https://www.coinspeaker.com/top-5-strictest-crypto-regulations/>
- Albrecht, C. Duffin, K. Hawkins, S & Morales Rocha, V (2019). The Use Of Cryptocurrencies In The Money Laundering Process. Journal of Money Laundering Control. Haettu Kohteesta Doi:10.1108/JMLC-12-2017-0074
- Alan Greene. (2017). Defining terrorism. One size fits it all? Durham university law school.
- Alkadri, S. (2019). Defining and regulating cryptocurrency: Fake internet money or legitimate medium of exchange.
- Ben-Sasson, Chiesa, Garman, Green, Miers, Tromer, et al. (2014). Zerocash: decentralized anonymous payments from Bitcoin, in 2014 IEEE symposium on Security and Privacy. 459-474.
- Breu, S. Seitz, T. (2018). Legislative regulations to prevent terrorism and organized crime from using cryptocurrencies and its effect on the economy and society. Lomonosov Moscow State University. Haettu Kohteesta: <https://deliverypdf.ssrn.com/delivery.php?ID=414065068026025126023071076117083002017016005008033085110094122005099068122064086004003032103103116031046074069120004024127101055010000046009116001088090092126070073009009083084010010009093026107003095113092122095120087110064075007082029108008101026103&EXT=pdf&INDEX=TRUE>
- Buchanan, B (2004). Money laundering – A global obstacle. Research in international business and finance, 115-127. Doi: 10.1016/j.ribaf.2004.02.001
- Bruce Scheier. (1994). One-Way Hash Functions.
- Brenig, C. Accorsi, R. Müller, G. (2015). Economic analysis of cryptocurrency backed money laundering. Association for information systems. Haettu kohteesta https://web.archive.org/web/20190828223207id_/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1019&context=ecis2015_cr
- CFI team. (2021). The illegal process of converting money earned from illegal activities into “clean money”. Haettu kohteesta. <https://corporatefinanceinstitute.com/resources/knowledge/finance/money-laundering/>
- Gowda, N. Chakravorty. (2021). Comparative study on cryptocurrency transaction and banking transaction. Science Direct. 530-534.
- Cowen, T. (2022). Crypto’s value comes from crypto’s volatility. Bloomberg. Haettu kohteesta. <https://www.bloomberg.com/opinion/articles/2022-06-02/how-should-we-value-crypto-by-how-volatile-crypto-assets-are>
- Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston. 2019. Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats. Rand corporation

Change. ICMB INTERNATIONAL CENTER FOR MONETARY AND BANKING STUDIES

- Dosset, J. (2022). Are cryptocurrency Transactions Actually Anonymous. CNET. Haettu kohteesta. <https://www.cnet.com/personal-finance/crypto/are-cryptocurrency-transactions-actually-anonymous/>
- Daj, J & Vasarhelyi, M.A.(2017). Towards blockchain-based accounting and assurance. *Journal of information systems*. 5-21.
- Dyntu, V. Dykyi,O. (2018). Cryptocurrency in the system of money laundering. FATF-OECD. (1999). Money laundering. Policy Brief. Haettu kohteesta https://www.bahamasb2b.com/b2b/big_picture/download/FATF_Laundering.pdf
- Fabian Maximilian, J. T. (2018). Financing terrorism through cryptocurrencies – a danger for europe? *Journal of Money Laundering Control*, 21(4), 513-519. Haettu kohteesta. <https://www.emerald.com/insight/content/doi/10.1108/JMLC-06-2017-0024/full/html>
- Freeman & Ruehsen. (2013). Terrorism financing methods. Perspectives on terrorism. Haettu Kohteesta https://www.jstor.org/stable/26296981#metadata_info_tab_contents
- Haums, M. (2021). Banning cryptocurrencies to counter crime is a nonsensical excuse. Cointelegraph. Haettu kohteesta <https://cointelegraph.com/news/banning-cryptocurrencies-to-counter-crime-is-a-nonsensical-excuse>
- Juntunen, HM. (2022). Virtuaalivaluutat rahanpesun-ja terrorismin rahoittamisen- sääntelyn ja rikosten ennaltaehkäisemisen näkökulmasta. Lapin Yliopisto. Pro-Gradu.
- Kuo Chuen, Guo, L & Wang, Y (2018). Cryptocurrency: A new investment opportunity? *The journal of alternative investments*. 16-40. Doi 10.3905/jai.2018.20.3.016
- Lansky, J. (2018). Possible state approaches to cryptocurrencies. University of Finance and administration in Prague. Haettu kohteesta <https://pdfs.semanticscholar.org/c14a/cbbb00b5baee7f10b24d224d429ee6b39e0e.pdf>
- Lawrence H, White. (2015). The market for cryptocurrencies. HeinOnline. Haettu kohteesta. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/catoj35&div=32&id=&page=>
- Leible,S. Schlager, S. Schobotz, M. (2019). A Review on Blockchain technology and Blockchain Projects Fostering Open Science. *Frontiers*. Haettu kohteesta. <https://www.frontiersin.org/articles/10.3389/fbloc.2019.00016/full>.

- Michael Casey, Jonah Crane, Gary Gensler, Simon Johnson and Neha Narula. 2018. The Impact of Blockchain Technology on Finance: A Catalyst for
- Minnaar, A. (2017). Online 'underground' marketplaces for illicit drugs: the prototype case of the dark web website 'Silk road'. Southern African journal of criminology. Haettu kohteesta
- Möser, M. Soska, K.Heilman, E. et al (2018). An empirical analysis of traceability in the monero blockchain.
- Nakamoto, Satoshi. (2008). Bitcoin: A Peer-To-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>
- Natri, Santtu. (2018). Kansainvälinen tutkimus: Huumeiden ostaminen netistä on Suomessa yleisempää kuin muualla. Yle. Haettu kohteesta. <https://yle.fi/uutiset/3-10195755>
- Paavoseppä. (2022). Mikä on Swift. OP media. haettu kohteesta. <https://www.op-media.fi/talous/mika-on-swift/>
- Russo, C. (2018). Bitcoin Speculators, Not drug dealers, Dominate crypto use now. Haettu Kohteesta: <https://www.bloomberg.com/news/articles/2018-08-%202007/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now>
- Royal, J. Beers, B.(2022). 12 most popular types of cryptocurrency. Bankrate. Haettu kohteesta <https://www.bankrate.com/investing/types-of-cryptocurrency/>
- Reitman, R. (2019). Why Outlawing Cryptocurrency Purchases Is A terrible Idea. EFF. Haettu kohteesta. <https://www.eff.org/deeplinks/2019/05/why-bill-banning-cryptocurrency-purchases-americans-terrible-idea>
- U.S Department of State. Foreign Terrorist Organizations. Terror designations and state sponsors of terrorism. Haettu kohteesta. <https://www.state.gov/foreign-terrorist-organizations/>
- Wang, S. Zhu, X. (2022). Evaluation of potential cryptocurrency development ability in terrorist financing. Institute of finance and economics, Central university of finance and Economics, Peking.
- Weimann, G (2016). Going Dark: terrorism on the dark web. Studies in conflict & Terrorism. 195-206. Haettu kohteesta <https://psycnet.apa.org/doi/10.1080/1057610X.2015.1119546>
- Zheng,Z. Xie,S. Dai, H. Chen, X & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE international Congress on Big Data. S 557-564. 10.1109/Big-DataCongress.2017.85.