Kryptovaluuttojen käytön ja sääntelyn haasteet rahanpesussa, terrorismin rahoituksessa ja huumekaupassa

Lapin yliopisto
Oikeustieteiden tiedekunta
Maisteritutkielma
Niko Kleemola
Rikosoikeus
Syksy 2021

Lapin yliopisto

Tiedekunta: Oikeustieteiden tiedekunta

Työn nimi: Kryptovaluuttojen käytön ja sääntelyn haasteet rahanpesussa, terrorismin rahoituksessa ja huumekaupassa

Tekijä: Niko Kleemola

Koulutusohjelma/oppiaine: Oikeustiede

Työn laji: Pro gradu -tutkielma/Maisteritutkielma X Lisensiaatintutkimus__

Sivumäärä: XXVIII + 89

Vuosi: 2021

Tiivistelmä:

Tässä tutkimuksessa on selvitetty kryptovaluuttojen käytön ja sääntelyn haasteita rahanpesussa, terrorismin rahoituksessa ja huumekaupassa. Tutkimuksessa tehdään käsitteellinen ero virtuaalivaluuttojen ja kryptovaluuttojen välille. Kryptovaluutat ovat pseudo-anonyyminen digitaalisen käteisen muoto, joka mahdollistaa taloudellisten transaktioiden tekemisen ilman keskitettyjen tahojen valvontaa. Hajautettu teknologia on tuottanut uusia haasteita lainsäätäjille ja lainvalvontaviranomaisille. Tutkimuksessa pyritään löytämään vastauksia näihin haasteisiin.

Tutkimus on metodologisesti oikeusdogmaattinen, oikeussosiologinen, oikeuspoliittinen ja oikeusvertaileva. Tutkimuksen lähdeaineistoon kuuluu kotimaista oikeuskirjallisuutta, ulkomaisia tieteellisiä artikkeleja, virallisaineistoja, kuten erinäisten järjestöjen laatimia raportteja sekä muita verkkolähteitä. Aiheen laajempaa yhteiskuntaa koskettavan kontekstuaalisen luonteen vuoksi lähdeaineisto on monin paikoin poikkitieteellistä.

Tutkimuksessa on neljä pääosiota. Ensin käsitellään yleisimpiä kryptovaluuttoja ja lohkoketjuteknologian ominaisuuksia, jotka edesauttavat kryptovaluuttojen rikollista käyttöä. Teknisemmästä ja aihetta taustoittavasta osiosta siirrytään käsittelemään kryptovaluuttojen asemaa kansainvälisessä rahanpesun ja terrorismin vastaisessa järjestelmässä sekä etenkin EU:n säädöksissä. Tämän jälkeen edetään kryptovaluuttoihin osana kansainvälistä rikollisuutta, käydään läpi kryptovaluuttojen käyttöä rikostyypeittäin sekä eritellään joitakin oikeudellisia erityisongelmia. Tutkimuksen viimeisessä pääosiossa pohditaan kryptovaluuttojen sääntelyvaihtoehtoja, kuten sääntelyn toteuttamista hajautetussa ympäristössä.

Tutkimuksen tärkeimpänä tuloksena tuodaan esiin, että kryptovaluuttojen rikollisen käytön ehkäiseminen kansainvälisessä rahanpesun ja terrorismin vastaisessa järjestelmässä sekä huumausaineiden kaupassa edellyttää kansainvälistä yhteistyötä, kansallisella tasolla proaktiivista suhtautumista ja pitkällä aikavälillä tapahtuvaa poikkitieteellistä yhteistyötä uuteen teknologiaan perustuvien valvonta- ja sääntelyratkaisujen luomiseksi. Tehokas sääntely vaatii kaksitasoista järjestelmää. Keskitettyjen ilmoitusvelvollisten toimijoiden sääntelyn tulee perustua yhdenmukaiseen käsitteistöön. Toiseksi on kehitettävä hajautetussa ympäristössä tapahtuvaa teknologialähtöistä sääntelyä.

Avainsanat: lohkoketju, kryptovaluutta, virtuaalivaluutta, kryptovarallisuus, virtuaalivarallisuus, rahanpesu, terrorismin rahoittaminen, huumausainerikokset, rahanpesudirektiivi.

Tutkielma ei sisällä muita kuin tekijän/tekijöiden omia henkilötietoja.

Sisällys

LÄHTEET VI

LYHENTEET XXVIII

1. JOHDANTO 1

1.1. Aluksi 1

1.2. Tutkimuskysymykset ja aiheen rajaus 3

1.3. Tutkimusmetodi ja oikeuslähteet 4

1.4. Keskeisistä käsitteistä 5

1.4.1. Kryptovaluutta ja virtuaalivaluutta käsitteiden oikeellisuudesta 5

1.4.2. AML/CFT-järjestelmä 6

2. KRYPTOVALUUTAT JA LOHKOKETJUTEKNOLOGIA 7

2.1. Kryptovaluuttojen oikeudellinen kehys 7

2.2. Bitcoin 9

2.3. Ethereum ja älysopimukset 10

2.4. Yksityisyysvaluutta Monero 12

2.5. Fiat-valuutat 12

2.6. Digitaalisen rahan historia osana rikollisuutta 13

2.7. Kryptovaluuttojen tekninen toimintatapa 14

2.7.1. Desentralisaatio eli hajautuneisuus 14

2.7.2. Lohkoketjun sisäänrakennettu ”luottamukseton luottamus” 16

2.7.3. Yksityisyys eli anonymiteetti 17

2.7.4. Lompakot ja niiden tarjoajat 19

2.7.5. Initial Coin Offering (ICO) 20

2.7.6. Kryptovaluutta-sekoittimet 21

3. KRYPTOVALUUTAT KANSAINVÄLISESSÄ AML/CFT-JÄRJESTELMÄSSÄ JA EU:N LAINSÄÄDÄNNÖSSÄ 22

3.1. Aluksi 22
3.2. Rahaa, hyödykkeitä vai jotain muuta – mihin sääntelyintressi perustuu? 22
3.3. Vastatoimien kansainvälinen sopimustausta 24
3.4. Financial Action Task Force ja riskiperusteinen arviointi 26
3.5. Suurimmat haasteet taistelussa kryptovaluuttojen välityksellä tapahtuvaa rahanpesua ja terrorismin rahoittamista vastaan 28
3.6. EU:n AML/CFT-järjestelmä 29
3.6.1. Jäsenmaiden suhtautuminen kryptovaluuttoihin ennen EU:n viidettä rahanpesudirektiiviä 29
3.6.2. Viides rahanpesudirektiivi 30
3.6.3. Rahanpesurikosdirektiivi 32
3.6.4. Kotimainen lainsäädäntö 33
3.6.5. Ilmoitusvelvolliset tahot järjestelmän portinvartijoina 36
3.6.6. Asiakkaiden tuntemismenettely 38
3.7. EU:n järjestelmä ei ole FATF:n suositusten mukainen 39
3.8. Ehdotuksia EU:n järjestelmän kehittämiseksi 41
3.9. Euroopan komission lainsäädäntöpaketti 20.7.2021 45
4. KRYPTOVALUUTAT OSANA KANSAINVÄLISTÄ RIKOLLISUUTTA 49
4.1. Kryptovaluuttojen asema kansainvälisessä rikollisuudessa 49
4.2. Rahanpesu ja kryptovaluutat 51
4.3. Terrorismin rahoittaminen ja kryptovaluutat 54
4.3.1. Terroristiryhmien rahoituskanavien laajentaminen kryptovaluutoilla 56
4.3.2. Kryptovaluuttojen käyttö yksittäisten terrori-iskujen rahoittamisessa 58
4.3.3. Kryptovaluuttojen terroristisen käytön haasteet 59
4.3.4. Kryptovaluuttapohjainen kyberrikollisuus ja terrorismi 60
4.3.5. Riskinä terroristien oman kryptovaluutan luominen 61
4.4. Kryptovaluutat varkauden kohteena 62
4.5. Huumausaineiden kauppa, kryptovaluutat ja Silk Road 63

4.6. Kryptovaluuttoihin liittyviä oikeudellisia erityiskysymyksiä 65
4.6.1. Kryptovaluuttojen vaikutus näyttökysymysten arviointiin – tapaus KKO:2018:3 65
4.6.2. Todistustaakka, tarkoituksenmukaisuus ja esitutkinnan rajoittaminen 66
4.7. Rikoshyödyn hallussa pitäminen 69
4.8. Menettämisseuraamukset 70
5. MITEN KRYPTOVALUUTTOJA TULISI SÄÄNNELLÄ? 73
5.1. Eri valtioiden lainsäätäjien suhtautumistavat 73
5.2. Lohkoketjuteknologian hyödyt on syytä huomioida 74
5.3. Vertailukohteena Saksa – vastatoimien kehittäminen kansallisesti 75
5.4. Keskuspankin digitaalinen valuutta – ratkaisu rahanpesuun? 77
5.5. Rikollisuuden demokratiateoria ja nykyisen sääntelyn riittämättömyys 78
5.6. Vaihtoehtoinen sääntelytapa – laillisen ja laittoman käytön erottaminen toisistaan konsensustasolla 81
6. LOPUKSI 84

LÄHTEET

Kirjallisuus

Aarnio, Aulis. Luentoja Lainopillisen Tutkimuksen Teoriasta. Helsinki 2011. (*Aarnio* 2011)

Atallah, Max – Hautamäki, Jon – Koskikare, Karri: Virtuaalivaluutan tarjoaminen – käsikirja virtuaalivaluuttalain soveltamiseen. Keuruu 2019. (*Atallah – Hautamäki – Koskikare* 2019*)*

Boon, Kristen – Huq, Aziz – Lovelace, Douglas: Terrorism: Commentary on Security Documents vol. 106. Oxford 2010. (*Boon – Huq – Lovelace* 2010*)*

Halila, Jouko: Todistustaakan jaosta. Silmällä pitäen erityisesti varallisuusoikeudellisia oikeussuhteita. Helsinki 1955. (*Halila* 1955)

Hyttinen, Tatu: Rahanpesu ja rikosvastuu: teoria ja käytäntö. Helsinki 2021. (*Hyttinen* 2021)

Hyttinen, Tatu – Tapani, Jussi – Tolvanen, Matti: Rikosoikeuden yleinen osa: vastuuoppi. 3. uudistettu painos. Helsinki 2019. (*Hyttinen – Tapani – Tolvanen* 2019)

Johansson, Patrik Elias – Eerola, Mikko – Innanen, Antti – Viitala, Juha: Lohkoketju – Tiekartta päättäjille. Liettua 2019. (*Johansson ym.* 2019)

Kimpimäki, Minna: Kansainvälinen rikosoikeus, Helsinki 2015. (*Kimpimäki* 2015)

Melander, Sakari: EU-rikosoikeus. 2. uudistettu painos. Helsinki 2015. (*Melander* 2015)

Metsäpelto, Leena: KKO 2004:72 Osallisuus törkeään huumausainerikokseen. Teoksessa: KKO:n ratkaisut kommentein 2004: II, toim. Pekka Timonen; Helsinki 2005 (*Metsäpelto* 2005)

Pölönen, Pasi: Henkilötodistelu rikosprosessissa. Helsinki 2003. (*Pölönen* 2003)

Sahavirta, Ritva: Rahanpesu rangaistavana tekona. Helsinki 2008. (*Sahavirta* 2008)

Siro, Jukka: Huumausainerikokset. Keuruu 2017. (*Siro* 2017)

Tirkkonen, Tauno: Suomen rikosprosessioikeus II. 2. uudistettu painos. Porvoo 1972. (*Tirkkonen* 1972)

Vuorenpää, Mikko. Prosessioikeuden perusteet: prosessioikeuden yleisiä lähtökohtia sekä menettely käräjäoikeuden tuomioon asti. Helsinki 2009. (*Vuorenpää* 2009)

Tieteelliset artikkelit

Adem, Efe Gencer – Basu, Soumya – Eyal, Ittay – Sirer, Emin Gün – van Renesse, Robbert: Decentralization in Bitcoin and Ethereum Networks. arXiv 2018. Saatavissa https://arxiv.org/abs/1801.03998. Viitattu: 15.5.2021 (*Adem ym.* 2018)

Ahuja, Aditya – Pal, Raj – Ribeiro, Vinay J.: A Regulatory System for Optimal Legal Transaction Throughput in Cryptocurrency Blockchains. 2021. Saatavissa: https://arxiv.org/pdf/2103.16216.pdf. Viitattu: 19.7.2021 (*Ahuja – Pal – Ribeiro* 2021)

Aldridge, Judith – Paoli, Giacomo Persi – Ryan, Nathan – Warnes, Richard: Behind the curtain, The illicit trade of firearms, explosives and ammunition on the dark web. Santa Monica, CA: RAND Corporation, 2017. Saatavissa: https://www.rand.org/pubs/research_reports/RR2091.html. Viitattu: 5.6.2021 (*Aldridge* ym. 2017)

Baron, Joshua – Dion-Schwarz, Cynthia – Manheim, David – O'Mahony, Angela: National Security Implications of Virtual Currency, Examining the Potential for Non-State Actor Deployment. RAND Corporation, Santa Monica 2015. Saatavissa: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf. Viitattu: 3.6.2021 (*Baron ym.* 2015)

Barontini, Christian – Holden, Henry: Proceeding with caution – a survey on central bank digital currency. BIS Papers 101/2019. Saatavissa: https://www.bis.org/publ/bppdf/bispap101.htm. Viitattu: 11.7.2021 (*Barontini – Holden* 2019)

Bates, Jim: Trojan horse: AIDS information introductory diskette version 2.0. Virus Bulletin 1990, s. 3–6. 1990. https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf. Viitattu: 8.6.2021 (*Bates* 1990)

Bindseil, Ulrich: Central bank digital currency: financial system implications and control. International Journal of Political Economy 48(4) 2019, s. 303-335. Saatavissa: https://ssrn.com/abstract=3385283. Viitattu: 11.7.2021 (*Bindseil* 2019)

Biryukov, Alex – Khovratovich, Dmitry – Tikhomirov, Sergei: Privacy-preserving KYC on Ethereum. European Society for Socially Embedded Technologies (EUSSET) 2018. Saatavissa: https://www.semanticscholar.org/paper/Privacy-preserving-KYC-on-Ethereum-Biryukov-Khovratovich/32822ed9ad03be0f6b03e633b79f29b72b564b69. Viitattu: 10.8.2021 (*Biryukov – Khovratovich – Tikhomirov* 2018)

Bratspies, Rebecca M.: Cryptocurrency and the Myth of the Trustless Transaction. Michigan Technology Law Review 24(2) 2018. Saatavissa: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1242&context=mttlr. Viitattu: 18.5.2021 (*Bratspies* 2018)

Accorsi, Rafael – Brenig, Christian – Müller, Günter: Economic Analysis of Cryptocurrency Backed Money Laundering. ECIS 2015 Completed Research Papers 20/2015. Saatavissa: https://aisel.aisnet.org/ecis2015_cr/20. Viitattu: 3.6.2021 (*Accorsi – Brenig – Müller* 2015)

Breuker, Dominic – Böhme, Rainer – Möser, Malte: An inquiry into money laundering tools in the bitcoin ecosystem. eCRS 2013. Saatavissa: https://maltemoeser.de/paper/money-laundering.pdf. Viitattu: 6.6.2021 (*Breuker – Böhme – Möser* 2013)

Brown, Claude – Butler, Karen – Dolan, Tim: Crypto-assets and initial coin offerings. Teoksessa: *Madir, Jelena* (Eds.): Fintech – Law and Regulation, Cheltenham, Edward Elgar Publishing 2019. s. 74–101. Saatavissa: https://www.e-elgar.com/shop/gbp/fintech-9781788979016.html. Viitattu: 3.8.2021 (*Brown – Butler – Dolan* 2019)

Camenisch, Jan – Piveteau, Jean-Marc – Stadler, Markus: Fair blind signatures. Advances in Cryptology — EUROCRYPT '95 1995, s. 209–219. Saatavissa: https://link.springer.com/content/pdf/10.1007/3-540-49264-X_17.pdf. Viitattu: 28.5.2021 (*Camenisch – Piveteau – Stadler* 1995)

Chaum, David: Blind signatures for untraceable payments, s. 199–203, teoksessa: Advances in Cryptology toim. *Chaum, David – Rivest, Ronald L. – Sherman, Alan,* Springer, Boston, MA. 1983. Saatavissa: https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF. Viitattu: 28.5.2021 (*Chaum* 1983)

Chawki, Mohamed – Darwish, Ashraf – Khan, Mohammad Ayoub – Tyagi, Sapna: Cybercrime, Digital Forensics and Jurisdiction. Springer 2015. Saatavissa: http://cybercrime-fr.org/wp-content/uploads/2020/04/My-book.pdf?fbclid=IwAR1DPaiyIw-muWHXFuS-mePyYWRQtCoMjM_sUzw-YejUOo0w9BJck4YOQ3qg. Viitattu: 10.6.2021 (*Chawki ym.* 2015)

Chohan, Usman: Oversight and regulation of cryptocurrencies: BitLicense. Discussion Paper Series: Notes on the 21st Century 3.3.2018. Saatavissa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3133342. Viitattu: 7.7.2021 (*Chohan* 2018a)

Chohan, Usman: International Law Enforcement Responses to Cryptocurrency Accountability: Interpol Working Group. International Political Economy: Monetary Relations eJournal 2018.

Saatavissa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3156531. Viitattu: 23.5.2021 (*Chohan* 2018b)

De Filippi, Primavera – Wright, Aaron: Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electronic Journal 2015. Saatavissa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. Viitattu: 1.6.2021 (*De Filippi – Wright* 2015)

Dion-Schwarz, Cynthia – Johnston, Patrick B. – Manheim, David: Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Santa Monica, CA 2019. Saatavissa: https://www.rand.org/pubs/research_reports/RR3026.html. Viitattu: 11.6.2021 (*Dion-Schwarz – Johnston – Manheim* 2019)

Nishith Desai Associates: The Blockchain: Industry Applications and Legal Perspectives. 2018. Saatavissa: http://www.nishithdesai.com/fileadmin/user-upload/\pdfs/ResearchPapers/The-Blockchain.pdf. Viitattu: 22.6.2021 (Nishith Desai Associates 2018)

Fromberger, Mathias – Haffke, Lars – Zimmermann, Patrick: Virtual Currencies and Anti-Money Laundering – The Shortcomings of the 5th AML Directive (EU) and How to Address Them. Journal of Banking Regulation 2019, s. 125-138. Saatavissa: https://ssrn.com/abstract=3328064. Viitattu: 18.7.2021 (*Fromberger – Haffke – Zimmermann* 2019)

Goldfeder, Steven – Kalodner, Harry – Narayanan, Arvind – Reisman, Dillon: When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. Proceedings on Privacy Enhancing Technologies 4/2018, s. 179-199. Saatavissa: https://doi.org/10.1515/popets-2018-0038. Viitattu: 6.6.2021 (*Goldfeder ym.* 2018)

Grinberg, Reuben: Bitcoin: An Innovative Alternative Digital Currency. Hastings Science & Technology Law Journal 4/2011, s. 159–208. Saatavissa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857. Viitattu: 17.7.2021 (*Grinberg* 2011)

Hardy, Robert – Norgaard, Julia: Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. Journal of Institutional Economics 12(3) 2016, s. 515–539. Saatavissa: https://www.cambridge.org/core/journals/journal-of-institutional-economics/article/reputation-in-the-internet-black-market-an-empirical-and-theoretical-analysis-of-the-deep-web/560A8645D47BBDDC4E71101EC1C100CA. Viitattu: 16.5.2021 (*Hardy – Norgaard* 2016)

Hinduja, Sameer: Deindividuation and internet software piracy. CyberPsychology & Behavior 11(4) 2008, s. 391–98. Saatavissa: https://www.researchgate.net/publication/23188046_Deindividuation_and_Internet_Software_Piracy. Viitattu: 25.5.2021 (*Hinduja* 2008)

Hoang, Dinh Thai – Hu, Peizhao – Kim, Dong In – Niyato, Dusit – Wang, Ping – Wang, Wenbo – Wen, Yonggang – Xiong, Zehui: A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access 7 2019, s. 22328-22370. Saatavissa: https://arxiv.org/abs/1805.02707. Viitattu: 16.7.2021 (*Hoang ym.* 2019)

Houben, Robby – Snyers, Alexander: Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion. Euroopan parlamentin tutkimus 2018. Saatavissa: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf. Viitattu: 18.7.2021 (*Houben – Snyers* 2018)

ISDA – Linklaters: Whitepaper, Smart Contracts and Distributed Ledger – A Legal Perspective. 3.8.2017. Saatavissa: https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf. Viitattu: 6.6.2021 (*ISDA – Linklaters* 2017)

Juels, Ari – Kosba, Ahmed – Shi, Elaine: The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, New York 2016, s. 283-295. Saatavissa: https://dl.acm.org/doi/pdf/10.1145/2976749.2978362. Viitattu: 20.5.2021 (*Juels – Kosba – Shi* 2016)

Kiviat, Trevor: Beyond Bitcoin: Issues in Regulating Blockchain Transactions. Duke Law Journal 65(3) 2015, s. 569-608. Saatavissa: https://scholarship.law.duke.edu/dlj/vol65/iss3/4. Viitattu: 3.7.2021 (*Kiviat* 2015)

Kotov, Vadim – Rajpal, Mantej: Understanding crypto-ransomware: In-Depth Analysis of the Most Popular Malware Families. Bromium whitepaper 2014. Saatavissa: https://www.augenakademie.at/elearning/pluginfile.php/245/mod_resource/content/16/bromium-report-ransomware.pdf. Viitattu: 18.6.2021 (*Kotov – Rajpal* 2014)

Levi, Michael: Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation. Trends in Organized Crime 24(1) 2021, s. 96–110. Saatavissa: https://link.springer.com/article/10.1007/s12117-020-09401-y. Viitattu: 9.7.2021 (*Levi* 2021)

Nabilou, *Hossein:* How to Regulate Bitcoin? Decentralized Regulation for a Decentralized Cryptocurrency. International Journal of Law and Information Technology 27(3) 2019, s. 266-291. Saatavissa: https://orbilu.uni.lu/bitstream/10993/39134/1/How%20to%20regulate%20bitcoin.pdf. Viitattu: 15.8.2021 (*Nabilou* 2019)

Naccache, David – von Solms, Sebastiaan: On blind signatures and perfect crimes. Computers & Security 11(6) 1992, s. 581–583. Saatavissa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.9796&rep=rep1&type=pdf. Viitattu: 20.5.2021 (*Naccache – von Solms* 1992)

Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Saatavissa: https://bitcoin.org/bitcoin.pdf. Viitattu: 15.5.2021 (*Nakamoto* 2008)

Nissinen, Matti: Esitutkinnan rajoittaminen – mahdollisuuksien taidetta. Defensor Legis 1/2007, s. 55. Saatavissa: https://www-edilex-fi.ezproxy.ulapland.fi/defensor_legis/4388.pdf. Viitattu: 4.6.2021 (*Nissinen* 2007)

Oftedal, Emilie: The financing of jihadi terrorist cells in Europe. Norwegian Defence Research Establishment (FFI) 6.1.2015. Saatavissa: https://publications.ffi.no/nb/item/asset/dspace:2469/14-02234.pdf. Viitattu: 1.6.2021 (*Oftedal* 2015)

Sahavirta, Ritva: Käännetty todistustaakka rikosprosessioikeudessa. Teoksessa Ojala, Timo ja Lappalainen, Juha (toim.): Kirjoituksia todistusoikeudesta, s. 225–242. 2006. Saatavissa: https://oikeus.fi/hovioikeudet/helsinginhovioikeus/material/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/painetutjulkaisut/kirjoituksiatodistusoikeudesta2006/J5kHw8Cch/17_Kaannetty_todistustaakka_rikosprosessioikeudessa_Ritva_Sahavirta.pdf. Viitattu: 5.6.2021 (Sahavirta 2006)

Shaffer, Gregory: The New Legal Realist Approach to International Law. Leiden Journal of International Law 28(2) 2015, s. 189-210. Saatavissa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605198. Viitattu: 13.6.2021 (*Shaffer* 2015)

Small, Stephen: Bitcoin: The Napster of Currency. Houston Journal of International Law 37(2) 2015. Saatavissa: http://www.hjil.org/articles/hjil-37-2-small.pdf. Viitattu: 29.5.2021 (*Small* 2015)

Yeoh, Peter: Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance 25(2) 2017, s. 196-208. Saatavissa: https://www.emerald.com/insight/content/doi/10.1108/JFRC-08-2016-0068/full/html. Viitattu: 7.7.2021 (*Yeoh* 2017)

Virallisaineisto ja raportit

Bundeslagebild Cyber-crime 2017. Saksan liittovaltionpoliisin (Bundeskriminalamt) julkaisema raportti kyberrikollisuudesta. 27.9.2018. Saatavissa: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html. Viitattu: 15.7.2021 (Bundeslagebild Cyber-crime 2017)

Carlisle, David – Keatinge, Tom – Keen, Florence: Virtual currencies and terrorist financing: assessing the risks and evaluating responses. STUDY For the TERR committee 2018. Saatavissa: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf. Viitattu: 15.6.2021 (*Carlisle – Keatinge – Keen* 2018)

Chainalysis crypto crime report: The 2020 state of crypto crime, everything you need to know about darknet markets, exchange hacks, money laundering and more. 2020. https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf. Viitattu: 5.6.2021 (Chainalysis crypto crime report 2020)

Ciphertrace cryptocurrency intelligence: Q3 2019 Cryptocurrency Anti-Money Laundering Report. 2019. Saatavissa: https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/. Viitattu: 13.7.2021 (Ciphertrace cryptocurrency intelligence: Q3 2019 Cryptocurrency Anti-Money Laundering Report 2019)

Cybercrime und Digitale Spuren Jahresbericht 2016. Baden-Württembergin paikallishallinnon raportti kyberrikollisuudesta. 2016. Saatavissa: https://lka.polizei-bw.de/wp-content/uploads/sites/14/2017/06/Cybercrime_Digitale_Spuren.pdf. Viitattu: 15.7.2021 (Cybercrime und Digitale Spuren Jahresbericht 2016)

Decreto Legislativo 25 maggio 2017, n. 90 Attuazione della Direttiva (UE) 2015/849 Relativa alla Prevenzione dell'Uso del Sistema Finanziario a Scopo di Riciclaggio dei Proventi di Attivita Criminose e di Finanziamento del Terrorismo. Italialaista kryptovaluuttoja koskevaa AML/CFT-lainsäädäntöä. 25.5.2017. Saatavissa: https://perma.cc/YQX5-BJWK. Viitattu: 16.6.2021 (Decreto Legislativo 2017)

EMCDDA – Europol: Drugs and the darknet Perspectives for enforcement, research and policy. Lissabon marraskuu 2017. Saatavissa: https://www.emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet_en. Viitattu: 10.6.2021 (EMCDDA – Europol 2017)

Euroopan arvopaperimarkkinaviranomainen: Advice on Initial Coin Offerings and Crypto-Assets. 9.1.2019. Saatavissa: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf. Viitattu: 19.7.2021 (ESMA: Advice on Initial Coin Offerings and Crypto-Assets 2019)

Euroopan keskuspankki: Virtual currency schemes – a further analysis. 2015. Saatavissa: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf. Viitattu: 19.7.2021 (EKP: Virtual currency schemes – a further analysis 2015)

Euroopan komissio: Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules. Brysseli 20.7.2021. Saatavissa: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690. Viitattu: 27.7.2021 (Euroopan komissio: Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules 2021)

Euroopan komissio: Commission Staff Working Document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. SWD(2019) 650 final, 2019. Saatavissa: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019SC0650&from=EN. Viitattu: 2.8.2021 (Euroopan komissio: Commission Staff Working Document SWD(2019) 650 final 2019)

Euroopan komissio: Komission ensimmäisen varapuheenjohtajan Frans Timmermansin, varapuheenjohtaja Valdis Dombrovskisin ja komissaari Věra Jourovàn lausuma viidennen rahanpesunvastaisen direktiivin hyväksymisestä Euroopan parlamentissa. 19.4.2018. Saatavissa: https://ec.europa.eu/commission/presscorner/detail/fi/STATEMENT_18_3429. Viitattu: 24.5.2021 (Euroopan komissio: Timmermansin, Dombrovskin ja Jourovàn lausuma viidennen rahanpesunvastaisen direktiivin hyväksymisestä Euroopan parlamentissa 2018)

Euroopan komissio: Komission kertomus Euroopan parlamentille ja neuvostolle sisämarkkinoihin vaikuttavia ja rajat ylittäviin toimiin liittyviä rahanpesun ja terrorismin rahoituksen riskejä koskevasta arvioinnista. COM(2019) 370 final, Bryssel 24.7.2019. Saatavissa: https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX:52019DC0370. Viitattu: 6.7.2021 (Euroopan komissio: Komission kertomus sisämarkkinoihin vaikuttavia ja rajat ylittäviin toimiin liittyviä rahanpesun ja terrorismin rahoituksen riskejä koskevasta arvioinnista 2019)

Euroopan komissio: Komission tiedonanto EU:n turvallisuusunionistrategiasta. COM(2020) 605 final, Bryssel 24.7.2020. Saatavissa: https://eur-lex.europa.eu/legal-

content/FI/TXT/?uri=CELEX:52020DC0605. Viitattu: 1.8.2021 (Euroopan komissio: Komission tiedonanto EU:n turvallisuusunionistrategiasta)

Euroopan komissio: Money laundering. Euroopan komission verrkosivut. Saatavissa: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en. Viitattu: 14.6.2021 (Euroopan komissio: Money laundering)

Euroopan komissio: Report on Asset recovery and confiscation: ensuring that crime does not pay, COM(2020) 217 final. 2.6.2020. Saatavissa: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200602_com-2020-217-commission-report_en.pdf. Viitattu: 2.8.2021 (Euroopan komissio: Report on Asset recovery and confiscation: ensuring that crime does not pay 2020)

Euroopan pankkiviranomainen: EBA Opinion on virtual currencies. 4.7.2014. Saatavissa: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf. Viitattu: 18.6.2021 (EPV: Opinion on virtual currencies 2014)

Euroopan pankkiviranomainen: Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD). 11.8.2016. Saatavissa: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1547217/32b1f7f2-90ec-44a8-9aab-021b35d1f1f7/EBA%2520Opinion%2520on%2520the%2520Commission%25E2%2580%2599s%2520proposal%2520to%2520bring%2520virtual%2520currency%2520entities%2520into%2520the%2520scope%2520of%25204AMLD.pdf?retry=1. Viitattu: 2.7.2021 (EPV: Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD) 2016)

Euroopan pankkiviranomainen: Report with advice for the European Commission on crypto-assets. 9.1.2019. Saatavissa: https://eba.europa.eu/eba-reports-on-crypto-assets. Viitattu: 27.6.2021 (EPV: Report with advice for the European Commission on crypto-assets 2019)

Euroopan unionin neuvosto: Neuvoston päätelmät rahanpesun ja terrorismin rahoituksen torjuntaa koskevista strategisista prioriteeteista. Bryssel 5.12.2019. Saatavissa: https://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/fi/pdf. Viitattu: 17.6.2021 (Euroopan unionin neuvosto: Neuvoston päätelmät rahanpesun ja terrorismin rahoituksen torjuntaa koskevista strategisista prioriteeteista 2019)

Europol: Changes in modus operandi of Islamic State terrorist attacks. Haag 18.1.2016. Saatavissa: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks. Viitattu: 12.6.2021 (Europol: Changes in modus operandi of Islamic State terrorist attacks 2016)

Europol: Cryptocurrency laundering as a service: members of a criminal organisation arrested in Spain. Europol 8.5.2019. Saatavissa: https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain. Viitattu: 21.7.2021 (Europol: Cryptocurrency laundering as a service: members of a criminal organisation arrested in Spain 2019)

Europol: Does crime still pay? Criminal asset recovery in the EU. 1.2.2016. Saatavissa: https://www.europol.europa.eu/publications-documents/does-crime-still-pay. Viitattu: 20.7.2021 (Europol: Does crime still pay? Criminal asset recovery in the EU 2016)

Europol: European union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime. Publications Office of the European Union, Luxembourg 12.4.2021. Saatavissa: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment. Viitattu: 28.5.2021 (Europol: European union serious and organised crime threat assessment 2021)

Europol: Internet organised crime threat assessment (IOCTA) 2017. Report 27.9.2017. Saatavissa: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017. Viitattu: 30.5.2021 (Europol: IOCTA 2017)

Europol: Money laundering with digital currencies: working group established. Press Release 9.9.2016. Saatavissa: https://www.europol.europa.eu/newsroom/news/money-laundering-digital-currencies-working-group-established. Viitattu: 3.7.2021 (Europol: Money laundering with digital currencies 2016)

Europol: Ten hackers arrested for string of sim-swapping attacks against celebrities. Press Release 10.2.2021. Saatavissa:https://www.europol.europa.eu/newsroom/news/ten-hackers-arrested-for-string-of-sim-swapping-attacks-against-celebrities. Viitattu: 7.7.2021 (Europol: Ten hackers arrested for string of sim-swapping attacks against celebrities 2021)

Europol: World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down. Press Release 25.4.2018. Saatavissa: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-

taken-down. Viitattu: 5.6.2021 (Europol: World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down 2018)

FATF: Anti-money laundering and counter-terrorist financing measures Finland Mutual Evaluation Report. Pariisi 16.4.2019. Saatavissa: https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-finland-2019.html. Viitattu: 9.7.2021 (FATF: Finland Mutual Evaluation Report 2019)

FATF: Draft updated Guidance for a risk-based approach to virtual assets and VASPs. 2020. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf. Viitattu: 26.7.2021 (FATF: Draft updated Guidance for a risk-based approach to virtual assets and VASPs. 2020)

FATF: Financing of Recruitment for Terrorist Purposes. Pariisi 2018. Saatavissa: http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf. Viitattu: 20.6.2021 (FATF: Financing of Recruitment for Terrorist Purposes 2018)

FATF: Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. 21.6.2019. Saatavissa: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. Viitattu: 9.6.2021 (FATF: Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers 2019)

FATF: Guidance for a Risk-Based Approach: Virtual Currencies. Pariisi 2015. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Viitattu: 12.6.2021 (FATF: Guidance for a Risk-Based Approach: Virtual Currencies)

FATF: IX Special Recommendations on Terrorist Financing. 2001. Saatavissa: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/ixspecialrecommendations.html. Viitattu: 14.6.2021 (FATF: IX Special Recommendations on Terrorist Financing 2001)

FATF: Professional Money Laundering. Pariisi 26.7.2018. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf. Viitattu: 25.6.2021 (FATF: Professional Money Laundering 2018)

FATF: Report to G20 Finance Ministers and Central Bank Governors. Pariisi 8.4.2019. Saatavissa: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf. Viitattu: 5.6.2021 (FATF: Report to G20 Finance Ministers and Central Bank Governors 2019)

FATF: Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs. Pariisi 5.7.2021. Saatavissa: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html. Viitattu: 28.7.2021 (FATF: Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs 2021)

FATF: Virtual Currencies: Key Definitions and Potential AML/CFT Risks. Pariisi 2014. Saatavissa: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Viitattu: 2.7.2021 (FATF: Virtual Currencies: Key Definitions and Potential AML/CFT Risks 2014)

Finanssivalvonta: Standardi 2.4 Asiakkaan tunteminen - rahanpesun ja terrorismin rahoittamisen estäminen. 22.6.2010. Saatavissa: https://www.finanssivalvonta.fi/globalassets/fi/saantely/maarayskokoelma/standardit/2.4/2.4.std5.pdf. Viitattu: 14.6.2021 (Finanssivalvonta: Standardi 2.4 Asiakkaan tunteminen 2010)

Heiskanen, Hanna: Kryptovaluutat ja ICO (Initial Coin Offering) sijoituskohteina, onko kyse kuplasta? Finanssivalvonnan tiedotteet 22.11.2017. Saatavissa: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2017/kryptovaluutat-ja-ico-initial-coin-offering-sijoituskohteina-onko-kyse-kuplasta/. Viitattu: 13.8.2021 (*Heiskanen* Finanssivalvonta 2017)

Huberman, Gur – Leshno, Jacob D. – Moallemi, Ciamac: Monopoly without a monopolist: An economic analysis of the bitcoin payment system. Research Discussion Papers 27/2017, Bank of Finland 5.9.2017. Saatavissa: https://helda.helsinki.fi/bof/handle/123456789/14912. Viitattu: 17.7.2021 (*Huberman – Leshno – Moallemi* 2017)

Huberman, Gur – Leshno, Jacob D. – Moallemi, Ciamac: Monopoly without a monopolist: An economic analysis of the bitcoin payment system. Columbia Business School Research Paper No. 17-92 27.1.2021. Saatavissa: https://moallemi.com/ciamac/papers/bitcoin-2017.pdf. Viitattu: 17.7.2021 (*Huberman – Leshno – Moallemi* 2021)

Kiinan valtioneuvoston rahoitusvakaus- ja kehityskomitea: Liu He presided over the 51st meeting of the State Council Financial Stability and Development Committee. Saatavissa: https://translate.google.com/translate?sl=auto&tl=en&u=http://www.gov.cn/guowuyuan/2021-05/21/content_5610192.htm. Viitattu: 19.6.2021 (Kiinan valtioneuvoston rahoitusvakaus- ja kehityskomitean lausunto)

Luxemburgin rahoituksenvalvontaviranomaisen (Commission de surveillance du secteur financier, CSSF) julkaisut:
Commission de Surveillance du Secteur Financier: Avertissement sur les monnaies virtuelles.

14.3.2018. Saatavissa: https://www.cssf.lu/fr/2018/03/avertissement-sur-les-monnaies-virtuelles/. Viitattu: 4.7.2021 (CSSF: Avertissement sur les monnaies virtuelles) Commission de Surveillance du Secteur Financier: Avertissement sur les Initial Coin Offerings (ICOs). 14.3.2018. Saatavissa: https://www.cssf.lu/fr/2018/03/avertissement-sur-les-initial-coin-offerings-icos-et-tokens/. Viitattu: 4.7.2021 (CSSF: Avertissement sur es Initial Coin Offerings (ICOs))

Maltan kryptovaluuttoja koskevasta lainsäädännöstä Art. 57 (3) Virtual Financial Assets Act ja Art. 8 (4) d, ii) Innovative Technology Arrangement and Services Act (ITAS). Saatavissa: https://www.consob.it/documents/46180/46181/Malta_act_XXX_2018.pdf/89dfef93-aa00-45d7-b9a8-127eace3c422. Viitattu: 5.7.2021 (Malta: Virtual Financial Assets Act)

OMFIF & IBM: Retail CBDCs: The next payments frontier. 2019. Saatavissa: https://www.omfif.org/wp-content/uploads/2019/11/Retail-CBDCs-The-next-payments-frontier.pdf. Viitattu: 2.7.2021 (OMFIF & IBM: Retail CBDCs 2019)

Rahanpesun selvittelykeskuksen vuosikertomus 2020. Saatavissa: https://poliisi.fi/documents/25235045/67733116/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf/e340331f-f04c-7eec-2756-111628ae368a/2020-Rahanpesun-selvittelykeskus-vuosikertomus-2020.pdf?t=1617010848853. Viitattu: 2.8.2021 (Rahanpesun selvittelykeskus 2020)

Suomen Pankki: Bitcoin involves risks. 14.1.2014. Saatavissa: https://www.suomenpankki.fi/en/media-and-publications/news/2014/bitcoin-involves-risks/. Viitattu: 15.6.2021 (Suomen Pankki: Bitcoin involves risks 2014)

The Law Library of Congress: Regulation of Cryptocurrency around the World. 2018. Saatavissa: https://jolt.richmond.edu/files/2021/02/Bull_cryptocurrency-world-survey.pdf. Viitattu: 20.7.2021 (The Law Library of Congress: Regulation of Cryptocurrency around the World 2018)

U.S. House of Representatives, Financial Innovation and Defense Act, H.R. 4752 20.1.2018. Saatavissa: https://www.congress.gov/115/bills/hr4752/BILLS-115hr4752ih.pdf. Viitattu: 10.7.2021 (U.S. House of Representatives, Financial Innovation and Defense Act, H.R. 4752 2018)

Valtiovarainministeriön hanke VM191:00/2020. Toimikausi/aikataulu 1.1.2021 – 31.8.2021. Saatavissa: https://vm.fi/hanke?tunnus=VM191:00/2020. Viitattu: 23.7.2021 (Valtiovarainministeriön hanke VM191:00/2020)

Verohallinto: Harmaan talouden selvitysyksikön raportti, Harmaan talouden tilannekuva 3/2011. (Verohallinto: Harmaan talouden tilannekuva 3/2011)

YK:n erityisjärjestö Maailmanpankki: Global financial development report 2014: financial inclusion. 1(82556) 10.11.2013. Saatavissa: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/225251468330270218/global-financial-development-report-2014-financial-inclusion. Viitattu: 22.5.2021 (Maailmanpankki: Global financial development report 2014)

YK:n huumeiden ja rikollisuuden torjunnasta vastaava toimisto (UNODC): Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. 2014. Saatavissa: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Viitattu: 30.7.2021 (UNODC: Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies 2014)

Kansainväliset sopimukset

SopS 44/1994 Yhdistyneiden Kansakuntien yleissopimus huumausaineiden ja psykotrooppisten aineiden laitonta kauppaa vastaan.

SopS 74/2002 Terrorismin rahoituksen torjumista koskeva kansainvälinen yleissopimus.

SopS 20/2004 Kansainvälisen järjestäytyneen rikollisuuden vastainen Yhdistyneiden Kansakuntien yleissopimus.

SopS 71/2006 Kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen lisäpöytäkirja ihmiskaupan, erityisesti naisten ja lasten kaupan ehkäisemisestä, torjumisesta ja rankaisemisesta.

SopS 73/2006 Kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen lisäpöytäkirja maitse, meritse ja ilmateitse tapahtuvan maahanmuuttajien salakuljetuksen kieltämisestä.

SopS 74/2011 Kansainvälisen järjestäytyneen rikollisuuden vastaisen yhdistyneiden kansakuntien yleissopimuksen ampuma-aseiden, niiden osien ja komponenttien sekä ampumatarvikkeiden laittoman valmistuksen ja kaupan torjumista koskeva lisäpöytäkirja.

Euroopan unionin direktiivit ja säädösehdotukset

Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/849 rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2005/60/EY ja komission direktiivin 2006/70/EY kumoamisesta (neljäs rahanpesudirektiivi).

Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/843 rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen annetun direktiivin (EU) 2015/849 ja direktiivien 2009/138/EY ja 2013/36/EU muuttamisesta (viides rahanpesudirektiivi).

Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1673, annettu 23 päivänä lokakuuta 2018, rahanpesun torjumisesta rikosoikeudellisin keinoin (rahanpesurikosdirektiivi).

Commission staff working document impact assessment Accompanying the Anti-money laundering package Brussels, 20.7.2021 SWD(2021) 190 final. Saatavissa: https://ec.europa.eu/finance/docs/law/210720-impact-assessment_en.pdf.

Proposal for a directive of the European parliament and of the council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849 Brussels, 20.7.2021 COM(2021) 423 final 2021/0239 (COD). Saatavissa: https://ec.europa.eu/finance/docs/law/210720-proposal-amld6_en.pdf.

Proposal for a regulation of the European parliament and of the council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010. Brussels, 20.7.2021 COM(2021) 421 final 2021/0240 (COD). Saatavissa: https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft-authority_en.pdf.

Proposal for a regulation of the European parliament and of the council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Brussels, 20.7.2021 COM(2021) 420 final 2021/0239 (COD). Saatavissa: https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft_en.pdf.

Proposal for a regulation of the European parliament and of the council on information accompanying transfers of funds and certain crypto-assets (recast) Brussels, 20.7.2021 COM(2021) 422 final 2021/0241 (COD). Saatavissa: https://ec.europa.eu/finance/docs/law/210720-proposal-funds-transfers_en.pdf.

Suomen valmisteluasiakirjat

HE 15/1990 vp Hallituksen esitys Eduskunnalle riita-asiain oikeudenkäyntimenettelyn uudistamista alioikeuksissa koskevaksi lainsäädännöksi.

HE 80/2000 vp Hallituksen esitys Eduskunnalle menettämisseuraamuksia koskevan lainsäädännön uudistamiseksi.

HE 285/2010 vp Hallituksen esitys Eduskunnalle laeiksi rikoslain 32 luvun 6 ja 14 §:n sekä kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 §:n muuttamisesta.

HE 167/2018 vp Hallituksen esitys eduskunnalle laiksi pankki- ja maksutilien valvontajärjestelmästä ja eräiksi siihen liittyviksi laeiksi.

HE 261/2020 vp Hallituksen esitys eduskunnalle laeiksi rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain, rahanpesun selvittelykeskuksesta annetun lain sekä pankki- ja maksutilien valvontajärjestelmästä annetun lain 6 §:n muuttamisesta.

Oikeustapaukset

KKO 2017:12

KKO 2018:3

Kemptenin (Baijeri) alioikeuden ratkaisu asiassa BGH 1 StR 412/16–27. heinäkuu 2017 (LG Kempten) https://www.hrr-strafrecht.de/hrr/1/16/1-412-16.php.

Helsingin HAO 6.7.2018 18/0426/3 https://oikeus.fi/hallintooikeudet/helsinginhallinto-oikeus/fi/index/hallintooikeusratkaisut/1530879000488.html.

Muut verkkolähteet

Al Jazeera: Hamas calls for supporters to send bitcoins. Al Jazeera 30.1.2019. Saatavissa: https://www.aljazeera.com/economy/2019/01/30/hamas-calls-for-supporters-to-send-bitcoins/. Viitattu: 3.6.2021 (Al Jazeera 2019)

Almeida, Yasmin – Habermeier, Karl – Haksar, Vikram – He, Dong – Kashima, Mikari – Kyriakos-Saad, Nadim – Leckow, Ross – Oura, Hiroko – Saadi Sedik, Tahsin – Stetsenko, Natalia – Verdugo-Yepes, Concepcion: Virtual Currencies and Beyond: Initial Considerations. IMF Staff Discussions

Note 16.3.2016. Saatavissa: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf. Viitattu: 12.7.2021 (*Almeida ym*. IMF Staff Discussions Note 2016)

Ashok, India: The anatomy of a "Cyber Jihad" – analysing the future and evolution of terrorism in cyberspace. International Business Times 20.6.2016. Saatavissa: https://www.ibtimes.co.uk/anatomy-cyber-jihad-analysing-evolution-future-terrorism-cyber-space-1566184. Viitattu: 3.6.2021 (*Ashok* International Business Times 2016)

BBC News: Bitcoin: El Salvador makes cryptocurrency legal tender. BBC News 9.6.2021. Saatavissa: https://www.bbc.com/news/world-latin-america-57398274. Viitattu: 16.7.2021 (BBC News 2021)

BBC News: Cyber-attack: US and UK blame North Korea for WannaCry. BBC News 19.12.2017. Saatavissa: https://www.bbc.com/news/world-us-canada-42407488. Viitattu: 5.7.2021 (BBC News 2017)

Beedham, Matthew: Nike now holds patent for blockchain-based sneakers called 'CryptoKicks'. TNW 10.12.2019. Saatavissa: https://thenextweb.com/news/nike-blockchain-sneakers-crypto-kick-patent. Viitattu: 1.6.2021 (*Beedham* TNW 2019)

Bitcoin.org-verkkosivu. Saatavissa: https://bitcoin.org/en/vocabulary#bit. Viitattu (Bitcoin.org)

Bitcoinin laillisuuden tila maittain. Wikipedia. Saatavissa: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory. Viitattu: 2.7.2021 (Bitcoinin laillisuuden tila maittain)

Bitstamp kryptovaluuttapörssin AML-käytännöt. Saatavissa: https://www.bitstamp.net/aml-policy/. Viitattu: 18.6.2021 (Bitstamp AML-policy)

Blue, Violet – Day, Zero: CryptoLocker's crimewave: A trail of millions in laundered Bitcoin. ZDNet 22.12.2013. Saatavissa: https://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/. Viitattu: 5.7.2021 (*Blue – Day* ZDNet 2013)

Callimachi, Rukmini: Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots from Afar. New York Times 4.2.2017. Saatavissa: https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html. Viitattu: 6.6.2021 (*Callimachi* New York Times 2017)

Carlisle, David: Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic. Rusi.org 2.3.2017. Saatavissa: https://rusi.org/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic. Viitattu: 6.6.2021 (*Carlisle* Rusi.org 2017)

Changing Minds: Deindividuaation määritelmä. Saatavissa: http://changingminds.org/explanations/theories/deindividuation.htm. Viitattu: 29.5.2021 (Changing Minds: Deindividuaation määritelmä)

Chipolina, Scott: Art Has a Money Laundering Problem. NFTs Could Make It Worse. Decrypt 8.5.2021. Saatavissa: https://decrypt.co/70190/art-has-a-money-laundering-problem-nfts-could-make-it-worse. Viitattu: 28.5.2021 (*Chipolina* Decrypt 2021)

Conti, Robyn – Schmidt, John: What You Need To Know About Non-Fungible Tokens (NFTs). Forbes 14.5.2021. Saatavissa: https://www.forbes.com/advisor/investing/nft-non-fungible-token/. Viitattu: 28.5.2021 (*Conti – Schmidt* Forbes 2021)

Criddle, Cristina: Bitcoin: $1bn address with Silk Road links 'being transferred'. BBC News 4.11.2020. Saatavissa: https://www.bbc.com/news/technology-54810976. Viitattu: 13.6.2021 (*Criddle* BBC News 2020)

Dedi, Dylan: Is Venezuela's "Petro" Really a Cryptocurrency?. CryptoSlate, 7.12.2017. Saatavissa: https://cryptoslate.com/venezuelas-petro-really-cryptocurrency/. Viitattu: 18.6.2021 (*Dedi* CryptoSlate 2017)

Digital Asset Transfer Authorityn verkkosivut. Saatavissa: https://datauthority.org/. Viitattu: 26.7.2021 (Digital Asset Transfer Authorityn verkkosivut)

Erb, Kelly Phillips: IRS Will Pay Up To $625,000 If You Can Crack Monero, Other Privacy Coins. Forbes 14.9.2020. Saatavissa: https://www.forbes.com/sites/kellyphillipserb/2020/09/14/irs-will-pay-up-to-625000-if-you-can-crack-monero-other-privacy-coins/. Viitattu: 13.7.2021 (*Erb* Forbes 2020)

Ethereum.org. Saatavissa: https://ethereum.org/en/. Viitattu: 25.5.2021 (Ethereum.org)

Faife, Corin: Live Free or Mine: How Libertarians Fell in Love With Bitcoin. Coindesk 8.10.2016. Saatavissa: https://www.coindesk.com/live-free-or-mine-how-libertarians-fell-in-love-with-bitcoin. Viitattu: 20.6.2021 (*Faife* Coindesk 2016)

Fedotov, Yury: In Just Two Decades, Technology Has Become A Cornerstone Of Criminality. HuffPost UK 23.10.2017. Saatavissa: https://www.huffingtonpost.co.uk/yury-fedotov/in-just-two-decades-techn_b_18330400.html?ncid=engmodushpmg00000004. Viitattu: 16.5.2021 (*Fedotov* HuffPost UK 2017)

Frankenfield, Jake: Bitcoin Wallet. Investopedia 9.6.2021. Saatavissa: https://www.investopedia.com/terms/b/bitcoin-wallet.asp. Viitattu: 15.6.2021 (*Frankenfield* Investopedia 2021)

Frier, Sarah – Mehrotra, Kartikay: Twitter hack hits Obama, Biden, Musk in Bitcoin scam. Bloomberg News 16.7.2020. Saatavissa: https://www.bnnbloomberg.ca/elon-musk-bill-gates-appear-to-have-twitter-accounts-hacked-1.1466035. Viitattu: 23.7.2021 (*Frier – Mehrotra* Bloomberg News 2020)

Gordon, Karrie: Binance Investigation Sparks Fear in Crypto Markets. ETF Trends 14.5.2021. Saatavissa: https://www.etftrends.com/crypto-channel/binance-investigation-sparks-fear-in-crypto-markets/. Viitattu: 7.6.2021 (*Gordon* ETF Trends 2021)

Greenberg, Andy: 'Dark Wallet' is about to make Bitcoin money laundering easier than ever. Wired 4.29.2014. Saatavissa: http://www.wired.com/2014/04/dark-wallet/. Viitattu: 29.6.2021 (*Greenberg* Wired 2014)

Hajdarbegovic, Nermin: Bitcoin Ransomware Now Spreading via Spam Campaigns. Coindesk 26.1.2015. Saatavissa: https://www.coindesk.com/bitcoin-ransomware-now-spreading-via-spam-campaigns. Viitattu: 23.6.2021 (*Hajdarbegovic* Coindesk 2015)

Hara, Jyrki – Harjumaa, Marika – Heikkilä, Markus – Keränen, Timo: Vastaamon asiakkaat saavat nyt kiristysviestejä sähköposteihinsa: viesteissä vaaditaan 200–500 euron arvosta bitcoineja – Poliisi: Vaatimuksiin ei tule suostua. Yle 24.10.2020. Saatavissa: https://yle.fi/uutiset/3-11612183. Viitattu: 5.6.2021 (*Hara ym.* Yle 2020)

Helms, Kevin: ECB Chief Christine Lagarde Calls for Global Bitcoin Regulation — Says BTC Conducts 'Funny Business'. Bitcoin News 14.1.2021. Saatavissa: https://news.bitcoin.com/ecb-christine-lagarde-global-bitcoin-regulation-btc/. Viitattu 1.6.2021. (*Helms* Bitcoin News 2021a)

Helms, Kevin: Janet Yellen Reveals Plans for Bitcoin — Sees Cryptocurrencies Used Mainly for Illicit Financing. Bitcoin News 20.1.2021. Saatavissa: https://news.bitcoin.com/janet-yellen-bitcoin-cryptocurrencies-illicitfinancing/. Viitattu 1.6.2021. (*Helms* Bitcoin News 2021b)

Izenman, Kayla – Moiseienko, Anton: Gaming the System: Money Laundering Through Online Games. RUSI's Centre for Financial Crime & Security Studies 11.10.2019. Saatavissa: https://rusieurope.eu/sites/default/files/20191011_newsbrief_vol39_no9_moiseienko_and_izenman_web.pdf. Viitattu: 19.7.2021 (*Izenman – Moiseienko* RUSI 2019)

Johnson, Tim: Computer hack helped feed an Islamic State Death List. McClatchy DC Bureau 20.7.2016. Saatavissa: http://www.mcclatchydc.com/news/nation-world/national/article90782637.html. Viitattu: 3.6.2021 (*Johnson* McClatchy DC Bureau 2016)

Kasireddy, Preethi: ELI5: What do we mean by "blockchains are trustless"?. Medium 2.2.2018. Saatavissa: https://preethikasireddy.medium.com/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6. Viitattu: 6.6.2021 (*Kasireddy* Medium 2018)

Kharpal, Arjun: China has given away millions in its digital yuan trials. This is how it works. CNBC 4.11.2021. Saatavissa: https://www.cnbc.com/2021/03/05/chinas-digital-yuan-what-is-it-and-how-does-it-work.html. Viitattu: 12.7.2021 (*Kharpal* CNBC 2021)

Levitt, Matthew: Hezbollah's Transnational Organized Crime. The Washington Institute for Near East Policy 21.4.2016. Saatavissa: https://www.washingtoninstitute.org/policy-analysis/hezbollahs-transnational-organized-crime. Viitattu: 9.6.2021 (*Levitt* The Washington Institute for Near East Policy 2016)

Lu, Seres: What is the dark web and who uses it?. The Globe and Mail 19.8.2015. Saatavissa: https://www.theglobeandmail.com/technology/tech-news/what-is-the-dark-web-and-who-uses-it/article26026082/. Viitattu: 18.6.2021 (*Lu* The Globe and Mail 2015)

McConville, Anton: Prevent ransomware attacks with blockchain. IBM 17.5.2017. https://www.ibm.com/blogs/cloud-archive/2017/05/blockchain-prevent-ransomware-attacks/. Viitattu: 21.6.2021 (*McConville* IBM 2017)

Merriam-Webster: fiat money. Saatavaissa: https://www.merriam-webster.com/dictionary/fiat%20money. Viitattu 2.7.2021 (Merriam-Webster)

Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg. Virtuelle kriminalität, Cybercrime 2021. Saatavissa: https://im.baden-wuerttemberg.de/de/sicherheit/polizei/kriminalitaetsbekaempfung/cybercrime/. Viitattu: 20.7.2021 (Ministerium des Inneren 2021)

Moneron verkkosivut. Saatavissa: https://www.getmonero.org/. Viitattu: 15.7.2021 (Moneron verkkosivut)

Nuortennetti: Laki ja netti. Nuortennetti 20.4.2021. Saatavissa: https://www.nuortennetti.fi/netti-ja-media/laki-ja-netti/. Viitattu: 30.5.2021 (Nuortennetti 2021)

Pavy, Eeva: Toissijaisuusperiaate. Faktatietoja Euroopan unionista 2021. Saatavissa: https://www.europarl.europa.eu/factsheets/fi/sheet/7/the-principle-of-subsidiarity. Viitattu: 20.7.2021 (*Pavy* Faktatietoja Euroopan unionista 2021)

Personaldatasecurity: PGP Salaus. Windows 7/8/10 yksityisyyden suoja 18.8.2014. Saatavissa: https://personaldatasecurity.wordpress.com/pgp-salaus/. Viitattu: 1.6.2021 (*Personaldatasecurity* 2014)

Robinson, Matt: SEC Sues Five BitConnect Promoters Over $2 Billion Scheme. Bloomberg 29.5.2021. Saatavissa: https://www.bloomberg.com/news/articles/2021-05-28/sec-sues-five-bitconnect-promoters-over-2-billion-scheme. Viitattu: 13.8.2021 (*Robinson* Bloomberg 2021)

Rooney, Kate: Record $1 billion worth of bitcoin linked to the Silk Road seized by U.S. government. CNBC 5.11.2020. Saatavissa: https://www.cnbc.com/2020/11/05/1-billion-worth-of-bitcoin-linked-to-the-silk-road-seized-by-the-us.html. Viitattu: 5.6.2021 (*Rooney* CNBC 2020)

Ruotsin keskuspankin julkaisu Bitcoinin oikeudellisesta luonteesta: Bitcoin är inte pengar. 14.3.2018. Saatavissa: https://www.riksbank.se/sv/press-och-publicerat/nyheter-och-press-meddelanden/nyheter/2018/bitcoin-ar-inte-pengar/. Viitattu: 7.6.2021 (Ruotsin keskuspankin julkaisu: Bitcoin är inte pengar 2018)

Seth, Shobhit: Central Bank Digital Currency (CBDC). Investopedia 6.4.2021. Saatavissa: https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp. Viitattu: 7.7.2021 (*Seth* Investopedia 2021)

Staufenberg, Jess: Isis shows off currency with gold dinar coin worth £91 each – in quest for "world domination". Independent 31.8.2015. Saatavissa: https://www.independent.co.uk/news/world/middle-east/isis-shows-off-new-currency-with-gold-dinar-coins-worth-91-each-in-quest-for-world-domination-10480121.html. Viitattu: 17.7.2021 (*Staufenberg* Independent 2015)

Sundararajan, Sujha: Chinese City to Use Blockchain In Fight Against Tax Evasion. Coindesk 25.5.2018. Saatavissa: https://www.coindesk.com/tencent-partners-with-city-authority-to-combat-tax-evasion-with-blockchain. Viitattu: 20.6.2021 (*Sundararajan* Coindesk 2018)

Sykes, Patrick: Iran Bans Bitcoin Mining, Echoing China, After Blackouts. Bloomberg 26.5.2021. Saatavissa: https://www.bloomberg.com/news/articles/2021-05-26/iran-bans-crypto-mining-to-keep-the-lights-on-over-summer. Viitattu: 23.6.2021 (*Sykes* Bloomberg 2021)

Söderberg, Gabriel: Ekonomiska kommentarer, Är Bitcoin och andra kryptotillgångar pengar? Sveriges Riksbank 5/2018. Saatavissa: https://perma.cc/PDP4-X2HU. Viitattu: 7.6.2021 (*Söderberg* Sveriges Riksbank 2018)

The Guardian: Hacker who gave Isis 'hitlist' of US targets jailed for 20 years. The Guardian 24.9.2016. Saatavissa: https://www.theguardian.com/world/2016/sep/24/hacker-who-gave-isis-hitlist-of-us-targets-jailed-for-20-years. Viitattu: 15.6.2021 (The Guardian 2016)

Tor FAQ. Saatavissa: https://2019.www.torproject.org/docs/faq.html.en. Viitattu (Tor FAQ)

Torpey, Kyle: U.S. Lawmakers Are Realizing They Can't Ban Bitcoin. Forbes 30.7.2019. Saatavissa: https://www.forbes.com/sites/ktorpey/2019/07/30/us-lawmakers-are-realizing-they-cant-ban-bitcoin/. Viitattu: 28.6.2021 (*Torpey* Forbes 2019)

Tulli: Suomen tulli takavarikoi Sipulimarket-verkkopalvelimen sisällön – onnistuminen anonyymissä Tor-verkossa. Tullin verkkosivut 11.12.2020. Saatavissa: https://tulli.fi/en/-/suomen-tulli-takavarikoi-sipulimarket-verkkopalvelimen-sisallon-onnistuminen-anonyymissa-tor-verkossa. Viitattu: 17.7.2021 (Tulli 2020)

Vahiajun, Shivam: China's Bitcoin miners are looking at US, Kazakhstan, Canada, and Europe amid the exodus — but not every option fits the bill. Business Insider 24, 2021 Saatavissa: https://www.businessinsider.in/cryptocurrency/news/chinas-bitcoin-miners-are-looking-at-us-kazakhstan-canada-and-europe-amid-the-exodus/articleshow/83806714.cms. Viitattu: 1.7.2021 (*Vahiajun* Business Insider 2021)

Yuniar, Resty Woro: Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says. Wall Street Journal 9.1.2017. Saatavissa: https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198. Viitattu: 12.6.2021 (*Yuniar* Wall Street Journal 2017)

LYHENTEET

AML/CFT	Rahanpesun ja terrorismin rahoittamisen vastustamisen järjestelmä
AMLA	EU AML Authority eli EU:n uusi rahanpesun vastainen toimielin
AMLD5	Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/843
CBDC	Keskuspankin digitaalinen valuutta
EKP	Euroopan keskuspankki
EPV	Euroopan pankkiviranomainen
ESMA	Euroopan arvopaperimarkkinaviranomainen
FATF	Financial Action Task Force
Fiat-valuutta	Jonkin maan lailliseksi maksuvälineeksi nimetyt metallirahat ja setelit sekä sähköinen raha, joka on hyväksytty vaihdantavälineeksi liikkeeseen-laskumaassa
KYC	Asiakkaan tunteminen
OECD	Taloudellisen yhteistyön ja kehityksen järjestö
P2P	Peer-to-peer
PoS	Proof of Stake
PoW	Proof of Work
UNODC	YK:n huumeiden ja rikollisuuden torjunnasta vastaava toimisto

1. JOHDANTO

1.1. Aluksi

Yhdistyneiden kansakuntien huumeiden ja rikollisuuden torjunnasta vastaavan toimiston pääjohtaja Yury Fedotov totesi vuonna 2017 puheessaan, että ”kahdessakymmenessä vuodessa rikollisista on tullut teknologian ja globalisaation edunsaajia. Kryptovaluuttojen avulla rikolliset ovat lisänneet ulottuvuuttaan, rikoksiaan ja voittojaan. Aivan kuten Internet on muuttanut elämämme jokaisen osa-alueen, siitä on tullut myös rikollisen toiminnan kulmakivi.” — ”kryptovaluuttojen suosion räjähdysmäinen kasvu helpottaa rahanpesua ja alentaa kiinnijäämisriskiä.”[1]

Taloudellisen yhteistyön ja kehityksen järjestö OECD:n yhteydessä toimiva hallitusten välinen toimintaryhmä FATF (Financial Action Task Force)[2], joka tekee rahanpesun sekä terrorismin ja joukkotuhoaseiden rahoittamisen vastaista kansainvälistä yhteistyötä totesi raportissaan G20-maille, että ” […] virtuaalivaluuttojen helppo globaali käyttö houkuttelee rikollisia hyödyntämään niitä rahanpesuun ja terrorismin rahoittamiseen.” — ”yhteys kryptovaluuttojen ja muiden esirikosten välillä on kasvussa.”[3]

Kryptovaluuttojen, kuten Bitcoinin käyttö taloudellisissa transaktioissa lisääntyy kiihtyvään tahtiin. Kryptovaluuttojen käytön yleistymisen myötä myös niiden rikollinen käyttö on yleistynyt, koska lohkoketjuteknologiaa on mahdollista hyödyntää tehokkaasti niin rikollisiin kuin laillisiinkin käyttötarkoituksiin. Erityisiä huolenaiheita liittyy kryptovaluuttojen valtioiden rajat ylittävään luonteeseen ja siihen, miten tehokkaasti ne fasilitoivat perinteisiä rikosmuotoja toimintaympäristössä, johon lainsäätäjän ja lainvalvontaviranomaisten on vaikea puuttua. Tiettyjä kryptovaluuttoja pystytään esimerkiksi vaihtamaan ja siirtämään täysin anonyymisti ilman, että näistä transaktioista jää mitään havainnoitavaa jälkeä, tai jälkien seuraaminen vaatisi niin runsaasti resursseja, ettei se ole korkeiden kustannusten vuoksi järkevää. Tämäntyyppisiä kryptovaluuttoja käytetään erityisesti valtioiden rajat ylittävien rikosten tuottojen rahanpesuun, kuten myöhemmin osoitetaan.

Kryptovaluutoilla ja etenkin niiden perustana olevalla lohkoketjuteknologialla on myös yhteiskuntaa monin tavoin hyödyttäviä laillisia käyttötarkoituksia. Niiden käyttö mahdollistaa muun muassa transaktiokustannusten minimoinnin etenkin kansainvälisissä varainsiirroissa. Kustannustehokkuus perustuu kryptovaluuttojen tekniseen rakenteeseen, lohkoketjuun, joka

[1] Ks. *Fedotov* HuffPost UK 2017.
[2] FATF:n toimintaa käsitellään tarkemmin jäljempänä luvussa 3.4.
[3] FATF: Report to G20 Finance Ministers and Central Bank Governors 2019.

mahdollistaa perinteisten välittäjätahojen poissulkemisen varainsiirroista. Satoshi Nakamoto loi Bitcoinin, ensimmäisen ja tunnetuimman kryptovaluutan, joka on rakenteeltaan hajautettu sähköisen rahan vaihdannan vertaisverkko.[4] Tällainen uudenlainen hajautettu rakenne sulkee pois perinteiset tahot, kuten pankit, välittäjät sekä muut vastaavat tahot, joiden läsnäolo varallisuudensiirroissa edellyttää tyypillisesti luottamusta ja aiheuttaa lisäkustannuksia sekä mahdollisia komplikaatioita.

Kryptovaluutat auttavat myös niitä, jotka ovat keskitettyjen rahoituslaitosten ulkopuolella. Huomattavan suuri osa maailman väestöstä on perinteisten finanssipalveluiden ulottumattomissa. Kryptovaluutat mahdollistavat perinteisten pankkipalveluiden kaltaiset palvelut niille, jotka eivät ole perinteisten palveluiden piirissä tai eivät halua niitä käyttää. Bitcoin-verkon käyttöön tarvitaan ainoastaan toimiva Internet-yhteys. Minkään kolmannen osapuolen ei tarvitse antaa hyväksyntäänsä Bitcoin-verkkoon liittymiselle, vaan kaikki verkon osanottajat ovat tasaarvoisia.[5]

Kryptovaluuttoihin liittyvien mahdollisuuksien ja riskien sekä niiden kiihtyvää tahtia lisääntyvän käytön vuoksi niistä on tullut viime vuosina merkittävän yleisen kiinnostuksen ja lainsäädäntötarpeen kohde. Perinteisiin valuuttoihin kuten Yhdysvaltain dollariin ja euroon verrattuna kryptovaluuttoja ei ole kattavasti huomioitu kansallisissa tai kansainvälisissä lainsäädäntömekanismeissa. Säädännöllinen tyhjiö on herättänyt huolenaiheita kryptovaluuttojen käytöstä muun muassa rahanpesuun ja esimerkiksi Europol, Interpol ja Basel-instituutti perustivat työryhmän tutkimaan virtuaalivaluuttoihin liittyvää rahanpesua.[6] Tulevaisuuden kannalta on tärkeää, että kryptovaluutta-alaan kohdistettava sääntely mahdollistaa tehokkaat keinot kryptovaluuttojen laittoman käytön estämiseksi, rajoittamatta tarpeettomasti kryptovaluuttojen laillisia ja yleishyödyllisiä käyttömuotoja. Tässä tutkielmassa analysoidaan muun muassa keinoja tämän tasapainon löytämiseen, sekä arvioidaan kriittisesti jo olemassa olevien lähestymistapojen toimivuutta, tutkitaan kryptovaluuttojen käyttöä osana kansainvälistä rikollisuutta ja esitetään mahdollisia ratkaisuvaihtoehtoja. Käytettävää terminologiaa on täsmennettävä ja lainsäädäntöä täydennettävä. Samalla on kehitettävä uusia mekanismeja, jotta hajautetussa toimintaympäristössä tapahtuviin laittomuuksiin olisi mahdollista puuttua nykyistä keskitettyjen toimijoiden sääntelyyn keskittyvää preventiivistä järjestelmää tehokkaammin.

---

[4] Ks. *Nakamoto* 2008. Jo Bitcoinin julkaisuartikkelin otsikossa mainitaan teknologian ydin olemus, ”Bitcoin: A Peer-to-Peer Electronic Cash System”.

[5] Ks. Maailmanpankki: Global financial development report 2014. Noin puolella maailman aikuisväestöstä (2,5 miljardia) ei ole perinteistä pankkitiliä.

[6] Ks. Europol: Money laundering with digital currencies 2016.

1.2. Tutkimuskysymykset ja aiheen rajaus

Tutkielman tutkimuskysymyksenä on tarkoitus selvittää kryptovaluuttojen käytön ja sääntelyn haasteita rahanpesussa, terrorismin rahoituksessa ja huumekaupassa. Käsittelyssä on kiinnitetty huomiota etenkin EU:n rahanpesudirektiiveihin. Tutkimuskysymyksen voi pilkkoa käsittelyn selkeyden vuoksi neljään osaan. Tällöin syntyy seuraavanlainen käsittelyjärjestys, joka vastaa tutkielman päälukujen kirjoitusjärjestystä. Tarkoituksena on selvittää:

a) *Mitä kryptovaluutat ovat?*
b) *Mihin kryptovaluuttojen sääntely perustuu ja mitä sääntelyongelmia niihin EU:n lainsäädännössä liittyy?*
c) *Mikä on kryptovaluuttojen asema kansainvälisessä rikollisuudessa ja mitä oikeudellisia erityiskysymyksiä kryptovaluuttoihin liittyy?*
d) *Miten kryptovaluuttoja tulisi säännellä?*

Tutkimuskysymykseen rakennetaan vastausta edellä esitetyssä järjestyksessä. Tutkielman johdanto-osion jälkeen seuraa teknisempi toinen pääluku, jonka tarkoituksena on avata kryptovaluuttojen rikollisen käytön kannalta merkityksellisiä ominaisuuksia.

Kolmannessa pääluvussa selvitetään tarkemmin, miten kryptovaluutat on sisällytetty olemassa olevaan kansainväliseen AML/CFT-järjestelmään[7] ja etenkin EU:n lainsäädäntöön. Kryptovaluuttojen sääntely perustuu vankasti muun muassa FATF:n suosituksiin ja sen luomaan riskiperusteiseen arviointimalliin, jossa kryptovaluuttapörssit ja palveluntarjoajat tunnistettiin merkittäväksi sääntelyä edellyttäväksi riskitekijäksi.

Neljäs pääluku keskittyy kryptovaluuttoihin osana kansainvälistä rikollisuutta. Tässä luvussa käsiteltävät kolme rikostyyppiä: rahanpesu, terrorismin rahoittaminen ja huumausainerikokset muodostavat eheän tutkittavan kokonaisuuden, sillä niillä on selkeitä keskinäisiä yhteyksiä, mutta kryptovaluuttojen käyttöaste näiden rikostyyppien osana vaihtelee merkittävästi. Esimerkiksi terrorismin rahoituksessa varsinainen käyttöaste on yhä matala, mutta potentiaaliset riskit ovat merkittäviä. Kryptovaluutat voivat olla myös rikoksen kohteena, kuten esimerkiksi petoksissa sekä yksityishenkilöihin tai virtuaalivaluuttojen kauppapaikkoihin kohdistuvissa hakkeroinneissa. Kryptovaluutoista on tullut rahanpesun spesialistien uusi työväline, joka helpottaa toimintaa ja madaltaa kiinnijäämisriskiä. Huumausaineiden kaupankäynnissä kryptovaluuttoja käytetään yleisesti maksuvälineenä yhdessä yksityisyyttä parantavien sovellusten, kuten Tor-verkon kanssa, mikä puolestaan johtaa näyttöongelmiin. Neljännen pääluvun loppupuolella

[7] AML/CFT-käsitteen määritelmä on jäljempänä luvussa 1.4.2.

keskitytään oikeudellisiin erityiskysymyksiin, kuten näyttökysymyksiin, rikoshyödyn hallussa pitämiseen sekä menettämisseuraamuksiin liittyvään problematiikkaan. Korkeimman oikeuden linja on ollut, ettei näyttökynnystä saa huumausainerikoksissa laskea.[8] Kryptovaluuttojen käyttö huumausaineiden kaupassa on kuitenkin johtanut tilanteeseen, jossa tapausten selvittäminen on vaikeutunut, konkreettisen näytön etsimisen kustannukset ovat nousseet merkittävästi ja kustannustehokkuussyistä on jouduttu tekemään tutkinnanrajoituksia.

Viidennessä pääluvussa avataan eri lainsäätäjien näkökulmia ja pohditaan ratkaisuvaihtoehtoja sääntelyongelmiin. Tutkimuksen perusväite on, että kryptovaluuttojen sääntelytarve on kaksitasoinen. Perinteisen keskitetyn sääntelyn lisäksi tarvitaan uudenlaista hajautettua sääntelyä.

1.3. Tutkimusmetodi ja oikeuslähteet

Tutkimusmetodilla viitataan tutkimusmenetelmään, jolla tietoa muodostetaan ja perustellaan. Tämän tutkimuksen pääasiallisena tutkimusmetodina on lainoppi eli oikeusdogmatiikka, jonka avulla systematisoidaan voimassa olevaa oikeutta. Tutkin aiheeseen soveltuvin osin voimassa olevia lakeja, kuten rikoslakia sekä kansainvälisiä sopimuksia ja EU-tason säädöksiä ja selvitän, miten kryptovaluuttoja käytetään rahanpesussa, terrorismin rahoituksessa ja huumausainerikoksissa sekä mitä sääntelyongelmia kryptovaluuttoihin liittyy etenkin EU:n rahanpesudirektiiveissä. Tutkielman pääteemana on analysoida kriittisesti nykyisen rahanpesun- ja terrorismin rahoituksen vastaisen järjestelmän heikkouksia, etsiä ratkaisuja ja korostaa vaihtoehtoisten, perinteisen sääntely-ympäristön ulkopuolisten, toimien tärkeyttä.

Muita metodeja ovat oikeussosiologia, oikeuspolitiikka (kriminaalipolitiikka) ja oikeusvertailu. Kryptovaluutat ovat poikkitieteellinen ilmiö, jota on tarkoituksenmukaista tutkia laajemmasta yhteiskunnallisesta näkökulmasta. Kryptovaluuttoihin liittyvän rikollisuuden tason, rikoksentekijöiden sekä rikosten ehkäisyn ymmärtäminen vaatii myös itse kryptovaluuttojen yhteiskunnallisen merkityksen ymmärtämistä. Tämä näkyy siinä, miten paljon uutta sääntelyä kryptovaluutat ovat vaatineet ja miten usein sitä on jälkikäteen täydennetty. Oikeuspoliittinen suunta ilmenee tutkimuksen loppuosassa, jossa käsitellään protokollatasolla tapahtuvaa hajautettua sääntelyä. Tutkielman tavoitteena on korostaa perinteisen järjestelmän puutteiden korjaamisen lisäksi mahdollisuutta aivan uudenlaisiin ratkaisuvaihtoehtoihin, ja kiinnittää huomiota preventiivisen sääntelyn siirtämiseen lohkoketjun hajautettuun toimintaympäristöön.

[8] Ks. KKO 2018:3, jota käsitellään jäljempänä luvussa 4.7.

Kryptovaluuttojen aiheuttamaa paradigmanmuutosta kuvaa hyvin niiden maineen kehittyminen viimeisen vuosikymmenen aikana. Esimerkiksi Bitcoin, jota sen alkuvuosina käytettiin lähinnä huumausainekaupan maksuvälineenä, on nyt matkalla pienten valtioiden viralliseksi valuutaksi. Vallanpitäjät alkavat ymmärtää lohkoketjuteknologian mahdollisuuksia ja olisi luonnollista, että lainsäätäjien suhtautumistavassa tapahtuisi muutos. Lohkoketjuteknologian uhkia ei voi kartoittaa, jos teknologian potentiaaliin ei suhtauduta realistisesti ja kaikkia vaihtoehtoja tutkita. Tämän tutkimuksen avainkysymyksenä on tarkastella kriittisesti edeltäviä teorioita, käsitteitä ja periaatteita ja niiden asianmukaisuutta. Päämääränä on erityisesti kiinnittää huomiota olemassa olevan järjestelmän puutteisiin ja etsiä niihin ratkaisuja. Oikeuden yleistieteiden lisäksi tutkimus nojautuu myös muihin tieteisiin ajan yhteiskunnallisten vaatimusten selvittämiseksi. Oikeusvertailu näkyy eri lainkäyttöalueiden sääntelyratkaisujen vertailussa.

Kotimaiset kirjallisuuslähteet, hallituksen esitykset ja EU-direktiivit muodostavat hyvän rungon tutkielman ydinkysymysten käsittelylle, mutta huomattavan suuri osa tutkielmasta rakentuu myös ulkomaisten tieteellisten artikkelien varaan. Tämä johtuu siitä, että kryptovaluutat ovat verrattain tuore ilmiö ja niitä koskevaa suomalaista kirjallisuutta on saatavilla vähän. Tutkimuksessa viitataan myös erilaisiin verkosta löytyviin raportteihin, joita ovat laatineet muun muassa eri valtiot, Europol, sekä kryptovaluuttojen analysointiin keskittyvät itsenäiset tahot, kuten esimerkiksi Chainalysis.

1.4. Keskeisistä käsitteistä

1.4.1. Kryptovaluutta ja virtuaalivaluutta käsitteiden oikeellisuudesta

Tämän tutkielman käsittelyn keskiössä ovat kryptovaluutat. Oikeuskirjallisuudessa käytetään vaihtelevasti ja synonyymin tapaisesti käsitteitä kryptovaluutta ja virtuaalivaluutta. Käsitteiden käyttö täysin samanarvoisina on kuitenkin teknisestä näkökulmasta virheellistä ja oikeudellisesta näkökulmasta harhaanjohtavaa. Virtuaalivaluutta on yleiskäsite, joka kattaa sekä hajautetut että hajauttamattomat virtuaalivaluutat. Kryptovaluutoista puhuttaessa tarkoitetaan yleisesti ottaen nimenomaan hajautettuja virtuaalivaluuttoja. Ero on merkittävä muun muassa siksi, että suurin osa niistä lainsäädännöllisistä haasteista, joita tässä tutkielmassa käsitellään, aiheutuu virtuaalivaluuttojen hajautetusta luonteesta. Hajauttamattomiin eli keskitettyihin virtuaalivaluuttoihin ei liity läheskään yhtä mittavia lainsäädännöllisiä haasteita kuin hajautettuihin kryptovaluuttoihin.

Keskitettyjen virtuaalivaluuttojen takana on aina jokin keskitetty taho, joka on mahdollista asettaa vastuuseen ja johon sanktiotoimet voidaan kohdistaa.[9] Hajautetut virtuaalivaluutat eivät sen sijaan tarvitse keskitettyä liikkeellelaskijaa tai auktoriteettia transaktioiden varmentamiseen tai uusien vaihdantayksikköjen luomiseen. Kryptovaluutta on vakiintunut synonyymiksi hajautetuille virtuaalivaluutoille ja kuvaa paremmin sitä teknisen kehityksen jatkumoa, joka vaatii myös lainsäätäjiltä uudenlaista suhtautumistapaa. Kryptovaluutat ovat avoimen lähdekoodin P2P-ratkaisu[10], jossa arvonsiirrot varmennetaan kryptografian avulla ilman pankkien tai muiden finanssilaitosten väliintuloa. Yksinkertaisimman määritelmän mukaan kyse on digitaalisesta käteisestä, jota eivät koske samat fyysiset rajoitukset kuin perinteisen käteisen vaihdantaa.

Tutkielma on lähestymistavaltaan rikosoikeudellinen ja hajautuneisuus on suurin rikollisen käytön mahdollistaja. Näin ollen on loogista puhua kryptovaluutoista. Virtuaalivaluutta käsitettä käytetään tässä tutkielmassa, kun kyseinen termi esiintyy säädöksessä, johon viitataan. Toisinaan erilaisissa asiakirjoissa nähdään puhuttavan myös krypto- tai virtuaalivarallisuudesta. Yhtenä näiden termien käyttöön liittyvänä etuna on, etteivät ne sisällä sanaa ”valuutta”. Tämä on hyödyllistä siitä syystä, että kryptovaluutoilla on paljon sisarprojekteja, jotka perustuvat samoihin teknologisiin ratkaisuihin, mutta joiden pääasiallisena tarkoituksena ei ole toimia valuuttana. Tällaisia projekteja ovat muun muassa erilaiset hyöty- ja hallintopoletit. Lainsäädännössä esiintyvässä terminologian vaihtelu ja epäjohdonmukaisuus luo pahimmassa tapauksessa lainsäädännöllisiä aukkokohtia, joita rikolliset voivat käyttää hyväksi.

1.4.2. AML/CFT-järjestelmä

Käsite AML/CFT-järjestelmä viittaa tässä tutkielmassa rahanpesun ja terrorismin rahoituksen estämisen järjestelmään. Lyhenne AML viittaa englanninkieliseen ilmaisuun ”Anti-money Laundering”. Ulkomaisissa artikkeleissa esimerkiksi käsite ”AML-systems” on yleinen. Lyhenne CFT viittaa puolestaan englanninkieliseen ilmaisuun ”Combating the Financing of Terrorism”. Ilmiöt, joihin näillä käsitteillä viitataan, ovat lähellä toisiaan, joten kansainvälisessä kontekstissa puhutaankin usein AML/CFT-järjestelmästä. Olemassa oleva järjestelmä, johon myös kryptovaluutat on sovitettu ja jonka kautta niitä säännellään, perustuu etenkin AML/CFT-riskien ehkäisyyn.

---

[9] Myöhemmin luvussa 4.4. käsiteltävä Venezuelan ”petro” on hyvä esimerkki keskitetystä virtuaalivaluutasta. Sen käyttöönotto aiheutti välittömän vastareaktion muun muassa USA:ssa, joka asetti Venezuelaa kohtaan pakotteita. Hajautettujen virtuaalivaluuttojen kohdalla tällaisten sanktiotoimenpiteiden toteuttaminen ei ole mahdollista, koska niillä ei ole keskitettyä vastuutahoa.

[10] Peer-to-Peer eli vertaisverkko tarkoittaa verkkoa, jossa vaihdanta tapahtuu suoraan verkon jäsenten välillä ilman keskitettyä valvojaa.

2. KRYPTOVALUUTAT JA LOHKOKETJUTEKNOLOGIA

2.1. Kryptovaluuttojen oikeudellinen kehys

Verkkorikollisuus muodostaa nykypäivänä laajan uhan useimpien maiden kriittiselle infrastruktuurille. Viimeisen kymmenen vuoden aikana tietojärjestelmistä on tullut yhä hienostuneempia ja yhteenliitettävyys on lisääntynyt. Samalla on kuitenkin syntynyt uudenlaisia haavoittuvuuksia, joihin ei ole vielä kyetty tehokkaasti puuttumaan. Verkkorikollisuuden nopea kehitys ja standardisoidun määritelmän puuttuminen tekee eri virastojen välisestä yhteistyöstä ja konkreettisten verkkorikollisuutta koskevien lakien säätämisestä haastavaa. Kryptovaluuttojen myötä lisääntynyt desentralisaatio[11] on lisännyt ja helpottanut verkkorikollisuutta. Kuten verkkorikollisuus, myös kryptovaluutat ovat luoneet määrittely- ja sääntelytarpeen. Euroopan unionin alueella sääntely perustuu vuonna 2018 voimaantulleeseen EU:n viidenteen rahanpesudirektiiviin.

Suomessa edellä mainittu direktiivi johti 26.4.2019 voimaan tulleeseen lakiin virtuaalivaluuttojen tarjoajista 572/2019 (jatkossa myös virtuaalivaluuttalaki). Lakia sovelletaan sen 1 §:n mukaan ”virtuaalivaluutan tarjoajien harjoittamaan liiketoimintaan”. Lain 4 §:ssä säädetään, että ”elinkeinonharjoittaja saa tarjota virtuaalivaluuttaan liittyviä palveluita vain, jos se on rekisteröity tämän lain mukaisesti virtuaalivaluutan tarjoajaksi”.

Virtuaalivaluuttalaki tarjoaa myös määritelmän virtuaalivaluutoille sekä virtuaalivaluutan tarjoajille. Sen 2 §:n 1 momentin 1 kohdan määritelmän mukaan:

1) ”virtuaalivaluutalla tarkoitetaan digitaalisessa muodossa olevaa arvoa.
a) jota keskuspankki tai muu viranomainen ei ole laskenut liikkeeseen ja joka ei ole laillinen maksuväline;
b) jota henkilö voi käyttää maksuvälineenä; ja
c) joka voidaan siirtää, tallentaa ja vaihtaa sähköisesti.”

2 §:n 1 momentin 2 kohdassa määritellään virtuaalivaluutan tarjoaja:

2) *”Virtuaalivaluutan tarjoajalla* virtuaalivaluutan liikkeeseenlaskijaa, virtuaalivaluutan vaihtopalvelua ja sen markkinapaikkaa sekä lompakkopalvelun tarjoajaa”

Ennen nykyisen sääntelykehyksen muodostumista kryptovaluutat ja niiden tarjoajat olivat käytännössä sääntelemättömiä. Kryptovaluuttojen laajan suosion huomioon ottaen sääntelemätön tila oli merkittävä riski niin kuluttajille, sijoittajille kuin myös yleiselle turvallisuudelle. Hallituksen esityksessä HE 167/2018 vp viitataan Euroopan pankkiviranomaisen heinäkuussa 2014 laatimaan selvitykseen, jossa kartoitetaan kryptovaluuttoihin liittyviä turvallisuusriskejä:

[11] Desentralisaatiosta eli hajautuneisuudesta kerrotaan lisää myöhemmin osiossa 2.7.1.

> ”Euroopan pankkiviranomainen on lausunnossaan heinäkuussa 2014 yksilöinyt noin 70 virtuaalivaluuttoihin liittyvää riskiä, joista 29 kappaletta on suuria riskejä. Yleisiä virtuaalivaluuttoihin liittyviä suuria riskejä ovat muun muassa riskit käyttäjille valuutanvaihtajan petoksista, valuutan arvon rajut heilahtelut, valuuttaan kohdistuvat varkaudet, henkilöllisyyden väärinkäytökset ja valuutanvaihtojärjestelmän epäluotettavuus. Rahoitusjärjestelmän luotettavuuden kannalta virtuaalivaluuttoihin liittyy merkittävä riski siitä, että niitä käytetään rahanpesun ja terrorismin rahoittamisen tai muun rikollisen toiminnan tarkoitusperiin. Käyttäjille aiheutuu merkittäviä riskejä virtuaalivaluutan epäluotettavuudesta maksuvälineenä, mikä saattaa ilmetä esimerkiksi siten, että valuuttaa ei hyväksytä maksuvälineenä, valuuttaa veloitetaan väärin, valuuttaa ei voida muuntaa lailliseksi maksuvälineeksi, valuutanvaihtajan toiminta päättyy tai valuutan arvoa manipuloidaan.” [12]

EU:n rahanpesudirektiivin neuvotteluissa päädyttiin lopputulokseen, joka ei pitänyt sisällään viittausta virtuaalivaluuttojen tarjoajiin. Kuitenkin Ranskassa vuonna 2015 sattuneiden terroriiskujen motivoimana komissio julkaisi toimintasuunnitelman terrorismin rahoituksen torjunnan tehostamiseksi. Osana tätä suunnitelmaa tietyt rahanpesudirektiivin osat otettiin uudestaan käsittelyyn, jotta voitaisiin puuttua haavoittuvuuksiin terrorismin rahoituksen torjunnassa Euroopassa, mukaan lukien virtuaalivaluuttojen ostamiseen ja käyttöön liittyvään anonymiteettiin.[13] Tehdyt muutokset johtivat EU:n viidennen rahanpesudirektiivin säätämiseen ja toivat virtuaalivaluutan tarjoajat sääntelyn piiriin. Direktiivi myös tehosti valvovien viranomaisten välistä tietojenvaihtoa sekä laajensi asiakkaan tuntemiseen sovellettavia toimenpiteitä. Tästä säädetään nykyään virtuaalivaluuttalain 13 §:ssä, jonka mukaan:

> ”virtuaalivaluutan tarjoajan on tunnettava asiakkaansa. Virtuaalivaluutan tarjoajan on tunnistettava asiakkaan tosiasiallinen edunsaaja ja henkilö, joka toimii asiakkaan lukuun, sekä lisäksi tarvittaessa todennettava näiden henkilöllisyys. Tässä momentissa säädettyä velvollisuutta täytettäessä voidaan hyödyntää 2 momentissa tarkoitettuja järjestelmiä.
>
> Virtuaalivaluutan tarjoajalla on oltava riittävät riskienhallintajärjestelmät, joilla se voi arvioida asiakkaista toiminnalleen aiheutuvia riskejä.
>
> Asiakkaan tuntemisessa on lisäksi voimassa, mitä rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä annetussa laissa (444/2017) säädetään.”

[12] Ks. HE 167/2018 vp, s. 45
Ks. myös EPV: Opinion on virtual currencies 2014. Raportissa käsitellään virtuaalivaluuttoihin liittyviä turvallisuusriskejä. Riskejä eritellään tarkemmin raportin sivuilla 5 ja 21–27.
[13] EPV: Opinion of the European Banking Authority on the EU Commission’s proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD) 2016, s. 2.

2.2. Bitcoin

Kryptovaluutat yhdistetään yleisesti niin sanottuun lohkoketjuteknologiaan. Tunnetuin ja alkuperäinen lohkoketjusovellus on nimimerkillä Satoshi Nakamoto esiintyneen henkilön tai tahon luoma Bitcoin-kryptovaluutta.[14] Bitcoin on virtuaalinen, hajautettu ja pseudo-anonyyminen valuutta, joka ei ole minkään hallituksen tai oikeushenkilön tukema.[15]

Bitcoin on lailliseen maksuvälineeseen vaihdettavissa oleva virtuaalivaluutta. Se on myös ensimmäinen kryptovaluutta eli salausalgoritmiikkaan perustuva virtuaalivaluutta, jota salaus suojaa. Kryptovaluutta rakentuu julkisiin ja yksityisiin avaimiin, joilla arvoa siirretään henkilöltä toiselle ja jotka salataan ennen jokaista siirtoa. Kryptovaluuttajärjestelmän turvallisuus, eheys ja saldo perustuvat louhijoiden[16] keskinäiseen luottamussuhteeseen.[17]

Bitcoin-yksikkö[18] koostuu ainutlaatuisesta numeroiden ja kirjaimien yhdistelmästä. Bitcoinin arvo markkinoilla perustuu kysyntään ja tarjontaan. Bitcoinit ovat siirrettävissä sähköisesti käyttäjien välillä, ja niitä voidaan vaihtaa fiat-valuuttoihin[19] tai toisiin kryptovaluuttoihin. Kuka tahansa voi käyttää Bitcoin-verkkoa ja Bitcoin-osoitteita voi hallinnoida joko kryptovaluuttapörssi, käyttäjä itse pilvipalveluna tarjottavassa lompakossa tai fyysisin talletusvälinein. Maksuliikenne on julkisesti nähtävissä käyttäjien rekisterissä yksilöitynä Bitcoin-tilinumeroihin, mutta nähtävät tunnisteet eivät ole yhdistettävissä suoraan kehenkään yksittäiseen henkilöön. Bitcoineja tulee ajan kuluessa olemaan korkeintaan 21 miljoonaa kappaletta, sillä niiden enimmäismäärä on rajattu. Tämä liikkeeseen laskettava määrä arvioidaan saavutettavan noin vuoteen 2140 mennessä.[20]

Bitcoinin kaltaisten kryptovaluuttojen perusideana ja tavoitteena on poistaa tarve luotettavien kolmansien osapuolien olemassaololle tavanomaisissa rahaliikenteen transaktioissa ja tarjota pseudo-anonyyminen vaihtoehto maksuliikenteelle yksilöiden välillä. Bitcoinilla on monia hyviä käyttötarkoituksia, mutta sen tekniset ominaisuudet houkuttelevat puoleensa myös rikollisia. Bitcoin on esimerkiksi edistänyt erilaisten lunnashaittaohjelmien[21] käyttöä, sitä hyödynnetään

[14] Ks. *Nakamoto* 2008.
[15] Ks. *Grinberg* 2011, s. 160.
[16] Louhijoiden asemasta verkoston osana kerrotaan lisää konsensusalgoritmeja käsittelevässä luvussa 5.6.
[17] HE 167/2018 vp, s. 45.
[18] Puhuttaessa esimerkiksi Bitcoin-verkosta kirjoitetaan Bitcoin yleensä isolla. Jäljempänä puhutaan joissakin yhteyksissä bitcoineista vaihdettavina laskentayksikköinä, jolloin valuutan nimi kirjoitetaan pienellä. Ks. myös bitcoin.org verkkosivulta lisätietoja Bitcoin-sanastosta.
[19] Fiat-valuutan määritelmä on jäljempänä luvussa 2.5.
[20] HE 167/2018 vp, s. 45.
[21] Ks. *Hajdarbegovic* Coindesk 2015.

osana modernia rahanpesua[22] ja käytetään laittoman kaupankäynnin maksuvälineenä dark web-bissä.

2.3. Ethereum ja älysopimukset

Myöhemmin on luotu myös runsain mitoin muita kryptovaluuttoja, joista merkittävimpiin kuuluu ohjelmoitava lohkoketju Ethereum, jolla toimii erilaisia lohkoketjuteknologiaa hyödyntäviä desentralisoituja sovelluksia[23]. Ethereum-lohkoketjulla toimivat sovellukset ovat hajautettuja, eli toisin sanoen mikään yksittäinen kokonaisuus tai ihminen ei niitä ohjaa. Hyvin merkittävä osa tämän hetken olemassa olevista kryptovaluutoista toimii osana Ethereum-verkkoa. Tarjolla olevat palvelut vaihtelevat uudenlaisista desentralisoidun talouden[24] sovelluksista kryptovaluuttalompakoihin, desentralisoituihin markkinapaikkoihin, peleihin ja moniin muihin ohjelmoituihin sovelluksiin.[25]

Ethereumin ohjelmoitavuus perustuu niin sanottuihin älysopimuksiin. Älysopimuksen voi määritellä kahdesta näkökulmasta. Se voi juridisessa mielessä tarkoittaa sopimusta tai sopimuksen osia, jotka jokin ohjelmisto toteuttaa. Älysopimuksen voi myös määritellä tietoteknisestä näkökulmasta koodinpätkäksi, joka on suunniteltu toteuttamaan tietyt toiminnot ennalta määrättyjen ehtojen täyttyessä. Nämä ehdot ovat yleensä tallennettuna hajautettua kirjanpitoteknologiaa[26] eli lohkoketjua käyttäen. Hyvä esimerkki älysopimuksesta on esimerkiksi kryptovaluutta, johon on ohjelmoitu ennalta määrätty äänestysmekanismi.[27]

Molemmat tulkinnat sisältäväksi määritelmäksi voidaan ottaa seuraavanlainen tulkinta. Älysopimus on automatisoitava ja täytäntöönpanokelpoinen sopimus. Se on tietoteknisesti automatisoitu, vaikka joidenkin osien soveltaminen saattaa edellyttää ihmisen työpanosta. Älysopimus on täytäntöönpantavissa joko oikeuksien ja velvoitteiden valvonnan kautta tai suorittamalla peukaloimatonta[28] tietokonekoodia.[29]

---

[22] Ks. *Greenberg* Wired 2014.
[23] Eng. decentralized applications, "Dapps".
[24] Eng. decentralized finance.
[25] Ks. Ethereum.org. sivustolta lisätietoja ohjelmoitavan lohkoketjun ominaisuuksista ja käyttötarkoituksista.
[26] Eng. distributed ledger technology (DLT).
[27] Ks. ISDA – *Linklaters* 2017, s. 4–5. Älysopimuksella on olemassa sekä juridinen, että tietotekninen määritelmä.
[28] Peukaloimattomuudella viitataan tässä koodin eheyteen eli siihen, että se vastaa ohjelman alkuperäistä tarkoitusta.
[29] Ks. ISDA – *Linklaters* 2017, s. 5. Älysopimuksen määritelmässä on mahdollista yhdistää juridinen ja tietotekninen määritelmä tavalla, jolloin merkitys on molemmista näkökulmista hyväksyttävä.

Älysopimusten perusominaisuuksiin kuuluva desentralisaatio muodostaa kuitenkin dilemman. Koska mikään yksittäinen kokonaisuus tai ihminen ei hallitse verkkoa ovat ne samat ominaisuudet, jotka tekevät älysopimuksista hyödyllisiä, vapaasti myös rikollisten hyödynnettävissä. Seuraavaksi kuvataan kolmen tällaisen ominaisuuden positiivisia ja negatiivisia vaikutuksia.

Ensimmäinen ominaisuus on reilu vaihto, joka tarkoittaa mahdollisuutta toteuttaa älysopimuksen välityksellä vaihtoja toisiaan kohtaan epäluuloisten osapuolten välillä. Älysopimus poistaa luottamuksen ja maineen tarpeen, sillä sopimuksen ehdot voidaan toteuttaa peruuttamattomasti älysopimuksella ilman, että kumpikaan osapuoli voi huijata toista esimerkiksi vetäytymällä vaihdosta. Kääntöpuolena tämä koskee myös rikollisia. Rikollistenkaan ei tarvitse älysopimuksen ansiosta luottaa toisiinsa, joten rikollisilla ei ole tarvetta enää hyödyntää sellaisia perinteisiä välittäjätahoja, joiden hyödyntäminen lisäisi toimintaan luottamuselementin ja siten nostaisi kiinnijäämisriskiä.[30]

Seuraava ominaisuus on minimaalinen vuorovaikutus, jolla viitataan siihen, että koska transaktiot voidaan hoitaa peruuttamattomasti ja varmasti älysopimuksen avulla, ei ole enää tarvetta esimerkiksi tapaamisille. Tämä tarkoittaa toisaalta myös, että lainvalvontaviranomaisten on vaikeampi valvoa laitonta toimintaa, koska havaittavia vuorovaikutustilanteita ei ole tai niitä on vähemmän.[31]

Viimeisenä mainittavana ominaisuutena ovat ulkomaailmaan liittyvät johdannaiset voivat tarkoittaa esimerkiksi lohkoketjulla varmennettua osakkeiden johdannaismarkkinaa. Lohkoketjuteknologiaa on käytetty myös esimerkiksi reaalimaailman tapahtumiin liittyvässä vedonlyönnissä. Rikollisille transaktiot voivat olla esimerkiksi reaalimaailman fyysisten rikosten lohkoketjupohjaisia johdannaisia. Tämä tarkoittaa, että rikollistaho pystyisi esimerkiksi tilaamaan terroristijärjestöltä pommi-iskun ja iskun tullessa yleiseen tietoon älysopimuksen algoritmi toteaisi esimerkiksi uutisvirran perusteella sopimuksen täytetyksi ja suorittaisi vastineen.[32]

Desentralisoidut älysopimusjärjestelmät toimivat samalla tapaa pseudo-anonyymisesti kuin Bitcoin eli transaktiot eivät suinkaan ole näkymättömiä, mutta niitä voi olla vaikea yhdistää reaalimaailman henkilöihin. Jäljittämisen vaikeus ja edellä mainitut ominaisuudet ovat omiaan tekemään älysopimuksista houkuttelevan työkalun rikollisille.

---

[30] Ks. *Juels – Kosba – Shi* 2016, s. 285.
[31] Ibid. s. 285.
[32] Ibid. s. 285–286.

2.4. Yksityisyysvaluutta Monero

Kryptovaluuttojen muodostama uhka ei rajoitu ainoastaan Bitcoiniin. Vaihtoehtoisia kryptovaluuttoja on useita ja niiden ominaisuudet vaihtelevat tarpeen mukaan. Osa kryptovaluutoista keskittyy juuri yksityisyyden maksimointiin. Hyvänä esimerkkinä tällaisesta kryptovaluutasta on Monero, jonka lohkoketju ei Bitcoinin ja Ethereumin tavoin ole läpinäkyvä.

Monero käyttää erilaisia yksityisyyttä parantavia tekniikoita taatakseen käyttäjiensä yksityisyyden.[33] Monero vaikuttaisi näennäisesti olevan teknisten ominaisuuksiensa ansiosta suorastaan täydellinen rikolliseen käyttöön. Rikollisen käytön vuoksi esimerkiksi Yhdysvaltojen verotoimisto IRS tarjoaa jopa 625 000 dollarin suuruista palkkiota Moneron koodin murtamisesta.[34]

2.5. Fiat-valuutat

Fiat-valuutat ovat yksinkertaisesti valtioiden liikkeeseen laskemia valuuttoja, joilla ei ole itseisarvoa. Niiden arvo ei perustu kultaan, hopeaan tai muuhun vastaavaan fyysiseen hyödykkeeseen, vaan valtionhallinnon luomiin säännöksiin tai lakeihin sen asemasta laillisena maksuvälineenä. Fiat-valuutan arvo perustuu kysynnän ja tarjonnan suhteeseen ja liikkeeseen laskevan valtion vakauteen. Suurin osa nykyaikaisista paperivaluutoista on fiat-valuuttoja, mukaan lukien Yhdysvaltain dollari, euro ja muut tärkeimmät globaalit valuutat.[35]

Lainsäätäjät ovat keskittyneet fiat-ramppien[36] sääntelyyn, koska rikollisilla on tarve käyttää keskitettyjä toimijoita valuutanvaihtoihin fiat-valuutoista kryptovaluutoiksi ja toisinpäin. On todennäköistä, että kryptovaluuttoihin liittyvä rikollisuus irtautuu ainakin osin fiat-valuuttojen käytöstä, kun kryptovaluuttojen käyttö maksuvälineenä yleistyy ja varainsiirrot takaisin fiat-valuutaksi vähenevät.

[33] Ks. Moneron verkkosivut.
[34] Ks. *Erb* Forbes 2020.
[35] Ks. Merriam-Webster. "fiat money."
[36] Eng. "fiat on/off ramp" tarkoittaa esimerkiksi kryptovaluuttapörssiä, joka vaihtaa dollareita, euroja tai muuta globaalisti tunnettua fiat-valuuttaa kryptovaluutoiksi ja toisinpäin.

2.6. Digitaalisen rahan historia osana rikollisuutta

Alkeellisempia virtuaalivaluuttoja on ollut olemassa jo ennen Bitcoinin, Ethereumin ja muiden lohkoketjupohjaisten älysopimusjärjestelmien olemassaoloa. Tähän peilaten on tärkeää ymmärtää, että vaikka virtuaalivaluuttojen yhteydessä puhutaan usein lohkoketjusta ei tämä tarkoita, että kaikki virtuaalivaluutat olisivat aina perustuneet lohkoketjuteknologiaan. Virtuaalivaluutan määritelmän sisälle mahtuu myös muihin teknisiin toteutustapoihin perustuvia ratkaisuja.[37]

Anonyymin elektronisen valuutan käyttöä jäljittämättömien maksujen suorittamiseen alettiin tutkia jo vuonna 1982[38] ja jo varhain pohdittiin mahdollisuutta ”täydellisten rikosten” tekemiseen hyödyntäen valuutanvaihdon anonyymiyttä, tehden rikosten jäljittämisestä mahdotonta.[39]

Varhaiset elektronisen käteisen järjestelmät perustuivat käteistalletuksiin, joissa luotettava kolmas osapuoli linkitti eri osapuolet ja maksusuoritukset. Linkitys oli mahdollista klassisissa elektronisen käteisen järjestelmissä, joissa käyttäjä tunnistaa itsensä anonyymin käteisnoston yhteydessä, mutta kyse ei ollut Bitcoinin kaltaisista pseudo-anonyymisesti toimivista kryptovaluutoista.[40]

Internetaikakauden tyypillisiin haittaohjelmiin kuuluvia niin sanottuja Ransomware-viruksia on esiintynyt jo vuodesta 1989 asti.[41] Nykymuotoiset Ransomware-hyökkäykset hyödyntävät Bitcoinin pseudo-anonyymisyyttä lunnaiden maksuun. Esimerkiksi tunnetuimpiin variantteihin lukeutuvien CryptoLocker- ja CryptoWall-haittaohjelmien on arvioitu levinneen vuosien aikana useisiin miljooniin tietokoneisiin ja keränneen lunnaina yhteensä satojen miljoonien, ellei jopa miljardien arvosta kryptovaluuttoja, kuten Bitcoinia.[42] Haittaohjelmat olivat jo vuonna 2013 saastuttaneet yli 250 000 laitetta ja hyökkäykset olivat kohdistuneet muun muassa valtion virastoihin kuten poliisiasemiin.[43]

Lunnaita vaadittiin bitcoinien muodossa myös vuonna 2020 sattuneessa psykoterapiakeskus Vastaamon tapauksessa, jossa Vastaamon asiakkaat saivat sähköposteihinsa arkaluonteisia tietojaan koskevia kiristysviestejä, joissa heitä vaadittiin maksamaan kiristäjille 200–500 euron

[37] Ks. *Atallah – Hautamäki – Koskikare* 2019, s. 7.
[38] Ks. *Chaum* 1983. s. 199–203.
[39] Ks. *Naccache – von Solms* 1992, s. 581–583.
[40] Ks. *Camenisch – Piveteau – Stadler* 1995, s. 209–219.
[41] Ks *Bates* 1990, s. 3–6.
[42] Ks. *Kotov – Rajpal* 2014, s. 3.
[43] Ks. *Blue – Day* ZDNet 2013.

suuruisia lunnasmaksuja. Kiristäjät uhkasivat julkaista uhrien tietoja, mikäli maksua ei suoritettu annetun ajan kuluessa.[44]

Perinteinen verkkorikollisuus on ottanut kehitysaskelia hyödyntäen kryptovaluuttojen tarjoamaa anonymiteettiä ja transaktioiden jäljittämisen vaikeutta. Taitavat rikolliset osaavat siirrellä valuuttoja siten, että niiden osoitteet häivytetään sekoittamalla bitcoinit keskenään niin sanottujen mikserien avulla tehden maksuliikenteen seuraamisesta lähes mahdotonta.[45]

2.7. Kryptovaluuttojen tekninen toimintatapa

2.7.1. Desentralisaatio eli hajautuneisuus

Tutkielmassa asetetun tutkimuskysymyksen käsittelyn kannalta on olennaista selvittää myös kryptovaluuttojen käytännön toiminnan keskeiset tekniset lähtökohdat. Esimerkiksi sellaiset kryptovaluuttojen tyypilliset ominaisuudet kuten desentralisaatio, luottamukseton luottamus, muuttamattomuus, yksityisyys ja transaktioiden lopullisuus ovat olennaisia ominaisuuksia niin kryptovaluuttojen laillisessa kuin myös rikollisessa käytössä.

Ennen lohkoketjun keksimistä yksittäisten toimintojen koordinointi internetin välityksellä ei ollut mahdollista ilman keskitettyä tahoa. Toisilleen tuntemattomille henkilöille ei ollut mahdollista varmistaa transaktioiden toteutumista, ilman keskitettyä tahoa, joka varmistaa, että transaktiot ovat todella toteutuneet eikä niihin liity vilppiä tai virheitä.[46]

Lohkoketjun hajautettu konsensusmekanismi mahdollistaa avoimuuden ja innovaation sellaisillakin sektoreilla, joilla piti aiemmin luottaa johonkin keskitettyyn auktoriteettiin. Juuri keskitetyn auktoriteetin puuttuminen on lohkoketjun ja kryptovaluuttojen merkittävin ominaisuus. Ilman hajautettua rakennetta vastaavanlaiset palvelut olisi teknisesti helppo toteuttaa, mutta tällöin jouduttaisiin luottamaan keskitettyyn tahoon.[47]

Kryptovaluuttojen tekninen toteutusmuoto mahdollistaa esimerkiksi täysin hajautetun maksuliikenteen. Näin ollen yksilöt voivat lähettää ja vastaanottaa valuuttaa suoraan keskenään ilman perinteisen kolmannen keskitetyn tahon läsnäoloa. Ostajat ja myyjät käyvät keskenään kauppaa lohkoketjun välityksellä eikä minkään yksittäisen osapuolen häiriö voi kaataa koko verkon toimintaa. Hajautuneisuus tekee verkosta jatkuvasti saatavilla olevan ja toimintavarman. Siinä

[44] Ks. *Hara ym.* Yle 2020.
[45] Ks. *Breuker – Böhme – Möser* 2013.
[46] Ks. *De Filippi – Wright* 2015.
[47] Ks. *Adem ym.* 2018, s. 1.

missä pörssit ja pankit ovat aika ajoin kiinni kryptovaluutat toimivat ympäri vuorokauden ja läpi vuoden.

Nykymaailmassa merkittävä osa mediasisällöstä ja kuluttajille kaupattavasta viihdeaineistoista, kuten esimerkiksi musiikki, elokuvat ja videopelit, ovat digitaalisessa muodossa. Yhä harvempi ostaa näissä tapauksissa fyysisen tuotteen kaupan hyllyltä ja monet tuotteet tilataan kotiovelle. Innovaatioihin kuuluvat myös niin sanotut NFT:t[48] eli ”non-fungible tokenit”[49], jotka mahdollistavat täysin uniikkien mediasisältöjen, kuten digitaalisen taiteen jakamisen. Perinteisen fyysisen taidekaupan rahanpesuongelma näyttäisi NFT:iden kasvaneen suosion myötä olevan siirtymässä digitaaliseen taiteeseen. Joidenkin NFT-kauppapaikkojen asiakkaantuntemisen toimenpiteissä on puutteita, joita on mahdollista hyödyntää rahanpesuun.[50] NFT:itä käytetään myös reaalimaailman tuotteiden, kuten kenkien aitouden todistamiseen.[51] Jakamistalouden ja vertaisverkkojen aikakaudella on loogista, että myös valuutansiirrot on mahdollista toteuttaa ilman välikäsiä.

Kryptovaluuttoja ja lohkoketjuteknologiaa käytetään hyödyllisten ja laillisten tarkoituksien lisäksi myös laittomuuksiin. Osin tästä syystä ajatus kryptovaluuttojen totaalisesta kieltämisestä on aika ajoin noussut esiin mediassa. Hajautuneisuus aiheuttaa kuitenkin tässä pyrkimyksessä valtioille ja lainsäätäjille päänvaivaa. Verkon hajautettu rakenne nimittäin tarkoittaa, että verkkoa ylläpitävät tahot sijaitsevat globaalisti ympäri maailmaa, eikä verkkoa ole edes mahdollista sulkea saattamalla jokin yksittäinen taho vastuuseen. Yhdysvaltain senaatin pankki-, asunto- ja kaupunkiasiain komitea piti 30.7.2019 kuulemistilaisuuden, jossa käsiteltiin kryptovaluuttoja ja lohkoketjuteknologiaa koskevaa lainsäädäntöä. Osana tuota kuulemistilaisuutta Senaatin pankkikomitean puheenjohtaja *Mike Crapo* lausui mahdollisesta Bitcoin kiellosta seuraavaa:

> ”Jos Yhdysvallat päättäisi - enkä sano, että sen pitäisi - jos Yhdysvallat päättäisi, ettemme halua kryptovaluuttoja käytettävän Yhdysvalloissa ja yrittäisimme kieltää niiden käytön, olen melko varma, että emme onnistuisi siinä, sillä tämä on globaali innovaatio.”[52]

---

[48] Ks. *Conti – Schmidt* Forbes 2021. Artikkelissa kerrotaan tarkemmin mikä on NFT.
[49] ”Token” suomentuu poletiksi. Non-fungible on termi, jolla viitataan kyseessä olevan poletin ainutlaatuisuuteen. Poletti ei ole suoraan korvattavissa toisella vastaavanlaisella poletilla, vaan siihen liittyy ominaisuuksia, jotka tekevät siitä uniikin. NFT-polettien ja normaalien polettien merkittävimpänä erona on juuri vaihdettavuus. Siinä missä esimerkiksi yhden Bitcoinin voi pilkkoa moniin pieniin osiin on NFT aina yksi kokonainen poletti.
[50] Ks. *Chipolina* Decrypt 2021.
[51] Ks. *Beedham* TNW 2019. Artikkeli kertoo Niken ”CryptoKicks” patentista lohkoketjupohjaiseen aitousvarmenteeseen, jolla pystytään todistamaan kenkien aitous ja alkuperä.
[52] Ks. Torpey Forbes 2019. Yhdysvaltain senaatin pankki-, asunto- ja kaupunkiasiain komitea pohti 30.7.2019 pidetyssä kuulemistilaisuudesta muun muassa Bitcoinin täyskiellon mahdollisuutta.

Hajautetut verkostot ovat mitä todennäköisimmin osa tulevaisuutta, halusivat hallitukset sitä tai eivät.

2.7.2. Lohkoketjun sisäänrakennettu ”luottamukseton luottamus”

Kryptovaluutoista puhuttaessa mainitaan usein se, että ne poistavat tarpeen perinteiselle luottamukselle, eli ne ovat luottamuksettomia[53]. Yksi lohkoketjun pääominaisuuksista on sen sisäänrakennettu luottamus. Voidaan myös puhua eräänlaisesta ”luottamuksettomasta luottamuksesta” eli luotetaan toisen osapuolen sijasta koodiin, joka toteuttaa transaktion. Tällä lohkoketjun sisäänrakennetulla luottamuksella pystytään korvaamaan perinteinen osapuolten välinen luottamus esimerkiksi erilaisissa laittomuuksiin liittyvissä transaktiotilanteissa, kuten käteisen rahan ja tavaroiden vaihdossa jossakin fyysisessä sijainnissa.

Tosiasiassa lohkoketju ei poista luottamusta täysin, vaan se minimoi vaadittavan luottamuksen hajauttamalla luottamuksen järjestelmän toiminnan mahdollistaville tahoille. Bitcoinin ja Ethereumin tapauksessa louhijoille[54], joilla on taloudellinen motiivi verkon ylläpitämiseen ja transaktioiden suorittamiseen niin sanotun Proof of Work -konsensusalgoritmin kautta.[55]

Transaktioiden tekeminen lohkoketjua hyödyntäen ei edellytä luottamusta perinteisiin välittäjätahoihin, kuten pankkeihin, vaan luottamus kohdistuu sen sijaan itse transaktioalustaan eli lohkoketjuteknologiaan. Vaihdannan osapuolet luottavat lohkoketjun huolehtivan kaikista niistä vaihdannan vaiheista, jotka tavallisesti ovat perinteisen kolmannen osapuolen, kuten pankin vastuulla. Lohkoketju mahdollistaa siirron, varmistaa lähettäjän autenttisuuden ja takaa vaihdetun valuutan aitouden. Tämä on mahdollista kryptografian (joka validoi lähettäjän autenttisuuden) ja konsensusmekanismin (joka takaa transaktioiden aitouden) avulla.[56]

Vaikka kryptovaluuttojen hyödyntämä luottamuksettoman luottamuksen malli välttää perinteiseen luottamukseen liittyvät ongelmat ei sekään ole täysin aukoton. Myös kryptovaluuttojen luottamukseton malli rakentuu itseasiassa monen luottamustekijän varaan. Käyttäjien ensinnäkin on luotettava siihen, että alustan kehittäjät ovat rakentaneet ohjelmistosta tietoturvallisen. Tämän lisäksi on luotettava siihen, etteivät kryptovaluutan louhijat hyökkää lohkoketjua

---

[53] Eng. ”trustless” eli viitataan perinteisen luottamuksen korvaamiseen lohkoketjun sisäänrakennetulla luottamuksella.
[54] Eng. “miners” tarkoittaa kryptovaluutan louhijoita.
[55] Ks. *Kasireddy* Medium 2018.
Ks. myös myöhempänä tässä tutkimuksessa oleva konsensusalgoritmeja käsittelevä luku 5.6.
[56] Ks. *Nakamoto* 2008.

vastaan. On myös luotettava siihen, ettei kryptovaluutan hallintoprosessi salli mahdollista haitallista jakautumisprosessia[57].[58]

Itse kryptovaluutan käyttöön liittyen käyttäjien on luotettava siihen, ettei kryptovaluuttojen markkinoita manipuloida. Lompakkojen, joissa kryptovaluuttaa säilytetään, on myös oltava turvallisia. Tämän lisäksi kryptovaluuttojen markkinapaikkojen tulee soveltaa parhaita mahdollisia turvallisuuskäytäntöjä, jotta ne välttyvät tietomurroilta ja varkauksilta.[59]

Kuten edellä esitetystä havaitaan, kryptovaluuttojen toiminnalle ja käytölle keskeiseen niin kutsuttuun ”luottamuksettomaan luottamukseen”, liittyy yllättävän paljon luottamustekijöitä, jotka ovat alttiita väärinkäytöksille. Merkittävimpänä erona perinteisemmillä markkinoilla esiintyviin luottamustekijöihin on, että suurinta osaa kryptovaluuttojen luottamuksesta ei ole kirjoitettu mihinkään laillisesti pätevässä sopimusmuodossa, johon voisi vedota tilanteessa, jossa yksi tai useampi edellä mainituista luottamuksen osatekijöistä murtuu.

2.7.3. Yksityisyys eli anonymiteetti

Anonymiteetillä on merkittävä asema kyberavaruudessa. Se mahdollistaa yksilöiden ja ryhmien liikkumisen kyberavaruudessa suhteellisen huomaamattomasti viranomaisilta. Netissä liikkuvat yksilöt saattavat helposti tuntea olevansa näkymättömissä muilta käyttäjiltä ja tuntevat, että heidän käyttäytymisensä netissä on perinteisten rajoittavien tekijöiden ulottumattomissa. Kyberavaruus sokaisee helposti käyttäjät omalta vastuultaan. Tämä itsetietoisuuden ja itsesäätelyn puute johtaa helposti epänormaaliin ja kiellettävänä pidettävään käyttäytymiseen. Tosin sanottuna yksi kyberavaruuden perusominaisuuksista ja kulmakivistä on jo perusluonteeltaan rikollisuutta helpottava tekijä. Anonymiteetin positiivisia vaikutuksia on mielekästä verrata siihen, miten se fasilitoi rikollisuutta.[60]

Internetin käytön helppous saattaa joillakin henkilöillä johtaa mielikuvaan, että internetissä kaikki on sallittua. Yksilö kadottaa netissä liikkuessaan helposti itsetietoisuutensa ja voi syyllistyä täysin vahingossa rikoksiin.[61] Sosiaalipsykologian deindividuaatio-teorian mukaan henkilö,

---

[57] Eng. ”malicious hardfork”, viittaa kryptovaluutalle haitalliseen jakautumiseen, jossa lohkoketju jakautuu ulkopuolisen hyökkäyksen, kuten 51 % hyökkäyksen vuoksi ja verkossa olleita kryptovaluuttoja saatetaan varastaa tai koko verkon toiminta estyy.
[58] Ks. *Bratspies* 2018, s. 19.
[59] Ibid. s.19–20.
[60] Ks. *Hinduja* 2008, s. 391–398.
[61] Ks. Nuortennetti 2021. Kirjoituksesta ilmenee hyvin, miten hämärtynyt käsitys yksilöillä saattaa toisinaan olla lain rajoista internetympäristössä.

joka on vapaa moraalisista ja sosiaalisista vastuistaan kadottaa helposti itsetietoisuutensa ja kykynsä itsesääntelyyn. Anonyymi yksilö unohtaa itsensä.[62] Sellaisilla yksilöillä, joilla on taipumuksia laittomuuksiin, on verkossa liikkuessaan entisestään alentunut kynnys toteuttaa näitä taipumuksiaan. Tällä ei tarkoiteta, että anonyymiys automaattisesti saisi kenessä tahansa yksilössä aikaan rikollista käyttäytymistä vaan sitä, että anonyymiys toimii kannustimena sellaisille henkilöille, joilla on jo taipumuksia poikkeavaan käyttäytymiseen, mutta jotka tarvitsevat rikollisten taipumustensa toteuttamiseen verkkoympäristön tarjoaman anonymiteetin sekä niin fyysisen kuin moraalisen erkaantumisen tekojensa seurauksista. Henkilö, joka ei missään olosuhteissa esimerkiksi varastaisi itse tuotteita suoraan kaupasta tai osallistuisi fyysisesti huumekauppaan, saattaa olla valmis maksamaan varastetun tavaran toimittamisesta verkon välityksellä tai tilaamaan huumausaineita postitse.

Monissa maissa on vallassa yksilön oikeuksia sortavia hallituksia. Esimerkiksi Kiinassa laaja sensuuri ja yksityishenkilön alentunut anonymiteetti ovat arkipäivää. Sensuuri tai kiellot eivät silti poista kiellon kohteena olevien tuotteiden kauppaa, vaan se siirtyy deep webiin eli niin sanottuun ”syväverkkoon”. Kyse on yksinkertaisesti verkosta, joka ei näy perinteisten hakukoneiden tuloksissa. Syväverkkoa käytetään laajalti myös länsimaissa, vaikka ihmisten sananvapaus ja yksityisyydensuoja ovat paremmalla tolalla. Käyttö vain kohdistuu mediasisältöjen levittämisen sijaan laittomaan kaupankäyntiin. Dark web puolestaan on deep webin osa, johon pääsyyn tarvitsee erillisen juuri dark webin käyttöön tarkoitetun hakukoneen. Dark webissä myydään esimerkiksi varastettuja salasanoja, huumausaineita, aseita ja lapsipornoa.[63]

Rikollisessa käytössä kryptovaluuttojen rooli on toimia anonyyminä vaihdannan välineenä edellä mainittujen laittomien kaupankäynnin kohteiden vaihdannassa. Kaupankäynnissä käytetään usein tunnetuinta kryptovaluuttaa eli Bitcoinia. Virtuaalivaluuttana Bitcoin on pseudo-anonyyminen. Tällä viitataan siihen, että bitcoineja säilytetään digitaalisessa lompakossa, joka ei ole täysin näkymätön vaan sillä on oma Bitcoin-osoite. Osoitteen transaktioita on mahdollista seurata, sillä ne näkyvät lohkoketjulla, jota kuka tahansa voi tarkastella. Ilman asianmukaisia salauskeinoja Bitcoin-osoite on edelleen yhdistettävissä käyttäjän IP-osoitteeseen, joten käytännössä poliisin on mahdollista jäljittää rikollisia Bitcoin-transaktioiden jättämien jälkien avulla. Rikolliset kuitenkin kiertävät seurantaongelman erityisten salaussovellusten, kuten Tor-verkon[64] ja kryptovaluuttasekoittimien avulla.

---

[62] Ks. Changing Minds: Deindividuaation määritelmä.
[63] Ks. *Lu* The Globe and Mail 2015.
[64] Ks. Tor FAQ.

2.7.4. Lompakot ja niiden tarjoajat

Kryptovaluuttojen ostamista ja hallinnoimista varten tarvitaan pari kryptografisesti salattuja avaimia (alfanumeerisia koodeja). Julkinen avain toimii osoitteena käyttäjän kryptovaluutoille ja se on lohkoketjun muiden käyttäjien nähtävissä. Julkista avainta voi verrata esimerkiksi pankkitilin tilinumeroon.[65] Jos joku haluaa lähettää kryptovaluuttoja toiselle henkilölle, hänen täytyy allekirjoittaa transaktio käyttäen omaa yksityisavaintaan.[66] Yksityisavain tulee säilyttää salassa eikä sitä tule antaa kenenkään muun käyttöön.[67] Lohkoketjukäyttäjät säilövät yksityisavaimensa niin sanotussa lompakossa. Lompakkoja on lukuisia erityyppisiä ja ne erotellaan toisistaan yksityisavaimen säilytyspaikan perusteella. Mikäli yksityisavain on kirjoitettu paperille, on kyseessä paperilompakko, kun taas yksityisavaimen säilyttämistä erityisellä tietoturvallisella fyysisellä laitteella kutsutaan hardware- tai kylmälompakoksi. Jos yksityisavain säilötään mobiilisovelluksessa tai verkkosivustolla kutsutaan näitä lompakoita mobiili- ja online-lompakoiksi. [68]

Lohkoketjukäyttäjillä on myös mahdollisuus käyttää niin sanottua lompakkopalveluntarjoajaa yksityisavaimien tallettamiseen. Näitä palveluita on kahdentyyppisiä. Joko palveluntarjoaja säilyttää käyttäjien yksityisavaimia tai se tarjoaa käyttäjille keinon säilyttää niitä itse erityisellä laitteella. Esimerkiksi jotkut kryptovaluuttapörssit säilyttävät käyttäjiensä yksityisavaimia transaktioiden helpottamiseksi. Tällöin käyttäjän tarvitsee ainoastaan tietää omat sisäänkirjautumistunnuksensa ja salasanansa eikä yksityisavainta tarvitse erikseen muistaa. Tämä helpottaa transaktioiden tekemistä, sillä yksityisavain on tyypillisesti epäkäytännöllisen pitkä ja monimutkainen. Kryptovaluuttapörsseistä voi ostaa erilaisia kryptovaluuttoja. Nämä palvelut muistuttavat perinteisiä fiat-valuutanvaihtopisteitä ja ne fasilitoivat fiat-valuutan vaihtoa kryptovaluutaksi.

[65] Ks. *Small* 2015, s. 588.
[66] Ks. *Nakamoto* 2008.
[67] Ks. *Small* 2015, s. 588.
[68] Ks. *Frankenfield* Investopedia 2021. Lisätietoja eri lompakkotyypeistä.

2.7.5. Initial Coin Offering (ICO)

Termi ICO viittaa useimmiten yrityksiin tai yksilöihin, jotka laskevat liikkeeseen poletteja joukkorahoittaakseen projektejaan. ICO osallistujat antavat liikkeeseen laskijalle esimerkiksi fiat-valuuttaa ja saavat vastineeksi liikkeeseen laskettavaa kryptovaluuttaa.[69] ICO on samankaltainen tapahtuma kuin IPO eli ”Initial Public Offering” (ensimmäinen julkinen liikkeeseenlasku) eli yrityksen ensimmäinen listautumisanti. Kummankin tarkoituksena on kerätä riskirahoitusta.

IPOn ja ICO:n välillä on kuitenkin joitakin merkittäviä eroavaisuuksia. Esimerkiksi onnistunut pörssilistautuminen edellyttää yleisesti ottaen yhtiöltä jonkinlaista aiempaa toimihistoriaa ja mainetta. Sitä vastoin ICO:n voi käynnistää missä vaiheessa tahansa. ICO:t ovat helposti toteutettavissa, lyhyessä ajassa ja pienin kustannuksin esimerkiksi liikkeeseen laskijan verkkosivujen kautta. ICO:ta edeltää usein projektin linjanvedon[70] julkaiseminen. Kyse on asiakirjasta, jossa kuvataan projektin toimintarakennetta.

ICO keräyksiin liittyy merkittävä sijoitusriski ja jotkut ICO:t ovat paljastuneet huijauksiksi. Rikoslain 17 luvun 16 c §:ssä säädetään rahankeräysrikoksista. Pykälän 2 momentin 3 kohdassa säädetään, että ”rahankeräysrikoksesta tuomitaan myös se, joka kerää rahaa tai virtuaalivaluuttaa rahankeräyslain 7 §:n 2 momentissa kielletyllä tavalla”. Kyseinen rahankeräyslain kohta on seuraavanlainen:

> ”Kiellettyä on lisäksi kerätä rahaa ja virtuaalivaluuttaa:
>
> 1) ketjukirjeen avulla siten, että toimintaan osallistuvalle luvataan taloudellinen etu sitä vastaan, että hän lähettää ketjukirjeen edelleen tai ketjukirjeeseen rinnastettavalla tavalla siten että sähköisessä tai muussa muodossa lähetetyssä viestissä kehotetaan lähettämään rahaa tai virtuaalivaluuttaa aiemmin toimintaan liittyneille; tai
>
> 2) pyramidipelin muodossa siten, että toimintaan liittyvän henkilön ansainta- tai voittomahdollisuudet osaksi tai kokonaan muodostuvat vastikkeetta niistä maksuista, joita toimintaan myöhemmin mukaan liittyvät maksavat osallistumismaksuina tai muina kerta- tai toistuvaissuorituksina.”

Kryptovaluutta-alan tunnetuin Ponzi-huijaus oli Bitconnect, joka kavalsi noin 2 miljardia dollaria sijoittajien rahoja. Huijaus perustui pyramidirakenteeseen, jossa toimintaan myöhemmin mukaan liittyneet maksoivat aiemmin mukana olleiden voitot. Kolmen vuoden tutkinnan jälkeen tapauksesta on syytettynä viisi henkilöä.[71]

---

[69] Ks. *Heiskanen* Finanssivalvonta 2017.
[70] Eng. white paper.
[71] Ks. *Robinson* Bloomberg 2021.

2.7.6. Kryptovaluutta-sekoittimet

Kryptovaluuttasekoittimet ovat yritysten tarjoamia palveluita, joiden tarkoituksena on auttaa lohkoketjunkäyttäjiä kätkemään polettiensa[72] alkuperä. Yleensä[73] jokaisella poletilla on oma uniikki tunnistekoodinsa. Lohkoketju tallentaa transaktiodatan jokaisesta poletista tämän tunnistekoodin avulla. Tästä seuraa, että useimmissa tapauksissa polettien transaktiohistoria on julkisesti nähtävissä. Mikäli polettia on käytetty osana laittomia toimia sen käyttäminen ja siitä muodostuva transaktiohistoria saattaa olla viranomaisille riittävä johtolanka rikollisten löytämiseksi.

Tämä jäljittämisen mahdollisuus korostaa laittomuuksia tekevien lohkoketjukäyttäjien tarvetta tehdä transaktioistaan mahdollisimman anonyymejä. Transaktiot, jotka halutaan tehdä mahdottomaksi jäljittää, saadaan häivytettyä lähettämällä poletit sekoitinpalveluun. Sekoitin simuloi suuren määrän transaktioita lähettämällä käyttäjän poletit useasti osoitteesta toiseen. Kaikki käytetyt osoitteet ovat sekoitinpalvelun hallinnoimia. Tämä yksityiskohta ei näy itse lohkoketjulla mitenkään, sillä osoitteiden hallinnointisuhteita ei voi varmistaa. Koska useat eri ihmiset käyttävät sekoitinpalveluita, palvelu sekoittaa eri käyttäjien poletit keskenään. Tämän prosessin jälkeen palvelu lähettää sekoitetut poletit takaisin käyttäjälle (yleensä toiseen osoitteeseen, kuin mistä poletit alun perin lähetettiin sekoitinpalveluun) ja perii toimenpiteestä maksun. Lohkoketjulla sekoitettujen polettien alkuperää on hyvin vaikea selvittää.[74] Näin ollen viranomaisten on miltei mahdotonta käyttää sekoitettujen polettien transaktiodataa rikollisten jäljittämiseen.

On olemassa myös toisenlaisia kryptovaluuttasekoittimia, jotka eivät lähetä sekoitettuja poletteja takaisin samalle käyttäjälle, joka lähetti ne sekoittimeen. Sen sijaan ne lähetetään käyttäjän pyynnöstä sekoituspalvelun jälkeen kolmannelle osapuolelle. Jotkut laittomat transaktiot hoidetaan suoraan sekoitinpalvelun kautta, jolloin tämän tyyppistä sekoitinpalvelua käytetään välittäjätahona osapuolten välillä.

[72] Käsite ”poletti” viittaa tässä johonkin tietyn henkilön omistamaan määrään kryptovaluuttaa. Henkilö voi esimerkiksi omistaa X määrän Monero-poletteja.
[73] Ei aina, sillä eri lohkoketjujen välillä on eroja.
[74] Ks. *Goldfeder ym*. 2018 s. 179–199. Eräissä harvinaisissa tapauksissa myös sekoitetut poletit voi jäljittää.

3. KRYPTOVALUUTAT KANSAINVÄLISESSÄ AML/CFT-JÄRJESTELMÄSSÄ JA EU:N LAINSÄÄDÄNNÖSSÄ

3.1. Aluksi

Kryptovaluuttojen käyttö ylittää kansalliset rajat ja niitä pystytään tehokkaasti hyödyntämään rahanpesussa. Ajan kuluessa tämä rikollinen käyttö todennäköisesti yleistyy. Mitä vakiintuneemmaksi kryptovaluuttojen rikollinen käyttö muodostuu, sitä hankalampaa yksittäisen valtion on sitä torjua. Kansainvälinen yhteistyö ja mahdollisimman yhdenmukainen linja suhtautumisessa kryptovaluuttojen käyttöön on tärkeää siksi, ettei yksittäisistä sallivammista lainkäyttöalueista muodostuisi rahanpesun turvasatamia.

Kansainväliset sopimukset ja eri järjestöjen suositukset ovat viitoittaneet kehityskulkua kohti kryptovaluuttojen sisällyttämistä EU:n viidenteen rahanpesudirektiiviin. Rahanpesun ja terrorismin rahoittamisen estäminen on keskeistä EU:n taistelussa talousrikollisuutta vastaan. EU on näin päättänyt sisällyttää myös kryptovaluutat säänneltäväksi AML/CFT-järjestelmän kautta. Rahanpesu ja terrorismin rahoittaminen kuuluvat huumausainerikosten ohella rikostyyppeihin, joilla on selkeä yhteys kryptovaluuttoihin. Kryptovaluuttojen digitaalisuus, helppo siirrettävyys, rajat ylittävä luonne ja pseudo-anonyymisyys takaavat, että ne kiinnostavat myös rikollisia.[75]

3.2. Rahaa, hyödykkeitä vai jotain muuta – mihin sääntelyintressi perustuu?

Eri puolilla maailmaa kryptovaluutat on kategorisoitu vaihtelevasti eri omaisuusluokkiin. Esimerkiksi suhtautuminen Bitcoinia kohtaan on vaihdellut voimakkaasti eri valtioiden välillä, ja moni valtio on ajan kuluessa myös muuttanut suhtautumistaan. Suomen Pankki antoi vuonna 2014 lausunnon, jossa se varoitti Bitcoinin olevan vain riskialtis sijoitus. Se totesi myös, ettei Bitcoin täytä mitään maksuvälineeltä edellytettäviä kriteerejä, sillä siltä esimerkiksi puuttuu vastuussa oleva liikkeellelaskija. Huolenaiheena oli myös Bitcoinin sääntelemättömyys.[76] Myöhemmin vuonna 2017 Suomen Pankin julkaisemassa tutkimusraportissa Bitcoinia kuvailtiin ”vallankumoukselliseksi”, sen ”funktionaalisuuden ja hyödyllisyyden tulisi rohkaista ekonomeja tutkimaan sitä enemmän” ja ”Bitcoinia ei ole säännelty eikä sitä voi säännellä”.[77] Saman raportin

[75] Ks. *Houben – Snyers* 2018, s. 100.
[76] Ks. Suomen Pankki: Bitcoin involves risks 2014.
[77] *Huberman – Leshno – Moallemi* 2017, s. 36.

vuoden 2021 versiossa myönnettiin käänteisesti lohkoketjuteknologian toimivuus: ”Lohkoketjuprotokolla olisi ansainnut taloustieteilijöiden huomiota vaikka se ei olisi toiminut.”[78]

Ruotsissa Bitcoinia pidetään sijoitusomaisuutena ja Ruotsin hallitus voi määrätä Bitcoinin myyntivoitoista veron. Vuonna 2018 Ruotsin keskuspankki antoi lausunnon, jonka mukaan Bitcoin ei ole rahaa,[79] viitaten pankin laatimaan kryptovaluuttoja käsittelevään tutkimusraporttiin.[80] Suomessa verottajan omaksuma linja kryptovaluuttojen ja niillä tehtävien kauppojen verotuksen suhteen on herättänyt keskustelua. Kryptovaluuttojen kaupoissa syntyneitä voittoja verotetaan, mutta kaupankäynnin tappioita ei voida verotuksessa vähentää. [81]

Helsingin hallinto-oikeus linjasi kuitenkin, että kryptovaluuttoja kaupatessa syntyneet tappiot voidaan vähentää luovutusvoittoa koskevilla säännöillä. Oikeus esitti perusteluiksi, että vaikka virtuaalivaluutalla ei ole lainsäädäntöön perustuvaa virallista asemaa, on sitä kuitenkin pidettävä omaisuutena, jolla on erilaisten aineettomien oikeuksien tavoin lähtökohtaisesti varallisuusarvoa ja jonka omistusoikeus on mahdollista luovuttaa. Kun virtuaalivaluuttojen kohdalla ei verolainsäädännössä ollut olemassa erityisiä säännöksiä, hallinto-oikeus katsoi, ettei kuvatuista virtuaalivaluuttojen vaihdoista saatuun voittoon ollut perusteita olla soveltamatta omaisuuden luovutusvoittoa koskevia säännöksiä.[82] Oikeustila on vaihteleva ja muutoksia tapahtuu jatkuvasti.

Vaikka eri valtioiden omaksumissa määrittelyissä on eroja, on selvää, että valtioilla on huomattava intressi luoda uusia tulovirtoja kryptovaluuttojen verotuksella. Kryptovaluuttojen arvon eksponentiaalinen arvonnousu huomioon ottaen tämä suhtautuminen on ymmärrettävää.

Kryptovaluuttojen laittoman käytön vuoksi ne on huomioitava myös AML/CFT-järjestelmän kannalta. Kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen 2 artiklassa on seuraavat omaisuuden ja rikoksen tuottaman hyödyn määritelmät:

> (d) "Omaisuus" tarkoittaa kaikenlaista aineellista tai aineetonta ja irtainta tai kiinteää varallisuutta, sekä oikeudellisia asiakirjoja, jotka osoittavat omistusoikeuden tai osuuden sellaiseen omaisuuteen;
>
> (e) "Rikoksen tuottama hyöty" tarkoittaa rikoksen avulla suoraan tai välillisesti saatua omaisuutta;

[78] *Huberman – Leshno – Moallemi* 2021, s. 36–37.
[79] Ks. Ruotsin keskuspankin julkaisu: Bitcoin är inte pengar 2018.
[80] Ks. *Söderberg* Sveriges Riksbank 2018.
[81] Ks. *Johansson ym.* 2019, s. 207–208.
[82] Ks. Helsingin HAO 6.7.2018 18/0426/3.

Kansainvälisen terrorismin rahoituksen torjumisesta tehdyn yleissopimuksen (CFT-sopimus)[83] 1 artiklassa on seuraavat varojen ja tuoton määritelmät:

> 1. "Varat" tarkoittavat kaikenlaista aineellista tai aineetonta, irtainta tai kiinteää omaisuutta sen hankintatavasta riippumatta, sekä kaikenlaisia oikeudellisia asiakirjoja, mukaan luettuna sähköiset tai digitaaliset asiakirjat, jotka todistavat tällaiseen varallisuuteen liittyvän omistusoikeuden tai edun, mukaan luettuna, ei kuitenkaan yksinomaan pankkiluotot, matkashekit, pankkishekit, maksumääräykset, osakkeet, takuut, velkakirjat, asetteet ja remburssit.
>
> 3. "Tuotto" tarkoittaa varoja, jotka on saatu suoraan tai välillisesti 2 artiklassa mainitun rikoksen teon kautta.

Kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen määritelmä omaisuudelle on kaikenkattava. Olennaista on, että kryptovaluutat ovat asia, jolla on arvoa. AML/CFT-järjestelmä koskee laittomia transaktioita riippumatta niiden teoreettisesta määrittelystä. Edellä esitettyyn peilaten voidaan todeta, että kryptovaluutat ovat rahoitusvaroja, koska niillä on taloudellista arvoa omistajilleen. Näin kategorisoituna kryptovaluutat voidaan lukea AML/CFT-järjestelmän piiriin.

3.3. Vastatoimien kansainvälinen sopimustausta

Todettakoon aluksi, että lähemmän tarkastelun aloittaminen kansainvälisistä sopimuksista käsin on pragmaattista tutkielmassa käsiteltävän ilmiön rajat ylittävän luonteen vuoksi. Kansainvälisiin sopimisinstrumentteihin keskittyminen on linjassa sen toteamuksen kanssa, etteivät tässä tutkielmassa käsiteltävät ongelmat ole eksklusiivisesti minkään tietyn yksittäisen valtion toimivallan alaisuudessa. Kansainvälinen yhteisö on vuosien aikana ryhtynyt lukuisiin vastatoimiin rahanpesun ja siihen liitännäisten rikosten estämiseksi. Vaikka toimien tarkka luonne vaihtelee sen mukaan mikä taho ne on toteuttanut, on kansainvälisissä toimissa tietty läpileikkaava yhdistävä tekijä. Nimittäin sen tosiseikan tunnistaminen, että teknologisen kehityksen myötä uusien rajat ylittävien rikosmuotojen esiintulo on vääjäämätöntä.

Kansainvälisissä AML/CFT-strategioissa on pyritty heikentämään rikollisjärjestöjen ja terroristien toimintakykyä rajoittamalla näiden järjestöjen taloudellisia resursseja. Tämän pyrkimyksen toteuttamiseksi on ollut elintärkeää puuttua niihin mahdollisuuksiin, joita rikolliset hyödyntävät tuottojensa pesemiseen.[84]

---

[83] SopS 74/2002.
[84] Ks. *Boon – Huq – Lovelace* 2010, s. 379.

Kansainvälisellä tasolla vastatoimien tehostumisen alkusykäyksenä toimi Yhdistyneiden Kansakuntien huumausaineiden ja psykotrooppisten aineiden laittoman kaupan vastainen yleissopimus, (Wienin yleissopimus)[85] joka oli ensimmäinen rahanpesun määritelmän sisältänyt kansainvälinen sopimus. Termiä ”rahanpesu” ei Wienin yleissopimuksessa käytetä, mutta sopimus antaa selkeän velvoitteen sopimusvaltioille kriminalisoida rahanpesuksi luokiteltavat tahalliset tekomuodot.[86] Koska Wienin sopimus koskee nimenomaan huumausaineiden ja psykotrooppisten aineiden laitonta kauppaa, on esirikosten ala rajattu tässä sopimuksessa vain huumausainerikoksiin.[87]

Myöhemmissä sopimuksissa esirikosten (ja myös jälkitekojen) luetteloa on laajennettu kattamaan esimerkiksi ihmiskaupan, siirtolaissalakuljetuksen ja terrorismin rahoittamisen. Vuonna 2000 laadittu YK:n Kansainvälisen järjestäytyneen rikollisuuden vastainen yleissopimus (Palermon yleissopimus)[88] on toinen YK:n piirissä laadittu rahanpesukriminalisointien kannalta merkityksellinen sopimus ja sen 6 artiklaan on otettu pitkälti Wienin sopimuksen määritelmää muistuttava rahanpesun määritelmä.[89] Sopimuksen 6 artiklan otsikointitapa ”Rikoksen tuottaman hyödyn pesemisen säätäminen rangaistavaksi teoksi” tarkoittaa, että rahanpesu tunnistetaan omaksi rikostyypikseen, mikä rikkoo Wienin yleissopimuksessa olevan ajatuksen rahanpesusta huumausainerikollisuuteen liittyvänä oheisrikollisuutena, jolla ei olisi huumausainerikollisuudesta riippumatonta itsenäistä arvoa.[90]

Palermon sopimuksen 6 (2) (b) artiklassa velvoitetaan sopimusvaltioita pitämään esirikoksina kaikkia yleissopimuksen 2 artiklan määritelmän mukaisia vakavia rikoksia. Terrorismin rahoittamista olisi luontevinta pitää rahanpesun jälkitekona, sillä tämä kategorisointi kuvaa paremmin näiden kahden rikostyypin välistä yhteyttä. Näiden rikostyyppien kontekstissa rahanpesu tapahtuu yleensä ennen ”vakavampaa” terrorismin rahoittamista. Näin ollen teon tarkoituksena ei niinkään ole pestyjen varojen hankkiminen, vaan rahanpesu on yksi väline terroristisen toiminnan fasilitointiin. Terrorismin rahoitukseen käytettyjen varojen ei ole pakko olla peräisin laittomasta toiminnasta. Rikostyyppien välinen yhteys näkyy myös siinä, että useat rahanpesun torjumiseen omaksutut mekanismit soveltuvat luontevasti myös terrorismin rahoituksen torjuntaan. Esimerkiksi tässä tutkielmassa puhutaan AML-järjestelmän sijaan AML/CFT-järjestelmästä.

---

[85] SopS 44/1994.
[86] Ks. *Hyttinen* 2021, s. 35.
[87] Ks. *Kimpimäki* 2015, s. 338.
[88] SopS 20/2004.
[89] Ks. *Kimpimäki* 2015, s. 338–339.
[90] Ks. *Hyttinen* 2021, s. 37.

Palermon sopimuksen 7 artikla sisältää määräyksiä rahanpesun vastustamiseksi omaksuttavista toimista. Toimenpiteet liittyvät muun muassa pankkien ja muiden rahoituslaitosten sääntelyyn ja valvontaan, viranomaisten yhteistyöhön ja tiedonvaihtoon kansallisella ja kansainvälisellä tasolla sekä rahan ja arvopaperien liikkeiden seurantaan. Näiden nimenomaan rahanpesun vastustamiseen liittyvien määräysten lisäksi rahanpesun yhteydessä tulevat sovellettavaksi myös sopimuksen yleiset lainkäyttövaltaa, rikoksentekijän luovuttamista, omaisuuden menetetyksi tuomitsemista, valtioiden keskinäistä oikeusapua ja lainvalvontaviranomaisten välistä yhteistyötä koskevat määräykset.[91]

Vaikka toimenpiteet rahanpesun estämiseksi perustuvat pitkälti kansainvälisiin sopimuksiin, kuten edellä mainittuihin Wienin ja Palermon yleissopimuksiin, kuuluu rahanpesun estämiseen myös muita toimenpiteitä. Näitä ovat muun muassa eri tahojen ja järjestöjen laatimat ohjeistukset, suositukset ja parhaat käytännöt, jotka kaikki toimivat yhdessä kansainvälisen AML/CFT-järjestelmän taustalla.

3.4. Financial Action Task Force ja riskiperusteinen arviointi

Vuonna 1989 perustettu Financial Action Task Force on Money Laundering (FATF) on kansainvälinen hallitustenvälinen yhteistyöelin, jonka tehtävänä on kehittää ja koordinoida rahanpesuun liittyvää kansainvälistä yhteistyötä. FATF kehittää ja ottaa käyttöön rahoitusjärjestelmän rikollista hyväksikäyttöä ehkäiseviä standardeja ja mekanismeja sekä arvioi kansallisella ja kansainvälisellä tasolla käytössä olevia rahanpesun vastustamistoimia.[92]

Kansainvälinen yhteisö on FATF:n perustamisesta lähtien pyrkinyt ylläpitämään vankkoja ja koordinoituja puitteita laittoman rahoitusjärjestelmän hyväksikäytön estämiseksi. FATF ja EU ovat yhdessä sitoutuneet arvioimaan ja seuraamaan kryptovaluuttoihin liittyviä riskejä, kuten niiden käyttöä terrorismin rahoitukseen, sekä varmistamaan, että jäsenmaat ovat implementoineet asianmukaiset preventiiviset toimenpiteet. Esimerkiksi EU:n viidennessä rahanpesudirektiivissä on keskitytty sääntelemään kolmansia osapuolia, tässä tapauksessa virtuaalivaluutantarjoajia, kuten kryptovaluuttapörssejä. Monilla lainkäyttöalueilla ei ole kuitenkaan vielä riittävästi selvennetty sääntelykantaa virtuaalivaluuttojen suhteen, mikä on johtanut epäyhtenäiseen

[91] *Kimpimäki* 2015, s. 339.
[92] Ks. *Kimpimäki* 2015, s. 339.
Ks. myös FATF:n verkkosivut fatf-gafi.org.

kansainväliseen sääntelykehykseen, jättäen tarpeen johdonmukaisemmille ja koordinoidummille kansainvälisille sääntelytoimille.[93]

Syyskuun 11. päivän terrori-iskut nostivat terrorismin rahoitukseen puuttumisen kansainvälisen turvallisuuden prioriteetiksi ja johtivat FATF:n uusiin toimenpiteisiin ja järjestelyihin. FATF lisäsi alkuperäisten 40 suosituksen joukkoon 9 uutta terrorismin rahoituksen vastaista suositusta.[94] Näihin suosituksiin kuuluivat muun muassa terrorismin rahoituksen kriminalisointi ja terroristien omaisuuden takavarikointi.

Yhdeksässä erityissuosituksessa täsmennettiin, että maiden tulisi säännellä vaihtoehtoisia rahanlähetysjärjestelmiä, kuten hawala-verkkoja ja muita epävirallisia arvonsiirtomekanismeja, joita perinteisen säännellyn rahoitusjärjestelmän ulkopuolella on. Tällä täsmennyksellä on ollut merkitystä myös FATF:n myöhemmässä suhtautumisessa digitaalisiin ekosysteemeihin, kuten virtuaalivaluuttoihin.

FATF julkaisi ensimmäisen nimenomaan virtuaalivaluuttoja käsittelevän raporttinsa vuonna 2014.[95] FATF kuvailee raportissa virtuaalivaluuttojen ”olevan globaalin luonteensa vuoksi täysin minkään yksittäisen valtion määräysvallan ulottumattomissa”.[96] FATF kiinnitti raportissaan huomiota muun muassa anonyymiyteen liittyviin ongelmiin ja keskitetyn valvojatahon puuttumiseen.[97] FATF kehitti nopeasti uudenlaisen kryptovaluuttoja koskevan riskiperusteisen arviointimallin, jonka se julkaisi vuonna 2015.[98] FATF on myös pyrkinyt tarkemmin ennakoimaan kryptovaluuttojen roolia terrorismin rahoittamisessa ja se julkaisi samana vuonna uusia terroristisen toiminnan rahoituksen riskejä koskevan raportin.[99]

Riskiperusteinen arviointimalli auttaa valtioita arvioimaan oikeasuhtaisesti kryptovaluuttoihin liittyviä riskejä ja soveltamaan FATF:n suosituksia paremmin kryptovaluuttoihin. FATF arvioi suurimman osan riskeistä kohdistuvan niihin järjestelmän kohtiin, joissa kryptovaluutat ovat vaihdettavissa muihin valuuttoihin. Näin ollen riskiperusteisen arvion näkökulmasta valtioiden olisi tehokkainta kohdistaa rahanpesun- ja terrorismin rahoituksen vastaiset toimensa näihin vaihtopisteisiin. Perusteluna tälle arviolle oli, että rikollisilla on tarve tehdä vaihtoja kryptovaluuttojen ja fiat-valuuttojen välillä, joten näiden vaihtopisteiden olisi syytä olla koko kryptovaluutta-ekosysteemin läpinäkyvin ja valvotuin kohta. Riskiperusteinen arviointimalli viitoitti tien

[93] Ks. *Carlisle – Keatinge – Keen* 2018.
[94] Ks. FATF: IX Special Recommendations on Terrorist Financing 2001.
[95] Ks. FATF: Virtual Currencies: Key Definitions and Potential AML/CFT Risks 2014.
[96] Ibid. s.10.
[97] Ibid. s. 9.
[98] Ks. FATF: Guidance for a Risk-Based Approach: Virtual Currencies.
[99] Ks. FATF: Financing of Recruitment for Terrorist Purposes 2018, s. 20.

myös EU:n myöhemmälle keskitettyjen toimijoiden valvontaan perustuvalle preventiiviselle sääntelylle ja kryptovaluutat sisällytettiin osaksi EU:n viidettä rahanpesudirektiiviä.

3.5. Suurimmat haasteet taistelussa kryptovaluuttojen välityksellä tapahtuvaa rahanpesua ja terrorismin rahoittamista vastaan

Kryptovaluutoilla saavutettava anonymiteetti muodostaa yhden suurimmista haasteista niiden sääntelylle. Anonymiteetin aste vaihtelee pseudo-anonyymisyydestä täyteen anonymiteettiin. Anonymiteetti estää kryptovaluuttatransaktioiden riittävän valvonnan ja mahdollistaa rikollisten transaktioiden tekemisen lainsäädäntökehyksen ulottumattomissa. Rikollisjärjestöille on auennut anonymiteetin myötä uusi väylä ”puhtaaseen rahaan” (kun varoja on mahdollista helposti siirtää kryptovaluutoista käteiseksi ja toisin päin).

Anonymiteetin kohdalla kysymys on kaksijakoinen. Toisaalta lainsäädännössä päämääränä on löytää ratkaisu, joka lieventää haitallisen anonymiteetin vaikutuksia, mahdollistaa lainvalvontaviranomaisille tehokkaammat keinot puuttua rikolliseen toimintaan ja madaltaa siten korkeita esitutkintakustannuksia. Silti nämä tavoitteet on tasapainotettava kyberturvallisuusnäkökohtien kanssa siten, ettei yksittäisten käyttäjien tietoturva vaarannu.

Anonymiteetin lisäksi kryptovaluuttojen rajat ylittävä luonne muodostaa toisen merkittävän haasteen lainsäätäjille.[100] Kryptovaluuttapörssi tai muu palveluntarjoaja voi esimerkiksi sijaita sellaisella lainkäyttöalueella, jossa ei ole tehokkaita sääntelymekanismeja rahanpesun ja terrorismin rahoittamisen estämiseksi.[101] Kryptovaluuttojen sääntely voi olla tehokasta ainoastaan, kun se toteutuu tarpeeksi laajasti kansainvälisellä tasolla.

Kolmas haaste liittyy siihen, että kryptovaluuttojen ekosysteemissä ei ole aina olemassa mitään keskitettyä toimijaa johon sääntely kohdistuisi. Esimerkiksi suuri osa kryptovaluuttojen keskinäisestä vaihdannasta tapahtuu hajautetuissa[102] pörsseissä. Tästä voidaan johtaa kysymys siitä, mihin toimijaan lainsäädäntö tulisi kohdistaa niissä tilanteissa, joissa keskitettyä välittäjätahoa ei ole olemassa.[103]

Yksi lohkoketjuteknologian perustavanlaatuisimmista ominaisuuksista on, että se sulkee vaihdannasta ulos perinteiset välittäjätahot. Tulevan sääntelyn kannalta voisi kuitenkin olla toimiva

[100] Ks. *Almeida ym*. IMF Staff Discussions Note 2016, s. 25 ja 27.
[101] Ks. EKP: Virtual currency schemes – a further analysis 2015.
[102] Eng. decentralized exchange, DEX.
[103] Ks. *Almeida ym*. IMF Staff Discussions Note 2016, s. 25.

ratkaisu luoda lohkoketjujärjestelmiin jokin objektiivinen välikäsi, joka mahdollistaisi sääntelyn kohdistamisen tunnistettaviin henkilöihin, mikä mahdollistaisi tehokkaamman valvonnan. Tällainen ratkaisu olisi toki selvässä ristiriidassa lohkoketjun perimmäisen tarkoituksen kanssa. Oikean tasapainon löytäminen tehokkaan sääntelyn ja taloudellisen innovaation välillä on kuitenkin merkittävä vaikutin lohkoketjuteknologian laajempaan omaksumiseen ja sopivan sääntelybalanssin löytäminen on teknologialle hyödyksi.[104]

3.6. EU:n AML/CFT-järjestelmä

3.6.1. Jäsenmaiden suhtautuminen kryptovaluuttoihin ennen EU:n viidettä rahanpesudirektiiviä

EU:n sääntely oli rahanpesun kohdalla pitkään melko seremoniallista. Jäsenvaltiot ovat olleet jo sitoutuneita kansainvälisiin sopimuksiin, kuten Wienin yleissopimukseen ja säätäneet rahanpesun rangaistavaksi kansallisissa rikoslaeissaan.[105] Tietyt jäsenvaltiot toteuttivat jo ennen EU:n viidettä rahanpesudirektiiviä toimenpiteitä selkiyttääkseen kryptovaluutta-alan toimijoiden AML/CFT-velvoitteita. Näin ollen joidenkin jäsenmaiden lainvalvontaviranomaiset ja oikeuslaitokset ovat jo varhain soveltaneet rahanpesun ja terrorismin vastaisia sääntöjä kryptovaluuttoihin. Monet EU:n jäsenmaat, kuten esimerkiksi Saksa, ovat laatineet proaktiivisesti kansallista lainsäädäntöä ja ovat yhä lisääntyvän harmonisoinnin sekä direktiivien aikakaudella alan edelläkävijöitä ja pioneereja. Esimerkiksi Italia oli jo sisällyttänyt kansalliseen lainsäädäntöönsä viittauksen kryptovaluuttoihin.[106] Malta puolestaan laajensi rahanpesun ja terrorismin rahoittamisen vastaisten sääntelyn soveltamisalaa osana laajempaa monialaista lainsäädäntöhanketta, jolla pyrittiin luomaan kryptovaluuttataloutta tukeva lainsäädäntökehys.[107]

Osa jäsenmaista oli omaksunut jo ennen EU-direktiiviä tapauskohtaisen lähestymistavan, jossa kryptovaluuttayrityksen toiminta edellyttää asianmukaista lisenssiä. Lisenssin saaminen puolestaan edellyttää asiakkaan tuntemisen menetelmiä, raportointia ja yhteistyötä valvovien viranomaisten kanssa. Hyvä esimerkki tällaisesta lähestymistavasta on Luxemburg, jonka

[104] Mahdollisuutta lohkoketjun konsensustasolla tapahtuvaan sääntelyyn tutkitaan myöhemmin luvussa 5.6.
[105] Ks. *Hyttinen* 2021, s. 54.
[106] Ks. Decreto Legislativo 2017. Italia laati kryptovaluuttoja koskevaa AML/CFT-lainsäädäntöä jo ennen EU-direktiiviä.
[107] Ks. Malta: Virtual Financial Assets Act.

rahoituksenvalvontaviranomaisesta tuli vuonna 2014 ensimmäinen viranomaistaho EU-alueella, joka oli myöntänyt kryptovaluuttapörssille maksupalveluntarjoajan aseman.[108]

EU:n neljännen rahanpesudirektiivin aikana oikeustila oli sellainen, etteivät kryptovaluuttapörssit, lompakontarjoajat, sekoitinpalveluntarjoajat ja muut alan toimijat kuuluneet direktiivin piiriin. Näillä tahoilla ei näin ollen ollut varsinaisia EU:n lainsäädäntöön perustuvia AML/CFT-velvoitteita eikä niiden tarvinnut esimerkiksi tunnistaa asiakkaitaan asiakkaan tuntemisen menetelmien kautta, eikä myöskään ilmoittaa epäilyttävistä transaktioista. Käytännössä jotkut palveluntarjoajat kuitenkin pyrkivät korostamaan toimintansa legitiimiyttä toimimalla oikeustilan epäselvyydestä huolimatta läpinäkyvästi.

Pseudo-anonyymisten kryptovaluuttatransaktioiden seuranta oli jo itsessään niin haastavaa, ettei ollut realistista olla puuttumatta oikeustilaan. Mikäli kryptovaluuttapalveluntarjoajat eivät olisi yhteistyöhaluisia olisi tämä aiheuttanut mittavan turvallisuusriskin. EU:n viidennellä rahanpesudirektiivillä lainsäätäjät halusivat varmistaa, että jäsenvaltioiden toimivaltaiset viranomaiset voivat suorittaa asianmukaista valvontaa.

3.6.2. Viides rahanpesudirektiivi

Kryptovaluuttojen pseudo-anonyyminen ja hajautettu rakenne tekee niistä erityisen houkuttelevan välineen rikollisille, jotka käyttävät niitä muun muassa rahanpesuun ja terrorismin rahoittamiseen. Lisääntynyt käyttö rahanpesussa johti EU:n lainsäätäjien tarpeeseen tuoda kryptovaluutat ja niihin liittyvät palvelut osaksi AML/CFT-järjestelmää. Euroopan unionissa tämä toteutettiin säätämällä Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/843 rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen annetun direktiivin (EU) 2015/849 ja direktiivien 2009/138/EY ja 2013/36/EU muuttamisesta. Direktiivi tunnetaan myös EU:n viidentenä rahanpesudirektiivinä.[109]

EU:n viides rahanpesudirektiivi (jatkossa myös AMLD5) toimii neljättä rahanpesudirektiiviä täydentävänä lisädirektiivinä. Sen tuoma tärkein uusi sisältö on virtuaalivaluuttoja koskeva sääntelyvelvoite.[110] Direktiivi on tärkein oikeudellinen väline rahanpesun ja terrorismin rahoituksen

[108] Ks. Luxemburgin rahoituksenvalvontaviranomaisen julkaisut:
CSSF: Avertissement sur les monnaies virtuelles.
CSSF: Avertissement sur es Initial Coin Offerings (ICOs).
[109] Ks. Euroopan komissio: Timmermansin, Dombrovskin ja Jourovàn lausuma viidennen rahanpesunvastaisen direktiivin hyväksymisestä Euroopan parlamentissa 2018.
[110] Ks. *Hyttinen* 2021, s. 51–52.

estämiseksi EU:n finanssijärjestelmässä. Direktiivi asettaa kattavan oikeudellisen kehyksen rahan keräämisen estämiseksi terroristisiin tarkoituksiin, edellyttämällä kaikkia EU:n jäsenvaltioita tunnistamaan, ymmärtämään ja vähentämään rahanpesuun ja terrorismin rahoitukseen liittyviä riskejä.

Direktiivin johdanto-osan kappaleessa 8 todetaan valvontaan liittyen, että:

> ” […] Toimivaltaisten viranomaisten olisi rahanpesun ja terrorismin rahoituksen torjuntaa varten voitava valvoa virtuaalivaluuttojen käyttöä ilmoitusvelvollisten kautta. Tällaisella valvonnalla saataisiin aikaan tasapuolinen ja oikeasuhteinen lähestymistapa, joka turvaisi vaihtoehtoisen rahoituksen ja yhteiskunnallisen yrittäjyyden alalla saavutetun teknisen kehityksen ja pitkälle viedyn avoimuuden.”

Johdanto-osan kappaleessa 9 perustellaan valvontaa anonyymiyteen liittyvillä riskeillä:

> ” […] Anonyymiyteen liittyvien riskien torjumiseksi kansallisten rahanpesun selvittelykeskusten olisi voitava hankkia tietoja, joiden avulla ne voivat yhdistää virtuaalivaluuttojen verkko-osoitteet virtuaalivaluutan omistajan henkilöllisyyteen.”

Direktiivissä on pyritty huomioimaan kryptovaluuttojen yleistyvään käyttöön liittyvät riskit ja myös mahdollisuudet. Komissio keskittyi direktiivialoitetta laatiessaan virtuaalivaluuttojen pitkän aikavälin hyötynäkökohtiin ja taloudellisiin vaikutuksiin. Euroopan unionin jäsenmaiden olisi komission mukaan hyvä omaksua lohkoketjuteknologia, koska se auttaa talousaluetta pysymään kilpailukykyisenä. Komissio kuitenkin tunnisti myös kryptovaluuttojen laittomaan käyttöön liittyvät rahanpesutoimintaa ja terrorismia koskevat riskit. Näin ollen se päätyi ehdottamaan, että kryptovaluuttapörssejä ja lompakontarjoajapalveluita säänneltäisiin viidennen rahanpesudirektiivin nojalla. Direktiivin ohella sovelletaan myös muita terrorismin vastaisia toimenpiteitä.

EU:n viides rahanpesudirektiivi täydentää EU:n neljättä rahanpesudirektiiviä ja direktiivin päätavoitteisiin kuuluu ehkäistä virtuaalivaluutan anonyymiin käyttöön osana terrorismin rahoittamista liittyviä riskejä ja rajoittaa prepaid-korttien käyttöä. Tavoitteena on myös parantaa yritysten omistussuhteiden avoimuutta tosiasiallisten omistajien rekistereillä ja vahvistaa korkean riskin kolmansiin maihin suuntautuvien ja niistä lähtevien rahoitustoimien seurantaa. Lisäksi pyritään parantamaan EU:n rahanpesun selvittelykeskuksen toimivaltaa ja pääsyä tietoihin, mukaan lukien keskitettyihin pankkitilirekistereihin. Keskitettyjen kansallisten pankki- ja maksutilirekistereiden tai keskitettyjen tiedonhakujärjestelmien varmistaminen on otettu tavoitteeksi kaikissa jäsenvaltioissa.

3.6.3. Rahanpesurikosdirektiivi

Vuosina 1991–2015 annetut neljä rahanpesudirektiiviä sekä vuonna 2018 annettu neljättä rahanpesudirektiiviä täydentävä viides rahanpesudirektiivi koskevat ensisijaisesti rahanpesun preventiivistä sääntelyä. Lokakuussa 2018 annettiin puolestaan rahanpesurikosdirektiivi, joka on ensimmäinen nimenomaan rahanpesun rikosoikeudellista sääntelyä harmonisoiva direktiivi.[111]

Rahanpesurikosdirektiivi synnyttää aidosti ylikansallista rahanpesurikosoikeutta. Pyrkimyksenä on, että 2020-luvulla rahanpesu olisi kriminalisoitu hyvin samankaltaisesti kaikissa rikosoikeudelliseen yhteistyöhön sitoutuneissa EU:n jäsenvaltioissa.[112] Direktiivillä saavutetaan tulevaisuudessa EU:n sisällä yhtenäisemmät esirikosluettelot ja rahanpesurikosten rangaistusasteikot. Direktiivi sisältää myös rikoshyödyn menetetyksi tuomitsemista ja kansallisvaltioiden lainkäyttövaltaa koskevia klausuuleja.[113]

Rahanpesurikosdirektiivi velvoittaa jäsenmaat kriminalisoimaan rahanpesun tiettyjen vähimmäisstandardien mukaisesti. Kansallisten tuomioistuinten tehtäväksi jää rahanpesurikoslainsäädännön soveltaminen, mutta lähtökohtaisesti rahanpesusta rangaistaan tulevaisuudessa yhteneväisesti.[114]

EU:n sääntelytoimet mahdollistavat tulevaisuudessa sen, että ainakaan EU:n sisälle ei pääse muodostumaan haitallisia löyhemmän AML/CFT-sääntelyn turvasatamia. Rikoshyödyn menetetyksi tuomitseminen ja takaisinsaanti voi kuitenkin kryptovaluuttojen kohdalla olla teknisen anonymiteetin vuoksi vaikeaa. Myös rikoshyödyn määrän arviointi ja varojen sijainnin selvittäminen on hyvin haastavaa. Vaikka viranomaiset tietäisivät esimerkiksi rikollisen käyttämän Bitcoin-osoitteen, on varoihin mahdotonta päästä käsiksi ilman yksityisavainta. Varoja on mahdollista siirtää lainvalvontaviranomaisten valvonnan alta ja käytännössä tätä tapahtuukin. Silk Road -ajalta peräisin olevia Bitcoin-osoitteita on useiden vuosien jälkeen alkanut aktivoitua. Rikoshyödyn piilottamista edesauttavat lisäksi erilaiset yksityisyyskryptovaluutat ja sekoitinpalvelut.[115]

---

[111] Ibid, s. 54–55.
[112] Ibid, s. 55–56.
[113] Ibid, s. 56–57.
[114] Ibid, s. 58.
[115] Ks. *Criddle* BBC News 2020. Silk Road -palveluun liittyvän, artikkelin julkaisuhetkellä noin miljardin dollarin arvoisen, Bitcoin-osoitteen varoja alettiin siirrellä.

3.6.4. Kotimainen lainsäädäntö

Verohallinto oli ensimmäinen kryptovaluutat huomioinut taho Suomessa, kun se sisällytti ne harmaan talouden tilannekuvaan vuonna 2011.[116] Kryptovaluuttoja suoraan koskevia lainsäädäntötoimia tehtiin Suomessa kansallisella tasolla vasta AMLD5:n myötä. Viidennen rahanpesudirektiivin täytäntöönpanemiseksi säädettiin viisi lakia ja yksi asetus. Suomi on näillä säädöksillä pyrkinyt suojaamaan EU:n rahoitusmarkkinoita ja estämään rahanpesua. Suomen säätämät lait ovat osa EU:n jäsenvaltioiden yhteistä pyrkimystä torjua digitalisaation myötä lisääntyneitä rahanpesun ja terrorismin rahoittamisen muotoja. Hallituksen esityksessä eduskunnalle laiksi pankki- ja maksutilien valvontajärjestelmästä ja eräiksi siihen liittyviksi laeiksi kuvaillaan virtuaalivaluuttojen tarjoajien sääntelyä seuraavasti:

> ”Virtuaalivaluuttojen tarjoajien toiminnan tullessa lainsäädännön piiriin, lisää tämä avoimuutta ja luotettavuutta toimijoita kohtaan. Lisäksi virtuaalivaluuttojen tarjoajien asiakkaan tuntemisvelvoite ja rekisteröitymisvelvoite voivat olla omiaan vähentämään virtuaalivaluuttojen käyttöä rikollisessa toiminnassa. Kuitenkin virtuaalivaluutat liikkuvat kansainvälisesti rajojen yli ja niitä tarjotaan maailmanlaajuisesti, minkä takia kansalliseen tai EU:n sääntelyn piiriin tuleminen voi siirtää virtuaalivaluutan tarjoajat toimimaan valtioissa, joissa vastaavanlaisia lainsäädännön vaatimuksia ei ole.”[117]

AMLD5:n 32 a artikla velvoittaa jäsenmaat perustamaan keskitettyjä automatisoituja mekanismeja pankki- ja maksutilien sekä tallelokeroiden haltijoiden tunnistamiseksi. Suomessa säädettiin 32 a artiklan noudattamiseksi laki pankki- ja maksutilien valvontajärjestelmästä 571/2019. Lain tarkoituksena on sen 1 §:n 2 momentin mukaan: ”edistää viranomaisten sähköistä tiedonsaantia pankki- ja maksutileistä sekä tehostaa viranomaisten tiedustelujen oikeaa kohdentumista.”

Lain myötä otettiin käyttöön pankki- ja maksutilien valvontajärjestelmä, joka muodostuu pankki- ja maksutilien tiedonhakujärjestelmästä sekä pankki- ja maksutilirekisteristä. Lain 4 §:n 1 momentin mukaan:

> ”Luottolaitoksen on ylläpidettävä sähköistä pankki- ja maksutilien tiedonhakujärjestelmää, jonka avulla se välittää välittömästi ja salassapitosäännösten estämättä 2 momentissa tarkoitettuja tietoja asiakkaistaan toimivaltaiselle viranomaiselle. […]”

4 §:n 2 momentissa puolestaan eritellään mitä tietoja toimivaltaiselle viranomaiselle tiedonhakujärjestelmän kautta luovutetaan:

> ”Tilihaltijan ja sen käyttöoikeudenhaltijan, myös oikeushenkilön, yksilöiviä tietoja; rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain 1 luvun 5–7 §:ssä

[116] Ks. Verohallinto: Harmaan talouden tilannekuva 3/2011.
[117] HE 167/2018 vp s. 68.

> tarkoitettujen tosiasiallisten edunsaajien henkilötietoja; pankki- ja maksutilin IBAN-numero tai muu yksilöintitunnus sekä tilin avaamis- ja sulkemispäivä; sekä tallelokeron vuokraajan ja sen käyttöoikeutetun, myös oikeushenkilön, henkilötietoja."

Laki virtuaalivaluutan tarjoajista 572/2019 soveltuu sen 1 §:n mukaan "virtuaalivaluutan tarjoajien harjoittamaan liiketoimintaan". Lain 4 § edellyttää, että "elinkeinonharjoittaja saa tarjota virtuaalivaluuttaan liittyviä palveluita vain, jos se on rekisteröity tämän lain mukaisesti virtuaalivaluutan tarjoajaksi". Kuten lain 5 §:ssä todetaan, "Finanssivalvonta pitää rekisteriä virtuaalivaluutan tarjoajista. Sen, joka aikoo tarjota virtuaalivaluuttoihin liittyviä palveluita, on tehtävä ilmoitus Finanssivalvonnalle rekisteriin merkitsemistä varten". Mitä erinäisiin laiminlyönteihin tulee, voi Finanssivalvonta lain 17 §:n mukaisesti "kieltää virtuaalivaluutan tarjoajaa jatkamasta toimintaansa, kunnes laiminlyönti on korjattu".

Virtuaalivaluuttalain 2 § tarjoaa myös määritelmän virtuaalivaluutoille sekä virtuaalivaluutan tarjoajille. Määritelmät vastaavat AMLD5:ssä käytettyjä määritelmiä ja niihin liittyy samoja puutteita.[118]

Laki rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain muuttamisesta 573/2019 tuo rekisteröitymisvelvolliset virtuaalivaluutan tarjoajat rahanpesulainsäädännön soveltamisalaan. Tämän lain myötä virtuaalivaluutan tarjoajille asetetaan asiakkaantuntemisvelvoitteita sekä velvollisuus ilmoittaa epäilyttävistä transaktioista Rahanpesun selvittelykeskukselle. Vuoden 2019 joulukuussa virtuaalivaluutan tarjoajat tekivät 75 rahanpesuilmoitusta. Koko vuodelle 2021 on ennakoitu noin 70 000 rahanpesuilmoitusta.[119]

Finanssivalvonnasta annetun lain 878/2008 1 §:ssä on ilmaistu tiiviisti Finanssivalvonnan toiminnan tavoitteena olevan "finanssimarkkinoiden vakauden edellyttämä luotto-, vakuutus- ja eläkelaitosten ja muiden valvottaviksi säädettyjen vakaa toiminta, vakuutettujen etujen turvaaminen sekä yleinen luottamus finanssimarkkinoiden toimintaan".

Laki Finanssivalvonnasta annetun lain muuttamisesta 574/2019 toi lakiin joitakin muutoksia ja esimerkiksi lain 45 § sisältää nykyään maininnan virtuaalivaluutan tarjoajista:

> "Finanssivalvonta valvoo, että valvottavat, asunto-omaisuuteen liittyvien kuluttajaluottojen välittäjät, vakuutuksentarjoajat ja virtuaalivaluutan tarjoajat noudattavat niihin sovellettavia markkinointia ja sopimusehtojen käyttöä sekä kuluttajan kannalta hyvän tavan vastaista tai muutoin sopimatonta menettelyä asiakassuhteessa koskevia säännöksiä. Rahoitusvälineiden markkinointia koskevien säännösten noudattamisen valvonnasta säädetään lisäksi arvopaperimarkkinalaissa, sijoituspalvelulaissa ja muualla laissa."

[118] Virtuaalivaluuttalain 2 §:n määritelmät esitetty aiemmin osiossa 2.1.
[119] Rahanpesun selvittelykeskus 2020, s. 8–9.

71 §:n mukaan:

> ”Sen lisäksi, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään, Finanssivalvonnalla on oikeus luovuttaa salassapitosäännösten estämättä tietoja:
>
> 15) rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain 7 luvun 1 §:n 1 momentissa tarkoitetuille viranomaisille ja 2 momentissa tarkoitetulle asianajajayhdistykselle sekä niitä vastaavalle ETA-valtion viranomaiselle tai toimielimelle, jos tiedot ovat välttämättömiä rahanpesun ja terrorismin rahoittamisen estämiseksi ja paljastamiseksi, sekä rahanpesun selvittelykeskukselle sen tehtävien hoitamiseksi; (26.4.2019/574)”

Laki Finanssivalvonnan valvontamaksusta annetun lain muuttamisesta 575/2019 lisäsi virtuaalivaluutan tarjoajat maksuvelvollisten listaan suorittamaan Finanssivalvonnan valvontamaksun.

Valtioneuvoston asetuksessa rahanpesun ja terrorismin rahoittamisen estämisestä annetussa laissa tarkoitetuista merkittävistä julkisista tehtävistä 610/2019 säädetään sen 1 §:n mukaan:

> ”rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain (444/2017), jäljempänä rahanpesulaki, 1 luvun 4 §:n 11 kohdassa tarkoitetuista merkittävistä julkisista tehtävistä, joissa toimivaa tai toiminutta henkilöä on pidettävä poliittisesti vaikutusvaltaisena henkilönä.”

Suomi sai Euroopan komissiolta 25.1.2019 perustellun lausunnon, jonka mukaan Suomi ei ole saattanut kansallista lainsäädäntöään kaikkien neljännen rahanpesudirektiivin säännösten mukaisiksi. Komission kiinnitettyä erityistä huomiota joihinkin direktiivin säännöksiin, Suomen hallitus aikoi arvioida tarvetta mahdolliseen lainsäädännön täsmentämiseen.[120] FATF nosti vuosina 2018–2019 laatimansa maa-arvion perusteella Suomen toiminnassa esiin puutteita, joiden vuoksi kansallisia rahanpesun ja terrorismin rahoittamisen estämistä koskevia säännöksiä, erityisesti rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain säännöksiä tulee muuttaa tai täydentää kansallisen lainsäädännön yhteensovittamiseksi FATF:n suositusten kanssa. Suomi on maa-arvioinnin jälkeen FATF:n tehostetussa seurannassa.[121]

Suomi asetti työryhmän arvioimaan, miten rahanpesun ja terrorismin rahoittamisen estämistä koskevaa lainsäädäntöä tulisi muuttaa. Muutoksessa tulee ottaa huomioon EU:n rahanpesudirektiivien kansallisessa täytäntöönpanossa havaitut puutteet, FATF:n huhtikuussa 2019 julkaisemassa Suomen maa-arvioraportissa esitetyt toimenpidesuositukset sekä kansalliset rahanpesun ja terrorismin rahoittamisen estämiseen liittyvät lainsäädännön muutostarpeet.[122]

---

[120] HE 261/2020 vp s. 3.
[121] Ks. FATF: Finland Mutual Evaluation Report 2019.
[122] Ks. Valtiovarainministeriön hanke VM191:00/2020.

3.6.5. Ilmoitusvelvolliset tahot järjestelmän portinvartijoina

Ilmoitusvelvolliset toimijat ovat ikään kuin EU:n AML/CFT-järjestelmän portinvartijoita. Ne ovat EU:n järjestelmässä rahanpesun estämisen ja terrorismin rahoittamisen estämisen kannalta keskeisiä toimijoita, joihin sääntelytoimet on helpoin kohdistaa.[123] Tärkeimpiä ilmoitusvelvollisia tahoja ovat kryptovaluuttapörssit ja lompakkopalveluntarjoajat. Portinvartijoilla tarkoitetaan tässä yhteydessä EU:n järjestelmässä tunnettuja kahta tahoa, lompakkopalveluntarjoajia ja palveluntarjoajia, jotka hoitavat valuutansiirtoja kryptovaluuttojen ja fiat-valuuttojen välillä.

Kryptovaluuttapörssien merkitys AML/CFT-järjestelmässä on huomattavan suuri. Vaikka Bitcoin-verkko itsessään on hajautettu, voidaan kryptovaluuttapörssejä pitää keskitettyinä toimijoina, vaikka ne hoitavat transaktioita globaalisti. Kryptovaluuttapörssit ovat merkittävä väylä rahaliikenteelle etenkin fiat-valuuttojen ja kryptovaluuttojen välillä, mahdollistaen kryptovaluuttojen oston ja myynnin sekä long- ja short-positiot. Kryptovaluuttapörssit ovat helppokäyttöisiä ja globaalisti kaikkien käytettävissä.

Ilmoitusvelvollisten tahojen on sovellettava palveluihinsa lainsäätäjän edellyttämiä AML/CFT-toimenpiteitä ja valvottava, että niiden asiakkaat noudattavat eri lainkäyttöalueiden lakeja. Tämä valvonta tapahtuu käytännössä asiakkaan tuntemismenettelyn kautta ja kansallisille valvontatahoille tehtävin ilmoituksin. Jotkut palveluntarjoajat laativat omia AML/CFT-käytäntöjään jo ennen laajamittaisia EU:n lainsäädäntöhankkeita. Esimerkiksi slovenialainen Bitstamp-kryptovaluuttapörssi, asetti omat AML/CFT-käytäntönsä, jotka ovat nähtävissä palvelun verkkosivuilla.[124] EU:n asettamien standardien noudattaminen korostaa palveluiden legitiimiyttä ja pyrkimystä laittomien toimien ehkäisemiseen.[125]

Kryptovaluuttapörssit kuuluvat FATF:n suositusten mukaan AML/CFT-järjestelmän piiriin rahoituslaitoksena. FATF määrittelee suosituksissaan rahoituslaitoksen olevan:

> ”mikä tahansa luonnollinen henkilö tai oikeushenkilö, joka harjoittaa liiketoimintaa yhdellä tai useammalla seuraavista tavoista asiakkaidensa puolesta tai heidän lukuunsa:
>
> 1. Talletusten ja muiden takaisin maksettavien varojen hyväksyminen yleisöltä
>
> 4. Rahan- tai arvonsiirron palvelut”

[123] Ks. Euroopan komissio: Money laundering. Euroopan komission verkkosivuilla kerrotaan lisää EU:n rahanpesun vastaisista toimista.
[124] Ks. Bitstamp AML-policy.
[125] Esimerkiksi Bitstamp ei saa hoitaa määrätyillä sanktiolistoilla olevien tahojen transaktioita ja sen vuoksi se tutkii Yhdistyneiden kansakuntien, Euroopan unionin, Ison-Britannian valtiovarainministeriön ja Yhdysvaltain ulkomaisen omaisuuden valvonnan toimiston (OFAC) pakoteluetteloita kaikilla lainkäyttöalueilla, joilla palvelu toimii.

Kryptovaluuttapörssit täyttävät kummatkin edellä mainituista rahoituslaitoksen tunnusmerkeistä, joten tästä näkökulmasta niiden harjoittamaa liiketoimintaa tulee kohdella oikeudellisesti samalla tapaa kuin perinteisten rahoituslaitosten toimintaa. Kuten edellä Bitstampin kohdalla todettiin, osa kryptovaluuttapörsseistä harjoittaa mittavaa itsesääntelyä korostaakseen toimintansa legitiimiyttä ja kryptovaluuttojen asemaa vaihtoehtoisena ja ennen kaikkea laillisena transaktiovälineenä.

On kuitenkin epärealistista luottaa pelkästään kryptovaluuttapörssien itsesääntelyyn. Esimerkiksi maailman suurin kryptovaluuttapörssi Binance[126] on tällä hetkellä Yhdysvaltojen veroviraston ja oikeusministeriön tutkinnan kohteena mahdollisten rahanpesu- ja veronkiertotapausten vuoksi.[127]

Lohkoketjun rikosteknistä tutkimusta harjoittava Chainalysis kokosi vuonna 2020 raportin kryptovaluuttoihin liittyvästä rikollisuudesta. Raportista ilmenee muun muassa, että noin 27,5 % kaikesta laittomasta alkuperästä olevista bitcoineista kulkeutuu Binanceen. Toisena raportissa on kiinalainen Huobi, jonne laittomista bitcoineista kulkeutui 24,7 %.[128]

Joukko alan johtavia toimijoita on perustanut Digital Asset Transfer Authority (DATA) komitean, jonka tarkoituksena on kehittää kryptovaluuttojen hallinnan alalle yleisesti hyväksyttyjä standardeja. Komitean ohjesäännöt perustuvat edellä mainittuihin FATF:n suosituksiin ja ne on tarkoitettu erityisesti auttamaan alan toimijoiden itsesääntelyä.[129]

Edellä esitetyn laittoman bitcoinliikenteen tilaston perusteella voidaan kuitenkin sanoa, etteivät pelkät itsesääntelyyn viittaavat ohjeet takaa riittäviä AML/CFT-toimia kryptovaluuttapörsseiltä. Rahanpesun ja terrorismin rahoittamisen estämistä koskevaa lainsäädäntöä on viime vuosina uudistettu merkittävästi EU:ssa ja kansallisella tasolla. Ilmoitusvelvollisten tahojen velvollisuuksia lisätään ja tarkennetaan jatkuvasti.

[126] Binance on rekisteröity Caymansaarille, sillä on toimisto Singaporessa, mutta yhtiöllä ei ole missään varsinaista yksittäistä päämajaa. Useiden kryptovaluuttapörssien kohdalla on epäselvyyksiä siitä, mihin lainkäyttöalueeseen ne kuuluvat.
[127] Ks. *Gordon* ETF Trends 2021.
[128] Ks. Chainalysis crypto crime report 2020, s. 10.
[129] Ks. Digital Asset Transfer Authorityn verkkosivut.

3.6.6. Asiakkaiden tuntemismenettely

AML/CFT-järjestelmän keskeinen ennaltaehkäisevä mekanismi on asiakkaiden tuntemismenettely[130]. Ennaltaehkäisy edellyttää epäilyttävien transaktioiden ilmoittamista, seurantaa ja havaitsemista. Asiakkaiden tuntemismenettelyyn kuuluu velvoite tuntea asiakkaansa[131]. Tällä tarkoitetaan toimia, joilla esimerkiksi pankit vahvistavat asiakkaidensa henkilöllisyyden ennen pankkitilin avaamista tai epäilyttävien transaktioiden hyväksymistä. Asiakkaiden tuntemismenettely velvoittaa myös pitämään kirjaa tilitapahtumista, ilmoittamaan epäilyttävistä transaktioista valvontaa tekeville tahoille ja olemaan mainittujen tahojen valvonnassa. Merkittävä ennaltaehkäisevä vaikutus on, että asiakkaiden tuntemismenettelytoimet auttavat lainvalvontaviranomaisia jäljittämään epäilyttävien transaktioiden osapuolia.[132]

Asiakkaan tuntemisesta on säädetty laissa rahanpesun ja terrorismin rahoittamisen estämisestä (444/2017). Lakia muutettiin vuonna 2021 lailla rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain muuttamisesta (376/2021). Muutetun lain 3 luvun 1 §:n 1 momentin mukaan asiakkaan tunteminen ja riskiperusteinen arviointi edellyttää, että:

> ”Ilmoitusvelvollisen on asiakassuhteeseen liittyviä rahanpesun ja terrorismin rahoittamisen riskejä arvioidessaan otettava huomioon uusiin ja jo olemassa oleviin asiakkaisiin, maihin tai maantieteellisin alueisiin sekä uusiin, kehitettäviin ja jo olemassa oleviin tuotteisiin, palveluihin ja liiketoimiin sekä jakelukanaviin ja teknologioihin liittyvät rahanpesun ja terrorismin rahoittamisen riskit (*riskiperusteinen arviointi*).”

Asiakkaan tunnistamisesta ja henkilöllisyyden todentamisesta säädetään 3 luvun 2 §:n 1 momentissa:

> ”Ilmoitusvelvollisella ei saa olla tässä pykälässä säädettyjä poikkeuksia lukuun ottamatta anonyymeja tai tekaistuilla nimillä olevia tilejä tai asiakkuuksia. Ilmoitusvelvollisen on tunnistettava asiakkaansa ja todennettava tämän henkilöllisyys vakituista asiakassuhdetta perustettaessa. Lisäksi ilmoitusvelvollisen on tunnistettava asiakkaansa ja todennettava tämän henkilöllisyys, jos:
>
> 1) asiakkuus on satunnainen ja:
>
> a) liiketoimen suuruus tai toisiinsa kytkeytyvien liiketoimien suuruus yhteensä on vähintään 10 000 euroa;
>
> b) kyse on maksajan tiedot -asetuksen 3 artiklan 9 kohdassa tarkoitetusta varojen siirrosta, jonka määrä ylittää 1 000 euroa; tai
>
> c) kyse on virtuaalivaluutan tarjoajista annetussa laissa tarkoitetussa virtuaalivaluuttaan liittyvässä palvelussa tehdystä liiketoimesta, jonka määrä ylittää 1 000 euroa;”

[130] Eng. customer due diligence (CDD).
[131] Eng. know your customer (KYC).
[132] Ks. Finanssivalvonta: Standardi 2.4 Asiakkaan tunteminen 2010.

Käytännössä monilla virtuaalivaluutan palveluntarjoajilla on ollut merkittäviä vaikeuksia suoriutua esimerkiksi lain 4 luvun 1 §:n 1 momentin mukaisesta ilmoitusvelvollisuudesta:

> ”Ilmoitusvelvollisen on täytettyään 3 luvun 4 §:n 3 momentissa säädetyn selonottovelvollisuuden viipymättä ilmoitettava rahanpesun selvittelykeskuksesta annetussa laissa (445/2017) tarkoitetulle rahanpesun selvittelykeskukselle epäilyttävästä liiketoimesta ja terrorismin rahoittamisen epäilystä. Ilmoitus epäilyttävästä liiketoimesta on tehtävä riippumatta siitä, onko asiakassuhde perustettu tai siitä kieltäydytty, ja siitä, onko liiketoimi suoritettu, keskeytetty tai siitä kieltäydytty.”

Perinteiset rahoituslaitokset ovat AML/CFT-järjestelmässä keskeisessä asemassa. Rahoituslaitokset pystyvät keskitettyjen operatiivisten järjestelmiensä avulla tehokkaasti noudattamaan asiakkaiden tuntemismenettelyä. Sitä vastoin osa kryptovaluuttaverkoista on rakenteeltaan äärimmäisen hajautettuja ja niiden käyttäjät asuvat kaikkialla ympäri maailmaa. Jos verkossa ei ole keskitettyä valvontaviranomaista on vaikeaa asettaa AML/CFT-vaatimuksia ja varmistaa, että niitä myös noudatetaan. Tämä on säädännöllinen aukko, jota rikolliset voivat hyödyntää ja jota lainsäätäjät yrittävät paikata.

3.7. EU:n järjestelmä ei ole FATF:n suositusten mukainen

Kun AMLD5:n mukaista EU:n AML/CFT-järjestelmää verrataan FATF:n suosituksiin havaitaan, ettei EU:n järjestelmä vastaa FATF:n asettamaa kansainvälistä standardia. Esimerkiksi virtuaalivaluutan ja lompakkopalvelujen määritelmät poikkeavat toisistaan. AMLD5:n myötä 3 artiklaan lisättiin alakohdat 18 ja 19, joissa käsitteet on määritelty seuraavasti:

> ”18) ’virtuaalivaluutoilla’ digitaalisia arvonkantajia, jotka eivät ole keskuspankin tai viranomaisen liikkeeseen laskemia tai takaamia, joita ei välttämättä ole kytketty lailliseksi maksuvälineeksi vahvistettuun valuuttaan ja joilla ei ole samaa oikeudellista asemaa kuin valuutalla tai rahalla, mutta jotka luonnolliset henkilöt tai oikeushenkilöt hyväksyvät vaihdantavälineenä ja joita voi siirtää, varastoida ja myydä sähköisesti;
>
> 19) ’lompakkopalvelujen tarjoajalla’ yhteisöä, joka tarjoaa palveluja yksityisten salausavaimien turvaamiseksi asiakkaidensa puolesta virtuaalivaluuttojen säilyttämiseksi, varastoimiseksi ja siirtämiseksi.”

Vastaavat käsitteet on ilmaistu FATF:n suosituksissa huomattavasti laajemmin:[133]

> “Virtuaalivarallisuus tarkoittaa digitaalista arvoesitystä, jolla voidaan digitaalisesti käydä kauppaa tai siirtää ja jota voidaan käyttää maksamiseen tai sijoittamiseen. Virtuaalivarallisuus ei sisällä digitaalisia vastineita fiat-valuutoista, arvopapereista ja muita rahoitusvaroja, jotka on jo katettu muualla FATF:n suosituksissa;

[133] Ks. FATF: Draft updated Guidance for a risk-based approach to virtual assets and VASPs. 2020, s. 18.

> Virtuaalipalvelujen tarjoaja tarkoittaa jokaista sellaista luonnollista henkilöä tai oikeushenkilöä, jota ei käsitellä muualla suosituksissa, ja joka liiketoimintana harjoittaa yhtä tai useampaa seuraavista toiminnoista toisen luonnollisen henkilön tai oikeushenkilön puolesta tai lukuun:
>
> i. Vaihto virtuaalivarojen ja fiat-valuuttojen välillä;
> ii. Vaihto yhden tai useamman virtuaalisen omaisuuden muodon välillä;
> iii. Virtuaalivarojen siirto; ja
> iv. Virtuaalivarojen säilytyspalveluiden tarjoaminen ja/tai sijaishallinta virtuaalivarojen hallinnan mahdollistamiseksi;
> v. Rahoituspalvelujen tarjoaminen, joka liittyy liikkeeseenlaskijan tarjoukseen ja/tai virtuaalisen omaisuuden myyntiin."

Kuten edellä esitetystä havaitaan, EU:n viidennen rahanpesudirektiivin tarjoama määritelmä virtuaalivaluutoille ei ole yhtä kattava kuin FATF:n suositusten mukainen määritelmä. FATF:n suosituksissa puhutaan virtuaalivaroista, kun taas EU:n direktiivissä puhutaan virtuaalivaluutoista. EU:n järjestelmä ei yhtä kattavasti tunnista eri alustatyyppejä, kuin mihin FATF:n suosituksilla on pyritty. AMLD5:ssä ei esimerkiksi mainita kryptovaluuttojen lisäksi muita virtuaalivarallisuuden tyyppejä, kuten rahakkeita[134]. AMLD5:stä puuttuu myös useita FATF:n suosituksissa mainittuja kryptovaluutta-alan toimijoita, kuten: alustat, jotka tarjoavat vaihtopalveluita ainoastaan kryptovaluutasta toiseksi (crypto-to-crypto); alustat, jotka fasilitoivat kryptovaluuttojen siirtoja välittäjätahona; ja rahoituspalvelujen tarjoaminen, joka liittyy liikkeeseenlaskijan tarjoukseen ja/tai virtuaalisen omaisuuden myyntiin.[135]

AMLD5:ttä laadittaessa lainsäätäjä ei kiinnittänyt riittävästi huomiota näiden toimijoiden olemassaoloon ja niihin liittyviin AML/CFT-uhkiin. Riskitietoisuus on myöhemmin kohonnut EU:n toimijoissa, kuten Euroopan arvopaperimarkkinaviranomaisessa (ESMA)[136] ja Euroopan pankkiviranomaisessa (EPV).[137] Lisäksi jäsenvaltioiden kansalliset toimijat ovat valveutuneet niihin riskeihin, joita AMLD5 ei riittävästi kattanut.[138] Vaikka direktiivi on verrattain uusi, on se säädännöllisestä näkökulmasta katsottuna jo vanhentunut ja riittämätön vastaamaan nykypäivän AML/CFT-uhkiin.

[134] Rahakkeilla tarkoitetaan esimerkiksi erilaisia sijoitus- ja hyötypoletteja, joiden pääasiallinen funktio ei ole vaihdanta.
[135] Ks. *Houben – Snyers* 2018, s. 76–80.
[136] Ks. ESMA: Advice on Initial Coin Offerings and Crypto-Assets 2019, s. 36.
[137] Ks. EPV: Report with advice for the European Commission on crypto-assets 2019, s. 20–21.
[138] Ks. Euroopan komissio: Commission Staff Working Document SWD(2019) 650 final 2019, s. 101–102.

3.8. Ehdotuksia EU:n järjestelmän kehittämiseksi

Jotta EU:n AML/CFT-järjestelmä vastaisi paremmin FATF:n suosituksia ja siten kansainvälistä tasoa, on tehtävä joitakin muutoksia. Seuraavaksi käsitellään FATF:n suosituksiin perustuvia lisäyksiä, joiden myötä EU:n järjestelmää voitaisiin kehittää.

1) Virtuaalivaluuttojen käsitteen laajentaminen

Ensinnäkin EU:n käyttämä virtuaalivaluutan käsite ei ole riittävän laaja ja nykymuodossaan se ei tuo tarpeeksi montaa eri käyttömuotoa sääntelyn piiriin. Jotta EU:n käyttämä virtuaalivaluutan määritelmä olisi tarpeeksi laaja, tulisi sen sisältää ainakin seuraavat virtuaalivaluutan muodot:

a. Poletit

EU:n nykymuotoinen virtuaalivaluutan määritelmä kattaa ainoastaan digitaaliset arvoesitykset, jotka hyväksytään vaihdon välineenä. Määritelmä on yllä esiteltyä FATF:n virtuaalivarojen määritelmää huomattavasti ohuempi, koska se ei sisällä sijoitus- ja hyötypoletteja[139], vaan kattaa ainoastaan kryptovaluutat.

ESMA[140] ja EPV[141] ilmaisivat 2019 tammikuussa julkaistussa virtuaalivarallisuutta koskevassa raportissa, että olisi järkevää laajentaa virtuaalivaluuttojen määritelmä koskemaan kaikenlaisia virtuaalivaroja, siitä syystä, että polettien ja muiden virtuaalivarallisuuden muotojen toiminta perustuu samaan teknologiaan kuin kryptovaluuttojen toiminta. Tekninen samanlaisuus mahdollistaa kryptovaluuttojen kanssa täysin yhtäläisen siirtämisen, tallentamisen ja vaihtamisen digitaalisesti. Vaihdot tapahtuvat vieläpä yleensä samoja kryptovaluuttapörssejä käyttäen.[142] Poletit toimivat samalla tavalla arvon siirron välineenä, joten ne ovat yhtä sopivia käytettäväksi rahanpesuun ja terrorismin rahoittamiseen. Suppean ja eksklusiivisen virtuaalivaluuttojen määritelmän käyttäminen ei ole millään tapaa perusteltua.

b. Keskuspankkien virtuaalivaluutat (CBDC)

Kryptovaluuttojen ja rahakkeiden lisäksi EU:n virtuaalivaluuttojen määritelmää olisi syytä laajentaa kattamaan keskuspankkien virtuaalivaluutat eli niin sanotut CBDC:t[143]. CBDC:t ovat valtiollisia valuuttoja ja niitä voidaan käyttää taloudellisten sanktioiden kiertämiseen.[144]

---

[139] Ks. *Fromberger – Haffke – Zimmermann* 2019, s. 13.
[140] Ks. ESMA: Advice on Initial Coin Offerings and Crypto-Assets 2021, s. 36.
[141] Ks. EPV: Report with advice for the European Commission on crypto-assets 2019, s. 20–21.
[142] Ks. *Fromberger – Haffke – Zimmermann* 2019, s. 13.
[143] Eng. Central Bank Digital Currency.
[144] Ks. Ciphertrace cryptocurrency intelligence: Q3 2019 Cryptocurrency Anti-Money Laundering Report 2019. Erityisesti Venezuelan sanktioita käsittelevä osa.

Sisällyttämällä keskuspankkien virtuaalivaluutat EU:n AML/CFT-järjestelmään ja laajentamalla ilmoitusvelvollisten toimijoiden luetteloa, EU voisi varmistaa, että epäilyttävät kolmansien maiden tahot, jotka pyrkivät liikuttamaan varojaan EU:n finanssijärjestelmässä CBDC:itä hyödyntäen kyettäisiin tunnistamaan ja lainvalvontaviranomaisten toiminta helpottuisi.

c. Pelinsisäiset valuutat

Suosittujen verkkopelien pelinsisäisiä valuuttoja on käytetty myös rahanpesutarkoituksiin. Rahanpesukäyttö perustuu siihen, että tämän tyyppisillä valuutoilla saattaa olla arvoa myös pelin ulkopuolella ja niitä voi olla mahdollista siirtää pelaajalta toiselle. Pelinsisäisten valuuttojen jälleenmyynti dark webissä ja sosiaalisen median alustojen kautta on yleistä.[145]

2) Portinvartijoiden luettelon laajentaminen

EU:n AML/CFT-järjestelmässä on virtuaalivaluuttoihin liittyen mainittu kaksi tunnettua portinvartijaa, kryptovaluuttapörssit ja lompakkopalveluntarjoajat. Alan toimijoiden lista on todellisuudessa paljon tätä laajempi, ja kaikki muun tyyppisissä palveluissa tapahtuva toiminta on nykyisellään AMLD5:n ulkopuolella. Puutteellinen nykytila jättää järjestelmään aukkoja, joita rikolliset voivat hyödyntää. Tästä syystä listaan on tehtävä lisäyksiä:

a. Kryptovaluutasta–kryptovaluutaksi-vaihtopalvelut

Vaihtopalvelut, jotka tarjoavat vaihtoja vain kryptovaluutasta kryptovaluutaksi, ja jotka eivät tarjoa lompakkopalveluja, eli ne eivät hallinnoi käyttäjiensä avaimia, eivät ole AMLD5:n piirissä. Tällaiset palvelut voivat tehdä kryptovaluuttojen alkuperän selvittämisestä vaikeampaa samalla tapaa kuin sekoitinpalvelut häivyttävät kryptovaluuttojen transaktiohistorian. Tällaiset palvelut olisi syytä lisätä EU:n järjestelmään ilmoitusvelvollisten joukkoon.

b. Rahoituspalvelut

Rahoituspalvelujen tarjoaminen, joka liittyy liikkeeseenlaskijan tarjoukseen ja/tai virtuaalisen omaisuuden myyntiin ei ole AMLD5:n piirissä. Tämänkaltaiset palvelut harjoittavat samantapaista toimintaa kuin perinteiset finanssilaitokset, jotka osallistuvat arvopaperien kauppaan. Näin ollen palveluihin liittyy samoja riskejä kuin perinteisiin toimijoihin, joten niitä olisi syytä säännellä samalla tapaa.[146]

[145] Ks. *Izenman – Moiseienko* RUSI 2019.
[146] Ks. FATF: Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers 2019.

c. Vaihtoalustat

Vaihtoalustoilla tarkoitetaan palveluita, joiden välityksellä ostajat ja myyjät käyvät kauppaa suoraan toistensa kanssa.[147] Tällaisista palveluista on olemassa sekä keskitettyjä että hajautettuja versioita. Keskitetyt vaihtoalustat olisi syytä sisällyttää EU:n järjestelmään FATF:n suositusten mukaisesti. Hajautettujen vaihtoalustojen sääntely on luonnollisesti lähes mahdotonta, koska niillä ei ole keskitettyä vastuutahoa johon sääntelytoimet voisi kohdistaa. Hajautettujen palveluiden toiminnan valvontaan tarvitaan kehittyneempää ja teknisempää lähestymistapaa, jota käsitellään myöhempänä.

d. Louhijat

Kun AMLD5:ttä laadittiin, Euroopan komissio perusteli louhijoiden poisjättämistä portinvalvojien listalta sillä, että louhijoita pidettiin enemmänkin teknisenä palveluntarjoajana kuin portinvartijana virtuaalisen maailman ja reaalimaailman välillä. Louhijoiden ajateltiin myös sijaitsevan enimmäkseen Kiinassa, joten tehokas sääntely olisi lähes mahdotonta.

Tilanne on kuitenkin muuttunut huomattavan paljon siitä, kun komissio nämä perustelunsa esitti. Louhinta on maantieteellisesti paljon hajautuneempaa ja Kiina on kohdistanut ankaria kieltotoimenpiteitä kryptovaluuttoihin sekä ryhtynyt toimiin suurten Bitcoin-louhintafarmien purkamiseksi. Nämä louhijat ovat siirtämässä toimintansa etenkin Pohjois-Amerikkaan sekä myös Eurooppaan.[148] Näin ollen louhijat ovat siirtymässä sellaisille alueille, joissa ne olisi helpompi sisällyttää sääntelyn piiriin. Louhijat muodostavat erittäin merkittävän osan koko kryptovaluuttaekosysteemiä, joten niiden sivuuttaminen olisi vastuutonta.

Rikolliset voivat kryptovaluuttojen louhinnalla joko suoraan itse tai välitahon kautta luoda puhdasta varallisuutta. Esimerkiksi uusia bitcoineja pidetään puhtaina, koska niillä ei ole olemassa olevaa transaktiohistoriaa, mikä tekee niistä tiettyjen tahojen silmissä halutumpia. Kun ”puhtaita” kryptovaluuttoja vaihdetaan fiat-valuutaksi ovat myös nämä varat puhtaita. Rikollisten suorittama louhinta muodostaa merkittävän lainsäädännöllisen aukon, johon on perinteisin sääntelykeinoin vaikea puuttua. Teknisin keinoin toteutettavaa konsensustason sääntelyä käsitellään tarkemmin kuudennessa pääluvussa.

[147] Tällä tarkoitetaan, että kaupankäynti tapahtuu vertaisten tahojen tekemän sopimuksen mukaan. Alusta ainoastaan auttaa kaupan osapuolia löytämään toisensa.
[148] Ks. *Vahiajun* Business Insider 2021.

3) EU:n oma AML/CFT-valvontaa suorittava toimielin

Lainvalvontaviranomaisten ja valvontaa suorittavien tahojen yhteistyö on välttämätöntä EU:n AML/CFT-järjestelmän tehokkaan toiminnan kannalta. Tämä edellyttää tietojen jakamista ja rajat ylittävää yhteistyötä.[149] Euroryhmä (ECOFIN) pyysi 5.12.2019 Euroopan komissiota selvittämään erityisesti mahdollisuuksia, etuja ja haittoja, jotka liittyvät tiettyjen rahanpesun torjunnan valvontaan liittyvien tehtävien ja valtuuksien siirtämiseen unionin elimelle, joka olisi rakenteeltaan riippumaton ja jolla olisi suoraa toimivaltaa suhteessa tiettyihin ilmoitusvelvollisiin, jotka EU:n elin on valinnut riskiperusteisen lähestymistavan mukaisesti rajat ylittävät näkökohdat huomioon ottaen, ja esittämään kattavan analyysin perusteella asiaa koskevia lainsäädäntöehdotuksia sellaisten toimien ohella, joilla pyritään nostamaan yhdenmukaistamisen tasoa rahanpesun vastaisen asetuksen avulla.[150] Tällaisen toimielimen perustamisesta voisi olla merkittävää hyötyä unionin AML/CFT-järjestelmässä olevien aukkojen paikkaamiseksi. Kryptovaluuttoihin liittyvien riskien arviointi vaatii laajaa IT-alan osaamista ja tällaisen toimielimen perustaminen auttaisi EU:ta pysymään kehityksessä ajan tasalla.

4) Subsidiariteettiperiaate ja kansalliset lainsäädäntötoimet

Subsidiariteetti- eli toissijaisuusperiaate on tärkeä EU-oikeuden periaate, jolla rajoitetaan unionin toimivaltaa suhteessa jäsenvaltioihin. Euroopan unionista tehdyn sopimuksen (SEU) 5 artiklan 3 kohdan mukaan unioni toimii aloilla, jotka eivät kuulu sen yksinomaiseen toimivaltaan, ainoastaan jos ja siltä osin kuin jäsenvaltiot eivät voi riittävällä tavalla saavuttaa suunnitellun toiminnan tavoitteita, vaan ne voidaan suunnitellun toiminnan laajuuden tai vaikutusten vuoksi saavuttaa paremmin unionin tasolla.[151]

Rahanpesu ja terrorismin rahoittaminen eivät ole minkään tietyn lainkäyttöalueen sisälle rajattuja ilmiöitä, vaan kyse on globaalista uhasta, jonka torjuntaan vaaditaan globaalia yhteistyötä. FATF ja sen antamat suositukset ovat hyvä esimerkki onnistuneesta kansainvälisestä yhteistyöstä, sillä FATF:n antamia suosituksia kunnioitetaan ja valtiot pyrkivät aktiivisesti ottamaan ne huomioon. FATF:n suositukset on otettu osittain huomioon EU:n lainsäädännössä ja niitä on osittain hyödynnetty AMLD5:n laatimisessa. Osana EU:n AML/CFT-järjestelmää, suositukset auttavat takaamaan EU:n sisämarkkinoiden ja finanssijärjestelmän toimivuutta.[152] FATF:n

[149] Ks. Euroopan komissio: Komission kertomus sisämarkkinoihin vaikuttavia ja rajat ylittäviin toimiin liittyviä rahanpesun ja terrorismin rahoituksen riskejä koskevasta arvioinnista 2019, s. 20.
[150] Ks. Euroopan unionin neuvosto: Neuvoston päätelmät rahanpesun ja terrorismin rahoituksen torjuntaa koskevista strategisista prioriteeteista 2019.
[151] Ks. *Melander* 2015, s. 133–134.
[152] Ks. *Brown – Butler – Dolan* 2019, s. 79.

suositukset ovat kuitenkin paljon EU:n nykyistä oikeustilaa kattavammat ja AMLD5 oli sisällöltään vanhentunut jo sillä hetkellä, kun jäsenmaiden tuli implementoida se viimeistään 10.1.2020.

Toissijaisuusperiaatteella turvataan jäsenvaltioiden mahdollisuudet tehdä päätöksiä ja toteuttaa toimia.[153] Yksittäiset jäsenmaat saattavat haluta mennä kansallisessa lainsäädännössään AMLD5:n viitoittamaa tietä pidemmälle vastatakseen paremmin FATF:n suosituksia ja ehkäistäkseen tehokkaammin rahanpesun ja terrorismin rahoittamisen vastatoimia. Suuret erot jäsenvaltioiden välisessä sääntelyssä eivät ole hyväksi, mutta kunnes EU-tason sääntelyä päivitetään saattaa jäsenmailla olla tarve paikata oikeustilan selkeimpiä haavoittuvuuksia. On kuitenkin selvää, että pelkät kansalliset toimet eivät ole riittäviä vaan EU:n olisi syytä ryhtyä uusiin lainsäädäntöhankkeisiin pikimmiten tilanteen korjaamiseksi. Mahdollisissa kansallisissa lainsäädäntöhankkeissa on syytä tehdä tarkoituksenmukaisuusarviointia ja suhteuttaa lainvalvontaviranomaisten kyky suorittaa tehokasta valvontaa yksilöiden tietosuojaan. Muun muassa Saksassa lainvalvontaviranomaisten kanssa työskentelee IT-alan ammattilaisia, joiden tietotaito on huomattavasti tehostanut viranomaisten toimintaa kryptovaluuttoihin liittyvissä tapauksissa.

3.9. Euroopan komission lainsäädäntöpaketti 20.7.2021

Euroopan unioni on ryhtynyt toimiin parannusten tekemiseksi EU:n AML/CFT-järjestelmään. Euroopan komissio teki 20.7.2021 ehdotuksen kunnianhimoisesta uudesta säädöspaketista, johon kuuluu toimenpiteitä rahanpesun ja terrorismin rahoituksen torjumiseksi. Pakettiin kuuluu uusi EU:n kuudes rahanpesudirektiivi, asetus uuden rahanpesun vastaisen EU-toimielimen perustamisesta sekä asetus rahanpesun ja terrorismin rahoittamisen estämisestä EU:n finanssijärjestelmässä. Näiden lisäksi uudistetaan asetusta 2015/847/EU varainsiirtojen mukana toimitettavista tiedoista, johon otetaan nyt mukaan tietyt kryptovarallisuuden tyypit. Säädöskokonaisuus on osa komission sitoumusta suojella EU:n kansalaisia ja EU:n finanssijärjestelmää tunnistamalla epäilyttävät transaktiot ja tapahtumat sekä paikkaamalla EU:n AML/CFT-järjestelmässä olleita heikkouksia, joita rikolliset ovat hyödyntäneet rahanpesuun ja terrorismin rahoittamiseen.[154] Euroopan unionin turvallisuusstrategiassa vuosille 2020–2025 todettiin myös, että EU:n AML/CFT-järjestelmää tehostamalla pystytään paremmin suojelemaan eurooppalaisia terrorismilta ja järjestäytyneeltä rikollisuudelta.[155]

---

[153] Ks. *Pavy* Faktatietoja Euroopan unionista 2021.
[154] Ks. Euroopan komissio: Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules 2021.
[155] Ks. Euroopan komissio: Komission tiedonanto EU:n turvallisuusunionistrategiasta 2020.

Lainsäädäntöpaketin yleisenä tavoitteena on kohentaa EU:n AML/CFT-järjestelmää siten, että jatkossa järjestelmä olisi tarpeeksi joustava kyetäkseen sopeutumaan EU:ta kohtaaviin uhkiin ja haavoittuvuuksiin. EU:n tulisi suhtautua riskeihin monipuolisesti ja vähentää kielteisiä vaikutuksia taloudelliseen toimintaan, kansalaisten yksityisyyteen ja henkilötietojen suojaan sen verran kuin on välttämätöntä ja suhteellista.[156] Tarkemmiksi tavoitteiksi on asetettu EU:n rahanpesusäädösten selkiyttäminen ja yhdenmukaistaminen kansainvälisten standardien kanssa; AML/CFT-valvonnan tehokkuuden ja tasalaatuisuuden parantaminen; sekä rahanpesun selvittelykeskusten välisen yhteistyön lisääminen.[157] Lainsäädäntöpaketti selkiyttää myös EU-säädöksissä esiintyviä käsitteitä ja näin ollen tekee lainsäädännöstä kattavampaa ja ymmärrettävämpää.

Lainsäädäntöpakettiin kuuluvalla asetuksella perustetaan uusi AML/CFT-valvontaa suorittava EU-toimielin. ”EU AML Authority” eli AMLA tulee tehostamaan rahanpesun selvittelykeskusten välistä yhteistyötä, toimien itse samalla keskitettynä auktoriteettina, jonka vastuulla on koordinoida kansallisten viranomaisten toimintaa varmistaakseen, että yksityisellä sektorilla noudatetaan EU:n säännöksiä. AMLA tukee myös rahanpesun selvittelykeskusten analyyttistä toimintakykyä. AMLA:n tavoitteena on yhden integroidun AML/CFT-valvontajärjestelmän perustaminen EU-alueelle, jonka toiminta perustuu yhteisiin valvontamenetelmiin ja jäsenmaiden valvontastandardien lähentämiseen.[158] Sen tarkoituksena on myös valvoa suoraan joitakin riskialttiimpia rahoituslaitoksia, jotka toimivat useissa jäsenvaltioissa tai jotka edellyttävät välittömiä toimia riskien torjumiseksi.[159] AMLA tulee lisäksi valvomaan ja koordinoimaan rahoituslaitoksia valvovia kansallisia valvontayksiköitä sekä niitä valvontayksiköitä, jotka valvovat muita kuin rahoituslaitoksia.[160] AMLA tukee kansallisten rahanpesun selvittelykeskusten välistä yhteistyötä ja helpottaa niiden välistä koordinointia sekä yhteisien analyysien tekemistä rajat ylittävien laittomien rahoituskanavien havaitsemisen tehostamiseksi.[161]

Asetus rahanpesun ja terrorismin rahoittamisen estämisestä EU:n finanssijärjestelmässä sisältää suoraan velvoittavia sääntöjä, muun muassa asiakkaan tunnistamisesta ja tosiasiallisista omistussuhteista. Rahanpesusäädösten johdonmukaiseksi noudattamiseksi kaikkialla sisämarkkinoilla on selkiytetty valvontaa ja menettelyjä, mukaan lukien asiakkaiden tuntemista koskevia

[156] Ks. Commission staff working document impact assessment Accompanying the Anti-money laundering package Brussels, 20.7.2021 SWD(2021) 190 final, s. 27.
[157] Ibid, s. 27–28.
[158] Proposal for a regulation of the European parliament and of the council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, s. 3.
[159] Ibid, s. 2.
[160] Ibid, s. 3.
[161] Ibid, s. 2.

toimenpiteitä, jotka ovat jatkossa vaihtelevampia asiakkaan riskitasoon perustuen.[162] Asetukseen kuuluu myös EU:n laajuinen 10 000 euron raja suurille käteismaksuille. Rajoitus estää tavaroiden tai palvelujen kauppiaita hyväksymästä yli 10 000 euron suuruisia käteismaksuja yhdestä ostoksesta, mutta jäsenvaltioilla on vapaus ylläpitää alempiakin rajoja.[163]

Uusi EU:n kuudes rahanpesudirektiivi korvaa nykyisen direktiivin 2015/849/EU, jota täydennettiin EU:n viidennellä rahanpesudirektiivillä. Direktiivi sisältää säännöksiä, jotka saatetaan osaksi kansallista lainsäädäntöä. Ne koskevat muun muassa jäsenvaltioiden kansallisia valvontatahoja ja rahanpesun selvittelykeskuksia. Kuudes rahanpesudirektiivi sallii jäsenvaltioissa, joissa virtuaalivaluuttojen liikkeeseenlaskijat, maksupalveluntarjoajat ja virtuaalivaluuttapalveluntarjoajat toimivat, jäsenvaltioiden valvontatahojen määrittää näille valvottaville kohteille yhteyspisteitä jäsenvaltiossa. Määrätty yhteyspiste toimii palveluntarjoajan vastuun ankkurina jäsenmaassa ja takaa, että AML/CFT-säädöksiä noudatetaan.[164] Yhteyspistejärjestelmästä tulee tehokas keino estää sellaisten palveluntarjoajien toimintaa, jotka eivät noudata AML/CFT-säädöksiä.

Kunkin jäsenvaltion on suoritettava kansallinen riskiperusteinen arvio rahanpesuun ja terrorismin rahoittamiseen liittyvien riskien yksilöimiseksi, arvioimiseksi, ymmärtämiseksi ja lieventämiseksi. Jäsenvaltion on pidettävä riskiarvio ajantasaisena ja tarkistettava se vähintään neljän vuoden välein.[165] Komissio suorittaa vastaavan riskiperusteisen arvion unionin tasolla viimeistään neljän vuoden kuluttua siitä päivästä, kun tämä direktiivi on tullut saattaa kansallisesti voimaan. Raportissa yksilöidään, arvioidaan ja analysoidaan riskejä unionin tasolla. Komissio päivittää raportin tiedot neljän vuoden välein tai tarvittaessa useammin.[166]

Yhdistämällä jäsenvaltioiden keskitetyt automatisoidut mekanismit, kansalliset rahanpesun selvittelykeskukset voisivat saada nopeasti rajat ylittäviä henkilötietoja kohteen pankki- ja maksutileistä sekä tallelokeroista, jotka sijaitsevat toisessa jäsenvaltiossa, mikä vahvistaisi niiden yhteistyökykyä. Suora rajat ylittävä pääsy pankki- ja maksutilejä ja tallelokeroita koskeviin tietoihin

[162] Proposal for a regulation of the European parliament and of the council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Brussels, 20.7.2021 COM(2021) 420 final 2021/0239 (COD), s. 2.
[163] Ibid, s. 10.
[164] Proposal for a directive of the European parliament and of the council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849 Brussels, 20.7.2021 COM(2021) 423 final 2021/0239 (COD), s. 8 ja 35.
[165] Ibid, s. 37–38.
[166] Ibid, s. 36–37.

mahdollistaa rahanpesun selvittelykeskusten toimivan riittävän lyhyessä ajassa mahdollisen rahanpesun ja terrorismin rahoittamisen havaitsemiseksi sekä takaa nopeat lainvalvontatoimet.[167]

Lainsäädäntöpaketin yhteydessä uudistetaan asetusta 2015/847/EU varainsiirtojen mukana toimitettavista tiedoista. Uudistuksen tavoitteena on mahdollistaa kryptovaluuttatransaktioiden tehokkaampi jäljittäminen. Merkittävä asetukseen tehtävä parannus liittyy kryptovarallisuuden käsitteen käyttöön varainsiirtojen käsitteen rinnalla. Sana kryptovarallisuus esiintyy uudessa asetuksessa 87 kertaa.[168] Asetusta 2015/847/EU sovelletaan nykyisellään vain varainsiirtoihin, mutta on asianmukaista laajentaa soveltamisalaa kattamaan myös virtuaalisen omaisuuden siirrot ja nostaa kryptografisesti salattu varallisuus tasa-arvoiseen asemaan.[169] Käsitteiden selkiyttäminen parantaa huomattavasti sääntelyn tehokkuutta, koska uudet käsitteet koskevat aiempaa laajempaa joukkoa alan palveluntarjoajia.

Asetuksella implementoidaan niin sanottu FATF:n matkasääntö[170]. Matkasääntö perustuu FATF:n 15. suositukseen ja edellyttää, että palveluntarjoajat hankkivat ja säilyttävät vaadittuja riittävän tarkkoja tietoja kryptovarallisuuden lähettäjistä ja siirronsaajista sekä toimittavat nämä tiedot siirron vastaanottavalle palveluntarjoajalle välittömästi ja turvallisesti. Nämä tiedot tulee myös asettaa lainvalvontaviranomaisten saataville siten, että tiedot luovutetaan asianomaisille viranomaisille pyynnöstä. Tämä säädös on osa EU:n yhteistä sääntökirjaa, jota sovelletaan suoraan ja välittömästi. Näin poistetaan poikkeavan soveltamisen mahdollisuus eri jäsenvaltioissa.[171]

Asetuksen edellyttämät erityisvelvoitteet tuottavat teknisiä haasteita palveluntarjoajille. Niiden on kehitettävä uusia teknisiä ratkaisuja ja protokollia tietojen keräämiseksi ja jakamiseksi toisten palveluntarjoajien sekä viranomaisten kanssa. Asetus parantaa merkittävästi palveluntarjoajien valvontaa ja tuo EU:n ja sen jäsenvaltiot paremmin linjaan FATF:n suosituksissa vaadittujen toimenpiteiden kanssa.

---

[167] Ibid, s. 20.
[168] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast) Brussels, 20.7.2021 COM(2021) 422 final 2021/0241 (COD), s. 11–45.
[169] Ibid, s. 11–12.
[170] Eng. FATF travel rule.
[171] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast) Brussels, 20.7.2021 COM(2021) 422 final 2021/0241 (COD), s. 8.

4. KRYPTOVALUUTAT OSANA KANSAINVÄLISTÄ RIKOLLISUUTTA

4.1. Kryptovaluuttojen asema kansainvälisessä rikollisuudessa

Kryptovaluuttoja hyödynnetään erityisesti luonteeltaan rajat ylittävässä rikollisuudessa. Siitä, mitkä rikokset kuuluvat kansainvälisen rikosoikeuden alaan, on erilaisia näkemyksiä. Suppean käsityksen mukaan kansainvälinen rikosoikeus kattaa vain varsinaiset kansainvälisen oikeuden vastaiset rikokset[172] joiden kriminalisointi perustuu kansainväliseen tapaoikeuteen. Tämän näkemyksen mukaan kansainvälisiin sopimuksiin perustuvat kansalliset kriminalisoinnit eivät kuulu kansainvälisen rikosoikeuden piiriin vaan ovat osa kansallista rikosoikeutta. Laajasti ymmärrettynä kansainvälisiksi rikoksiksi määritellään kaikki sellaiset teot, joiden vastustamiseen useat valtiot ovat yhdessä pyrkineet omaksumalla niitä koskevia kansainvälisen oikeuden sääntöjä. Laajemman näkemyksen mukaan rikosoikeuden alaan kuuluvat varsinaisten kansainvälisen oikeuden vastaisten rikosten lisäksi myös niin sanotut maailmanrikokset[173] eli kriminalisoinnit, jotka on otettu valtioiden kansalliseen rikoslainsäädäntöön kansainvälisiin sopimusvelvoitteisiin perustuen.[174]

Ensimmäinen ryhmä kattaa vakavimmat rikokset kuten joukkotuhonnan, hyökkäysrikokset ja erilaiset sotarikoksien muodot. Ne perustuvat kansainväliseen tapaoikeuteen ja kuuluvat Rooman perussäännön artiklojen 5–9 mukaan kansainvälisen rikostuomioistuimen toimivaltaan. Maailmanrikoksia, eli kansainvälisiin sopimusvelvoitteisiin perustuvia rikoksia ovat yleisemmät kansainväliset rikokset kuten ihmiskauppa[175], asekauppa[176], siirtolaiskauppa[177], esirikokset (esimerkiksi laiton timanttikauppa)[178] ja terrorismi[179]. Vaikka näille rikostyypeille on olemassa omat kansalliset määritelmänsä, on kansainvälinen yhteisö tunnistanut rikostyypeissä joitakin niitä yhdistäviä piirteitä ja nähnyt tarpeelliseksi koota rikokset kansainvälisiin sopimuksiin. Nämä rikokset ovat luonteeltaan kansalliset rajat ylittäviä, rikkovat useiden eri valtioiden lakeja ja niillä on merkittävä vaikutus koko kansainväliseen yhteisöön.

---

[172] Eng. core international crimes.
[173] Eng. Treaty crimes of international concern.
[174] Ks. *Kimpimäki* 2015, s. 28.
[175] SopS 71/2006 Kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen lisäpöytäkirja ihmiskaupan, erityisesti naisten ja lasten kaupan ehkäisemisestä, torjumisesta ja rankaisemisesta.
[176] SopS 74/2011 Kansainvälisen järjestäytyneen rikollisuuden vastaisen yhdistyneiden kansakuntien yleissopimuksen ampuma-aseiden, niiden osien ja komponenttien sekä ampumatarvikkeiden laittoman valmistuksen ja kaupan torjumista koskeva lisäpöytäkirja.
[177] SopS 73/2006 Kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen lisäpöytäkirja maitse, meritse ja ilmateitse tapahtuvan maahanmuuttajien salakuljetuksen kieltämisestä.
[178] SopS 20/2004 Palermon sopimus.
[179] SopS 74/2002 Terrorismin rahoituksen torjumista koskeva kansainvälinen yleissopimus.

Kryptovaluuttojen käyttö kansainvälisten rikosten yhteydessä ei ole yllättävää, sillä kryptovaluutat eivät ole sidottuja mihinkään tiettyyn hallitukseen eivätkä ne myöskään ole minkään keskitetyn rahoituslaitoksen liikkeelle laskemia. Kryptovaluuttojen käytön ideologinen tausta perustuu uusliberalistiseen ajatteluun siitä, että yksilöiden tulisi pystyä hoitamaan liiketoimiaan yksityisesti ilman valtion säädännöllisen kehyksen vaikutuksia tai nämä vaikutukset minimoiden.[180]

Kryptovaluuttojen hajautetun luonteen vuoksi niiden sääntely pelkästään yksittäisen valtion omassa lainsäädännössä on vaikea toteuttaa tehokkaasti. Tämä on ilmeistä siinä, miten jotkut valtiot, kuten Kiina ja Intia ovat tuloksetta kansallisella tasolla kieltäneet kryptovaluutat jopa useaan kertaan. Kryptovaluuttojen aseman horjuttaminen kansainvälisessä rikollisuudessa vaatii uudenlaisen lähestymistavan. Uuden oikeusrealistisen[181] näkökannan perusteella yksittäiset kansakunnat eivät voi yksinään tehokkaasti vaikuttaa kryptovaluuttojen käyttöön rahanpesussa ja muussa rajat ylittävässä rikollisuudessa. Tehokkaan uuden oikeudellisen kehyksen muodostaminen edellyttää sen sijaan valtioiden käyvän vuoropuhelua paitsi keskenään, myös asianmukaisten kansainvälisten instituutioiden kanssa, joilla on valmiuksia rahanpesun ja muun kansainvälisen rikollisuuden torjuntaan. Yhteistyötä tekemällä vältettäisiin myös tilanteet, joissa yhden valtion kryptovaluuttoihin kohdistamat toimet (esimerkiksi takavarikot ja kiellot) johtaisivat toisen valtion kansalaisten oikeudenmenetyksiin.

Seuraavaksi käsitellään kolmea rikostyyppiä: rahanpesua, terrorismin rahoitusta ja huumausaineiden kauppaa. Käsittelyn pääpainopiste on rahanpesussa. Siihen liitännäisen terrorismin rahoittamisen sääntely on kehittynyt pitkälti rahanpesusäädöksien pohjalta ja huumausaineiden kauppaa käsitellään rahanpesun esirikoksena. Huumausaineiden kaupasta siirrytään käsittelemään joitakin merkittävimpiä kryptovaluuttojen käyttöön liittyviä oikeudellisia erityiskysymyksiä.

[180] Ks. *Faife* Coindesk 2016.
[181] Ks. *Shaffer* 2015.

4.2. Rahanpesu ja kryptovaluutat

Rahanpesulla tarkoitetaan erilaisia toimia, joiden avulla pyritään peittämään tai häivyttämään rikollisin keinoin hankitun omaisuuden laiton alkuperä. Onnistunut rahanpesu saa omaisuuden vaikuttamaan laillisesti hankitulta.[182]

Suomen lainsäädännössä rahanpesusäännös on rikoslain 32 luvun 6 §:ssä:

> ”Rahanpesu. 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.”

Rahanpesun tehokas torjunta edellyttää mahdollisimman monien valtioiden ja talousalueiden rahanpesulainsäädännön yhtenäisyyttä ja tehokasta täytäntöönpanoa. Epäyhtenäinen tai puutteellinen kansallinen sääntely mahdollistaa hyvin organisoituneiden ja ammattitaitoisten rahanpesijöiden toiminnan näillä alueilla. Rahanpesun torjuntakeinojen tehokkuus alenee, jos jossakin muualla on mahdollista turvallisesti ja tehokkaasti kiertää rahanpesusäädöksiä sekä laillistaa rikoksella saatua hyötyä.[183]

Rahanpesun määritelmä sisältyy myös useaan kansainväliseen sopimukseen. Kansainvälisen järjestäytyneen rikollisuuden vastaisen Yhdistyneiden Kansakuntien yleissopimuksen 6 artiklan (a) momentin (i) kohdassa rahanpesua määritellään olevan:

> ”(a) (i) omaisuuden muuntaminen tai luovuttaminen tietoisena siitä, että omaisuus on saatu rikoksen avulla, tarkoituksena salata tai peittää omaisuuden laiton alkuperä tai auttaa sellaiseen esirikokseen osallistunutta henkilöä välttämään tekojensa oikeudelliset seuraamukset;”

Rahanpesua on 6 artiklan (a) momentin (ii) kohdan mukaan myös:

---

[182] Ks. *Kimpimäki* 2015, s. 337.
[183] Ks. *Sahavirta* 2008, s. 61.

> ”(ii) omaisuuden todellisen luonteen, alkuperän, sijainnin, hallinnan siirron tai omaisuuden siirtämisen tai siihen liittyvän omistusoikeuden tai muun oikeuden salaaminen tai peittäminen tietoisena siitä, että omaisuus on saatu rikoksen kautta;”

Rahanpesu on liitännäinen rikos, eli se edellyttää esirikosta, josta rahanpesutoimenpiteiden kohteena oleva taloudellinen hyöty on peräisin.[184] Rahanpesu on perinteisesti ollut rikollisen toiminnan päätepysäkki. Tarpeellinen viimeinen porras, jotta rikollisin keinoin ansaitut varat saadaan legitimoitua. Europolin raportin mukaan yleisimmät predikaattirikokset, joiden tienestejä rahanpesussa pestään ovat huumausainerikokset ja erilaiset petosrikokset. Rikollisverkostoista, joiden pääasiallisena toimialana arvioiden mukaan on rahanpesu lähes puolet (49 %) oli mukana myös huumausainekaupassa ja kolmasosalla (33 %) oli petostoimintaa.[185]

Rahanpesusta on ajan kuluessa tullut yhä enenevässä määrin myös rikollisuuden mahdollistaja. Rahanpesu ei ole pelkästään tapa kierrättää predikaattirikoksista saatua tuottoa laillisiin kanavoihin, vaan se on myös keino rahoittaa tulevia rikoksia.[186] Useissa maissa on havaittu toimivan erikoistuneita rikollisryhmiä, joiden toiminta keskittyy tarjoamaan muille rikollisille rahanpesupalveluja. Rikollisverkostot yhä useammin ulkoistavat rahanpesutoimintansa näille erikoisryhmille. Syinä tälle on arvioitu olevan joko halu etääntyä itse predikaattirikoksesta, tai pakon sanelema tarve kääntyä rahanpesun ammattilaisen[187] puoleen.

Näillä ammattilaisilla on riittävä tekninen asiantuntemus, tarvittavat yhteydet ja laaja infrastruktuuri lailliseen talousverkostoon, esimerkiksi hyödyntämällä korruptoituneita kontaktejaan. Näin ollen he voivat tarjota laajan valikoiman rahanpesupalveluitaan alihankkijaperusteisesti muille maksua vastaan. Palveluiden joukossa on muun muassa valuutanmuunnoksia, tekaistuja fiktiivisiä sopimuksia, valheellisia laskutuksia sekä tosiasiallisten omistussuhteiden häivyttämistä esimerkiksi erilaisten yritys- ja tilinhallintajärjestelyjen kautta.[188]

Viime vuosina rahanpesuun erikoistuneet rikollisryhmät ovat laajentaneet toimintaansa myös kryptovaluuttoihin. Espanjassa poliisi pidätti kahdeksan yksilöä, jotka olivat osallistuneet vakaviin rahanpesurikoksiin, joissa fiat-valuuttoja vaihdettiin kryptovaluutoiksi tarkoituksena piilottaa rahojen laiton alkuperä. Toimintaa varten oli perustettu peiteyritys, joka pyöritti muun muassa kahta kryptovaluutta-automaattia, joiden kautta käteistä rahaa muutettiin

[184] Ks. *Kimpimäki* 2015, s. 337.
[185] Ks. Europol: European union serious and organised crime threat assessment 2021, s. 28.
[186] Ks. *Levi* 2021.
[187] Ks. FATF: Professional Money Laundering 2018.
[188] Ks. Europol: European union serious and organised crime threat assessment 2021, s. 28–29.

kryptovaluutoiksi. Varoja hajautettiin useille reaalimaailman tileille, epäilyttävän suuren rahaliikenteen herättämän huomion välttämiseksi.[189]

EU-alueen rahanpesun torjuntaa koskeva lainsäädäntö on kehittynyt ja sen seurauksena esimerkiksi pankkisektorin valvontaa on voimistettu. Tämä on vaikeuttanut rikollisten verkostojen tuottojen siirtämistä lailliseen talouteen perinteisten pankkikanavien kautta, ja sitä myötä pakottanut rikolliset innovoimaan. Rahanpesu siirtyy enenevässä määrin sektoreille, joissa valvontaa on vähemmän ja rikolliset ovat alkaneet hyödyntämään toiminnassaan vaikeasti seurattavia pseudo-anonyymisiä kryptovaluuttoja.[190]

Kryptovaluuttojen rahanpesukäyttö on tehnyt rikoksen keinoin saatujen varojen löytämisestä ja palauttamisesta yhä vaikeampaa. Koska useimmiten rikosten taustalla on taloudellinen motiivi, on varojen takaisinperintä tehokas pelote rikollisuuden torjunnassa. Takaisinperinnällä riistetään rikollisilta heidän laittomalla toiminnallaan haltuun saamansa omaisuus, estetään varallisuuden uudelleeninvestointi tuleviin rikoksiin ja saadaan integroitua varat takaisin talouden valtavirtaan. Takaisinperintä on kuitenkin ollut EU-alueella hyvin epävarmaa ja arvioiden mukaan yli 98 % kaikkien rikosten tuotoista jää rikollisten haltuun.[191]

Seuraava esimerkki kuvaa konkreettisesti, miten kryptovaluuttoja voidaan käyttää rahanpesuun:

> A on saanut laittomista toimistaan käteistä rahaa. A laittaa rahat pankkiin sellaisessa maassa, jossa AML/CFT-lainsäädännöllä on matalat standardit. A haluaa vaihtaa rahansa kymmeneen Monero-polettiin (XMR), jotka tarjoavat korkean anonyymiyden tason. Näitä poletteja myydään kryptovaluuttapörsseissä, joten A luo käyttäjän yhteen tällaiseen palveluun. Pörssi antaa A:lle lompakon (julkinen avain ja yksityisavain). A voi nyt siirtää varansa kryptovaluuttapörssiin. Tässä vaiheessa A pystyy vaihtamaan fiat-valuuttansa bitcoineiksi. Nyt A luo käyttäjätilin toiseen kryptovaluuttapörssiin, joka antaa A:lle toisen lompakon. Tämän jälkeen A siirtää bitcoininsa tähän toiseen palveluun, jossa hän vaihtaa bitcoininsa Monero-poletteihin.
>
> A voisi vaihtaa Moneronsa takaisin käyväksi rahaksi seuraamalla edellä esitettyjä vaiheita käänteisessä järjestyksessä. Koska poletteja voi siirtää eri maiden ja eri lompakoiden välillä, A voi vaihtaa polettinsa takaisin fiat-valuuttaan missä tahansa maassa. Vaihtoehtoisesti A voi siirtää poletit jonkun toisen henkilön haltuun, joka sitten suorittaa vaihtotoimenpiteen. Saadakseen lisäsuojaa A voi myös käyttää kryptovaluuttasekoitin palveluita varojen sekoittamiseen. Näin A on pessyt laittomin keinoin hankitun varallisuuden.

[189] Ks. Europol: Cryptocurrency laundering as a service: members of a criminal organisation arrested in Spain 2019.
[190] Ks. Europol: European union serious and organised crime threat assessment 2021, s. 29.
[191] Ks. Europol: Does crime still pay? Criminal asset recovery in the EU 2016.

4.3. Terrorismin rahoittaminen ja kryptovaluutat

Huoli kryptovaluuttojen terroristisesta käytöstä on nostettu esiin EU:n viidennen rahanpesudirektiivin johdanto-osan 8 kappaleessa.

> ”8. Virtuaalivaluuttojen ja fiat-valuuttojen (eli jonkin maan lailliseksi maksuvälineeksi nimettyjen metallirahojen ja seteleiden sekä sähköisen rahan, joka on hyväksytty vaihdantavälineeksi liikkeeseenlaskumaassa) välisten vaihtopalvelujen ja lompakkopalvelujen tarjoajilla ei ole unionista johtuvaa velvollisuutta tunnistaa epäilyttävää toimintaa. Näin ollen terroristiryhmät saattavat pystyä siirtämään rahaa unionin rahoitusjärjestelmään tai virtuaalivaluuttaverkostoissa salaamalla siirrot tai hyödyntämällä näiden palvelujen tietynasteista anonyymiyttä. Sen vuoksi on olennaisen tärkeää laajentaa direktiivin (EU) 2015/849 soveltamisalaa niin, että se kattaa myös virtuaalivaluuttojen ja fiat-valuuttojen välisten vaihtopalvelujen ja lompakkopalvelujen tarjoajat. Toimivaltaisten viranomaisten olisi rahanpesun ja terrorismin rahoituksen torjuntaa varten voitava valvoa virtuaalivaluuttojen käyttöä ilmoitusvelvollisten kautta. Tällaisella valvonnalla saataisiin aikaan tasapuolinen ja oikeasuhteinen lähestymistapa, joka turvaisi vaihtoehtoisen rahoituksen ja yhteiskunnallisen yrittäjyyden alalla saavutetun teknisen kehityksen ja pitkälle viedyn avoimuuden.”

Suomen lainsäädännössä terrorismin rahoittaminen on rangaistavaa rikoslain 34 a luvun 5 §:n perusteella:

> ”Terrorismirikoksen rahoittaminen
>
> Joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan jotakin 1, 1 a, 2–4, 4 a–4 c, 5 c tai 5 d §:ssä tarkoitettua rikosta, on tuomittava *terrorismirikoksen rahoittamisesta* vankeuteen vähintään neljäksi kuukaudeksi ja enintään kahdeksaksi vuodeksi.”

& rikoslain 34 a luvun 5 a §:n perusteella:

> ”Terroristin rahoittaminen
>
> Joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan henkilöä, joka tekee 1 tai 1 a §:ssä tarkoitettuja rikoksia tai osallistuu niiden tekemiseen 5 luvun 3–6 §:ssä tarkoitettuna rikokseen osallisena, on tuomittava terroristin rahoittamisesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään kuudeksi vuodeksi.”

& rikoslain 34 a luvun 5 b §:n perusteella:

> ”Terroristiryhmän rahoittaminen
>
> Joka suoraan tai välillisesti antaa tai kerää varoja rahoittaakseen tai tietoisena siitä, että niillä rahoitetaan 6 §:n 2 momentissa tarkoitettua terroristiryhmää, on tuomittava terroristiryhmän rahoittamisesta vankeuteen vähintään neljäksi kuukaudeksi ja enintään kuudeksi vuodeksi.”

Suomessa on myös säädetty erikseen laki rahanpesun ja terrorismin rahoittamisen estämisestä. Kyseisen lain 1 luvun 2 §:ssä eritellään lain soveltamisalaa ja 8 a momentissa on viittaus virtuaalivaluutan tarjoajista annetussa laissa tarkoitettuun virtuaalivaluutan tarjoajaan.

Terrorismin rahoituksen torjumista koskeva kansainvälisen yleissopimuksen 18 artiklan 2 momentin a ja b kohdissa edellytetään, että:

> ”2. Sopimusvaltiot toimivat myös yhteistyössä 2 artiklassa tarkoitettujen rikosten ehkäisemiseksi harkitsemalla:
>
> a) kaikkien maksuja välittävien yhtiöiden valvontatoimenpiteitä, esimerkiksi toimintalupien vaatimista;
>
> b) toteutettavissa olevia toimenpiteitä havaitakseen tai valvoakseen konkreettista käteisvarojen ja haltijapapereiden kuljettamista rajojen yli, noudattaen tarkkoja tietojen asianmukaisen käytön varmistavia suojatoimenpiteitä ja haittaamatta millään tavalla pääoman vapaata liikkumista.”

Tämä ilmentää sitä, ettei epäilyttävän toiminnan seuraaminen ole yksin rahoituslaitosten vastuulla. Vastuun jakamisella pyritään ehkäisemään mahdollista korruptiota rahoituslaitoksissa.

Sekä terroristit että muut rikollisryhmät toimivat lain ulkopuolella ja molempien tavoitteena on pysyä lainvalvonnan ulottumattomissa. Terrorismin ja järjestäytyneen rikollisuuden ydinmotiivit kuitenkin poikkeavat toisistaan. Siinä missä järjestäytyneen rikollisryhmän toiminta perustuu taloudellisen voiton tavoitteluun, keskittyvät terroristit ennen kaikkea ideologisiin ja poliittisiin tavoitteisiinsa. Järjestäytynyttä rikollisuutta ja terroristeja yhdistää kuitenkin se, että molemmat ryhmät saavat resursseja samoja kanavia pitkin. Esimerkiksi kryptovaluuttoja saatetaan hyödyntää samaan tapaan terrorismin rahoittamisessa kuin niitä hyödynnetään osana järjestäytynyttä rikollisuutta.

Kryptovaluuttojen käytöstä osana terroristisen toiminnan rahoitusta on esitetty erisuuntaisia arvioita. Esimerkiksi vielä vuoden 2016 tammikuussa Europolin julkaisemassa raportissa “Changes in modus operandi of Islamic State terrorist attacks” todettiin, että ”kolmansien osapuolien ilmoittamista havainnoista huolimatta, kryptovaluuttojen, kuten Bitcoinin, käyttöä osana terroristista toimintaa eivät ole lainvalvontaviranomaiset varmistaneet”.[192] Euroopan pankkiviranomainen klassifioi tästä huolimatta kryptovaluuttojen käytön osana terroristista toimintaa korkean luokan uhaksi.[193]

Kryptovaluuttoja saatetaan käyttää terroristisolujen toiminnan rahoittamiseen. Tällaisten transaktioiden jäljittäminen on miltei mahdotonta, mikä näkyy esimerkiksi siinä, ettei aiemmin mainitussa Europolin raportissa voitu olla varmoja kryptovaluuttojen käytöstä, koska siitä ei ollut varmistettuja havaintoja. Lohkoketjulla liikkuu runsaasti pieniä transaktioita ja, kun pienen

[192] Ks. Europol: Changes in modus operandi of Islamic State terrorist attacks 2016, s. 7.
[193] Ks. EPV: Opinion on virtual currencies 2014, s. 33

terroristisolun kustannukset ovat verrattain matalat ei ole mitään mahdollisuuksia erottaa tällaista terroristiseen tarkoitukseen menevää transaktiota tavallisista transaktioista.[194] Silti todettuja tapauksia kryptovaluuttojen terroristisesta käytöstä on ollut esimerkiksi Indonesiassa, jossa islamistiset militantit lähettivät varoja terroristisoluille Bitcoin-muodossa. Itse transaktiota ei tuolloinkaan havaittu, mutta terroristit jäivät kiinni vaihtaessaan varoja käteiseksi.[195]

Valtioiden huoli kryptovaluuttojen käytöstä terroristisen toiminnan osana on hiljalleen nousussa. Esimerkiksi Yhdysvaltojen kongressissa tehtiin tammikuussa 2018 lakiesitys, jossa ehdotettiin riippumattoman rahoitusteknologian työryhmä Independent Financial Technology Task Forcen perustamista. Työryhmän tarkoituksena on priorisoida uuden finanssiteknologian, mukaan lukien kryptovaluuttojen, tutkimusta ja selvittää teknologian käyttöä osana terroristista toimintaa. Työryhmä myös palkitsee pidätyksiin johtavista tiedoista, jotka liittyvät kryptovaluuttojen terroristiseen käyttöön. Osana työryhmän toimintaa perustetaan myös FinTech-innovaatiorahasto, jonka tarkoituksena on rohkaista sellaisten teknologisten ratkaisujen kehittämistä, jotka ehkäisevät kryptovaluuttojen rikollista ja terroristista käyttöä.[196]

4.3.1. Terroristiryhmien rahoituskanavien laajentaminen kryptovaluutoilla

Terroristisen toiminnan yleisimpiä rahoituksen lähteitä ovat valtiotason sponsorit, erilaiset lahjoitukset, laiton toiminta (huumausainekauppa, salakuljetus, petokset, kiristys ja pikkurikollisuudesta saadut tulot) sekä lisäksi lailliset tulonlähteet (palkkatyö, lailliset yritykset sekä henkilökohtaiset tai luottopohjaiset lainat).[197] Terroristiryhmät valikoivat tulonlähteensä vaihtelevasti riippuen siitä, mikä tulonlähde on helpoimmin saatavilla. Tarpeet ja toimintatavat kehittyvät ajan myötä myös sen mukaan, miten lainvalvontaviranomaiset reagoivat terroristiryhmien toimintaan ja miten tehokkaasti viranomaiset kykenevät rahankeruukykyä rajoittamaan. Viranomaiset ajavat terroristit etsimään vaihtoehtoisia varainhankintamenetelmiä, mikä puolestaan johtaa viranomaisten tarpeeseen kehittää yhä uusia vastatoimenpiteitä. Kryptovaluutat ovat seuraava looginen askel tässä jatkumossa.[198]

Kryptovaluuttojen välityksellä saadut lahjoitukset eivät tiettävästi ole minkään yksittäisen terroristijärjestön pääasiallinen tulonlähde, vaan ne rahoittavat toimintaansa myös muilla tavoin:

---

[194] Ks. *Oftedal* 2015, s. 7.
[195] Ks. *Yuniar* Wall Street Journal 2017.
[196] Ks. U.S. House of Representatives, Financial Innovation and Defense Act, H.R. 4752 2018.
[197] Ks. *Oftedal* 2015.
[198] Ks. *Dion-Schwarz – Johnston – Manheim* 2019, s. 8.

veron keruulla hallinnoimiltaan alueilta, ryövättyä omaisuutta myymällä, öljyllä ja erilaisilla laittomilla tulonlähteillä. Jotkut terroristijärjestöt, kuten Hizbollah, nojaavat enenevässä määrin valtiotason avustuksiin, kun niiden laittomat tulonlähteet ovat tyrehtyneet.[199]

Kryptovaluutat voivat mahdollistaa uudestaan yhden vaikeaksi muodostuneen rahoituskeinon, nimittäin yksityishenkilöiden tekemät lahjoitukset. Vaikka vain hyvin pieni osa maailman muslimiväestöstä kannattaa äärimmäisiä ajattelutapoja, on niillä silti tarpeeksi kannatusta, ettei mahdollista yksityishenkilörahoitteista kryptovaluuttaliikennettä voida uhkana sivuuttaa. Perinteiset fiat-valuuttasiirrot ovat helposti jäljitettävissä ja muodostavat yksilölle suuren kiinnijäämisriskin. Tarpeeksi turvallisen, toimintavarman ja anonyymin kryptovaluutan käyttö saattaisi mitätöidä olemassa olevan yksilöön kohdistuvan kiinnijäämisriskin tai alentaisi sitä tarpeeksi merkittävästi, että yksityishenkilöiden tekemistä lahjoituksista muodostuisi jälleen merkittävä terroristisen toiminnan rahoitusmuoto.[200] Terroristijärjestöt, kuten Isisin propagandajaosto Ibn Taymiyaah[201] ja palestiinalainen militanttiryhmä Hamas[202], ovat keränneet kryptovaluuttalahjoituksia kannattajiltaan.

On todennäköistä, että terroristijärjestöt käyttävät kryptovaluuttoja myös tukemaan muita tulonlähteitään. Kuten aiemmin on esitetty, kryptovaluutat ja niin kutsuttu dark web kuuluvat nykyisin tiiviisti yhteen alamaailman kaupankäynnissä. Näin ollen kryptovaluutat saattavat kriittisellä tavalla mahdollistaa terroristiryhmien rahoitusta osana niiden harjoittamaa huumekauppaa ja muuta dark webissä harjoitettua laittoman tavaran myyntiä.[203]

Narkoterroristiset ryhmät eli terroristiryhmät, jotka harjoittavat myös laajaa huumekauppaa, muodostavat eräänlaisen väliportaan puhtaan terroristijärjestön ja järjestäytyneen rikollisuuden välillä. Tällaisella ryhmällä on sekä ideologisia, että taloudellisia motiiveja ja se on kytköksissä molempiin alamaailman sektoreihin. Kryptovaluutat ovat jo laajassa käytössä dark webin huumausainekaupassa, ja ne saattavat levitä narkoterroristisen ryhmien kautta vertikaalisesti osaksi perinteisempien terroristijärjestöjen toimintoja, joihin näillä ryhmillä on yhteyksiä.[204]

---

[199] Ks. *Levitt* The Washington Institute for Near East Policy 2016.
[200] Ks. *Dion-Schwarz – Johnston – Manheim* 2019, s. 9.
[201] Ks. *Carlisle* Rusi.org 2017.
[202] Ks. Al Jazeera 2019.
[203] Ks. *Dion-Schwarz – Johnston – Manheim* 2019, s. 10.
[204] Ks. *Baron ym.* 2015, s. 19–20.

4.3.2. Kryptovaluuttojen käyttö yksittäisten terrori-iskujen rahoittamisessa

Vaikka varsinaiset tunnetummat terroristijärjestöt ja niiden alajaostot eivät vielä hyödyntäisi kryptovaluuttoja laajamittaisesti, saattaa niiden käyttö edesauttaa niin sanottujen ”yksinäisten susien” toimintaa. Yksinäisellä sudella tarkoitetaan tyypillisesti henkilöä, joka on motivoitunut terroristijärjestön ideologiasta ja haluaa oma-aloitteisesti toteuttaa terrori-iskun. Tällainen henkilö ei ainakaan aluksi ole osa terroristiryhmän komentoketjua, mutta saattaa iskua valmistellessaan pyrkiä saamaan tarvikkeita tai ohjeita terroristijärjestöltä. Teknologinen kehitys tekee yksinäisten susien tunnistamisesta haastavampaa. On hyvin mahdollista, että näennäisesti yksin toiminut iskun tekijä on tosiasiassa koko prosessin ajan ollut yhteydessä terroristijärjestöön. Terroristijärjestö on organisoinut ja rahoittanut iskun, mutta anonyymien maksumenetelmien ansiosta tapauksen todellisen luonteen selvittämisestä tulee mahdotonta.[205]

Aiemmin todettiin, että kryptovaluuttojen välityksellä yksityishenkilöt voivat madaltuneen kiinnijäämisriskin myötä aiempaa helpommin lahjoittaa rahaa terroristijärjestöille. Tämä toimii kuitenkin myös toiseen suuntaan, sekä terroristisesti motivoituneiden yksilöiden kesken. Terroristijärjestö voisi kryptovaluuttojen avulla helposti rahoittaa yksittäisen iskuntekijän operaation tai tämä voisi saada varat iskun toteuttamiseen joukkorahoitustyyppisesti vertaisiltaan, jotka ovat motivoituneita rahoittamaan yksittäisen henkilön harjoittamaa terroristista toimintaa. Yksinäiset sudet saattavat usein saada tukea läheisiltään. Kryptovaluuttojen antaman anonymiteetin ansiosta nämä tahot lienevät aiempaa valmiimpia antamaan terrori-iskua suunnittelevalle henkilölle taloudellisen tukensa. Teknisen käytön esteiden madaltuessa kryptovaluuttojen käyttö leviää helpommin erilaisten terroristitahojen keskuuteen ja johtaa uusiin toimintatapoihin. Näennäisesti itsenäisten iskujen ohjaaminen ja valvonta terroristiryhmien taholta on mahdollisesti jatkossa helpompaa. Terroristiryhmät voivat maksaa tarvikkeista kryptovaluutoilla ja jopa tilata ne toimitettavaksi suoraan iskun tekijälle.[206]

[205] Ks. *Callimachi* New York Times 2017.
[206] Ibid.

4.3.3. Kryptovaluuttojen terroristisen käytön haasteet

Kryptovaluutat ovat yhä verrattain tuore keksintö ja niiden käytössä ja suosiossa on havaittavissa suurta vaihtelua. Puhuttaessa muista kryptovaluutoista kuin Bitcoinista käytetään yleisnimitystä ”alt-coins” eli vaihtoehtoiset kolikot.[207] Nämä ovat, kuten nimestä ilmenee, vaihtoehtoja alkuperäiselle lohkoketjuperustaiselle Bitcoinille. Näitä vaihtoehtoisia kryptovaluuttoja ilmentää erityisesti se, että ne kamppailevat keskenään suosiosta ja monet niistä ovat teknisiltä ominaisuuksiltaan hyvin samankaltaisia. Tämä samankaltaisuus ja kryptovaluuttojen suosion vaihtelu vaikeuttaa spekulatiivista sijoittamista, mutta myös laittomia käyttötarkoituksia, kuten käyttöä terrorismin rahoitukseen. Mikään kryptovaluutta ei ole ainakaan vielä noussut siinä määrin rikollisten suosikiksi, että sillä olisi laaja verkostovaikutus, joka tekisi siitä alamaailman transaktioiden standardin. Rikollisilla ei myöskään välttämättä ole tarpeeksi laajaa osaamista teknologian käytöstä. Maksuliikenteen hoitumiselle on välttämätöntä, että sekä lähettäjä- että vastaanottajataholla on teknistä osaamista.

Yksi kryptovaluuttojen suurimmista potentiaalisista käyttötarkoituksista terroristisessa toiminnassa on mahdollisuus rahoittaa terrori-iskuja nykyisiä fiat-valuuttoja tehokkaammin. On myös mahdollista, että terroristit käyttävät kryptovaluuttoja dark webin markkinapaikoilla suorien asehankintojen tekemiseen. Todennäköisempi toimintatapa, josta on myös olemassa havaintoja, on että terroristit vastanottavat rahasiirtoja kryptovaluuttana, jonka he myöhemmin muuttavat käteiseksi rahaksi, jolla varsinaiset terroristiselle toiminnalle keskeiset transaktiot hoidetaan.[208] Käteisen rahan suosiminen johtuu siitä, että terroristit toimivat usein alueilla, joilla internetyhteys on heikko ja näin ollen kryptovaluuttojen käyttö ei etäisimmillä alueilla onnistu.

On tärkeää muistaa, että varmennettuja tapauksia kryptovaluuttojen terroristisesta käytöstä on vain vähän.[209] Mahdollisuus käytön yleistymiselle on olemassa, mutta myös kryptovaluuttojen laajamittaista terroristista käyttöä vastaan puhuvia tekijöitä on useita. Terroristiryhmät toimivat usein syrjäisillä alueilla, joilla internetyhteyden kattavuus on heikko. Näin ollen kryptovaluuttoihin käsiksi pääsy ei ole kaikissa sijainneissa mahdollista. Tästä syystä kryptovaluutat on usein muutettava käteiseksi, jotta varoja voidaan hyödyntää missä ja milloin tahansa. Tähän liittyvä toinen ongelma on käteisnostoautomaattien vähäisyys. Kryptovaluutta-automaatit, joissa on käteisnosto-ominaisuus ovat länsimaissakin verrattain harvinaisia ja ovat vasta hiljalleen yleistymässä. Konkreettinen mahdollisuus tehdä tarvittuja käteisnostoja syrjäisillä alueilla

[207] Luvussa 2.4. käsitelty yksityisyysvaluutta Monero on hyvä esimerkki alt-coinista.
[208] Ks. *Aldridge* ym. 2017.
[209] Ks. *Carlisle – Keatinge – Keen* 2018, s. 9.

puuttuu täysin. Myös itse kryptovaluuttoihin liittyy turvallisuusuhkia, jotka saattavat johtaa varojen menetykseen. Tällainen uhka voisi olla esimerkiksi kysymys siitä kenellä on hallussaan yksityisavaimet ryhmän kryptovaluuttalompakkoon. Etenkin järjestäytyneiden rikollisryhmien keskuudessa on havaittu sisäisiä petoksia, joissa joku ryhmän jäsen on kavaltanut ryhmän varat itselleen. Kryptovaluutat ovat erityisen alttiita, kun ryhmän sisällä vallitsee epäluottamus ja erityisesti silloin, kun usealla taholla on pääsy yksityisavaimiin.

4.3.4. Kryptovaluuttapohjainen kyberrikollisuus ja terrorismi

Kryptovaluuttapohjainen kyberrikollisuus on varteenotettava vaihtoehto tietyille toimijoille, jotka pyrkivät aiheuttamaan laajamittaista häiriötä, muodostaen kuitenkin samalla mittavia tulovirtoja kryptovaluuttojen avulla. Tällaisiin toimijoihin lukeutuu muun muassa Pohjois-Korea, joka hankkii kyberrikollisuuden keinoin varoja selvitäkseen kansainvälisistä sanktioista. Pohjois-Korea oli esimerkiksi Iso-Britannian terveydenhuoltojärjestelmään kohdistetun WannaCry-lunnashaittaohjelman takana.[210]

Kryptovaluuttapohjainen kyberrikollisuus muodostaa todistetusti uuden kannattavan hyökkäysväylän terroristiryhmille ja jopa valtiotason toimijoille. Europolin vuonna 2017 julkaistussa raportissa kuitenkin todetaan, että vaikka terroristit käyttävät toiminnassaan internetiä ja netin kommunikaatioväyliä toimiensa koordinoimiseen ja propagandan levitykseen, on terroristiryhmien kyky toteuttaa kyberhyökkäyksiä ollut vielä toistaiseksi rajallinen.[211]

Ilmiö on kuitenkin saanut sen verran huomiota, että tietoverkoissa tapahtuvasta terrorismista on jo käytetty nimitystä ”kyber-jihad”. Sillä viitataan tilanteeseen, jossa kyberympäristö on oleellinen osa terroristien toimintaa ja terroristijärjestöt, kuten Isis muodostavat näin ollen aktiivisen kyberturvallisuusuhan työskentelemällä yhteistyössä erilaisten hakkeriryhmien kanssa.[212]

Hyvä esimerkki tämäntyyppisestä uudenlaisesta kyberterrorismista on vuoden 2015 elokuussa sattunut tapaus, jossa kosovolainen hakkeri Ardit Ferizi levitti haittaohjelmaa saadakseen haltuunsa Yhdysvaltojen hallinnon ja armeijan työntekijöiden henkilötietoja. Tiedot myytiin sitten Isisille, joka julkaisi niiden perusteella laaditun tappolistan.[213] Ferizi vaati myöhemmin

[210] Ks. BBC News 2017.
[211] Ks. Europol: IOCTA 2017, s. 52–54.
[212] Ks. *Ashok* International Business Times 2016.
[213] Ks. The Guardian 2016.

haittaohjelman poistamiseksi Bitcoin-muodossa suoritettavia lunnaita.[214] Tapaus osoittaa, että yksittäisillä terroristisilla toimijoilla on kyky hakkeroida tietokantoja ja hankkia sitä kautta arkaluonteisia tietoja. Vaikka monen terroristisen toimijan näkökulmasta häiriön aiheuttaminen ylittää taloudelliset motiivit, kuvaa Ferizin tapaus näiden motiivien yhteneväisyyttä.

Yleistyessään kyberrikollisuudesta voi kehittyä merkittävä terrorismin rahoituksen väylä. Tilannetta vaikeuttaa entisestään se, että kyberrikosten tekemisestä on tullut helpompaa. Halukkaat tahot voivat yksinkertaisesti palkata tarvitsemansa kyberrikollisuuden asiantuntijat, tai ostaa haittaohjelmia suoraan verkosta. Hyvänä esimerkkinä toimii haittaohjelmia kaupannut webstresser.org-sivusto, jonka Europol sulki huhtikuussa 2018. Sivusto hyväksyi kryptovaluuttamaksuja vastineeksi haittaohjelmista, joilla tehtiin finanssialan ja julkisen sektorin infrastruktuuriin kohdistettuja DDOS-hyökkäyksiä. Siinä missä aiemmin DDOS-hyökkäysten tekeminen vaati tietoteknistä osaamista, oli sivustolta hankituilla ohjelmistoilla mahdollista toteuttaa vakavia DDOS-hyökkäyksiä halvimmillaan noin 15 euron kuukausimaksulla.[215] Tulevaisuuden kannalta kehitys on huolestuttavaa, sillä kryptovaluutat mahdollistavat uudenlaisten kyberrikoksiin erikoistuneiden spesialistien toiminnan, jossa kyberrikollisuuden ammattilaiset fasilitoivat eri rikollisryhmien, kuten terroristien, toimintaa tarjoamalla edullisesti sellaisia palveluita, joihin ryhmillä ei välttämättä muussa tapauksessa riittäisi tietoteknistä osaamista. Rikollisryhmien tiivistynyt yhteistyö edellyttää myös valtioiden lainvalvontaviranomaisilta yhä tiiviimpää yhteistyötä.

4.3.5. Riskinä terroristien oman kryptovaluutan luominen

Puhuttaessa kryptovaluuttapohjaisesta kyberrikollisuudesta ja terrorismista, on pohdittava myös sitä mahdollisuutta, että terroristiryhmät ottaisivat käyttöön oman kryptovaluuttansa. Jopa valtiotasolta löytyy esimerkkejä, joissa jokin taho on yrittänyt keksiä ratkaisuja globaalin finanssijärjestelmän kiertämiseksi. Esimerkiksi Venezuela yritti joulukuussa 2017 torjua hyperinflaatiota lanseeraamalla oman petro-virtuaalivaluuttansa. Petro on öljyyn sidottu virtuaalivaluutta. Se on näennäisesti rakenteeltaan hyvin keskitetty eli siltä puuttuu kryptovaluutoille perinteisesti oleellinen hajautuneisuus. Näin ollen, on kyseenalaista, voidaanko sitä edes pitää kryptovaluuttana.[216] Silti pelkkä petron olemassaolo todistaa, että on olemassa tahoja, joilla on merkittävä intressi lisätä suvereeniuttaan omalla virtuaalivaluutalla.

---

[214] Ks. *Johnson* McClatchy DC Bureau 2016.
[215] Ks. Europol: World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down 2018.
[216] Ks. *Dedi* CryptoSlate 2017.

Vuonna 2015 tehdyssä arviossa todettiin riskin siitä, että joku valtiosta riippumaton toimija loisi oman kryptovaluuttansa, olevan matala.[217] On silti huomattava, kuten edellisessä luvussa käsitellystä havaitaan, että esimerkiksi terroristiryhmien ja kyberrikollisten toiminta on kryptovaluuttojen kautta lähentynyt toinen toistaan. Ei ole lainkaan epätodennäköistä, ettei tämän lähentymisen vuoksi terroristijärjestölle olisi mahdollista luoda omaa kryptovaluuttaa. Esimerkiksi Isis ilmoitti vuonna 2015 luoneensa oman fyysisen valuuttansa kultaisen dinaarin. Isis perusteli oman valuutan luomista tarpeella irtisanoutua ”amerikkalaisten orjuuttajien kapitalistisesta järjestelmästä”.[218]

Selkeä motiivi oman valuutan luomiseen on olemassa. Käytännössä preventiivinen keskitettyihin toimijoihin kohdistuva valvonta kuitenkin ehkäisee tehokkaasti terroristiryhmiä luomasta omaa kryptovaluuttaansa. Mikäli sellainen kuitenkin saataisiin luotua, ja sitä onnistuttaisiin ylläpitämään, täytyisi kansainvälisen yhteisön reagoida uhkaan nopeasti. Esimerkiksi Venezuelan tapauksessa Yhdysvallat kielsi kansalaisiaan käymästä kauppaa petrolla tai millään Venezuelan hallituksen kehittämällä vastaavalla ratkaisulla. Todennäköisin skenaario on kuitenkin, että terroristien tietoteknisten valmiuksien noustessa ryhmät siirtyvät käyttämään jo kehitettyjä avoimen lähdekoodin ratkaisuja.

4.4. Kryptovaluutat varkauden kohteena

Kryptovaluutat voivat olla myös rikosten kohteena.[219] Tällä viitataan yleensä erilaisiin kyberrikoksiin. Kyseiset rikokset edellyttävät korkeaa teknistä asiantuntemusta ja tuovat esiin kyberturvallisuuteen liittyviä ongelmia.[220] Kryptovaluuttoihin kohdistuvalla rikollisuudella voidaan tarkoittaa esimerkiksi lukuisia erilaisia hakkerointi-, varkaus- ja kavallustapauksia, joita on kohdistettu kryptovaluuttapörsseihin ja yksityishenkilöihin.

Varsin yleinen ja helposti toteutettava rikos on niin sanottu SIM-swap hyökkäys, joka toteutetaan käyttämällä rikollisen haltuun päätynyttä uhrin puhelinnumeroa tämän SIM-kortin deaktivoimiseen. Tämän jälkeen puhelinnumero siirretään rikollisen hallinnoimalle SIM-kortille. Rikollisilla on usein apunaan puhelinoperaattorilla työskentelevä sisäpiiriläinen, joka tekee tarvittavat tekniset toimenpiteet. Merkittävä SIM-swap hyökkäysten sarja tapahtui vuonna 2020, jolloin rikolliset ottivat kohteekseen erityisesti vaikutusvaltaisia julkisuuden henkilöitä.

[217] Ks. *Baron ym.* 2015.
[218] Ks. *Staufenberg* Independent 2015.
[219] Ks. Europol: European union serious and organised crime threat assessment 2021.
[220] Ks. *Chawki ym.* 2015, s. 6.

Hyökkäysten yhteydessä rikolliset usein vaihtavat uhrin salasanat ja tyhjentävät mahdolliset kryptovaluuttoja sisältävät heikosti suojatut[221] lompakot.[222] Rikolliset saattavat SIM-swap hyökkäyksen yhteydessä myös murtautua uhrin sosiaalisen median käyttäjätileille ja tehdä huijauspostauksia, joissa ihmisiä pyydetään lähettämään kryptovaluuttoja rikollisten hallinnoimiin osoitteisiin.[223]

4.5. Huumausaineiden kauppa, kryptovaluutat ja Silk Road

Huumausainerikoksista säädetään rikoslain 50 luvussa. Kryptovaluuttoja käytetään yleisesti maksuvälineenä huumausaineiden verkkokaupassa, joten ne liittyvät lähinnä 50 luvun 1 §:n 4 ja 5 momentteihin, joiden mukaan huumausainerikokseen syyllistyy se:

> ”Joka laittomasti
>
> 4) myy, välittää, toiselle luovuttaa tai muulla tavoin levittää tai yrittää levittää huumausainetta, tai
>
> 5) pitää hallussaan tai yrittää hankkia huumausainetta, on tuomittava *huumausainerikoksesta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.”

Salatussa Tor-verkossa tapahtuva huumausainekauppa on viime vuosina yleistynyt uusi ilmiö.[224] Silti merkittävä osa huumekaupasta on jo siirtynyt verkon salatuille kauppapaikoille dark webiin. Yksi laajimmista huumausaineiden nettimyynnin toimijoista oli helmikuussa 2011 perustettu ja Yhdysvaltojen viranomaisten lokakuussa 2013 sulkema Silk Road. Anonyymiys on dark webin käytön keskeisin ominaisuus. Jokaisella käyttäjällä (ostajilla ja myyjillä) on käyttäjänimi, jotta heidän todellinen henkilöllisyytensä pysyisi salattuna. Käyttäjät etsivät haluamiaan tietoja tai kauppatavaraa dark webin eri foorumeilta ja blogeista. Dark webissä asiointi on tehty käyttäjille hyvin helpoksi ja käyttökokemus muistuttaa aivan tavallista nettishoppailua. Verkkoliikenne anonymisoidaan Tor-verkon kautta ja maksuvälineenä käytetään vaikeasti jäljitettäviä kryptovaluuttoja, kuten Bitcoinia. Kommunikaatio hoituu PGP-salatun[225] sähköpostiviestinnän välityksellä, jonka kautta osapuolet saattavat hioa yksityiskohdat kuntoon ennen kaupantekoa.

---

[221] ”Heikosti suojatulla” viitataan tässä lompakkopalveluihin, jotka helppokäyttöisyyden vuoksi edellyttävät käyttäjältä kirjautumisen yhteydessä ainoastaan salasanaa ja sähköpostiosoitetta. SIM-swapin yhteydessä molemmat tiedot on helppo vaihtaa. SIM-swap hyökkäysten yleistymisen vuoksi esimerkiksi monet kryptovaluuttapörssit ovat kokonaan poistaneet kirjautumisvaihtoehdoista tekstiviestivarmennuksen, jota aiemmin pidettiin turvallisuutta lisäävänä ominaisuutena.
[222] Ks. Europol: Ten hackers arrested for string of sim-swapping attacks against celebrities 2021.
[223] Ks. *Frier – Mehrotra* Bloomberg News 2020.
[224] Ks. *Siro* 2017, s. 1–2.
[225] Ks. *Personaldatasecurity* 2014.

Nämä kolme päätekijää, Tor-verkko, kryptovaluutat ja viestinnän salaus, luovat teknologisen kivijalan, jonka päälle koko dark webin infrastruktuuri rakentuu.[226]

Teknologinen kehitys on johtanut totaaliseen paradigman muutokseen. Huumekauppiaiden kannalta katsottuna moni vanha riskitekijä on poistunut kokonaan tai vähintään madaltunut. Myyjätahon ei tarvitse esimerkiksi enää mennä tapaamaan asiakkaita henkilökohtaisesti, vaan paketit toimitetaan helposti postitse asiakkaan ilmoittamaan osoitteeseen. Kun henkilökohtaisia kohtaamisia ei tarvita ei ole myöskään riskiä siitä, että jompikumpi osapuoli kävisi fyysisesti toisen kimppuun tai, että virkavalta väijyttäisi osapuolet kaupan hetkellä. Etänä toimimisen hyötynä on myös, ettei osapuolten tarvitse luottaa toisiinsa, sillä kryptovaluuttatransaktiot voidaan ohjelmoida niin, että maksusuoritus ei saavu myyjälle ennen kuin toimitus on perillä.[227]

Silk Road muistutti eBayn kaltaista perinteistä verkkokauppaa. Erona perinteisiin verkkokauppoihin on kuitenkin se, että Silk Roadin kaltaisilla kauppapaikoilla, missä transaktiot hoidetaan kryptovaluutoilla ei niitä voi peruuttaa. Kryptovaluutan saapuminen myyjälle voidaan estää, mikäli kaupatun tuotteen toimituksessa menee jokin pieleen, mutta lohkoketjutransaktioiden lopullisuudesta johtuen suoritetun summan palauttaminen ostajalle ei ole mahdollista. Huumekauppiailla ei luonnollisesti ole tuotteille palautusosoitetta.[228] Silk Roadin tapauksessa Yhdysvaltojen oikeusministeriö takavarikoi tuhansia bitcoineja, joiden taloudellinen arvo on huomattavan suuri.[229]

[226] Ks. *Hardy – Norgaard* 2016.
[227] Ibid. s. 515–539.
[228] Ibid.
[229] Ks. *Rooney* CNBC 2020.

4.6. Kryptovaluuttoihin liittyviä oikeudellisia erityiskysymyksiä

4.6.1. Kryptovaluuttojen vaikutus näyttökysymysten arviointiin – tapaus KKO:2018:3

Kryptovaluuttojen ja anonyymien verkkojen kuten Tor-verkon käyttö ovat aiheuttaneet konkreettisen näytön puutteen rikosprosessissa. Tapauksessa KKO:2018:3 on kyse tilanteesta, jossa tosiasiallisen rikoksentekijän selvittäminen on osoittautunut näytön arviointia koskevien seikkojen takia erittäin vaikeaksi. Kuten tutkielmassa on aiemmin esitetty, kryptovaluuttojen tekniset ominaisuudet yhdessä anonymiteetin mahdollistavien sovellusten, kuten Tor-verkon kanssa laskevat huomattavasti huumausainekaupan ja muun rikollisuuden kiinnijäämisriskiä. Tapaus on omiaan vaikuttamaan ennakkotapauksena tulevaan oikeuskäytäntöön ja siihen, millaista näyttöä huumausainerikoksissa vaaditaan, jotta syyllisyydestä ei jää varteenotettavaa epäilystä.

> ”Tapauksessa A:ta syytettiin huumausainerikoksesta. Syytettä perusteltiin sillä, että A oli tuonut postitse maahan 10 grammaa 99-painoprosenttista amfetamiinia. Kirjelähetys oli saapunut postissa ulkomailta A:n nimellä ja kotiosoitteella. A kiisti tilanneensa lähetystä tai tietävänsä siitä mitään. Syytteen mukaan aine oli sen määrä ja pitoisuus huomioon ottaen ainakin osittain tarkoitettu levitykseen tai oli ainakin olemassa suuri vaara, että aine päätyisi myös muiden kuin A:n käyttöön.
>
> Käräjäoikeus oli alun perin hylännyt syytteen katsoen, että A:n syyllisyydestä oli jäänyt varteenotettava epäily. Vaikka väitettä siitä, että joku muu olisi A:n tietämättä tilannut postilähetyksen tämän osoitteeseen pidettiin epäuskottavana, oli A kuitenkin omalla uskottavaksi katsottavalla kertomuksellaan riittävästi kyennyt horjuttamaan näyttöä, jota syytteen tueksi oli esitetty. Käräjäoikeus katsoi, ettei syytteen tueksi ollut esitetty riittävää näyttöä.
>
> Hovioikeus kumosi käräjäoikeuden tuomion ja tuomitsi A:n syytteen mukaisesta huumausainerikoksesta neljän kuukauden ehdolliseen vankeusrangaistukseen. Hovioikeuden mukaan A:n kertomus ei ollut kyennyt horjuttamaan lähtökohtaista olettamaa siitä, ettei kukaan tilaisi toisen henkilön nimellä ja osoitteella huumausainetta tämän tietämättä. Hovioikeus tuomitsi A:n syytteen mukaisesta huumausainerikoksesta neljän kuukauden ehdolliseen vankeusrangaistukseen.
>
> A:lle myönnettiin valituslupa korkeimpaan oikeuteen, joka lopulta kumosi tuomion ja hylkäsi syytteen huumausainerikoksesta. Korkein oikeus päätyi perusteluissaan siihen johtopäätökseen, että syyte on perustunut postilähetyksen vastaanottajatietoihin ja niiden merkittävään näyttöarvoon lähetyksen tilaajasta. Asiassa esitetty todistelu on vain niukasti tukenut muuta syytettä tukevaa näyttöä. A:n kertomuksen uskottavuudesta lausuttu huomioon ottaen korkein oikeus katsoo, etteivät syytteen tueksi esitetyt todisteet ja muut asian käsittelyssä esiin tulleet syytettä tukevat seikat riitä sulkemaan pois varteenotettavaa epäilyä siitä, ettei A ole laittomasti tuonut maahan kysymyksessä olevaa huumausainetta. Tämän vuoksi syyte on hylättävä.”

Korkeimman oikeuden perusteluissa mainitaan, ettei huumausaineiden postitilauksissa yleisesti hyödynnettyjen niin sanottujen virtuaalivaluuttojen käytöstä ole jutussa esitetty näyttöä. Tämä on merkittävää siitä syystä, että etenkin yhdessä Tor-verkon kaltaisten salausmekanismien

kanssa kryptovaluutoilla käydyssä huumausainekaupassa on mahdollista saavuttaa täydellinen tai ainakin lähes täydellinen transaktioiden anonymiteetti. Verkossa tapahtuvassa huumausainekaupassa anonymiteetin takaavia keinoja on useita ja niillä voidaan tehokkaasti laskea kiinnijäämisriskiä ja kuten tässä tapauksessa, pienentää mahdollisten todisteiden määrää ja siten vaikeuttaa huumausainerikoksen tutkintaa.[230]

Huumausainerikoksissa esiintyvää näyttöä on verrattu oikeuskirjallisuudessa muun muassa kokoamattoman palapelin paloihin, jotka eivät yksinään osoita mitään, mutta kokonaisuutena tarkasteltuna niistä paljastuu mistä jutussa on todella kyse.[231] Kryptovaluuttojen ja Tor-laudan tapaisten sovellusten käyttö tekee osasta palasia vaikeasti löydettäviä ja niiden etsimisestä kallista.

4.6.2. Todistustaakka, tarkoituksenmukaisuus ja esitutkinnan rajoittaminen

Rikosasiassa todistustaakka on kantajalla eli syyttäjällä tai asianomistajalla. Tämä ilmenee oikeudenkäymiskaaren 17 luvun 1 §:n 2 momentista, jossa ilmaistaan, että ”rikosasiassa kantajan tulee näyttää toteen ne seikat, joihin hänen vaatimuksensa nojautuu”.[232] Syyttäjän todistustaakka on rikosprosessioikeudessa poikkeukseton. Kantajan ensisijainen näyttövelvollisuus johtuu jo asian luonteesta. Olisi nimittäin yleiseltä kannalta paljon vahingollisempaa langettaa väärä syylliseksi julistava tuomio, kuin virheellinen vapauttava tuomio.[233] Syyttäjän laaja riski todistelussa perustuu siihenkin, että muussa tapauksessa kansalaisten turvallisuudentunne järkkyisi, mikäli olisi mahdollista tulla kevyin perustein tuomituksi jostakin, mitä ei voida selvästi todistaa. Todistustaakan jako perustuukin prosessilajin erityisluonteeseen ja siitä oikeusturvatarpeisiin.[234] Sama ajatus toistuu myös uudemmassa oikeuskirjallisuudessa. Syyttömien suojaaminen on oikeusvaltiossa keskeinen arvo, mitä rikosprosessioikeuden todistustaakkanormi ilmentää. Tämä arvopohja ylittää konkreettisesti rikosten selvittämisintressin.[235] Ihmisoikeuksien julistuksen 8–11 artiklat liittyvät oikeudenmukaiseen oikeudenkäyntiin ja mielivaltaisen pidätyksen kieltoon. 11 artiklassa säädetään, että:

> ”1. Jokaisen rikollisesta teosta syytteessä olevan henkilön edellytetään olevan syytön siihen asti kunnes hänen syyllisyytensä on laillisesti todistettu julkisessa oikeudenkäynnissä, jossa hänelle turvataan kaikki hänen puolustustaan varten tarpeelliset takeet. 2. Ketään

[230] Ks. *EMCDDA – Europol* 2017.
[231] Ks. *Metsäpelto* 2005.
[232] Ks. Sahavirta 2006, s. 225.
[233] Ks. *Tirkkonen* 1972, s. 149–154.
[234] Ks. *Halila* 1955, s. 87–88.
[235] Ks. *Pölönen* 2003, s. 133.

> ei pidä tuomita rangaistavaksi teoista tai laiminlyönneistä, jotka eivät kansallisen tai kansainvälisen oikeuden mukaan olleet rikollisia tekohetkellä. Myöskään ei pidä tuomita ankarampaan rangaistukseen, kuin mikä oli sovellettavissa rangaistavan teon suoritushetkellä."

Syyttäjällä on todistustaakkaan perustuva suuri vastuu näyttää toteen, että tapauksessa syytetty on oikeasti syyllistynyt väitettyyn tekoon. Näin vankka periaatepohja muodostuu konkreettiseksi esteeksi tuomitsemiselle tapauksissa, joissa tarvittavaa näyttöä on esimerkiksi teknisillä keinoilla saavutetun anonymiteetin takia mahdotonta tai vaikeaa selvittää tarpeeksi kattavasti, jotta syytetty voitaisiin osoittaa edellytetyllä varmuudella syylliseksi. Se, että näytön hankkiminen on vaikeaa tai lähes mahdotonta ei saa vaikuttaa näyttökynnykseen.

Vastapainona syyttäjän esittämälle tapahtumankululle oikeus arvioi useita mahdollisia vaihtoehtoisia tapahtumienkulkuja, joista myös syytetyllä on mahdollisuus esittää näkemyksensä. Syytettä vastaan puhuvat seikat otetaan huomioon samoin kuin sen puolesta puhuvat seikat. Asian käsittelyssä esiin tulleiden seikkojen perusteella arvioidaan, mikäli vaihtoehtoinen tapahtumienkulku on mahdollinen ja siinä määrin todennäköinen, ettei sen olemassaoloa voida sulkea riittävällä varmuudella pois. Näin sovelletaan yleisiä kokemussääntöjä ja tarkastellaan vaihtoehtoisia tapahtumankulkuja osana näytön harkintaa. Rikosasioiden näyttökynnyksestä on säädetty oikeudenkäymiskaaren 17 luvun 3 §:n 2 momentissa, jonka mukaan "tuomion, jossa vastaaja tuomitaan syylliseksi, edellytyksenä on, ettei vastaajan syyllisyydestä jää varteenotettavaa epäilyä". Rikosasioiden arvioinnissa lähtökohtana on aina syyttömyysolettama.[236]

Konkreettisen näytön puuttuminen ylitti tapauksessa nekin seikat, että syytetty myönsi käyttäneensä aiemmin Tor-lautaa ja polttaneensa kannabista. Aikaisempi käyttö osoittaa, että syytetty osaa käyttää Tor-verkkoa ja tekee todennäköiseksi sen, että syytetty saattaa jatkossakin käyttää huumausaineita. Anonyymien verkkojen käyttö ja kryptovaluutat luovat siis huumausainerikosten ehkäisylle ja selvittämiselle selkeän ongelmakohdan. Rikosten havaitseminen on vaikeaa, koska dark webin kaupankäyntiä on Tor-verkon vuoksi teknisesti vaikea jäljittää. Toiseksi, kuten tapauksesta KKO 2018:3 havaittiin, syytteen ajaminen menestyksekkäästi vaikeutuu, sillä kryptovaluutoilla suoritetut transaktiot on nykyään helppo häivyttää näkymättömiin, mikä puolestaan lisää näyttöongelmia. Viime aikoina on havaittu näyttökynnyksen madaltumista huumausainerikoksissa, mikä näkyy siinä, että puuttuvaa yksiselitteistä näyttöä on vaikeaa hankkia, joten sitä on täydennetty näytön kokonaisarvioinnilla. Korkeimman oikeuden kanta näyttökynnyksen alenemista kohtaan on kuitenkin ollut kriittinen. Se on tapauksessa KKO 2017:12

[236] Ks. *Siro* 2017, s. 226.

todennut, ettei huumausainerikosten näyttökynnys saa olla muita rikoksia alempi välittömän ja yksiselitteisen näytön hankkimiseen liittyvistä vaikeuksista huolimatta. Teknisistä seikoista johtuvat näyttövaikeudet eivät saisi johtaa näyttökynnyksen alentamiseen, vaan syyte on epäselvissä tapauksissa hylättävä.[237]

Rikosprosessin tarkoituksenmukaisuus edellyttää, että keinot rikoksen selvittämisintressi suhteutetaan rikoksen vakavuuteen. Tarkoituksenmukaisuusperiaatteen mukaan tavoitteena on, että oikeudenkäynnit olisivat varmoja, nopeita ja halpoja. Nämä tekijät ovat prosessitavoitteita, tavoiteltavan prosessin ominaisuuksia. Lainsäätäjän ja lainkäyttäjän tehtävänä on prosessitavoitteiden yhteensovittaminen. Prosessitavoitteet ovat suhteessa toisiinsa sinänsä paradoksaalisia, etteivät ne kaikki voi käytännössä toteutua samanaikaisesti.[238] Etusija annetaan yleensä varmuustavoitteelle, kuten ilmenee hallituksen esityksestä HE 15/1990 vp:

> ”Menettelyn ulkoista kulkua järjestettäessä pyritään ainoastaan luomaan mahdollisimman hyvät takeet aineellisesti oikean ratkaisun saavuttamiselle. Lisäksi menettelyä järjestettäessä on pyrittävä tyydyttämään ainakin kaksi muuta vaatimusta. Näistä ensimmäinen on se, että ratkaisu asiassa on tehtävä niin nopeasti kuin se oikeusturvallisuutta vaarantamatta on mahdollista. Tämä vaatimus koskee kaikkia asioita. Toinen vaatimus koskee menettelyn kustannuksia. Menettely tulisi järjestää sellaiseksi, ettei siitä aiheudu suhteettoman suuria kustannuksia.”

Rikollisella on nykypäivänä käytössään tekniset keinot tehdä kryptovaluuttojen ja salausverkkojen avulla näytön hankkimisesta niin työlästä ja niin runsaasti resursseja vaativaa, että rikoksen selvittämisen kustannukset olisivat suhteettoman suuret. Näin ollen osa huumausainerikollisuudesta ei etene prosessiekonomisista syistä tuomioistuinkäsittelyyn asti, kun esitutkinnassa ei pystytä löytämään riittävää näyttöä.

Esitutkinnan rajoittamisen normiperusta tulee esitutkintalain 4 §:n 3 momentista, jossa säädetään, että:

> ”Syyttäjä voi tutkinnanjohtajan esityksestä määrätä, ettei esitutkintaa toimiteta tai että se lopetetaan, jos hän oikeudenkäynnistä rikosasioissa annetun lain (689/1997) 1 luvun 7 tai 8 §:n taikka muun vastaavan lainkohdan nojalla tulisi jättämään syytteen nostamatta eikä tärkeä yleinen tai yksityinen etu vaadi syytteen nostamista.”

Neljännessä momentissa säädetään, että:

> ”Syyttäjä voi tutkinnanjohtajan esityksestä määrätä, että esitutkinta lopetetaan, jos tutkinnan jatkamisesta aiheutuvat kustannukset olisivat selvässä epäsuhteessa tutkittavana olevan asian laatuun ja siitä mahdollisesti odotettavaan seuraamukseen, taikka jos jo suoritettujen esitutkintatoimenpiteiden perusteella on varsin todennäköistä, että syyttäjä tulisi jättämään syytteen nostamatta muulla kuin 3 momentissa mainitulla perusteella.

[237] Ibid. s. 226.
[238] Ks. *Vuorenpää* 2009, s. 61–64.

> Esitutkinnan lopettaminen edellyttää lisäksi, ettei tärkeä yleinen tai yksityinen etu vaadi esitutkinnan jatkamista. Esitutkinta on kuitenkin aloitettava uudelleen, jos siihen asiassa ilmenneiden uusien seikkojen vuoksi on perusteltua syytä."

Neljännen momentin alkuosaan sisältyy puhtaasti kustannusperusteinen rajoittaminen ilman normatiivista yhteyttä syyttämättä jättämiseen ja sen muualla laissa säädettyihin perusteisiin. Säännös muodostaa eräänlaisen rikosprosessiekonomisen suhteellisuusperiaatteen ja peilaa julkisen sektorin yhä kustannustietoisempaa ajattelutapaa.[239]

Lähetyksen postittaminen tiettyyn osoitteeseen antaa aiheen epäilylle, mutta kuten tapauksessa KKO 2018:3 havaittiin, sekään ei yksinään riitä osoittamaan syyllisyyttä, vaan muodostaa ainoastaan osan sitä kokonaiskuvaa, joka tapauksesta tulee muodostaa, ettei syyllisyydestä jää varteenotettavaa epäilyä. Vastaavanlaiset tapaukset tulevat merkittävästi yleistymään ja erityisesti vähäisten huumausainerikosten kohdalla esitutkintatoimenpiteitä tullaan rajoittamaan, kun kustannukset ylittävät vähäisten rikosten selvittämisintressin.

4.7. Rikoshyödyn hallussa pitäminen

Rikoslain kätkemis- ja rahanpesurikoksia koskeva 32 luvun 6 §:n 1 momentin 1 kohdassa olevan ryhtymistekotapaluettelon viimeisenä mainittu tekotapa on rikoshyödyn hallussa pitäminen. Suomessa hallussapidon rangaistavuus on sidottu ensisijaisesti tarkoitustahallisuuteen. Rikosoikeudellinen vastuu rikoshyödyn hallussapidon perusteella edellyttää Suomessa esimerkiksi rahanpesurikoksissa rahanpesuaktiksi luokiteltavaa intentiota, kuten pyrkimystä peittää tai häivyttää rikoshyödyn alkuperä.[240]

Esimerkiksi henkilön pitäessä hallussaan bitcoineja, jotka hän on ostanut kryptovaluuttapörssistä tarkoitustahallisuuden puuttuessa, ei kyse voi olla rikoshyödyn hallussa pitämisestä. Vastakkainen tulkinta olisi mahdoton myös siihen nähden, että bitcoinien rahallinen arvo oli kehityksen alkuvaiheessa hyvin pieni ja laittomien käyttötarkoitusten osa transaktioista hyvin suuri. Kun huomioidaan myös, että louhinta oli alussa nopeampaa, tarkoittaa tämä sitä, että hyvin suurella osaa tänä päivänä markkinoilla kiertävistä bitcoineista on laittomiin tarkoituksiin liittyvää transaktiohistoriaa.

---

[239] Ks. *Nissinen* 2007, s. 55.
[240] *Hyttinen* 2021, s. 309.

Myös hyvin lyhytaikainen rikoshyödyn hallussapito voidaan kuitenkin luokitella rikoshyödyn hallussapidoksi. Myös muut kuin rikoshyödyn fyysiset hallintatilanteet, voidaan luokitella rikoshyödyn hallussapidoksi.[241] Esimerkiksi kryptovaluuttojen salausavainten hallussapito voi täyttää hallussapidon tunnusmerkistötekijän riippumatta salausavainten sijainnista.[242] Käytännössä voi olla kuitenkin hyvin haastavaa selvittää onko henkilöllä salausavaimia hallussaan, sillä salausavainten talletusvaihtoehtoja on useita. Tämä on näkynyt viime vuosina siinä, että viranomaisten seuraamilta[243] tileiltä on onnistuneesti siirretty varoja ilman, että viranomaisilla on mitään mahdollisuutta tietää, kuka siirron käytännössä teki.

4.8. Menettämisseuraamukset

Rikoshyödyn menettämisestä säädetään menettämisseuraamuksia käsittelevässä rikoslain 10 luvussa. Menettämisseuraamuksella eli konfiskaatiolla tarkoitetaan rikosoikeudessa lakiin perustuvaa omaisuuden korvauksetonta menettämistä rikoksen tekemisen seuraamuksena valtiolle.[244] Menettämisseuraamusta ei lueta rangaistukseksi, vaikka menettämisseuraamus perustuu rikokseen ja sillä voi olla sekä yleis- että erityisestävää merkitystä. Kyse on turvaamistoimesta, jonka tarkoituksena on rikosten tekemisen ehkäiseminen tai rikoksesta hyötymisen ehkäiseminen.[245]

Kryptovaluuttojen konfiskaatioon liittyy erityisiä haasteita, mutta tästä huolimatta esimerkiksi Suomen tulli on vuosien aikana onnistunut takavarikoimaan merkittävän määrän bitcoineja. Yksi merkittävä takavarikko toteutettiin 2020 joulukuussa, kun Suomen tulli takavarikoi Sipulimarket-verkkopalvelimen ja bitcoineja.[246] Kryptovaluutat ovat luonteeltaan hajautettuja, niillä ei ole tiettyä keskitettyä hallinnoijaa, eivätkä ne ole fyysisesti olemassa. Kaikki nämä seikat nostavat esiin haasteita lainvalvontaviranomaisille ja oikeuslaitokselle. Kuitenkin jo vuoden 2014 kesäkuussa YK:n huumeiden ja rikollisuuden torjunnasta vastaava toimisto (UNODC) julkaisi perusoppaan virtuaalivaluuttojen avulla pestyn rikoshyödyn selvittämiseksi.[247]

Pseudo-anonyymisyydestä johtuen kryptovaluutat aiheuttavat helposti hyödyn määrään liittyvää epäselvyyttä. Rikoslain 10 luvun 2 §:n 2 momentin mukaan, jos hyödyn määrästä ei ole

[241] HE 285/2010 vp, s. 14.
[242] Ks. *Hyttinen* 2021, s. 309.
[243] Ks. *Criddle* BBC News 2020.
[244] HE 80/2000 vp, s. 4.
[245] Ks. *Siro* 2017, s. 159.
[246] Ks. Tulli 2020.
[247] Ks. UNODC: Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies 2014.

saatavissa selvitystä tai se on vain vaikeuksin esitettävissä, hyöty on arvioitava ottaen huomioon rikoksen laatu, rikollisen toiminnan laajuus ja muut olosuhteet.

Tämän tutkielman katsannossa keskeisimmät rikosmuodot: huumausainerikokset, rahanpesu- ja terrorismin rahoittaminen ovat selkeässä yhteydessä myös rikoslain 10 luvun 3 §:n 1 momentin 1–4 ja 6 kohtiin:

> ”Laajennettu hyödyn menettäminen
>
> Jos on tehty
>
> 1) rikos, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;
>
> 2) kätkemisrikos tai rahanpesu;
>
> 3) salakuljetus;
>
> 4) huumausainerikos tai huumausainerikoksen edistäminen;
>
> 6) järjestäytyneen rikollisryhmän toimintaan osallistuminen;”

Nämä rikostyypit kattavat suurimman osan kryptovaluuttoihin liittyvästä rikollisuudesta, joten laajennettu hyödyn menettäminen tulee usein kyseeseen. Kryptovaluutat voivat olla myös rikoslain 10 luvun 4 §:n 2 momentin 1 kohdan mukainen ”esine tai omaisuus, jota on käytetty tahallisen rikoksen tekemisessä”.

Kryptovaluuttojen konfiskaatio ilman kohteena olevan tahon yhteistyötä tai jonkinlaista yksityisavainten hallinnoinnissa tapahtunutta virhettä on käytännössä mahdotonta. Yksityisavaimet ovat yleensä ainoa keino päästä käsiksi kryptovaluuttoihin.[248] Vaikka viranomaiset tietäisivät mikä krypto-osoite kuuluu menettämisseuraamuksen kohteena olevalle taholle, ei sen hallinnointi onnistu ilman yksityisavaimia. Varhaisessa vaiheessa bitcoinien säilyttäminen tietokoneen kovalevyllä oli yleistä. Tällöin pääsy varoihin edellytti myös kovalevyllä sijaitsevan lompakkotiedoston hallinnointia. Tällaisissa tapauksissa konfiskaatiossa saadaan vähintäänkin estettyä kohdetta pääsemästä käsiksi varoihinsa, sillä niillä on fyysinen tallennuskohde. Kätkemistapauksissa olennaista onkin, onko tekijällä mahdollisuus päästä myöhemmin hyötymään omaisuudesta.[249] Kryptovaluuttojen kohdalla tämä hyötymismahdollisuus on erittäin todennäköinen. Kätkemistapauksissa kyseeseen tulee arvon menettämistä koskeva rikoslain 10 luvun 8 §.

> ”Arvon menettäminen

---

[248] Kryptovaluuttapörssien tapauksessa palveluntarjoaja hallinnoi yksityisavaimia ja käyttäjä pääsee varoihinsa käsiksi kirjautumalla sisään kyseessä olevan palveluntarjoajan palveluun. Tällaisissa tilanteissa lainvalvontaviranomaisten on helpompaa tehdä yhteistyötä itse palveluntarjoajan kanssa ja jäädyttää käyttäjätili.
[249] HE 80/2000 vp, s. 32.

> Jos 4 tai 5 §:ssä tarkoitettua esinettä tai omaisuutta ei voida tuomita menetetyksi 6 §:n 1 momentissa säädetyn rajoituksen vuoksi tai siksi, että esine tai omaisuus on kätketty tai sitä ei muutoin tavoiteta, rikoksentekijä, rikokseen osallinen ja se, jonka puolesta tai suostumuksin rikos on tehty, voidaan tuomita esineen tai omaisuuden sijasta menettämään kokonaan tai osaksi sen arvo. Arvon menettämiseen voidaan tuomita myös se, jolle esine tai omaisuus on siirretty, jos hän sen vastaanottaessaan on tiennyt sen liittymisestä rikokseen tai hänellä on ollut perusteltu syy sitä epäillä taikka hän on saanut sen lahjana tai muuten vastikkeetta."

Kätketyn omaisuuden arvon määrittäminen voi kuitenkin olla hyvin hankalaa. Kätketyn omaisuuden tarkka määrä ei ole välttämättä tiedossa tai omaisuus voi olla hajautettuna useille eri tileille, joista osa ei ole lainvalvontaviranomaisten tiedossa.

5. MITEN KRYPTOVALUUTTOJA TULISI SÄÄNNELLÄ?

5.1. Eri valtioiden lainsäätäjien suhtautumistavat

Lainsäätäjillä on ollut vaikeuksia löytää sopivia keinoja säännellä kryptovaluuttoja, sillä ne poikkeavat niin perusteellisella tavalla perinteisestä finanssijärjestelmästä. Rahanpesun ja terrorismin rahoittamisen riski sekä suuri mahdollisuus muuhun rikolliseen käyttöön, ovat kuitenkin luoneet akuutin tarpeen lainsäädännölle.

Yleisin ensiasteen toimenpide johon valtiot ovat ryhtyneet suhteessa kryptovaluuttoihin on, että ne ovat varoittaneet kansalaisiaan kryptovaluuttojen käyttöön liittyvistä riskeistä. Nämä varoitukset ovat yleensä keskuspankkien antamia ja vetoavat kryptovaluuttojen arvonvaihteluun, rajalliseen hyväksyntään maksuvälineenä ja niiden laittomiin käyttömuotoihin sekä riskiin rikoksen kohteeksi joutumisesta.[250]

Valtiot ovat reagoineet kryptovaluuttoihin vaihtelevasti ja jotkut maat ovat olleet kryptovaluuttoja kohtaan suotuisampia kuin toiset. Osa on omaksunut tiukkoja säännöksiä ja joissakin maissa kryptovaluuttoja koskee täyskielto. Esimerkiksi Kiina on taas viime aikoina kohdistanut tiukkoja rajoitustoimenpiteitä kryptovaluuttojen käyttöä ja louhintaa kohtaan.[251] Rajoitustoimenpiteiden uskottavuutta tai pysyvyyttä voitaneen kuitenkin epäillä, sillä Kiina on jo aiemmin useaan otteeseen eri tavoilla ilmaissut kieltävänsä Bitcoinin louhinnan tai kryptovaluuttojen käytön.

Poliittisesta näkökulmasta kryptovaluuttojen täyskielto Kiinassa olisi kuitenkin ymmärrettävä. Kiinan poliittinen rakenne on nimittäin jo perusluonteeltaan ristiriidassa kryptovaluuttojen lähtökohtien, kuten hajautuneisuuden kanssa. Kiinassa valta on hyvin keskitetysti kommunistisella puolueella, joten hajautetut valuutat tarkoittaisivat, että osa valtiontalouden tuotoista pääsisi vuotamaan kommunistisen puolueen ulottumattomiin. Kiinalla on myös vakaa pyrkimys luoda oma digitaalinen keskuspankkivaluuttansa (Central Bank Digital Currency)[252]. Kiinan tekemän ilmoituksen jälkeen myös Iran ilmoitti kryptovaluuttojen louhinnan kiellosta.[253] Vaikuttaisikin siltä, että valtiot, jotka ovat yleisesti ottaen totalitäärisempiä suhtautuvat kryptovaluuttoihin kriittisemmin. Keskittyneelle vallalle hajautettu innovaatio muodostaa merkittävän uhan.

---

[250] Ks. UNODC: Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies 2014, s. 55.
[251] Ks. Kiinan valtioneuvoston rahoitusvakaus- ja kehityskomitean lausunto.
[252] Ks. *Seth* Investopedia 2021.
CBDC:itä käsitellään jäljempänä luvussa 5.4.
[253] Ks. *Sykes* Bloomberg 2021.

Niillä lainsäädäntöalueilla, joilla kryptovaluuttojen käyttöä tai louhintaa ei ole kielletty, mutta kryptovaluuttoja on kuitenkin haluttu säännellä, on sääntely kohdistettu kryptovaluuttapörsseihin. Kryptovaluuttapörssit tarjoavat asiakkailleen mahdollisuuden fiat-valuuttojen vaihtamisen kryptovaluuttoihin ja toisinpäin. Pörsseihin on kohdistettu asiakkaan tuntemisen sääntöjä, joiden avulla on pyritty ehkäisemään kryptovaluuttojen mahdollistaman anonyymiyden riskejä. Valtiot kuten Australia ja Kanada ovat säätäneet rahanpesun ja terrorismin rahoituksen torjumiseen keskittyviä lakeja, joilla pyritään helpottamaan lainmukaista ja valvottua kaupankäyntiä lakia noudattavissa kryptovaluuttapörsseissä ja rahoituslaitoksissa.[254] Myös EU:ssa on säännelty keskitettyjä vaihdantapaikkoja, kuten kolmannessa luvussa tuotiin esiin.

Hyvin hiljattain 9.6.2021 El Salvadorista tuli ensimmäinen maa, jossa Bitcoin on virallisen valuutan asemassa ja bitcoineja ostetaan valtion reservivarantoihin. Bitcoinista tuli samalla pääomatuloverovapaata.[255] Aika näyttää mikä vaikutus tällä tulee olemaan maailmanlaajuisesti, mutta jo ensimmäisen kuukauden aikana El Salvadorin sääntelytoimista, useat Etelä-Amerikan ja Afrikan valtiot osoittivat kiinnostusta vastaavaa ratkaisua kohtaan. Järjestelmän legitimoiminen ja laajempi käyttöönotto luo selkeämmän lähtökohdan hajautetun teknologian sääntelyyn.

5.2. Lohkoketjuteknologian hyödyt on syytä huomioida

On tärkeää muistaa, että itse lohkoketjuteknologia, johon kryptovaluuttojen toiminta perustuu, on mullistava keksintö, jolla voi tulevaisuudessa olla runsaasti reaalimaailman käyttötarkoituksia. Lainvalvonnan näkökulmasta vastuumekanismien olemassaolo alan toimijoille on olennainen keino estää kryptovaluuttojen laitonta käyttöä.[256] On kuitenkin tärkeää, että lainsäädäntötoimet ovat oikeasuhteisia, etteivät ne tukahduta teknistä innovaatiota.

Lohkoketjuteknologiaa on hyödynnetty useilla legitiimeillä aloilla, mukaan lukien liiketaloudessa ja julkisella sektorilla. Lohkoketjuteknologiaa on kaavailtu hyödynnettävän myös IT-turvallisuuden alalla suojamekanismina lunnasohjelmia vastaan. Ajatuksena on, että lohkoketjun avulla arkaluonteisia tietoja voidaan tallentaa hajautetusti nykyisen keskitetyn tallentamisen sijaan. Tietojen tallentaminen hajautetusti vaikeuttaa tietojen linkittämistä tiettyyn henkilöön, joten rikollisten on vaikeampi tietää keneltä lunnaita tulisi vaatia. Lisäksi tiedoista on hajautetussa järjestelmässä useita kopioita, joten rikollisten on vaikeaa pitää niitä kaikkia panttivankina.

[254] Ks. The Law Library of Congress: Regulation of Cryptocurrency around the World 2018.
[255] Ks. BBC News 2021.
[256] Ks. *Chohan* 2018b, s. 3.

Lohkoketjuteknologialla toimivaan hajautettuun järjestelmään kohdistuvat hyökkäykset pystytään myös havaitsemaan nopeammin ja ne ovat helposti tunnistettavissa.[257]

Kenties paras esimerkki lohkoketjuteknologian hyödyllisyydestä on Kiina. Se suhtautuu hyvin ankarasti kryptovaluuttoihin ja kryptovaluuttapörsseihin, mutta hyödyntää kuitenkin lohkoketjuteknologiaa. Siellä lohkoketjua hyödynnetään veropetosten torjuntaan osana Tencentin ja Shenzhenin kansallisen verotoimiston välistä yhteistyötä.[258] Koska itse teknologia ei siis ole pohjimmiltaan rikollisille suunnattua, on lainsäädäntötyössä olennaista keskittyä kryptovaluuttojen rikollisen käytön estämiseen.

5.3. Vertailukohteena Saksa – vastatoimien kehittäminen kansallisesti

Kryptovaluuttojen välityksellä tehtäviin rikoksiin liittyy useita niiden selvittämistä vaikeuttavia tekijöitä. Rikokset eivät yleensä tapahdu paikallisesti vaan, kuten kyberympäristössä tapahtuville rikoksille on yleistä, rikoksentekijä voi sijaita lähes missä tahansa. Tämä edellyttää eri valtioiden viranomaisilta yhteistyötä kansainvälisellä tasolla. Käytännössä kansainvälisen yhteistyön ongelmana on kuitenkin se, etteivät valtiot ole omaksuneet yhdenmukaista suhtautumistapaa kryptovaluuttoihin, vaan esimerkiksi FATF:n suosituksia noudatetaan hyvin erilaisessa laajuudessa eri lainkäyttöalueilla.

Mielenkiintoinen näkökulma virtuaalimaailman rikollisuuteen tulee Saksan oikeudellisesta doktriinista. Saksan järjestelmässä nimittäin nähdään, että kaikkia virtuaalimaailman rikollisia toimijoita yhdistää tarve olla yhteydessä reaalimaailmaan.[259] Tämä näkökanta on auttanut Saksan lainvalvontaviranomaisia rikosten selvittämisessä muita valtioita tehokkaammin. Lisäksi Saksassa lainvalvontaviranomaiset ovat jo varhaisessa vaiheessa alkaneet hyödyntää IT-alan asiantuntijoiden osaamista kyberrikosten selvittämiseksi.[260]

Saksassa kyberrikollisuus kattaa kaikki rikokset, jotka kohdistuvat internetiin, tietojärjestelmien lisädataverkkoihin tai niiden tietoihin kansallisen määritelmän mukaisesti. Kyberrikollisuus kattaa myös informaatioteknologian avulla tehdyt rikokset.[261] Saksassa lainvalvontaviranomaiset soveltavat hyvin laajaa kyberrikollisuuden käsitettä, joka kattaa laajan joukon rikoksia. Tästä

[257] Ks. *McConville* IBM 2017.
[258] Ks. *Sundararajan* Coindesk 2018.
[259] Ks. *Accorsi – Brenig – Müller* 2015, s. 753–759.
[260] Ks. Ministerium des Inneren 2021.
[261] Ks. Cybercrime und Digitale Spuren Jahresbericht 2016.

huolimatta Saksassa törmätään siltä osin samaan ongelmaan kuin muuallakin. Uusia rikosmuotoja ilmaantuu nopeammin kuin lainsäätäjä ehtii niihin reagoimaan.

Saksan liittovaltionpoliisi (Bundeskriminalamt) julkaisi vuonna 2017 raportin, joka käsitteli kyberrikollisuuden tilaa Saksassa.[262] Raportti käsittelee myös kryptovaluuttoja koskevaa rikollisuutta ja etenkin haittaohjelmia, jotka käyttäjän huomaamatta käyttävät tietokoneen resursseja kryptovaluuttojen louhintaan. Nykyään tällaisen haittaohjelman ei tarvitse edes asentua suoraan tietokoneelle, vaan tietokoneen resursseja hyödyntävät skriptit voivat olla verkkosivun osana. Esimerkiksi käyttäjän katsellessa lähetyksiä laittomasta suoratoistopalvelusta hänen tietokoneensa resursseja käytetään samanaikaisesti kryptovaluuttojen louhintaan, niin kauan kuin kyseisen palvelun käyttö jatkuu ja verkkosivulla oleva skripti voi jatkaa toimintaansa.

Ongelma tämänkaltaisen toiminnan kvalifioinnissa rikokseksi on, että näin toimiva ohjelma ei varsinaisesti vahingoita järjestelmän eheyttä, vaan ainoastaan lisää sen resurssien käyttöä. Skripti pysähtyy heti käyttäjän sulkiessa verkkosivun tai selaimen, eikä näin ollen vahingoita järjestelmää. Saksan rikoslain 27 luvun 303 a § kohdistaa rikosvastuun tekoihin, joilla ”laittomasti poistetaan, tukahdutetaan, tehdään käyttökelvottomaksi tai muokataan käyttäjien tietoja”. Jotta edellä kuvatun kaltainen skripti täyttäisi 303 a §:n asettamat kriteerit, pitäisi siitä jäädä järjestelmään pysyvä jälki, joka ylläpitää yhteyden palvelimeen, jolta skripti on peräisin.

Kemptenin käräjäoikeus Baijerissa päätyi 27.7.2017 käsitellyssä tapauksessa tulokseen, että 303 a §:ssa mainittu ”tietojen muuttaminen” tapahtuu milloin tahansa, kun loukkauksen myötä tietoja muutetaan. Merkitystä ei ole sillä, onko muutos negatiivinen vai positiivinen. Keskeistä on ainoastaan se, että järjestelmän tilaan on tullut muutos. Käyttäjällä on samalla velvollisuus puolustautua tällaisia muutoksia aiheuttavia uhkia kohtaan esimerkiksi palomuurilla.[263]

Saksassa omaksuttujen käytäntöjen ja tulkintojen valossa voidaan todeta, että rikoslain muuttamiseksi on olemassa erilaisia vaihtoehtoisia lähestymistapoja. Ensinnäkin kryptovaluuttoihin liittyvää rikollisuutta voidaan säännellä olemassa olevien rikoslaissa määriteltyjen kriminalisointien kautta. Toisena vaihtoehtona on uusien kryptovaluuttoihin soveltuvien kriminalisointien perustaminen ja määrittely. Kolmantena vaihtoehtona on omaksua rikoslain erityiseen osaan kryptovaluuttoihin liittyviä normeja, jotka selkeyttävät niihin liittyvien rikosten tulkintaa koskevia käytäntöjä.

[262] Ks. Bundeslagebild Cybercrime 2017.
[263] Ks. Kemptenin (Baijeri) alioikeuden ratkaisu asiassa BGH 1 StR 412/16–27.7.2017 (LG Kempten).

Saksan oikeustilaa tarkastelemalla huomataan, että yksittäisen valtion on mahdollista olla proaktiivinen suhteessa teknologisen kehityksen mukanaan tuomiin haasteisiin. Suomen olisi syytä olla proaktiivisempi suhteessa kryptovaluuttojen luomiin uhkiin. Suomen olisi mahdollista toteuttaa tehokkaampaa kansallista valvontaa ryhtymällä AMLD5:ttä pidemmälle meneviin lainsäädäntötoimiin, jotka noudattaisivat paremmin FATF:n suosituksia. Yksittäisen valtion toimivalta on loppujen lopuksi aina rajallista, minkä vuoksi tarvitaan merkittäviä panostuksia kansainväliseen yhteistyöhön, mutta proaktiivisuus on hyvä tapa turvata omia kansallisia intressejä lyhyellä aikavälillä ja luoda kehityspaineita EU:n suuntaan.

FATF:n suorittamassa maa-arviossa vuosien 2018–2019 aikana Suomen keskeisenä heikkoutena nostettiin esiin valvontatoiminnan riittämätön riskiperusteisuus. Syynä mainittiin valvojien rajallinen riskituntemus valvottavista aloista yhdistettynä huomattavaan resurssien alimitoitukseen vastuisiin ja työmäärään nähden. Suomi voisi ottaa mallia Saksasta ja laajentaa lainvalvonnan resursseja riittävälle tasolle.[264]

5.4. Keskuspankin digitaalinen valuutta – ratkaisu rahanpesuun?

Kryptovaluuttojen ja lohkoketjuteknologian kasvava suosio ovat saaneet useat keskuspankit kiinnostumaan teknologian mahdollisuuksista, ja monet niistä ovat tutkineet tapoja hyödyntää lohkoketjuteknologiaa keskuspankkien omien digitaalisten valuuttojen luomiseen perinteisten setelien ja kolikoiden korvikkeeksi.[265] Suunnitelmat digitaalisten valuuttojen käyttöönottamiseksi ovat vielä pitkälti teoreettisella tasolla.[266] Keskuspankkien digitaalisen valuutan projekteista käytetään yleisesti lyhennettä CBDC[267]. Kyse on yksinkertaisesti keskuspankin liikkeeseen laskemasta digitaalisesta maksuvälineestä.[268] Kryptovaluutat ja CBDC:t ovat molemmat digitaalisia valuuttoja, mutta siihen yhteneväisyydet pitkälti loppuvatkin. Siinä missä kryptovaluutat ovat luonteeltaan yksityisiä, hajautettuja ja niiltä puuttuu keskitetty vastuutaho, ovat CBDC:t julkisia ja keskitettyjä.[269]

Teoreettisesta näkökulmasta käteisvarojen korvaaminen julkisella ja jäljitettävällä CBDC:llä voisi olla toimiva ratkaisu useiden eri rikosten, kuten rahanpesun torjumiseen. Mikäli kaikki

[264] HE 261/2020 vp s. 3.
[265] Ks. OMFIF & IBM: Retail CBDCs 2019, s. 35.
Ks. myös *Bindseil* 2019, s. 2.
[266] Ks. *Barontini – Holden* 2019, s. 11.
[267] Eng. ”Central Bank Digital Currency”.
[268] Ks. OMFIF & IBM: Retail CBDCs 2019, s. 2 ja 9.
[269] Ks. *Barontini – Holden* 2019, s. 3.
Keskuspankin digitaalisen valuutan ei tarvitse perustua samaan teknologiaan kuin kryptovaluutat.

transaktiotiedot olisivat välittömästi lainvalvontaviranomaisten saatavilla tai ainakin helposti haettavissa, monet rikollisten toimijoiden operaatiot muuttuisivat mahdottomiksi. Näin täydellisen kontrollin toteuttamiseen liittyy kuitenkin haasteita. On nimittäin hyvin epätodennäköistä, että käteistransaktiot loppuisivat ainakaan lähiaikoina täysin. Ihmiset tuskin myöskään suostuisivat siihen, että valtio tarkkailee kansalaistensa jokaista maksusuoritusta. Ihmiset eivät halua luopua yksityisyydestään siinä määrin, että keskuspankeilla ja valtion viranomaisilla on pääsy kaikkiin yksilön tekemiin maksusuorituksiin. Näin ollen sellaisen yhteiskunnan luominen, jossa käteismaksuja ei käytetä lainkaan ja valtio seuraa kaikkea maksuliikennettä on poliittisesta näkökulmasta katsottuna lähes utopiaa. Etenkään läntisissä demokratioissa näin laajamittainen CBDC:n käyttöönotto tuskin onnistuisi. CBDC:n laajempi käyttö voisi onnistua esimerkiksi Kiinan kaltaisessa autoritäärisessä valtiossa, jossa digitaalisen yuanin kehitys on jo pitkällä.[270]

5.5. Rikollisuuden demokratiateoria ja nykyisen sääntelyn riittämättömyys

Rikollisuuden demokratiateoreettisesta näkökulmasta voidaan sanoa, että toimivien demokratioiden kohdalla rahanpesuun, kuten mihin tahansa muuhunkin rikollisuuteen, reagoidaan aina oikealla tavalla. Tämä johtuu siitä, että mikäli reagointi olisi liian ankaraa, löyhää tai kallista kansalaiset voivat äänestää valtaan uudet päättäjät, jotka ovat valmiita madaltamaan rikollisuuden kontrollin kustannuksia tai panostamaan enemmän rikollisuuden ehkäisemiseen.[271] Sääntelytoimet vastaavat siis periaatteessa aina kansan tahtoa. Tästä näkökulmasta voidaan tehdä johtopäätös, että mikäli kryptovaluutoista muodostuu merkittävä ihmisten elämää helpottava innovaatio, on todennäköistä, että ihmiset äänestävät valtaan sellaisia henkilöitä, jotka suhtautuvat kryptovaluuttoihin realistisesti ja äänestävät ulos liian ankaria toimia ehdottavat päättäjät.

Demokratiateoreettinen näkökulma voidaan kuitenkin myös kyseenalaistaa. Ihmisten äänestyspäätöksiin vaikuttaa moni muukin tekijä kuin rikollisuuden kontrolloiminen ja tästä aiheutuvat kustannukset. Demokratiateoreettinen malli ei myöskään sovellu kansalaisille vieraampiin rikostyyppeihin, jotka herättävät vähemmän tunteita. Esimerkiksi vaaleissa käyty keskustelu seksuaalirikoksista ja niiden rangaistuskäytännöstä vaikuttaa todennäköisesti enemmän kansalaisten äänestyspäätöksiin kuin keskustelu rahanpesusta ja sen kontrollista.[272] Tämä vertaus voidaan ulottaa osin myös kryptovaluuttoihin. Ne ovat verrattain tuore ilmiö, eivätkä ne ole vielä saavuttaneet laajaa suosiota. Tästä johtuen niitä koskevaa sääntelykeskustelua dominoivat

[270] Ks. *Kharpal* CNBC 2021.
[271] Ks. *Hyttinen – Tapani – Tolvanen* 2019, s. 42–43.
[272] Ks. *Hyttinen* 2021, s. 103.

sellaisten tahojen näkökannat, joita kryptovaluutat uhkaavat eniten. Tällä viitataan perinteisiin keskitettyihin rahoituslaitoksiin, jotka ovat hajautettujen kryptovaluuttojen suora kilpailija. Toistaiseksi tämä saattaa johtaa perustelemattoman ankaraan suhtautumiseen, kun vallanpitäjät keskittyvät luomaan kryptovaluuttojen haittoja estävää preventiivistä sääntelyä.

Haasteita aiheuttaa myös se, että kansainvälisellä tasolla eri maiden kansalaisilla ja päättäjillä saattaa olla hyvinkin erilaisia näkemyksiä siitä millainen lainsäädäntö on järkevää. Esimerkiksi puutteellinen rahanpesusääntely saattaa olla jollekin valtiolle tai alueelle taloudellisesti hyödyllinen seikka. Tällaisia valtioita on erityisesti kehitysmaiden joukossa, jolloin rikollisen toiminnan lieveilmiöt kohdistuvat yleensä näistä valtioista ulospäin muihin valtioihin, eivätkä niinkään aiheuta vakavia ongelmia lähdevaltiossa.[273] Koska kryptovaluutat uhkaavat erityisesti perinteistä finanssijärjestelmää, on loogista, että valtiot, joiden asema perinteisessä kansainvälisessä finanssijärjestelmässä on heikko ovat myötämielisiä uudelle häiriötä aiheuttavalle innovaatiolle. Tällaisia valtioita ovat esimerkiksi Väli-Amerikassa sijaitsevat Costa Rica ja El Salvador, jotka pyrkivät myötämielisellä lainsäädännöllä houkuttelemaan maihinsa kryptovaluutta-alan investointeja.

Joidenkin rikostyyppien, kuten esimerkiksi rahanpesun kontrollointi ja siitä aiheutuvat kustannukset perustuvat kansainvälisiin sopimuksiin ja oikeudellisiin instrumentteihin, joista tinkiminen on Suomen kaltaiselle pienelle valtiolle vaikeaa. Suomi on sitoutunut tiettyihin rikosoikeudellisiin toimiin, jotka on toteutettava päättäjien intresseistä riippumatta. Kansainvälistaustaisten rikosoikeudellisten säännösten legitimiteetti on demokratian toteutumisen näkökulmasta totuttua ohuempaa. Merkittävämpi ongelma liittyy siihen, että ylikansallinen kriminaalipolitiikka voi johtaa tilanteeseen, jossa rikostorjunnan kustannukset ylittävät rikoksen torjunnasta saatavat hyödyt.[274] Kryptovaluuttojen kohdalla tämä ongelma on erityisen ilmeinen huumausainerikoksien yhteydessä. Näyttökynnystä ei saa madaltaa, mutta näytön etsiminen on joissain tapauksissa kryptovaluuttojen anonymisoivien ominaisuuksien vuoksi mahdotonta.

Esimerkiksi rahanpesun preventiivisen sääntelyn kohdalla selkeänä pyrkimyksenä on rahanpesun ennalta estäminen, paljastaminen ja selvittäminen. Tämä on johtanut tilanteeseen, jossa rahanpesun torjuntaan käytetään merkittävästi aikaa ja voimavaroja, mutta preventiivisen sääntelyn lisäämisen hyödyllisyydestä ei voida olla varmoja. Preventiivinen sääntely johtaa uusiin tekomuotoihin, joita voimassa oleva preventiivinen sääntely ei tavoita. Sääntelyn legitiimiyden vuoksi tarvitaan jatkuvasti yhä uusia preventiivisiä sääntelyn muotoja, jotka käytännössä

[273] Ks. *Sahavirta* 2008, s. 61.
[274] Ibid, s. 103–104.

synnyttävät uusia rahanpesun muotoja, jotka jälleen edellyttävät uutta preventiivistä lainsäädäntöä ja niin edelleen.[275]

Hyttinen viittaa esimerkkinä virtuaalivaluuttojen rahanpesukäyttöön. Pankit velvoitettiin puuttumaan rahanpesuun tarkemmin ja seurauksena rahanpesijät siirtyivät käyttämään virtuaalivaluuttoja. Myös virtuaalivaluutan tarjoajat sidottiin vuonna 2019 rahanpesun preventiiviseen sääntelyyn. Hyttisen mukaan, mikäli sääntely tehoaa virtuaalivaluuttarahanpesuun, rahanpeseminen saa jälleen uusia muotoja.[276]

Myös viidennen rahanpesudirektiivin johdanto-osan 9 kappaleessa todetaan tämä ongelma:

> ”Virtuaalivaluuttojen anonyymiys mahdollistaa niiden väärinkäytön rikollisiin tarkoituksiin. Virtuaalivaluuttojen ja fiat-valuuttojen välisten vaihtopalvelujen ja lompakkopalvelujen tarjoajien sisällyttäminen direktiivin soveltamisalaan ei ratkaise kokonaisuudessaan virtuaalivaluuttojen avulla toteutettujen liiketoimien anonyymiyteen liittyvää ongelmaa, sillä suuri osa virtuaalivaluuttojen toimintaympäristöstä pysyy edelleen anonyyminä sen vuoksi, että käyttäjät voivat toteuttaa liiketoimia myös ilman tällaisia tarjoajia. Anonyymiyteen liittyvien riskien torjumiseksi kansallisten rahanpesun selvittelykeskusten olisi voitava hankkia tietoja, joiden avulla ne voivat yhdistää virtuaalivaluuttojen verkko-osoitteet virtuaalivaluutan omistajan henkilöllisyyteen. Lisäksi olisi selvitettävä tarkemmin mahdollisuutta antaa käyttäjien tehdä vapaaehtoinen ilmoitus nimetyille viranomaisille.”

Kuten 9 kohdassa todettiin, uusi direktiivi ei ratkaise ongelmia kokonaisuudessaan, sillä suuri osa virtuaalivaluuttojen toimintaympäristöstä pysyy edelleen anonyyminä, koska käyttäjät voivat yksinkertaisesti käyttää laittomiin tarkoituksiinsa hajautettuja pörssejä keskitettyjen pörssien sijaan. Keskitetyt virtuaalivaluutan tarjoajat ovat vain osa koko ekosysteemiä. Jotta kryptovaluuttojen laittomaan käyttöön voidaan tehokkaasti ja kestävällä tavalla puuttua, on kehitettävä uusia ratkaisuja preventiivisen ja keskitetyn sääntelyn lisäksi. Vaihtoehtoisia sääntelytapoja tutkitaan seuraavassa osiossa.

[275] Ibid, s. 104.
[276] Ibid. s. 104.

5.6. Vaihtoehtoinen sääntelytapa – laillisen ja laittoman käytön erottaminen toisistaan konsensustasolla

Muun muassa Yhdysvaltain valtiovarainministeriö[277] ja Euroopan keskuspankki[278] ovat kiinnittäneet huomiota kryptovaluuttojen rikolliseen käyttöön ja korostaneet uuden digitaalisen talouden sääntelytarvetta. Kun sääntelytarve lisääntyy, mutta perinteisien sääntelyratkaisujen teho heikkenee, on omaksuttava uudenlainen lähestymistapa. Keskitettyjen toimijoiden ohella sääntely on kohdistettava itse teknologiaan. Laittoman käytön ongelman ratkaisuksi on esitetty muun muassa Bitcoinin käytössä lohkoketjuun konsensustasolla tehtäviä muutoksia, jotta ainoastaan lailliset transaktiot vahvistettaisiin. Tällä tavoin pystyttäisiin konkreettisesti estämään laittomien transaktioiden tekeminen. Teoriassa näin pystyttäisiin alentamaan huomattavan korkeita kustannuksia, joita viranomaisilta kuluu esimerkiksi huumausainerikosten selvittämiseen, kun epäilyttäviä transaktioita ei pystyisi ylipäätään suorittamaan. Käytännön tasolla näiden tarvittavien muutosten tekemiseen liittyy joitakin merkittäviä haasteita.

Lohkoketjujärjestelmät ovat rakenteeltaan nelikerroksisia. Alhaalta ylös kuvattuna ne ovat verkostokerros (network layer), konsensuskerros (consensus layer), älysopimuskerros (smart contract layer) ja sovelluskerros (application layer).[279] Konsensusalgoritmit ovat mekanismeja yhteisymmärryksen eli konsensuksen saavuttamiseksi. Niiden avulla saadaan tieto siitä, missä tilassa kukin lohkoketjun muuttuja on tietyllä hetkellä. Näin ollen konsensusmekanismi mahdollistaa järjestelmän toiminnan, epärehellisistä toimijoista huolimatta.[280] Bitcoin-lohkoketju käyttää niin sanottua Proof of Work- eli PoW-konsensusalgoritmia verkon toiminnan varmistamiseen. PoW-konsensusalgoritmin toiminta perustuu verkon osanottajien suorittaman laskennan määrään sidottuna siihen käytettyyn aikaan, mikä puolestaan luo yhteisymmärryksen siitä, mitkä transaktiot lisätään missäkin järjestyksessä Bitcoin-tilikirjaan.[281]

Toinen yleisesti käytetty konsensusalgoritmi on Proof of Stake eli PoS-konsensusalgoritmi. PoS poikkeaa PoW:sta tavassa, jolla verkon osapuolten yhteisymmärrys muodostuu. Eri konsensusalgoritmeihin perustuvilla lohkoketjuilla on toisistaan eroavia ominaisuuksia ja tästä aiheutuu se, että eri käyttökohteisiin parhaiten soveltuva konsensusalgoritmi voi vaihdella.[282] PoS-konsensusalgoritmista on tulossa valtavirtaa, ja esimerkiksi toiseksi suurin PoW-lohkoketju,

[277] Ks. *Helms* Bitcoin News 2021b.
[278] Ks. *Helms* Bitcoin News 2021a.
[279] Ks. *Hoang ym.* 2019.
[280] Ks. *Johansson ym.* 2019, s. 62.
[281] Ibid, s. 62.
[282] Ibid, s. 63.

Ethereum, on vaihtamassa PoS-konsensusalgoritmiin. Vaihdos tekee 51 prosentin hyökkäyksistä Ethereumia vastaan lähes mahdottomia toteuttaa.[283]

On arvioitu, että ainakin Bitcoin-lohkoketjulla suoritetaan runsaasti vahvistettuja laittomia transaktioita, ja asianmukaisia sääntelymekanismeja on pantava täytäntöön, jotta kryptovaluuttojen laillinen käyttö pystyttäisiin selkeästi erottamaan niiden laittomasta käytöstä. Yksi mahdollinen keino luoda sääntelykehys kryptovaluutoille olisi kohdistaa sääntely lohkoketjun transaktoreihin ja konsensusalgoritmin toimeenpanijoihin. Konsensustasolla tapahtuvaa sääntelyä voisi toteuttaa lisensoimalla lohkoketjun konsensusalgoritmin toimeenpanijat, joiden vastuulla on lisätä todistettavasti lailliset transaktiot lohkoihin ja suorittaa konsensusalgoritmia näillä laillisten transaktioiden lohkoilla.[284]

Ongelmaksi esimerkiksi Bitcoin-lohkoketjun konsensusalgoritmin muokkauksessa kuitenkin muodostuu, että olisi vaikeaa saada tarpeeksi lohkoketjun jäseniä hyväksymään konsensusalgoritmiin tehtävät tarpeelliset muutokset. Konsensus perustuu louhintaan ja verkkoon kuuluvia louhijoita on ympäri maailmaa. Laajat Bitcoin-louhintaa harjoittavat yritykset Yhdysvalloissa ja Kiinassa muodostavat hyvin suuren osan Bitcoin-verkon laskentatehosta. Toisaalta ei sovi myöskään unohtaa pienempiä yksilötason toimijoita. Tähän louhijoiden hajautuneisuuteen peilaten olisi poliittisesta näkökulmasta lähes mahdotonta saada tarpeeksi laskentatehoa muutoksen taakse. On esitetty matemaattisia arvioita siitä, että sääntelyviranomaisen olisi saatava lisensoitua yli 58 % kaikista konsensusresursseista, jotta koko verkko saataisiin suorittamaan konsensusalgoritmia vain laillisten transaktioiden lohkoilla.[285]

Tähän päivään mennessä yhtäkään olemassa olevaa lohkoketjuprotokollaa ei ole suunniteltu siltä pohjalta, että sääntely tapahtuisi konsensustasolla. Tämä lisää lainsäätäjien skeptisyyttä lohkoketjuprotokollien omaksumista kohtaan sellaisenaan. Sääntelyä ei ole toteutettu osana protokollaa, vaan teknologia on yritetty sovittaa perinteiseen lainsäädäntökehykseen, mikä taas on osoittautunut tehottomaksi ja aiheuttaa jatkuvasti suuria valvontakustannuksia (esimerkiksi huumausainerikosten selvittämisen vaikeus ja siihen liittyvät korkeat kustannukset).

---

[283] 51 prosentin hyökkäys vaatii kyseisen määrän verkon laskentatehosta. PoS-verkossa ei ole louhijoiden ylläpitämää laskentatehoa, ja verkon toiminta perustuu louhijoiden sijaan verkon varmentajien hallinnoimien kryptovaluuttayksiköiden määrään. Käytännössä Ethereum-vekko on niin laaja, ettei kenenkään ole mahdollista ostaa Etheriä hyökkäyksen toteuttamiseksi. Sen sijaan nykyisessä PoW-verkossa tällaiset hyökkäykset ovat teoriassa mahdollisia. Esimerkiksi nykyinen Ethereum on haarauma sen edeltäjästä, joka tunnetaan nykyisin nimellä Ethereum Classic. Vanha verkko haarautettiin juuri 51 % hyökkäyksen vuoksi, ja Ethereum Classic on toisinaan yhä hyökkäysten kohteena.
[284] Ks. *Ahuja – Pal – Ribeiro* 2021.
[285] Ibid.

Lohkoketjuteknologialle ei ole myöskään vielä olemassa tarpeeksi kattavaa kansainvälistä sääntelykehystä.[286] Säänneltyä lohkoketjuteknologialle perustuvaa kaupankäyntiä varten tarvitaan tulevaisuudessa lainkäyttöalueet ylittävää hallitustenvälistä yhteistyötä.[287] Tällainen yhteistyö olisi luontevinta perustaa johonkin tekniseen sääntelykeinoon, kuten esimerkiksi edellä mainittuun konsensusprotokollatason sääntelyratkaisuun.

Myös kryptovaluuttojen laillisen käytön lisensointia on kokeiltu ottaa käyttöön esimerkiksi New Yorkin rahoituspalveluosaston liikkeelle laskemilla virtuaalivaluutan BitLicense-yrityslisensseillä.[288] Monet maat, kuten Iso-Britannia, Australia, Yhdysvallat, Hong Kong, Malesia, Singapore, Sveitsi, Thaimaa ja Yhdistyneet Arabiemiraatit ovat joko harkinneet tai implementoineet 'säädännöllisiä testausympäristöjä' suosituille lohkoketjuille.[289] Euroopan unionissa on keskitytty oman alueellisen lainsäädännön kehittämiseen. On kuitenkin selvää, että tulevaisuudessa on tarpeellista tehdä entistä enemmän lainsäädäntöalueiden välistä yhteistyötä, jotta lohkoketjupohjainen talousjärjestelmä voisi toimia tehokkaasti kansainvälisellä tasolla.

Bitcoinin ja muiden kryptovaluuttojen uskottavuus on vuosien kuluessa kärsinyt huomattavasti sen vuoksi, miten helppoa teknologian hyödyntäminen laittomiin käyttötarkoituksiin on. Esimerkiksi Silk Roadin tapaus johti siihen, että Bitcoinia pidettiin vuosikausia lähinnä nettihuumekaupan maksuvälineenä. Lainsäätäjien epäluuloisuus on johtanut yrityksiin säännellä kryptovaluuttoja perinteisin keinoin ja kielloin, mikä ei niiden hajautetun luonteen vuoksi ole aina toimivin ratkaisu.[290] Esimerkiksi kryptovaluuttojen täyskieltoa on käytännössä mahdoton toteuttaa.

Hajautetussa verkossa toimivissa lohkoketjuissa jokaisella verkon osaottajalla voi olla täydellinen kopio ketjun sisältämästä datasta. Yksittäisen osanottajan poistuminen verkosta ei siis haittaa sen toimintaa, kun tiedot ovat myös muissa verkkoon liittyneissä laitteissa.[291] Näin ollen hajautettua teknologiaa on hyvin vaikeaa rajoittaa tai kieltää täysin, sillä esimerkiksi Bitcoin-verkon kaataminen vaatisi joka ikisen Bitcoinin louhintaa harjoittavan ja verkon laskentatehoa ylläpitävän laitteen, sekä joka ikisen Bitcoin-solmun etsimistä, sillä niillä kaikilla on täydellinen kopio lohkoketjusta. Hajautettua teknologiaa, on siis syytä myös säännellä hajautetusti.

---

[286] Ks. *Kiviat* 2015.
[287] Ks. *Yeoh* 2017.
[288] Ks. *Chohan* 2018a.
[289] Ks. Nishith Desai Associates 2018.
[290] Ks. Bitcoinin laillisuuden tila maittain.
[291] Ks. *Johansson ym.* 2019, s. 62.

6. LOPUKSI

Tutkielman tutkimuskysymyksenä on selvittää kryptovaluuttojen käytön ja sääntelyn haasteita rahanpesussa, terrorismin rahoituksessa ja huumekaupassa. Olemassa olevan sääntelyn analysoiminen ja kritiikki on perusteltua muun muassa siitä syystä, että EU:n useiden miljardien arvoinen rahanpesun ja terrorismin rahoittamisen vastainen järjestelmä tavoittaa vain noin yhden prosentin kaikista rikollisista varoista.[292] Vaikka suurin osa tästä varallisuudesta sijoittuu yhä perinteiseen finanssijärjestelmään, on kryptovaluuttojen käyttö rahanpesussa, terrorismin rahoituksessa ja huumausaineiden kaupassa nopeasti kasvava uhka.

Tämän tutkielman kannalta merkittävä oikeudellinen ongelma on, miten kryptovaluuttoja koskevaa sääntelyä voitaisiin kehittää. Aarnion mukaan ”hyvän tutkielman tulee aina sisältää jokin tai joitakin *perusväitteitä*. Jos tutkielmassa ei väitetä mitään, se on pelkkä asioiden kuvaus tai ongelmien listaus”.[293] Tutkielmani perusväite on, että kryptovaluuttojen sääntelytarve on kaksitasoinen. Voidaan puhua perinteisestä keskitetystä sääntelystä ja uudenlaisesta hajautetusta sääntelystä. Keskitettyjen toimijoiden sääntely on tärkeää, koska suurin osa kryptovaluuttaalan rahaliikenteestä kulkee niiden kautta. Ongelmien tärkeysjärjestystä arvioitaessa, keskitetyn sääntelyn kehittäminen on lyhyellä aikavälillä käytännönläheisempää ja vaikutuksiltaan ennakoitavampaa. Tämä ei kuitenkaan syrjäytä uudenlaisen hajautetun sääntelyn tutkimistarvetta, vaan ainoastaan viestii lainsäätäjien tämänhetkisistä intresseistä. EU-tason direktiivit ja asetukset, joilla kohdistetaan velvoitteita kryptovaluutta-alan ilmoitusvelvollisiin tahoihin ovat pitkälti jatkumoa perinteisten finanssilaitosten sääntelylle, kun taas juridiikan siirtäminen hajautettuun toimintaympäristöön olisi perustavanlaatuinen muutos koko oikeustieteen alalla.

Sääntelystä ja rikosten torjunnasta tekee haastavaa se, että pelkkä keskitetty sääntely ei voi yksinään saavuttaa merkityksellisiä tuloksia ilman, että suuri joukko valtioita ryhtyy riittävän mittaviin yhdenmukaisiin lainsäädäntötoimiin. Sääntelyn sovittamisvaikeus uuteen järjestelmään näkyy siinä, että vanhoihin säädöksiin joudutaan jatkuvasti lisäämään uusia, kryptovaluutta-alan toimijoita koskevia määritelmiä. Direktiivit ovat jatkuvassa muutostilassa ja alan kehitys on niin nopeaa, että esimerkiksi EU:n viides rahanpesudirektiivi oli jo voimaantulohetkellään käytännössä vanhentunut. Uusien säädösten voimaantulohetkellä on ehtinyt ilmaantumaan uusia toimintatapoja, jotka ovat sääntelyn ulkopuolella. Osa kryptovaluutta-alan toimijoista, kuten hajautetut pörssit, eivät myöskään teknisistä syistä sovellu lainkaan perinteiseen järjestelmään,

[292] Ks. Euroopan komissio: Report on Asset recovery and confiscation: ensuring that crime does not pay 2020.
[293] *Aarnio* 2011, s. 111.

koska niillä ei ole sellaista tahoa johon vastuun voisi ylipäätään kohdistaa, vaan kyseiset palvelut toimivat hajautetusti.

Edellä mainittujen seikkojen vuoksi keskitetyssä sääntelyssä olisi tärkeää huomioida kryptovaluuttojen toiminnan perusluonne ja ominaisuudet. Keskitetyssä sääntelyssä tulee pyrkiä parantamaan valtioiden keskinäistä yhteistyötä, valvontaorgaanien teknisiä valmiuksia tunnistaa laitonta toimintaa ja laatia sääntelystä riittävän joustavaa, jotta mikään tuleva toimintamuoto ei jää täysin puuttumiskeinojen ulkopuolelle. Euroopan komission 20.7.2021 julkaisema lainsäädäntöpaketti ilmentää EU:n muutosvalmiutta ja sisältää merkittäviä parannuksia tässä tutkielmassa käsiteltyihin ongelmiin.

Myös FATF:n tulevat, vuoden 2021 marraskuussa julkaistavat, suositukset saattavat edellyttää jatkouudistuksia. Keskitetyn sääntelyn kehitys on kiertänyt hitaasti kehää. Alalla tapahtuvat muutokset johtavat FATF:n uusiin suosituksiin, joiden perusteella laaditaan EU:n direktiivejä. Direktiivit tulevat osaksi kansallista lainsäädäntöä, joka tulee voimaan niin hitaasti, että se ei ole voimaantulohetkellä monin paikoin enää relevanttia. Tämä ylhäältäpäin johdetun ylikansallisen prosessin hitaus kuitenkin tarkoittaa, että esimerkiksi EU:n jäsenmailla on subsidiariteetin nojalla mahdollisuus proaktiivisesti tehdä merkityksellisiä oikeudellisia ratkaisuja ja suunnata kehitystä, kuten esimerkiksi Saksa on tehnyt.

Proaktiivinen suhtautuminen kryptovaluutta-alan lainsäädäntöä kohtaan auttaa valtioita ehkäisemään rahanpesua, terrorismin rahoitusta ja huumausaineiden anonyymiä kauppaa. FATF:n 5.7.2021 julkaiseman raportin mukaan vain 58 lainkäyttöaluetta 128 raportoivasta lainkäyttöalueesta oli toteuttanut tarvittavat FATF:n suositusten mukaiset muutokset kansallisessa lainsäädännössään. Jäljelle jäävät 70 lainkäyttöaluetta muodostavat näin ollen merkittävän aukon kansainväliseen AML/CFT-järjestelmään ja mahdollistavat kryptovaluuttapalveluntarjoajien siirtymän suotuisammille lainkäyttöalueille.[294] On esimerkiksi yleistä, että yksilöt ja yritykset muuttavat kevyemmän lainsäädännön alueille verotaakkansa keventämiseksi. Rahanpesun torjunnan kannalta olisi tärkeää, ettei niin sanottuja veroparatiisivaltioita muodostuisi lainkaan.[295]

Tehokas keskitetty sääntely edellyttää myös täsmällistä ja perusteltua käsitteistöä. Tutkielman alussa vertailtiin keskenään virtuaalivaluutan ja kryptovaluutan käsitteiden soveltuvuutta. Samassa yhteydessä mainittiin käsite krypto- tai virtuaalivarallisuus. Tämä määritelmä jättää kokonaan pois sanan valuutta, sillä se on osoittautunut ongelmalliseksi. Sana valuutta, kuvaa

[294] Ks. FATF: Second 12-Month Review of Revised FATF Standards - Virtual Assets and VASPs 2021.
[295] Ks. *Sahavirta* 2008, s. 61.

sinänsä huonosti kryptojen luonnetta, sillä ne eivät, El Salvadoria lukuun ottamatta, ole yleisesti hyväksytyn laillisen maksuvälineen asemassa. Suomen virtuaalivaluuttalaissa olevat virtuaalivaluutan ja virtuaalivaluutan tarjoajan määritelmät ovat ristiriitaisia ja puutteellisia.

FATF:n suosituksissa on jo pitkään puhuttu virtuaalivarallisuudesta. Euroopan unionin komission 20.7.2021 julkistama lainsäädäntöpaketti on puolestaan tuomassa kryptovarallisuuden käsitteen EU-sääntelyyn. Ehdotan, *de lege ferenda,* virtuaalivaluuttalain 2 §:ssä oleviin määritelmiin tehtäväksi seuraavia muutoksia ja lisäyksiä, jotta ne vastaisivat paremmin FATF:n suosituksia ja heijastaisivat kansainvälistä kehitystä kohti laajempia käsitteitä, jotka kattavat huomattavasti laajemman joukon alan palveluita:

1) *virtuaalivarallisuudella* digitaalisessa muodossa olevaa arvoa:
a) jota keskuspankki tai muu viranomainen ei ole laskenut liikkeeseen ja joka ei ole laillinen maksuväline;
b) jota henkilö voi käyttää maksu- tai sijoitusvälineenä;
c) jota voidaan siirtää, tallentaa ja vaihtaa sähköisesti;"

2) *virtuaalivarallisuuden tarjoajalla* virtuaalivarallisuuden liikkeeseenlaskijaa, virtuaalivarallisuuden vaihtopalvelua, virtuaalivarallisuuden markkinapaikkaa sekä virtuaalivarallisuuden lompakkopalvelun tarjoajaa, joka tarjoaa yhtä tai useampaa seuraavista palveluista:
a) vaihdot virtuaalivarojen ja fiat-valuuttojen välillä;
b) vaihdot yhden tai useamman virtuaalisen omaisuuden muodon välillä;
c) virtuaalivarojen siirto;
d) virtuaalivarojen säilytyspalveluiden tarjoaminen ja/tai sijaishallinta virtuaalivarojen hallinnan mahdollistamiseksi;
e) rahoituspalvelujen tarjoaminen, joka liittyy liikkeeseenlaskijan tarjoukseen ja/tai virtuaalisen omaisuuden myyntiin.

Tällä hetkellä eletään kryptovaluutta-alan murroskautta. Etenkin murroksen aikakaudella vaaditaan herkkyyttä syvempiin systemaattisiin ja kontekstuaalisiin pohdintoihin. Kryptovaluuttarikollisuuden torjumiseksi lainsäätäjien on tehtävä yhteistyötä teknologian alan asiantuntijoiden kanssa ja oltava kaukonäköisiä tarvittavan lainsäädännön suhteen. Mikäli kryptovaluuttoja sääntelytäisiin teknologiasta käsin, eikä sen ulkopuolelta, kyettäisiin niiden laiton käyttö estämään riippumatta yksittäisten lainkäyttöalueiden AML/CFT-käytännöistä.

Sääntelytarpeen toinen taso sijaitsee vääjäämättä hajautetussa ympäristössä. Lohkoketjuteknologia asettaa keskitetylle sääntelylle konkreettisia rajoja, joita sen on mahdoton ylittää. Tämä ilmenee tässä tutkimuksessa muun muassa kryptovaluuttoihin liittyvien oikeudellisten erityiskysymysten kohdalla. Teknologia muodostaa paradoksin suhteessa perusoikeuksiin. Kryptovaluuttojen pseudo-anonyymisyys aiheuttaa näyttöongelmia ja yksityisavaimia asianmukaisesti hallinnoivalta taholta on mahdotonta takavarikoida kryptovaluuttaosoitteessa olevaa varallisuutta.

Nykymuotoinen oikeusjärjestelmä ei pysty tehokkaasti selvittämään ja tuomitsemaan tiettyjä rikostyyppejä.

Tästä syystä, vaikka hajautettujen sääntelyratkaisujen tutkiminen ja toteutus veisi vuosikausia ja vaikutukset tulisivat näkyviin viiveellä, vuosien tai vasta vuosikymmenten päästä, on vaihtoehtoisten ratkaisujen tutkiminen kannattavaa. Tämä kanta muodostuu kryptovaluuttojen käytön yleistyessä päivä päivältä perustellummaksi. Ongelma kryptovaluuttojen sääntelyssä hajautetulla teknisellä tasolla on, että se sotii osittain kryptovaluuttojen perusluonnetta vastaan. Lisätty sääntely on kuitenkin tarpeellista alan legitimoimiseksi. Lohkoketjuteknologian avulla on mahdollista toteuttaa uudenlaisella käyttäjäystävällisellä tavalla esimerkiksi asiakkaan tunnistaminen, ilman pysyvää henkilötietojen tallennusta.[296]

Tutkimuksen tarkoituksena on myös visioida sitä mahdollisuutta, että meneillään on merkittävin internetin kehittämisen jälkeen tapahtunut paradigman muutos. Myös itse internet voi lohkoketjuteknologian ansiosta siirtyä hajautettuun ympäristöön tavalla, joka tekee siitä uudella tavalla vapaan ja puolueettoman. Tämä paradigman muutos vaatii lopulta myös juridiikan siirtämisen hajautettuun ympäristöön. Väitän, että vaikka kansainvälisen AML/CFT-järjestelmän lainsäädäntö olisi lähes täydellisen yksimielistä, puuttuisi yhtälöstä merkittävä palanen.

Tutkimuksessa käsiteltävien ongelmien oikeusalakohtainen ja yhteiskunnallinen relevanssi rikosoikeuden kannalta liittyy myös siihen, että kyse on hyvin uudesta teknologiasta. Alkuvuosina yksi perustavanlaatuisimmista kryptovaluuttoihin liitetyistä lähtöoletuksista oli, että niitä käyttävät ainoastaan rikolliset. Mikä on rikollista ei voi olla legitiimiä. Jotta voitaisiin laajemmin keskittyä lohkoketjuteknologian hyödyllisiin sovellutuksiin, on etsittävä vastauksia ja ratkaisuja sen rikolliseen käyttöön. Kun laillisen ja laittoman käytön rajat selkiytyvät, yleinen suhtautuminen kryptovaluuttoihin muuttuu, minkä vuoksi kryptovaluuttojen rikollisen käytön ehkäiseminen on tärkeää. Tämä puolestaan edellyttää siirtymää hajautuneeseen ympäristöön, koska pelkkä keskitetty sääntely ei ole ollut riittävän tehokasta ja voisi väärin toteutettuna tappaa innovaation.[297] Lohkoketjuteknologialle on hyödyllistä käyttöä myös sopimusoikeudessa, insolvenssioikeudessa sekä useilla muilla oikeudenaloilla.

---

[296]Ks. *Biryukov – Khovratovich – Tikhomirov* 2018.

[297] Vert. *Nabilou* 2019, joka on sitä mieltä, että vaikka teknologian sääntely olisi mahdollista, paras sääntelystrategia on siitä huolimatta kohdistaa sääntely portinvartijoihin. Tämänkin tutkielman tulosten näkökulmasta lyhyellä aikavälillä selkein vaihtoehto on kohdistaa sääntely portinvartijoihin, mutta korostan avoimen suhtautumisen tärkeyttä tulevaisuudessa. Vastuun sysääminen portinvartijoille viestii markkinavetoisesta suhtautumisesta, joka näkee kryptovaluutat lähinnä sijoituskohteena. Preventiivinen sääntely on reaktiivista ja kehittyy hitaasti, mikä johtaa eritasoiseen oikeustilaan eri lainkäyttöalueilla. Teknissidonnaisen sääntelyn kehittäminen on teknologiapositiivisempi lähestymistapa ja voi edesauttaa teknologian leviämistä ja ehkäistä tulevia konflikteja.

Valtioiden on yhdessä ylikansallisten järjestöjen kanssa kehitettävä poikkitieteellisiä monipuolisia ja tehokkaita keinoja suorittaa sääntelyä reaalimaailman lisäksi myös hajautetussa ympäristössä. Toistaiseksi yhtäkään toiminnassa olevaa lohkoketjuprotokollaa ei ole suunniteltu tekemään konsensustason sääntelyä, mutta toteutustavoista tehdään tutkimusta. Tilanne on käytännössä se, että tekniset toteutuskeinot ovat olemassa, mutta toistaiseksi ei ole ollut poliittista tahtoa tämäntyyppisen ratkaisun omaksumiseen. Konsensustason sääntelyä saatetaan kokeilla käytännössä, kun jokin valtio haluaa hyödyntää lohkoketjuteknologiaa omiin tarkoituksiinsa, mutta sen on voitava ennakoida ja hallinnoida lohkoketjun toimintaa tietyllä tapaa. Samalla tulee tarjota jonkinlainen taloudellinen kannustin juuri kyseisen konsensusalgoritmin toimeenpanemiseksi, mikä saattaa tarkoittaa esimerkiksi lisensointia. Näiden lisensoitujen toimeenpanijoiden vastuulla on lisätä todistettavasti lailliset transaktiot lohkoihin ja suorittaa konsensusalgoritmia näillä laillisten transaktioiden lohkoilla. Jokin lohkoketju saattaa myös olla rakenteeltaan sellainen, että sen pohjalta on mahdollista luoda rinnakkaisketjuja, jotka soveltuvat eri aloille. Näillä rinnakkaisketjuilla voi kullakin olla omat sääntönsä, toimintaperiaatteensa ja käyttötarkoituksensa, mutta ne voivat pohjimmiltaan perustua samaan teknologiseen ratkaisuun.

Koska konsensusalgoritmeja on olemassa monenlaisia ja teknisiä toteutustapoja vielä enemmän, on mahdotonta ennakoida miltä tulevaisuus näyttää. Sekin mahdollisuus on olemassa, että jokin muu menetelmä tulevaisuudessa syrjäyttää lohkoketjun. Valtiot ja keskuspankit todennäköisesti jossain vaiheessa hyväksyvät lohkoketjuteknologian ja myöntävät sen hyödyt. Ne eivät kuitenkaan tule hyväksymään täysin hajautettua talousjärjestelmää. Edellä kuvatut lisensointiin perustuvat konsensustason hajautetun sääntelyn mekanismit saattavat vaikuttaa lohkoketjuteknologian vapausajatteluun perustuvista periaatteellisista lähtökohdista katsottuna vierailta, mutta tosiasia on se, että olemassa oleva taloudellinen ja poliittinen valta-asetelma tulee johtamaan kompromisseihin ja näin ollen säänneltyjen ja sääntelemättömien lohkoketjujen rinnakkaiseen olemassaoloon.

Lohkoketjutransaktioiden varmuus voi huomattavasti helpottaa varojen varmentamista ja turvaamista. Yhteiskunnan reaaliset vaatimukset ja uudistuva ajattelu edellyttävät muutosta. Näin ollen uudesta teknologiasta saattaa tulla keino puuttua juuri niihin ongelmiin, joita sen pelättiin alun perin lisäävän. Lohkoketjuteknologiaa on mahdollista käyttää rikosten ehkäisyyn ja teknologian mahdollistama täydellinen varmuus ja transaktioiden peruuttamattomuus tarjoaa yhden ratkaisuvaihtoehdon maailmanlaajuiseen rahanpesuongelmaan.

Kriminaalipoliittisesta ja oikeustaloustieteellisestä näkökulmasta voidaan tämän tutkimuksen perusteella arvioida, että hyöty–haitta-punninnassa kryptovaluuttojen täyskielto on epäsopivin

ratkaisu, mutta yhtä lailla täysi sääntelemättömyys on huono asia. Sopivan asteinen keskitettyjen toimijoiden sääntely yhdistettynä uuden hajautetussa ympäristössä tapahtuvan sääntelyn mahdollisuuksien tutkimiseen, johtaa pitkällä aikavälillä tehokkaimpaan lopputulokseen.

Tutkielmassa käytetyt menetelmät: oikeusdogmatiikka, oikeussosiologia, oikeuspolitiikka (kriminaalipolitiikka) ja oikeusvertailu, mahdollistivat laajan aihepiirin tehokkaan arvioinnin. Jatkotutkimusta ajatellen aihepiirin laajentaminen myös muihin kuin tämän tutkielman kolmeen rikostyyppiin, sekä oikeudellisten erityisongelmien käsittelyn laajentaminen olisi luontevaa ja lisäisi tutkimuksen tulkintalainopillisuutta. Tämän tutkielman toteutuneessa laajuudessa erityiskysymysten tarkastelussa kuvattiin esimerkkitapauksen kautta nykyjärjestelmän puutteita. Tutkielma esittää ratkaisuvaihtoehtoja käytännön oikeudellisiin ongelmiin rahanpesun sääntelyssä, mutta myös teoreettisempia ratkaisuvaihtoehtoja, joiden toteutusmuotojen tutkiminen edellyttää jatkossa vielä poikkitieteellisempää, toisin sanoen hajautetumpaa, otetta.