Aalto-yliopisto
Aalto-universitetet
Aalto University

Yritysjuridiikan maisteriohjelma

Kryptovarojen riskit rahanpesussa

Vaikutukset pankkien riskienhallintaan

Karoliina Koponen

Pro gradu
2024

Aalto-yliopisto
Aalto-universitetet
Aalto University

Tekijä Karoliina Koponen

Työn nimi Kryptovarojen riskit rahanpesussa – vaikutukset pankkien riskienhallintaan

Koulutusohjelma Yritysjuridiikan maisteriohjelma

Työn ohjaaja Petri Kuoppamäki

Päivämäärä 19.5.2024 **Sivumäärä** 63 **Kieli** Suomi

Tiivistelmä

Lohkoketjuteknologia on mahdollistanut uudenlaisten valuuttojen ja maksutapojen kehittämisen. Lohkoketjujen avulla on kehitetty erilaisia virtuaalivaroja, joiden markkina on kasvanut suureksi ja samalla se on herättänyt huolta väärinkäytösten mahdollisuuksista. Virtuaalivarojen avulla on mahdollista suorittaa osittain anonyymeja ja nopeita transaktioita ilman pankkien osallistumista transaktioihin. Anonymiteetti, sääntelyn vähäisyys ja toiminta ilman pankkeja on kasvattanut kryptovarojen käytön kiinnostusta myös rikollisten osalta. Viranomaiset haluavat tarkempaa sääntelyä alalle, sillä rahanpesun riski kryptovarojen osalta on kohonnut.

Tämän tutkielman tarkoitus on tutkia kryptovaroihin liittyvää sääntelyä ja sen tulevaisuutta sekä kryptovarojen aiheuttaman rahanpesuriskin vaikutuksia pankeille. Tässä tutkielmassa selvennetään tämän hetken kryptovarojen sääntelykokonaisuutta sekä siihen liittyviä muutoksia sekä näiden haasteita. Lisäksi tutkielmassa pureudutaan kryptovaroihin liittyvään taksonomiaan, lohkoketjujen ja kryptovarojen toimintalogiikkaan sekä käyttötarkoituksiin ja kryptovaroihin liittyvään rahanpesuriskiin. Tutkielmassa selvitetään myös kryptovarojen aiheuttamaa rahanpesuriskiä pankeille sekä tutkitaan sitä, miten pankit voivat hallita kryptovarojen rahanpesuriskiä.

Tutkielmassa selviää, että kryptovaroja hyödynnetään rahanpesussa erityisesti niiden osittaisen anonymiteetin, sääntelyn vähäisyyden sekä palveluiden monimuotoisuuden ja keskitetyn hallinnon puutteen takia. Kryptovarojen käyttö rahanpesussa nostaa myös pankkien rahanpesuriskiä, jota on vaikea ennustaa ja hallita. Sääntely on kuitenkin kryptovarojen osalta kiristymässä jo vuoden 2024 aikana, jonka tarkoituksena on hallita kryptovaroihin liittyviä riskejä myös rahanpesun osalta sekä laajentaa lainsäädännön soveltamisalaa koskemaan laajemmin erilaisia kryptovaroja myös virtuaalivaluuttojen ulkopuolelle.

Pankkien rahanpesuriskien hallinta kryptovarojen osalta on haastavaa, sillä kryptovarat aiheuttavat riskejä, joita on vaikea havaita, ennustaa ja niihin voi olla haastavaa reagoida. Kuitenkin perinteisiä pankkien riskienhallintakeinoja kuten, riskiarviota, monitorointia ja asiakkaan tuntemista hyödyntämällä voidaan mahdollisesti estää kryptovaroihin liittyvien rahanpesuriskien realisoitumista. Myös uusia teknologisia ratkaisuja on markkinoilla, jotka voivat hyödyttää pankkeja kryptovarojen rahanpesuriskien hallinnassa.

Avainsanat Kryptovarat, virtuaalivaluutat, lohkoketju, rahanpesu, riskienhallinta, asiakkaan tunteminen, pakotteet

Aalto-yliopisto
Aalto-universitetet
Aalto University

Author Karoliina Koponen

Title of thesis Risks of crypto assets in money laundering – impacts on banks' risk management

Programme Master of Science in Economics and Business Administration

Major Business Law

Thesis advisor Petri Kuoppamäki

Date 19.5.2024 **Number of pages** 63 **Language** Finnish

Abstract

Blockchain technology has enabled the development of new currencies and payment methods. Blockchains have been used to develop various virtual assets and the market has grown significantly and at the same time it has raised concerns about the potential for abuse. Virtual currencies make it possible to carry out partially anonymous and fast transactions without the involvement of banks. Anonymity, low regulation, and operations without banks involved have increased interest in the use of crypto assets in criminal activities. Authorities want more detailed regulation to the sector, as the risk of money laundering in crypto assets has increased.

The purpose of this thesis is to investigate the regulation and future of crypto assets, as well as the impact of the money laundering risk posed by crypto assets on banks. This thesis clarifies the current regulatory framework for crypto assets, changes in regulation in the future, and challenges of the regulatory framework. In addition, the thesis examines the taxonomy related to crypto assets, the logic behind blockchains and crypto assets and risk of money laundering related to crypto assets. The thesis also examines the money laundering risk posed by crypto assets to banks and examines how banks can manage the money laundering risk of crypto assets.

The study shows that crypto assets are used for money laundering, especially due to their partial anonymity, low level of regulation, diversity of services and lack of centralized governance. The use of crypto assets for money laundering also increases banks' money laundering risk, which is difficult to predict and manage. However, regulation of crypto-assets will tighten already during 2024, with the aim of managing risks related to crypto-assets also in terms of money laundering and extending the scope of the legislation to cover a wider range of crypto-assets also outside virtual currencies.

Managing banks' money laundering risks with regard to crypto-assets is challenging, as crypto assets pose risks that are difficult to detect, predict and react to. However, traditional banks' risk management tools, such as risk assessment, monitoring, and customer due diligence, can potentially prevent the realization of money laundering risks related to crypto assets. There are also new technological solutions on the market that can benefit banks in managing money laundering risks for crypto assets.

Keywords Cryptoassets, cryptocurrencies, blockchain, anti-money laundering, risk management, know your customer, sanctions

Aalto-yliopisto
Aalto-universitetet
Aalto University

Sisällys

Lähteet

Virallislähteet

ESMA.
Markets in Crypto-Assets Regulation (MiCA). [Viitattu 21.4.2024] Saatavissa: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

European Banking Authority.
Ohjeet, jotka on annettu direktiivin (EU) 2015/849 17 artiklan ja 18 artiklan 4 kohdan nojalla asiakkaan tuntemisvelvollisuudesta sekä tekijöistä, joita luotto- ja finanssilaitosten olisi tarkasteltava arvioidessaan yksittäisiin liikesuhteisiin ja yksittäisiin liiketoimiin liittyvää rahanpesun ja terrorismin rahoituksen riskiä (jäljempänä 'rahanpesun ja terrorismin rahoituksen riskitekijöitä koskevat ohjeet') ja joilla kumotaan ja korvataan ohjeet JC/2017/37 EBA/GL/2021/02

Eurooppa-neuvosto.
Rahanpesun torjunta: neuvosto ja parlamentti sopuun tiukemmista säännöistä. 18.1.2024. [Viitattu 10.3.2024] Saatavissa: https://www.consilium.europa.eu/fi/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/

Eurooppa-neuvosto.
Terrorismin torjunta EU:ssa. [Viitattu 27.5.2024] Saatavilla: https://www.consilium.europa.eu/fi/policies/fight-against-terrorism/fight-against-terrorist-financing/#AMLA

Euroopan keskuspankki.
A stocktake on the digital euro. Summary report on the investigation phase and outlook on the next phase. 18.10.2023. [Viitattu 21.4.2024] Saatavilla: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.dedocs231018.fi.pdf

Euroopan komissio.
Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) 2024. [Viitattu 27.4.2024] Saatavilla: https://finance.ec.europa.eu/document/download/553ff649-fce8-4e31-b54c-01f562ca0bb3_en?filename=240424-anti-money-laundering-faqs_en.pdf

FATF.
The FATF recommendations. International Standards

On Combating Money Laundering And The Financing Of
Terrorism & Proliferation 2023. [Viitattu 21.4.2024] Saatavilla: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

FATF.
Updated guidance for a risk-based approach. Virtual assets and virtual asset service providers, October 2021. [Viitattu 10.3.2024] Saatavilla: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

FATF.
Virtual Currencies Key Definitions and Potential AML/CFT Risks 2014. [Viitattu 12.4.2024] Saatavilla: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

FATF.
What we do. [Viitattu 13.4.2024] Saatavilla: https://www.fatf-gafi.org/en/the-fatf/what-we-do.html

FATF.
FATF clarifies risk-based approach: case-by-case, not wholesale de-risking 2014. [Viitattu 30.4.2024] Saatavilla: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Rba-and-de-risking.html

Finanssivalvonta
Määräykset ja ohjeet 02/2023. Rahanpesun ja terrorismin rahoittamisen estäminen. FIVA/2023/1289

Finanssivalvonta.
Finanssivalvonta on määrännyt seuraamusmaksun S-Pankki Oy:lle sekä antanut julkisen varoituksen FIM Varainhoito Oy:lle laiminlyönneistä asiakkaan tuntemisessa. Lehdistötiedote 18.12.2019. [Viitattu 28.4.2024] Saatavilla: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2019/finanssivalvonta-on-maarannyt-seuraamusmaksun-s-pankki-oylle-seka-antanut-julkisen-varoituksen-fim-varainhoito-oylle-laiminlyonneista-asiakkaan-tuntemisessa2/

Finanssivalvonta.
Määräykset ja ohjeet 03/2024. Pakotesääntelyn ja kansallisten jäädyttämispäätösten noudattamiseen liittyvä asiakkaan tunteminen.

Finanssivalvonta.

Määräykset ja ohjeet 4/2019. Virtuaalivaluutan tarjoajat.

Finanssivalvonta.
Toimintakertomus 2023. [Viitattu 30.4.2024] Saatavilla: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/toimintakertomukset/toimintakertomus-2023/teemat/pakotteet-osaksi-finanssivalvonnan-valvontaa/

HE 31/2024 vp
Hallituksen esitys eduskunnalle laiksi kryptovarapalvelun tarjoajista ja kryptovaramarkkinoista sekä eräiksi muiksi laeiksi

Valtiovarainministeriö a.
Valtiovarainministeriön julkaisuja 2024:8. Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2023.

Valtionvarainministeriö b.
Suomi on vahvistanut rahanpesun ja terrorismin rahoittamisen estämistä – pääsee pois tehostetusta seurannasta. Rahanpesun ja terrorismin rahoittamisen vastainen toimintaryhmä 24.10.2023. [Viitattu 13.5.2024] Saatavilla: https://vm.fi/-/suomi-on-vahvistanut-rahanpesun-ja-terrorismin-rahoittamisen-estamista-paasee-pois-tehostetusta-seurannasta

Vasara, Pekka.
Suomi pääsi pois rahanpesun torjunnan tarkkailuluokalta.
Finanssivalvonnan blogi 04/2023.
[Viitattu 27.4.2024] Saatavissa: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2023/suomi-paasi-pois-rahanpesun-torjunnan-tarkkailuluokalta/

Rahanpesun selvittelykeskus.
Rahanpesun selvittelykeskuksen vuosikertomus 2023.
[Viitattu 25.4.2024] Saatavissa: https://rahanpesu.fi/documents/25235045/67733116/vuosikertomus-saavutettava.pdf/da6396ec-eb64-814a-3006-89b38baca942/vuosikertomus-saavutettava.pdf?t=1709018951850

Rahanpesun selvittelykeskus.
Rahanpesun selvittelykeskuksen vuosikertomus 2022. [Viitattu 10.3.2024] Saatavissa: https://poliisi.fi/documents/25235045/67733116/Rahanpesun-selvittelykeskuksen-vuosikertomus-2022.pdf/d4d07605-68b5-ee84-ffd7-ec09541dc9d7/Rahanpesun-selvittelykeskuksen-vuosikertomus-2022.pdf?t=1679478208148

Kirjallisuuslähteet

Aarnio, Aulis.
Tulkinnan taito: ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta.
Talentum Media. Helsinki 2006.
(Aulis 2006)

Alman, Susan – Hirsh, Sandra.
Blockchain.
American Library Association. Chicago. 2019.
(Alman – Hirsh 2019)

Bashir, Imran.
Mastering Blockchain, 4th edition. Packt Publishing. Birmingham. 2023.
(Bashir 2023)

Bashir, Imran.
Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition. Packt Publishing. Birmingham. 2018.
(Bashir 2018)

Beckett Velez, Sophia
Compliance and Financial Crime Risk in Banks: A Practitioners Guide.
Emerald Publishing Limited, Leeds 2024.
(Beckett Velez 2024)

Cawrey, Daniel – Lantz, Lorne
Mastering Blockchain.
O'Reilly Media. 2022.
(Cawrey – Lantz 2022)

Carlisle, David.
The crypto launderers: crime and cryptocurrencies from the Dark Web to DeFi and beyond.
John Wiley & Sons Ltd, Chichester 2024.
(Carlisle 2024)

Chapman, Rose.
Anti-Money Laundering.
Kogan Page, Lontoo. 2018.
(Chapman 2018)

Dill, Alexander.
Bank Regulation, Risk Management, and Compliance.

Informa Law from Routledge, New York 2020.
(Dill 2020)

Eerola, Mikko – Innanen, Antti – Johansson, Patrik Elias – Viitala, Juha
Lohkoketju – tiekartta päättäjille
Alma Talent. Helsinki 2019.
(Eerola ym. 2019)

Fabe, Amparo Pamela – Kaunert, Christian – Romaiuk, Scott
Countering Terrorist and Criminal Financing
Taylor & Francis, Oxfordshire 2023.
(Fabe – Kaunert – Romaniuk 2023)

Gurulé, Jimmy – King, Colin – Walker, Clive
The Palgrave Handbook of Criminal and Terrorism Financing Law.
Palgrave Macmillan, Lontoo 2018.
(Gurulé – King – Walker 2018)

Hirvonen, Ari.
Mitkä metodit? Opas oikeustieteen metodologiaan.
Yleisen oikeustieteen julkaisuja 17, Helsinki 2011.
(Hirvonen 2011)

Hyttinen, Tatu.
Rahanpesu ja rikosvastuu.
Alma Talent Oy, Helsinki 2021.
(Hyttinen 2021)

Jeegers, Thomas.
Understanding Crypto Fundamentals: Value Investing in Cryptoassets and Management of Underlying Risks.
Apress, New York 2023.
(Jeegers 2023)

Letto-Vanamo, Pia.
Johdatus oikeuteen ja oikeudelliseen ajatteluun.
Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja, Helsinki 2020.
(Letto-Vanamo 2020)

Määttä, Kalle.
Oikeustaloustieteen perusteet.
Otavan Kirjapaino Oy, Keuruu 2016
(Määttä 2016)

Määttä, Kalle
Oikeustaloustieteen aakkoset.
Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut.
Hakapaino Oy, Helsinki 1999.
(Määttä 1999)

Pursiainen, Aleksi
Kansainväliset pakotteet ja vientivalvonta.
Alma Talent, Helsinki 2021.
(Pursiainen 2021)

Riccardi, Michele
Money Laundering Blacklists.
Routledge, New York 2022.
(Riccardi 2022)

Artikkelit

Goldman, Kate – Kumar, Arnav
A Taxonomy of Digital Assets. Milken institute 2021.
(Goldman – Kumar 2021)

Lam, James
How Banks Can Finally Get Risk Management Right. Harvard Business Review 2023. [Viitattu 28.4.2024] Saaatavilla: https://hbr.org/2023/04/how-banks-can-finally-get-risk-management-right

Lauslahti, Kristian – Mattila, Juri – Seppälä, Timo
Älykäs sopimus: Miten blockchain muuttaa sopimuskäytäntöjä? ETLA Report, No. 57, The Research Institute of the Finnish Economy (ETLA), Helsinki, 2016.
(Lauslahti – Mattila – Seppälä 2016)

Lin, Runhui – Wang, Lun – Li, Biting – Lu, Yanhong – Qi, Zhiqiang – Xie, Linyu
Organizational governance in the smart era: The implications of blockchain. Nankai Business Review International, 14(2), 197–229. 2023.
(Lin ym. 2023)

Mattila, Juri.
Blockchain Systems as Multi-sided Platforms.
Aalto University, doctoral dissertations 122/2021 ETLA Economic Research, Series A, No 51.

(Mattila 2021)

Mattila, Juri – Seppälä, Timo
Distributed Governance in Multi-sided Platforms: A Conceptual Framework from Case: Bitcoin. In: Smedlund, A., Lindblom, A., Mitronen, L. (eds) Collaborative Value Co-creation in the Platform Economy. Translational Systems Sciences, vol 11. Springer, Singapore, 2018.
(Mattila – Seppälä 2018)

Nakamoto, Satoshi
Bitcoin: A peer-to-peer electronic cash system.
Decentralized Business Review, 21260, 2018.
(Nakamoto 2018)

Rodeck, David
Digital Currency: The Future Of Your Money.
Forbes Advisor. 16.2. 2023. [Viitattu 21.4.2024] Saatavilla: https://www.forbes.com/advisor/investing/cryptocurrency/digital-currency/
(Rodeck 2023)

Sharman, Jason
The Money Laundry. Regulating Criminal Finance in the Global Economy, Cornell University Press, 2011.
(Sharman 2011)

Szabo, Nick
Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). 1997.
(Szabo 1997)

Internetlähteet

Balestrino, Mike – Ghosh, Samir – Kok, Steven Alexander – Kronhellner, Bernhard – Macintosh, James – Scmid, Christian N.
Managing Risk for the Next Wave of Digital Currencies. Boston Consulting Group 24.7.2023. [Viitattu 1.5.2024] Saatavilla: https://www.bcg.com/publications/2023/managing-risk-for-next-wave-of-digital-currencies

Berger, Pierre. E. – Boeve, Martjin – Kalokyris, Nicolas.
MiCA & TFR: the two new pillars of the EU crypto-assets regulatory framework. DLA Piper, 20.7.2023. [Viitattu 23.4.2024] Saatavilla: https://www.dlapiper.com/en/insights/publications/2023/06/mica-tfr-the-two-new-pillars-of-the-eu-cryptoassets-regulatory-framework

Bitnodes
Bitnodes estimates the relative size of the Bitcoin peer-to-peer network by finding all of its reachable nodes. [Viitattu 14.4.2024] Saatavilla: https://bitnodes.io/#google_vignette
Cambridge Bitcoin Electricity Consumption Index
[Viitattu 14.4.2024] Saatavilla: https://ccaf.io/cbnsi/cbeci/comparisons

Bloomberg Law.
Banking, Professional Perspective - AML Issues in Cryptocurrency and Blockchain Technology 03/2021. [Viitattu 1.5.2024] Saatavilla: https://www.bloomberglaw.com/external/document/XB8LV1T4000000/banking-professional-perspective-aml-issues-in-cryptocurrency-an

Buch, Claudia.
Bridges to the future: managing bank risk amid uncertainty. European Central Bank 2024. [Viitattu 28.4.2024] Saatavilla: https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240312~5990ccfce7.en.html

Ceicdata
Finland Nasdaq Helsinki: Market Capitalization
[Viitattu 10.3.2024] Saatavilla; https://www.ceicdata.com/en/finland/nasdaq-helsinki-market-capitalization

Chainalysis.
Crypto investigations. [Viitattu 26.42024] Saatavilla: https://www.chainalysis.com/solution/crypto-investigations-discover/

Chainalysis.
U.S. Sanctions Crypto Mixer Sinbad.io for Role in North Korean Laundering Activities, 29.11.2023. [Viitattu 1.5.2024] Saatavilla: https://www.chainalysis.com/blog/crypto-mixer-sinbad-sactioned-north-korean-laundering/

Comply advantage.
The biggest AML fines in 2023, 5.2.2024. [Viitattu 28.4.2024] Saatavilla: https://complyadvantage.com/insights/aml-fines-2023/

Elliptic.
What is… a DEX? 1.10.2022. [Viitattu 27.4.2024] Saatavilla: https://www.elliptic.co/blockchain-basics/what-is-a-dex

Eromäki, Veikko
Maailman suurimman kryptopörssin toimitusjohtaja eroaa – myöntää laiminlyönnit rahanpesun estämisessä. Yle 22.11.2023. [Viitattu 9.3.204] Saatavissa: https://yle.fi/a/74-20008814/64-3-193127

Europol.
European Financial And Economic Crime Threat Assessment 2023. [Viitattu 1.5.2024] Saatavilla: https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf

Finanssivalvonta.
Mitä tarkoittaa virtuaalivaluutta, kryptovaluutta, kryptovara, ICO tai lompakkopalvelu? 17.10.2019. [Viitattu 10.3.2024] Saatavissa: https://www.finanssivalvonta.fi/kuluttajansuoja/virtuaalivaluutat/

Forbes.
Cryptocurrency Prices Today By Market Cap. [Viitattu 10.3.2024] Saatavilla: https://www.forbes.com/digital-assets/crypto-prices/?sh=ae3911524785

Forrester Research.
True Cost of Financial Crime Compliance Study – Europe, The Middle East and Africa 2023. [Viitattu 26.4.2024] Saatavilla: https://risk.lexisnexis.com/global/en/about-us/press-room/press-release/20240306-true-cost-of-compliance-emea

Jones, How
Tougher EU money laundering rules target crypto and oligarchs"favourite toys'. Reuters 18.1.2024. [Viitattu 9.3.2024] Saatavilla: https://www.reuters.com/markets/currencies/eu-agrees-stricter-rules-combat-moneylaundering-capture-cryptoassets-2024-01-18/

Jussila, Janne.
OP: Rikolliset käyttävät kuumia bitcoin-markkinoita huijausten tehtailuun. Helsingin Sanomat 9.4.024. [Viitattu 11.5.2024] Saatavilla: https://www.hs.fi/talous/art-2000010347819.html

Korte, Henriikka.
Norjalais-miljonääriä epäiltiin vaimonsa murhasta – Poliisi päätti lopettaa tutkinnan. Helsingin Sanomat 26.4.2024. [Viitattu 11.5.2024] Saatavilla: https://www.hs.fi/ulkomaat/art-2000010387024.html

KPMG.

Financial Crimes in Digital Assets and Cryptocurrencies 2024. [Viitattu 1.5.2024] Saatavilla: https://kpmg.com/us/en/articles/2023/financial-crimes-in-digital-assets.html

Niemi, Liisa.
Bitcoin jälleen uuteen ennätykseen: Arvo nousi yli 71 000 dollariin. Helsingin Sanomat 11.3.2024. [Viitattu 11.5.2024] Saatavilla: https://www.hs.fi/talous/art-2000010286005.html

OP Ryhmä.
Talousrikollisuuden torjunta. [Viitattu 30.4.2024] Saatavilla: https://www.op.fi/op-ryhma/tietoa-ryhmasta/talousrikollisuuden-torjunta

Pietarinen, Harri
Bitcoin hiipii kohti uutta ennätystä, nyt arvo nousi jo 65 000 dollariin. Helsingin Sanomat 4.3.2024. [Viitattu 9.3.204] Saatavilla: https://www.hs.fi/talous/art-2000010269400.html

Pietiläinen, Tuomo
Osuuspankki alkoi äkisti irti-sanoa haamu-asiakkaitaan, kun valvoja aloitti tarkastuksen. Helsingin Sanomat 27.8.2023. [Viitattu 30.4.2024] Saatavilla: https://www.hs.fi/talous/art-2000009772463.html

Räisänen, Perttu.
Bitcoin-etf:t saivat lentävän lähdön – Osa varainhoitajista jätti sijoittajat rannalle. Kauppalehti 12.1.2024. [Viitattu 15.5.2024] Saatavilla: https://www.kauppalehti.fi/uutiset/bitcoin-etft-saivat-lentavan-lahdon-osa-varainhoitajista-jatti-sijoittajat-rannalle/3dedfbad-f2f3-4e37-bb75-7b827735dba6

Salaterä, Jalmari
Valamiehistö totesi kryptohuijari Sam Bankman-Friedin syylliseksi. Yle 3.11.2023. [Viitattu 9.3.2024] Saatavissa: https://yle.fi/a/74-20008814/64-3-188380?utm_medium=social&utm_source=copy-link-share

Stanford University
How does blockchain work? [Viitattu 13.4.2024] Saatavissa: https://online.stanford.edu/how-does-blockchain-work

Statista. 2024.
Number of cryptocurrencies worldwide from 2013 to January 2024. [Viitattu 20.4.2024] Saatavissa: https://www-statista-com.libproxy.aalto.fi/statistics/863917/number-crypto-coins-tokens/

Storås, Niclas.
Internetin kartoittaja. Helsingin Sanomat 9.5.2024. [Viitattu 18.5.2024] Saatavilla https://www.hs.fi/visio/art-2000010363077.html

Tanninen, Tytti.
Uusi EU-asetus lisää asteittain valvontaa kryptovara-alalle. Finanssivalvonnan blogi 02/2023. [Viitattu 22.4.2024] Saatavissa: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2023/uusi-eu-asetus-lisaa-asteittain-valvontaa-kryptovara-alalle/

United Nations, Office on Drugs and Crime.
Money Laundering. [Viitattu 25.4.2024] Saatavissa: https://www.unodc.org/unodc/en/money-laundering/overview.html

U.S. Department of Justice. 2023.
Binance and CEO Plead Guilty to Federal Charges in $4B Resolution. [Viitattu 9.3.2024] Saatavissa: https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution

U.S. Immigration and Customs Enforcement. 2015.
Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website. [Viitattu 13.4.2024] Saatavissa: https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating

Valpola, Auli.
Bitcoin-etf:t saivat siunauksen USA:ssa – Näin maailman sijoittajat ja viranomaiset pyrkivät kiinni kryptovaluuttoihin. Kauppalehti 20.1.2024 [Viitattu 15.5.2024] Saatavilla: https://www.kauppalehti.fi/uutiset/bitcoin-etft-saivat-siunauksen-usassa-nain-maailman-sijoittajat-ja-viranomaiset-pyrkivat-kiinni-kryptovaluuttoihin/cd2707f3-42b2-4f8f-a928-e0dac1bbbd3a

Washington state department of financial institutions.
Virtual Currency, Cryptocurrency, and Digital Assets Primer. [Viitattu 21.4.2024] Saatavissa: https://dfi.wa.gov/consumers/virtual-currency/primer

Yle.
Analyysi: Nordea ummisti silmänsä rahanpesulta vuosikausia – jättimäinen sisäinen selvitys tehtiin vasta, kun pankki luopui Baltian-toimistaan, 13.6.2022. [Viitattu 30.4.3024] Saatavilla: https://yle.fi/a/3-12475350

Yle.

Suomesta värvätään "muuleja" rahanpesuun, 25.3.2011 päivitetty 6.4.2012. [Viitattu 30.4.2024] Saatavilla: https://yle.fi/a/3-5331600

Lyhenteet

AML/CTF	Rahanpesun ja terrorismin rahoittamisen estäminen
AMLA	EU AML Authority
EBA/EPV	Euroopan pankkiviranomainen
EKP	Euroopan keskuspankki
EU	Euroopan unioni
ESMA	Euroopan arvopaperimarkkinaviranomainen
FATF	Rahanpesun ja terrorismin rahoittamisen vastainen toimintaryhmä, Financial Action Task Force
HE	Hallituksen esitys
HMT	His Majesty's Treasury
KYC	Asiakkaan tunteminen
MiCA	Asetus (EU) 2023/1114 kryptovarojen markkinoista
OECD	Taloudellisen yhteistyön ja kehityksen järjestö, Organisation for Economic Co-operation and Development
OFAC	The United States Department of the Treasury's Office of Foreign Assets Control
PEP	Politically exposed person, poliittisesti vaikutusvaltainen henkilö
UN	United Nations, Yhdistyneet Kansakunnat

1 Johdanto

1.1 Aiheen tausta ja merkitys

Harva on todennäköisesti pystynyt välttämään uutisointia kryptovaroista, niihin liittyvästä rikollisuudesta tai kryptovaluuttojen arvonnousuista sekä -laskuista. On sitten kyse Bitcoin-huijausten yleistymisestä[1], Norjalaismiljonäärin kidnapatun vaimon lunnaista[2] tai Bitcoinin arvon 70 % noususta alkuvuodesta 2024[3] ovat uutispalvelut täyttyneet kryptovaroihin liittyvistä uutisista. Tämä kertoo markkinan laajasta kasvusta niin hyvässä kuin pahassa.

Kryptovarojen markkinoiden kasvusta ei kerro pelkästään viimeaikainen uutisointi. Virtuaalivaluuttojen markkina-arvo koko maailmassa oli maaliskuussa 2024 noin 2,77 biljoonaa dollaria (noin 2,53 biljoonaa euroa).[4] Kyseessä on siis merkittävä markkina monellakin mittarilla. Vertailukohteena voidaan tarkastella esimerkiksi Nasdaq Helsingin markkina-arvoa, joka ilmoitettiin tammikuussa 2024 olevan noin 260 miljardia euroa.[5]

Virtuaalivaluutat ja kryptovarat yleisesti ovat yleistyneet ja niihin kohdistuu kasvavia riskejä. FATF:n eli Financial Action Task Force on määrittelyt, että kryptovarat toimialana on erityisen riskialtis. Alaan liittyy paljon riskejä koskien anonymiteettiä ja monenlaisia rahanpesun ja terrorismin rahoittamiseen, huijauksiin (fraud) ja markkinamanipulointiin liittyen.[6]

Kryptovaluutat voivat mahdollistaa laittomien tuotteiden ostamisen anonyymisti erilaisilta verkkoalustoilta tavallisen fiat-valuutan sijaan. Esimerkiksi Silk Road oli tunnettu verkkosivu, joka mahdollisti laittomien tuotteiden ostamisen hyödyntämällä kryptovaluutta Bitcoinia. Bitcoinin käyttö laittomien tuotteiden ostamisessa oli houkuttelevaa, sillä ajateltiin, ettei Bitcoinin käytön myötä varoja voida jäljittää. Tapauksessa kuitenkin FBI kykeni jäljittämään Bitcoin-siirtoja ja myöhemmin tapaus päättyi verkkosivuston sulkemiseen ja rikostuomioihin.[7]

Vaikka kryptovaroja on hyödynnetty rikoksiin, on kuitenkin tärkeää huomioida myös kryptovarojen tuomat edut. Kryptovarat tuovat mahdollisuuksia toteuttaa transaktioita helpommin, halvemmalla ja nopeammin. Uusia mahdollisuuksia tuo juuri taustalla toimiva lohkoketjuteknologia, jonka keskeiset

[1] Jussila 2024.
[2] Korte 2024.
[3] Niemi 2024.
[4] Forbes 2024.
[5] Ceicdata 2024.
[6] FATF 2021, s. 7.
[7] U.S. Immigration and Customs Enforcement 2015.

hyödyt liittyvät erityisesti läpinäkyvyyteen ja tehokkuuteen. Transaktiot ovat todennettavissa ja jäljitettävissä. Lohkoketjuteknologiaa voidaan myös hyödyntää erilaisissa älysopimuksissa ja toimitusketjun seurannassa. [8]

Globaali trendi kryptovarojen yleistymisestä näkyy myös Suomessa. Verohallinnon kyselyn mukaan covid-19 pandemian aikana kryptomarkkinat kasvoivat lisää Suomessa. Ulkomaisten neo-pankkien hyödyntäminen virtuaalivaluuttojen transaktioissa on myös lisääntynyt, joka vaikeuttaa rahanpesun estämistä. Ongelmana on se, että maksujen välillä ei välttämättä ole ollenkaan kolmatta osapuolta, jota velvoittaisi epäilyttävien liiketoimien valvonta.[9]

Lisääntyneistä riskeistä kertoo myös rahanpesun selvittelykeskukselle tulleet rahanpesuilmoitukset. Rahanpesun selvittelykeskuksen mukaan heille vuonna 2022 tulleista rahanpesuilmoituksista noin reilu kolmannes koski virtuaalivaluuttoja.[10]

Kryptovaroihin liittyy myös lisääntynyt erilaisten huijausten riski. Europolin selvityksen mukaan Euroopassa suurin osa sijoitushuijauksista liittyy juuri virtuaalivaluuttoihin. Suomessa virtuaalivaluuttoihin liittyvien huijausten vahinkojen arvo on ollut jopa yli miljoona euroa.[11] Valuuttojen nopeaa arvonnousua on myös hyödynnetty huijauksissa, jolloin ihmisille luvataan ennätyksellisiä voittoja, sillä huijauksen tekijät voivat todistaa markkinoiden nopean kasvun. Todellisuudessa kuitenkin varat menevät huijauksen tekijöiden omiin kryptolompakkoihin.[12]

Kryptovarayhtiöt ja niiden johtajat ovat olleet myös useasti otsikoissa viime vuosina ei niin mairittelevista syistä. Marraskuussa 2023 otsikoihin päätyivät FTX:n Sam Bankman-Fried talousrikosten takia[13] sekä maailman suurimman kryptopörssin Binancen toimitusjohtaja Changpeng Zhao rahanpesun estämisen laiminlyönneistä[14]. Lisäksi maaliskuussa 2024 uutisoitiin kryptovaluutta Bitcoinin kurssin nousseen ennätyslukemiin.[15]

Erityisesti Binancen rahanpesun estämisen laiminlyönneistä aiheutuneita 4,3 miljardin dollarin sakkoja voidaan pitää merkittävänä kohtana virtuaalivaluuttatoimijoiden sääntelyssä. Binance ja Changpeng myönsivät

[8] Stanford University.
[9] Vero.fi 2023; Valtionvarainministeriö 2024, s. 79.
[10] Rahanpesun selvittelykeskus 2022, s.11
[11] Valtionvarainministeriö a 2023, s. 79.
[12] Jussila 2024.
[13] Salaterä 2023.
[14] Eromäki 2023.
[15] Pietarinen 2024.

syyllistyneensä rahanpesun estämisen laiminlyöntiin sekä taloudellisten pakotteiden noudattamisen laiminlyöntiin.[16] Nämä uutiset kertovat siitä, kuinka volatiili ja altis markkina on muutoksille sekä siitä, kuinka kryptovaroja on mahdollista hyödyntää rahanpesussa, terrorismin rahoituksessa sekä finanssipakotteiden kiertämisessä ja kuinka tällaista toimintaa aktiivisesti harjoitetaan.

Korkeasta rahanpesuriskistä kertoo myös virtuaalivaluuttojen lisääntynyt sääntely. Vuoden 2024 alussa kerrottiin sisältöä EU:n tulevista rahanpesun estämisen säädöksistä, jotka ottavat tarkemmin kantaa myös virtuaalivaluuttoihin.[17]

Säädösten tarkoitus on lisätä suurin osa kryptoalasta mukaan tiukennetun sääntelyn piiriin, joiden tulee noudattaa asiakkaan tuntemisvelvollisuutta. Komission tavoite on saada kryptovarasiirroista jäljitettäviä ja avoimempia.[18]

Lainsäätäjien sääntelytarpeet ovat edellä mainittujen uutisten ja rahanpesuriskien valossa ymmärrettäviä mutta haasteita sääntelyn toteutumiseen aiheuttavat kryptovarojen taustalla oleva toimintalogiikka ja ajatus toimimisesta ilman keskuspankkia tai yksittäistä hallintoelintä.[19] Tarve säännellä kryptovaroja ja luoda kontrolleja asiakkaiden tunnistamiseen ja siirtojen jäljittämiseen on ristiriidassa kryptovarojen taustalla toimivan ideologian kanssa, joka varmasti haastaa myös lainsäätäjiä.

Kryptovarojen ajankohtaisuuden lisäksi myös lisäykset EU:n tasolla rahanpesun ja terrorismin rahoittamisen sekä pakotteiden hallinnan sääntelyyn luovat lisää mielenkiintoa aihetta kohtaan. Uuden rahanpesuasetuksen ja rahanpesudirektiivin on tarkoitus yhtenäistää rahanpesun ja terrorismin rahoittamisen estämisen sääntelyä EU:ssa, parantaa organisointia jäsenmaissa sekä luoda myös uusi valvontaviranomainen AMLA. [20]

Uudet lisäykset ja panostukset rahanpesun torjuntaan ja valvontaan kertovat tarpeesta säännellä kryptovaroja tarkemmin EU:n sisällä. Rahanpesun ja terrorismin rahoittamisen uhka on todellinen ja siitä nousevia riskejä hallitakseen on tarvetta luoda uusia säädöksiä myös uusia teknologioita ja innovaatioita kohtaan, joiden katsotaan sisältävän korkean riskin. On siis tärkeää tutkia sitä, millaista sääntelyä aihepiiriin liittyy sekä miten se mahdollisesti tulee tulevaisuudessa muuttumaan. Lisäksi uudet säädökset koskevat

[16] U.S. Department of Justice. 2023.
[17] Jones, 2024.
[18] Eurooppa-neuvosto, 2024.
[19] Finanssivalvonta, 2019.
[20] Eurooppa-neuvosto, 2024.

erityisesti pankkeja, joten on mielekästä tarkentaa huomiota siihen, millä tavoin pankit voivat näitä riskejä hallita.

Tämän työn tarkoituksena onkin selvittää tarkemmin kryptovarojen toimintaa, niihin liittyvää sääntelyä sekä rahanpesuriskejä. Lisäksi työssä pyritään selvittämään, miten finanssijärjestelmä voi tukea lainsäätäjien tavoitteita ja kuinka erityisesti pankkien riskienhallintafunktio voi olla osana kryptovarojen rahanpesuriskien estämisessä.

1.2 Tutkimuskysymykset ja rajaukset

Tämän tutkielman tarkoituksena on ymmärtää, millaista sääntelyä kryptovaroihin kohdistuu tällä hetkellä EU:ssa ja kuinka sääntely on muuttumassa. Lisäksi työssä on tarkoitus selvittää, millaisia rahanpesuriskejä kryptovarat tuovat finanssialan yrityksille ja kuinka niitä on mahdollista hallita.

Tämän tutkielman päätehtävänä on vastata neljään tutkimuskysymykseen:

1. *Millä tavoin kryptovaroja säännellään tällä hetkellä Euroopassa ja mitä haasteita sääntelyyn liittyy?*
2. *Miten kryptovaroja koskeva sääntely tulee Euroopassa muuttumaan?*
3. *Millaisia riskejä kryptovarat tuovat rahanpesun ja terrorismin rahoittamisen näkökulmasta pankeille?*
4. *Miten kryptovarojen rahanpesuriskiä voidaan hallita lainsäädännön sekä pankkien riskienhallinnan kautta?*

Ensimmäisen kysymyksen avulla on tarkoitus selvittää millainen sääntelykehikko kryptovaroja koskien on tällä hetkellä voimassa EU:ssa ja mitkä asiat tuovat siihen haasteita. Toisen kysymyksen avulla työssä paneudutaan sääntelyn tulevaisuuteen. Tulevaisuuden sääntelyn osalta erityisesti käsitellään Markets in Crypto Assets -asetusta sekä Maksun tiedot -asetusta.

Kolmas kysymys kohdistaa katseet pankkeihin ja erityisesti pankkeihin kohdistuviin riskeihin kryptovarojen suhteen. Kolmannen kysymyksen kohdalla paneudutaan lisäksi tarkemmin siihen, mitä rahanpesulla ja terrorismin rahoittamisella tarkoitetaan ja mitä sääntelyä aihepiiriin liittyy.

Neljännen kysymyksen avulla tutkitaan sitä, miten kryptovarojen luomaa rahanpesuriskiä voitaisiin hallita lainsäädännöllisesti tulevaisuudessa sekä miten pankit voisivat muokata riskienhallinnallisia lähestymistapoja tulevaisuudessa kryptovarojen suhteen.

Tutkielma on rajattu koskemaan sääntelyä EU:n tasolla, sillä relevantein ja tuorein lainsäädäntö liittyy juuri EU:n sääntelypaketteihin. Työssä kuitenkin käytetään esimerkkejä Yhdysvaltojen viranomaisista ja heidän toiminnastaan, mutta työ on rajattu koskemaan sääntelyä EU:ssa sekä Suomessa. Pankkien riskienhallinnan kehikko on kansainvälinen mutta sovellukset ja ehdotuksen on eritoten rajattu koskemaan eurooppalaisia ja erityisesti suomalaisia pankkeja sääntelyn ja markkinoiden vuoksi.

1.3 Metodit ja keskeiset lähteet

Oikeustieteessä metodi voidaan tulkita oikeuden näkökulmaksi.[21] Metodit kertovat tavoista hankkia ja analysoida tieteellistä tietoa. Metodeja käytetään siis tieteellisenä tutkimusmenetelmänä. Metodit toimivat tutkijan apuna tiedon hankkimiseen, muodostamiseen ja perustelemiseen.[22] Voisi siis sanoa, että metodit antavat tutkijalle keinoja etsiä lopputulosta.

Tässä tutkielmassa pääasiallisena metodina käytetään lainoppia eli oikeusdogmatiikka. Lainoppi metodina pyrkii systematisoimaan ja käsitteellistämään voimassa olevaa oikeutta.[23] Lainoppi tutkii voimassa olevaa oikeutta, jota se pyrkii systematisoimaan ja tulkitsemaan.[24] Koska tutkielma käsittelee pääasiassa EU-oikeutta, käytetään lainoppia selvittämään voimassa olevan oikeuden tarkoitusperiä. Lainopillisessa tutkimuksessa käytetään erilaisia tulkintamenetelmiä, joista yleisesti EU-oikeuden parissa käytetään tarkoitusperäopillista tulkintaa.[25]

Tutkielman tarkoitus on tulkita voimassa olevaa lainsäädäntöä de lege lata – tutkimuksena, jonka tarkoitus on pohtia voimassa olevaa lainsäädäntöä sekä sen tarkoituksenmukaisuutta. Lainsäädäntö liittyen kryptovaroihin on kuitenkin tuoretta ja aihepiiriin on odotettavissa uusia lainsäädännöllisiä uudistuksia, joten työssä pohditaan myös tulevaa lainsäädäntöä, jolloin kyse on de lege ferenda – tutkimuksesta.

Kalle Määttä huomauttaa teoksessaan *Oikeustaloustieteen perusteet,* että myös tulevaa lainsäädäntöä tulkitseva oikeustieteellinen de lege ferenda – tutkimus voi olla lainopillisin metodein toteutettu.[26] Lisäksi on huomioitava, että de lege ferenda – tutkimus voidaan nähdä yhteiskunnallisten ongelmien

[21] Aarnio 2005, s. 237.
[22] Hirvonen 2011, s. 4.
[23] Letto-Vanamo 2020, s. 77.
[24] Hirvonen 2011, s. 22.
[25] Ibid, s. 40.
[26] Määttä 2016, s. 65.

ratkaisemisena oikeudellisin keinoin.[27] Toisin sanoen, de lege ferenda – tutkimus ei kaikissa tapauksissa tulkitse tulevaa lainsäädäntöä tai anna lainsäätäjille kehitysehdotuksia vaan tutkimuksen sisältö voi myös keskittyä jonkin ongelman, tässä tilanteessa kryptovarojen tuomien rahanpesuriskien hallinnan haasteiden, ratkaisemiseen oikeudellisin keinoin.

Tämän tutkielman tarkoituksena on systematisoida ja tulkita kryptovaroihin kohdistuvaa sääntelyä tällä hetkellä sekä sen tulevaisuutta ja lisäksi havainnoida sääntelyn edellyttämiä muutoksia finanssialan yritysten riskienhallinnassa. Metodini on *oikeusdogmaattinen* eli lainopillinen.

Keskeisinä lähteinä tutkielmassa toimivat EU-direktiivit sekä asetukset ja kotimaiset hallituksen esitykset sekä erinäiset kirjallisuuslähteet Suomesta ja ulkomailta. Lisäksi tutkielman lähteinä toimivat erilaisten valvovien viranomaisten sekä erilaisten toimielimien niin EU:ssa kuin Suomessa antamat tulkinnat ja ohjeet sekä määräykset.

Aihepiiri on tuore, joten kotimaista tieteellistä kirjallisuutta aiheen ympärille ei ole paljon rakentunut, joten työssä hyödynnetään pääosin ulkomaista kirjallisuutta sekä tuoreita artikkeleita. Rahanpesun kontekstissa kirjallisuuden osalta on hyödynnetty niin ulkomaista kuin kotimaista kirjallisuutta. Lisäksi aiheen tuoreuden myötä työssä on hyödynnetty aiheen asiantuntijapalveluita tarjoavien yhtiöiden raportteja ja artikkeleita, jotta voidaan taata tutkielman tuoreus.

1.4 Tutkimuksen rakenne

Tutkielma on rajattu kahdeksaan eri osaan. Ensimmäisessä luvussa avataan työn taustoja, tutkimuskysymyksiä sekä tutkimuksen metodeja ja käsitellään työn osalta keskeiset käsitteet.

Toisessa luvussa käsitellään tarkemmin kryptovarojen taustalla toimivan lohkoketjuteknologian toimintaperiaatteita sekä eri käyttötarkoituksia. Lisäksi luvussa on avattu tarkemmin erilaisia kryptovaroja ja niiden toimintaperiaatteita sekä määrittelyjä.

Kolmas luku keskittyy tarkastelemaan kryptovaroihin liittyvää sääntelyä nykyhetkessä sekä sääntelyyn tulevia muutoksia tulevaisuudessa. Kappaleessa käsitellään sääntelyä EU:n tasolla sekä kansallisella tasolla.

[27] Leskinen 2002, s. 1164.

Neljäs luku avaa tarkemmin puolestaan rahanpesun estämisen kokonaisuutta määrittelemällä rahanpesua sekä siihen liitännäisiä teemoja. Lisäksi luvussa käsitellään rahanpesunsääntelyn kokonaisuutta EU:ssa ja Suomessa.

Tutkielman viides luku syventyy tarkastelemaan pankkien riskienhallinnan kehikkoa ja kuudennessa luvussa käsitellään kryptovarojen hyödyntämistä rahanpesussa.

Lopuksi seitsemäs luku vastaa tarkemmin rahanpesun sääntelyn haasteisiin sekä niiden ratkaisuihin ja kahdeksannessa luvussa käsitellään vastauksia tutkimuskysymyksiin.

1.5 Keskeisiä käsitteitä

Virtuaali- tai kryptovaluutat on määritelty virtuaalivaluuttojen tarjoajista annetun lain (26.4.2019/572) 2§:ssä sekä rahanpesudirektiivin (EU 2015/849) kolmannessa artiklassa, jonka mukaan virtuaalivaluutat ovat digitaalisessa muodossa olevaa arvoa, niitä ei ole laskettu liikkeelle keskuspankin tai muun viranomaisen toimesta eivätkä ne toimi laillisena maksuvälineenä. Niitä voidaan kuitenkin käyttää maksuvälineenä ja siirtää, vaihtaa ja tallentaa sekä myydä sähköisesti. Virtuaalivaluutoilla ei ole EU:ssa samaa asemaa kuin fiat-rahalla.

Fiat-rahalla viitataan yleisesti esimerkiksi jonkun valtion liikkeeseen laskemaan rahaan, joka toimii vaihdannan välineenä. Fiat-rahaa on esimerkiksi euron kolikot ja setelit. Virtuaalivaluutat erotellaan fiat-rahasta. [28]

Virtuaalivaluuttojen lisäksi puhutaan nykyään yleisemmin **virtuaali- ja kryptovaroista**. FATF käyttää myös termiä virtual assets (virtuaalivarat), jotka ovat digitaalisessa muodossa olevaa arvoa, jolla voidaan käydä kauppaa, jota voidaan siirtää ja käyttää maksuvälineenä. [29] MiCA-asetuksen (Markets in Crypto Assets) (EU) 2023/1114 kolmannen artiklan määritelmissä käytetään myös termiä kryptovara, joka on vakiinnuttanut virtuaali- ja kryptovara termien käyttöä. Tässä työssä käytetään termejä virtuaalivaluutta ja kryptovara. Virtuaalivaluutta-termiä käytetään erityisesti silloin, kun halutaan kohdistaa huomio juuri valuuttoina toimiviin virtuaalivaroihin. Yleisesti aiheesta puhuttaessa käytetään termiä kryptovara, joka on tällä hetkellä vakiintuneempi termi kuvaamaan kaikkia erilaisia kryptovaroja.

[28] FAFT 2014, s. 4.
[29] FATF 2023, s. 137.

AML/CTF = Anti money laundering eli rahanpesun estäminen ja counter terrorism financing eli terrorismin rahoituksen estäminen. Lyhenteitä käytetään yleisesti viittaamaan rahanpesun ja terrorismin rahoituksen estämisen toimiin.

FATF eli Financial Action Task Force on itsenäinen elin, joka toimii OECD:n alaisuudessa. FATF tutkii rahanpesua ja terrorismin rahoittamisen estämistä, julkaisee erilaisia toimintaohjeita sekä suosituksia ja tulkitsee, millä tavoin valtiot noudattavat rahanpesun ja terrorismin rahoittamisen estämistä. [30]

Pakotteilla tarkoitetaan poliittisia toimia ja päätöksiä, joiden tarkoitus on estää esimerkiksi taloudellinen yhteistyö toisen valtion tai jonkun toimijan kanssa. Pakotteita asetetaan tahoille, joiden katsotaan vaarantavan kansallista tai kansainvälistä turvallisuutta ja rauhaa. Pakoteohjelmat voivat sisältää esimerkiksi vienti- ja tuontipakotteita, finanssipalveluiden tarjoamisen rajoittamista sekä varojen jäädytyspäätöksiä. Suomessa tulee noudattaa YK:n ja EU:n pakotelistoja mutta myös OFAC:n pakotelistauksia voidaan katsoa noudatettavan myös Suomessa. Lisäksi myös Iso-Britannian HMT-pakotelistaus on merkittävä Euroopassa.[31]

[30] FATF, what we do.
[31] Pursiainen 2021, s. 21–29, 117–123, 190.

2 Lohkoketjut ja kryptovarat

Jotta voidaan ymmärtää kryptovarojen toimintaa, tulee hahmottaa perusperiaatteet lohkoketjuteknologiasta. Tässä työssä ei ole tarkoitus tarkastella lohkoketjuteknologiaa teknisestä näkökulmasta vaan selventää sen toimintalogiikkaa sekä sen tarjoamia mahdollisuuksia ja uhkia yleisellä tasolla.

Tässä kappaleessa selvennetään toimintalogiikkaa erilaisten kryptovarojen sekä virtuaalivaluuttojen taustalla ja lohkoketjuteknologioiden tuomia muita mahdollisuuksia erityisesti finanssisektorilla. Lisäksi tarkastellaan lohkoketjuteknologioiden käyttötarkoituksia.

2.1 Lohkoketjuteknologian keskeiset periaatteet

Lohkoketjuteknologiaa on verrattu innovaationa jopa internetiin ja on arvioitu, että se tulisi muuttamaan maailmaa ehkäpä enemmän kuin internet aikoinaan. Lisäksi esimerkiksi Kiinassa on arvioitu lohkoketjun taloudellisen arvon olevan paljon korkeampi kuin internetin, jopa yli kymmenkertainen.[32]

Aihepiiri sai paljon huomiota ja kiinnostusta, kun vuonna 2008 nimimerkki Satoshi Nakamoto julkaisi kirjoituksensa, jossa kuvattiin uutta Bitcoin-järjestelmää. Kirjoituksessa käytännössä kuvattiin hajautettua lohkoketjujärjestelmää, joka mahdollistaa varojen siirrot ilman rahoituslaitoksia tai muita välikäsiä. [33] Kuitenkaan Nakamoto ei käyttänyt termiä lohkoketju kirjoituksessaan vaan hän puhui datalohkoista (*engl. chain of blocks*). Artikkelissa kuvataan rakennetta, joka on sarja datalohkoja, jotka ovat kryptografisesti ketjutettu digitaaliseksi ketjuksi.[34] Nakamoton kirjoituksella on kuitenkin ollut valtava merkitys lohkoketjuteknologian ja kryptovarojen kehittymiselle.[35]

Voidaan myös katsoa, että vuoden 2008 finanssikriisillä oli merkittävä vaikutus vaihtoehtoisen varojensiirtojärjestelmän kehittämiselle. Ihmisiltä oli kadonnut usko finanssijärjestelmään ja sen suuriin toimijoihin, ja he kaipasivat vaihtoehtoja perinteiselle järjestelmälle. Erityisesti lohkoketjujärjestelmän läpinäkyvyys kiinnosti monia ja erotti sen perinteisestä pankkijärjestelmästä.[36]

[32] Eerola ym. 2019, kappale 1.0.2.
[33] Nakamoto, 2018.
[34] Lauslahti – Mattila – Seppälä 2016, s. 3.
[35] Eerola ym. 2019, kappale 1.0.1.
[36] Ibid.

Lohkoketjuista käytetään myös ajoittain termiä hajautetun tilikirjan teknologia eli DLT (*engl. Distributed Ledger Technology*). Yleisellä tasolla molemmilla termeillä tarkoitetaan samaa teknologiaa.[37] Tulee kuitenkin huomata, että teknisesti lohkoketjut ovat aina hajautettuja tilikirjoja mutta kaikki hajautetut tilikirjat eivät kuitenkaan ole aina lohkoketjuja. [38]

Yksinkertaistettuna, lohkoketjun voi ajatella olevan tilikirja digitaalisessa muodossa, johon merkataan aikajärjestyksessä tapahtuvia tapahtumia. Transaktiot eli tapahtumat muodostavat lohkoja, jotka sitten yhdistetään toisiinsa liittämällä ne kryptografisesti yhteen ketjuttamalla. On kuitenkin huomioitava, että kaikki lohkoketjujärjestelmät eivät välttämättä tuota lohkoja. Tämän vuoksi termi hajautetun tilikirjan teknologia voi kuvata järjestelmiä paremmin.[39] Lisäksi eroavaisuuksia on siinä, että hajautetut tilikirjat eivät välttämättä kasva lohkojen avulla suuremmiksi. On olemassa hajautettuja tilikirjoja, jotka eivät käytä toiminnassaan lohkoja.[40]

Akateemisessa ympäristössä lohkoketjuteknologia ja siihen liittyvä terminologia ei ole täysin vakiintunut eikä sitä ole tarkasti määritelty.[41] Lohkoketjuteknologia mahdollistaa mm. virtuaalivaluuttojen toiminnan mutta teknologiaa voidaan hyödyntää myös paljon muuhun. Teknologian ydinidea on uudenlainen tapa tallentaa erilaista dataa varmalla ja luotettavalla tavalla.[42]

Yksi tapa määritellä lohkoketju on ajatella lohkoketjua transaktioiden tallentamisena siten, että kaikki sitä käyttävät ovat yhtä mieltä transaktioista, siis siitä, mitä on tapahtunut ja millaisessa järjestyksessä. Tähän tietokantaan tallennetaan tiedot transaktioista, joita ei voi muokata enää tallentamisen jälkeen.[43]

Tämän lisäksi voidaan ajatella, että lohkoketju on luotettava julkinen rekisteri erilaisista tapahtumista. Luotettavuus ei tarkoita sitä, että mukana tulisi olla jokin virallinen instituutio tai järjestö vaan luotettavuus taataan matemaattisesti. Merkintöjen tekemiseen tarvitaan kaikkien mukana olevien toimijoiden yhteisymmärrys ja enemmistön hyväksyntä. Järjestelmän luotettavuus perustuu siis matemaattisiin sääntöihin ja erilaisiin salausjärjestelmiin.[44]

---

[37] Eerola ym. 2019, kappale 1.0.2.
[38] Bashir 2018, s. 31.
[39] Eerola ym. 2019, kappale 1.0.2.
[40] Bashir 2018, s.31.
[41] Mattila 2021, s. 12.
[42] Eerola ym. 2019, kappale 1.0.2.
[43] Ibid.
[44] Ibid.

Edellä kuvatun lisäksi lohkoketjuteknologia sisältää erilaisia piirteitä, joiden takia sitä pidetään mullistavana ideana. Tärkeimmät ja houkuttelevimmat piirteet lohkoketjuteknologiassa voidaan jakaa neljään osaan:

1. Avoin lähdekirja
2. Vertaisverkko (*engl. peer-to-peer*)
3. Kryptografiset salausmenetelmät
4. Konsensusalgoritmit[45]

Edellä mainitut piirteet luovat lohkoketjuille niiden vahvan salauksen ja hajautetun luonteen sekä erityisesti luotettavuuden ja tietojen yhteisyyden periaatteet. Näiden eri ominaisuuksien ansioista lohkoketjuja voidaan käyttää moneen eri tarkoitukseen, kuten älysopimuksiin tai kryptovaluuttoihin.[46]

2.1.1 Lohkoketjujen toiminta

Lohkoketjujen yksi tärkeimmistä osista ovat hajautetut tilikirjat (*engl. ledger*), joilla tarkoitetaan tapahtumarekisteriä. Tilikirjaan tallentuu tiedot kaikista tapahtumista eikä niitä voida enää jälkikäteen muuttaa. Tietoja voi myös kaikki verkon osapuolet tarkistaa reaaliaikaisesti.[47]

Tämän järjestelmän tarkoitus on varmistaa, että tallennettuja tietoja ei voida muuttaa enää jälkikäteen ja että verkostossa on konsensus tapahtumien oikeellisuudesta. Nämä periaatteet tuovat turvallisuutta ja läpinäkyvyyttä, joka luo järjestelmästä luotettavan ilman, että mukana tarvitsee olla viranomaisia tai muita välikäsiä.[48]

Lohkoketjut käyttävät konsensusalgoritmeja, joiden avulla varmistetaan, että verkosto on samaa mieltä ja tiedot voidaan tallentaa. Konsensusmekanismeja voi olla erilaisia eivätkä kaikki mekanismit sovi kaikkiin järjestelmiin. Yksi esimerkki konsensusalgoritmista on Bitcoinin käyttämä Proof-of-Work-algoritmi. Mekanismi perustuu sille, että tietty laskennallinen teho on käytetty ennen kuin verkostossa voidaan hyväksyä uuden arvon lisäys.[49]

Lohkoketjut käyttävät myös salakirjoitustekniikkaa eli kryptografiaa väärinkäytösten ja peukaloinnin estämiseksi. Kryptografian avulla voidaan datan luotettavuutta ja eheyttä sekä varmuutta.[50]

---

[45] Mattila 2021, s. 12.
[46] Eerola ym. 2019, kappale 1.0.2.
[47] Ibid.
[48] Bashir 2018, s. 17.
[49] Ibid.
[50] Eerola ym. 2019, kappale 1.0.3.

Louhinta on oleellinen prosessi, joka liittyy konsensusalgoritmeihin ja kryptografiaan. Louhijat ovat tärkeä osa verkon toimintaa. He käsittelevät tietojen syötteitä ja tapahtumia alustan käyttäjien välillä ja näin osallistuvat verkon konsensuksen eli yhteisymmärryksen muodostamisen prosessiin. He ratkaisevat erilaisia matemaattisia ongelmia ja antavat koneidensa laskentatehon käyttöön transaktioiden varmentamiseksi salausprosessissa, josta käytetään termiä hajautus (*engl. hashing*). Tällä tavoin toimii Proof-of-Work ja louhijoille annetaan tästä palkkioiksi louhimaansa valuuttaa.[51]

Bitcoin-järjestelmä käyttää tällaista louhintaprosessia. Louhijat ovat vapaaehtoisia noodeja ja heitä tarvitaan siihen, että lohkoihin voidaan lisätä lisää dataa ja että on mahdollista kytkeä lohkoja toisiinsa. Tulee kuitenkin huomata, että kaikki lohkoketjut eivät käytä tällaista toimintalogiikkaa ja säännöt määräävät sen, millä tavoin lohkoja lisätään ketjuun.[52]

Edellä mainitut noodit ovat puolestaan tietokoneita tai tietokoneohjelmistoja, jotka muodostavat itse lohkoketjuverkon. Noodeilla on tärkeä rooli, sillä ne ylläpitävät hajautettua tietokantaa. Noodit toimivat itsenäisesti muista riippumatta ja ne voivat olla täysiä tai osittaisia.[53] Noodit prosessoivat transaktioita ja niiden tarkoitus on ylläpitää lohkoketjun datasta olevia kopioita. Täysi noodi sisältää kaikki transaktiot, joita lohkoketjussa on suoritettu ja osittainen noodi voi sisältää vain osittaisen listan transaktioista.[54]

Lohkoketjujen lohkot sisältävät puolestaan dataa, esimerkiksi transaktiodataa, kuten Bitcoinissa. Yhteen lohkoon tallennetaan viimeisimmät lohkoketjuverkkoon lähetetyt tiedot, joita ei ole tallennettu aiemmin syntyneisiin lohkoihin. Lohkot sisältävät aina viitteen sitä edeltäneeseen lohkoon ja tällä tavoin ne muodostavat katkeamattoman ketjun. Lohkojen sisältö on aina salattu ja se on järjestetty tietynlaiseen muotoon.[55]

Kryptografinen salausjärjestelmä tekee lohkoketjuista luotettavia, sillä sen avulla pyritään luomaan järjestelmä, jota ei pysty peukaloimaan.[56] Julkisen avaimen salauksella suojataan sähköisen tiedon kulku erilaisissa järjestelmissä. Salaus toimii kahden avaimen järjestelmänä, toinen on julkinen ja toinen yksityinen avain ja ne muodostetaan parina. Julkinen avain voidaan julkaista kaikille mutta yksityinen tulisi pitää itsellään omana tietonaan. Yksityinen avain on henkilökohtainen avain, joka kuuluu vain omistajalleen.

[51] Mattila 2021, s. 154.
[52] Eerola ym. 2019, kappale 1.0.3.
[53] Mattila – Seppälä 2018, s. 190.
[54] Eerola ym. 2019, kappale 1.0.3.
[55] Ibid.
[56] Alman – Hirsh 2019, s. 36.

Yksityisellä avaimella salatut tiedot voidaan avata vain sen julkisella vastinparilla.[57]

Lohkoketjujen yksi tärkeimmistä ominaisuuksista on vertaisverkot (*engl. Peer-to-Peer*). Kuten aiemmin on jo tullut ilmi, lohkoketjut toimivat eri toimijoiden yhteistyössä. Osallistujat ovat tasa-arvoisia osallistuja verkon toiminnassa. Vertaisverkoissa osallistuja voi hyödyntää verkkoa mutta myös tuo siihen omia resurssejaan esimerkiksi tarjoamalla verkon käyttöön laskennallisia resurssejaan.[58] Tällä tavoin lohkoketjut voivat toimia jaettuna järjestelmänä ilman keskusviranomaisia.[59] Vertaisverkkojen avulla mahdollistetaan osallistujien transaktiot toisilleen ilman välikäsiä, esimerkiksi pankkeja.[60]

2.1.2 Julkiset ja yksityiset lohkoketjut

Lohkoketjut voivat olla julkisia tai yksityisiä. Esimerkiksi Bitcoin ja Ethereum ovat julkisia lohkoketjuja. Julkiset lohkoketjut ovat nimensä mukaisesti julkisia, kukaan tietty taho ei yksin omista niitä. Jokaisella on mahdollisuus osallistua noodina julkisen lohkoketjun päätöksentekoprosessiin.[61]

Julkisiin lohkoketjuihin voi siis kuka tahansa osallistua noodina, liittyä verkon jäseneksi, ylläpitää jaettua tilikirjaa ja osallistua konsensuksen ylläpitoon. Kenelläkään ei yksin ole valtaa hallita lohkoketjun toimintaa vaan julkiset lohkoketjut ovat hajautettuja.[62] Esimerkiksi Bitcoinia ylläpitää huhtikuussa 2024 noin 18700 noodia.[63]

Usein julkiset lohkoketjut hyödyntävät jotakin kannustinmekanismia, jotta saadaan uusia käyttäjiä liittymään mukaan. Noodeja saadaan mukaan ylläpitämään verkkoa, sillä heille luvataan esimerkiksi Bitcoinin ja Ethereumin osalta lohkoketjun sisäistä valuuttaa eli esimerkiksi Bitcoineja, jos he pitävät verkkoa toiminnassa varmistamalla transaktioita.[64]

Haasteita julkiset lohkoketjut kohtaavat siinä, että noodit ratkaisevat paljon resursseja vaativia ongelmia, jotta transaktiot voidaan varmistaa. Matemaattisten ongelmien ratkaisu on suhteellisen hidasta ja lohkoketjut eivät kykene

[57] Eerola ym. 2019, kappale 1.0.3.
[58] Ibid.
[59] Mattila – Seppälä 2018, s. 183.
[60] Bashir 2018, s. 16.
[61] Ibid.
[62] Eerola ym. 2019, kappale 1.0.2.
[63] Bitnodes 2024.
[64] Eerola ym. 2019, kappale 1.0.2.

varmistamaan suuria määriä transaktioita.[65] Tämä kuluttaa lisäksi suuria määriä sähköä. Cambridgen Yliopiston ylläpitämän laskurin ennusteen mukaan Bitcoin pelkästään kuluttaisi vuonna 2024 yhteensä 174,48 TWh sähköä. Se on enemmän kuin mitä koko Egyptin valtio kuluttaa vuodessa.[66]

Yksityiset lohkoketjut ovat tarkoitettu vain tunnistetuille osapuolille. Jotta järjestelmään pääsee, tulee osallistujan esimerkiksi varmentaa oma identiteetti tai saada kutsu. Yksityisen lohkoketjun perustaja voi asettaa erilaisia rajoja osallistujille sekä määrittää, millaisia transaktioita järjestelmässä voi tehdä tai ovatko transaktiot esimerkiksi julkisia transaktioon kuulumattomille osapuolille. Yksityisissä lohkoketjuissa ei välttämättä tule eksklusiivisuuden takia samanlaista ongelmaa konsensuksen saavuttamisessa kuin julkisissa lohkoketjuissa, sillä osallistujamäärän ollessa pienempi voidaan konsensus saavuttaa nopeammin ja silloin myös transaktiot toteutuisivat nopeammin.[67]

Teorian tasolla olemassa on myös puolittain yksityisiä lohkoketjuja. Näissä toiminta on jaettu yksityiseen ja julkiseen puoleen. Esimerkiksi louhinta voitaisiin ulkoistaa julkiselle puolelle ja samalla jokin yksityinen joukko kontrolloi verkostoa.[68]

2.2 Lohkoketjujen käyttötarkoitukset

Lohkoketjujen kehityksen alkuvuosina keskityttiin eniten erilaisten varojen tai tokeneiden (*engl. tokens)* tallentamiseen tai siirtämiseen järjestelmässä. Lohkoketjuja kuitenkin lähestyttiin myöhemmin erilaisesta näkökulmasta, jossa kiinnitettiin enemmän huomiota siihen, milloin ja miten tietyt tokenit pystyvät siirtymään lohkoketjujärjestelmässä tililtä toiselle. Hyödyntämällä Turing-täydellisiä ohjelmointikieliä voidaan luoda, säilyttää ja toteuttaa älysopimuksia lohkoketjussa.[69]

Älykkäät sopimukset eivät ole kuitenkaan mikään uusi lohkoketjuteknologian luoma keksintö vaan älykkäistä sopimuksista on puhunut ensimmäisen kerran Nick Szabo 1990-luvulla.[70]

Szabon mukaan älykkäät sopimukset ovat elektronisia transaktioprotokollia, jotka noudattavat sopimuksessa määriteltyjä ehtoja. Järjestelmän

[65] Eerola ym. 2019, kappale 1.2.
[66] Cambridge Bitcoin Electricity Consumption Index 2024.
[67] Eerola ym. 2019, kappale 1.0.3.
[68] Bashir 2018, s. 32.
[69] Mattila 2021, s. 12.
[70] Eerola ym. kappale 1.2.

tarkoituksena on vähentää välikäsiä ja estää vilpillisiä toimia.[71] Szabon idea on tuotu käytäntöön paljon hänen julkaisunsa jälkeen. Bitcoin esimerkiksi osittain hyödyntää älykkäiden sopimusten toiminnallisuuksia.[72]

Lohkoketjuteknologiaa voidaan hyödyntää muihinkin tarkoituksiin. Ethereumin avulla voidaan hyödyntää edellä mainittuja älysopimuksia, hajautettu rahoitus (*engl. decentralized finance, DeFi*) sekä NFT:t (*engl. non-fungible tokens)* kiinnostavat monia ja ovat saavuttanet paljon suosiota. Lisäksi tietenkin krypto- ja virtuaalivaluutat ja Metaversumit (*engl. Metaverse*) hyödyntävät lohkoketjuja.[73]

Lohkoketjuteknologiaa ja älykkäitä sopimuksia voidaan hyödyntää myös osana hajautettua rahoitusta. Vuoden 2023 elokuussa Euroopan arvopaperimarkkinaviranomainen, ESMA, arvioi hajautetun rahoituksen markkinaosuuden olevan noin 4 % koko kryptovaramarkkinasta.[74] Kyse ei ole siis tällä hetkellä vielä kovin suuresta ilmiöstä.

Hajautettua rahoitusta voidaan pitää uudenlaisena finanssijärjestelmänä, joka hyödyntää lohkoketjua ja älykkäitä sopimuksia, jolloin välikäsiä ei tarvita.[75] Kuitenkin hajautetusta rahoituksesta voidaan puhua myös silloin, kun mukana on jokin yksi taho, joka käyttää järjestelmässä merkittävää vaikutusvaltaa.[76]

Hajautetun rahoituksen avulla voidaan tuottaa perinteisesti pankkien tuottamia palveluita, mutta kaikki on rakennettu lohkoketjujen päälle. Hajautetun rahoituksen ominaisuuksina käyttäjät pystyvät hallitsemaan omia varojaan, kaikilla on mahdollisuus käyttää järjestelmää, yksittäinen taho ei kontrolloi järjestelmää tai sen tapahtumia, järjestelmän toiminta on läpinäkyvää ja kuka tahansa voi tehdä tarkastuksia ja järjestelmässä on mahdollista luoda uusia rahoitustuotteita.[77]

Vaikka hajautettu rahoitus ei ole vielä markkinaosuudeltaan suuri ilmiö, se aiheuttaa kuitenkin riskejä. Vastuun kohdentaminen on haastavaa ja mikäli esimerkiksi rahanpesun estämisen sääntelyn noudattamista ei voida kohdentaa kehenkään, se avaa riskejä systeemin hyödyntämiselle talousrikoksiin.[78]

---

[71] Szabo 1997.
[72] Bashir 2023, kappale 22.
[73] Ibid, kappale 1.
[74] Valtionvarainministeriö 2024, s. 77.
[75] Cawrey – Lantz 2022, kappale 7.
[76] Valtionvarainministeriö 2024, s. 77.
[77] Bashir 2023, kappale 21.
[78] Valtionvarainminsteriö 2024, s. 77.

Hajautettuun rahoitukseen liittyy myös kasvava ilmiö eli hajautetut pörssit, DEX:t (*engl. decentralized exchanges*). Hajautettujen pörssien suosio on ylittänyt sijoittajien transaktioiden määrän perusteella hajauttamattomien pörssien suosion viimeisen reilun vuoden aikana. Perinteisiä hajauttamattomia kryptopörssejä ovat esimerkiksi Binance ja Coinbase, joissa pystytään vaihtamaan esimerkiksi kryptovaroja fiat-valuuttaan.[79]

Hajautetut pörssit käyttävät apuna älysopimuksia ja itse pörssi ei ota haltuun missään vaiheessa itse varoja. Pörssin avulla on mahdollista tuoda yhteen tahot, jotka haluavat vaihtaa varoja keskenään ja se tapahtuu automaattisesti älysopimusten avulla. Hajautetuissa pörsseissä ei ole myöskään käytössä asiakkaan tuntemisen menetelmiä, jotka lisäävät pörssien riskejä.[80]

Lohkoketjujen ensimmäinen soveltaminen tapahtui virtuaalivaluutoilla. Bitcoin ensimmäisenä virtuaalivaluuttana jo vuonna 2008 loi tilaa myös muille tavoille hyödyntää lohkoketjuteknologiaa. Vuonna 2013 ensimmäisellä kolikkoannilla (*engl. ICO eli Initial Coin Offering*[81]) syntyi MasterCoin ja myöhemmin erittäin onnistuneen kolikkoannin seurauksena Ethereum.[82]

Kolikkoanteja verrataan usein listautumisantiin tai osakeantiin (IPO). Listautumisannin yhteydessä pörssiin listautuvan yhtiön osakkeet tulevat kaupankäynnin kohteiksi, kun he listaavat osakkeensa pörssiin. Tällä tavoin yhtiöt voivat esimerkiksi kasvattaa omaa pääomaansa. Kolikkoanti eroaa kuitenkin tässä suhteessa listautumisannista, sillä kolikkoannissa sijoittaja saa itselleen vain julkaistua virtuaalivaluuttaa tai poletteja itselleen, ei osuutta itse yhtiöstä.[83]

2.3 Kryptovarat

Kryptovaroihin liittyvä taksonomia ei ole yhdenmukainen ja terminologia muuttuu lisääntyvän lainsäädännön mukana ja markkinoiden muuttuessa. Tässä kappaleessa on tarkoitus syventyä siihen, mitä kryptovarat ovat ja selventää niihin liittyvää termistöä.

Suuri osa rahasta on tällä hetkellä jo sähköisessä muodossa, eli maailmantalous toimii jo pitkälti digitaalisessa muodossa olevalla rahalla. Sähköisessä muodossa olevaa fiat-valuuttaa ei kuitenkaan tule sekoittaa virtuaali- ja kryptovaluuttoihin.

---

[79] Elliptic 2022.
[80] Ibid.
[81] vrt. IPO eli Initial Public Offering eli listautumisanti
[82] Bashir, 2023, kappale 22.
[83] Eerola ym. 2019, kappale 1.2.3.

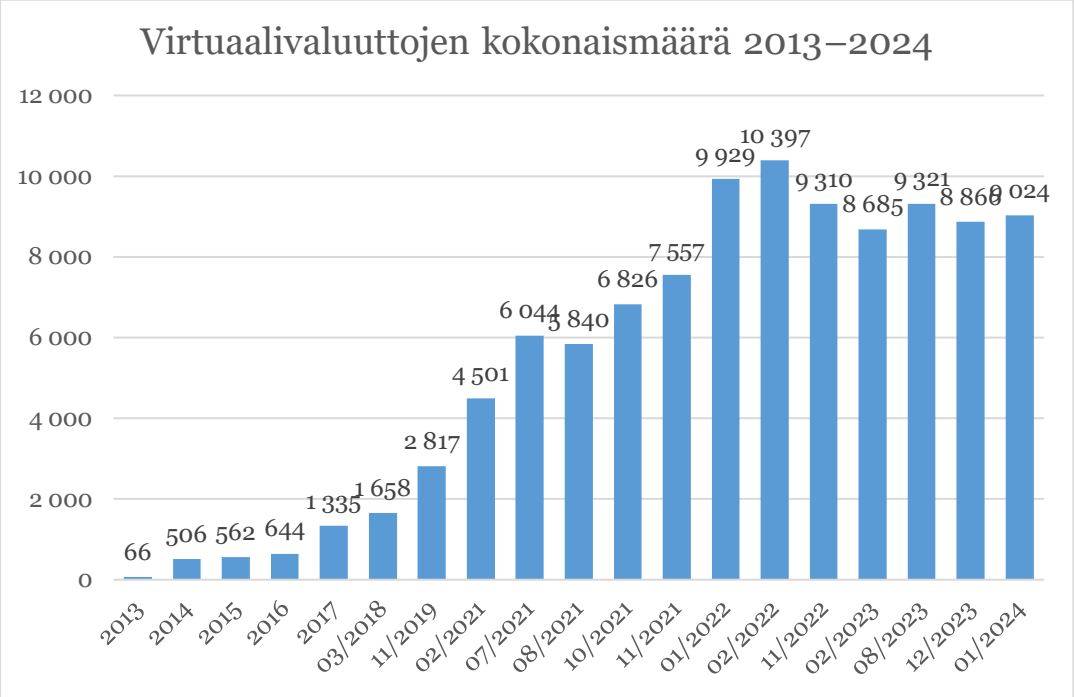
Vaikka usein virtuaali- ja kryptovaluutoista keskusteltaessa ensimmäisenä suurena innovaationa pidetään Bitcoinia, ei se kuitenkaan ole ensimmäinen digitaalinen valuutta. Vuonna 1989 David Chaumin DigiCash-yhtiö tarjosi kahta erilaista digitaalista valuuttaa, eCashia sekä Cyberbucksia. Näiden digitaalisten valuuttojen taustalla toimi Chaumin jo vuonna 1982 kehittämä sokea allekirjoitusprotokolla. Protokollan avulla käyttäjät pysyivät anonyymeina sekä jäljittämättöminä.[84]

Tämän lisäksi vuonna 1994 CyberCash luottokorttiyhtiö tarjosi digitaalisia mikromaksupalveluita. Lisäksi myöhemmin yrityksellä oli CyberCoin-niminen mikromaksujärjestelmä.[85]

Virtuaalivaluutoista puhuttaessa yleensä keskustelu kohdistuu Bitcoiniin. Bitcoinin ajatuksen toi julkisuuteen vuonna 2018 nimimerkki Satoshi Nakamoto, joka julkaisi kirjoituksensa järjestelmästä, joka toimisi ilman keskitettyä hallintaa ja sen avulla olisi mahdollista suorittaa sähköisiä transaktioita.[86]

Kuten alla oleva taulukko virtuaalivaluuttojen määrästä kertoo, vuoden 2018 jälkeen on ollut merkittävää kasvua uusien virtuaalivaluuttojen määrässä. Vaikka eri valuuttojen määrä on laskenut vuoden 2022 huipun jälkeen, on määrä pysynyt silti merkittävänä. Tammikuussa 2024 eri virtuaalivaluuttoja on ollut jopa 9 024 kappaletta.[87]

[84] Cawrey – Lantz 2022, kappale 1.
[85] Eerola ym. 2019, kappale 1.1.4.
[86] Cawrey – Lantz 2022, kappale 1.
[87] Statista 2024.



Taulukko 1 Virtuaalivaluuttojen määrät vuosina 2013–2024 [88]

Virtuaalivaluuttojen määrän nousu ja määrien pysyminen korkeana kertoo siitä, että markkina on pysynyt kiinnostavana eikä kiinnostuksen laantumisesta näy tämän osalta merkkejä. Virtuaalivaluuttojen lasku voi osittain selittyä myös markkinan vakiintumisella.

2.3.1 Kryptovarojen määrittely

Kuten on jo aiemmin todettu, on virtuaalivarojen määrittely haastavaa. Määritelmät muuttuvat markkinan ja lainsäädännön muutosten mukana. Kuitenkin useat eri tahot ovat määritelleet virtuaalivaroja tarkemmin ja osa määritelmistä vakiintuvat varmasti tulevan lainsäädännön voimaantulon myötä.

FATF käyttää julkaisuissaan termiä virtuaalivarat. Virtuaalivarat ovat digitaalisessa muodossa olevaa arvoa, jota voidaan digitaalisesti vaihtaa, siirtää tai käyttää maksuvälineenä. Näitä virtuaalivaroja ei kuitenkaan tule sekoittaa digitaalisessa muodossa oleviin fiat-valuuttoihin.[89]

EU:n MiCA-asetuksessa käytetään termiä kryptovarat, joka on määritelty seuraavasti asetuksen kolmannessa artiklassa seuraavasti: ” ’kryptovaralla’ arvon tai oikeuden digitaalista edustajaa, joka pystytään siirtämään ja

[88] Statista 2024.
[89] FATF 2023, s. 137.

tallentamaan sähköisesti käyttäen hajautetun tilikirjan teknologiaa tai vastaavaa teknologiaa". MiCA-asetus erottaa lisäksi toisistaan sähkörahatokenit ja omaisuusreferenssitokenit sekä muut kuin edellä mainitut. Sähkörahatokeneiden arvo on sidottu viralliseen valuuttaan ja omaisuusreferenssitokenit toiseen omaisuuserään tai niiden yhdistelmään.

Lisäksi Euroopan Parlamentin ja Neuvoston Direktiivi (EU) 2018/843 (viides rahanpesudirektiivi) määritelmä virtuaalivaluutoista on hieman edeltävää erilaisempi. Viides rahanpesudirektiivi määrittelee vain virtuaalivaluutat, jotka ovat direktiivin kolmannen artiklan mukaan *"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*".

Lisäksi Suomessa laki virtuaalivaluuttojen tarjoajista (572/2019) 2 § määrittelee virtuaalivaluutat seuraavasti: *" Tässä ¨ laissa tarkoitetaan:*
1) virtuaalivaluutalla 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"

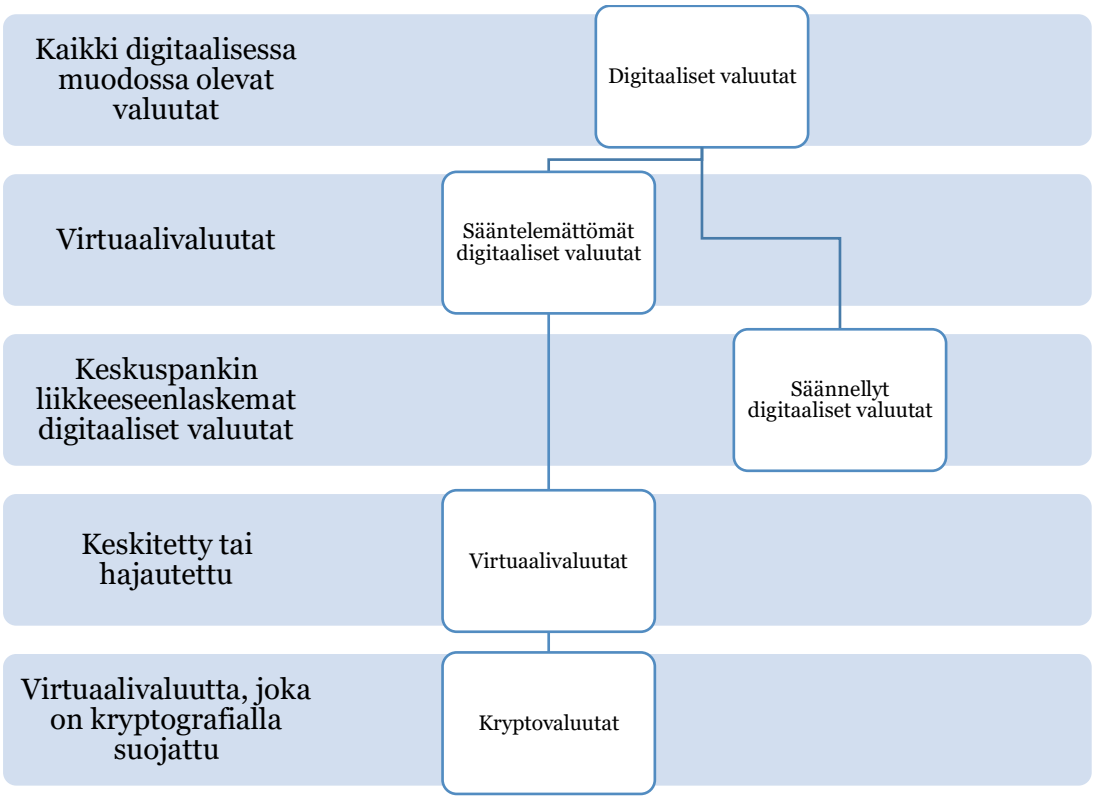
Yhtenäistä siis näille määrittelyille on se, että kryptovaroiksi tai -valuutoiksi katsotaan digitaalisessa muodossa olevat arvot, joita täytyy pystyä siirtämään ja vaihtamaan sekä käyttämään maksuvälineenä sähköisesti. Lisäksi ne tulee erottaa laillisista maksuvälineeksi vahvistetuista valuutoista.

2.3.2 Virtuaalivaluuttojen jaottelu

Virtuaalivaluuttoja on määritelty yllä olevassa kappaleessa ja nämä määritelmät jo osoittavat, että kyse on laajasta joukosta erilaisia varoja ja valuuttoja.

Usein termejä virtuaalivaluutta ja kryptovaluutta käytetään sekaisin tarkoittamaan samaa asiaa, mutta asia ei ole useinkaan niin. Kuten alla olevasta kuviosta nähdään, ovat kryptovaluutat virtuaalivaluuttoja mutta kaikki virtuaalivaluutat eivät ole kryptovaluuttoja.[90]

[90] Rodeck 2023.



Kuvio 1. Virtuaalivaluuttojen taksonomiaa[91]

Yllä olevan kuvion tarkoitus on hahmottaa yksinkertaistetusti sitä, millä tavoin digitaalisessa muodossa olevia valuuttoja voidaan jaotella. Digitaalisiksi valuutoiksi katsotaan myös säännellyt digitaaliset valuutat, jotka ovat keskuspankin liikkeeseen laskemia. Nämä ovat digitaalisia keskuspankkirahoja (CBDC).[92] Myös Euroopassa suunnitellaan digieuroa, joka olisi Euroopan keskuspankin liikkeeseen laskema digitaalinen euron muoto.[93]

Virtuaalivaluutat voivat olla keskitettyjä, jolloin niitä ylläpitää jokin yksittäinen taho. Hajautetut virtuaalivaluutat toimivat usein lohkoketjuteknologian avulla ja hajautetun järjestelmän verifioinnin takia ei tarvita keskushallintoa.[94] Tällaiset virtuaalivaluutat ovat usein kryptovaluuttoja, joita käsitellään tarkemmin seuraavassa kappaleessa.

Virtuaalivaluutat voidaan jakaa myös vaihtokelpoisiin ja vaihtokelvottomiin virtuaalivaluuttoihin. Vaihtokelpoisilla virtuaalivaluutoilla on yhtenevä arvo jonkin oikean valuutan kanssa. Lisäksi tällaisia virtuaalivaluuttoja voidaan

[91] Mukaillen Goldman – Kumar 2021, s. 3.
[92] Rodeck 2023.
[93] Euroopan keskuspankki 2023, s. 8.
[94] Bashir 2018, s. 32.

vaihtaa oikeaksi valuutaksi tai oikeaa valuutta virtuaalivaluutaksi. Tällaiset virtuaalivaluutat voivat olla keskitettyjä tai hajautettuja.[95]

Vaihtokelvottomia virtuaalivaluuttoja ei voi nimensä mukaisesti vaihtaa oikeaksi valuutaksi tai joksikin toiseksi virtuaalivaluutaksi. Tällaisesta esimerkkinä toimii World of Warcraft Gold. Kaikki vaihtokelvottomat virtuaalivaluutat ovat keskitettyjä.[96]

2.3.3 Kryptovarat

Tässä luvussa käsitellään tarkemmin kryptovaroja. Tässä kohtaa käytetään termiä kryptovara, jotta aihetta voidaan kuvata kryptovaluuttoja laajemmin. Kuitenkaan tässä työssä ei ole tarkoituksenmukaista lähteä tutkimaan laajemmin muita kryptovaroja kuin kryptovaluuttoja, joten kappaleessa keskitytään pääosin kryptovaluuttoihin.

Kryptovarat voidaan jakaa kolmeen alakategoriaan; kryptovaluuttoihin (kuten Bitcoin), kryptotokeneihin ja kryptohyödykkeisiin. Kryptotokenit ovat digitaalisia tuotteita ja palveluita ja kryptohyödykkeet puolestaan digitaalisia resursseja, joita voidaan hyödyntää valmiin tuotteen tekemiseen.[97]

Kryptovaluutat ovat virtuaalivaluuttoja, jotka on suojattu kryptografialla. Ne toimivat julkisella tilikirjalla ja niitä vaihdetaan, luodaan ja hallinnoidaan keskittämättömän vertaisverkon avulla.[98]

Kryptovaluutat voidaan jakaa myös itseorganisoituviin kryptovaluuttoihin, yritysten kryptovaluuttoihin sekä valtion kryptovaluuttoihin. Itseorginasoituvia kryptovaluuttoja ei hallita keskitetyn tahon puolesta vaan ne ovat hajautettuja. Tällainen kryptovaluutta on esimerkiksi Bitcoin.[99]

Yritykset voivat myös julkaista kryptovaluuttoja, kuten esimerkiksi Diemin (entinen Libra) kohdalla on tehty, jolloin Meta (entinen Facebook) julkaisi oman kryptovaluutan Diemin. Näiden lisäksi valtiot voivat julkaista kryptovaluuttoja, tällainen on esimerkiksi Kiinan valtion julkaisema China's Digital Currency Electronic Payment (DCEP).[100] Samaan kategoriaan menevät myös muut digitaaliset keskuspankkirahat, kuten digitaalinen euro.[101]

---

[95] Washington state department of financial institutions.
[96] Ibid.
[97] Jeegers 2023, kappale 2.7.
[98] Ibid.
[99] Storås 2024.
[100] Jeegers 2023, kappale 2.7
[101] Euroopan keskuspankki 2023, s. 8.

Kryptovaluutat käyttävät toiminnassaan julkisia avaimia, joiden avulla saadaan avattua salattuja tietoja, ja yksityisiä avaimia, joiden avulla tiedot saadaan salattua. Esimerkiksi Bitcoinin kohdalla kirjauduttaessa Bitcoin-lompakkoon, saadaan julkinen ja yksityinen avain sekä Bitcoin-osoite. Osoite on käännös julkisesta avaimesta ja toimii identiteettinä lompakolle, josta varat lähtevät tai saapuvat. Bitcoinin yksityisiä avaimia käytetään allekirjoittamaan transaktiot. Tällä tavoin voidaan todeta, että Bitcoin-osoitteen omistajalle kuuluu oikeasti tuo osoite ja että hän voi valtuuttaa maksun.[102]

Kryptovaluuttojen transaktiot vaativat yksityisen avaimen allekirjoituksen, jonka jälkeen yksityistä avainta vastaava julkinen avain vahvistaa allekirjoituksen ja vahvistaa transaktion. Transaktiot, jotka julkaistaan lohkoketjun osaksi, ovat hyväksyttyjä.[103]

Kryptovaluuttoja säilytetään edellä mainituissa lompakoissa. Lompakoissa käytännössä säilytetään kryptografialla salattuja avaimia. On olemassa kahdenlaisia lompakkoja, hallussa pidettyjä lompakkoja (*engl. custodial*) ja ei-hallussa pidettyjä (*engl. non-custodial*) lompakkoja. Hallussa pidettyjä lompakkoja kontrolloi jokin luotettu taho ja tällaisina lompakkoina toimivat esimerkiksi vaihtopalvelut (*engl. exchange*). Vaihtopalvelut pitävät jonkun tahon omistamat kryptovaluutat tilillä ja samalla hallinnoivat ja omistavat yksityisen avaimen. Esimeriksi Coinbase on tällainen palvelu.[104]

Ei-hallussa pidetyt lompakot antavat käyttäjälle täyden hallinnan avaimiin. Haittapuoli tässä on se, että jos käyttäjä kadottaa avaimen, hän ei pääse käsiksi kryptovaroihinsa enää.[105]

[102] Cawrey – Lantz, 2023, kappale 2.
[103] Bashir 2023, kappale 7.
[104] Cawrey – Lantz 2023, kappale 2.
[105] Ibid.

3 Kryptovarojen sääntely

Krypto- ja virtuaalivaroihin kohdistuu sääntelyä, joka on lisääntynyt viime aikoina. Uudet säädökset paikkaavat aukkoja sääntelyssä krypto- ja virtuaalivarayhtiöiden osalta koko EU:n osalta.

Tämän työn kannalta olennaisinta on rahanpesusääntely mutta ymmärtääksemme tarkemmin krypto- ja virtuaalivarojen sääntelykokonaisuutta, on tässä kappaleessa käsitelty myös muuta sääntelyä. Lisäksi on oleellista tämän työn kannalta pohtia mahdollisia lainsäädännöllisiä aukkoja ja sääntelyn tulevaisuutta niin koko EU:n kuin kansallisesti Suomen osalta.

3.1 Markets in Crypto-Assets (MiCA)

Tällä hetkellä yhtenäistä eurooppalaista lainsäädäntöä kryptovaramarkkinoille ei ole, lukuun ottamatta rahanpesusäädöksiä. Tämä aukko sääntelyssä altistaa monenlaisille riskeille, kuten markkinoiden väärinkäytölle ja talousrikollisuudelle. Ongelmana on, ettei yhtenäistä sääntelyä laajasti eri kryptotoimijoille ole ollut.[106]

Vaikka kryptomarkkinat eivät ole niin suuret, että ne uhkaisivat rahoitusvakautta, on kuitenkin mahdollista, että tulevaisuudessa joidenkin kryptovarojen liikkeeseenlasku voisi aiheuttaa ongelmia rahoitusvakaudelle ja maksujärjestelmien toiminnalle. Toisaalta yhtenäisen sääntelyn hyviä puolia olisi palveluntarjoajien toimilupien selkeyttäminen, joka selkeyttäisi kilpailuedellytyksiä. Yhtenäisen sääntelyn puuttuminen on estänyt toimiluvallisten kryptovarapalvelujen tarjoamisen jäsenvaltiosta toiseen.[107]

Vuonna 2023 voimaan tullut ja vuoden 2024 aikana vaiheittain sovellettavaksi tuleva asetus (EU) 2023/1114 kryptovarojen markkinoista (MiCA) sääntelee kuitenkin virtuaali- ja kryptovaroja EU:ssa. Asetuksen tarkoitus on yhdenmukaistaa sääntöjä EU:n alueella kryptovaluuttojen liikkeeseenlaskijoille, joita ei ole vielä muualla säädelty. Näiden lisäksi asetuksessa säädellään kryptopalveluiden tarjoajia. Asetus koskee kryptovarojen liikkeeseenlaskijoita ja palveluntarjoajia, esimerkiksi kauppapaikkoja ja lompakoita, jotka toimivat kryptovarojen säilytyksessä. Asetus ei koske sellaisia kryptovaroja, jotka ovat rahoitusvälineitä tai ovat keskenään vaihtokelvottomia.[108]

Asetuksen avulla luodaan yhtenäistä sääntelyä EU:n alueelle ja pyritään estämään edellä mainittuja haasteita. Asetuksen yksi tärkeimmistä

[106] Berger – Boeve – Kalokyris 2023.
[107] HE 31/2024 vp, s. 6.
[108] ESMA.

päämääristä on lainsäädännön yhtenäistäminen EU:n alueella sekä sääntelyn soveltamisalan laajentaminen koskemaan useampia kryptotoimijoita, jotta toimialaan kohdistuviin riskeihin voidaan puuttua.

Asetuksen kolmannessa artiklassa on määritelty ja eroteltu toisistaan sähkörahatokenit, omaisuusreferenssitokenit sekä muut kryptovarat kuin edellä mainitut. Sähkörahatokeneilla tarkoitetaan kryptovaroja, joiden arvo on suhteutettu johonkin viralliseen valuuttaan. Omaisuusreferenssitokenit ovat puolestaan kryptovaroja, joiden arvon vakaus liittyy johonkin toiseen omaisuuserään tai sellaisten koriin. Kryptovaroille ominaista puolestaan on se, että ne ovat digitaalisia ja niitä pystytään tallentamaan ja siirtämään sähköisesti ja tähän hyödynnetään hajautetun tilikirjan teknologiaa.

Lisäksi kryptovarapalvelut on määritelty asetuksen 3 artiklassa seuraavasti:

” ’kryptovarapalvelulla’ mitä tahansa seuraavista mihin tahansa kryptovaraan liittyvistä palveluista ja toiminnoista:
a) kryptovarojen säilytyksen tarjoaminen ja hallinnointi asiakkaiden puolesta;
b) kryptovarojen kaupankäyntialustan ylläpito;
c) kryptovarojen vaihto varoihin;
d) kryptovarojen vaihto muihin kryptovaroihin;
e) kryptovaroja koskevien toimeksiantojen toteuttaminen asiakkaiden puolesta;
f) kryptovarojen kohdennettu tarjoaminen;
g) kryptovaroja koskevien toimeksiantojen vastaanottaminen ja välittäminen asiakkaiden puolesta; h) kryptovaroja koskevan neuvonnan tarjoaminen;
i) kryptovaroja koskevan salkunhoidon tarjoaminen;
j) kryptovarojen siirtopalvelujen tarjoaminen asiakkaiden puolesta;”

Asetuksen II osastossa säädetään muista kryptovaroista kuin omaisuusreferenssitokeneista tai sähkörahatokeneista ja niiden ottamisesta kaupankäynnin kohteeksi. Muiden kryptovarojen tarjoajan tulee asetuksen mukaan olla oikeushenkilö, sen tule julkaista kuvaus kryptovarasta sekä julkaista markkinointiviestintää, toimittava rehellisesti ja ammattimaisesti, yhteydenpito varojen haltijoihin tulee olla selkeää ja tasapuolista, eturistiriitoja tulee tunnistaa ja ehkäistä ja varojen haltijoille on annettava peruutusoikeus.

Asetuksen III osaston 1 luvussa kerrotaan, että omaisuusreferenssitokeneita yleisölle tarjoavien tahojen sekä tahojen, jotka ottavat omaisuusreferenssitokeneita kaupankäynnin kohteeksi, on haettava toiminnalleen toimilupaa. Luottolaitokset voivat hyödyntää heillä jo olevaa toimilupaa omaisuusreferenssitokeneiden tarjoamiseen, mikäli he täyttävät asetuksen vaatimat tiedot heidän kryptovaran kuvauksessaan. Muutos kryptovarapalveluiden

tarjoajien luvanvaraisuuteen on erityisen kiinnostava, sillä se lisää merkittävästi toimijoiden velvollisuuksia.

III osaston 2 luvussa säädetään omaisuusreferenssitokenien liikkeeseenlaskijoiden velvollisuuksista. Tällaisen tahon on oltava oikeushenkilö ja sillä on oltava edellä mainittu toimilupa. Lisäksi heidän tulee julkaista kryptovarojen kuvaus sekä markkinointiviestintää, toimia tokenien haltijoiden edun mukaisesti, ottaa käyttöön valituksenkäsittelyyn liittyvät menettelyt ja ylläpitää omaisuusreserviä. Lisäksi valvojan tulee hyväksyä omaisuusreferenssitokenin kuvaus ennen liikkeeseenlaskua.

Asetuksen IV osastossa säädetään sähkörahatokeneista ja niiden liikkeeseenlaskijoihin kohdistuvista vaatimuksista. Sähkörahatokeneita voidaan tarjota yleisölle tai hakea sähkötokeneita kaupankäynnin kohteeksi, jos liikkeeseenlaskijalla on luottolaitoksen tai sähköisen rahan liikkeeseenlaskijan toimilupa. Lisäksi liikkeeseenlaskijan tulee antaa viranomaiselle kryptovaran kuvauksen artiklan 51 säädösten mukaisesti. Lisäksi tokenit tulee laskea nimellisarvon mukaisesti vastaanottaessa varoja, lunastettava tokenit, kun haltija niin pyytää, sekä ”*sijoitettava varat suojattuihin vähäriskisiin omaisuuseriin samana valuuttana ja talletettava ne erilliselle tilille luottolaitoksessa”* ja samalla tavoin, kun omaisuusreferenssitokeneiden liikkeeseenlaskijoiden, laadittava palautumis- ja lunastussuunnitelmat.

Sähkörahatokeneita koskee MiCA-asetuksen lisäksi tavallinen sähköistä rahaa koskeva sääntely ja täten näitä tokeneita voi laskea liikkeelle vain tahot, jotka voivat laskea liikkeelle muutakin sähköistä rahaa. Perinteisten kryptovarojen arvonheilahtelua on pyritty sähkörahatokeneissa välttämään niin, että niiden arvo on sidottu johonkin yhteen viralliseen valuuttaan.[109]

Mikäli sähkörahatokenit tai omaisuusreferenssitokenit katsotaan ”merkittäviksi” Euroopan pankkiviranomaisen (EBA) toimesta, liikkeeseenlaskijoihin sovelletaan lisävaatimuksia. Näiden tahojen valvonnasta vastaa silloin EBA. Lisäksi toimivaltaisena viranomaisena toimii ESMA. Lisäksi osaston VII mukaan jäsenvaltioiden tulee nimetä oma toimivaltainen viranomainen. Hallituksen esityksen eduskunnalle laiksi kryptovarapalvelun tarjoajista ja kryptovaramarkkinoista sekä eräiksi muiksi laeiksi mukaan Suomessa toimivaltainen viranomainen tulisi olemaan Finanssivalvonta.[110]

Niin sähkörahatokeneja kuin omaisuusreferenssitokeneja koskee kielto maksaa korkoja. Lisäksi MiCA-asetuksessa on kielletty myös muunlaisen etuuden maksaminen näille tokeneille, joka perustuu tokenin hallussapitoajan

[109] Tanninen 2023.
[110] HE 31/2024 vp, s. 33.

pituuteen. Korkojen maksaminen on kiellettyä niin liikkeeseenlaskijoita kuin kryptovaroja tarjoavia yrityksiä.[111]

Asetuksen osastossa V säädetään kryptovarapalvelua tarjoavien toimiluvista. Toimiluvista säädetään 59 artiklassa, jonka mukaan oikeushenkilöllä tai yrityksellä tulee olla toimilupa tai jos kyseessä on *"luottolaitos, arvopaperikeskus, sijoituspalveluyritys, markkinoiden ylläpitäjä, sähköisen rahan liikkeeseenlaskijalaitos, yhteissijoitusyrityksen rahastoyhtiö tai vaihtoehtoisen sijoitusrahaston hoitaja"* saavat he tarjota kryptovarapalveluja artiklan 60 nojalla.

Osaston V luvussa 2 säädellään kaikkia kryptovarojen tarjoajia koskevia velvoitteita. Kaikkien kryptovaroja tarjoavien on toimittava ammattimaisesti, annettava selkeitä tietoja asiakkaille, ilmoitettava kryptovarojen hinnoittelu, kustannukset, ilmastoon ja ympäristöön liittyvät vaikutukset sekä palkkiopolitiikan verkkosivustolla ja käytettävä vakavaraisuustakeita. Lisäksi kryptovarojen tarjoajien ylimmän johdon tulee olla hyvämaineisia ja ammattitaitoisia.

MiCA-asetus tuo siis merkittäviä muutoksia kryptovaratoimijoille ja lisää toimijoiden vaatimuksia. Sisällöltään vaatimukset muistuttavat Komission delegoitua asetusta (EU) 2017/565 eli MiFID-asetusta, jossa määrätään erityisesti sijoittajansuojaan liittyviä kokonaisuuksia. Erityisesti MiCA-asetuksen vaatimukset liittyen hinnoitteluun ja yleisesti asiakkaille tarjottavaan tietoon muistuttavat MiFID-asetusta. Tämä on varmasti hyvä asia, sillä näiden vaatimusten avulla kryptovaramarkkinaa on mahdollista vakauttaa ja tasata kuluttajien ja yritysten välistä epäsuhtaa.

3.2 Laki virtuaalivaluutan tarjoajista

Suomessa kansallisesti kryptovaroja säädetään laissa virtuaalivaluutan tarjoajista (572/2019). Vuonna 2019 voimaantulleen lain mukaan virtuaalivaluutan tarjoajien tulee rekisteröityä virtuaalivaluutan tarjoajaksi toimiakseen sellaisena (4 §). Finanssivalvonta ylläpitää rekisteriä virtuaalivaluutan tarjoajista.

Lain 7 §:ssä on määritelty virtuaalivaluutan tarjoajan luotettavuuteen vaikuttavista tekijöistä. Jotta rekisteröijä voidaan katsoa 6 §:n mukaan luotettavaksi, ei hakijalla saa olla edelliseen viiteen vuoteen vankeusrangaistusta ja edelliseen kolmeen vuoteen sakkorangaistusta jostakin sellaisesta rikoksesta, joka tekisi hakijasta sopimattoman toimimaan virtuaalivaluutan

[111] Tanninen 2023.

tarjoajana. Myöskään omistajana, toimitusjohtajana tai sen sijaisena tai hallituksen jäsenenä ei voi olla tällainen taho.

Lain 11 §:ssä säädetään asiakasvarojen säilyttämisestä. Varat tulee säilyttää sekoittamatta niitä ja varat tulee säilyttää tilillä keskuspankissa tai muussa luottolaitoksessa tietyin ehdoin tai varat voi sijoittaa vähäriskisiin sijoituskohteisiin.

12 §:n mukaan markkinointimateriaalin tulee pitää sisällään merkittävät tiedot asiakkaan taloudellisen turvan kannalta. 13 §:ssä säädetään asiakkaan tuntemisvelvollisuudesta, joka koskee asiakkaan henkilöllisyyden tunnistamista sekä tosiasiallisten edunsaajien selvittämistä. Lisäksi virtuaalivaluuttojen tarjoajilla tulee olla tarvittavat riskienhallintajärjestelmät, jotta se pystyy arvioimaan asiakkaistaan kohdistuvia riskejä.

Laki virtuaalivaluutan tarjoajista ei aseta rajoituksia rekisteröityneille toimijoille siihen, mitä muuta toimintaa he voivat harjoittaa. Muuta toimintaa sitoo siihen liitännäinen sääntely. Edellä läpikäyty MiCA asetus ei tuo muutoksia tähän, sillä jatkossa myös kryptovarapalvelua ja esimerkiksi maksupalveluja tarjoava taho tarvitsee niin kryptovarapalvelun toimiluvan kuin maksulaitoksen toimiluvan.[112]

Tällä hetkellä laki virtuaalivaluutan tarjoajista ei kata laajemmin kryptomarkkinaa, joka aiheuttaa riskejä liittyen toimialaan virtuaalivaluuttojen tarjoajien ulkopuolella. Tähän ratkaisuna on tulossa oleva MiCA-asetus, joka laajentaa sääntelykehikkoa muihinkin kryptotoimijoihin kuin vain virtuaalivaluutan tarjoajiin. Hallituksen esitys eduskunnalle laiksi kryptovarapalvelun tarjoajista ja kryptovaramarkkinoista sekä eräiksi muiksi laeiksi tulee siten voimaantullessaan kansallisesti täyttämään MiCA:n velvoitteet.

3.3 Rahanpesusääntely

EU:ssa ja Suomessa on tapahtunut muutoksia rahanpesusääntelyssä, jotka koskevat myös joitain virtuaali- tai kryptovarayhtiöitä. Tiettyjä toimijoita koskee tiukemmat rahanpesun ja terrorismin rahoittamisen estämisen toimenpiteet erityisesti asiakkaan tuntemiseen liittyen.

EU:n viidennessä rahanpesudirektiivissä säädellään virtuaalivaluuttojen vaihtopalveluita sekä lompakkopalveluita. Direktiivin edellyttämänä kyseisten toimijoiden tulee rekisteröityä. Tarkoituksena on saada virtuaalivaluuttojen vaihtopalvelut sekä lompakkopalvelut osaksi rahanpesun ja terrorismin rahoittamisen estävää toimintaa sekä valvonnan piiriin.

[112] HE 31/2024 vp, s. 34.

Direktiivissä säädellään asiakkaan tuntemisvelvollisuudesta, tosiasiallisista omistajista ja edunsaajista hankittavista tiedoista, salassapitovelvollisuudesta, tietojen säilyttämisestä ja tietosuojasta. Asiakkaan tuntemisvelvollisuuksista kerrotaan tarkemmin luvussa 4.

Suomessa laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444 (rahanpesulaki) säätää myös virtuaalivaluutan tarjoajia koskevia säädöksiä liittyen rahanpesun ja terrorismin rahoittamisen estämiseen. Virtuaalivaluutan tarjoajien tulee lain 3 luvun 2 §:n mukaan noudattaa asiakkaan tuntemiseen liittyviä toimenpiteitä ja tunnistettava asiakkaansa. Lisäksi lain 3 luvussa säädetään myös mm. tosiasiallisten edunsaajien tunnistamisesta (6 §), poliittisesti vaikutusvaltaisten henkilöiden tehostetusta tuntemisvelvollisuudesta (13 a §) ja pakotesääntelyn noudattamiseen liittyvistä tuntemisvelvollisuuksista (16 §). 4 luvun perusteella virtuaalivaluutan tarjoajien tulee tehdä ilmoituksia epäilyttävistä liiketoimista rahanpesun selvittelykeskukselle (1 §) sekä liiketoimien keskeyttämisestä (5 §). Näiden lisäksi rahanpesulain 9 luvussa säädellään mm. työntekijöiden koulutusvelvoitteista (1 §).

Tällä hetkelläkin on siis voimassa sääntelyä, joka velvoittaa virtuaalivaluuttojen tarjoajia sekä virtuaalivaluuttojen lompakkopalveluita ja -vaihtopalveluita ottamaan toiminnassaan huomioon myös rahanpesusääntelyn. Kuitenkin tästä huolimatta sääntelyn ulkopuolelle jää muita kryptotoimijoita.

3.4 Muut lait ja määräykset

Haasteena kryptovarojen sääntelyssä on ollut kryptovarasiirtojen jäljitettävyyden haasteet. Aiemmin ei ole ollut Euroopan unionin sisäistä yhtenäistä sääntelyä sille, että kryptovaroja olisi voitu jäljittää samalla tavalla kuin perinteisiä varoja.[113] Tähän on kuitenkin saatu juuri muutos.

Euroopan parlamentti ja neuvosto on antanut asetuksen (EU) 2023/113 varainsiirtojen ja tiettyjen kryptovarojen siirtojen mukana toimitettavista tiedoista ja direktiivin (EU) 2015/849 muuttamisesta (uudelleenlaadittu)[114], jonka piirissä ovat myös MiCA:ssa määritellyt kryptovarapalvelut ja kryptovarapalveluiden tarjoajat. Uudelleenlaaditulla asetuksella entisestä varainsiirtojen mukana toimitettavista tiedoista ja asetuksen (EY) N:o 1781/2006 kumoamisesta annettu Euroopan parlamentin ja neuvoston asetuksesta

[113] HE 31/2024 vp, s. 6.
[114] Työssä asetuksesta käytetään myöhemmin termiä maksun tiedot -asetus.

(EU) 2015/847 eli maksun tiedot-asetuksesta, on saatu lisävelvollisuuksia kryptovarojen tarjoajille.

Asetuksen I osan mukaan kryptovarojen tarjoajien tulee sisällyttää varainsiirtoon mukaan mm. seuraavat tiedot: toimeksiantajan nimi ja osoite, tilinumero tai esimerkiksi hajautetun tilikirjan tai virtuaalivaratilin osoite tai numero, henkilötietoasiakirjan numero, asiakasnumero tai syntymäaika ja syntymäpaikka sekä varojen saajan nimi ja tilinumero tai vastaava tieto.

Lisäksi kryptopalveluntarjoajan, joka vastaanottaa varat on varmistettava, että siirron toimeksiantajasta on tarvittavat tiedot saatavilla ja että näitä tietoja monitoroidaan. Lisäksi, mikäli toimeksiantaja tai saaja on oikeushenkilö, tulee oikeushenkilö- eli LEI-tunnus tai vastaava sisällyttää maksun tietoihin, mikäli mahdollista.

Maksun tiedot -asetuksen 38 artiklassa säädetään muutoksista rahanpesudirektiiviin, jonka tarkoituksena on lisätä rahanpesudirektiiviin soveltamisalan pariin MiCA-asetuksessa määritellyt kryptovarapalvelut sekä määritelmä mm. isännöimättömistä osoitteista. Lisäksi artiklassa säädetään EBA:n velvoitteesta luoda ohjeet riskitekijöistä, jotka liittyvät kryptovaratoimijoihin, jotka aloittavat liikesuhteita tai tekevät liiketoimia kryptovaroilla.

Kryptovarojen tarjoajat tulivat myös tammikuussa 2023 voimaan tulleeseen rahoitusmarkkinoiden digitaalista häiriönsietokykyä koskevan asetuksen eli DORA-asetuksen (Digital Operational Reilience Act, (EU) 2022/2554) piiriin. Asetus antaa sitovat säännöt IT-riskien hallinnasta, poikkeamaraportoinnista, digitaalisen häiriönsietokyvyn testauksesta ja kolmansien osapuolien riskienhallinnasta.

Näiden asetusten lisäksi Finanssivalvonnalla on määräykset ja ohjeet kokoelmia, joissa käsitellään myös kryptovarojen tarjoajia. Virtuaalivaluutan tarjoajista koskevassa määräykset ja ohjeet kokoelmassa määrätään mm. riskiarviosta asiakasvarojen säilyttämisestä ja suojaamisesta, millä ehdoin asiakasvaroja voi tallettaa rahasto-osuuksiin sekä kuinka paljon riskiarvioon perustuen asiakasvaroja voi olla sijoitettuna julkiseen tietoverkkoon kytketyssä järjestelmässä.[115]

Määräykset ja ohjeet kokoelmassa Finanssivalvonta myös ohjeistaa, että asiakasvaroja olisi sijoitettuna julkisessa tietoverkkoon kytketyssä järjestelmässä vain sen verran, kuin se omista varoistaan tai muulla järjestelyllä pystyy kattamaan, mikäli varat menetetään. Lisäksi kokoelmassa ohjeistetaan

[115] Finanssivalvonta määräykset ja ohjeet 04/2019.

virtuaalivaluutan tarjoajia käyttämään analyysiohjelmaa asiakkaan tuntemista ja sen seurantaa varten.[116]

Lisäksi Finanssivalvonnan määräykset ja ohjeet kokoelmassa 2/2023 rahanpesun ja terrorismin rahoittamisen estämisessä on määräyksiä ja ohjeita, jotka koskevat myös virtuaalivaluutan tarjoajia.

[116] Finanssivalvonta määräykset ja ohjeet 04/2019.

4 Rahanpesusääntely

Rahanpesusääntelyä on tiukennettu EU:ssa paljon viime vuosina ja uusi rahanpesun ja terrorismin rahoittamisen estämisen lakipaketti on tulossa. EU:n alueella halutaan vahvistaa yhtenäisiä käytäntöjä, jotta rikollisille ja rikolliselle rahalle ei löytyisi porsaanreikiä kansallisista säädöksistä. Lisäksi EU:n alueella halutaan vahvistaa sääntelyn valvontaa ja uusi viranomainen AMLA tulee vastaamaan tästä.

Vaikka työssä pääosin keskitytään rahanpesuun liittyviin riskeihin, ei rahanpesun estämisestä voi puhua mainitsematta terrorismin rahoittamisen estämistä, pakotteita ja niiden kiertämistä, asiakkaan tuntemista sekä väärinkäytösten estämistä. Kaikki nämä osa-alueet nivoutuvat yhdeksi suureksi kokonaisuudeksi, joista jokaiselle osa-alueella on tärkeä merkitys rahanpesun estämisen kokonaisuudessa. Tästä syystä tässä kappaleessa käsitellään rahanpesun lisäksi muita aiheeseen liittyviä kokonaisuuksia.

4.1 Rahanpesun määritelmä

Rahanpesu on käsitteenä suhteellisen uusi ilmiö. Voidaan kuitenkin olettaa, että rikollisen alkuperän omaavaa rahaa on haluttu pestä niin kauan kuin on ollut rikollisuutta, josta on muodostunut taloudellista hyötyä. Rahanpesusta on alettu puhumaan kuitenkin vasta noin 100 vuotta sitten.[117]

Likainen eli pestävä raha syntyy jonkin rikoksen taloudellisena hyötynä. Käteisen rahan säilyttäminen ja käyttö on haastavaa ja voi herättää epäilyksiä, joten rahat halutaan saada helpommin käytettävään ja erityisesti lailliseen muotoon. Rikoksesta saatu taloudellinen hyöty ja sen alkuperä yleensä pyritään häivyttämään ja peittämään eli raha pestään, jolloin puhutaan rahanpesusta.[118]

Rikoksesta saadun taloudellisen hyödyn määrä koko maailman bruttokansantuotteesta on arvioitu olevan 2–5 %.[119] Todellisen määrän arvioiminen on kuitenkin haastavaa, sillä tarkkoja tietoja ei ole. Voidaan kuitenkin katsoa, että arvioiden mukaan rikoksista saatua taloudellista hyötyä pyörii maailman taloudessa Ranskan vuosittaisen bruttokansantuotteen verran.[120]

Rahanpesulle olennaista on peittää ja häivyttää varojen rikollinen alkuperä. Käytännössä rahanpesurikokset eivät välttämättä ole hienostuneita ison

[117] Sharman 2011, s. 15.
[118] Hyttinen 2021, s. 2.
[119] UN, Office on Drugs and Crime.
[120] Hyttinen, 2021, s. 2.

rahan rikoksia, vaan rahanpesusyytteet ovat voineet tulleet esimeriksi osana näpistystä tai varkautta. [121]

Rahanpesun esirikoksen tekijä haluaa päästä hyödyntämään rikoksella saatuja varoja. Tämä rahanpesun prosessi koostuu kolmesta eri vaiheesta. Ensimmäisenä pestävä raha tulee sijoittaa talousjärjestelmään, joka on laillinen. Tämän jälkeen varat peitetään ja häivytetään. Tällöin puhutaan harhauttamisesta. Kolmannessa vaiheessa varat on puhdistettu ja ne otetaan osaksi laillista taloutta.[122]

Kaikista kriittisin vaihe on rahanpesun ensimmäinen vaihe, jolloin varat sijoitetaan talousjärjestelmään. Tämän takia lainsäädäntö rahanpesun estämisessä on lähtökohtaisesti preventiivistä, eli pyritään tekemään toimia, jotka estäisivät rahanpesun ensimmäisen vaiheen.[123] Yksi tärkeimmistä rahanpesun estämisen sääntelyistä liittyy asiakkaan tuntemiseen, jonka tarkoituksena on puuttua juuri tuohon rahanpesun ensimmäiseen vaiheeseen, jotta varojen alkuperä ja niiden haltija voidaan heti tunnistaa ja tuntea.[124]

Siinä vaiheessa, kun varat on saatu pestyä, voidaan laillisessa järjestelmässä olevat varat sijoittaa esimeriksi osakkeisiin ja johonkin kiinteään omaisuuteen ja vaikka laillisen yrityksen perustamiseen. Varoja käytetään usein myös uusien rikoksien tekemiseen.[125]

Rahanpesurikos vaatii aina jonkin esirikoksen. Esirikoksessa syntyy taloudellista hyötyä, joka sitten pestään erilaisin keinoin. Likaisella rahalla viitataan juuri tuohon taloudellisen hyötyyn, jota rikoksesta on saatu. Suomessa likainen raha, joka on syntynyt jostain sellaisesta teosta, jota ei ole määrätty rangaistavaksi rikoslaissa vaan jossakin toisessa laissa, katsotaan silti rikoksesta saaduksi taloudelliseksi hyödyksi eli likaiseksi rahaksi. Likainen raha voi muuttaa muotoaan esimeriksi käteisestä autoksi ja silti omaisuutta pidetään likaisena rahana.[126]

4.2 Rahanpesun ja terrorismin rahoittamisen estäminen

Likaista rahaa pyörii maailmanlaajuisesti paljon talousjärjestelmässä. Suomessa rahanpesun selvittelykeskus vastaanottaa rahanpesuilmoituksia, joiden avulla päästään ajoittain käsiksi erilaisiin rahanpesurikoksiin.

[121] Chapman 2018, s. 6.
[122] Sharman 2011, s. 17–18.
[123] Hyttinen 2021, s. 25.
[124] Sharman 2011, s. 27.
[125] Hyttinen 2021, s. 26.
[126] Ibid, s. 222–223.

Ilmoitusmäärät rahanpesun selvittelykeskukselle lisääntyivät vuoden 2023 aikana, kuten alla olevasta taulukosta voidaan nähdä.

Ilmoittajaluokka	*2021*	*2022*	*2023*
Yleistä maksujenvälitystä tarjoava (sis. valuutanvaihdon)	19 593	19 199	310 863
Luotto- ja rahoituslaitos (pankki)	13 877	13 337	19 847
Virtuaalivaluuttapalvelun tarjoaja	3 631 789	84 055	4 802
Kaikki ilmoitukset yhteensä	3 692 641	230 171	347 012

Taulukko 2 Rahanpesuilmoitusten määrät ilmoittajaluokittain 2021–2023.[127]

Pankkien tekemät ilmoitukset kasvoivat 49 % edellisestä vuodesta. Eniten ilmoituksia on tullut yleistä maksujenvälitystä tarjoavilta ilmoittajilta. Vuonna 2021 virtuaalivaluuttapalvelun tarjoajat tekivät merkittävän osan ilmoituksista, mutta ilmoitusten määrä on sen jälkeen pudonnut merkittävästi.[128]

Ilmoituksen määrät kertovat siitä, että ilmoitusvelvolliset ovat tärkeässä osassa rahanpesun tunnistamisessa. Kuten jo aiemmin on mainittu, lainsäädäntökin pyrkii erityisesti olemaan preventiivistä eli estämään likaisen rahan pääsyn rahoitusjärjestelmään. Virtuaalivaluuttapalvelun tarjoajien osalta voidaan myös nähdä, kuinka lainsäädännöllä voidaan vaikuttaa siihen, miten uudenlaisten palveluiden tarjoajat saadaan mukaan estämään rahanpesua.

Vuonna 2021 virtuaalivaluuttapalveluiden tarjoajat tekivät ennätysmäisen määrän ilmoituksia rahanpesun selvittelykeskukselle. Vaikka määrät ovat oikeutetustikin tasaantuneet sen jälkeen, on tämä esimerkki siitä, miten lainsäädännöllä on mahdollista osallistaa myös kryptotoimijat rahanpesun estämiseen luomalla heidän toimintaansa samanlaisia kontrolleja ja vastuita, kuin esimeriksi pankeilla on tähän mennessä ollut.

[127] Mukaillen Rahanpesun selvittelykeskus 2023, s. 14.
[128] Rahanpesun selvittelykeskus 2023, s. 14–15.

Talousrikollisuuden torjunnan estämisen lainsäädännöllistä kehikkoa Euroopassa hallinnoi EU:n komissio. 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 (jäljempänä viides rahanpesudirektiivi) on säännellyt rahanpesun estämistä EU:ssa jo vuodesta 2018.

Viimeiset viisi vuotta on ollut kehitteillä uusi direktiiviehdotus jäsenvaltioissa toteutettavista toimenpiteistä rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen ja direktiivin (EU) 2015/849 kumoamisesta, CoM(2021) 423 final (jäljempänä kuudes rahanpesudirektiivi) sekä asetusehdotus rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen, CoM(2021) 420 final, (jäljempänä rahanpesuasetusehdotus) ja uudesta valvontaviranomaisen AMLA:n perustamisesta annetusta asetusehdotus eurooppalaisen rahanpesun ja terrorismin rahoittamisen estämisviranomaisen perustamisesta, CoM(2021) 421 final (jäljempänä AMLA-asetusehdotus). Näiden lisäksi pakettiin kuuluu uusi maksun tiedot -asetus, jota on käsitelty luvussa 3.4.

Näiden lisäksi sääntelykehikkoon kuuluu kansallisesti implementoitu viides rahanpesudirektiivi, eli Suomessa laki rahanpesun ja terrorismin rahoittamisen estämisestä. Näiden lisäksi esimerkiksi EBA ja Finanssivalvonta antavat ohjeita ja määräyksiä lainsäädännön noudattamiseen käytännössä. Lisäksi FATF:n standardit ja selvitykset sääntelyn noudattamisen tilasta antavat ohjeistuksia maailmanlaajuisesti ja pitävät silmällä sitä, millä tavoin rahanpesusääntelyä ja FATF:n ohjeistuksia noudatetaan.[129]

4.2.1 Rahanpesun ja terrorismin rahoittamisen estämisen sääntelykehikko

EU:n sääntelykehikko rahanpesun ja terrorismin rahoittamisen estämisestä perustuu vahvasti FATF:n ohjeistuksiin ja standardeihin. Terrorismin rahoittamisen osalta FATF:n suositukset koskevat terrorismin rahoittamisen kriminalisointia, kansallisten talouspakoteohjelmien yhtenäistämistä YK:n pakoteohjelmiin sekä erityistä huomiota kiinnitettäviin yleishyödyllisiin yhdistyksiin, jotka ovat alttiita terrorismin rahoittamiselle.[130]

EU:n tavoite terrorismin rahoittamisen estämisessä on ollut häiritä, estää ja hajottaa terrorismin rahoittamisen verkkoja. Tarkoituksena on vähentää

[129] FATF, What we do.
[130] Fabe – Kaunert – Romaniuk 2023, s. 329–334.

olemassa olevia resursseja terrorismille sekä jäljittää osallisia ja estää osallistumasta terrorismin rahoittamisen toimenpiteisiin. Tärkeänä osana rahanpesua ja terrorismin rahoittamisen estämistä EU:ssa ovat rahanpesudirektiivit, joista tällä hetkellä voimassa on jo viides direktiivi.[131]

Moni EU:n toimenpiteistä terrorismin rahoittamisen osalta valuu pakoteregiimien alle, joita käsitellään tarkemmin luvussa 4.3.

Ensimmäinen EU:n rahanpesudirektiivi on tullut voimaan vuonna 1991. Tämän jälkeen direktiivejä on uusittu useaan otteeseen. Muutos riskiperusteiseen lähestymistapaan tapahtui kolmannessa rahanpesudirektiivissä.[132]

Neljännen rahanpesurdirektiivin tarkoituksena oli estää unionin rahoitusjärjestelmän hyödyntäminen rahanpesuun. Direktiivissä säännellään mm. riskiperusteisesta lähestymistavasta, asiakkaan tuntemisvelvollisuudesta, tosiasiallisia edunsaajia koskevien tietojen selvittämisestä ja sääntelyn kohteena olevien ilmoitusvelvollisuuksista.

Riskiperusteisen lähestymistavan tarkoitus on ohjata resursseja sinne, missä riskejä havaitaan eniten. Valvottavien tulee itse määritellä oma riskiarvio, jossa asiakkaat jaotellaan eri riskiluokkiin sekä määritellä tehostetun tuntemisen toimet esimerkiksi PEP-asiakkaiden kohdalla.[133]

Viidennen rahanpesudirektiivin 33 artiklassa, määrätään valvottavien ilmoitusvelvollisuudesta. Rahanpesun selvittelykeskukselle on ilmoitettava kaikki epäilyttävät liiketoimet sekä niiden yritykset.

Rahanpesudirektiivissä on säädelty myös automatisoiduista järjestelmistä, joilla pankkitilien haltijoiden tietoja voidaan toimittaa viranomaisille, sääntelyn tuleminen osaksi virtuaalivaluuttojen tarjoajia ja taidekauppiaita sekä toimenpiteistä asiakkaan tuntemiseen ja tehostetun tuntemisen toimenpiteisiin. Asiakkaan tuntemista käsitellään tarkemmin luvussa 4.3.

Rahanpesun estämiseen liittyy myös toinen maksajan tiedot -asetus. Taustalla on FATF:n suositukset sähköisistä varainsiirroista. Varainsiirron mukana tulee toimittaa tiedot maksajasta sekä maksun saajasta. Näitä tietoja ovat maksun saajan nimi ja tilinumero. Lisäksi tietojen oikeellisuus on todennettava maksunpalveluntarjoajan toimesta ja heillä on oltava tehokkaat toimenpiteet sen varmistamiseksi, että tietojen puuttuminen tai puutteellisuus havaitaan.

[131] Fabe – Kaunert – Romaniuk 2023, s. 288–289.
[132] Gurulé – King – Walker 2018, kappale 3.
[133] Ibid.

Kansallisesti Suomessa on ollut haasteita ja heikkouksia rahanpesun ja terrorismin rahoittamisen torjunnassa. Vuonna 2019 Suomi joutui FATF:n tarkkailuun, sillä Suomessa on ollut puutteita rahanpesun ja terrorismin rahoittamisen estämisessä. FATF:lle raportoitiin vuosittain kehitystoimenpiteet ja lokakuussa 2023 Suomi päästettiin tästä tarkkailusta pois.[134]

Puutteita oli erityisesti valvonnan resursseissa, joita oli liian vähän, riskiperusteisuus puuttui valvonnasta, rahanpesun estämisen puutteista ei annettu sanktioita ja valvottavilla ei ollut selkeitä ohjeistuksia, kuinka rahanpesua ja terrorismin rahoittamista tulisi estää. Kaikkia edellä mainittuja kohtia on paranneltu mutta kuitenkin tulee huomioida, että FATF:n velvoitteet kehittyvät ja Suomen tulee pystyä tehokkaaseen valvontaan ja ohjeistuksiin. Haasteita Finanssivalvonnan mukaan tuovat erityisesti talouspakotteiden valvominen sekä kryptotoimijoiden valvonta.[135]

Kansallisesti EU:n rahanpesudirektiivit on saatettu kansalliseen lainsäädäntöön laissa rahanpesun ja terrorismin rahoittamisen estämisestä. Suomessa rahanpesun valvontarekisteriä ylläpitää Aluehallintovirasto rahanpesulain 5 luvun 2 §:n mukaan. Lisäksi valvonnasta säädetään rahanpesulain 7 luvussa. Valvonnasta vastaavat Finanssivalvonta, poliisihallitus, patentti- ja rekisterihallitus sekä aluehallintovirasto.

4.2.2 Rahanpesuasetus ja kuudes rahanpesudirektiivi

Europolin tutkimuksen mukaan jopa 1 % Euroopan vuosittaisesta bruttokansantuotteesta liittyy epäilyttäviin liiketoimiin liitettäviin varoihin. Rahanpesu on merkittävä riski Euroopan alueen taloudelle ja kansalaisten turvallisuudelle. Euroopan komissio on luonut merkittävän lainsäädännöllisen paketin liittyen rahanpesun ja yleisesti talousrikollisuuden torjunnan riskien hallitsemiseksi EU:n alueella.[136]

Yhtenä tärkeimmistä päämääristä on yhtenäistää EU:n alueen sääntelyä. Aiemmin ei ole ollut voimassa kaikkia jäsenmaita velvoittavaa rahanpesuasetusta mutta paketti sisältää nyt ehdotuksen sellaisesta. Tarkoitus on myös lisätä yhteistyötä rahanpesun selvittelykeskusten välillä ja lisätä myös sääntelyn valvontaa luomalla uusi viranomainen, AMLA.[137]

Esitys uudesta rahanpesuasetuksesta pitää sisällään lisäyksiä uusista ilmoitusvelvollisista, joihin kuuluisivat mm. kryptovarapalveluiden tarjoajat ja

[134] Vasara 2023.
[135] Ibid.
[136] Euroopan komissio 2024, s. 1.
[137] Ibid.

joukkorahoitusalustat, sijoittamiseen perustuvia oleskeluoikeusjärjestelyitä välittävät toimijat sekä ylellisyystuotteiden kauppiaat sekä esimerkiksi jalkapalloseurat.[138]

Lisäksi tarkennuksia tulisi tosiasiallisten edunsaajien analysointiin. Tosiasiallisten edunsaajien kohdalla tulisi analysoida niin omistusta kuin määräysvaltaan perustuvaa hallinnointia yrityksissä. Tarkoituksena on pystyä paremmin selvittämään omistajat ja edunsaajat myös EU:n ulkopuolelta, mikäli yhtiö harjoittaa toimintaa EU:ssa sekä poistaa omistuksen monikerroksisuuden hyödyntämisen mahdollistaminen.[139]

Asetuksessa myös määritetään käteisnostojen enimmäisraja 10 000 euroon. Jäsenmaiden on mahdollista asettaa kansallisesti vielä matalampi käteisnostoraja.[140]

Lisäksi tehostettua asiakkaan tuntemisvelvollisuutta tulee noudattaa kaikissa liiketoimissa ja liikesuhteissa, joissa on mukana korkean riskin kolmansia maita. FATF ylläpitää korkean riskin kolmansien maiden listausta.[141]

Asetukseen on siirtymässä ehdotuksen mukaan yksityisellä sektorilla sovellettavat säädökset. Kuudes rahanpesudirektiivi sisältäisi puolestaan kansalliseen lainsäädäntöön sisällytettäviä säännöksiä, joten se sisältäisi mm. rahanpesun selvittelykeskuksia ja kansallisia valvontaviranomaisia koskevaa sääntelyä sekä tosiasiallisten omistajien ja edunsaajien rekistereitä koskevaa sääntelyä.[142]

Direktiivissä tosiasiallisia omistajia ja edunsaajia koskevien rekistereiden tulee sisältää talouspakotteiden kohteena oleviin henkilöihin tai yhteisöihin yhteydessä olevat yhteisöt tai järjestelyt. Oikeus tarkastella rekisterin tietoja annettaisiin myös muille tahoille, kuten journalisteille.[143]

Lisäksi rahanpesun selvittelykeskuksilla tulee olla direktiiviehdotuksen mukaan pääsy suoraan ja välittömästi rahoitus-, hallinto- ja lainvalvontatietoihin. Myös EU:n tasolla sekä kansallisesti on edelleen tärkeää suorittaa riskiarviointeja.[144]

---

[138] Eurooppa-neuvosto 2024.
[139] Ibid.
[140] Ibid.
[141] Ibid.
[142] Ibid.
[143] Ibid.
[144] Ibid.

AMLA-asetusehdotuksen tarkoitus on lisätä ja yhtenäistää valvontaa EU-alueella ja tukea rahanpesun selvittelykeskusten yhteistyötä. AMLA perustetaan Frankfurtiin ja sen on tarkoitus aloittaa toimintansa vuoden 2025 puolivälissä.[145]

AMLA:n tarkoitus on valvoa korkeariskisimpiä finanssilaitoksia EU:ssa sekä kryptovarapalvelujen tarjoajia, koordinoida kansallisia rahanpesun selvittelykeskuksia, tukea myös finanssialan ulkopuolisia aloja, jotka ovat sääntelyn piirissä ja määrätä vakavien rikkomuksien kohdalla taloudellisia seuraamuksia.[146]

4.3 Asiakkaan tunteminen ja pakotteet

Asiakkaan tuntemisesta säädetään kansallisesti rahanpesulaissa luvussa 3. Laissa säädetyt tuntemistietoihin liittyvät toimet tulee toteutua tai muussa tapauksessa valvottava ei saa perustaa asiakassuhdetta tai suorittaa liiketointa. Riskiperusteista arviointia tulee noudattaa luvun 1 §:n mukaan, eli ottaa huomioon riskit, jotka kohdistuvat maantieteellisiin alueisiin, palveluihin ja tuotteisiin, liiketoimiin, jakelukanaviin ja teknologioihin.

Asiakkaat tulee tunnistaa ja todentaa heidän henkilöllisyys asiakassuhdetta perustettaessa 2 §:n mukaan. Lisäksi asiakas on tunnistettava ja henkilöllisyys todettava mm. tilanteissa, joissa kyseessä on satunnainen asiakkuus, liiketoimen suuruus on vähintään 10 000 euroa tai kyse on epäilyttävästä liiketoimesta.

Lisäksi tosiasialliset edunsaajat tulee selvittää ja tarvittaessa pyytää tarkempi omistusrakenteen kuvaus sekä saada selvitys asiakkaan liiketoiminnasta ja taloudellisesta asemasta. Asiakastietojen hankkimisessa saa hyödyntää 4 §:n mukaan eri tietolähteistä saatavilla olevia tietoja ja asiakastietoja tulee riskiperusteisen lähestymistavan mukaan seurata jatkuvasti.

Valvottava voi riskiperusteisen arvion mukaan hyödyntää yksinkertaistettua asiakkaan tuntemisvelvollisuutta. Puolestaan valvottava voi riskiperusteisen arvion mukaan hyödyntää tehostettua asiakkaan tuntemisvelvollisuutta. Lisäksi yksinkertaistettuun ja tehostettuun asiakkaan tuntemisvelvollisuuteen on annettu valtioneuvoston asetus, josta käy ilmi tapaukset, joissa kyseisiä velvollisuuksia tulee noudattaa.

[145] Eurooppa-neuvosto, Terrorismin torjunta EU:ssa.
[146] Ibid.

Valtioneuvoston asetus rahanpesun ja terrorismin rahoittamisen estämisestä annetussa laissa tarkoitetuista merkittävistä julkisista tehtävistä 610/2019 määrittelee PEP-aseman. PEP-statuksella oleville asiakkaille tulee kohdentaa tehostetun asiakkaan tuntemisen toimenpiteitä. Lisäksi rahanpesulain 12 §:n mukaan kirjeenvaihtajasuhteisiin ja 13 a §:n mukaan Euroopan talousalueen ulkopuoliseen korkean riskin valtioon liittyviin liiketoimiin ja maksuihin tulee kohdentaa tehostettuja tuntemistoimenpiteitä.

Rahanpesulain 16 §:ssä säädetään pakotesääntelyn ja jäädyttämispäätösten noudattamiseen liittyvästä asiakkaan tuntemisesta. Ilmoitusvelvollisten tulee seurata velvoittavaa pakotesääntelyä sekä jäädytyspäätöksiä.

YK:n turvallisuusneuvoston antamat pakotteet täytäntöön pannaan EU:ssa neuvoston päätöksillä ja asetuksilla ja lisäksi EU:n on mahdollista asettaa autonomisia rajoittavia toimenpiteitä pakotteiden osalta. Nämä pakotteet ovat Suomessa suoraan velvoittavaa sääntelyä. Lisäksi Suomen osalta noudatetaan myös Yhdysvaltojen OFAC:n asettamia pakotteita.[147]

Suomessa pakotesääntely liittyy lakiin eräiden Suomelle Yhdistyneiden kansakuntien ja Euroopan unionin jäsenenä kuuluvien velvoitusten täyttämisestä (659/1967) eli niin sanottu pakotelakiin. Lisäksi varojen jäädyttämisestä annettu laki varojen jäädyttämisestä terrorismin torjumiseksi 3.5.2013/325 on osa pakotesääntelykokonaisuutta.

Näiden lisäksi Finanssivalvonta julkaisi maaliskuussa 2024 ensimmäisen pakotteisiin liittyvän määräykset ja ohjeet kokoelman, joka koskee erityisesti asiakkaan tuntemisvelvollisuutta. Määräykset ja ohjeet kokoelmassa määrätään rahanpesulain mukaisien valvottavien pakotteita koskevan riskiarvion muodostamisesta, pakotemonitoroinnista, asiakkaan ja tosiasiallisten edunsaajien tunnistamisesta sekä vastuiden selkiyttämisestä.[148]

Asiakkaiden jatkuva seuranta ja pakotemonitorointi tulee olla tarpeeksi tehokasta ja siinä tulee ottaa huomioon pakkoteiden osalta tehty riskiarvio. Kirjeenvaihtajasuhteiden osalta tulee selvittää kirjeenvaihtajasuhteen osapuolen riittävät pakotetoimet. Asiakaskantaa tulee myös pakotemonitoroida liiketoimien ja maksujen ohella. Pakotemonitoroinnin osalta tulee noudattaa pakotesääntelyä ja kansallisia jäädytyslistoja ja listat tulee olla ajantasaiset ja päivittää viipymättä uusien listauksien mukaisiksi. Rahanpesun selvittelykeskukselle tulisi tehdä ilmoitukset mahdollisista pakotteiden kiertämisistä ja pakotteiden rikkomisista.[149]

---

147 Pursiainen 2021, s. 20–21.
148 Finanssivalvonta määräykset ja ohjeet 03/2024.
149 Ibid.

5 Pankkien riskienhallinta

Pankkeihin kohdistuu useita erilaisia riskejä, joita lainsäädännöllä pyritään hallitsemaan. Vakavaraisuuteen, luottoriskien hallintaan, stressitesteihin ja ympäristöriskien hallintaan on erilaista pankkeja koskevaa sääntelyä.[150] Tämän työn kannalta olennaista on kuitenkin käsitellä nimenomaan rahanpesuun liittyviä riskejä pankkien osalta.

Rahanpesun ensimmäisessä vaiheessa pyritään sijoittamaan likainen raha lailliseen järjestelmään.[151] Pankit ovat osa laillista taloudellista järjestelmää ja ne ovatkin usein ensimmäisen kohde, johon likaista rahaa tulee. Siksi pankkien riskienhallinta on erityisen tärkeässä roolissa rahanpesun estämisessä.[152]

Tässä kappaleessa käsitellään pankkien kohtaamia rahanpesun riskejä sekä näiden rahanpesuriskien hallintaa pankeissa.

5.1 Rahanpesuriskit

Pankit kohtaavat paljon erilaisia riskejä ja riskienhallinnan funktio pankkien toiminnassa on tärkeässä roolissa. Rahanpesun riskienhallinta on yksi kalliimmista riskienhallinnan funktioista. Se tuottaa pankeille paljon henkilöstökuluja mutta suuremmat kulut voivat realisoitua seuraamusmaksuina. Siksi rahanpesuriskien hallinta on erittäin tärkeää myös taloudellisesta näkökulmasta.[153]

Rahanpesun ensimmäisessä vaiheessa varat halutaan sijoittaa rahoitusjärjestelmään, jonka jälkeen pyritään häivyttämään rahan rikollinen alkuperä.[154] Jotta alkuperää ei päästäisi häivyttämään laillisessa talousjärjestelmässä, tulee pankeilla olla riskienhallinnallisia keinoja tämän toiminnan mahdollisimman tehokkaaseen estämiseen.

Rahaa voi virrata pankkeihin esimerkiksi huumekaupasta tai varoja halutaan hyödyntää terroristisiin tarkoituksiin. Rahanpesuriski voi liittyä myös rajat ylittäviin maksuihin tai toimintaan voi liittyä käteisvarat, joita on kuljetettu liian suuria määriä esimerkiksi valtioiden rajojen yli.[155] Monet rahanpesua

[150] Buch 2024.
[151] Sharman 2011, s. 17–18.
[152] Hyttinen 2021, s. 2.
[153] Dill 2020, s. 249.
[154] Riccardi 2022, s. 12.
[155] Ibid.

harjoittavista pyrkivätkin siirtämään varoja sellaisille alueille ja sellaisiin maihin, joissa rahanpesun kontrollit eivät ole niin tiukat. Siksi rahanpesun riski voi olla erityisen suuri juuri rajat ylittävissä maksuissa.[156]

Riskinä tietenkin on, että rikollinen raha pääsee osaksi järjestelmää. Rahanpesua voidaan harjoittaa myös muulitilien kautta. Suomessa on havaittu useita tapauksia, joissa yksityishenkilöille tarjotaan työtä, jonka tarkoituksena on hyödyntää kyseisen henkilön omaa tiliä muulitilinä. Muuleja on ketjussa usein useita ja kaikkien muulien tarkoitus on saada maksut näyttämään laillisilta ja häivyttää varojen alkuperää.[157]

Pankkeihin kohdistuu myös maineriskiä mahdollisesta rahanpesusta heidän järjestelmiensä kautta. Mediassa on useasti vuosien aikana uutisoitu erilaisista tapauksista, joissa pankit ovat saaneet sakkoja merkittävistä puutteista rahanpesun estämisessä. Esimerkiksi Danske Bank sai aikaan kohun vuonna 2018, jolloin paljastui, että heidän järjestelmiensä läpi oli virrannut jopa 200 miljardia rikollista alkuperää olevia varoja.[158]

Valitettavasti Danske Bank ei ole ainoa myös suomalaisten tuntema pankki, joka on saanut kyseenalaista huomiota rahanpesun estämisen haasteista. Nordean ja tanskalaisen DNB:n yhteisomistuksessa ollut Luminor joutui ison rahanpesukohun keskelle, kun Blackstone osti osan Luminorista ja oston yhteydessä huomattiin, että Luminorin tileiltä on virrannut epäilyttävistä lähteistä peräisin olevia varoja yhteensä jopa 3,9 miljardia euroa. Nordean Baltian toiminnot saivat suuren kolauksen uutisen yhteydessä, sillä osa Nordean asiakkaista oli saanut jatkaa pankin asiakkaana, vaikka heidän toiminta täytti rahanpesun kriteerit.[159]

Seuraamusmaksuja rahanpesun estämisen toimien laiminlyönneistä asettaa Suomessa Finanssivalvonta. Mikäli Finanssivalvonnan tarkastuksessaan selviää puutteita valvottavan rahanpesun ja terrorismin rahoittamisen tai pakoteriskien hallinnassa, voivat he asettaa seuraamusmaksuja valvottavalle. Lisäksi Finanssivalvonta voi antaa julkisia moitteita, jotka usein nostetaan myös mediassa esiin ja vaikuttavat valvottavan maineeseen. Vuosina 2021–2022 Finanssivalvonta tarkasti OP-Ryhmän pankkien rahanpesun estämisen toimintaa ja huomasi siellä puutteita. OP-Ryhmän asiakkaiden tuntemistiedoissa oli puutteita ja asia nousi mediassa esiin.[160] Vaikka OP-Ryhmä ei tässä tapauksessa saanut muuta kuin julkisen moitteen, tapausta puitiin mediassa

[156] Beckett Velez 2024, kappale 1.
[157] Yle 2011.
[158] Yle 2022.
[159] Ibid.
[160] Pietiläinen 2023.

ja tällaisilla tapauksilla voi olla vaikutuksia pankkien maineeseen luotettavana pankkina.

Finanssivalvonta seuraa myös pakotteiden noudattamista valvottaviensa osalta. Finanssivalvonta on ilmoittanut lisäävänsä myös pakotteiden osalta valvontaa ja tarkastuksia erityisesti vuoden 2024 aikana. Tämä voi mahdollisesti tarkoittaa pankeille seuraamusmaksuja, mikäli pakoteprosessit eivät ole kunnossa.[161]

Uusi Euroopan laajuinen rahanpesun estämistä valvova viranomainen AMLA tulee myös vaikuttamaan rahanpesun estämisen toimiin pankeissa. Komission asetusehdotuksen CoM(2021) 421 mukaan AMLA tulee valvomaan kaikista korkeariskisimpiä toimijoita ja AMLA:lla on myös mahdollisuus asettaa seuraamusmaksuja sääntelyn vastaisesta toiminnasta. On mahdollista, että AMLA:n aloittaessa tarkastuksia, saadaan tarkempaa yleistä käytäntöä valvojien osalta siihen, kuinka tarkastuksia tehdään ja missä tilanteissa seuraamusmaksuja annetaan.

Suomi on ollut aiemmin FATF:n tehostetussa seurannassa vuodesta 2019, jolloin FATF arvioi, että Suomella oli useita kehityskohtia rahanpesun ja terrorismin rahoittamisen estämisen toimissa. Yksi kehityskohteista Suomen osalta on ollut valvojien toimintavaltuudet.[162] Tämä kertoo siitä, että Suomen Finanssivalvonta on vasta viimeisien vuosien aikana kehittänyt toimintaansa nykyiseen suuntaan, joten tarkastuksien laadun sekä seuraamusmaksujen kehitystä vielä kaivataan lisää. Jotta kaikki valvottavat ottavat tosissaan valvojan arviot ja tarkastukset, tulisi rangaistukset myös olla tarpeeksi korkeita.

5.2 Rahanpesuriskien hallinta pankeissa

Rahanpesun riskienhallinta on tärkeässä osassa pankin toimintaa, ja pankit ovat oleellisessa roolissa rahanpesun estämisessä. Riskienhallinta ja sen luomat toimet ja prosessit kuvaavat aina pankin oman riskienottohalukkuuden tasoa ja riskienhallinta perustuu pankin riskiarvioon.[163]

Johto on yleisesti lopullisessa vastuussa yhtiöön kohdistuvista riskeistä. Riskienhallinnan funktion yksi tärkeimmistä rooleista onkin johdolle raportointi. Riskienhallinnan funktion tulee määritellä riskiarviossa riskinottohalukkuus ja tehdä toimia, joiden mukaan pankissa toimitaan riskien mitigoimiseksi.[164]

[161] Finanssivalvonta 2023.
[162] Valtionvarainministeriö b 2023.
[163] Chapman 2018, s. 38.
[164] Dill 2020, s. 96.

Rahanpesuriskien hallinta koostuu Chapmanin mukaan yhdeksästä eri tärkeästä osa-alueesta:

1. Hallinnosta ja ympäristön kontrolleista
2. Osaamisen resursseista; työntekijöiden kouluttamisesta, palkkauksesta ja johtamisesta
3. Riskiarviosta
4. Asiakkaan tuntemisen prosesseista
5. Transaktiomonitoroinnista
6. Datan hallinnasta ja tiedolla johtamisesta
7. Liiketoimintojen tuesta ja ohjeistamisesta
8. Sisäisestä ja ulkoisesta tarkastuksesta
9. Kokonaisvaltaisesta järjestelmien monitoroinnista ja kehityksestä AML strategiaympyrän mukaan

AML strategiaympyrä on strateginen työkalu, jonka avulla on mahdollista miettiä rahanpesun ja yleisesti talousrikollisuuden torjunnan riskienhallintaa. Chapman on nostanut AML strategiaympyrään koulutuksen ja toiminta-ohjeet, tietoisuuden riskeistä ja sitoutumisen riskienhallintaan, estämisen ja havaitsemisen tärkeyden, ilmoitukset ja tutkinnat, monitoroinnin ja arvioinnin.[165]

Suomen suurimalla finanssialan toimijalla OP:lla on verkkosivuillaan hyvä esimerkki siitä, mitä kaikkea rahanpesun ja pakoteriskien hallinta käytännössä tarkoittaa. Riskienhallinta koostuu asiakkaan tuntemisen prosesseista, pakotemonitoroinnista, käyttäytymisen ja maksuliikenteen monitoroinnista, huijausten ja väärinkäytösten ehkäisemisestä ja havaitsemisesta, ohjeistamisesta ja kouluttamisesta sekä teknologioiden kehittämisestä.[166]

Rahanpesun riskienhallinnassa oleellista on myös pankkien tekemät epäilyttävän liiketoimen ilmoitukset rahanpesun selvittelykeskukselle. Rahanpesulain 4 luvun 1 §:n mukaan SAR-ilmoitukset tulee tehdä aina, jos jotain epäilyttävää havaitaan sekä finanssivalvonnan pakotteita koskevien määräysten ja ohjeiden mukaan myös epäiltäessä esimerkiksi pakotteiden kiertämistä, tulee SAR-ilmoitus rahanpesun selvittelykeskukselle tehdä.[167]

Pankkien monitoroinnin tehokkuudessa ja toiminnassa on varmasti kehitettävää. Teknologiaa ja prosesseja tulisi kehittää tehokkaammaksi, jotta rahanpesun estäminen olisi tuottavampaa.[168] Riskienhallinnan toiminnot ovat erittäin kalliita toimintoja pankkien toiminnassa ja kustannuksien

[165] Chapman, 2018, s. 6.
[166] OP Ryhmä.
[167] Finanssivalvonta määräykset ja ohjeet 03/2024.
[168] Beckett Velez 2024, kappale 1.

minimoimiseksi ja tehokkuuden maksimoimiseksi tulisi kehittää erityisesti teknologioita tukemaan rahanpesun ja terrorismin rahoittamisen estämisen työtä.[169]

5.2.1 Riskinottohalukkuus ja riskiarvio

Riskienhallinnallisen kehikon kehittämisen ensimmäinen vaihe on riskiarvion luominen. Riskiarvion avulla tutkitaan ja selvitetään ulkoisia ja sisäisiä riskitekijöitä, jotka voivat vaikeuttaa pankin toimintaa. Kun riskit on havaittu ja tunnistettu, riskiarviossa analysoidaan niiden mahdolliset vaikutukset ja niiden todennäköisyydet.[170]

Riskiarviossa tulisi arvioida tunnistetut riskit, jotka ovat riskejä, joita on aiemmin kohdistunut pankkiin tai vähintään samankaltaisia kuin pankkiin aiemmin kohdistuneet riskit sekä arvioida myös tunnistamattomia riskejä. Kaikki riskejä tulisi mitata ja arvioida. Tunnistamattomien riskien arviointi onkin haastavampaa, sillä nimensä mukaisesti ne ovat vielä pankille tuntemattomia. Riskienhallinnan tulisi olla kuitenkin järjestäytynyt niin, että myös tuntemattomia tai ennalta-arvaamattomia riskejä voidaan sietää ilman liiketoiminnan keskeyttämistä tai loppumista.[171]

Riskiarviota tulee päivittää säännöllisesti ja riskejä tulee arvioida johdonmukaisesti koko ajan. Riskiarvion perusteella tehdään tarvittavat toimenpiteet, jotta havaittuja riskejä voidaan mitigoida tarpeellisilla toimilla.[172] Riskiarviossa tulisi arvioida maakohtaista riskiä, henkilöriskiä, tuoteriskiä ja jakelukanavia koskevaa riskiä sekä teknologiaan liittyviä riskejä.[173]

Euroopan pankkiviranomainen EBA on antanut ohjeita pankeille riskiarvion muodostamisesta.[174] Finanssivalvonta on lisännyt EBA:n ohjeistukset omaan määräykset ja ohjeet kokoelmaan.

Finanssivalvonnan määräykset ja ohjeet kokoelmat rahanpesun ja terrorismin rahoittamisen estämisestä 2/2023 sekä pakotesääntelyn ja kansallisten jäädyttämispäätösten noudattamiseen liittyvästä asiakkaan tuntemisesta 4/2023 antavat myös ohjeita pankeille siitä, millä tavoin rahanpesu- ja pakoteriskiä tulisi hallita. Määräyksiä ja ohjeita liittyy siihen, että niin rahanpesun ja terrorismin rahoittamisen estäminen kuin pakotteet tulee ottaa

[169] Beckett Velez 2024, kappale 6.
[170] Dill 2020, s. 100.
[171] Ibid, s. 100–101.
[172] Ibid, s. 96.
[173] Chapman 2018, s. 63.
[174] EBA/GL/2021/02

huomioon riskiarviossa ja niiden todellisia riskejä tulee arvioida pankkia kohtaan.[175]

Finanssivalvonnan määräyksissä ja ohjeissa kuitenkin huomioidaan valvottavan koko sekä toiminnan laajuus. Riskiarvion sisältö ei siis valvottavan koko ja toiminnan laajuus huomioon ottaen ole saman laajuinen eri kokoisten pankkien välillä.[176] On luonnollista, että pienemmällä toimijalla ei ole esimerkiksi yhtä suurta asiakaskantaa kuin isommalla toimijalla sekä palvelut voivat vaihdella eri pankkien välillä koosta ja toiminnan laajuudesta riippuen. On siis kohtuullista, että tämä näkyy myös valvojan vaatimuksissa riskiarvion suhteen.

Riskiarviossa tulee selvitä, millaista rahanpesun riskiä palvelut ja tuotteet aiheuttavat ja miten niitä voidaan hyödyntää rahanpesussa ja terrorismin rahoittamisessa. Lisäksi jäännösriskistä pitää tehdä arvio ja arvioida salliiko pankin riskinottohalukkuus jäännösriskin. Riskiarvio tulee päivittää aina tarpeen tullen ja tarkastaa, että se on edelleen ajantasainen vähintään vuosittain.[177]

Riskiarvion osana määritellään pankin riskinottohalukkuus. Sillä tarkoitetaan tiettyä riskin tasoa, jota pankki on valmis sietämään määriteltyjen toimenpiteiden valossa. Riskinottohalukkuutta olisi tärkeää määrittää laadullisten kriteerien lisäksi myös kvantitatiivisin menetelmin, jotta olisi mahdollista muodostaa mahdollisimman objektiivinen käsitys hallinnoitavista riskeistä. Riskinottohalukkuuden arvion tulee perustua pankin riskiprofiiliin sekä sen riskikapasiteettiin.[178]

Riskiarvion ja määritellyn riskinottohalukkuuden tulee olla sellaisella tasolla, että sitä voidaan soveltaa kaikkiin pankin toimialueisiin. Sen tulee sisältää toimet, joiden avulla riskejä mitigoidaan ensimmäisessä puolustuslinjassa sekä miten niistä raportoidaan johdolle.[179]

Riskinottohalukkuuden linjaus tulee olla tehtynä pitkälle aikavälille. Riskinottohalukkuutta kuvaava linjaus tulee lisäksi hyväksyttää sisäisellä tarkastuksella.[180]

5.2.2 Riskiperusteinen lähestymistapa

[175] Finanssivalvonta määräykset ja ohjeet 2024.
[176] Finanssivalvonta määräykset ja ohjeet 2023 ja 2024.
[177] Finanssivalvonta määräykset ja ohjeet 2023.
[178] Dill 2020, s. 96–97.
[179] Dill 2020, s. 97.
[180] Finanssivalvonta määräykset ja ohjeet 2023.

Pankkien tulee hyödyntää riskiperusteista lähestymistapaa niissä toimissa, joiden avulla se pyrkii mitigoimaan rahanpesuriskejä. Riskiperusteisen lähestymistavan tarkoitus on mitoittaa toimet riskiarviossa tunnistettuihin riskeihin ja niiden hallintaan oikeasuhtaisesti. Mikäli johonkin palveluun, asiakasryhmään tai muuhun vastaavaan huomataan kohdistuvan korkeampaa riskiä, tulisi riskiperusteisen lähestymistavan mukaan kyseisiin asiakasryhmiin tai palveluihin kohdistaa tehostettuja toimia. Sama toimii myös toisinpäin. Mikäli jokin asiakasryhmä tai palvelu ei aiheuta merkittäviä riskejä ja riskiarviossa huomataan, että riskit ovat pienet, voidaan silloin hyödyntää yksinkertaisempia riskienhallintatoimia siinä tapauksessa.[181]

Esimerkiksi kryptovarojen osalta, mikäli riskiarviossa arvioidaan kryptovarojen suhteen kohonnut riski, voidaan siihen kohdistaa tehostettuja riskienhallintatoimenpiteitä. Tämä voi tarkoittaa esimeriksi tehostettua transaktiomonitorointia kryptovaratoimijoiden osalta tai voidaan pohtia, pitäisikö esimerkiksi asiakkuuksien avaaminen kryptovaratoimijoiden osalta kieltää.

Pankit hyödyntävät riskienhallintakeinona myös de-riskingiä eli pyrkivät välttämään kokonaan esimerkiksi korkeariskisten asiakkaiden asiakkuuksien avaamista. De-risking liittyy riskinottohalukkuudessa siihen, että ei haluta tehdä liiketoimia tiettyjen tahojen, valtioiden tai alueiden kanssa, joihin liittyy kohonnut rahanpesun ja terrorismin rahoittamisen riski. Pankit, jotka hyödyntävät paljon de-riskingiä, eivät joudu panostamaan teknologian kehityskuluihin yhtä paljon ja siksi tämä ratkaisu voidaan nähdä houkuttelevana.[182]

FATF on kuitenkin ottanut kantaa de-riskingiin ja sen tuomiin riskeihin. FATF:n mukaan on ymmärrettävä, että mikäli kaikki korkean riskin asiakkaat tai toimialat ajetaan pois pankeista, ne siirtyvät todennäköisesti hyödyntämään sellaisia kanavia, jotka eivät ole reguloituja samalla tavoin kuin pankit.[183]

Esimerkiksi kryptovaratoimijoiden osalta, joihin voidaan katsoa liitettävän korkea rahanpesuriski, riskiarvio ja riskinottohalukkuus tulisi asettaa niin, ettei riskinä ole alan toimijoiden keskittyminen vähemmän säännellylle markkinalle. Tämä voisi pahimmillaan lisätä jo muutenkin korkeariskisen toimialan rahanpesun riskejä.

Riskiperusteista lähestymistapaa käytetään myös asiakassuhteen perustamisessa, jonka aikana pyritään selvittämään asiakkaan kohdistuvat riskit ja sen

[181] FATF 2023 s. 10.
[182] Beckett Velez 2024, kappale 12.
[183] FATF 2014.

perusteella mitigoimaan jatkossa asiakkaaseen kohdistuvaa riskiä. Asiakassuhteen perustamisen yhteydessä onkin erityisen tärkeää selvittää asiakassuhteen tarkoitus ja luonne, miksi asiakas haluaa pankin asiakkaaksi ja mitä palveluita se haluaa käyttää ja mistä syystä. Lisäksi yritysasiakkaiden kohdalla on tärkeää ymmärtää toiminnan luonne ja laajuus sekä tunnistaa kaikki tosiasialliset edunsaajat niin omistuksen kuin määräysvallan perusteella.[184]

Asiakassuhteen alussa on tärkeää löytää korkeariskiset asiakkaat, esimerkiksi PEP-henkilöt, kirjeenvaihtajasuhteet, private banking-asiakkaat sekä esimerkiksi kryptovaratoimijat, joihin kohdistuu kohonnut rahanpesuriski.[185] Kaikki asiakkaat tulee jaotella riskiluokkiin, joiden perusteella asiakkaan riskejä hallitaan. Riskiluokittelumallin tulee huomioida useita eri tekijöitä riskiluokittelussa.[186] Korkean riskin asiakkaiden riskiarvio olisi hyvä päivittää vuosittain, keskiriskin ja matalan riskin asiakkaat harvemmin.[187]

5.2.3 Kolmen puolustuslinjan malli

Jotta riskienhallinta on organisoitu mahdollisimman tehokkaasti ja sitä valvotaan, pankit hyödyntävät kolmen puolustuslinjan mallia. Ensimmäinen puolustuslinja on liiketoiminta, jossa rahanpesuriskien mitigointi näkyy arjessa, toinen puolustuslinja on riskienhallintatoiminto ja vaatimusten valvoja ja kolmas on sisäinen tarkastus.[188]

EBA:n ohjeiden mukaan ensimmäinen puolustuslinja edustaa liiketoimintayksiköitä, jotka tunnistavat ja analysoivat riskejä luotujen prosessien mukaisesti. Liiketoimintayksiköiden tulee noudattaa operatiivisessa työssä pankin riskinottohalukkuutta ja riskiarviota sekä raportoitava johdolle.[189]

Toinen puolustuslinja eli compliance on vastuussa riskien tunnistamisesta, hallinnasta ja riskiarviosta. Compliance-toiminnon tarkoitus on auttaa liiketoimintayksiköitä tulkitsemaan riskiarviota ja riskinottohalukkuutta sekä auttaa liiketoimintayksiköitä muodostamaan tehokkaat prosessit riskienhallinnan mukaisesti. Lisäksi toiminnon tehtäviin kuuluu sisäisten ohjeiden noudattamisen seuranta ja raportointi johdolle.[190]

Kolmas puolustuslinja eli sisäinen tarkastus on itsenäinen ja riippumaton toiminto. Sisäinen tarkastus vastaa ensimmäisen ja toisen puolustuslinjan

[184] Beckett Velez 2024, kappale 1.
[185] Ibid.
[186] Finanssivalvonta määräykset ja ohjeet 2023.
[187] Beckett Velez 2024, kappale 1.
[188] Ibid, kappale 2.
[189] EBA/GL/2021/05.
[190] Ibid.

tarkastuksesta sekä sisäisen tarkastuksen tarkoitus on tehdä tarkastuksia, jotta varmistetaan, että prosessit ja toiminnot ovat tarpeeksi tehokkaita ja johdonmukaisia.[191]

Kolmen puolustuslinjan mallissa on myös kehitettävää. Esimerkiksi Silicon Valley -pankin kaatuminen Yhdysvalloissa osoitti sen, kuinka tärkeä osa pankkien kolmen puolustuslinjan malli on erilaisten riskien hallinnassa.[192] Vaikka Silicon Valley -pankin kaatuminen ei liity rahanpesuriskeihin suoraan, voidaan kuitenkin heidän virheistä oppia ja kehittää kolmen puolustuslinjan mallia paremmaksi, jotta sen avulla voidaan estää tehokkaammin myös rahanpesua pankkien osalta.

Yksi tärkeimmistä asioista on osaava riskienhallinnan johtaja, joka saa tarpeeksi resursseja sekä vapauksia ja auktoriteettia pankin sisällä hoitaakseen tehtäväänsä. Pankeilla tulisi olla lisäksi riskienhallinnan komitea, joka voi päättää riskitoleranssista, arvioida raportointia sekä huolehtia säännönmukaisesta toiminnasta. Komitealla tulisi olla pätevää ja asianmukaista riskienhallinnan kokemusta, jotta he todella voivat arvioida pankin kohtaamia riskejä ja kehittää niiden hallintaa.[193]

Näiden lisäksi pankeilla tulisi olla moderneja teknologisia ratkaisuja riskien arvioimiseksi. Pankkien tulisi hyödyntää analyyttisiä riskimalleja analysoidakseen eri riskejä, joita pankkiin kohdistuu. Malli nostaisi esiin merkittävimmät riskit, joihin tulisi puuttua. Myös valvojien valvonnan tehokkuus herättää kysymyksiä.[194] Onko valvonta tarpeeksi tehokasta, jotta heikot riskienhallintamallit ja toimintatavat löytyvät? Millä tavoin esimeriksi Suomessa Finanssivalvonta voisi tehostaa valvontaa rahanpesuriskien osalta? Seuraavaksi käsitellään talousrikollisuuden torjunnan tulevaisuutta.

5.3 Talousrikollisuuden torjunnan tulevaisuus pankeissa

Rahanpesun valvonta ja erityisesti sen tehokkuus on oleellinen kysymys pohdittaessa talousrikollisuuden torjunnan tulevaisuutta pankeissa. Valvojilla on olennainen rooli siinä, millaiset standardit kansallisesti ja pian myös EU:n tasolla rahanpesun torjuntaan sekä muuhun talousrikollisuuden torjuntaan asetetaan. Uuden EU-tason valvojan AMLA:n osalta valvonta tulee ainakin yhtenäistymään ja mahdollisesti myös kiristymään, kun saadaan koko unionia koskeva rahanpesun valvontaviranomainen.

[191] EBA/GL/2021/05
[192] Lam 2023.
[193] Ibid.
[194] Ibid.

Toki Finanssivalvonta on Suomessa tehnyt myös tarkastuksia pankkeihin ja määrännyt seuraamusmaksuja rahanpesulain puutteista. Esimeriksi vuonna 2019 S-Pankki Oyj sai 980 000 euron suuruisen seuraamusmaksun rahanpesulain velvoitteiden puutteista.[195] Yhdysvalloissa on nähtävillä rahanpesun estämisen seuraamusmaksujen määrän kasvu. Esimerkiksi eräs kansainvälinen pankki sai vuonna 2023 seuraamusmaksun 189 miljoonan dollarin edestä ja samainen pankki oli saanut seuraamusmaksun jo muutama vuosi aiemmin 99 miljoonan dollarin edestä.[196]

On kuitenkin mielestäni olennaista miettiä, ovatko esimerkiksi Euroopassa annettavat seuraamusmaksut tarpeeksi suuria, jotta rahanpesun torjunnan sääntelyä noudatetaan varmasti tarpeeksi korkealla tasolla? On huomioitava myös edellä mainitusta Yhdysvaltojen tapauksesta se, että tarkastuksen kohteena ollut pankki sai ensin seuraamusmaksun rahanpesulain puutteista mutta ei kyennyt tekemään tarvittavia toimenpiteitä, jolloin viranomaiset langettivat uuden, suuremman seuraamusmaksun. Oliko seuraamukset liian pienet suhteessa siihen, kuinka paljon mahdollisesti kalliita muutoksia pankin olisi pitänyt tehdä, jotta he olisivat olleet sääntelyn mukaisia? Vai ovatko viranomaiset kuitenkin vielä hampaattomia, jolloin ei koeta realistisena uhkana sitä, että pankkien toiminta voisi pahimmassa tapauksessa, vaikka estyä, jos rahanpesun sääntelyä ei noudateta?

On myös huomioitava, että uusien toimijoiden astuessa mukaan finanssimarkkinalle, tulee pankkien kiinnittää erityisen paljon huomiota siihen, millä tavoin ne vaikuttavat heidän toimintaan sekä pankkeihin kohdistuviin riskeihin. Lainsäädäntö tulee aina myöhässä ja uudet teknologiat ja ratkaisut voivat toimia markkinalla pitkäänkin, ennen kuin porsaanreiät peittävää sääntelyä saadaan aikaiseksi. Uudet teknologiat ja toimijat eivät automaattisesti tarkoita uusia rahanpesun riskejä vaan uusien innovaatioiden riskit realisoituvat ja ne ymmärretään todennäköisesti aina viiveellä. Kuitenkin rikolliset pyrkivät hyödyntämään tapoja rahanpesuun uusien väyliä kautta ja erityisesti vähemmän säännellyt markkinat herättävät kiinnostusta. Siksi onkin tärkeää, että pankeissa panostetaan ketteriin järjestelmiin ja dynaamiseen riskiarvioon, jotta pystytään huomioimaan markkinoiden nopeat muutokset ja uudet korkeariskisemmät toimijat, kuten kryptovaratoimijat ajoissa ja niiden tuomat riskit saadaan osaksi riskiarviota ja riskienhallintaa.

Kuten tässä työssä on tullut ilmi useasti, lainsäädäntö kiristyy jatkuvasti rahanpesun ja terrorismin rahoittamisen estämisen, pakotteiden sekä asiakkaan tuntemiseen liittyvien prosessien osalta. Pankeille talousrikollisuuden

[195] Finanssivalvonta 2019.
[196] Comply advantage 2024.

torjunnan organisaatiot ovat suuri kuluerä. Riskienhallintaan ja compliance-toimintoihin palaa entistä enemmän rahaa sääntelyn kasvaessa.

Lisäksi uusi sääntely ja siihen nopeasti sopeutuminen on tärkeää, sillä myös valvojat kohdistavat huomiota entistä tarkemmin pankkien rahanpesusäänte-lyn noudattamiseen. Kuluja lisäisi merkittävästi myös seuraamusmak-sut.[197]

Forresterin vuonna 2023 tekemän tutkimuksen mukaan talousrikollisuuden torjunnan compliance-kustannukset ovat nousseet erityisesti vuoden 2023 aikana. Ranskassa vuosittaiset talousrikollisuuden torjunnan compliance-kustannukset ovat tutkimuksen arvioiden mukaan 25.3 miljardia dollaria ja Saksassa 32.5 miljardia dollaria. Lisäksi huomionarvoista tutkimuksessa on se, että yksi suurimmista uhkista liittyen rahanpesuun on vastaajien mukaan kryptovaroihin liittyvät liiketoimet, joiden määrä on kasvanut suuresti.[198]

Kulujen noustessa myös pankkeja kiinnostaa mahdollisuudet hyödyntää uu-sia teknologioita ja tapoja hallita riskejä sekä noudattaa alati muuttuvaa sääntelyä.

Kehittynyttä lohkoketjuteknologiaa voisi olla mahdollista hyödyntää asiak-kaan tuntemisen ja rahanpesun estämisen prosesseissa. Tällä hetkellä jokai-nen finanssilaitos ylläpitää omaa rekisteriä asiakastiedoista ja vaikka asiakas olisi asiakkaana esimerkiksi useammassa pankissa, jokaisessa pankissa ke-rätään ja analysoidaan erikseen saman henkilön tuntemistiedot.[199] KYC-pro-sessia voitaisiin tehostaa lohkoketjuteknologian avulla ja tämän avulla sääs-tää jopa 2,5 miljardia dollaria vuosittaisista kuluista.[200]

Lohkoketjuteknologian avulla voisi olla mahdollista säilyttää ihmisten oike-aksi tunnistettuja tuntemistietoja luotettavalla tavalla jokaisen finanssilai-toksen yhteisessä hajautetussa tilikirjassa. Jos asiakkaan tietoja päivitettäi-siin, se vaatisi kaikkien tahojen hyväksynnän, joka tarjoaisi avoimuutta ja mahdollisuuden tarkastaa tiedot oikeiksi. Tällä tavoin asiakkaan tuntemisen prosessiin voisi saada tehokkuutta mutta samalla luotettavuutta ja se vähen-täisi asiakkaan tuntemiseen käytettyjä resursseja pankeissa ja muissa finans-silaitoksissa.[201]

Tulee kuitenkin ymmärtää, että haasteita tietojen jakamiseen voi aiheuttaa GDPR-asetus sekä kilpailuoikeudelliset asetelmat. Edellä mainitut

[197] Beckett Velez 2024, kappale 6.
[198] Forrester Research 2023, s.9.
[199] Bashir 2023, kappale 21.
[200] Eerola ym. 2019, kappale 2.0.3.
[201] Bashir 2023, kappale 21.

mahdollisuudet ovat todennäköisesti tällä hetkellä vielä mahdottomia saavuttaa ainakaan Suomen pankkitoimialalla.

6 Kryptovarojen riskit rahanpesun välineenä

Kryptovarojen anonymiteetti tuottaa erityisesti haasteita niiden käytössä rahanpesuriskien hallinnan suhteen. Toisin kuin perinteisiä fiat-valuutalla tehtyjä transaktioita, kryptotransaktioita ei voida samalla lailla jäljittää. Lisäksi tämän hetken implementoitu lainsäädäntö ei sisällä kaikkia eri kryptovaratoimijoita, joka jättää aukon rahanpesun estämiseen monien toimijoiden osalta.[202]

On huomioitava, että kryptovarat ja sen taustalla oleva lohkoketjuteknologia eivät ole pohjimmiltaan pahoja innovaatioita, jotka olisi rakennettu rahanpesun jouhevoittaminen mielessä. Kyse on neutraaleista innovaatioista, jotka kuitenkin sisältävät sellaisia piirteitä, jotka selvästi kiinnostavat rikollisia pesemään rahaa näiden innovaatioiden avustuksella.

6.1 Kryptovarojen käyttö rahanpesussa

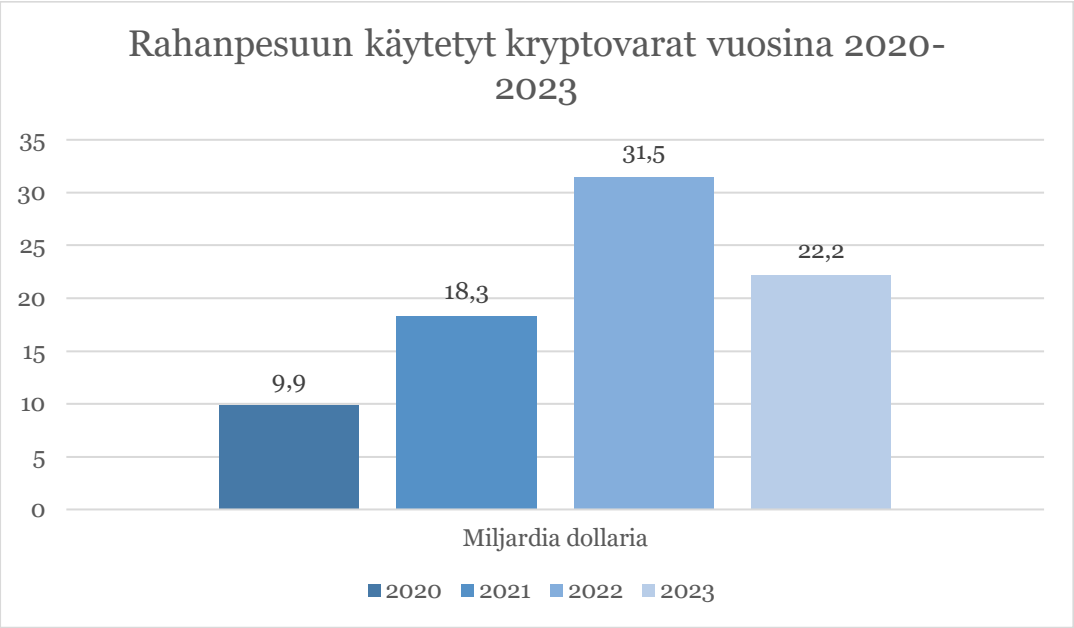
Yksi merkittävimmistä kryptovarojen historiaa muovanneista tapahtumista on Bitcoinin kehitys. Bitcoinin jälkeen kasvoi myös alustoja, joissa hyödynnettiin juuri Bitcoinin tuomaa anonymiteettiä. Ross Ulbricht kehitti pari vuotta Bitcoinin kehittämisen jälkeen Silk Road-nimisen kauppapaikan Torverkkoon, joka mahdollisti laittomien tuotteiden myynnin anonyymisti käyttämällä Bitcoinia maksuvälineenä.[203]

Yhdysvaltain viranomaiset pääsivät kuitenkin Bitcoin-transaktioiden jäljille, sillä he seurasivat lohkoketjulla transaktioita. Ulbricht pidätettiin ja hän sai tuomion mm. rahanpesusta.[204]

Kryptovarojen alkuaikoina ongelmaksi muodostuivat myös esimerkiksi Bitcoinin mahdottomuus hyödyntää sitä erilaisten tuotteiden ostamiseen, sillä se ei kelvannut maksuvälineenä virallisilla kauppapaikoilla. Tästä tarpeesta syntyi kryptolompakot, jotka mahdollistivat eri kryptovaluuttojen oston fiat-valuutalla.[205] Myöhemmin lompakkopalvelut ovat mahdollistaneet eri kryptovaluuttojen vaihdon sekä erilaisten kryptosijoitustuotteiden ostamisen. Lompakkojen käyttö auttaa myös rikollisia saamaan kryptovarat fiat-valuutaksi, joiden avulla rikollisella alkuperällä saadut varat on helpompi saada osaksi kansainvälistä laillista talousjärjestelmää ja varoja pääsee hyödyntämään.[206]

[202] Eerola ym 2019, kappale 3.0.2
[203] Carlisle 2024, s. 1–2.
[204] Ibid, s. 12–13.
[205] Bashir 2023, kappale 6.
[206] Carlisle 2024, s. 24–25.

Covid-19 pandemia vauhditti rikollisuuden kasvua verkossa. Kun koko maailma joutui eristäytymään koteihinsa ja hyödyntämään erilaisia digitaalisia palveluita, muutti se myös rikollisten tapaa toimia. Hajautetun rahoituksen palveluissa on sijoitettuna rikollista varaa ja kryptovaluutta pyritään hyödyntämään rahanpesussa. On kuitenkin huomioitava, että tällä hetkellä kaikista kryptotransaktioista noin 1 %:n on arvioitu liittyvän rikollisuuteen. Kryptovaluuttoja käytetään kuitenkin paljon esimerkiksi sijoitushuijauksissa.[207]



208

Chainalysisin arvioiden mukaan kryptovaroja hyödynnettiin vuoden 2023 aikana rahanpesussa 22.2 miljardia dollarin arvosta. Vaikka laskua on tapahtunut vuoteen 2022, jolloin arvioiden mukaan kryptovaroja pestiin 31,5 miljardia dollaria, on kaikkien kryptotransaktioiden määrä laskenut vuodesta 2022, joka heijastuu myös vuoden 2023 pestyjen varojen määrään.[209]

Kryptovaroja on myös hyödynnetty pakotteiden kiertämisessä. Venäjän hyökkäyssodan alkamisen jälkeen Ukrainassa, EU ja mm. Yhdysvallat on asettivat merkittävän määrän uusia pakotteita Venäläisille tahoille. Pakotteita on tullut jatkuvasti lisää ja sitä mukaa myös pakotteiden alaiset tahot pyrkivät etsimään keinoja kiertääkseen pakotteita, sillä Venäjä on pääosin suljettu globaalin rahansiirtojärjestelmän ulkopuolelle. Valtionvarainministeriö on nostanut pakotteiden kiertämisen virtuaalivarojen avulla merkittäväksi rahanpesun riskiksi. On vaikea arvioida tarkkaan, kuinka laajaa

[207] Europol 2023, s. 6.
[208] Mukaillen Chainalysis 2024, s. 24.
[209] Chainalysis 2024, s. 24.

toiminta on ollut mutta viranomaisten tietoon on tullut tapauksia, joissa venäläisiltä ruplatileiltä on tehty varainsiirtoja myös Suomeen hyödyntämällä kryptolompakkoja ja vaihtopalveluita.[210]

Tammikuussa 2023 myös suljettiin viranomaisten toimesta Bitzlato-niminen kryptoalusta, jota epäillään likaisen rahan pesemisestä sekä EU-pakotteiden kiertämisestä. Alustan avulla oli mahdollista vaihtaa nopeasti kryptovaluuttoja rupliksi. Vaihto-alustan on epäilty saaneen jopa 2.1 miljardia euroa varoja ja näistä varoista arvioidaan 46 % liittyneen rikollisuuteen.[211]

Myös maailman suurimmat kryptopörssit Binance ja Coinbase ovat mahdollistaneet venäläisten asiakkaidensa kaupankäynnin alustoilla kansainvälisistä pakotteista huolimatta. Kryptoalustat antavat siis mahdollisuuksia myös pakotteiden kiertämiseen.[212]

Kryptolompakkoja hyödynnetään usein rikollisuudessa, sillä kaikki eivät tunnista asiakkaitaan kuten pitäisi, joten väärällä henkilöllisyydellä on mahdollisuus siirtää käteistä kryptovaroiksi. Tämän jälkeen kryptovaroja vaihdetaan toiseen.[213] Tässä vaiheessa hyödynnetään myös miksereitä, joiden tarkoitus on yhdistää eri tahojen varoja ja siirtää niitä eteenpäin niin, että varojen alkuperää on todella vaikeaa selvittää. Chainalysis on arvioinut, että miksereiden avulla on pesty miljardien arvosta varoja.[214]

Rahanpesuun käytettyjä kryptovaroja lähetetään eteenpäin laittomista lompakoista. Varoja siirretään eniten keskitettyihin vaihtopalveluihin sekä hajautettuihin rahoituspalveluihin.[215] Rahanpesussa voidaan hyödyntää myös kryptokasinoita, joiden avulla voidaan pelata erilaisia uhkapelejä ja sijoittaa varoja sinne.[216]

Perinteiset kryptovaluutat kuten Bitcoin tarjoavat anonymiteettiä tai oikeastaan pseudoanonymiteettiä. Transaktiot on mahdollista jäljittää yksilöityjen tunnisteiden avulla lohkoketjusta, joka mahdollistaa myös rahanpesun selvittämistä. Kuitenkin markkinoille on tullut uusia täysin anonyymeja yksityisvaluuttoja, jotka käyttävät teknologiaa hyödyksi henkilöllisyyden peittämiseksi.[217]

---

[210] Valtionvarainministeriö 2024, s. 82.
[211] Europol 2023, s. 8.
[212] Valtionvarainministeriö 2024, s. 82.
[213] Europol 2023, s. 16.
[214] Chainalysis 2023.
[215] Chainalysis 2024, s. 25.
[216] Europol 2023, s. 15.
[217] Carlisle 2024, s. 68.

Monero on yksi tällaisista valuutoista, joita hyödynnetään mm. Silk Roadin kaltaisilla alustoilla anonymiteetin takaamiseksi. Anonyymi valuutta kiinnostaa erityisesti rikollisia, sillä se helpottaa rahanpesua merkittävästi.[218]

Hajautetut vaihto- ja rahoituspalvelut ovat myös rikollisten suosiossa. Hajautetut vaihtopalvelut eli DEX:t hyödyntävät älysopimuksia eikä hajauttamattoman vaihtopalvelun tavoin varoja oteta vaihtopalvelun puolesta haltuun vaan palvelussa varat siirtyvät haltijalta toiselle automatisoidun markkinan kautta. DEX:ien avulla on mahdollista myydä ja ostaa varoja ilman henkilöllisyyden todentamista.[219]

6.2 Kryptovarojen rahanpesuriskit pankeille

Pankeilla on mielenkiintoinen rooli tällä hetkellä kryptotoimijoiden osalta. Rikollista alkuperää olevia varoja voi virrata pankkien tileille ja sen seuranta on haastavaa. Lisäksi kryptovarapalveluita käyttää entistä enemmän pankkien asiakkaista ja pankkien tulisi myös miettiä omia mahdollisuuksiaan osallistua kryptomarkkinoille, jotta he eivät menetä asiakkaita kryptopalveluille.[220]

Pankeille kryptovarat tuovat kuitenkin tällä hetkellä eniten riskejä siinä, että rikollista alkuperää olevia varoja päätyy pankkien järjestelmiin. Transaktioiden seuraaminen on pankeille haastavaa, sillä maksupalveluntarjoajia voi olla ketjussa useampia eikä varmuutta tunnistamisen toimenpiteistä esimerkiksi ole.[221]

Kryptovaratoimijoilla on heikommat AML-kontrollit, joten sieltä siirtyville varoille pankkien tileillä on paljon riskejä. Kryptovaratoimijoilla on haasteita asiakkaan tuntemisessa, pakotemonitoroinnin puutteissa sekä riskienhallinnassa. Asiakkaaksi ottamisen yhteydessä kryptovaratoimijoille tulee tehdä tarkat ja tehostetut asiakkaan tuntemisen toimenpiteet.[222]

Kryptovaroja voidaan vaihtaa fiat-valuuttaan erilaisten tarjoajien toimesta. Kun varat on vaihdettu fiat-valuutaksi, voi pankkien olla haastavaa havaita varojen todellista alkuperää. Tällaisten varainsiirtojen huomaaminen esimerkiksi monitorointijärjestelmissä on haastavaa.[223]

---

[218] Carlisle 2024, s. 72.
[219] Ibid, s. 143–144.
[220] KPMG 2024.
[221] Valtionvarainministeriö 2024, s. 66.
[222] KPMG 2024.
[223] Bloomberg Law 2021.

Lisäksi bulvaanitoimintaa on haastavaa havaita. Asiakkaiden tilejä voidaan käyttää heidän tietämättään bulvaanitoimintaa, jossa varoja pyritään siirtämään uusille bulvaaneille ja kerrostaa varojen liikkeitä, jotta niiden alkuperän selvittäminen on haasteellisempaa.[224]

6.3 Kryptovarojen rahanpesuriskien hallinta

Kryptovaluuttojen ja kryptovaroja tarjoavien osalta kohonnutta rahanpesun riskiä tulee mitigoida pankeissa erilaisin toimin. Tietenkin lainsäädännöllä pyritään vaikuttamaan kryptovarojen rahanpesuriskiin ja siksi esimerkiksi MiCA asetus tuo paljon lisää rahanpesun ja terrorismin estämisen sääntelyä markkinalle. Kuitenkin myös pankeilla on tärkeä rooli siinä, miten he pystyvät mukautumaan uusiin innovaatioihin, jotka sisältävät korkean rahanpesun riskin.

FATF:n ohjeistukset kryptovaratoimijoille ovat liittyneet keskitettyihin palveluihin, jolloin kaikki tällaiset tahot ovat olleet osa FATF:n ohjeistuksia. Kuitenkin hajautettujen palveluiden lisääntyminen on aiheuttanut paljon rahanpesun riskejä, sillä esimerkiksi DEX:t eivät kerää henkilöllisyyksiä osallistujilta.[225] FATF:n päivitetyissä ohjeissa kuitenkin ohjeistetaan, että henkilöllisyydet tulee tunnistaa tahoilta, joilla on määräysvaltaa näissä järjestelmissä.[226] Vaikka jokin toimija toimii hajautetussa ympäristössä, kuuluu vastuu tuntemistoimenpiteistä ottaa.[227]

Puhuttaessa sääntelevien tahojen riskienhallinnasta, on hyvä mainita OFAC:n toiminta pakotelistauksissa, jotka liittyvät kryptomarkkinalla toimiviin tahoihin. OFAC on sanktioinut useita tahoja, jotka ovat hyödyntäneet virtuaalivaroja sekä kryptomarkkinaa esimerkiksi pakotteiden kiertämiseen. OFAC:n toimivalikoimaan kuuluu lisäksi näiden tahojen lohkoketjun yksilöityjien osoitteiden asettaminen sanktioiden kohteiksi, jolloin näiden kanssa ei saisi tehdä transaktioita.[228]

Pankkien riskienhallinnassa tulee huomioida kryptovaratoimijat myös niitä otettaessa pankin asiakkaiksi. Mikäli tällaisia tahoille avataan tili pankkiin tai tarjotaan muita palveluita, tulisi näihin tahoihin kohdistaa tehostettuja tuntemistoimenpiteitä ja jatkuvaa tehostettua seurantaa.[229] Riskiarviossa tulisi huomioida selkeästi tällainen asiakasryhmä, mikäli sellaisia on pankin asiakkaana. Pankkien tulisi varmistaa, että heillä on tehokkaat toimenpiteet

[224] Valtionvarainministeriö 2024, s. 66.
[225] Carlisle 2024, s. 153.
[226] FATF 2024.
[227] Carlisle 2024, s. 153.
[228] Chainalysis 2024, s. 70–71.
[229] KPMG 2024.

transaktiomonitorointiin ja pakotemonitorointiin erityisesti tällaisten asiakkaiden kohdalla ja asiakkaan tuntemistoimenpiteiden tärkeys korostuu tällaisissa tilanteissa.

Monet pankit eivät halua kuitenkaan tällaisia asiakkaita asiakkaikseen. On ymmärrettävää, että jotkut pankit riskiarviossaan ja riskinottohalukkuudessaan eivät halua ottaa riskiä kryptotoimijoista asiakkainaan. Näissä tilanteissa tulisi kuitenkin huomioida myös FATF:n ohjeistukset de-riskingistä. Todennäköistä on, että tällaiset toimijat siirtyvät esimerkiksi heikomman sääntelyn omaaviin valtioihin asiakkaiksi tai siirtyvät käyttämään sellaisia kanavia ja palveluita, joita ei säännellä ainakaan yhtä tiukasti.[230] Tämä nostaa kokonaisuudessa jo ennalta korkeaa riskiä tällaisen asiakasryhmän osalta.

Riskiarvion päivittäminen kryptotoimijoiden osalta on erityisen tärkeää, vaikka kryptotoimijoita ei olisikaan pankin asiakkaana. Mielestäni riskiarvion tulisi olla dynaaminen eikä vain kerran vuodessa tarkistettava ja päivitettävä pakollinen dokumentti. Riskiarviota voitaisiin hyödyntää jatkuvana, dynaamisena strategiatyökaluna, jonka avulla pankkien riskienhallintaa voitaisiin ketteröittää nopeasti muuttuvassa maailmassa.

Jotta pankit voivat mm. monitoroinnin avulla mitigoida kryptovaroista syntyvää rahanpesun riskiä, tulee toimiala tuntea todella hyvin. Kuten aiemmin on todettu, voi pankkien olla haastavaa havaita ulkopuolelta tulevista varoista sitä, liittyvätkö ne kryptovaroihin. Siksi olisi tärkeää, että alalla toimivat toimijat on tunnistettu, jotta näihin voidaan hyödyntää tehostettuja toimia.[231]

Transaktiomonitoroinnin osalta voidaan lisätä esimerkiksi kontrolleja kryptovaroja tarjoavien yritysten nimille, jotta järjestelmä hälyttää aina tällaiselle taholle menevästä tai saapuvasta maksusta. Lisäksi monitorointiin voisi lisätä kryptosanastoa, jotta kryptoliitännäisiä maksuja saataisiin tarkemmin kiinni ja selvitettyä niiden tarkoitus.[232]

Kryptotransaktioiden jäljittämiseen on tulossa muutoksia uuden maksun tiedot -asetuksen myötä. Asetuksen myötä kryptovarojen tarjoajien tulee sisällyttää varainsiirtoon mukaan mm. seuraavat tiedot: toimeksiantajan nimi ja osoite, tilinumero tai esimerkiksi hajautetun tilikirjan tai virtuaalivaratilin osoite tai numero, henkilötietoasiakirjan numero, asiakasnumero tai

[230] FATF 2014.
[231] Balestrino ym. 2023.
[232] Bloomberg Law 2021.

syntymäaika ja syntymäpaikka sekä varojen saajan nimi ja tilinumero tai vastaava tieto.

Rahanpesuriskin hallinnassa haasteita on tuonut juuri kryptotransaktioiden jäljittämisen haasteet. Vaikka Yhdysvalloissa esimerkiksi Silk Roadin jäljille ja lopulta sen sulkemiseen päästiin seuraamalla transaktioita lohkoketjussa, vaatii se paljon viranomaisresursseja ja yleensä tarpeeksi ison ja kiinnostavan rikoksen tai esimeriksi rikollisjärjestön, jotta resurssit transaktioiden jäljittämiseen saadaan.[233]

Tälläkin hetkellä on kuitenkin olemassa toimijoita, jotka tarjoavat palveluita ja järjestelmiä kryptovarasiirtojen jäljittämiseen. Esimerkiksi kryptotoimija Chainalysis tarjoaa palvelua, jonka kautta voi selvittää tarkemmin transaktioiden osapuolia ja jäljittää transaktioita.[234]

Pankeilla voisi olla myös käytössä älykäs lohkoketjuanalyysijärjestelmä, blockchain intelligence (BI). BI:n avulla voidaan monitoroida lohkoketjussa tapahtuvia transaktioita. Järjestelmän on mahdollista hyödyntää tekoälyä, joka oppii löytämään rahanpesuun liittyviä transaktioita. Nämä järjestelmät liittyvät usein viranomaisiin, jotka hyödyntävät näitä järjestelmiä selvittäessään rahanpesurikoksia. Järjestelmä voi hyödyntää myös talousrikollisuuden torjunnassa käytettyjä tekniikoita, joiden avulla voidaan havaita rahanpesua ja terrorismin rahoittamista sekä pakotteiden kiertämistä. Asiakkaan tuntemisen KYC-prosessien lisäksi on mahdollista hyödyntää transaktioiden tuntemisen KYT-prosesseja, joiden avulla jokainen lohkoketjun transaktio voidaan arvioida niiden toteutuessa. KYT-prosessi voi reaaliaikaisesti havaita, onko maksu menossa esimerkiksi sanktioituun lompakkoon.[235]

[233] Carlisle 2024, s. 22.
[234] Chainalysis, crypto investigations.
[235] Balestrino ym 2023.

7 Johtopäätökset

Kryptovarat luovat todellisen riskin rahanpesulle pankeissa maailmanlaajuisesti. Koska kyse on globaalista talousjärjestelmästä ja myös kryptovarat ovat globaali ilmiö, kohdistuu myös Suomeen todellisia uhkia.

Lisääntyvä sääntely nostaa pankkien kustannuksia, joista haetaan jatkuvasti säästökohteita. Jo valmiiksi runsaasti säännelty finanssiala ei ole ketterin toimija ottamaan omakseen uudenlaisia toimintatapoja ja teknologioita rahanpesun estämiseen ja löytääkseen rikollisia ja heidän likaista raha järjestelmästään. Kuitenkin pankit ovat tärkeässä roolissa rahanpesun estämisessä ja torjunnassa.

On väistämätöntä luoda uudenlaisia ratkaisuja rahanpesun estämiseen. Usein sanotaan, että rikollisten jahtaaminen on kissahiiri leikkiä, jossa lainsäätäjät ja finanssitoimijat tulevat auttamatta jäljessä, kun rikolliset keksivät hyödyntää nopeastikin uusia, erilaisia tapoja toimia. Tämä on nähty myös kryptovarojen osalta. Arvioiden mukaan vuonna 2023 noin 22,2 miljardin dollarin edestä kryptovaroja käytettiin rahanpesuun.[236] Vaikka uudenlaiset innovaatiot ja teknologiat antavat mahdollisuuksia kehittää esimerkiksi finanssijärjestelmää, luovat ne myös uhkia kansainväliselle talousjärjestelmälle ja voivat edesauttaa rikollisuutta.

Lisääntyvää sääntelyä ehdottomasti tarvitaan, jotta kryptoalan rahanpesuriskejä voidaan hallita. Haaste lisääntyvälle lainsäädännölle kryptovarojen osalta voi olla kuitenkin se, että kryptotoimijat siirtyvät kolmansiin maihin, joissa ei ole yhtä tiukkaa sääntelyä kuin esimerkiksi EU:ssa. Myöskään kansainvälisiä standardeja kryptovaratoimijoiden sääntelylle ei ole, joten rikolliset pyrkivät hyödyntämään palveluita siellä, missä sääntelyä on vähiten.[237]

Yhdysvaltojen sekä EU:n viranomaiset ovat kuitenkin onnistuneet myös löytämään rikollisia toimijoita kryptovaramarkkinoilta sekä lopettamaan rikolliseen tarkoitukseen käytettäviä palveluita. Palvelut ovat todennäköisesti kuitenkin olleet olemassa ja käynnissä ennen kuin niiden toimintaan on viranomaisten toimesta voitu puuttua. Kuitenkin viranomaiset ovat lisänneet asiantuntijoita, joiden tehtävänä on selvittää ja tutkia kryptotransaktioita, joiden avulla voidaan päästä rahanpesun ja rikollisuuden jäljille.[238]

Pankeilla on jo tällä hetkellä olemassa olevia työkaluja, joita voisi kehittää, jotta ne palvelisivat paremmin myös kryptovaroista tulevaa riskiä. Pankkien

[236] Chainalysis 2024.
[237] Valtiovarainministeriö 2023, s. 82.
[238] Carlisle 2024, s. 59.

pakollinen riskiarvio voisi olla dynaamisempi ja sen ympärille voisi rakentaa uudenlaisia prosesseja, jotta riskejä voidaan arvioida jatkuvasti. Maailma ympärillä muuttuu ja uusia teknologioita saapuu, jotka muuttavat myös globaalia talous- ja pankkijärjestelmää. Pankkien tulee pystyä toimimaan ketterämmin muuttuvassa markkinassa ja havaita riskejä tehokkaammin.

Lisäksi uudenlaisia monitorointiskenaarioita ja -algoritmeja vaaditaan, jotta uudenlaisten riskien perässä voidaan pysyä. Lisäksi asiakkaan tuntemisen tärkeys korostuu rahanpesuriskejä hallitessa erityisesti kryptovarojen osalta. On erityisen tärkeää tuntea asiakkaat ja niiden käyttäytyminen kunnolla sekä tuntea yritysasiakkaiden toimiala ja niihin kohdistuvat riskit. Yleisesti kryptoalan kokonaisvaltainen tunteminen, koulutus ja tiedon lisääminen ovat elintärkeitä toimia pankeille, jotka haluavat tehokkaasti hallita kryptovarojen rahanpesuriskiä.

Moni muutos tarvitsee alleen varmasti paljon teknologista kehitystä. Talousrikollisuuden torjunnan organisaatiot työllistävät suuren määrän ihmisiä pankeissa ja organisaatio on suuri kuluerä pankeille.[239] Uusilla teknologioilla voidaan tehostaa jo olemassa olevia toimia sekä tuoda ohelle uusia tapoja hallita kryptoriskejä.

Euroopassa on havaittu yleisesti varovaista suhtautumista kryptovaroihin ja niihin kohdistuvat riskit otetaan vakavasti. Esimerkiksi Ruotsissa useat pankit ovat sulkeneet heidän asiakkaiden tilejä, mikäli tileiltä on havaittu transaktioita kryptopörsseihin. Lisäksi Belgia on yrittänyt saada kryptopörssi Bianancen pois markkinoiltaan. Belgian rahoitusviranomainen on asettanut Binancen toimintakieltoon.[240]

Kuitenkin yleisesti kryptomarkkinan houkuttelevuus lisääntyy, kun tieto lisääntyy ja ihmiset ovat kiinnostuneita kokeilemaan esimerkiksi uudenlaisia sijoitustuotteita, jotka voivat liittyä kryptovaroihin. Esimerkiksi Yhdysvalloissa lanseerattiin tammikuussa 2024 ensimmäiset bitcoin-etf -sijoitustuotteet. Etf-tuotteiden suosio oli suuri heti markkinoille pääsyn jälkeen ja jo ensimmäisenä kauppapäivänä rahastoja vaihdettiin 4,6 miljardin dollarin verran.[241]

Pankkien on hyvä myös pohtia omaa rooliaan kryptomarkkinalla. Pankit voivat menettää asiakkaitaan kryptotoimijoille, joten on myös mahdollista, että nähdään pankkien ottavan roolia kryptomarkkinalla.

[239] Forrester Research 2023, s.9.
[240] Valpola 2024.
[241] Räisänen 2024.

Sääntelyn kannalta yksi merkittävin haaste on liittyy siihen, että monet kryptotoimijat ovat jääneet sääntelyn ulkopuolelle. Tähän on onneksi tulossa muutos uuden MiCA-asetuksen myötä, jonka avulla myös kryptolompakot ja muut toimijat tulevat sääntelyn piiriin. Tulee kuitenkin huomioida, että myös tuleva sääntely koskee vain kryptotoimijoita, ei itse valuuttoja.

Lisäksi uuden rahanpesun valvovan viranomaisen AMLA:n toiminnan käynnistyminen voi vaikuttaa kryptotoimijoihin, sillä AMLA:n tarkoitus on valvoa korkeariskisiä toimijoita ja mahdollisesti AMLA:n avulla saadaan uudenlaisia käytänteitä ja tapoja suorittaa valvontaa. On kuitenkin mahdotonta vielä tässä vaiheessa sanoa, millaisia mahdollisia vaikutuksia AMLA:n toiminnalla voisi olla.

Haasteena valvonnassa on aina kuitenkin resurssien riittämättömyys. On haastavaa valvoa tehokkaasti suurta määrää toimijoita, erityisesti toimialaa, joka muuttuu alati. Tämä nostaa riskiä kryptomarkkinalla, sillä on hyvin mahdollista, että valvovan viranomaisen tarkastukset ja toimet eivät kata riittävästi koko toimialaa ja valvojat pystyvät keskittymään vain pieneen osaan toimijoita kerralla.

8 Yhteenveto

Tämän tutkielman tarkoituksena oli vastata neljään eri tutkimuskysymykseen, joiden avulla oli tarkoitus selvittää kryptovaroihin liittyvää rahanpesuriskiä ja niiden hallintaa lainsäädännön sekä pankkien riskienhallinnan avulla. Tutkielman tavoitteeseen pääsemiseksi oli olennaista tarkastella ensin tarkemmin kryptovarojen taksonomiaa sekä kryptovarojen taustalla toimivaa lohkoketjuteknologiaa. Olennaista työn tavoitteeseen pääsemiseksi oli myös tutkia tarkemmin lainsäädäntöä liittyen kryptovaroihin sekä rahanpesuun ja tämän jälkeen pohtia pankkien riskienhallinnan funktiota rahanpesun estämisen kannalta ennen kuin oli järkevää selvittää, millä tavoin kryptovaroja käytetään rahanpesuun ja miten näitä riskejä voidaan pankeissa hallita.

Tutkielman ensimmäisenä tutkimuskysymyksenä oli *"Millä tavoin kryptovaroja säännellään tällä hetkellä Euroopassa ja mitä haasteita sääntelyyn liittyy?"*. Kuten tutkielmasta käy ilmi, on tällä hetkellä voimassa oleva sääntely puutteellista sen osalta, mitkä kaikki toimijat sääntelyn piiriin kuuluvat. Kansallisesti voimassa oleva laki virtuaalivaluutan tarjoajista nimensä mukaan sääntelee vain tahoja, jotka tarjoavat virtuaalivaluuttoja ja sääntely astui voimaan vuonna 2019 rahanpesudirektiivin muutoksista johtuen. Sääntelyn mukaisesti kryptovaluutan tarjoajien tulee rekisteröityä ja lain mukana toimijat tulivat rahanpesusääntelyn piiriin.

Toisen tutkimuskysymyksen avulla tutkielmassa tutkittiin sitä, millä tavoin sääntely Euroopassa tulee muuttumaan kryptovarojen osalta. Kuten on jo aiemmin käynyt ilmi, on uusi asetus kryptovaroista tulossa voimaan vuoden 2024 aikana. Markets in Crypto Assets -asetus on merkittävä muutos kryptovarojen sääntelyyn EU:ssa. Asetuksen avulla määritellään erikseen kryptovarat sekä stablecoinit eli omaisuusreferenssitokenit sekä sähkörahatokenit. Lisäksi sääntelyn avulla sääntelykehikkoa saadaan laajennettua ja yhä useampi kryptovaratoimija kuuluu sääntelyn piiriin. MiCA-asetuksen myötä sääntelyn piiriin kuuluvat kryptolompakot, -kauppapaikat sekä liikkeeseenlaskijat. Sääntelykokonaisuuden tarkoitus on mm. lisätä sijoittajan suojaa sekä luoda rekisteri sääntöjä noudattamattomista toimijoista.

MiCA-asetuksen lisäksi toinen merkittävä sääntelymuutos liittyy maksun tiedot -asetukseen. Aiempi asetus ei kohdistunut kryptotransaktioihin mutta uuden asetuksen myötä myös kryptovarasiirtojen mukana tulee toimittaa merkittävä määrä tietoja niin maksajasta kuin maksun saajasta. Tämän avulla on tarkoitus estää kryptovarojen anonymiteettiä ja lisätä varainsiirtojen läpinäkyvyyttä. Lisäksi asetuksessa määritellään muutoksia

rahanpesulainsäädäntöön, jotta kaikki myös MiCA-asetuksessa mainitut toimijat tulisivat rahanpesulainsäädännön piiriin.

Kolmas tutkimuskysymys *"Millaisia riskejä kryptovarat tuovat rahanpesun ja terrorismin rahoittamisen näkökulmasta pankeille?"* kohdistaa katseet pankkeihin kohdistuviin riskeihin kryptovarojen osalta. Jotta pankkien rahanpesun ja terrorismin rahoittamisen toimintoja voidaan tarkastella, on tutkielmassa käsitelty ensin rahanpesusääntelyä, joka pankkeja velvoittaa. Lisäksi neljänteen tutkimuskysymykseen *"Miten kryptovarojen rahanpesuriskiä voidaan hallita lainsäädännön sekä pankkien riskienhallinnan kautta?"* vastatessa oli olennaista tarkastella myös pankkien riskienhallinnan funktiota, jotta on mahdollista ymmärtää, miten kryptovaroihin liittyviä rahanpesuriskejä voidaan hallita.

Kuten tutkielmassa on selvinnyt, liittyy kryptovaroihin kohonnut rahanpesuriski. Vaikka kryptovaroja ei alunperin ole kehitetty rahanpesua varten, liittyy kryptovaroihin sellaisia ominaisuuksia, jotka tekevät niistä kiinnostavan vaihtoehdon rahanpesulle. Kryptovaroille ominainen anonymiteetti, erilaisten varojen alkuperän häivyttämisen palvelut sekä vähäinen sääntely on lisännyt houkutuksia hyödyntää kryptovaroja rahanpesun välineenä.

Pankeille yksi suurimmista riskeistä kryptovaroihin liittyen on niiden alkuperän haastava tunnistaminen ja selvittäminen. Pankkeihin virtaa varoja eri kryptoalustoilta mutta pankeilla on vähäiset resurssit niiden selvittämiseen. Lisäksi tutkielmassa esittelyt erilaiset mikseripalvelut sekä perinteisten muulien käyttö luo riskejä, joita on vaikea havaita ja hallita.

Rahanpesuriskien hallintaan tärkeimmät keinot ovat varmasti pankeille jo tutut riskienhallintakeinot, joita tulisi hienosäätää ja parannella. Oleellista on myös aiheesta kouluttaminen. Lisäksi erilaiset teknologiset kehitykset ja eri toimijoiden tarjoamat tuotteet tuovat mahdollisuuksia riskienhallinnan kehittämiseen. Oleellista on kuitenkin se, että riskienhallintafunktio otetaan pankeissa tosissaan, siihen ollaan valmiita panostamaan ja kehittämään sitä, jotta riskit eivät pääsisi realisoitumaan.