KRYPTOVALUUTTOJEN KÄYTTÖ RIKOLLISESSA TOIMINNASSA

Janne Suittio

10/2019

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

TIIVISTELMÄ

Tekijä(t)	Tutkinto
Janne Suittio	Poliisi (AMK)
Julkaisun nimi Kryptovaluuttojen käyttö rikollisessa toiminnassa	Julkisuusaste Julkinen
Ohjaaja Jani Niemi & Samuli Mikkola	Opinnäytetyön muoto Kuvaileva kirjallisuuskatsaus

Tiivistelmä

Opinnäytetyöni tarkoituksena on selvittää lukijalle mitä ovat kryptovaluutat sekä millaiseen rikolliseen toimintaan kryptovaluutat liittyvät.

Kryptovaluuttojen käyttö on lisääntynyt viime vuosien aikana ja siksi uskon, että myös rikollisuudessa kryptovaluuttoja käytetään tällä hetkellä yhä enenevissä määrin. Kryptovaluuttoja voidaan käyttää hyvinkin erilaisin keinoin, ja siksi ne avaavat myös uusia tapoja rikosten toteuttamiseen sekä rahoittamiseen.

Opinnäytetyöni on toteutettu kuvailevana kirjallisuuskatsauksena, jonka apuna on käytetty kvalitatiivisen tutkimuksen tutkimusmenetelmiä osana tiedonhakua. Nämä käyttämäni menetelmät ovat rahanpesun selvittelykeskuksen kahden asiantuntijan teemahaastattelu sekä tiedonhankintakeinona käyttämäni näytteiden ottaminen Darknetissä toimivista palveluista sekä sivustoista.

Opinnäytetyöni avaa lukijalle sen mitä kryptovaluutat ovat ja miten niitä käytetään. Sen lisäksi kerron kuinka kryptovaluuttoihin liittyvä rikollisuus voidaan jakaa neljään pääkategoriaan, jotka ovat: 1. kryptovaluutat laittomassa kaupankäynnissä maksuvälineenä, 2. kryptovaluutat rahanpesun välineenä, 3. kryptovaluutat rikoksen kohteena sekä 4. kryptovaluutat rikollisten liiketoimintana, sekä mitä nämä kategoriat sisältävät.

Näiden neljän pääkategorian sisältämillä rikostyypeillä on tietynlaisia ominaisuuksia, jotka yhdistävät eri rikollisuuden muotoja. Vaikka rikokset voidaan karkeasti rajata näihin neljään pääkategoriaan, ovat rikokset useimmiten kategorioiden rajoja ylittäviä. Esimerkiksi rahanpesu kytkeytyy jossakin muodossa useimpiin rikoksiin, joissa käytetään kryptovaluuttoja. Näihin rikoksiin, joissa kryptovaluutat ovat mukana, liittyy osittain myös Darknet sekä erilaiset pikaviestintäsovellukset.

Kryptovaluuttojen käyttöä rikollisessa toiminnassa pyritään ehkäisemään ja rajoittamaan regulaation avulla. Regulaatio on kokenut vuonna 2018 muutoksia, kun EU:n viides rahanpesudirektiivi julkistettiin, jonka pohjalta lainsäädäntöä on muutettu Suomessakin.

Sivumäärä	Tarkastuskuukausi ja -vuosi
48	11/2019

SISÄLLYS

1 JOHDANTO

Kryptovaluutat ovat suhteellisen uusi ilmiö, ja niiden käyttö on lisääntynyt suurissa määrin viime vuosien aikana. Kryptovaluutat ovat joidenkin mielestä tulleet korvaamaan nykyisen rahajärjestelmän tai ovat vähintäänkin digitaalista kultaa.[1] Kryptovaluuttojen etuna on se, että pääsääntöisesti ne eivät ole sidoksissa mihinkään valtioon tai pankkiin, vaikka nykyisin pankit ja valtiot ovatkin kiinnostuneita aiheesta.[2] Kryptovaluuttojen avulla rahaliikennettä ohjaillaan lohkoketjuteknologian avulla, jolloin verkossa olevaa laskentatehoa käytetään transaktioiden suorittamiseen ja turvaamiseen.[3] Kryptovaluutat ovat osittain saaneet sellaisen maineen, että rahan siirtoa henkilöiden välillä ei täten pystyttäisi seuraamaan ja valuutat olisivat nykyisessä julkisessa maailmassa varsin anonyymejä. Todellisuudessa nämä ovat todellisuudessa lähinnä pseudonyymejä.[4] Tämä on avannut myös rikollisille uusia polkuja käyttää näitä valuuttoja hyödykseen erilaisissa rikoksissa tai niiden rahoittamisessa.

Koska kryptovaluuttojen käyttö on lisääntynyt viime vuosien aikana uskon, että myös rikollisuudessa kryptovaluuttoja käytetään tällä hetkellä yhä enenevissä määrin. Siksi koen tarpeelliseksi selvittää opinnäytetyössäni sitä, mitä kryptovaluutat ovat sekä millaisia rikoksia näiden avulla nykyään tehdään ja miten kyseisiä rikoksia toteutetaan. Jotta tämän kaltaisia rikoksia voidaan jatkossa ehkäistä entistä tehokkaammin, on tärkeää, että poliisihallinnossa tiedetään mitä kryptovaluutat ovat ja miten niitä käytetään millaistenkin rikosten tekemiseen.

Koska kryptovaluutat ovat suhteellisen uusi ilmiö, ei aiheesta ole Suomessa vielä kovin paljon tehty tieteellisiä tutkimuksia, joka asettaa tietynlaisen haasteen materiaalin hankkimiseen. Lisäksi suurin osa kryptovaluuttoihin kohdistuvista tutkimuksista pohjautuu vain ja ainoastaan Bitcoiniin, joka on toiminut kryptovaluutoiden suunnan näyttäjänä, mutta on nykyään vain yksi monista kryptovaluutoista.

---

[1] Johannes Palmgren, Kryptovaluutan arvo kysynnän ja tarjonnan armoilla (Finanssiala.fi 16.7.2019)
[2] Mikä on kryptovaluutta ja mihin sitä tarvitaan? (Bitcoinkeskus.com 11.2.2019)
[3] Juho Rantala, Lohkoketjuteknologian yhteiskunta. Osa I: Bitcoinista Ethereumiin. niin & näin (1/2018, 45)
[4] Liam Morris, Anonymity analysis of Cryptocurrencies (4/2015, 3)

Tässä opinnäytetyössä käsittelen kryptovaluuttoja ja niiden taustalla olevaa teknologiaa, käyttötarkoituksia ja niiden käyttöä.

Jotta rikollisuutta kryptovaluutojen ympärillä voi ymmärtää, on tiedettävä perusasiat siitä mitä ne ovat. Näiden jälkeen aion pohtia sitä, millaiseen rikollisuuteen kryptovaluuttoja yleisimmin käytetään ja mikä kullekin rikostyypille on ominaista. Tämän lisäksi sivuan hieman sitä, että mitä muuta teknologiaa yleisimmin näiden käyttöön liittyy. Koska opinnäytetyöni tarkoitus on kertoa lukijalle yleisesti kryptovaluuttojen käytöstä rikollisuudessa, en aio pohtia sitä, miten näitä rikoksia ratkotaan tai kuinka paljon niitä määrällisesti tapahtuu. Ilman tätä rajausta opinnäytetyöstäni tulisi suhteettoman laaja.

Opinnäytetyöni on kuvaileva kirjallisuuskatsaus, jossa hyödynnän kryptovaluutoista kertovia kotimaisia sekä ulkomaisia artikkeleja ja tutkimuksia. Aion kokonaisuuden hahmottamiseksi suorittaa asiantuntijan teemahaastattelun, jossa perehdyn kryptovaluuttojen käyttöön rikollisessa toiminnassa. Lisäksi tutustun Darknetissä sijaitseviin palveluihin sekä keskustelufoorumeihin, joiden avulla voin tuoda työhöni erilaisia esimerkkejä rikosten ominaispiirteistä ja verrata niitä toisiinsa.

2 OPINNÄYTETYÖN PROSESSI

2.1 Kuvaileva kirjallisuuskatsaus

Kirjallisuuskatsaukset ovat jaettu kolmeen erilaiseen perustyyppiin, jotka ovat kuvaileva kirjallisuuskatsaus, systemaattinen kirjallisuuskatsaus sekä meta-analyysi[5]. Näistä olen omaan opinnäytetyöhöni valinnut kuvailevan kirjallisuuskatsauksen, koska sen avulla minun on mahdollista luoda aiheestani kattava yleiskatsaus.

Kuvaileva kirjallisuuskatsaus on ikään kuin yleiskatsaus, jostakin tutkittavasta ilmiöstä. Kuvaileva kirjallisuuskatsaus mahdollistaa tutkittavan ilmiön laajan kuvaamisen. Tämän vuoksi myös tutkimuskysymykset voivat olla laajempia ja se soveltuu tämän opinnäytetyön toteuttamiseen mielestäni parhaiten.[6]

Kuvailevan kirjallisuuskatsauksen alalajeihin kuuluva narratiivinen yleiskatsaus on prosessi, jonka tarkoituksena on kiteyttää aikaisemmin tehtyjä tutkimuksia yhteen. Narratiiviseen yleiskatsaukseen hankittu materiaali ei kuitenkaan yleensä käy läpi tiukkoja seuloja, joka taas tarkoittaa sitä, että varsinaista analyyttistä tulosta ei voida tämän avulla laatia. Tämä kirjoitusmenetelmä auttaa laatimaan laajan kuvan käsiteltävästä aiheesta ja kokoamaan ajankohtaista tietoa tutkimuskysymyksistä.[7] Siksi koen tämän kirjallisuuskatsauksen muodon tukevan opinnäytetyöni päämäärää parhaiten.

Kirjallisuuskatsaukseni tukena aion hyödyntää myös Darknetin tarjoamaa tietoa, ottamalla näytteitä Darknetistä, joiden avulla voin havainnollistaa kryptovaluuttojen käyttöä rikollisessa toiminnassa.

”Näyte on mikä tahansa osajoukko, joka on otettu tai valittu ns. perusjoukosta. Ei ole käytetty todennäköisyysotantaa, vaan tiedonantajat on poimittu mielivaltaisella tavalla. Näytteen perusteella ei voi tehdä yleistyksiä perusjoukkoon. Näyte koostuu yhdestä tai useam-

[5] Ari Salminen: Mikä kirjallisuuskatsaus? (Vaasa 2011, 6-8)
[6] ibid
[7] ibid

masta tiedonantajasta, informantista, joten aineistolähtöisessä tutkimuksessa ei käytetä käsitteitä havainto- tai tilastoyksikkö tai koehenkilö.'"[8]

Näytteen valintaan voidaan käyttää useita erilaisia kriteerejä, joista itse käytän näytteen ottamisessa sopivuuteen perustuvaa valintaa.[9] Tämä valintakriteeri mahdollistaa sen, että voin valita mielivaltaisesti sopivimman aihetta kuvaavan ja helpoiten saatavilla olevan lähteen Darknetistä.

Päästäkseni Darknetiin käytän Tor-selainta, josta pyrin löytämään opinnäytteeni teoriaosuuden tueksi esimerkkejä ja mahdollista lisätietoa. Koska kyseisien sivustojen kautta on mahdollista tukea tai ottaa osaa rikolliseen toimintaan, en aio eettisistä syistä merkitä tarkemmin lähdeluetteloon, mistä olen tiedon löytänyt.

Kirjallisuuskatsauksen tiedonhankintaa varten haastattelen myös rahanpesun selvittelykeskuksen asiantuntijoita. Haastattelua käytän yhtenä lähteenäni kirjallisuuskatsauksessa. Toteutan haastattelun asiantuntijan teemahaastatteluna, joka mahdollistaa haastattelun elämisen[10].

Teemahaastattelussa teemojen avulla pyritään selvittämään ilmiö ja saamaan ilmiöstä kokonaisvaltainen käsitys. Teemahaastattelu voidaan toteuttaa yksilö- tai ryhmähaastatteluna. Teemahaastattelun avulla tutkija pyrkii kaivamaan tutkimusongelmaansa liittyviä asioita ymmärtämisensä kasvattamiseksi. Teemahaastattelussa selvitettävät teemat elävät haastattelun aikana.[11]

Haastattelussa pyrin selvittämään, millaisiin eri rikoksiin kryptovaluuttoja käytetään, mitkä ovat niiden ominaispiirteitä sekä mitä muuta teknologiaa rikosten tekemiseen yleensä liittyy.

---

[8] Perusjoukko, Otanta, Otos ja Näyte (kamk.fi)
[9] ibid
[10] Jorma Kananen 2015: Opinnäytetyön kirjoittajan opas. Jyväskylä, Jyväskylän ammattikorkeakoulu, 145-150.
[11] ibid

2.2 Opinnäytetyön tarkoitus ja tavoitteet

Opinnäytetyöni tarkoitus on vastata tutkimuskysymyksiin: Mitä kryptovaluutat ovat ja miten niitä käytetään? Millaisiin rikoksiin kryptovaluuttoja käytetään ja millä tavoin? Siksi mielestäni kuvaileva kirjallisuuskatsaus, jonka tukena käytän tiedon haussa laadullisen tutkimuksen edellä mainitsemiani keinoja, toimii parhaiten näin laajan aiheen käsittelyyn. Tämä tutkimusmetodi mahdollistaa selkeän kuvan rakentamisen, jota lukijan on helppo seurata.

Opinnäytetyöni tavoite on koostaa mahdollisimman kattava yleisluontoinen katsaus kryptovaluuttojen perusteisiin sekä tuoda esille rikollisuuden muotoja, joihin kryptovaluuttoja nykyään käytetään.

2.3 Aineiston keruu

Kirjallisen aineisto on kerätty internetin eri hakukoneita hyödyntäen. Haun olen suorittanut manuaalisesti ja käyttäen useita eri hakusanoja, niin englanniksi kuin suomeksi.

Olen rajannut käytettävän materiaalin siten, että käytän opinnäytetyössäni ensisijaisesti aiheesta tehtyjä tutkimuksia sekä viranomaisten julkaisemia tiedotteita/vuosikertomuksia, jotka ovat saatavilla ilmaiseksi. Lisäksi käytän lähteinä kryptovaluuttatoimintaan aktiivisesti perehtyneiden sivustojen ja palvelujen artikkeleja sekä tarvittaessa esimerkin luontaisesti uutisartikkeleja. Kaikki käytetyt artikkelit ja tutkimukset pyrin rajaamaan siten, että ne ovat 2009-2019 väliseltä ajalta. Materiaalin hankinnassa poissulkukriteerinä oli AMK-opinnäytetyöt, muut ulkomaalaiset kuin englanninkieliset julkaisut sekä julkaisut, jotka eivät ole ilmaiseksi saatavilla.

2.4 Kirjallisuuskatsauksen analyysi

Analyysissä pyrin tiivistetysti avaamaan, mitä yhtäläisyyksiä ja eroavaisuuksia kryptovaluutoilla tehtävissä rikoksissa on. Lisäksi pyrin pohtimaan regulaation, eli sääntelyn, tulevaisuuden vaikutuksia rikoksiin, joissa kryptovaluuttoja käytetään. Analysoinnissa vertailen kuvailevan kirjallisuuskatsauksen avulla selvitettyjen rikollisuuden kategorioiden eroja ja yhtäläisyyksiä, sekä vertailen näiden rikollisuuden kategorioiden ominaispiirteitä regulaatioon aiheuttamiin muutoksiin.

2.5 Kirjallisuuskatsauksen kohderyhmä

Kirjallisuuskatsauksen avulla pyrin antamaan mahdollisimman kattavan kuvan kryptovaluutoista ja niiden käytöstä rikollisessa toiminnassa. Kirjallisuuskatsaus on suunnattu ensisijaisesti esitutkintaa suorittaville viranomaisille sekä poliisihallinnon toimijoille, jotka saattavat työnsä puolesta törmätä kryptovaluuttojen käyttöön rikollisuudessa. Jotta rikollisuutta näiden avulla voi ymmärtää, on mielestäni olennaista, että ymmärtää kryptovaluuttojen perustoimintatavan ja käyttötarkoituksen.

3 KRYPTOVALUUTAT

3.1 Lohkoketjuteknologia kryptovaluutoissa

Kryptovaluutat pohjautuvat kukin tavallaan lohkoketjuteknologiaan. Kryptovaluutoissa pääsääntöisesti käytettävä lohkoketjuteknologia on desentralisoitua, eli lohkoketju ei ole keskitetty yhden toimijan päätösten alaisuuteen.[12] Lohkoketjuteknologian periaatteena on luoda täysin avoin digitaalinen tilikirja, joka on hajautettu käyttäjille, jolloin siirtoihin ei tarvita välikättä kuten esimerkiksi pankkia. Tämä tarkoittaa sitä, että jokainen transaktio eli siirto tallentuu lohkoista muodostuvaan ketjuun, joka päivittyy jokaiselle käyttäjälle automaattisesti. Tämä on siis ikään kuin avoin tilikirja, jossa kaikki tapahtumat ovat julkisia. [13] Mikäli lohkoketjun tallentaa tietokoneelleen on mahdollista nähdä sieltä jokainen yksittäinen data mitä lohkoketjuun on tallentunut. Tämä tarkoittaa sitä, että esimerkiksi jokainen kryptovaluutan transaktio voidaan tarkistaa kyseisestä lohkoketjusta.[14]

Otetaan esimerkiksi kaikkien tuntemat, pankkikorteilla tehtävät maksut. Pankkikortilla maksettaessa jokaisesta ostosta tai varainsiirrosta jää jälki, mutta se jää vain ja ainoastaan pankkiin. Kuka tahansa ei pysty katsomaan siirtoja, koska kaikki siirrot tallentuvat vain palveluntarjoajan tietoihin, johon pääsy on vain palveluntarjoajalla. Lohkoketjuteknologian avulla jokainen pystyy siis näkemään nämä siirrot ja varsinaista palveluntarjoajaa ei tarvita, koska siirrot vahvistetaan käyttäjien kesken.

Lohkoa voidaan verrata pienen ajanjakson tilikirjaan, joka sisältää kaikki tapahtumat tietyn ajanjakson sisällä. Jokainen lohko sisältää uusia transaktioita sekä edellisen lohkon tiivistefunktion, joka on mistä tahansa datasta luotu satunnainen merkkijono, joka muodostuu jokaisella käyttäjällä aina samanlaiseksi. Tämä tiivistefunktio ikään kuin sisällyttää edellisen lohkon aina uudemman lohkon sisään, jolloin lohkot eivät ole irrallisia toisistaan. Lisäksi tämä tiivistefunktio pitää huolen siitä, että jokaisella käyttäjällä on sama versio lohkosta, joka taas ehkäisee sen, että joku käyttäjistä pääsisi muokkaamaan lohkon sisältämiä

[12] Juho Rantala: Lohkoketjuteknologian yhteiskunta. Osa I: Bitcoinista Ethereumiin. niin & näin (1/2018, 45–58)
[13] ibid
[14] Niclas Storås: Lohkoketjuteknologia pähkinänkuoressa – tämä kannattaa tietää (tivi.fi 5.4.2016)

tietoja. Kun nämä lohkot yhdistetään tällä tiivistefunktiolla, muodostuu niistä lohkoketju, joka sisältää kaiken datan koko lohkoketjun olemassaolon ajalta.[15]

Kryptovaluutoissa on julkinen ja yksityinen salausavain sekä osoite, joka on kryptovaluuttalompakko. Jokaista näistä tarvitaan varojen siirtämiseen, jotta kryptovaluutan käyttöoikeus siirtyy henkilöltä toiselle ja kyetään varmistamaan, että siirto on sallittu.[16]

Ne tahot, joilla on hallussaan kryptovaluutan lohkoketjun transaktiohistoriat, kutsutaan nodeiksi. Mikäli taholla on tallennettuna koko kryptovaluutan lohkoketju palvelimelleen, kutsutaan sitä silloin full nodeksi. Nodet ovat ikään kuin kryptovaluuttojen keskuspalvelimia, jotka valvovat verkon sisällä tehtyjä transaktioita. Valvominen tarkoittaa käytännössä sitä, että ”valvoja” tarkastaa, onko lompakossa, josta varoja ollaan siirtämässä, riittävästi katetta siirron suorittamiseksi. Tämän jälkeen tiedot transaktiosta lähetetään eteenpäin louhijoille. Kaikki vahvistamattomat siirrot eli transaktiot kerääntyvät yhteen paikkaan, jota kutsutaan memory pooliksi, jota louhijat käsittelevät.[17]

Siirtojen toteutuminen vaatii vahvistamista, jota kutsutaan kryptovaluutoissa yleensä louhimiseksi. Tässä louhijat eli henkilöt, jotka ylläpitävät verkkoa, antavat älypuhelimensa, tietokoneensa tai louhintaan tehdyn laitteensa laskentatehoa verkon käyttöön varmentaakseen kryptovaluutoissa tehtäviä siirtoja matemaattisia laskutoimituksia ratkomalla. Vastineeksi louhijat saavat palkaksi kyseistä kryptovaluuttaa.[18] Louhinnassa louhijat eli minerit kasaavat memory poolissa olevat odottavat transaktiot lohkoketjun seuraavaan lohkoon[19].

Vaikka kryptovaluutat käyttävät pääsääntöisesti desentralisoitua lohkoketjua on olemassa toinenkin lohkoketjuteknologia, joka on hajautettu lohkoketju. Tällaisessa hajautetussa ketjussa on yksi keskus, joka ohjailee lohkoketjun toimintaa. Tällaista teknologiaa käyttävät pääsääntöisesti yritykset, jotka hyödyntävät omassa toiminnassaan lohkoketjua. Loh-

[15] ibid
[16] Rantala: (n 12), 45
[17] Opas: Mikä on Bitcoin? (Bitcoinkeskus.com 15.4.2019)
[18] Rantala: (n 12), 45
[19] Bitcoinkeskus: (n 17)

koketjua ei siis käytetä vain ja ainoastaan kryptovaluutoissa, vaan sitä käytetään myös esimerkiksi erilaisten rekisterien tai älysopimusten ylläpitämiseksi.[20]

Mikäli kryptovaluutan ohjelmistokoodissa havaitaan jotakin, mitä verkon eri toimijat haluavat muuttaa, voidaan se toteuttaa forkeilla. Forkit ovat käytännössä ohjelmistopäivityksiä, joilla pyritään parantamaan kryptovaluutan turvallisuutta, korjaamaan koodissa olevia virheitä, lisäämään ominaisuuksia tai nopeuttamaan valuutan toimintaa. Tavalliseen käyttäjään nämä ohjelmistopäivitykset eivät juurikaan vaikuta eikä heillä ole vaaraa, että heidän käytössään oleva valuutta ei enää toimisi.[21]

Nämä päivitykset vaikuttavat vain nodejen toimintaan ja siksi myös nodet ovat ohjelmistopäivityksiä tuottava taho. Forkit voidaan jakaa kahteen eri tyyppiin. Toinen näistä on soft-fork ja hard-fork. Soft-forkissa lohkoketjua muutetaan siten, että uuden päivityksen käyttöönotto on vapaaehtoista ja se toimii yhdessä päivittämättömän version kanssa. Hard-fork tarkoittaa taas käytännössä sitä, että uusi versio ei enää toimi vanhan lohkoketjun kanssa yhteen. Tämä tarkoittaa sitä, että kryptovaluutta hajaantuu ja siitä irtoaa uusi kryptovaluutta. Hajaantumisessa vanha kryptovaluutta jatkaa toimintaa aikaisemmin käytössä olleella koodilla, ja uusi syntynyt valuutta jatkaa toimintaa päivitetyllä koodilla.[22]

3.2 Yleisesti kryptovaluutoista

Kryptovaluutoista monelle tulee ensimmäisenä mieleen Bitcoin. Vaikka Bitcoin on suurin kryptovaluutta, ja sen osuus kryptovaluuttojen reilun 222 miljardin dollarin markkinasta on noin 66%, on se vain yksi monista kryptovaluutoista maailmassa. Kryptovaluuttojen arvon seuraamisessa yksi suosituimpia internet-sivustoja on coinmarketcap.com, jonka mukaan maailmassa on tämän opinnäytetyön kirjoitushetkellä bitcoinin lisäksi 2391 erilaista kryptovaluuttaa, joista 905 on altcoineja ja 1486 tokeneita.[23]

Kryptovaluutat eli virtuaalivaluutat ovat ainakin osittain nimensä mukaisesti valuuttoja, jotka ovat vain ja ainoastaan virtuaalisia. Näistä valuutoista suurin osa ei ole sidoksissa

---

[20] Rantala: (n 12), 45
[21] Kryptovaluuttojen forkit: mitä ne oikein ovat? (Bitcoinkeskus.com 14.4.2018)
[22] ibid
[23] https://coinmarketcap.com

mihinkään viralliseen valuuttaan, kuten dollariin tai euroon. Kryptovaluutat eivät kuitenkaan ole virallisia FIAT-valuuttoja, eli virallisesti hyväksyttyjä valuuttoja. Tämä käy ilmi Suomen verottajan tulkinnasta, jossa kryptovaluutat ovat luokiteltu omaisuudeksi, mutta ei kuitenkaan arvopaperiksi[24]. Siksi esimerkiksi kauppojen ei tarvitse hyväksyä kryptovaluutoilla maksamista.

Kryptovaluuttojen tarkoitus on alun perin ollut virtuaalinen valuutta, joka korvaisi FIAT-valuutat tai toimisi ainakin niiden rinnakkaisvaluuttana. Kryptovaluuttojen etuna on lisäksi se, että ne eivät ole keskuspankkien kontrollissa ja näin ollen ihmiset, jotka eivät luota keskuspankkeihin tai valtioihin saavat käyttöönsä valuutan, jota ei mikään yksittäinen taho kontrolloi[25]. Nykyään kryptovaluuttoja käytetään huomattavasti eri tarkoituksiin ja uusia kryptovaluuttoja syntyy tämän tästä. Osa kryptovaluutoista on keskittynyt vain johonkin yhteen tiettyyn käyttötarkoitukseen eikä yleiseksi valuutaksi. Siksi kaikkia kryptovaluuttoja kutsutaan itseasiassa hieman virheellisesti kryptovaluutaksi. Vain pieni osa näistä on tehty vain toimimaan valuuttana. Suurin osa kryptovaluutoista onkin projekteja, jotka mahdollistavat kyseisen kryptovaluutan sisään rakennettavan applikaatioita tai uusia kryptovaluuttoja. Osa kryptovaluutoista onkin siis lähempänä ohjelmointialustoja kuin valuuttaa.[26]

Tällaisesta hyvä esimerkki on Ethereum, joka on virtuaalinen käyttöjärjestelmä. Ethereum sisältää oman ohjelmointikielen, jota voidaan käyttää hyväksi Ethereumin sisäisten älysopimuksia hyödyntävien sovellusten kehittelyssä. Tämä tarkoittaa sitä, että lohkoketjuun voidaan ohjelmoida sopimuksia, jotka sisältävät ehtoja ja näitä sopimuksia on mahdoton lahjoa tai muokata jälkeenpäin. Tämä mahdollistaa siis sovellusten luomisen, joiden sisältämä toiminta vaatii jonkinlaisen sopimuksen. Tällaisia sopimuksen vaativia toimintoja ovat esimerkiksi osakekaupat tai valuuttojen vaihdot.[27]

Koska kryptovaluutoilla on lukemattomia erilaisia käyttötarkoituksia, ei ole mielestäni opinnäytetyöni kannalta tarkoituksenmukaista käsitellä niitä enempää. Tärkeintä on ymmärtää se, että nämä eivät nimensä mukaisesti ole pelkästään valuuttoja.

---

[24] Virtuaalivaluuttojen verotus, VH/1982/00.01.00/2019 (vero.fi 7.10.2019)
[25] Bitcoinkeskus: (n 2)
[26] Miten kryptovaluuttojen arvo muodostuu? (Bitcoinkeskus.com 18.7.2019)
[27] Opas: Mikä on Ethereum? (Bitcoinkeskus.com 12.9.2019)

Kryptovaluuttoja käytetään ympäri maailmaa. Suurimman kryptovaluutan Bitcoinin käyttäjäkunta on jakautunut siten, että 2018 vuoden toisella neljänneksellä 39.9% käyttäjistä olivat eurooppalaisia, 35.8% amerikkalaisia, 18.2% aasialaisia, 4.1 % afrikkalaisia ja 2% oseanialaisia. Sen käyttäjistä taas 86.9% oli miehiä samalla ajanjaksolla tutkittuna.[28] Koska Bitcoin käsittää suurimman osan kryptovaluuttojen markkinasta, voidaan mielestäni olettaa, että myös muut kryptovaluutat jakautuvat käyttäjäkunnaltaan samalla tavalla.

3.2.1 Coinit ja altcoinit

Kuten edellä mainitsin, kryptovaluutat voidaan karkeasti jakaa coineihin ja tokeneihin, vaikka molemmista käytetään arkikielessä puhuttaessa termiä kryptovaluutta. Coinit ovat virtuaalista rahaa, joita käytetään vaihtoehtoisena valuuttana FIAT-valuutoille. Suurin näistä coineista on markkinoita johtava Bitcoin. Coinit vaativat sen, että niillä on käyttäjäkunta, joka hyväksyy näiden käytön yhteisenä valuuttana. Lisäksi kaikki coinit vaativat louhijoita.[29]

Kun puhutaan altcoineista eli alternative coineista, tarkoitetaan muita coineja kuin Bitcoinia vaikka nämä ovat myös coineja. Nimensä mukaan nämä ovat vaihtoehtoja Bitcoinille. Vaikka näiden päätarkoitus onkin sama kuin Bitcoinissa, on niiden luomisella pyritty ratkaisemaan Bitcoinissa olevia ongelmia ja näin ollen tarjoamaan parempi vaihtoehto valuutaksi. Siksi osa altcoineista onkin jonkun toisen kryptovaluutan hard forkeja.[30]

3.2.2 Tokenit

Tokenit ovat kryptovaluuttoja, joita ei käytetä pelkästään vaihdannan välineinä. Tokenit eivät toimi samanlaisessa lohkoketjussa kuin altcoinit. Ne toimivat esimerkiksi Ethereumin lohkoketjun sisällä.[31] Eli käytännössä tokenit toimivat vain tämän yhden rajatun toimintaympäristön sisällä, esimerkiksi tietyn tuotteen tai palvelun ostamiseen. Suurin ero coinei-

---

[28] Global Cryptocurrency Market Report (Ibinex, 9.10.2018, 40)
[29] Bitcoinkeskus: (n 25)
[30] Ibinex: (n 28), 11
[31] Ibinex: (n 28), 11

hin verrattuna on tokenien monipuolisuus, joka mahdollistaa niiden käytön rahan lisäksi myös muissa ominaisuuksissa, joita avaan hieman alempana.

Coinien ja tokenien erottaminen toisistaan on hyvin haastavaa ja siksi molemmat sisällytetään yleisesti termin kryptovaluutta alle.[32]

Tokenit jakautuvat kahteen eri luokkaan: Utility token ja Equity token. Utility tokenilla on erityisiä ominaisuuksia, jotka mahdollistavat pääsyn tiettyyn ohjelmistolliseen toiminnallisuuteen, tai sen avulla voi olla mahdollista lunastaa erilaisia tarjouksia. Equity token on taas lähempänä osaketta. Tämä mahdollistaa yrityksille ikään kuin osingonmaksun, jolloin yhtiön tulosta jaetaan tokenien omistajille. [33]

Tokeneita on mahdollista saada ICO:issa eli Initial Coin Offeringeissa, joiden avulla yritykset keräävät rahaa oman toimintansa rahoittamiseksi ja antavat yrityksen luomaa tokenia vastineeksi. Käytännössä tämä muistuttaa melko pitkälti tavanomaisilta pörssimarkkinoilta tuttua maksullista osakeantia, jolla yritykset keräävät rahaa toimintansa rahoittamiseen. ICO:ia järjestävät yritykset ovat normaalisti start-up yrityksiä, jotka luovat tällaisen tokenin kerätäkseen varoja. Yritykset luovat ennen tätä white-paperin, jossa kuvataan yrityksen tavoitteita sekä avataan heidän teknologiaansa. Tällä pyritään vakuuttamaan sijoittajalle miksi juuri heidän yrityksensä tulee menestymään. Tämän pohjalta sijoittajat voivat tehdä päätöksen ICO:iin liittymisestä.[34]

3.3 Kryptovaluuttojen säilytys

Kryptovaluuttoja voidaan säilyttää erilaisissa lompakoissa tai kryptovaluuttapörsseissä. Näitä pörssejä on olemassa coinmarketcap.com sivuston mukaan 20635 kappaletta[35].

Kryptovaluuttalompakkoja on useita erilaisia ja näitä ovat online-, desktop-, mobiili-, hardware-, ja paperilompakko.[36] Kryptovaluuttojen säilytys on hieman turvallisempaa

---

[32] Perustiedot: Kryptovaluutat (kryptokansalainen.fi 12.12.2017)
[33] ibid
[34] Ibinex: (n 28), 12
[35] Coinmarketcap (n 23)
[36] Opas: valitse oikea Bitcoin-lompakko (Bitcoinkeskus.com 25.11.2017)

lompakoissa kuin pörsseissä, koska niissä ei ole liikkeeseenlaskijariskiä. Tästä varoittavana esimerkkinä toimivat kryptovaluuttapörsseihin tehdyt hyökkäykset, joissa pörsseissä olevista lompakoista on anastettu hakkeroimalla miljoonien dollarien edestä kryptovaluuttoja.

Onlinelompakko on hieman pörssinkaltainen lompakko, joka on toimiva hyvin pienien summien säilyttämiseen. Tämä tapa perustuu siihen, että kryptovaluutat ovat jonkun yrityksen säilytyksessä. Esimerkiksi Suomalaisella Coinmotionilla on tarjolla holvi-palvelu, jossa kryptovaluuttoja voidaan säilyttää. Tämä säilytystapa on riippuvainen yrityksen turvallisuustasosta.[37]

Desktop- ja mobiililompakot taas ovat hieman turvallisempia kuin edellä mainittu onlinelompakko. Nämä lompakot ovat ohjelmistoja tai sovelluksia, jotka asennetaan tietokoneelle tai mobiililaitteelle. Nämäkin lompakot ovat edelleen online-yhteydessä koko ajan, eli ne ovat niin kutsuttuja hot walletteja. Erona näissä on, että privaattiavain, jolla tilin saa tarvittaessa palautettua, on vain ja ainoastaan käyttäjän hallinnassa, toisin kuin pörssissä tai onlinelompakossa säilytettäessä. Käytännössä tämä tarkoittaa, että varat ovat edelleen hakkeroitavissa, mutta tämä on huomattavasti epätodennäköisempää kuin esimerkiksi kryptovaluuttapörsseissä, koska ne eivät ole yhtä kiinnostavia kohteita hakkereille, niiden pienempien rahamäärien vuoksi.[38]

Seuraava säilytysvaihtoehto on hardware-lompakko, joka pääsääntöisesti muistuttaa muistitikkua. Tämä lompakko on cold wallet, joka ei ole jatkuvasti yhteydessä internetiin. Tällainen lompakko muistuttaa usein muistitikkua. Laite kytketään verkkoon vain kaupankäynnin tai siirtojen ajaksi, jolloin tikku ei altistu verkon vaaroille jatkuvasti. Tätä varten tietokoneelle asennetaan erikseen ohjelma, jolla lompakkoa pystytään hallinnoimaan. Sovellus ei kuitenkaan toimi ilman lompakkoa. Tällaisten lompakkojen lähestulkoon keulakuvana toimii Ledger Nano X. Tällaisessa lompakossa turvallisuudesta vastaa käytännössä vain käyttäjä itse. Mikäli tikun kadottaa voi lompakon saada haltuunsa vielä privaattiavaimen avulla. Siksi privaattiavain tulee säilyttää yhtä turvallisesti kuin fyysinen lompakkokin, jotta tämä ei joudu vääriin käsiin.

---

[37] ibid
[38] ibid

Viimeinen säilytysmahdollisuus on paperilompakko, joka on käytännössä hyvin lähellä hardware-lompakkoa, jokseenkin hieman yksinkertaistettu versio. Tässäkin tapauksessa, kuten hardware-lompakossa privaattiavain on internetin ulkopuolella säilytyksessä ja vain käyttäjän hallinnassa. Tällaisen paperilompakon voi luoda internetissä, ja kuten nimestäkin voi päätellä, lompakko on käytännössä vain paperilla, mutta sen saldon pystyy tarkistamaan privaattiavaimen avulla internetissä. Rahojen pois siirtämiseen lompakosta käyttäjä tarvitsee hot walletin.[39]

On myös olemassa fyysistä kolikkoa muistuttava Denarium-kolikko, joka käytännössä sisältää paperilompakon. Kolikolle voidaan tallettaa 0-2 Bitcoinia ja se voidaan ostaa joko tyhjänä tai siten, että sinne on valmiiksi ladattu Bitcoinia.[40]

3.4 Kryptovaluuttojen hankkiminen

Edellisessä kappaleessa perehdyin siihen, miten kryptovaluuttoja voidaan säilyttää erilaisissa paikoissa. Kryptovaluuttojen hankkimiseen on muutamia eri keinoja. Yksi helpoimmista keinoista on ostaa kryptovaluuttaa FIAT-valuutalla, eli virallisilla valuutoilla, kuten euroilla tai Yhdysvaltain dollareilla. Muita vaihtoehtoja ovat louhiminen, airdropit ja lahjoitukset.

Kryptovaluuttojen ostaminen vaatii sen, että ostajalla on olemassa oleva tili eli lompakko, jossa kryptovaluuttaa voidaan säilyttää. Suurin osa lompakoista tukee bitcoinia, joka on markkinoiden suurin kryptovaluutta. Mikäli halutaan säilyttää jotakin muuta kryptovaluuttaa, on käyttäjän huomioitava, että jokainen lompakko ei tue mitä tahansa kryptovaluuttaa.

Kryptovaluuttojen ostamisen voi suorittaa internetin välityksellä ja niitä on nykyään mahdollista ostaa useista eri yritysten ICO:ista, pörsseistä tai kauppapaikoista esimerkiksi suomalaisesta Coinmotion-palvelusta, josta pankkitunnuksia käyttämällä voi ostaa Bitcoinia. Pienemmillä kryptovaluutoilla on usein ongelmana, että niitä ei voida ostaa suoraan FIAT-valuutalla, vaan ensin pitää omistaa esimerkiksi Bitcoinia tai Ethereumia, jotka voidaan pörssissä vaihtaa joksikin muuksi kryptovaluutaksi.

---

[39] ibid
[40] Denarium Custom Kultapäällystetty 2019 (bittiraha.fi)

Bitcoinia sekä Litecoinia, joka on myös yksi kryptovaluutoista, voidaan ostaa Suomessa myös käteisellä. Tämä tapahtuu Bittimaattien eli bitcoin-automaattien välityksellä. Bittimaatit ovat suomalaisen Bittiraha.fi -yrityksen Suomeen tuomia automaatteja, joista ensimmäinen saapui Suomeen vuonna 2013. Nämä Bittimaatit toimivat lähestulkoon samankaltaisesti kuin normaalit nosto- ja talletusautomaatit.[41] Nykyään Bittimaatteja löytyy Suomesta 10 kappaletta[42].

FIAT-valuutalla voidaan ostaa kryptovaluuttoja myös suoraan joltakin henkilöltä. Esimerkiksi Internetin keskustelupalstoilla tai esimerkiksi Telegram- sovelluksen ryhmissä ihmiset voivat ostaa tai myydä kryptovaluuttoja. Silloin käytännössä vaihto tapahtuu siten, että toinen ihminen luovuttaa kryptovaluuttalompakkonsa tai siirtää toisen lompakkoon rahaa vastineeksi siitä, että hänelle maksetaan sovittu hinta esimerkiksi euroina. Tällaisessa ostotavassa tulee huomioida, että tämä on huomattavasti riskialttiimpaa kuin edelliset ostotavat.

3.4.1 Louhinta

Kryptovaluuttoja voidaan hankkia myös louhimalla niitä. Louhintaa voidaan toteuttaa kryptovaluutasta ja sen lohkoketjun louhinta-algoritmin vaikeustasosta riippuen erilaisilla välineillä. Näitä välineitä ovat muun muassa näytönohjaimet, prosessorit ja louhintaa varten rakennetut laitteet kuten ASIC- miner[43].

Louhintamarkkinat ovat huomattavan suuret. Esimerkiksi vuonna 2016 globaalin louhintamarkkinan arvo oli yhteensä 610.91 miljoonaa dollaria ja markkinan on odotettu kasvavan tulevaisuudessa huomattavasti. Louhintaan vaadittava laitteisto ja niiden sähkökustannukset aiheuttavat louhinnalle kuluja. Tällä hetkellä tehokkain kryptovaluuttojen louhimiseen käytettävä laite on Innosilicon G32-1800[44]. Tällainen laite maksaa tällä hetkellä noin 15 000 dollaria ja sen arvioitu tuotto päivässä on noin 149 dollaria. Louhiminen hankaloi-

[41] https://bittimaatti.fi/companies
[42] https://bittimaatti.fi/locations
[43] Ibinex: (n 28), 222
[44] https://www.asicminervalue.com/

tuu koko ajan ja tarvitaan enemmän tehoa, jotta lohkoketjua voidaan käsitellä kannattavasti.[45]

Koska louhinta on merkittävässä osassa kryptovaluuttojen toimimisessa, on alalle hakeutunut yrityksiä, jotka tekevät tätä omana toimialanaan. Vuonna 2017, 90% käytetystä louhintatehosta käytettiin Kiinassa. Tämä johtuu maan halvasta energian hinnasta. [46]

3.4.2 Lahjoitukset ja airdropit

Kryptovaluuttoja voidaan saada myös lahjoituksina toisilta käyttäjiltä tai niin kutsuttuina Airdroppina. Lahjoitukset toimivat täysin samanlaisesti kuin pankkisiirroilla tehtävät lahjoitukset. Käytännössä riittää, että kryptovaluuttalompakon osoite on tiedossa kryptovaluutan lähettäjällä.

Airdropit taas ovat kryptovaluutan kehittäjien ja liikkeeseenlaskijoiden tekemiä lahjoituksia. Näitä tehdään, jotta kryptovaluutalle saadaan näkyvyyttä sosiaalisessa mediassa, jonka tavoitteena on tuoda uusia käyttäjiä valuutalle. Yleensä lahjoitettava summa ei ole suuri, vaan puhutaan maksimissaan muutamista kymmenistä dollareista. Mikäli kyseinen kryptovaluutta menestyy tulevaisuudessa, nousee myös kryptovaluutan arvo ja näin ollen airdropin antama tuotto on suurempaa.[47]

3.5 Kryptovaluutat sijoituskohteena

Nykyään kryptovaluutat ovat nostaneet päätään kiinnostavana sijoituskohteena sen tarjoamien pikavoittojen ansiosta ja jotkut sijoittajat näkevät esimerkiksi Bitcoinin digitaalisena kultana[48]. Kryptovaluutat perustuvat pohjimmiltaan samaan kuin kaikki muutkin valuutat, eli rahalla on vain arvoa, jos ihmiset uskovat sillä olevan arvoa.[49]

---

[45] https://www.asicminervalue.com/miners/innosilicon/g32-1800
[46] Ibinex: (n 28), 228
[47] Uutiskatsaus 3.6: Ethereum, kryptovaluuttaranking, Charie Shrem, airdrop (Bitcoinkeskus.com 3.6.2018)
[48] Bitcoinkeskus: (n 26)
[49] Bitcoinkeskus: (n 2)

Sijoituskohteena kryptovaluutat ovat nousseet suosioon juuri siksi, että niiden valtavat arvonmuutokset ovat saaneet paljon julkisuutta erilaisissa medioissa. Tämä johtuu osittain siitä, että markkina on suhteellisen pieni ja se perustuu pääosin spekulointiin, minkä vuoksi markkinoille muodostuu herkästi hintakuplia[50]. Tällaisesta hyvä esimerkki on, kun Bitcoinin arvo nousi 2016 vuoden alusta vuoden 2017 joulukuuhun mennessä noin 1000 dollarista noin 19000 dollariin[51].

Tästä syystä osa ihmisistä on alkanut sijoittamaan näihin, koska eivät halua jäädä paitsi suurista voitoista, vaan haluavat muiden mukaisesti rikastua. Tätä on ruokittu esimerkiksi erilaisilla keskustelupalstoilla esimerkiksi Redditissä, jossa ihmiset jakavat tietoa eri kryptovaluutoista ja antavat toisille sijoitusvinkkejä. Lisäksi kryptovaluuttojen avulla rikastuneista on uutisoitu suhteellisen näkyvästi. Sen sijaan muutamia varoittavia esimerkkejä on olemassa, joissa ihmiset ovat ottaneet huomattavia määriä lainaa ja sijoittanut sen kryptovaluuttoihin niiden ollessa suhdanne huipulla.

Kryptovaluuttojen arvonmääritys on haastavaa, verrattuna perinteisiin rahastoihin tai osakkeisiin, joissa yrityksen tekemä tulos ja tulevaisuuden näkymät vaikuttavat paljolti näiden arvonmuodostukseen. Kryptovaluutat ovat suhteellisen uusi sijoitusluokka, eikä niihin siksi ole löytynyt vielä oikeaa arvonmääritystapaa. Sijoittajat usein käyttävät samankaltaisia tapoja arvioida näitä kuin osakkeitakin.[52]

Kryptovaluuttojen arvo pohjautuu pääosin sen käyttämän teknologian ja käyttötarkoituksen arvoon. Eli mikäli kyseinen valuutta nähdään jollakin tapaa hyödylliseksi ja toimivaksi nostaa se kyseisen kryptovaluutan arvoa. Suurin osa kryptovaluutoista seuraa tällä hetkellä erittäin vahvasti Bitcoinin hintaa, mikä vaikuttaa oleellisesti kryptovaluuttojen arvonmuodostukseen.[53]

Koska kryptovaluuttoja ei olla pystytty sääntelemään samanlaisesti kuin osakemarkkinoita, on kryptovaluuttamarkkinoiden manipuloiminen helpompaa. Tämä tarkoittaa sitä, että ”valaat” eli suuromistajat tai pump and dump- ryhmät voivat heilutella markkinoita haluamal-

[50] Bitcoinkeskus (n 26)
[51] https://coinmarketcap.com/currencies/bitcoin/
[52] Bitcoinkeskus: (n 50)
[53] ibid

laan tavalla suhteellisen vapaasti. Näissä pump and dump- ryhmissä käyttäjät sopivat esimerkiksi, että he ostavat suurella summalla jotakin kryptovaluuttaa tiettynä hetkenä ja jakavat tästä aktiivisesti positiivisia uutisia. Tämä aiheuttaa sen, että kyseinen kryptovaluutta lähtee tämän vuoksi räjähdysmäiseen nousuun, mikä korostuu vielä markkinoilla olevien spekulatiivisten sijoittajien vuoksi, jotka haluavat tehdä pikavoittoja. Kun hinta on pumpattu tarpeeksi ylös alkavat ryhmän jäsenet myydä näitä saamalla huomattavat voitot ja viimeisimpänä kryptovaluuttaa ostaneet sijoittajat korjaavat tappiot itselleen laskevista kursseista.[54]

[54] ibid

4 KRYPTOVALUUTAT OSANA RIKOLLISTA TOIMINTAA

4.1 Millaisiin rikoksiin kryptovaluuttoja käytetään

Selvitin kryptovaluuttojen käyttöä rikollisessa toiminnassa ensin toteuttamalla teemahaastattelun 16.10.2019, jossa haastattelin rahanpesun selvittelykeskuksen kahta asiantuntijaa. Heidän mukaansa kryptovaluuttojen käyttö rikollisessa toiminnassa voidaan jakaa neljään pääkategoriaan: 1. kryptovaluutat laittomassa kaupankäynnissä maksuvälineenä, 2. kryptovaluutat rahanpesun välineenä, 3. kryptovaluutat rikoksen kohteena, sekä 4. kryptovaluutat rikollisten liiketoimintana. Lisäksi haastattelussa käsittelimme hieman yleisesti, mitä muuta teknologiaa kryptovaluutoilla tehtäviin rikoksiin läheisesti liittyy.[55]

Teemahaastattelun lisäksi tutustuin itse Darknetissä tapahtuvaan rikolliseen toimintaan, johon liittyy kryptovaluutat, käyttäen Tor-verkkoa. Käytän näistä sivustoista keräämiäni tietoja sekä kuvakaappauksia havainnollistavina esimerkkeinä. Kuitenkaan eettisistä syistä en tarkemmin mainitse näiden lähdetietoja. Seuraavaksi avaan näiden pääkategorioiden sisältöä sekä kryptovaluutoilla tehtäviin rikoksiin läheisesti liittyvää teknologiaa.

4.2 Kryptovaluutoilla tehtäviin rikoksiin läheisesti liittyvää teknologiaa

Tässä kappaleessa avaan teknologiaa, joka useimmiten esiintyy yhdessä kryptovaluuttoihin liittyvän rikollisen toiminnan kanssa. Tätä teknologiaa on huomattavasti enemmän, mutta avaan mielestäni tämän opinnäytetyön ymmärtämisen kannalta oleellisimmat teknologiat, jotka liittyvät läheisesti kryptovaluuttoihin liittyvään rikolliseen toimintaan.

4.2.1 Darknet

Internet voidaan jakaa kolmeen osa-alueeseen, joita ovat normaali internet, deep web ja dark web. Normaaliin internettiin kaikilla on pääsy internetselaimen kautta. Deep webin sisältöön sen sijaan ei ole mahdollista päästä ilman sisällön pyytämistä. Deeb webin palvelut siis vaativat käytännössä jonkin asteisen tunnistautumisen, ja palvelut voivat olla yksityisessä organisaation sisäisessä verkossa tai julkisessa internetissä. Tällaisista palveluista esimerkkinä toimii Facebook, jonka sisällön saa auki kirjautuessaan omilla käyttäjätunnuk-

[55] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)

silla palveluun. Palveluun ei siis pääse näkemään kaikkea sisältöä suoraan internetselaimen kautta.[56]

Deep web sekoitetaan usein Dark webiin, joka koostuu Darkneteistä[57]. Darknettien käyttö vaatii erillisen ohjelmiston, joita on useita. Näistä esimerkkejä ovat Tor, Freenet sekä I2P, joista Tor on yleisimmin käytössä.[58]

Lyhyesti kerrottuna Tor, eli the Onion router, mahdollistaa internetin selaamisen siten, että käyttäjän identiteetti ei paljastu. Tor-verkon toiminta perustuu siihen, että normaalin suoran yhteyden datan lähtöpisteen ja päätepisteen välillä sijasta, käytetäänkin data useiden tor-reitittimien kautta, jotka yksistään tietävät vain, mistä reitittimestä data on tälle tullut ja mihin se jatkaa matkaansa. Kuitenkaan yhden yksittäisen reitittimen avulla ei kyetä osoittamaan minkä välillä data oikeasti liikkuu. Usein reitti, jota pitkin data liikkuu, vaihtuu muutamien minuuttien päästä, jolla jäljittämistä pyritään vaikeuttamaan.[59]

Tor-verkko mahdollistaa erilaisten salattujen palveluiden luomisen, joihin ei ole mahdollista päästä normaalia internetyhteyttä käyttäen, vaan sivulle päästäkseen pitää olla tähän soveltuva ohjelmisto käytössä, jota kutsutaan Tor-selaimeksi.[60] Lisäksi Tor-verkkoa voidaan käyttää ihan tavalliseen internet selaamiseen, mikäli käyttäjä haluaa lisätä internetin käyttönsä yksityisyyttä.[61]

Tämä tor-verkko on kehitetty Yhdysvaltojen tiedustelua sekä armeijaa varten, jotta valtion toimijat voivat jakaa tiedustelutietoa ja sopia operaatioita internetin välityksellä paljastamatta omaa identiteettiään IP-osoitteen kautta. Tämän ongelmana oli se, että verkkoa käytti vain valtion virassa olevat, jolloin ei ollut epäselvyyttä siitä, kuka internetsivustolla vierai-

---

[56] How Big is the Dark Web? (track.torproject.org)
[57] ibid
[58] David Glance: What Is The Dark Web? (theconversation.com 13.8.2015)
[59] Tor: Overview (torproject.org)
[60] Torproject: (n 56)
[61] Paul F. Syverson, Michael G. Reed, David M. Goldschlag: Private Web Browsing (Naval Research Laboratory 2.6.1997, 2)

lee käyttäen tor-selainta. Siksi tor-verkkoon oli saatava muita käyttäjiä, jolloin siitä saataisiin anonyymimpi ja se julkaistiin yleiseen käyttöön.[62]

4.2.2 Viestintäpalvelut

Kryptovaluutoilla tehtäviin rikoksiin liittyy myös läheisesti erilaiset viestintäpalvelut, joilla tavoitellaan yksityisempää keskusteluyhteyttä esimerkiksi kaupanteon yhteydessä. Tor-verkossa vieraillessani huomasin, että varsinkin Suomessa Wickr- sovellus on varsin yleisesti käytössä, kun kryptovaluuttojen avulla tehdään muun muassa huumekauppaa. Näiden lisäksi käytössä on muitakin sovelluksia kaupanteon yhteydessä.[63] Wickr- sovellus mahdollistaa salatun viestinnän kahden tai useamman hengen kesken. Sovelluksella voidaan keskustelun lisäksi jakaa kuvia sekä videoita.[64] Vaikka käytössä on Wickr:in kaltaisia sovelluksia, käytetään tor-verkossa viestintään myös salattuja sähköposteja sekä keskustelualustoja.[65]

4.3 Kryptovaluutat maksuvälineenä laittomassa kaupankäynnissä

Kryptovaluuttoja käytetään nykyään monissa rikoksissa maksuvälineenä. Tämä johtuu siitä, että kryptovaluutat mahdollistavat kauppojen tekemisen siten, että ostajan ja myyjän ei varsinaisesti tarvitse tuntea toisiaan tai edes koskaan fyysisesti tavata.

Siksi suuri osa kaupasta tehdään Dark Netin välityksellä erilaisilla DarkMarketeilla tai keskustelufoorumeilla. Näillä foorumeilla myyjät ja ostajat piiloutuvat nimimerkkien taakse ja sopivat kaupat esimerkiksi Wickr- sovelluksen avulla. Jotkut myyjät eivät välttämättä edes jätä ilmoituksia itse, vaan ottavat yhteyttä ostoilmoituksiin.[66]

Kauppaa käydään edelleen myös normaalin internetin välityksellä, jota voidaan tehdä normaalin internetin kautta esimerkiksi keskustelufoorumeilla tai sähköpostitse.[67]

---

[62] Yasha Levine: Almost Everyone Involved in Developing Tor war (or is) Funded by the US Goverment (pando.com 16.6.2014)
[63] Katsaus tor-verkkoon (10/2019)
[64] Why Wickr (wickr.com)
[65] Katsaus tor-verkkoon (10/2019)
[66] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[67] ibid

Kaupankäynnin kohteena voi olla mikä tahansa rikollinen palvelu tai tuote. Näitä tuotteita ovat muun muassa huumausaineet, aseet, väärennökset, maksuvälineet tai lapsiporno.[68]

4.3.1 Huumausainekauppa

Huumausaineiden tai niiksi luokiteltujen lääkeaineiden luvaton käyttö, myyminen, maahantuonti, välittäminen, valmistaminen ja kasvattaminen on Suomessa laitonta. Näistä huumausainerikoksista on säädetty rikoslain luvussa 50.[69] Huumausaineiden myynti on siirtynyt suurissa osin verkkoon, jossa myyjät ja ostajat löytävät toisensa helpommin. Yhä edelleen kauppaa tehdään myös avoimesti, mutta huumausainekauppa sisältää huomattavia riskejä, kuten ryöstetyksi tulemisen, joita voidaan kyetä pienentämään siirtämällä toimintaa verkkoon.

Aikaisemmin huumekauppaa tehtiin täysin suomalaisessa Silkkitie-kauppapaikassa. Silkkitiellä käytettiin Bitcoinia maksuvälineenä ja huumausaineet toimitettiin postitse. Sekä myyjät, että ostajat olivat suomalaisia. Juha Nurmi tutki väitöskirjassaan, Silkkitiellä käytävää huumausainekauppaa ja huomasi, että alle vuodessa huumausaineita myytiin jopa yli kahden miljoonan euron edestä Silkkitien kautta.[70]

Silkkitien, joka tunnettiin myös nimellä Valhalla, verkkopalvelimet takavarikoitiin ja sivusto suljettiin Tullin ja ulkomaalaisten viranomaisten yhteistyönä vuonna 2019[71]. Loppuvaiheessa sivustolla oli rekisteröitynä 1,15 miljoonaa ostajaa ja 5400 myyjää, jotka tekivät kansainvälisesti huumekauppaa, joka toteutettiin Bitcoinin ja Moneron välityksellä[72].

Nykyään käyttäjät ovat siirtyneet muille alustoille ja Suomessa yksi suosituimpia huumausaineiden kauppapaikkoja on Torilauta, joka toimii Tor-selaimella. Torilaudalla myydään

---

[68] ibid
[69] Rikoslaki 50 luku (39/1889, RL)
[70] Juha Nurmi: Understanding the Usage of Anonymous Onion Services, (Tampereen yliopisto 24.5.2019, 66)
[71] Suomen tulli takavarikoi Silkkitien verkkopalvelimen sisällön – merkittävä onnistuminen anonyymissä Tor-verkossa (tulli.fi 3.5.2019)
[72] Double blow to dark web marketplaces (europol.europa.eu 3.5.2019)

huumausaineita ympäri Suomea ja siellä on omat keskustelualueensa Suomen suurimmille kaupungeille.[73]

4.3.2 Laiton asekauppa

Ampuma-aseet ovat Suomessa luvanvaraisia ja niiden hallussapidosta, myymisestä, valmistamisesta, ynnä muusta on säädetty ampuma-aselaissa. *”Ampuma-aseella tarkoitetaan välinettä, jolla ruutikaasunpaineen, nallimassan räjähdyspaineen tai muun räjähdyspaineen avulla voidaan ampua luoteja, hauleja tai muita ammuksia taikka lamaannuttavia aineita. Ampuma-aseeksi katsotaan myös sellainen esine, joka on suunniteltu paukkupatruunoiden laukaisemista varten, jollei sen muuttamista 1 momentin mukaiseksi ole teknisesti estetty. Sisäministeriön asetuksella säädetään teknisistä vaatimuksista muuttamisen estämiseksi. Ampuma-aseeksi katsotaan myös muu esine, joka muistuttaa ampuma-asetta ja joka rakenteensa tai valmistusmateriaalinsa puolesta on muutettavissa ampuma-aseeksi.[74]”*

Laittomalla asekaupalla on monia yhtymäkohtia huumausainekauppaan DarkNetissä. DarkNetissä myynti tapahtuu pääsääntöisesti kryptomarkettien tai yksityisten myyjien ylläpitämien sivustojen kautta. Kryptomarketeissa on useita eri myyjiä, joista ostajat voivat valita mieleisensä. Näille marketeille ominaista on, että ostajat maksavat aseiden hinnan marketille, joka välittää rahat myyjälle, kun ostaja on saanut tuotteensa. Maksut suoritetaan kryptovaluutoilla ja ostajat voivat antaa palautetta ostotapahtumasta, joka julkaistaan marketin sivuilla. Toimitettavat aseet lähetetään postitse, usein osissa ja mahdollisimman huomaamattomasti.[75]

Moni myyjistä haluaa välttää kryptomarkettien välityspalkkiot sekä kryptomarketin mahdollisen exit-scamin ja siksi he myyvät aseita omilla sivuillaan DarkNetissä[76]. Exit-scam tarkoittaa sitä, että valuutantarjoaja, kryptovaluuttapörssi tai muu palvelu lopettaa toimintansa samalla pitäen kaikki asiakkaidensa varat.

---

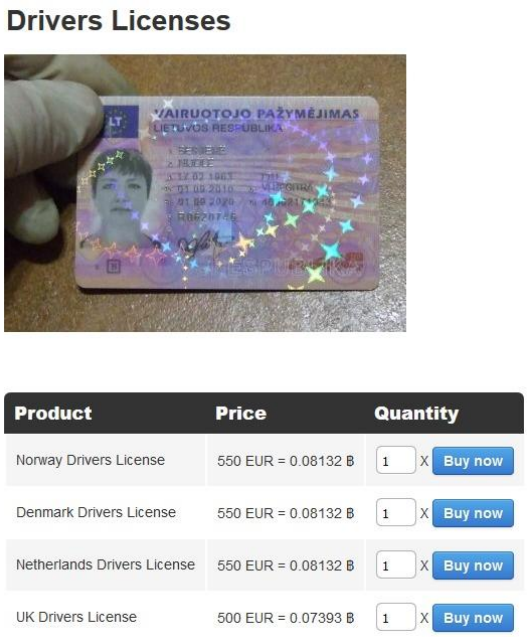
[73] Katsaus tor-verkkoon (10/2019)
[74] Ampuma-aselaki §2 (1998/1)
[75] Giacomo Persi Paoli: The trade in small arms and light weapons on the dark web (Unoda occasional papers no. 32 10/2018, 13)
[76] ibid

4.3.3 Väärennökset

Kryptovaluuttojen avulla kaupataan monenlaisia väärennöksiä, mutta selkeästi yleisimpiä on erilaiset henkilötodistukset ja käteinen raha. Esimerkiksi väärennettyjä seteleitä myydään Darknetissä useilla sivustoilla.[77]

Väärennettyä käteistä rahaa on myynnissä useissa eri valuutoissa. Pääsääntöisesti väärennökset painottuvat isoihin seteleihin. Väärennöksien hinta on huomattavasti alhaisempi kuin oikean rahan arvo, mutta silti merkittävä. Esimerkiksi yhdellä Darknetin kauppapaikalla väärennetyistä 100 euron seteleistä pyydetään 25 euroa kappaleelta ja 500 euron väärennetyistä seteleistä 85 euroa kappaleelta. Maksut suoritetaan pääsääntöisesti käyttäen Bitcoin kryptovaluuttaa.[78]

Darknetissä myydään myös eri maiden väärennettyjä henkilöllisyystodistuksia ja ajokortteja muun muassa Bitcoinin avulla. Näihin henkilöllisyystodistuksiin ja ajokortteihin on mahdollista saada oma valokuva ja näihin kortteihin on pääsääntöisesti yritetty tehdä mahdollisimman aidon näköiset turvatekijät. Kuvassa 1, on esimerkki Bitcoinilla myytävästä ajokortista, jossa on jäljitelty ajokortin turvatekijöitä.[79]



Kuva 1. Esimerkki Bitcoinilla myytävästä ajokortista, jossa jäljitelty kortin turvatekijöitä.

[77] Katsaus tor-verkkoon (10/2019)
[78] ibid
[79] ibid

Näiden väärennösten lisäksi verkossa kaupataan muun muassa väärennettyjä lääkkeitä, jotka ovat järjestäytyneen rikollisuuden suuri tulonlähde. Väärennettyjä lääkkeitä myydään useimmiten laittomissa verkkoapteekeissa, joiden toiminta on hajautettua usein eri maihin, jotta niiden jäljittäminen olisi haastavampaa. Nämä verkkoapteekit ovat sivustoiltaan usein rakennettu mahdollisimman siisteiksi, jotta kuluttajan on helppo luottaa toimintaan.[80]

4.3.4 Maksuvälineet

Kuten aikaisempiakin tuotteita, myös maksuvälineitä myydään eteenpäin kryptovaluuttojen avulla. Maksuvälineitä ovat muun muassa käteinen raha sekä luotto- ja pankkikortit. Kryptovaluutoilla tehtävässä kaupankäynnissä rikollisuus kohdistuu lähinnä maksukortteihin. Näiden kauppaaminen, on yleensä seurausta kortteihin kohdistuneesta rikollisuudesta, jossa joko maksuväline tai sen sisältämät tiedot pyritään saamaan rikollisen haltuun[81].

Maksuvälineet kiinnostavat rikollisia, koska niiden avulla saadaan käteistä rahaa[82]. Esimerkiksi, mikäli rikollinen haluaa vaihtaa kryptovaluuttansa FIAT-valuutaksi, on maksuvälineen ostaminen yksi keino tehdä niin.

Maksuvälinerikoksista on säädetty rikoslain luvussa 37, jossa maksukortteja koskevat rikokset ovat törkeä-, lievä-, ja perusmuotoinen maksuvälinepetos sekä maksuvälinepetoksen valmistelu.[83] Lisäksi maksukorteilla tehtäessä kauppaa, voidaan syyllistyä rahanpesuja kätkemisrikoksiin.[84] Maksuvälinerikokset ovat alkurikoksia, jotka mahdollistavat maksuvälineiden myymisen Darknetissä.

Osa Darknetissä toimijoista myy haltuunsa saamia paypal- käyttäjätilejä, pankkikortteja tai pankkitunnuksia eteenpäin. Näiden hinnat riippuvat siitä, kuinka paljon tileillä on rahaa,

[80] Sami Paaskoski: Uhkapeliä laittomilla nettilääkkeillä (sic.fimea.fi 29.9.2012)
[81] Maksukorttirikollisuus on kasvava rikosilmiö (poliisi.fi)
[82] ibid
[83] Rikoslaki 37 luku (39/1889, RL)
[84] Rikoslaki 32 luku (39/1889, RL)

missä pankissa tai palvelussa ne ovat käytössä ja kuinka paljon käyttöoikeuksien haltijoita on olemassa. Näitä vaihdetaan Darknetissä pääsääntöisesti Bitcoin-kryptovaluuttaan.[85]

4.3.5 Palvelut

Darknetissä on useita eri sivustoja, jotka ovat urautuneet joihinkin tiettyihin palveluihin. Lisäksi palveluita on tarjolla myös erilaisilla keskustelufoorumeilla, joista suurin osa on ulkomaalaisia.[86] Palveluita voi olla fyysiset toimeksiannot tai vaihtoehtoisesti pääsy palvelun kautta johonkin materiaaliin. Fyysisistä palveluista esimerkkeinä toimivat erilaiset palkkamurhaajapalvelut ja hakkerointi. Näitä palveluja ostetaan pääsääntöisesti Bitcoinia käyttämällä.[87] Palkkamurhaajapalveluissa on selvitetty mitä palveluja on mahdollista ostaa. Lisäksi kuvan 2 alalaidassa on tilauksen ehdot, joista ensimmäinen on Bitcoinilla maksaminen.

[85] Katsaus tor-verkkoon (10/2019)
[86] ibid
[87] ibid

Kuva 2. Esimerkki palkkamurhaajan palveluista Darknetissä, jotka maksetaan Bitcoinia käyttämällä.

Hakkeroinneissa tarjonta on suurta ja sitä voidaan kohdistaa niin valtion eri toimielimiä kuin yksityishenkilöitäkin kohtaan. Valtion tietoelimiltä voidaan yrittää hakkeroida erilaista dataa, joilla voidaan vaikuttaa muun muassa poliittisesti korkeassa asemassa olevien uraan. Yksityishenkilöiden kohdalla taas suurin osa tarjonnasta kohdistuu yksittäisten henkilöiden sosiaalisiin medioihin, tietokoneiden webkameroihin tai puhelimiin.[88]

Toiset palvelut tarjoavat pääsyn materiaaleihin, joita heillä on jo käytössään. Nämä palveluntarjoajat tarjoavat muun muassa pääsyn toisten ihmisten tietoihin, kuten spotify- tunnuksiin ja myyvät ohjeita eri alan rikollisuuteen tai ne tarjoavat pääsyn seuraamaan livelähetyksiä erilaisista väkivallanteoista, kuten kiduttamisesta. Toisten ihmisten tietoihin pääsystä esimerkkinä toimii Tor-verkosta löytämäni palvelu, joka kauppasi muun muassa vaikutusvaltaisten henkilöiden henkilötietoja.[89]

Osa palveluntarjoajista kauppaa myös anastettua omaisuutta. Suurin osa näistä anastetuista tuotteista ovat erilaista elektroniikkaa tai työkaluja. Elektroniikan osalta Darknetissä kaupattiin eniten Iphone-puhelimia sekä erilaisia kannettavia tietokoneita. Työkalujen osalta eniten tarjontaa tuntui olevan pienistä, mutta arvokkaista työkaluista, kuten akkuporakoneista.[90] Näitä tuotteita kaupataan paljon myös erilaisilla keskustelualustoilla sekä internetin puolella. Internetin puolella kaupattavien tavaroiden osalta niiden alkuperää ei kuitenkaan normaalisti juurikaan ilmoiteta.

Rikollisten palveluiden ostamisessa tekijä voidaan tuomita rikoslain viidennen luvun mukaan yllytyksestä, avunannosta tai rikoskumppanina toimimisesta tehtyyn rikokseen liittyen.[91]

---

[88] ibid
[89] ibid
[90] ibid
[91] Rikoslaki 5:3-6§ (39/1889, RL)

4.3.6 Lapsiporno

Rikoslain 17- luvun pykälissä 18§, 18 a§, ja 19§ käsitellään kuva- ja videotallenteita, jotka sisältävät lasten sukupuolisiveellisyyttä loukkaavaa materiaalia. Nämä ovat rikoslaissa määritelty laittomiksi, mikä tarkoittaa, että näiden hallussapitokin on yksistään rangaistavaa, kuten niiden levittäminenkin. Lapsina näissä rikoksissa käsitellään kaikki alle 18-vuotiaat. [92] Yleisesti näistä materiaaleista puhutaan lapsipornona.

Suurin osa lapsipornosta on nykyään sähköisessä muodossa ja sitä levitetään muun muassa Darknetin välityksellä. Darknet on mahdollistanut rikollisille helpomman tavan levittää ja tallentaa materiaalia, siten että kiinnijäämisen riski on pienempi. Darknetissa kauppaa näillä kuvilla ja videoilla käydään esimerkiksi Bitcoinilla. [93]

Yleensä näiden rikosten takana toimivat yksittäiset henkilöt, eikä varsinaista rikollisjärjestöä ole tekojen tai materiaalin jakamisen takana. Nämä yksittäiset henkilöt verkostoituvat keskenään esimerkiksi internet- tai darknet foorumien kautta. Verkostoituminen aiheuttaa sen, että nämä henkilöt jakavat video- ja kuvamateriaalin lisäksi ohjeita toisilleen aiheesta, miten välttää kiinnijäämistä.[94]

Kuvien ja videoiden lisäksi nykyään lapsipornoa myös live-streamataan eli lähetetään sosiaalisen median, applikaatioiden sekä keskustelualustojen kautta livelähetystä. Näitä lähetyksiä lähetetään pääsääntöisesti EU-alueen ulkopuolelta ja siksi kryptovaluutoiden käyttö ei ole vielä kovin yleisesti käytettyjä maksuvälineitä näiden live-lähetysten maksamisessa, koska niiden vaihtaminen FIAT-valuutaksi on haastavaa.[95]

---

[92] Rikoslaki 17 luku (39/1889, RL)
[93] Internet Organised Crime Threat Assessment 2018 (Europol, 21-31)
[94] Ibid, 33
[95] Ibid, 35

4.4 Kryptovaluutat rahanpesun välineenä

Rahanpesu on määritelty rikoslaissa seuraavanlaisesti ” *Joka*
1) ottaa vastaan, käyttää, muuntaa, luovuttaa, siirtää, välittää tai pitää hallussaan rikoksella hankittua omaisuutta, rikoksen tuottamaa hyötyä tai näiden tilalle tullutta omaisuutta hankkiakseen itselleen tai toiselle hyötyä tai peittääkseen tai häivyttääkseen hyödyn tai omaisuuden laittoman alkuperän tai avustaakseen rikoksentekijää välttämään rikoksen oikeudelliset seuraamukset taikka
2) peittää tai häivyttää rikoksella hankitun omaisuuden, rikoksen tuottaman hyödyn taikka näiden tilalle tulleen omaisuuden todellisen luonteen, alkuperän, sijainnin tai siihen kohdistuvat määräämistoimet tai oikeudet taikka avustaa toista tällaisessa peittämisessä tai häivyttämisessä,
on tuomittava rahanpesusta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
Yritys on rangaistava.[96] *”.*

Haastattelemieni rahanpesun selvittelykeskuksen asiantuntijoiden mukaan kryptovaluutat ovat nykyään lunastaneet paikkansa osana rahanpesua. Kryptovaluutoilla pyritään piilottamaan ja häivyttämään rahan alkuperää, joka on hankittu rikollisin keinoin.[97]

Rahanpesu on aina seurausta jostakin alkurikoksesta, joka voi olla mikä tahansa rikos, mistä rikoksen tekijät saavat taloudellista hyötyä, esimerkiksi huumausainekauppa tai veronkierto. Käytännössä siis rahanpesun takana voi toimia yksityinen henkilö, yhteisö tai vaikkapa yritys, joka harjoittaa laitonta liiketoimintaa. Rikoshyöty voi olla hankittu alun perin kryptovaluuttana tai se on voitu muuttaa kryptovaluutaksi rahanpesua varten.[98]

Kryptovaluutat ovat nykyään suuri osa rahanpesutoimintaa ja esimerkiksi finanssivalvonta on luokitellut kryptovaluuttoja koskevan rahanpesun riskin korkeaksi. Tämän vuoksi EU:n rahanpesudirektiiviin on tehty muutos, joka tuo kryptovaluutan vaihtopalvelut sekä lompakkopalvelut sääntelyn piiriin.[99]

---

[96] Rikoslaki 32:6§ (39/1889, RL)
[97] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[98] ibid
[99] Hanna Heiskanen: Virtuaalivaluuttoihin liittyvien palvelun tarjoajille ehdotetaan sääntelyä ja rekisteröintiä Finanssivalvontaan (Finanssivalvonta 19.9.2018)

Rahanpesijät käyttävät erilaisia tekniikoita rahan alkuperän häivyttämiseksi ja kryptovaluuttojen muuttamista FIAT-valuutaksi. Näihin tekniikoihin, joihin sisältyy suurempi rahanpesun riski, pyritään puuttumaan voimaan tulevalla sääntelyllä.[100]

4.4.1 Terrorismin rahoittaminen

Kryptovaluuttoihin on liitetty myös suuri terrorismin rahoittamisen riski.[101] Kryptovaluutat ovat antaneet terroristijärjestöille mahdollisuuden siirtää rahavaroja ilman varsinaista pankkiliikennettä. Esimerkiksi terroristijärjestö ISIS otti bitcoinin sekä toisen kryptovaluutan käyttöönsä 2017, jolloin ISIS alkoi ohjailemaan saamiansa lahjoituksia kryptovaluuttalompakkoihin, joita sivusto laati heille. Sen jälkeen ISIS siirtyi vastaanottamaan lahjoituksia myös prepaid-maksukorteille, joille talletetaan bitcoinia. Näitä varoja on käytetty muun muassa internetsivujen ylläpitoon sekä taistelijoiden varustamiseen. Vaikka kryptovaluutat ovatkin integroituneet osaksi terroristijärjestöjen käyttöön, ei tämä kuitenkaan ole heidän ainoa rahoitustapansa vaan osa rahaliikenteestä kulkee edelleen normaalien pankkitilien kautta. [102]

Terrorismin rahoittamisesta on säädetty rikoslaissa, jonka pykälien 34a:5§ ja 34a:5a§ mukaan rangaistaan sitä, joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen terroristista toimintaa tai terroristiryhmää tietoisesti.[103]

4.4.2 Pakotteiden kiertäminen

Kansainväliset pakotteet ovat tiettyihin valtioihin tai tiettyihin ryhmiin kohdistuvia toimia, joilla rajoitetaan tai keskeytetään kaupallinen tai taloudellisen yhteistyö, liikenne- ja viestiyhteydet tai diplomaattisia suhteet. Pakotteilla pyritään vaikuttamaan valtion tai ryhmän harjoittamaan kansainvälistä rauhaa sekä turvallisuutta uhkaavaan toimintaan.[104] Pakotteet voidaan kohdistaa myös nimettyihin henkilöihin ja yhteisöihin, jonka ansiosta pakotteista ei koidu yhtä laajaa negatiivista vaikutusta siviiliväestöön. Tämä mahdollistaa käytännössä

---

[100] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[101] Hanna Heiskanen: Virtuaalivaluuttoihin liittyvien palvelun tarjoajille ehdotetaan sääntelyä ja rekisteröintiä Finanssivalvontaan (Finanssivalvonta 19.9.2018)
[102] Internet Organised Crime Threat Assesment 2018 (Europol, 53)
[103] Rikoslaki 34a:5§ ja 34a:5a§ (39/1889, RL)
[104] Kansainväliset pakotteet (um.fi)

pakotteiden kohdentamisen juuri siihen tahoon, joka on vastuussa vastustettavasta politiikasta.[105]

Pakotteita voi asettaa yhdistyneiden kansakuntien (YK) turvallisuusneuvosto tai Euroopan Unionin (EU) neuvosto. YK:n turvallisuusneuvoston asettamat pakotteet koskevat kaikkia YK:n jäsenvaltioita. EU:ssa nämä pakotteet pannaan täytäntöön EU-tason lainsäädännöllä. Nämä lait ovat jokaisen jäsenvaltion osalta sitovia ja jokaisen jäsenvaltion viranomaisten sekä yksityisten toimijoiden on noudatettava näitä.[106]

Pakotteista Suomessa määrää Laki eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä. Mikäli tätä lakia rikkoo tai yrittää rikkoa, voidaan tuomita Rikoslain 46:1-3§ mukaan.[107] Nämä rikosnimikkeet ovat säännöstelyrikos, lievä säännöstelyrikos ja törkeä säännöstelyrikos.[108] Säännöstelyrikokseen syyllistyy yksityinen henkilö tai toimija: *” Joka rikkoo tai yrittää rikkoa*
1) eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä annetussa laissa (659/1967),
2) valuuttalaissa (954/1985),
3) hintasulusta annetussa laissa (717/1988),
4) valmiuslaissa (1552/2011),
5) kansainvälisestä energiaohjelmasta tehdyn sopimuksen eräiden määräysten hyväksymisestä ja sopimusten soveltamisesta annetussa laissa (1682/1991),
6) ulkomaankaupan hallinnosta sekä tarkkailu- ja suojatoimenpiteistä eräissä tapauksissa annetussa laissa (1521/1994),
7) Euroopan unionin antamissa tuontia ja vientiä koskevissa asetuksissa,
8) kaksikäyttötuotteiden vientivalvonnasta annetussa laissa (562/1996) tai
9) Euroopan unionin yhteisen ulko- ja turvallisuuspolitiikan alaan kuuluvissa Euroopan unionin toiminnasta tehdyn sopimuksen 215 artiklan nojalla talous- ja rahoitussuhteiden keskeyttämisestä kolmannen maan kanssa tai rajoittavien toimenpiteiden kohdistamisesta

---

[105] ibid
[106] ibid
[107] Laki eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä 4§ (659/1967)
[108] Rikoslaki 46:1-3§ (39/1889, RL)

luonnollisiin tai oikeushenkilöihin, ryhmiin tai muihin kuin valtiollisiin yhteisöihin annetuissa asetuksissa
säädettyä tai mainittujen säädösten nojalla annettua säännöstelymääräystä, on tuomittava säännöstelyrikoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
(24.4.2015/506)
Säännöstelyrikoksesta tuomitaan myös se, joka rikkoo varojen jäädyttämisestä terrorismin torjumiseksi annetun lain (325/2013) 6 §:ssä säädettyä kieltoa siirtää tai muuntaa varoja taikka 7 §:ssä säädettyä kieltoa luovuttaa varoja. (3.5.2013/326)".[109]

Vaikka pakotteet ovat useissa maissa sitovia, silti pakotteita pyritään kiertämään. Yksi keino pakotteiden kiertämiseen on löydetty kryptovaluutoista. Esimerkiksi Venezuela kehitti oman valtiollisen kryptovaluutan, jotta maa onnistuisi kiertämään Yhdysvaltojen asettamia talouspakotteita.[110]

4.5 Kryptovaluutat rikoksen kohteena

4.5.1 Kryptovaluuttapörsseihin kohdistuvat rikokset

Kryptovaluuttapörsseihin kohdistuu pääsääntöisesti kahden tyylisiä rikoksia. Näitä ovat pörssien hakkeroinnit tai tilien kalastelu valesivujen avulla. Pörssien hakkeroinnissa pyritään anastamaan kryptovaluuttapörssissä olevaa valuuttaa siirtämällä se pörssistä hakkereiden tilille.[111] Näistä rikoksista on säädetty rikoslain 38-luvussa.[112]

Kryptovaluuttapörssien hakkeroinnissa taas hakkerit pyrkivät murtautumaan kryptovaluuttaa pörssien tietoturva-aukkojen avulla sisään ja anastamaan suoraan pörssistä kryptovaluuttaa tai valuuttoja. Nämä hakkeroinnit ovat houkuttelevia rikollisille, koska pörsseissä on huomattavan suuria summia säilytyksessä. Esimerkiksi Coincheck- nimiseen kryptovaluuttapörssiin hyökättiin ja hakkeroijat veivät yhteensä noin 430 miljoonan euron edestä kryptovaluutta NEM:iä.[113]

---

[109] ibid
[110] Kryptovaluutat kiehtovat myös valtioita (aamulehti.fi 25.2.2018)
[111] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[112] Rikoslaki 38-luku (39/1889, RL)
[113] Elina Hakola: Hakkerit lähtivät kryptovaluuttavarkaisiin Japanissa – saaliina 430 miljoonan euron edestä kolikoita (talouselämä.fi 30.1.2018)

Toinen yleisesti käytetty rikostyyppi on valesivu, jonka internetosoitteessa on pieni virhe ja sivuston käyttäjä ohjautuu rikollisten tekemälle sivustolle. Näissä osoitteissa käytetään usein kyrillisiä aakkosia, joilla korvataan yksi merkki, jolloin internetosoite näyttää päällisin puolin samanlaiselta kuin oikeakin osoite. Näistä sivustoista pyritään tekemään ulkonäöltään samanlaisia, kuin oikeista sivuista, jotta käyttäjä ei huomaisi eroa ja yrittäisi kirjautua käyttäjätunnuksillaan sivulle. Jos käyttäjä kirjautuu, hänen kirjautumistunnuksensa taltioidaan ja niillä kirjaudutaan oikeaan kryptovaluuttapörssiin ja sitä kautta anastamaan tämän tilin kryptovaluutat.[114]

4.5.2 Käyttäjiin kohdistuvat rikokset

Kryptovaluuttojen käyttäjiin suoranaisesti kohdistuvat rikokset voidaan jakaa kolmeen eri kategoriaan. Näitä ovat tilien hakkeroinnit, kiristykset ja petolliset treidit.[115]

Tilien hakkeroinnissa hakkerit onnistuvat murtautumaan kryptovaluutan omistajan tilille ja anastamaan tämän varat. Kuitenkaan yksittäiset tilit eivät luultavimmin ole hakkereille yhtä mielenkiintoisia kohteita, kuin kryptovaluuttapörssit, koska niissä ei ole yhtä suuria määriä kryptovaluuttaa. Hakkerointien osalta rangaistaan rikoslain 38:8§ ja 38:8a§ pykälien mukaan[116].

Kryptovaluutoilla kiristäminen toteutetaan pääsääntöisesti Ransomwaren avulla, mutta maailmalla on ollut myös tapauksia, joissa kryptovaluuttojen suuromistajia, merkittäviä henkilöitä tai näiden läheisiä on kaapattu ja lunnaat ovat vaadittu maksamaan kryptovaluutoilla.[117] Kiristyksestä rangaistaan rikoslain 31:3-4§ mukaisesti.[118]

Ransomware on kiristyshaittaohjelma, joka perustuu useimmiten kryptografiaan. Ransomwaren avulla otetaan tietokoneen käyttäjän koko tietokone tai internetselain haltuun ja näyttö lukitaan siten, että siinä esitetään lunnasvaatimus, jonka maksettua käyttäjä saa oh-

---

[114] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[115] ibid
[116] Rikoslaki 38:8§ ja 38:8a§ (39/1889, RL)
[117] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[118] Rikoslaki 31:3-4§ (39/1889, RL)

jeet siihen, miten tietokone saadaan taas toimintaan. Yleisesti nämä lunnaat käsketään maksamaan kryptovaluutoilla. Tällaiset vaatimukset saattavat olla jopa naamioitu jonkun valtion viranomaisen tekemäksi ja lunnasvaatimus on naamioitu sakoksi, joka pitää maksaa.[119]

Yleisesti tällaisia Ransomwareja levitetään internetissä naamioimalla näitä toisiksi ohjelmiksi. Esimerkiksi yksi yleinen tapa on pitää internetissä virustentorjuntaohjelmiston sivua, josta käyttäjä voi ladata kyseisen ilmaisen ohjelman. Mikäli käyttäjä lataa tämän luulemansa virustentorjuntaohjelman, lataakin hän oikeasti tämän ransomwaren tietokoneelleen.[120]

Kolmas kryptovaluuttojen käyttäjiin kohdistuvista rikoksista on petolliset treidit. Petolliset treidit pohjautuvat siihen, että ihmiset sopivat keskenään vaihtavansa kryptovaluuttaa FIAT-valuuttaan tai johonkin muuhun kryptovaluuttaan. Näitä treidejä voidaan sopia esimerkiksi jollakin keskustelupalstalla tai sivustoilla, jotka ovat tehty tätä varten. Tällaisia vaihtoja kutsutaan peer-to-peer treidiksi.[121] Peer-to-peer treideissä pyritään saamaan toinen osapuoli toteuttamaan vaihto, mutta itse jätetään oma osuus suorittamatta.

4.6 Kryptovaluutat rikollisten liiketoimintana

4.6.1 Exit-Scam

Exit-scam tarkoittaa sitä, että valuutantarjoaja, kryptovaluuttapörssi tai muu palvelu lopettaa toimintansa samalla pitäen kaikki asiakkaidensa varat. Usein kryptovaluuttamarkkinoilla Exit-scam:it pohjautuvat ICO:hin, joista valitettavan suuri osa on tehty pelkästään ihmisten huijaamiseksi.[122] Tästä on tehty arvio, jonka mukaan vuoden 2018 ensimmäisen kahdeksan kuukauden aikana ICO:issa tehdyissä Exit-scameissä on anastettu yli 100 miljoonaa dollaria sijoittajien varoja[123].

---

[119] Hilarie Orman: Evil Offspring – Ransomware and Crypto Technology (IEEE Internet Computing 7-8/2016, 89-90)
[120] ibid
[121] A Guide to Making Money with P2P Traiding in 2019 (blog.localcoinswap.com 28.4.2019)
[122] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[123] Yessi Bello Perez: What's a cryptocurrency exit scam and how do i spot one? (thenextweb.com 16.7.2019)

Näitä ICO:ssa julkaistuja uusia kryptovaluuttoja markkinoidaan sijoittajille jotenkin edistyksellisinä ja toiminta saattaa olla jopa hetken aikaa oikeasti toiminnassa, mutta se ei ole välttämätöntä exit-scammin toteuttamiseksi. Tällä tavoin näiden erottaminen oikeista ICO:ista on tehty haastavaksi.[124]

Kaikkialla maailmassa sääntely ei ole vielä välttämättä yhtä edistyksellistä kuin Suomessa. Suomessa ICO:t ovat sääntelyn piirissä, jonka avulla on kyetty ehkäisemään suomalaisten yritysten tekemiä exit-scammejä.[125]

Exit-scammejä tapahtuu myös Darknetissä. Siellä olevat markkinapaikat tai palvelut, jotka säilyttävät asiakkaidensa varoja ja toimittavat nämä myyjille, kun asiakas on saanut tuotteen, voivat toteuttaa myös tällaisen exit-scammin, jossa palvelussa tai markkinapaikassa säilytettävät varat anastetaan. Tällaisesta hyvä esimerkki on Wall Street Marketin exit-scam, jossa asiakkaiden Bitcoineja anastettiin yhteensä noin 30 miljoonan dollarin edestä.[126] Exit-scammit ovat suuren rahasumman vuoksi usein törkeitä kavalluksia.[127]

4.6.2 Markkinamanipulaatio

Kryptovaluuttamarkkinoiden manipulointi on kiellettyä tähän mennessä vain Saksassa. Koska markkinat eivät ole vielä kovinkaan säänneltyjä, on huomattavan yleistä, että kryptovaluuttamarkkinoilla esiintyy niin kutsuttua pump & dump toimintaa.[128]

Manipulointeja järjestävä taho voi olla yksittäisten ryhmien tai henkilöiden sijaan, joskus myös kryptovaluuttapörssi. Se miksi pörssit lähtevät mukaan tällaiseen toimintaan johtuu siitä, että tarjolla on suuria voittoja. Pörssi voi haalia hallintaansa huomattavan määrän jotakin yksittäistä kryptovaluuttaa, jonka se sitten myy markkinoille, kun on pumpannut hinnan korkealle. Lisäksi pörssi saa huomattavasti enemmän välityspalkkioita toteutuneista kaupoista, kun pumpattavan kryptovaluutan volatiliteetti nousee huomattavasti. Käynnissä

[124] ibid
[125] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[126] Jamie Redman: Darknet Users Allege Wall Street Market Exit Scammed, Possibly Snatching $30M (news.bitcoin.com 20.4.2019)
[127] Rikoslaki 28:5§ (39/1889, RL)
[128] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)

olevassa pump & dump tapahtumassa pörssit pystyvät hyödyntämään käyttäjien osto- ja myyntitoimeksiantojen tietoja paremmin, joka helpottaa heidän toimintansa ajoittamista.[129]

4.6.3 Sijoitushuijaukset ja pyramidiverkostot

Sijoitushuijaukset ovat nimensä mukaisesti huijauksia, joissa sijoittaja pyritään saamaan sijoittamaan johonkin instrumenttiin rahaa. Tällaiset sijoitushuijaukset pääsääntöisesti sisältävät vakuutteluja siitä, että kyseessä on hyvä sijoituskohde ja tuotot ovat paljon parempia, kun monessa muussa sijoitusinstrumentissa. Vakuuttelussa saatetaan käyttää hyväksi keksittyjä tarinoita. Tallaiset tarjoukset yleensä kertovat, kuinka heidän avullaan on mahdollista rikastua jo pienelläkin summalla.[130] Tämä toiminta on rahankeräyslain vastaista ja näistä rahankeräysrikoksista rangaistaan rikoslain 17 luvun 16c ja 16d §:n mukaan.[131]

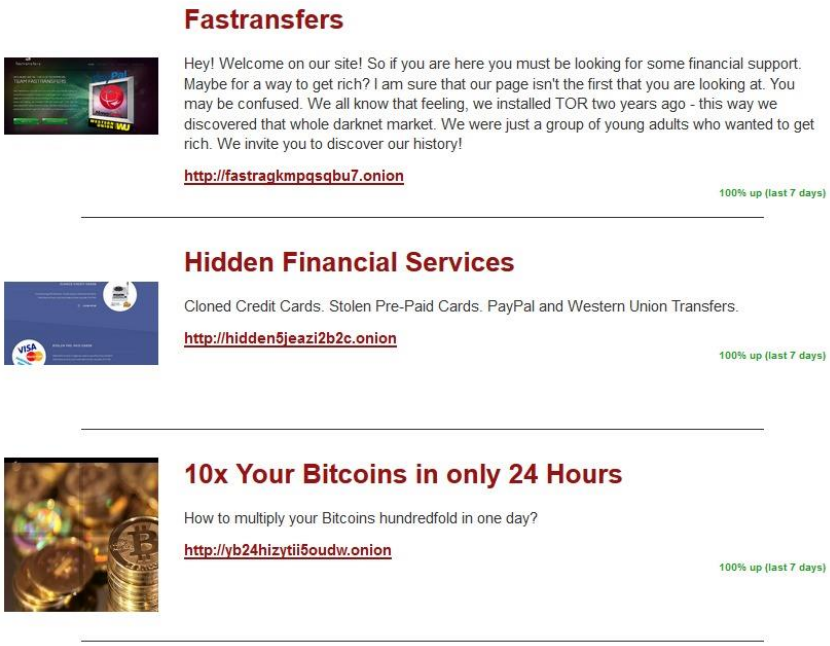
Esimerkiksi ponzi-huijauksissa uskotellaan sijoittajille, että perustajilla on jokin sijoituskohde olemassa tai kehitteillä, jonka avulla voidaan tienata huomattavia summia[132]. Ponzi-huijaukset pohjautuvat siihen, että uudet sijoittajat yhtyvät mukaan, jolloin järjestäjille ja ensimmäisille sijoittajille voidaan maksaa tuottoa. Ponzi-huijausten uusimmat sijoittajat ovat jo alusta asti tuomittuja menettämään sijoittamansa omaisuuden.[133]

Ponzi-huijaus päättyy yleensä, kun uusia sijoittajia ei tule enää markkinoille sijoituksessa mukana olevien paljouden vuoksi, tai siksi, että osa mukana olevista sijoittajista vaatii sijoittamaansa summaa takaisin.[134] Ponzi-huijauksen yksi muoto on pyramidihuijaus.

Kuvassa 3 esimerkki sijoituskohteesta, joka tarjoaa huomattavaa arvonnousua.

---

[129] Jiahua Xu ja Benjamin Livshits: The Anatomy of a Cryptocurrency Pump-and-Dump Scheme (usenix.org 28.8.2019, 1610)
[130] Tietoa Digihuijauksista (kuluttajaliitto.fi)
[131] Rikoslaki 17:16c§ ja 17:16d§ (39/1889, RL)
[132] U.S. Securities and Exchange Commission: Ponzi Schemes
[133] Weili Chen, Zibin Zheng, Edith Ngai, Peilin Zheng, Yuren Zhou: Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum (18.3.2019, 37576)
[134] Sec Enforcement Actions (U.S. Securities and Exchange Commission)



Kuva 3. Esimerkki sijoituskohteesta, joka tarjoaa huomattavaa arvonnousua.

Pyramidihuijaukset taas pohjautuvat verkostomarkkinointiin, jonka avulla pyritään värväämään uusia kauppiaita. Uusien verkostoon liittyvien kehotetaan yleisesti värväämään lisää edustajia verkostolle, jotta he saavat provision näiden tekemistä myynneistä. Edustajille usein väitetään, että heidän saamansa palkkio on peräisin hankkeen toiminnasta saaduista tuloista, vaikka tosiasiallisesti tulot ovat suoraan uusien asiakkaiden rahapussista.[135]

Kryptovaluuttamaailmassa pyramidiverkostot perustuvat yleensä koulutuspakettien myyntiin, vaikka toimijat väittävät tulojen lähteen olevan taustalla oleva lohkoketjuhanke.[136]

Useiden lähteiden perusteella yksi tällaisista huijauksista saattaa olla OneCoin-kryptovaluutta. OneCoin-kryptovaluutan oli määrä sivuuttaa Bitcoin markkinoiden suosituimpana kryptovaluuttana. Toiminnan on väitetty perustuvan siihen, että huijauksessa mukana olevat henkilöt myivät eri hintaisia koulutuspaketteja, joissa kerrottiin, kuinka kyseistä kryptovaluuttaa voitaisiin käyttää ja louhia. Lisäksi paketit sisälsivät optioita, jolla saa kryptovaluuttaa. Paketteja oli kuusi eri hintaista, joista kallein oli 25000 euroa. Jäse-

[135] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)
[136] ibid

neksi päästyään oli mahdollista myydä paketteja eteenpäin ja saada niiden hinnasta itselleen 10-25%.[137] Bloomberg-uutistoimiston mukaan kyseessä on pyramidihuijaus.[138]

4.7 Regulaatio Eu:ssa ja Suomessa

Kryptovaluuttojen käyttöä pyritään kansainvälisesti sekä kansallisesti säännöstelemään eli reguloimaan. Vuonna 2018 on tullut voimaan EU:n viides rahanpesudirektiivi, jonka vuoksi EU-tasolla kaikki kryptovaluuttapalvelujentarjoajat joutuvat allekirjoittamaan lain virtuaalivaluutoiden tarjoajista.[139]

Suomessa tämän direktiivin pohjalta on tullut 26.4.2019 voimaan Laki virtuaalivaluuttojen tarjoajista, jota sovelletaan virtuaalivaluutan tarjoajien harjoittamaan liiketoimintaan. Tämän lain mukaan jokaisen elinkeinoharjoittajan, joka tarjoaa virtuaalivaluuttoihin liittyviä palveluita joko päätoimintanaan tai satunnaisesti, on rekisteröidyttävä virtuaalivaluutan tarjoajaksi.[140]

Lisäksi Laki virtuaalivaluuttojen tarjoajista velvoittaa virtuaalivaluuttojen tarjoajaa suojaamaan asiakkaiden sekä toisten palveluntarjoajien varat, jotka tällä on hallussaan. Suurin tapahtunut edistysaskel regulaatiossa on ehkä se, että tämä laki velvoittaa palveluntarjoajan tuntemaan asiakkaansa.[141]

Lisäksi palveluntarjoajien asiakkaan tuntemista velvoittaa laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä. Mikäli palveluntarjoaja ei kykene toteuttamaan tunnistautumista ja noudattamaan tässä laissa annettuja säädöksiä, ei palveluntarjoaja saa solmia asiakassuhdetta kyseisen asiakkaan kanssa.[142]

---

[137] Jyri Hänninen: ”Haluatko tehdä miljoonan kuukaudessa?” – Uusi virtuaalivaluutta muistuttaa pyramidihuijausta (yle.fi 13.3.2016)

[138] Chris Dolmetsch: OneCoin Leaders Charged in Multibillion-Dollar Pyramid Scam (bloomberg.com 8.3.2019)

[139] Rahanpesun selvittelykeskuksen asiantuntijat (10/2019)

[140] Laki virtuaalivaluuttojen tarjoajista 1-4§ (572/2019)

[141] Laki virtuaalivaluuttojen tarjoajista 11-13§ (572/2019)

[142] Laki rahanpesun ja terrorismin rahoittamisen estämisestä 3:1§ (573/2019)

Nämä lait estävät sen, että kryptovaluuttoja pystyttäisiin käyttämään anonyymisti vaan pikemminkin pseudonyymisti, joka sekin on lakien vuoksi haastavampaa. Pseudonymisointi tarkoittaa käytännössä sitä, että henkilötietoja ei voida yhdistää tiettyyn henkilöön ilman lisätietoja. Anonymisointi sen sijaan tarkoittaa sitä, että tunnistaminen on estetty peruuttamattomasti siten, ettei rekisterinpitäjä tai muu ulkopuolinen taho voi sitä saada tunnistettua[143].

[143] Pseudonymisoidut ja anonymisoidut tiedot (tietosuoja.fi)

5 POHDINTA

5.1 Kirjallisuuskatsauksen analyysi ja johtopäätökset

Työn alkuvaiheessa esitin tutkimuskysymykseni: Mitä kryptovaluutat ovat ja miten niitä käytetään? Millaisiin rikoksiin kryptovaluuttoja käytetään ja millä tavoin?

Tutkiessani aihetta minulle selvisi, että kryptovaluutat ovat lohkoketjuteknologiaan perustuvaa virtuaalista valuuttaa, joka ei kuitenkaan ole saanut virallisen rahan statusta. Näillä kryptovaluutoilla on useita erilaisia käyttötarkoituksia, mikä näkyy myös rikollisuuden monimuotoisuudessa.

Kryptovaluuttojen käyttö rikollisessa toiminnassa voidaan jakaa neljään pääkategoriaan: 1. kryptovaluutat laittomassa kaupankäynnissä maksuvälineenä, 2. kryptovaluutat rahanpesun välineenä, 3: kryptovaluutat rikoksen kohteena sekä 4. kryptovaluutat rikollisten liiketoimintana. Yhteistä näille teemoille on se, että kryptovaluuttoja hyödynnetään rikoksen toteuttamisessa. Nämä rikostyypit eroavat huomattavasti toisistaan ja sen myötä myös kryptovaluuttojen osa rikoksen toteuttamisessa voi erota huomattavasti toisista rikoksista. Neljä esittelemääni kategoriaa jakavat selkeästi kryptovaluuttoihin liittyvän rikollisuuden, vaikka näiden kategorioiden alle mahtuukin useita erilaisia rikostyyppejä.

Osa näistä rikoksista voi ylittää näiden kategorioiden rajoja, kuten esimerkiksi Darknetissä toimivan huumausainekaupan tekemä exit-scam, jossa toimintaa pyöritetään jonkin aikaa, esimerkiksi vuoden verran, ja lopulta toiminnan pyörittäjä anastaa säilytyksessään olevat kryptovaluuttarajat.

Mielestäni kryptovaluutat rahanpesun välineenä on näistä kategorioista merkittävimmässä roolissa, koska lopulta jokaisen rikollisella tavalla hankitun varan alkuperä on häivytettävä, jos rahaa aiotaan käyttää normaalissa kaupankäynnissä. Onneksi tätä on huomattavasti vaikeutettu vuoden 2019 uudella EU:n rahanpesudirektiivillä. Tämä rahanpesudirektiivi avaa viranomaisille luultavasti yhä enemmän mahdollisuuksia taistelussa rahanpesua vastaan. Kun kryptovaluutan tarjoajien on varmistettava kryptovaluutoiden tosiasiallinen käyttäjä tulevat varat yhä helpommaksi jäljittää.

Luultavimmin kryptovaluuttojen käyttö tulee jatkossakin kasvamaan, ottaen huomioon tämän viimeisen kymmenen vuoden kehityshistorian. Tämä tarkoittaa, että myös rikollisuudessa nämä luultavasti jatkavat kehityskulkuaan ja yleistyvät enenevissä määrin. Regu-

laatio aiheuttaa rikollisuudelle haasteita, joka tarkoittaa sitä, että luultavasti osittain rikollisuus tulee muuttumaan ainakin osittain myös kryptovaluutoiden osalta.

Mielestäni valitsemani tutkimusmenetelmä soveltui erinomaisesti opinnäytetyöni tutkimuskysymysten selvittämiseen ja sen ansiosta koen saaneeni rakennettua kattavan perustietoa sisältävän yleiskatsauksen.

Ilman rahanpesun selvittelykeskuksen asiantuntijoiden teemahaastattelua olisi ollut huomattavasti vaativampaa jäsennellä rikollisuuden osa-alueita yhtä selkeästi. Tämä mahdollisti aiheen kirjallisen tutkimisen huomattavasti kattavammin, koska osasin etsiä oikeaa tietoa.

Darknettiin tekemäni katsaus taas auttoi havainnollistamaan sitä, millaista kryptovaluutoilla tehtävä rikollisuus on käytännön tasolla. Kuitenkaan näitä katsauksessa saatuja tietoja ei voida mielestäni yleistää koskemaan kaikkia tietyn tyylisiä rikoksia, koska samanlaisia sivustoja on useita, eikä kaikissa välttämättä käytetä edes kryptovaluuttoja rikoksen toteuttamiseksi.

Koska aihe on ollut huomattavan laaja, on sitä ollut mahdoton kuvata aihetta tai yksittäisiä kryptovaluuttoja yksityiskohtaisesti. Vaikka tieto osittain on hyvinkin pintapuolista, on mielestäni ollut tärkeää koota aihealueesta yleistietoa, jota halutessaan voi syventää.

Mielestäni opinnäytetyöni avaa lukuisia mahdollisuuksia jatkaa tutkimusta siitä mihin minun opinnäytetyöni päättyy. Esimerkiksi hyviä aiheita voisi saada jo pelkästään tutustumalla syvemmin pääkategorioihin tai tutkimalla sitä, kuinka kryptovaluutoilla tehtäviä rikoksia selvitetään tai ennaltaehkäistään.

Lisäksi hyviä tutkimusaiheita olisi määrälliset tutkimukset siitä, kuinka paljon mitäkin esittelemääni rikostyyppiä esiintyy ja millaisia rahasummia kryptovaluuttojen kautta liikkuu rikollisessa toiminnassa.

5.2 Opinnäytetyön eettisyys ja luotettavuus

Osa aineistosta on peräisin alalla toimivien yritysten artikkeleista, joka ei laadultaan välttämättä ole yhtä luotettavaa kuin alan tutkimukset. Alalla toimivat yritykset pääsääntöisesti ovat alansa ammattilaisia, joka nostaa mielestäni lähteiden luotettavuutta hieman.

Tutkimustietoa aiheesta on ollut saatavilla verrattain vähän, joten osittain aiheuttanut haasteita opinnäytetyön lähteiden hankkimisessa. Suuri osa käyttämistäni lähteistä on viranomaislähteitä, lakitekstiä tai aiheesta tehtyjä tutkimuksia, joita voidaan pitää yleisesti luotettavina lähteinä.

Asiantuntijoiden teemahaastattelun avulla saatua tietoa voidaan pitää luotettavana, koska he ovat alansa ammattilaisia ja alalla useita vuosia toimineita henkilöitä, jotka ovat työnsä puolesta perehtyneet aihealueeseen erityisen tarkasti.

Darknetistä ottamani näytteet ovat vain yksittäisiltä sivustoilta, eikä niiden suoria lähdeviittauksia olla työssäni tuotu esille eettisistä syistä. Tämän huonona puolena on se, että lukija ei voi arvioida itse lähteen luotettavuutta. Silti näen tämän ratkaisun perusteltuna lähteiden sisältämän materiaalin vuoksi.

Lisäksi näytteistä saatua informaatiota ei mielestäni voida yleistää näytteiden määrän ja valintakriteerien vuoksi. Näytteistä saatua informaatiota voidaan pitää faktatietona, koska kyseiset sivustot ovat rikollisten ”työvälineitä”, joissa on useita käyttäjiä ja selkeät toimintaohjeet. Opinnäytetyöni laajuuden kannalta saatu informaatio on ollut riittävää ja näiltä sivustoilta saaduilla tiedoilla on täydennetty muualta saatua informaatiota. Siksi näiden näytteiden voidaan katsoa tuovan luotettavuutta opinnäytetyöhöni.

Kokonaisuutena katsottaessa opinnäytetyötäni voidaan pitää luotettavana yleiskatsauksena, joka ei kuitenkaan ota huomioon yksittäisiä poikkeuksia eikä kaikkea saamaani tietoa voida yleistää.

Eettisyytensä puolesta opinnäytetyössäni ei ole esitetty suoria ohjeita rikollisen toiminnan kehittämiseksi tai sen toteuttamiseksi, eikä esimerkiksi tiettyjä palveluita, rikollisten hyödyntämiä kryptovaluuttoja tai suoria osoitteita rikollisia toimintoja tarjoavien palvelujen sivustoille ole tuotu esille opinnäytetyössäni.

LÄHTEET

Aamulehti 25.2.2018: Kryptovaluutat kiehtovat myös valtioita. Luettavissa: https://www.aamulehti.fi/paakirjoitukset/kryptovaluutat-kiehtovat-myos-valtioita-200767353

Ampuma-aselaki (9.1.1998/1)

Ankelo Johannes 13.11.2018: Ensiaskeleet ammattimaiseen treidaamiseen. Luettavissa: https://www.sijoitustieto.fi/sijoitusartikkelit/ensiaskeleet-ammattimaiseen-treidaamiseen

ASIC Miner Value: Innosilicon. Luettavissa: https://www.asicminervalue.com/miners/innosilicon/g32-1800

ASIC Miner Value: Miners profitability. Luettavissa: https://www.asicminervalue.com/

Binance 2019: Types of Order. Luettavissa: https://binance.zendesk.com/hc/en-us/articles/360033779452-Types-of-Order

Bitcoinkeskus 25.11.2019: Opas: valitse oikea Bitcoin-lompakko. Luettavissa: https://bitcoinkeskus.com/kryptovaluutta-lompakko/

Bitcoinkeskus 12.9.2019: Opas: Mikä on Ethereum? Luettavissa: https://bitcoinkeskus.com/ethereum-opas/

Bitcoinkeskus 18.7.2019: Miten kryptovaluuttojen arvo muodostuu? Luettavissa: https://bitcoinkeskus.com/miten-kryptovaluuttojen-arvo-muodostuu/

Bitcoinkeskus 15.4.2019: Opas: Mikä on Bitcoin? Luettavissa: https://bitcoinkeskus.com/bitcoin-opas/

Bitcoinkeskus 14.4.2019: Kryptovaluuttojen forkit: mitä ne oikein ovat? Luettavissa: https://bitcoinkeskus.com/kryptovaluuttojen-forkit-mita-ne-oikein-ovat/

Bitcoinkeskus 11.2.2019: Mikä on kryptovaluutta ja mihin sitä tarvitaan? Luettavissa: https://bitcoinkeskus.com/kryptovaluutta/

Bitcoinkeskus 3.6.2018: Uutiskatsaus 3.6: Ethereum, kryptovaluuttaranking, Charie Shrem, airdrop. Luettavissa: https://bitcoinkeskus.com/uutiskatsaus-3-6-ethereum-kryptovaluuttaranking-charlie-shrem-airdrop/

Bittimaatti: Automaattien sijainnit. Luettavissa: https://bittimaatti.fi/locations

Bittimaatti: Yritykset. Luettavissa: https://bittimaatti.fi/companies

Bittiraha: Denarium Custom Kultapäällystetty 2019. Luettavissa: https://bittiraha.fi/product/denarium-custom-kultapaallystetty-2019/

Chen Weili, Zheng Zibin, Ngai Edith, Zheng Peilin, Zhou Yuren, 18.3.2019: Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum. IEEE Access 18.3.2019. Luettavissa: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8668768

Coinmarketcap. Luettavissa: www.coinmarketcap.com

Dolmetsch Chris 8.3.2019: OneCoin Leaders Charged in Multibillion-Dollar Pyramid Scam. Bloomberg 8.3.2019. Luettavissa: https://www.bloomberg.com/news/articles/2019-03-08/onecoin-leaders-charged-in-u-s-with-operating-pyramid-scheme

Europol 3.5.2019: Double blow to dark web marketplaces. Luettavissa: https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

Europol 2018: Internet Organised Crime Threat Assessment 2018. Luettavissa: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

Giacomo Persi Paoli 2018: The trade in small arms and light weapons on the dark web. Unoda occasional papers no. 32 10/2018, 13. Luettavissa: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/10/occasional-paper-32.pdf

Glance David 13.8.2015: What Is The Dark Web? Saatavissa: http://theconversation.com/explainer-what-is-the-dark-web-46070

Hakola Elina 30.1.2018: Hakkerit lähtivät kryptovaluuttavarkaisiin Japanissa – saaliina 430 miljoonan euron edestä kolikoita. Talouselämä 30.1.2018. Luettavissa: https://www.talouselama.fi/uutiset/hakkerit-lahtivat-kryptovaluuttavarkaisiin-japanissa-saaliina-430-miljoonan-euron-edestakolikoita/017cd4f0-93f2-354c-98e5-f6c84183b8ed

Heiskanen Hanna 19.9.2019: Virtuaalivaluuttoihin liittyvien palvelun tarjoajille ehdotetaan sääntelyä ja rekisteröintiä Finanssivalvontaan. Finanssivalvonta 19.9.2019. Luettavissa: http://urn.fi/URN:NBN:fi:bof-201809252041

Hänninen Jyri 13.3.2016: ”Haluatko tehdä miljoonan kuukaudessa?” – Uusi virtuaalivaluutta muistuttaa pyramidihuijausta. Yle 13.3.2016. Luettavissa: https://yle.fi/uutiset/3-8736938

Ibinex 9.10.2018: Global Cryptocurrency Market Report. Luettavissa: https://media.ibinex.com/docs/Global_Cryptocurrency_Market_Report_2018.pdf

Kajaanin ammattikorkeakoulu: Perusjoukko, Otanta, Otos ja Näyte. Luettavissa: https://www.kamk.fi/fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Otantamenetelma

Kananen Jorma 2015: Opinnäytetyön kirjoittajan opas. Jyväskylä, Jyväskylän ammattikorkeakoulu.

Kryptokansalainen 12.12.2017: Perustiedot: Kryptovaluutat. Luettavissa: https://kryptokansalainen.fi/muut-kryptovaluutat/#coin

Kuluttajaliitto: Tietoa Digihuijauksista. Luettavissa: https://www.kuluttajaliitto.fi/hankkeet/huijarit-kuriin/tietoa-digihuijauksista/

Laki eräiden Suomelle Yhdistyneiden Kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä (659/1967)

Laki rahanpesun ja terrorismin rahoittamisen estämisestä (573/2019)

Laki virtuaalivaluuttojen tarjoajista (572/2019)

Levine Yasha 16.6.2014 Almost Everyone Involved in Developing Tor war (or is) Funded by the US Goverment. Luettavissa: https://pando.com/2014/07/16/tor-spooks/

Localcoinswap 28.4.2019: A Guide to Making Money with P2P Traiding in 2019. Luettavissa: https://blog.localcoinswap.com/a-guide-to-making-money-with-p2p-trading-in-2019/

Morris Liam: Anonymity analysis of Cryptocurrencies 4/2015. Luettavissa: https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=9771&=&context=theses&=&sei-re-dir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Dfi%2526as_sdt%253D0%25252C5%2526q%253DAnonymity%252Banalysis%252Bof%252BCryptocurrencies%2526btnG%253D#search=%22Anonymity%20analysis%20Cryptocurrencies%22

Nurmi Juha 24.5.2019: Understanding the Usage of Anonymous Onion Services. Tampereen yliopisto 24.5.2019, 66) ISBN 978-952-03-1091-2 (pdf) punamusta oy – yliopistopaino. Luettavissa: https://tutcris.tut.fi/portal/files/18769092/TUNI_nurmi.pdf

Orman Hilarie 2016: Evil Offspring – Ransomware and Crypto Technology. IEEE Internet Computing 7-8/2016. DOI: 10.1109/MIC.2016.90

Paaskoski Sami 29.9.2012: Uhkapeliä laittomilla nettilääkkeillä. Luettavissa: https://sic.fimea.fi/3_12/uhkapelia_laittomilla_nettilaakkeilla

Palmgren Johannes: Kryptovaluutan arvo kysynnan ja tarjonnan armoilla Luettavissa: http://www.finanssiala.fi/uutismajakka/Sivut/Kryptovaluutan-arvo-kysynnan-ja-tarjonnan-armoilla.aspx

Perez Yessi Bello 16.7.2019: What's a cryptocurrency exit scam and how do i spot one? Luettavissa: https://thenextweb.com/hardfork/2019/07/16/whats-a-cryptocurrency-exit-scam-and-how-do-i-spot-one/

Poliisi: Maksukorttirikollisuus on kasvava rikosilmiö. Luettavissa: https://www.poliisi.fi/rikokset/rikosilmioita/maksukorttirikollisuus

Rahanpesun selvittelykeskuksen asiantuntijat 10/2019. Vantaa 16.10.

Rantala Juho: Lohkoketjuteknologian yhteiskunta. Osa I: Bitcoinista Ethereumiin. niin & näin 1/2018. Luettavissa: https://netn.fi/sites/www.netn.fi/files/netn181-08.pdf

Redman Jamie 20.4.2019: Darknet Users Allege Wall Street Market Exit Scammed, Possibly Snatching $30M. Luettavissa: https://news.bitcoin.com/darknet-users-allege-wall-street-market-exit-scammed-possibly-snatching-30m/

Rikoslaki (39/1889, RL)

Salminen Ari: Mikä kirjallisuuskatsaus? (Vaasa 2011, 6-7) Luettavissa: https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Storås Niclas 2016: Lohkoketjuteknologia pähkinänkuoressa – tämä kannattaa tietää. Luettavissa: https://www.tivi.fi/uutiset/lohkoketjuteknologia-pahkinakuoressa-tama-kannattaa-tietaa/10d8a2ff-981a-3751-b881-df66fc52cdde

Syverson Paul F., Reed Michael G., Goldschlag David M.: Private Web Browsing. Naval Research Laboratory 2.6.1997. Luettavissa: https://www.onion-router.net/Publications/JCS-1997.pdf

Tietosuojavaltuutetun toimisto: Pseudonymisoidut ja anonymisoidut tiedot. Luettavissa: https://tietosuoja.fi/pseudonymisointi-anonymisointi

Tor: How Big is the Dark Web?. Luettavissa: https://trac.torproject.org/projects/tor/wiki/doc/HowBigIsTheDarkWeb
Tor: Overview. Luettavissa: https://2019.www.torproject.org/about/overview.html.en

Tulli 3.5.2019: Suomen tulli takavarikoi Silkkitien verkkopalvelimen sisällön – merkittävä onnistuminen anonyymissä Tor-verkossa. Luettavissa: https://tulli.fi/artikkeli/-/asset_publisher/suomen-tulli-takavarikoi-silkkitien-verkkopalvelimen-sisallon-merkittava-onnistuminen-anonyymissa-tor-verkossa

Ulkoministeriö: Kansainväliset pakotteet. Luettavissa: https://um.fi/pakotteet

U.S. Securities and Exchange Commission: Ponzi Schemes. Luettavissa: https://www.sec.gov/fast-answers/answersponzihtm.html

VH/1982/00.01.00/2019 Virtuaalivaluuttojen verotus. Luettavissa: https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen-verotus2/

Wickr: Why Wickr. Luettavissa: https://wickr.com/why-wickr/

Xu Jiahua ja Livshits Benjamin 28.8.2019: The Anatomy of a Cryptocurrency Pump-and-Dump Scheme. Usenix association 28.8.2019. Luettavissa: https://www.usenix.org/conference/usenixsecurity19/presentation/xu-jiahua