Cryptocurrency and their use in money laundering and terrorism financing

Aleksi Sneck

2024 Laurea

Laurea University of Applied Sciences

Cryptocurrencies and their use in money laundering and terrorism financing

Aleksi Sneck

Safety, Security and Risk Management

Thesis

December, 2024

Laurea University of Applied Sciences **Abstract**

Degree Programme in Safety, Security and Risk Management

Bachelor's thesis

Aleksi Sneck

Cryptocurrencies and their use in money laundering and terrorism financing

Year 2024 Pages 34

In recent years, cryptocurrencies have become more central in the global finance world. The purpose of this thesis is to explain an evolving landscape of cryptocurrency usage in money laundering, how it poses a challenge to global financial systems and legislation, and how cryptocurrencies are linked to terrorism financing. The thesis researches the very basics of cryptocurrencies, along with delving deeper into their potential for carrying out illicit financial activities. It investigates the three stages of money laundering, known as placing, layering, and integration, and providing examples from Russia attempting to integrate cryptocurrencies into the finance system to evade international sanctions. This thesis reveals the complex schemes of money laundering with the support of cryptocurrencies, including mixing services, over-the-counter trades, and cross-chain transfers. It points out an important role that crypto-exchanges, such as Russian-based Garantex, play in the processing of large volumes of darknet marketplace-related illicit transactions.

This thesis expands the theoretical framework, which encompasses blockchain technology and cryptographic techniques, along with a regulatory framework and international efforts concerning money laundering within the context of the Financial Action Task Force (FATF) as well as the regulatory environment in European Union laws and regulations. Additionally, it examines countries that are categorized as high-risk by FATF.

Even though the regulatory bodies have succeeded in addressing the emergence of cryptocurrency-related financial crimes, there is still a significant challenge in this regard, since these technologies are developing rapidly, and digital assets tend to be anonymous by nature. This research concludes with suggestions for improving anti-money laundering strategies, including incorporating more advanced blockchain analysis tools into monitoring systems, upgrading the protocols of know-your-customer, and building greater cooperation between public and private sectors.

Keywords: Cryptocurrency, money laundering, financial crime, cryptocurrency legislation

Laurea ammattikorkeakoulu **Tiivistelmä**

Turvallisuuden ja riskienhallinnan koulutus

Tradenomi (AMK)

Aleksi Sneck

Kryptovaluutat ja niiden esiintyminen rahanpesussa ja terrorismin rahoittamisessa

Vuosi 2024 Sivumäärä 34

Kryptovaluutat ovat viime vuosina nousseet yhä keskeisemmäksi globaalissa taloudessa. Tämän opinnäytetyön tarkoituksena on havainnollistaa, miten kryptovaluuttoja hyödynnetään rahanpesussa, millaisia haasteita se tuo kansainväliselle rahoitusjärjestelmälle ja lainsäädännölle, sekä miten kryptovaluutat linkittyvät terrorismin rahoittamiseen. Opinnäytetyö käsittelee kryptovaluuttojen perusteita ja syventyy niiden käyttöön laittoman taloudellisen toiminnan harjoittamiseen. Se tarkastelee rahanpesun kolmea vaihetta, jotka ovat sijoittaminen, kerrostaminen, sekä integrointi. Lisäksi työhön sisältyy käytännön esimerkkejä siitä, miten Venäjä on kiertänyt heille asetettuja kansainvälisiä pakotteita kryptovaluuttojen avulla. Opinnäytetyö käsittelee myös monimutkaisia rahanpesumenetelmiä, kuten varojen hajauttamista, over-the-counter- eli digitaalisen valuutan kaupankäynnin vaihdantaa, sekä lohkoketjun välisiä varojen siirtoja. Työssä tutkitaan myös laitonta kaupankäyntiä edistäviä kryptovaluuttapörssejä, kuten Venäjällä toimivaa Garantexia, jotka liittyvät pimeän verkon markkinakauppaan.

Opinnäytetyö laajentaa teoreettista viitekehystä, joka tutkii lohkoketjuteknologiaa, kryptografisia menetelmiä, sekä kansainvälistä rahanpesua koskevia toimia Financial Action Task Force (FATF)- toimintaryhmän sekä Euroopan Unionin lainsäädännön puitteissa. Lisäksi se tarkastelee valtioita, jotka FATF on luokitellut korkean riskin maiksi.

Vaikka sääntelyelimet ovat onnistuneet torjumaan kryptovaluuttaan liittyvien talousrikosten ilmaantumista, talousrikollisuus on edelleen merkittävä haaste, sillä kryptovaluuttaan liittyvät teknologiat kehittyvät nopeasti ja digitaaliset siirrot ovat luonteeltaan anonyymejä. Lopuksi tässä tutkimuksessa annetaan ehdotuksia rahanpesun torjuntatapojen vahvistamiseksi, mukaan lukien kehittyneempien lohkoketjuanalyysityökalujen sisällyttäminen valvontajärjestelmiin, asiakkaan tuntemiseen liittyvien menettelytapojen päivittämistä, sekä julkisen että yksityisen sektorin yhteistyön lisäämistä.

Asiasanat: kryptovaluutta, rahanpesu, talousrikollisuus, kryptovaluuttojen lainsäädäntö

Table of Contents

List of Abbreviations

AML Anti-Money Laundering

AMLA Anti-Money Laundering Authority

CASP Crypto Asset Service Providers

CTF Counter-Terrorist Financing

CEX Centralized Exchange

DeFi Decentralized Finance

DEX Decentralized Exchange

EBA European Banking Authority

ECB European Central Bank

FATF Financial Action Task Force

FIU Financial Intelligence Unit

KYC Know Your Customer

OFAC Office of Foreign Assets Control

MiCA Markets in Crypto-Assets

MER Mutual Evaluation Report

NFT Non-Fungible Token

NBI National Bureau of Investigation

PoW Proof of Work

PoS Proof of Stake

UNODC United Nations Office on Drugs and Crime

VASP Virtual asset service provider

1 Introduction

The aim of the thesis is to raise awareness on the latest money laundering methods and methods used for terrorism financing. Terrorism financing is spreading phenomenon worldwide and even occurring in Europe because of the ongoing war in Ukraine. This phenomenon has resulted in sanctions evasions, as Russia utilizes cryptocurrencies for transactions. This thesis also provides a comprehensive view of virtual currencies, blockchain analysis, and examines their darker side.

The rise of cryptocurrencies in the last decade has revolutionized global finance, creating opportunities as well as notable challenges. The borderless, decentralized, anonymity nature of cryptocurrencies unlocks opportunities for financial integration in regions with limited access to banking services. However, these characteristics have made cryptocurrencies appealing to individuals and organizations engaged in illicit activities. The primary concern is their involvement in money laundering and terrorism financing. Such illegal activities damage global financial stability, generate criminal enterprises, and pose risks to national security. Anonymity of a cryptocurrency transaction causes challenges to regulators and law enforcement who face difficulty tracing such illicit funds back to their origins or destination. (European Parliament 2019.)

2 Implementation of the research

I began the thesis by reading relevant literature, which consisted of reports published from known from reliable organisations such as Financial Action Task Force (FATF), the main entity to develop policies for combating money laundering, followed by articles from The United Nations, Europol and European Union. Additional literature was gathered online from Google Scholar and timely information from cryptocurrency analytics organizations Chainanalysis, TRM Labs and Sanction Scanner. Chainanalysis publishes crypto crime annual reports which provided relevant statistics for my research. The topic is relatively new with limited sources available, which resulted in some difficulties for the research. The thesis will be submitted to the client, whose name will remain confidential.

3 Key concepts

Cryptocurrency is a digital or virtual currency that functions on various cryptographic principles. Differing from the traditional currencies issued by central banks, cryptocurrencies are in their pure form and are digital, created and administered through blockchain technology. Traditional financial institutions operate under a central authority, such as a bank or government to control money circulation. However, cryptocurrencies are decentralized, therefore they operate on a distributed network that doesn't have any intermediaries, and instead, have direct interaction between users. This enables individuals to access banking systems despite their geographic location, but oppositely as a downside, it brings opportunities misuses for illicit purposes. Today, there are thousands of types of cryptocurrencies, each with their own unique features. The very first cryptocurrency is bitcoin, launched in 2009 by an anonymous entity known as Satoshi Nakamoto. Following the creation of bitcoin, ethereum launched with an innovation called smart contracts, which are self-executing contracts that execute automatically if terms of the agreement are met. (European Parliament 2019.)

Money laundering is a process of converting dirty funds acquired from illicit activity into traditional financial system by obscuring origin of the funds. Money laundering happens in three stages known as placement, layering and integration. (United Nations 2024.)

Terrorism financing involves providing or transferring funds to support terrorist activities. The aim is to fund operations of terrorism groups. Funds are transferred often from or through low jurisdiction countries, which lack financial system regulations. (United States Department of State 2024.)

3.1 Importance of the topic

This report highlights to the issue of anonymity considering that cryptocurrencies can be used in illicit ways. Unlike normal financial transactions, cryptocurrency transactions tend not to receive oversight in that such transactions are recorded and monitored by the banks or other relevant authorities. This decentralization, combined with the pseudonymous nature of blockchain addresses, can make it nearly impossible for regulators and law enforcement agencies to track who's behind a transaction. (Europol 2021.)

Cryptocurrencies represent a huge concern as they bypass a traditional financial system. The effect of Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) measures is much stronger in a traditional banking system, where there are rules and regulations for banks to inform the authorities for any suspicious behaviour. Such systems do not apply to cryptocurrencies, and most exchanges often hide in the vast expanse of anonymity. The research further examines how criminals would and could exploit this new technology that includes privacy coins and Decentralized Finance (DeFi) platforms.

Considering that digital currencies are being widely used for legitimate purposes, including investments, remittances, and online transactions, there is a need for regulation that would ensure this new avenue cannot become a hotspot for financial crimes. Beyond money laundering, the cryptocurrencies have also been shown to serve as an emerging source of funding for terrorist organizations. (Nistorescu, G.)

This characteristic of fast and anonymous transfer of large sums of money across borders raises a highly significant threat to international security. For instance, it has been reported that terrorist groups use cryptocurrencies as a means of seeking contributions from sympathizers especially in areas where financial monitoring is relatively weak. The decentralization of cryptocurrencies will most likely make it hard for governments and law enforcement services to detect or disrupt such activities hence the need for stronger regulations and international cooperation. (Ilijevski, I., Ilik, G., Babanoski, K 2023.)

This brings even more complex differences between legitimate and illegitimate uses of cryptocurrencies, for which tools and strategies addressing these new challenges must also be implemented in increasingly digital times.

4 Fundamentals of blockchain

Underneath every cryptocurrency lies the blockchain technology. A blockchain is a decentralized, or distributed, ledger that records each transaction within a cryptocurrency network. Transactions are compiled into a "block" and added to a chain of previous transactions-from which it gets the name "blockchain." The mechanism for this ensures transparency, security, and immutability-that once a transaction is put into the blockchain, it will never be altered or deleted. Such blockchain technology has these key features, which are very appealing to be used in the digital economy. Decentralization removes the need of middleman and enables Peer-to-Peer (P2P) transactions. (Elliptic 2020.)

The chances of fraud are minimal for this network since all parties have equal access to information. Blockchain can either be public, such as bitcoin, or private and applied for enterprise-level usage. A public blockchain is open to anyone who wants to participate in the network and validate the transactions. A private blockchain is closed between a certain set of participants. This independence from centralized authority is main characteristic of cryptocurrency, allowing peer-to-peer transfers between the users. (Chainanalysis 2023b.)

Here are some benefits from this model include:

a) Lower fees and costs: With the elimination of intermediaries, cryptocurrencies significantly lower the fees for transaction processes, particularly during cross-border payments. Traditional remittance services, for example, charge quite a high fee and can take several days before processing a transaction, whereas cryptocurrencies create nearly instant transactions. (Elliptic 2020.)
b) Higher Security: The attacks are feasible because the centralized financial systems represent single points of failure. Decentralized networks of cryptocurrency stand way more resilient to hacking, fraud, and manipulation. Every node in the network keeps a copy of the blockchain so that even if one node is compromised, the system will never be insecure. (Elliptic 2020.)
c) Financial Inclusion: A Cryptocurrency offers financial access to individuals who may not have access to or use the traditional banking systems. About 1.4 billion people around the world remain unbanked. (The World Bank 2024.)
d) Transparency: Every transaction is recorded and can be viewed by anyone with access to a network. Therefore, participants will be encouraged with trust, and fraudulent activities will be deterred. (Elliptic 2020.)
e) Immutability: The ledger record of a transaction, once recorded on a blockchain, is uneditable and safeguarded. (Elliptic 2020.)

4.1 Cryptographic techniques

Cryptocurrencies use cryptographic techniques to make sure that transactions are fulfilled securely and even regulate the creation of new units. Two primary cryptographic techniques are applied in most cryptocurrencies, which are hashing and public-key cryptography. Without these techniques applied, users are unable to trust the system and secure their funds system. (Blockchain Academy 2023.)

a) Hashing: It refers to the data transformation process into a fixed length of characters called hash. It is unique to the original data and can never be recreated. This hashing technique, by blockchain technology, ensures integrity during transactions. Once inserted into a block, a hashed transaction continues to become an immutable record on the blockchain. (Blockchain Academy 2023.)

b) Public-Key Cryptography: It involves two keys, one public and another private key. Here, a cryptocurrency is accessed with the help of a public key while the funds is signed as well as released using a private key. Here, only the owner has the private key, and it ensures that the system is secured. (Blockchain Academy 2023.)

c) Consensus Mechanisms: Consensus Mechanisms will validate transactions in such a way that all nodes on the network agree on what the blockchain state is. There are different types of mechanisms, each cryptocurrency having its form, most relevant mechanisms are either Proof of Work (PoW) or Proof of Stake (PoS), though PoW dominates the cryptocurrencies by far. (Blockchain Academy 2023.)

d) Proof of Work: This is the consensus algorithm used by Bitcoin and by the majority of other existing cryptocurrencies. In PoW, miners compete to be able to solve a problem or puzzle that is in general very complex and requires lots of computational power. As such, whoever solves first wins a share of freshly mined cryptocurrency. (Blockchain Academy 2023.)

e) Proof of Stake: As another form of mining gaining acceptance by other altcoins including Ethereum 2.0 and Cardano, the cryptocurrency was designed to exclude PoW altogether. In PoS, block validators are selected staked based on the size of a cryptocurrency they possess to stake, which is arguably more environmentally friendly manner than PoW. (Blockchain Academy 2023.)

f) Cryptocurrency Mining: Mining involves using computational power to solve complex puzzles to find a valid hash for a block of transactions. The first miner to find the valid hash is rewarded with cryptocurrency, known as block reward. The competition between the miners is intense and often leading miners to invest in more powerful set of computers. More powerful mining equipment improves the chances of solving the puzzles before others, but they also cause massive computational power which is negative for environmental impact. (Investopedia 2024.)

The Figure 1 represents that Bitcoin mining alone in 2022 accounted for 0.26% of the world's total energy production and 0.68% of electricity, which has drawn criticism, especially as global efforts focus on transitioning to greener and more sustainable energy practices (Investopedia 2024.)

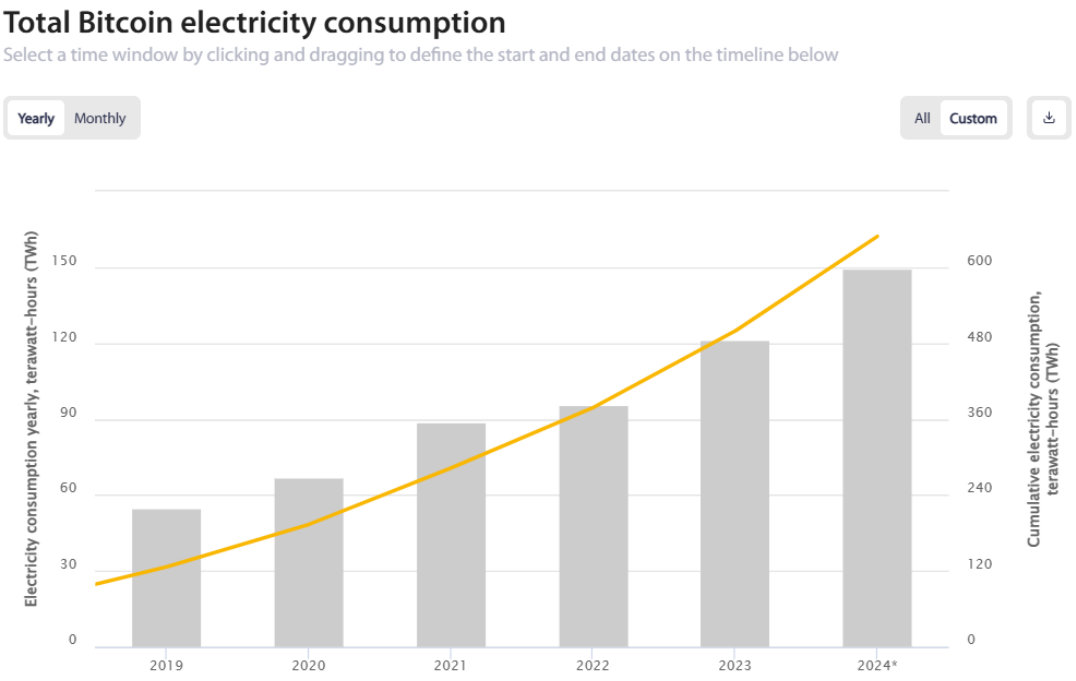

Figure 1: Bitcoin total energy consumption between 2019 and 2024 (Cambridge Bitcoin Electricity Consumption Index 2024)

g) Cryptocurrency storing: A digital wallet is a software application that allows users to securely transmit, receive, and store cryptocurrency. Cryptocurrencies are stored in digital wallets called hot wallets and cold wallets. Hot wallets, which include desktop, web, and mobile wallets, are digital wallets that are linked to the internet and controlled by third-party providers. They provide rapid transactions and are commonly used in trading. Cold wallets are not linked to the Internet, which improves security by shielding the users' private keys. For example, hardware wallets, such as USB devices. (Blockchain Academy 2023.)

5 Money laundering

Cryptocurrencies are very anonymous and their use in money laundering is becoming more popular as a medium of payment as seen in Figure 2. Although every transaction is logged on the blockchain, the identities of participants are masked by cryptographic addresses. It gives at least a certain level of privacy because it is hard to trace through who is participating in a transaction. However, the anonymity has attracted criminals, who use it in fraudulent activities, including money laundering and terrorism financing. Traditional finance systems are a lot more regulated when compared to cryptocurrencies. Banks must keep records of their

customers, which are comprehensive in line with KYC and AML legislation, whereas cryptocurrencies work in quite an unregulated environment. (Chainanalysis 2023a.)

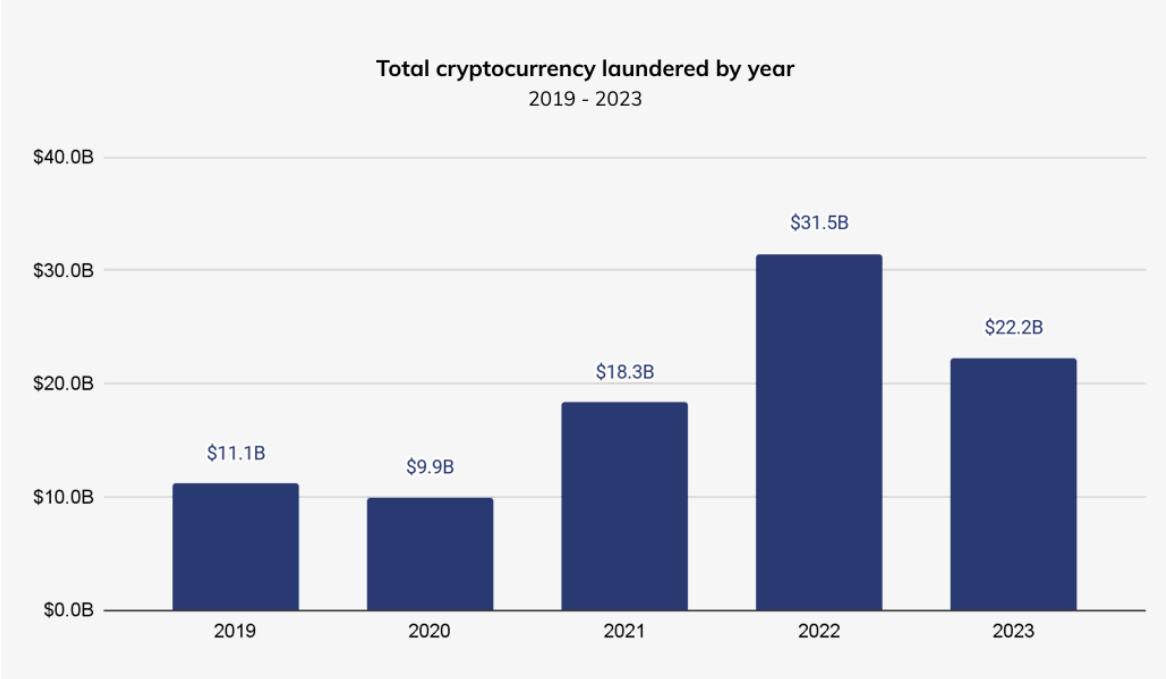

Figure 2: Total cryptocurrency laundered between 2019-2023 (Chainanalysis 2024)

The Figure 2 illustrates the total amount of cryptocurrency laundered between 2019-2024, which shows stable increase from 2020 to 2022, followed by decline in 2023. Cryptocurrencies are more generally described as "pseudonymous," rather than completely anonymous. This reason being is identities of users are not available publicly directly, but every user is identified by a unique cryptographic address in bitcoin and other cryptocurrencies. At such a time as when enough information has been collected, all these addresses can be traced back to the owners, though it is more of an effort that requires highly sophisticated techniques. On the other hand, there are cryptocurrencies which is being marketed as improving anonymity for users. There are three most popular kinds of such currencies offering privacy, which are Monero, Zcash and Dash. These currencies make use of advanced cryptography techniques to obscure identities as well as amounts handled in transactions. (Chainanalysis 2023.)

Some of the potential risks of anonymity in using cryptocurrencies are:

a) Money laundering: The cryptocurrency cannot track the origin of where money came from or even the place to which it is headed. The criminals employ the use of "mixers" or "tumblers," which they use to shuffle their cryptocurrencies with other people's so that they cannot trace transactions. (Chainanalysis 2023.)

b) Sanctions Evasion:

A major highlighted concern has been cryptocurrency potential use to bypass Western financial sanctions against Russia, following Russia's invasion of Ukraine. According to Reuters, Russia's central bank has encouraged businesses and individuals to utilize cryptocurrencies as a payment to circumvent the financial restrictions. (Reuters 2024.)

A crypto exchange Garantex, registered to Estonia, but operating in Russia has been in the spotlight for the past years for facilitating large amount of illicit crypto activity, especially concerning sanctions evasions. Garantex lost license to operate in Estonia since February 2022 but continues to operate in Russia into this day. Garantex has been processed of $100 billion in transactions, which has been estimated to be accounted for 82% of crypto volumes linked to sanctioned entities as well as crypto wallets used by Russian and Chinese entities involved production of military equipment. (Chainanalysis 2024, TRM Labs 2024.)

There is multiple crypto exchange besides Garantex such as Cryptex, Exved, 2PMBTC, Bitzlato, Suex, 100btc, Tetchange and Hydra Market, which was taken down in April 2022 by American and German law enforcers, that are operating primarily in Russia. Even though these exchanges are based in Russia, they also allow users outside of Russia which raises concerns about enabling illicit activities and sanctions evasion. (Chainanalysis 2024.)

c) Funding of Terrorism: Terrorist groups have been using the medium of cryptocurrencies as a channel to collect and transfer funds because it is much easier to move money without it being noticed in different parts of the world. To this purpose, such coins are more preferable since it renders anonymity.

d) Tax Evasion: Given the anonymity of cryptocurrencies, capital gains or income accruing from holding in such currencies is hard for the tax authorities to trace and tax. This had led to massive tax evasion subsequently, which the governments are now controlling with new regulations and reporting requirements.

From smuggled goods to an illegal arms trade, crimes like prostitution and drug trades, embezzlements, insider trading, briberies, and various computer fraud schemes, profits can be huge. Therefore, all these create some powerful incentives to make all these "dirty" money "clean" by dirtying them through money laundry activities. When there is a significant profit from an illegal action, the person or group engaged needs to figure out how to manage the money without drawing attention to themselves or the other participants. Criminals conceal the sources, alter the paperwork, or relocate the funds to a location where it is less likely to attract attention. (Basel AML Index 2023.)

5.1 Stages of money laundering

The core structure of any money laundering set-up includes three complex stages, placement, layering and integration. It is crucial to identify money laundering activity at every stage to recognize its indicators. These stages are explained in more detail in the next paragraphs (Nistorescu 2024.)

5.1.1 Placement

The placement stage entails bringing dirty money into the financial system. It is the initial stage of money laundering, where illegal money is funnelled into seemingly legitimate assets so that it doesn't seem as if large sums of money appear out of nowhere. The placement stage is considered to be the riskiest stage for offenders since it is the first move that indicates suspicious activity. (United Nations 2024.)

A few commonly known routes for the execution of this stage are:

a) Crypto ATMs pose a challenge to money laundering (AML) initiatives because of the lack of consistent regulations and lenient know-your-customer (KYC) procedures they often have in place. It is easier for illicit funds to enter the cryptocurrency ecosystem through these machines due to their ability to quickly convert cash into cryptocurrencies. (United Nations 2024.)

b) Decentralized exchanges have proven to be a choice for individuals engaging in unlawful activities like money laundering because they do not enforce KYC protocols and operate without centralized oversight in place. Decentralized exchanges such as Uniswap and dYdX allow users to exchange digital assets without the need for identity verification procedures which adds a layer of anonymity to transactions

A very common method in the placement stage is called “smurfing”, which means breaking down large sums of money into smaller, less suspicious amounts. For example, a launderer may deposit money in smaller amounts into banks or use it in gambling at a casino. The goal is to distance the illegal funds from their source for example by following methods:

a) Bank deposits: Instead of making a single large deposit, malicious actors make tiny, frequent deposits, aiming to avoid attention. (Financial Crime Academy 2024.)

b) Sending money to offshore foreign bank accounts: Launders convert the dirty funds to different currency which makes difficult in tracking the origin. (Financial Crime Academy 2024.)

d) False invoicing: Creating fake invoices to legitimise the movement of funds by a corporation without active business operations or significant assets. For this, the primary business

sectors are cash-intensive businesses, as manipulating billings is relatively easier. Common business sectors are nightclubs, casinos, restaurants and construction companies. (Financial Crime Academy 2024.)

e) Gambling platforms: Criminals buy gambling chips with unlawful funds, gamble only briefly, and then cash out the chips, making the money appear as genuine gambling wins. (United Nations 2024, Financial Crime Academy 2024.)

5.1.2 Layering

Layering is a practice in which a series of organizations, typically offshore entities to obscure the origin of illicit funds. This technique creates layers of camouflage to unlawfully obtained funds, making it difficult to trace connections by raising complexity of transactions. Multiple transactions ensure that money is travelled far away from its origin. The primary difference between layering and placement is that placement solely requires depositing money into the financial system, while layering is a method of concealing the source of these funds through a series of financial transactions. (United Nations 2024, Financial Crime Academy 2024.) After the placement process, in which the launderer slipped the dirty money into the legitimate banking system, criminals aim to complex the trail of funds even more.

a) Mixing and shuffling aims to break larger sums of cryptocurrencies send to many addresses or move it across bank accounts. Mixers, also known as tumblers, are individuals or businesses that split the funds across users and combine them to legitimate funds to obscure the origins and the owners as shown in Figure 3. (Financial Crime Academy 2024.)

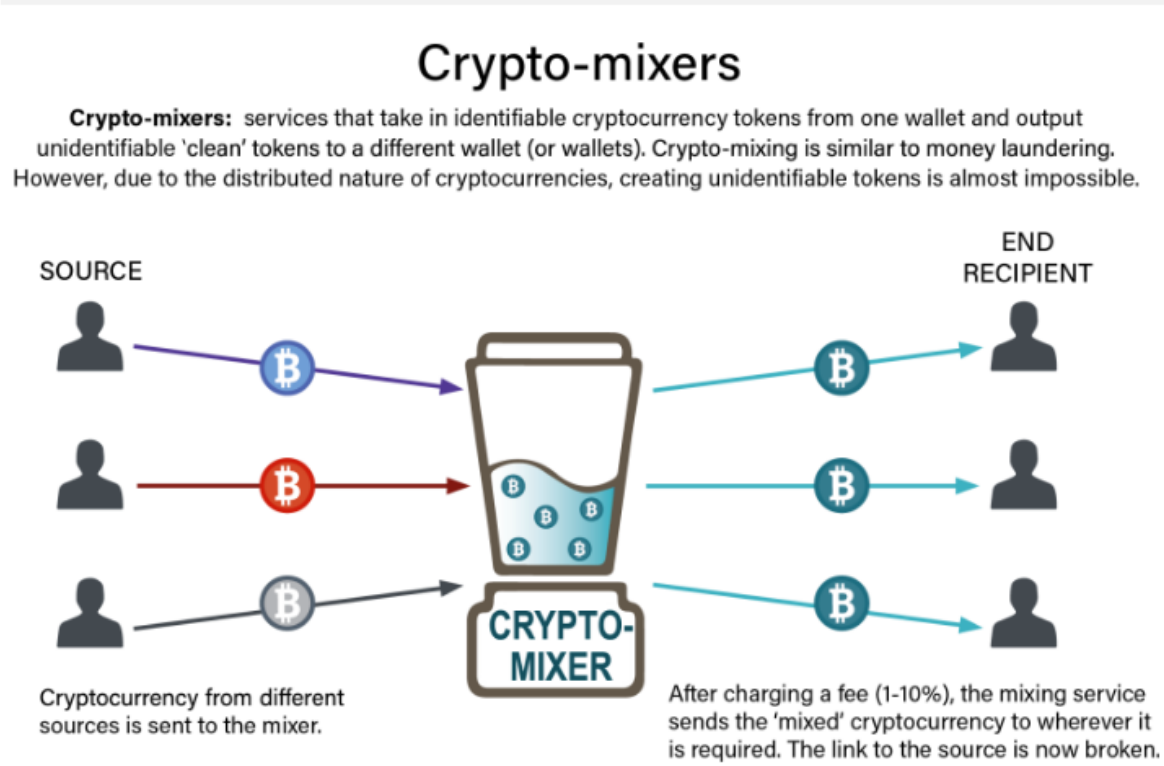

Figure 3: Crypto mixers explained (Bitinvestment 2023)

b) Over the Counter (OTC) Trading enables individuals to buy or sell cryptocurrencies directly, without using any cryptocurrency exchange. In OTC trading, a money launderer can use a broker to liquidate the dirty funds to fiat currency or exchange to other cryptocurrency without revealing their identity. (Financial Crime Academy 2024.)

c) Trading and investing methods are commonly used by criminals to purchase a variety of cryptocurrencies on different blockchains, creating an illusion that they are purchasing and selling crypto assets. The cash may be exchanged for digital currencies and then returned to fiat currency. (Financial Crime Academy 2024.)

d) Shell companies usually only exist on paper without any ongoing business activity. The dirty money funnels through a shell company and as a result the dirty funds can appear as a revenue from legitimate business. (Financial Crime Academy 2024.)

f) Crypto bridges enable the transfer of assets between multiple blockchain networks, and they have become popular tools for improving cross-chain interoperability and use cases of specific assets. As their popularity develops, malevolent actors are increasingly attempting to use cross-chain bridges to hide the origins of illicit funds by moving them across various blockchains. (United Nations 2024, Financial Crime Academy 2024.)

5.1.3 Integration

During the final stage of the money laundering process, known as integration, criminals attempt to reintegrate the money they have cleaned back into the mainstream legal economy and blending them to legal funds. Common assets used in this stage are usually highly valued such as real estate, luxurious goods and art. The art in particular has become a significant channel for integration due to the recent rise of non-fungible tokens (NFTs), one of the most valuable NFT known to be sold for $91.8 million, and the total value of NFT's is expected to reach $2.37 billion in 2024. Because NFTs are subjective and volatile, it is hard to establish a fair market value, making it easy for criminals to come up with inflated prices to justify the amount requested for money laundering. (Techopedia 2024, United Nations 2024.)

5.2 Real-world scenarios

The most known darknet marketplace is Silk Road, which opened in 2011 and focuses on illegal drugs and other illegal goods and services. Cryptocurrency, mostly bitcoin was used as a payment method between the sellers and buyers, which enabled anonymous transactions. Eventually in 2013, FBI shut down the site.

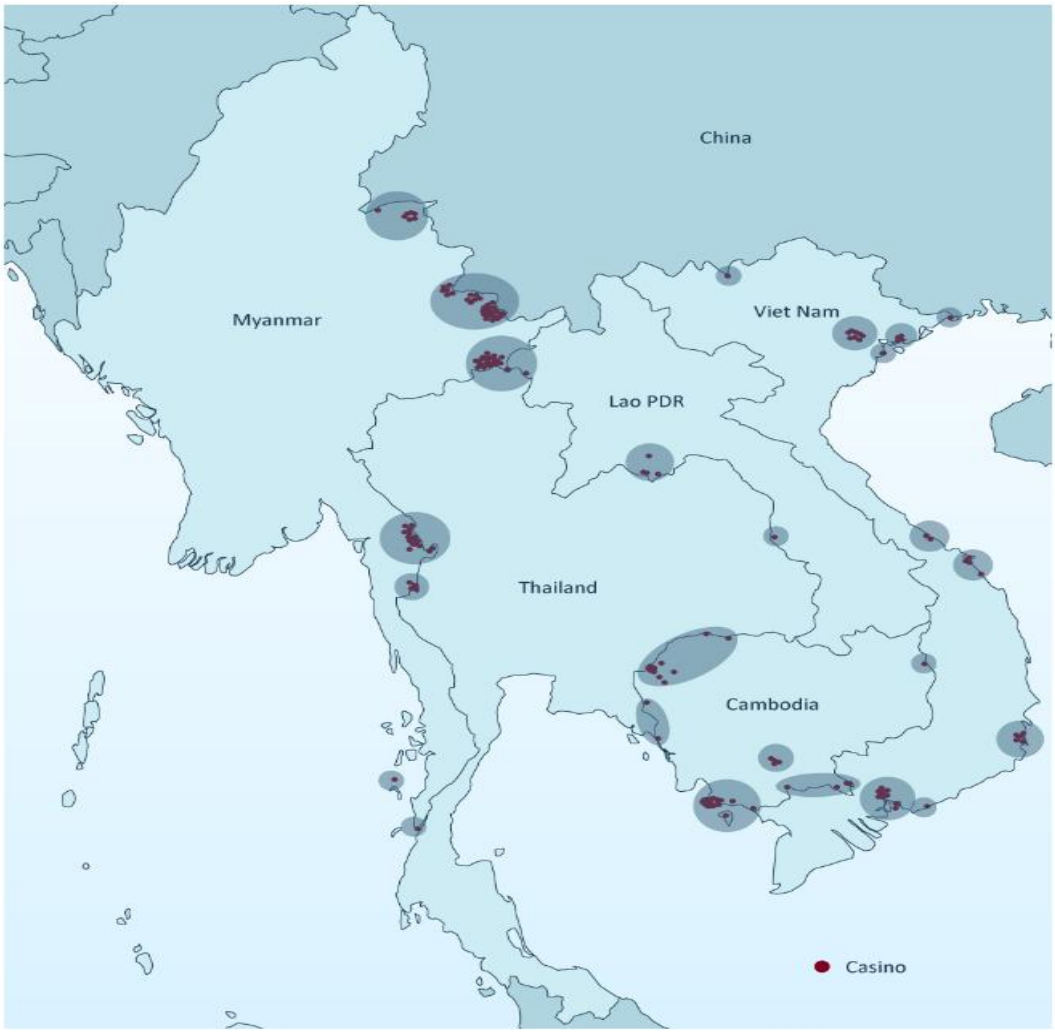

Figure 4: Underground casinos across Southeast Asia (UNODC 2024)

As illustrated in Figure 4, the use of cryptocurrencies in casinos have increasingly become a hub for money laundering, such as underground banking and cyberfraud in East and Southeast Asia. This phenomenon has enabled crime groups to transfer their dirty funds through underground casinos and banking networks quicker then law enforcers can chase or intercept them. According to UNODC analysis in 2022, the number of licensed and unlicensed land-based casinos were more than 340 in the region, with the majority already transitioned into live-dealing casinos. (UNDOC 2024.)

6 International action against money laundering

Concerns that cryptocurrencies pose is their potential to facilitate evasion of regulation. They offer individuals and organizations an opportunity to go through a decentralized system with characteristics of pseudonymity, hence evading some traditional financial regulations. Money

laundering continues to pose challenges to the global financial system. In response, network of various regulatory bodies and organizations have emerged worldwide to address illicit activity as shown on Figure 5. AML regulators are organizations that monitor financial transactions and detect suspicious activities. These organizations have crucial role of ensuring that financial institutions cope with the compliance regulations. (Sanctions Scanner 2024.)

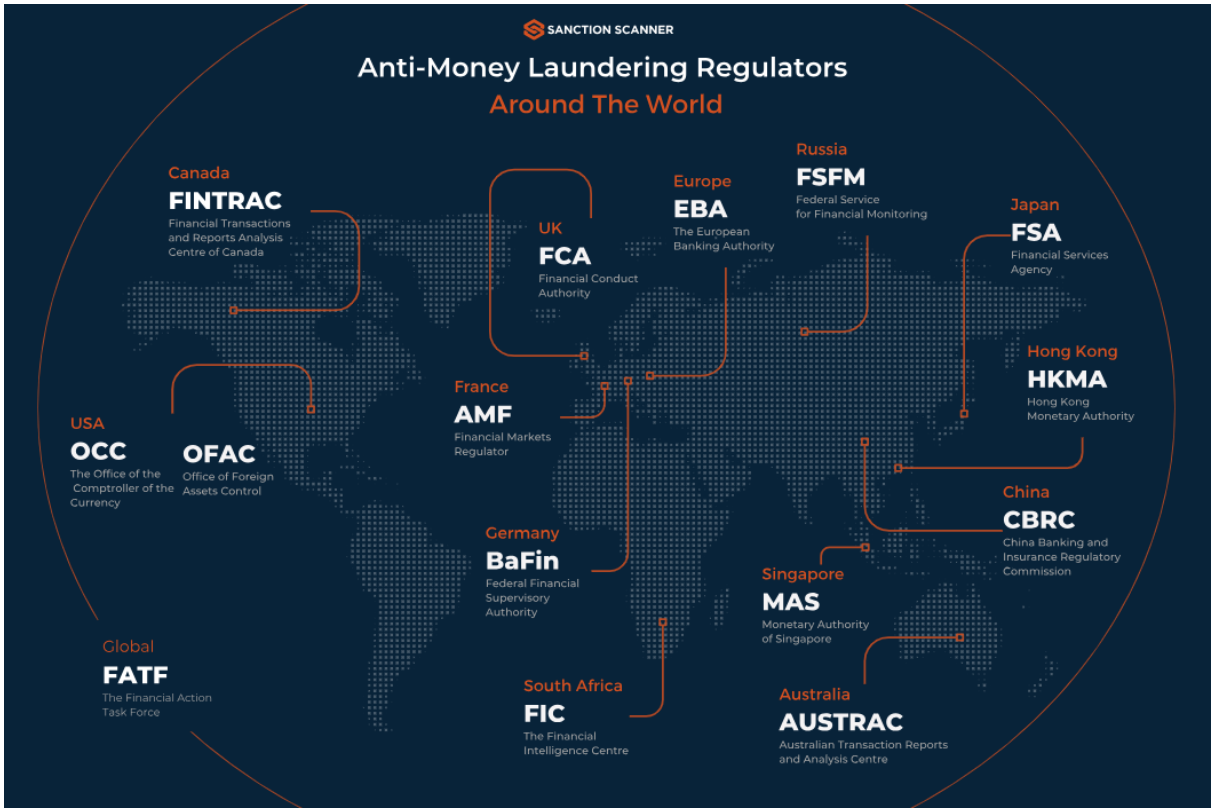

Figure 5: AML regulators around the world (Sanctions Scanner 2024)

6.1 Financial Action Tasks Force (FATF)

FATF serves as the primary global regulatory body. FATF is an international organization that sets and develops AML and CFT requirements for an international order to prevent money laundering and terrorist financing. FATF was established in 1989 with currently 40 country members spread across of the world. The standards developed by the FATF aims to ensure virtual assets (VAs) and virtual asset service providers (VASPs) are used for legitimate purposes. VASPs are businesses that exchange, use and transfer virtual assets. The regulatory requirements of VASPs must therefore be comparable by the traditional financial institutions and being compliant with AML and CTF policies. Often these individuals who commit crimes by exploiting weak AML and CTF controls in transferring money through financial networks. Therefore, it is on the core of what the FATF aims, to find jurisdictions with weaknesses in their AML/CFT system and strengthen those weaknesses. The FATF also adopted the "Travel Rule," which is the requirement for over the threshold amount of $1,000 USD/EUR, the VASP shall

collect the name of the sender, the number of the account or wallet address, and additional information such as physical address, national ID number, unique customer identification number or date and place of birth. However, four years after the adoption of the FATF standards on VAs and VASPs, the worldwide implementation is still very poor. Only around 75 percent of the jurisdictions are partially or non-compliant with the requirements given of FATF. Most jurisdictions are struggling with basic requirements such as performing a risk assessment and the Travel Rule. (FATF 2023.)

6.2 European Union regulations

The European Union (EU) has a well-established and evolving regulatory framework to combat money laundering and terrorism financing by The EU supervisory bodies, European Banking Authority (EBA), European Central Bank (ECB) and The European Anti-Money Laundering Authority (AMLA), is an EU agency who will start its operations in later 2025.

The EU has implemented comprehensive set of AML and CFT packages which includes:

a) A new AML Regulation (AMLR), harmonization of requirements and standards for combating money laundering and terrorist financing
b) The 6th AML Directive (AMLD6), addresses gaps in AML and CTF procedures and strengthens the frameworks
c) Anti-Money Laundering Authority (AMLA), a central EU body who will start to operate in 2025 by coordinating with national authorities and ensure consistent AML and CTF applications
d) The EU Transfer of Funds Regulation (TFR), which incorporates the existing FATF's Travel Rule, originally developed for traditional financial institutions, into the cryptocurrency sector

MiCA (Markets in Crypto-Assets Regulation) is a comprehensive EU regulation which came into effect in June 2023 and expected to be fully implemented by December 2024. MiCA aims to create a more stable, transparent, and regulated environment for crypto assets in the EU, potentially attracting more institutional investors while also increasing compliance requirements for businesses in the sector. MiCA affects Crypto-asset issuers, including stablecoin issuers, crypto-asset service providers (CASPs) such as exchanges and trading platforms, as well as consumers and investors in crypto-assets. (ESMA 2024.)

6.3 Risk-based approaches

The FATF Recommendations also supports the use of risk-based approach (RBAs) for countries, authorities and financial institutions. These approaches involve identifying, assessing and

understand risks associated with money laundering and terrorism financing, and take procedures to reduce the risks. (FATF 2023.)

The FATF guidelines for regulating cryptocurrencies go beyond the Travel Rule and RBAs; they also focus on licensing and registering VASPs and implementing preventative measures like keeping records and reporting suspicious transactions while promoting global collaboration in monitoring and investigating cryptocurrency-related offences as the world of cryptocurrency advances further in its development the FATFs regulatory strategy also progresses alongside it. The organization consistently revises its guidelines to tackle new obstacles and technological advancements. This ongoing procedure guarantees that the international regulatory structure stays current and efficient in coping with the evolution, within the realm of cryptocurrency. (FATF 2023.)

Risk-Based Approaches involve strategic approaches, that are implemented throughout different industries, especially in the financial sectors, to manage and minimize risks resulting from money laundering and financing terrorism. Organizations can commit assets and employ controls that are commensurate with the risks. (FATF 2023.)

Transaction Monitoring is actual time monitoring of transactions by financial institutions, where the aim is to detect unusual patterns of transactions that could imply money mulling. Some of the rapid transfers to cash deposits, structuring of transactions to avoid reporting requirements, unusual patterns of transactions, or high-risk jurisdiction-based transactions. (FATF 2023.)

Know Your Customer and Due Diligence on the Customer: In the activation of a banking service, all customers of banks undergo a KYC check. In this process, information sought and gathered about the identity of the customer, business activities, and financial transactions are done in detail. Customers whose risk seems significant or higher require an EDD process that, in turn, involves deeper insights into the source of funds and the nature of transactions which customers may conduct. KYC checks are performed at intervals throughout the customer life cycle. (FATF 2023.)

Geographical Risk Assessment: Depending on the type of geographies, financial institutions assess the risks. Some geographies are considered risky because of the economic conditions, political instability, or social situations of those geographies, or even documented levels of criminal activities that include money laundering or financing terrorism. There is a risk for financial institutions to put more extended controls or rejecting to serve clients from these regions. (FATF 2023.)

Sector-specific risk assessment: The nature of risk cuts across sectors. The real estate sector, for example, may have a greater likelihood of money laundering compared to others because

the sector involves huge deals. Financial institutions employ RBAs that benchmark the amount of risk in every sector and implement controls that resonate with the sector risk. (FATF 2023.)

Beneficial ownership: Businesses should also identify the actual beneficial owners beyond just mere performance of KYC and CDD. Where a money mule has opened a shell company for an individual, it is quite simple for businesses to trace and seek to understand who really owns that company and not permit its accounts to be used to launder money. (FATF 2023.)

Risk scoring models: Commercial banks prepare risk score models that provide a risk score to customers based on general characteristics, such as transaction history, account behaviour, and demographic information. Customers carrying greater-risk scores may have higher intensity scrutiny to capture suspect transactions. (FATF 2023.)

Behavioural Analysis: This seeks to know what the customer does by analysing customer information, login activities, transaction frequency, and geographic locations where the account is accessed. In this respect, financial institutions can mark some of the suspicious activities within the account of a customer. (FATF 2023.)

Network analysis: This is a review of the connections and transaction flows in accounts to detect networks of mules. It helps to identify connections that might not occur in connection with direct transaction monitoring. (FATF 2023.)

Suspicious Activity Reporting: If the financial institutions suspect that the transactions are suspicious, they file their SARs in the regulatory agency such as financial intelligence units. The SARs then provide law enforcement authorities with information required for investigation and prosecution of suspected financial crimes. (FATF 2023.)

7 High risk countries

As a leading international regulatory authority, FATF emphasizes the importance of countries to develop and enhance frameworks to ensure effective implementation of AML and CTF measures. FATF has established action plan, which is a framework that helps countries to address their deficiencies in their AML and CTF measures. These action plans are created when the FATF identifies weaknesses in a country's financial system that could facilitate money laundering, terrorist financing, or the proliferation of weapons of mass destruction. Based on the most recent updates from the FATF as of October 25, 2024, the list of high-risk countries and jurisdictions under increased monitoring has been updated.

In October 2024, FATF has stated three “blacklisted” countries with high money laundering and terrorism financing risks

Democratic People's Republic of Korea / North Korea

The FATF continues to classify North Korea as a high-risk jurisdiction subject to a call for action due to its significant deficiencies in AML and CTF measures. In its latest updates from October 25, 2024, the FATF has highlighted ongoing concerns regarding North Korea's failure to address these critical deficiencies, particularly linked to production and funding of weapons of mass destruction. (FATF 2024.)

Iran

Iran status regarding its commitment to FATF remains critical. As of the latest updates from FATF, Iran has not made any progress in their action plan and continues remaining as a high-risk jurisdiction subject to a call for action until action plan is completed. (FATF 2024.)

Myanmar (Burma)

Myanmar has been on the FATF's list of high-risk jurisdictions since October 2022. Although Myanmar made a commitment In February 2020 to improve its deficiencies, but eventually failed to meet the requirements of the action plan. The progress has been slow, and if no significant improvements are made by February 2025, the FATF may take further countermeasures. (FATF 2024.).

The FATF "grey list" includes countries that are under increased monitoring as of October 2024, which have committed to improving their AML and CTF frameworks within set timeframes. (FATF 2024.)

Algeria

Algeria has made commitment to fulfil and strengthen the AML and CTF procedures since October 2024 and have made some progress, but reasonable amount of work remains to further strengthen the frameworks. (FATF 2024.)

Angola

Angola has made commitment to fulfil and strengthen the AML and CTF procedures since October 2024. Angola adopted MER in June 2023 and there has been some progress towards MER recommended actions, but still needs to address remaining deficiencies on the action plan. (FATF 2024.)

Bulgaria

Bulgaria has taken steps forward for improving AML and CTF procedures since its commitment in October 2023, but still needs to address certain remaining deficiencies. (FATF 2024.)

Burkina Faso

Since February 2021, Mali has made commitment to fulfil and strengthen the AML and CTF procedures and has taken steps forward to enhancing them. However, the deadlines for current action plan have expired since December 2022, and now Burkina Faso must implement strategic deficiencies urgently. (FATF 2024.)

Cameroon

Since June 2023, Cameroon has made commitment to fulfil and strengthen the AML and CTF procedures. However, there has been some improvement, but significant work remains to strengthen the frameworks. (FATF 2024.)

Côte d'Ivoire

Côte d'Ivoire has made commitment to fulfil and strengthen the AML and CTF procedures since October 2024 and have made a great contribution for improving the current MER (mutual evaluation report) framework since its adoption in December 2023. (FATF 2024.)

Croatia

Croatia has taken steps forward for improving AML and CTF procedures since their commitment in June 2023, but still needs to address certain remaining deficiencies. (FATF 2024.)

Democratic Republic of the Congo

Democratic Republic of the Congo has taken steps forward for improving AML and CTF procedures since their commitment in October 2022, but still needs to address certain remaining deficiencies on the action plan. (FATF 2024.)

Haiti

Since June 2021, Haiti has made commitment to fulfil and strengthen the AML and CTF procedures and has taken steps forward for improving them. However, the deadlines for current action plan have expired, and now significant work remains to be done. (FATF 2024.)

Kenya

Kenya has made commitment to fulfil and strengthen the AML and CTF procedures since February 2024 and have made some progress for improving the current MER framework since its adoption in September 2022. (FATF 2024.)

Lebanon

Lebanon has faced issues with unlicensed financial activities, as well as bribery and corruption, and working further to improve the deficiencies in the action plan. Lebanon adopted MER in May 2023, and has taken steps forward for working MER recommended actions, but still needs to address remaining deficiencies on the action plan. (FATF 2024.)

Mali

Since October 2021, Mali has made commitment to fulfil AML and CTF requirements. However, the deadlines for current action plan have expired, and now Mali must implement strategic deficiencies urgently. (FATF 2024.)

Monaco

Monaco has made commitment to fulfil and strengthen the AML and CTF procedures since June 2024. Monaco has made great improvement for the current MER (mutual evaluation report) framework since its adoption in December 2022, by establishing a financial intelligence unit (FIU). (FATF 2024.)

Mozambique

Since June 2023, Mozambique has made commitment to fulfil and strengthen the AML and CTF procedures. Although there has been progress, additional work is required to fully strengthen the frameworks. (FATF 2024.)

Namibia

Since February 2024, Namibia has made commitment to fulfil and strengthen the AML and CTF procedures, but further work remains to strengthen the frameworks. (FATF 2024.)

Nigeria

Since February 2023, Nigeria has made commitment to fulfil and strengthen the AML and CTF procedures, but further work remains to strengthen the frameworks. (FATF 2024.)

Philippines

Philippines has made commitment to fulfil and strengthen the AML and CTF procedures since June 2021, and in 2024 FATF assessed that Philippines has fulfilled its action plan, but FATF continues to evaluate the current frameworks to ensure their sustainability in the future. (FATF 2024.)

South Africa

Since February 2023, South Africa has made commitment to fulfil and strengthen the AML and CTF procedures. Although there has been progress, additional work is required to fully strengthen the frameworks. (FATF 2024.)

South Sudan

Since June 2021, South Sudan has made commitment to fulfil AML and CTF requirements. However, the deadlines for current action plan have expired, and now significant work remains to be done. (FATF 2024.)

Syria

Since February 2010, Syria has made commitment to fulfil AML and CTF requirements. In June 2014, FATF assessed that Syria had partially completed their action plan. However, due to the ongoing unstable and fragile situation in the country, FATF has been unable to evaluate the current situation in the country. (FATF 2024.)

Tanzania

Since October 2022, Tanzania has made commitment to fulfil and strengthen the AML and CTF procedures. Although there has been progress, additional work is required to address deficiencies on the action plan. (FATF 2024.)

Venezuela

Venezuela has made commitment to fulfil and strengthen the AML and CTF procedures since June 2024. Venezuela adopted MER in November 2022 and there has been some progress towards MER recommended actions, but still needs to address remaining deficiencies on the action plan. (FATF 2024.)

Vietnam

Vietnam has made commitment to fulfil and strengthen the AML and CTF procedures since June 2023. However, progress has been limited, and FATF strongly urges Vietnam to enhance internal coordination to progress on its action plan for addressing strategic deficiencies. (FATF 2024.)

Yemen

Since February 2010, Yemen has made commitment to fulfil AML and CTF requirements. In June 2014, FATF assessed that Yemen had partially completed their action plan. However,

due to the ongoing unstable and fragile situation in the country, FATF has been unable to evaluate the current situation in the country. (FATF 2024.)

7.1 Money laundering in Finland

In Finland, cryptocurrency regulation is influenced by both European Union guidelines and Finland own legislations, including The Anti-Money Laundering Act which is complemented additional acts such as Act on Virtual Currency Providers. These regulations require financial institutions and crypto-asset service providers to conduct risk assessments, which evaluates the risks of money laundering and terrorist funding across sectors in Finland. (Ministry of Finance 2023.)

The Figure 6 framework illustrates Finland's systematic approach to combating financial crimes by implementing multiple levels of oversight, reporting, investigation, and enforcement. Financial and insurance sectors in Finland are under the supervision by Finnish Financial Supervisory Authority (FIN-FSA). Organizations obligated to report activities includes entities such as financial institutions, gambling operators, real estate agents and regulated professionals. When reports concerning money laundering are submitted for review, they are processed by Financial Intelligence Unit (FIU), who combats and investigates money laundering activities. (FIN-FSA 2024.) The entire system operates under the coordination of ministries to ensure both domestic and international cooperation in combating financial crimes. (Rahanpesun selvittelykeskus 2024.)

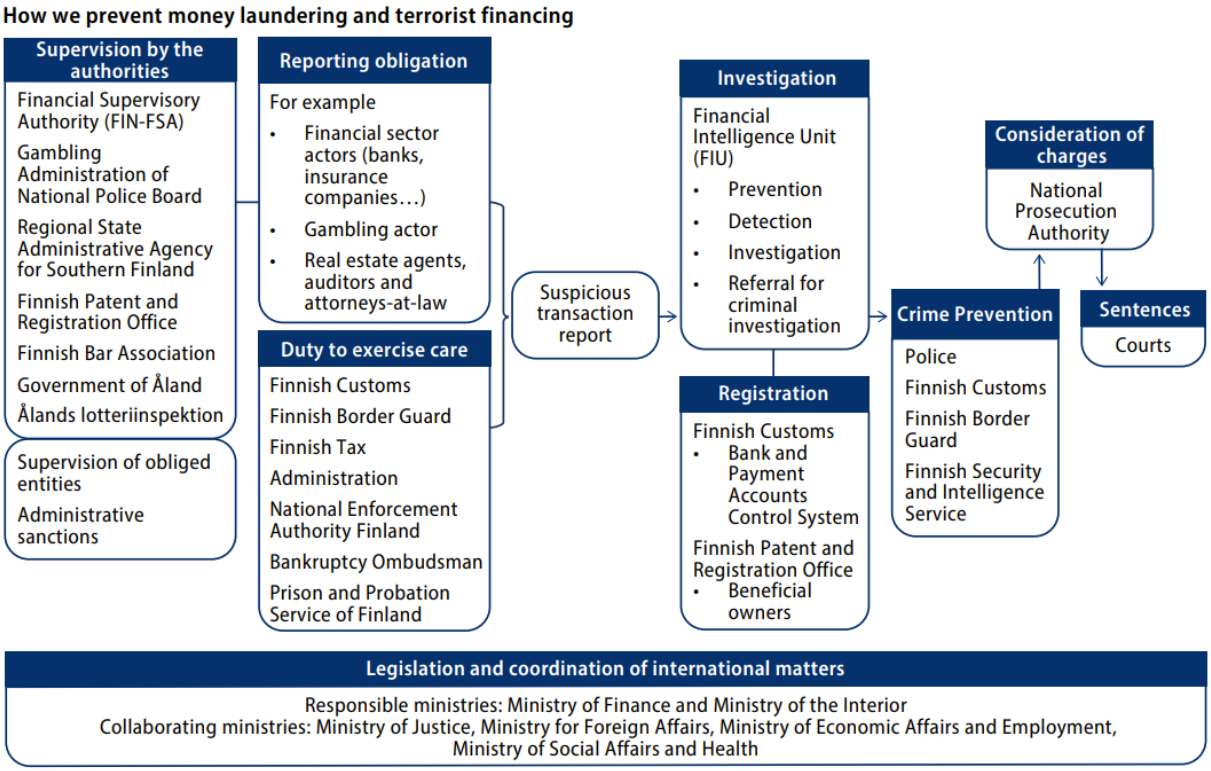

Figure 6: Finland coordinated system in place for preventing money laundering and terrorism (Ministry of Finance 2023)

According to the Finland FIU's 2023 annual report, cryptocurrencies use in money laundering has decreased over time, particularly when compared to money laundering reports from 2021. Despite the decline in number of reports, NBI has emphasized that the trend of illegal use of cryptocurrencies is moving towards frauds and terrorism financing. The recent arrival of European Union new AML package will bring significant changes in cryptocurrency regulations. The implementation of these EU regulations is expected to have positive impact on preventing money laundering involving crypto assets, as it strengthens the CASPs as they are required to collect more detailed information about the transactions.

In Finland, hawala is classified as having highest sector-specific risk level for money laundering, however virtual currencies are considered the highest individual risks according to the obliged entities. (Ministry of Finance 2023.)

Hawala meaning" transfer" in Arabic, is a money transfer method without the physical movement of cash. It operates outside of traditional banking systems by relying on a network of trusted individuals or company brokers (known as hawaladars) who transfer the money movement between the senders and the receivers. Hawala is used mainly in countries where banking systems aren't well developed or being financially strictly regulated by movement of funds. Hawala is comparable to cryptocurrencies, as it is not controlled by financial

institutions, hence it is also vulnerable to money laundering and terrorism financing. (Investopedia 2023.) According to the Finland FIU's 2024 annual report, OFAC (Office of Foreign Assets Control) has set sanctions in March 2024 on a hawala operator in Finland, who further supported al-Shabaab terrorist group money laundering operations.

The Ministry of Finance and the Ministry of the Interior have recently published the risk assessment action plan for 2024 and 2025, which specifically targets hawala operators. This reflects the Finland government's commitment to tackling rising risks in the financial sector, with the goal of strengthening the frameworks to combat money laundering and terrorist financing. (Ministry of Finance 2024.)

8 Results

The aim of the thesis was to raise awareness on the latest money laundering methods and methods used for terrorism financing. This phenomenon has resulted in sanctions evasions occurring worldwide, highlighting the necessity for financial institutions and other VASPs to have strong AML and CTF procedures. With strong frameworks in place, the organization can know their customers, identify and suspicious behavior and react on time. Additionally, they can identify low jurisdiction countries and monitor transactions associated with these regions and react on time. The importance of employee training for comprehending sanctions and the AML and CTF frameworks is also crucial.

As blockchain is public, with blockchain analytics tools it is possible to get insights of transaction patterns linked to terrorism networks. Once there is sight of movement in fund trail associated in terrorism activity, it is possible to investigate these transactions, report them and perhaps prevent the funds transferring to terrorism financing. Blockchain investigation analytic tools are provided by leading cryptocurrency organizations such as Chainanalysis and Elliptic. Development proposal is for financial institutions is to invest these tools from these organizations and employ procedures in place.

Cryptocurrency money laundering in Finland trend is decreasing compared to previous years according to Finland FIU's 2023 annual report. However, hawala money transfer is identified one of the riskiest methods of enabling money laundering to happen. This highlights the risks of risk associated with the hawala system and whether existence of hawala is inevitable.

This thesis will be submitted to the client, whose name will remain confidential. The outcome of the thesis provided useful, valuable and up-to-date information that will be supporting my future career. The findings will be presented, and guidance will be given on the use of cryptocurrency and their use in money laundering and terrorism financing in the form of an internal guide for the client.

9 Conclusion

Rapid growth of cryptocurrencies has brought to the global financial landscape lots of innovative opportunities, but on the other hand, many challenges were faced in fighting financial crimes. There is financial inclusion and increased transparency in the transactions, but then again, it has become an instrument for cases such as money laundering and sanctions evasion. So, this contrast underscores the complexity with which their impact can be managed on the financial system. Cryptocurrencies are highly appealing to criminals who want to launder illicit funds since they are pseudonymous, have relatively fast transaction speeds, and are accessible from anywhere in the world. Mixing services, cross-chain transfers, and over-the-counter trading have increased sophistication in the laundering process. The unregulated exchanges and the high-risk countries make this challenge much bigger, which is why international cooperation is essential. FATF plays a key role in coordinating efforts, while European Union regulatory helps standardizing and strengthening regulatory responses across borders.

With the dynamics of cryptocurrency technology changing as fast as it does, such regulatory frameworks need to be agile and adaptive. It would mean continued investments in blockchain analysis tools and strengthening AML-protocols, further cooperation between the public and private sectors toward staying ahead of criminals while maintaining integrity in the world's financial system. Detecting abnormal transaction patterns, tracking asset flows using blockchain explorers, and recognizing suspicious activities are essential for exposing money laundering schemes. This know-how improves compliance efforts by developing awareness for red flags and staying up to date with the most recent tools and techniques for tracking cryptocurrency transactions.

Furthermore, another challenge for both the regulators and the industry is the implications of cryptocurrency mining on environment, especially for proof-of-work systems such as bitcoin. The sustainable growth for such an ecosystem will require being heavily balanced between the advantages coming from blockchain technology and being weighed against the energy consumptions.

References

2024 World Bank Group. Referred 10.08.2024. https://digitalfinance.worldbank.org/

Basel Index. 2023. Snapshot of money laundering risks and trends (The Academy Bulletin). Referred 14.08.2024. https://baselgovernance.org/publications/basel-aml-index-2023-snapshot-money-laundering-risks-and-trends-academy-bulletin

Bitinvestment. 2023. Understanding Mixing Services in Cryptocurrencies. Referred 15.09.2024. https://bitvestment.software/understanding-mixing-services-in-cryptocurrencies/

Blockchain Academy. 2023. Hashing and Public Keys – The Cryptographic Foundations of Blockchain. Referred 14.08.2024. https://theblockchainacademy.com/hashing-and-public-keys-the-cryptographic-foundations-of-blockchain/

Nistorescu, G. 2021. Complex analysis of cryptocurrencies and their implications in the context of money laundering and terrorism financing. Referred 14.07.2024. https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1927/1880

Chainanalysis. 2024a. Russia's Cryptocurrency Pivot: Legislated Sanctions Evasion. Referred 10.12.2024. https://www.chainalysis.com/blog/russias-cryptocurrency-legislated-sanctions-evasion/

Chainanalysis 2024b. The Crypto Crime Report 2024. Referred 12.09.2024. https://go.chainalysis.com/crypto-crime-2024.html

Chainanalysis. 2023a. Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies. Referred 12.07.2024. https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/

Chainanalysis. 2023b. The Importance of Blockchain Security. Referred 18.12.2024. https://www.chainalysis.com/blog/blockchain-security/

Elliptic. 2020. A Brief Guide to Blockchain Analysis. Referred 07.07.2024. https://www.elliptic.co/blog/a-brief-guide-to-analytics-on-blockchain

ESMA. 2024. Markets in Crypto-Assets Regulation (MiCA). Referred 15.09.2024. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

European Parliament. 2019. Virtual Money: How Much do Cryptocurrencies Alter the Fundamental Functions of Money. Referred 25.07.2024. https://www.europarl.europa.eu/cms-data/207652/12.%20PE%20642.360%20LSE%20final%20publication-original.pdf

Europol. 2021. Tracing The Evolution of Criminal Finances. Referred 18.12.2024. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

FATF. 2024. Jurisdictions under Increased Monitoring - 25 October 2024. Referred 08.07.2024. https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2024.html

FATF. 2023. The FATF Recommendations. Referred 15.06.2024. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

FATF. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Referred 15.06.2024. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

FIN-FSA. 2024. Prevention of money laundering and terrorist financing. Referred 10.09.2024. https://www.finanssivalvonta.fi/en/prevention-of-money-laundering-and-terrorist-financing/

Finnish Government. 2024. Finland updates risk assessment of money laundering and terrorist financing. Referred 14.09.2024. https://valtioneuvosto.fi/en/-//10623/finland-updates-risk-assessment-of-money-laundering-and-terrorist-financing

Ilijevski, I., Ilik, G., Babanoski, K. 2023. Cryptocurrency Abuse for the Purposes of Money Laundering and Terrorism Financing: Policies and Practical Aspects in the European Union and North Macedonia. Referred 14.08.2024. https://eujournal.org/index.php/esj/article/view/16507/16351

Investopedia. 2023. What Is Hawala? Money Transfer Without Money Movement. Referred 16.10.2024. https://www.investopedia.com/terms/h/hawala.asp

Investopedia. 2024. Reports Warn of Crypto's Environmental Impacts. Referred 10.12.2024. https://www.investopedia.com/crypto-s-climate-impact-6544631

Ministry of Finance. 2023. Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2023. Referred 14.09.2024. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165433/VM_2023_8.pdf?sequence=1&isAllowed=y

Rahanpesun selvittelykeskus. 2024. Rahanpesun selvittelykeskuksen vuosikertomus 2023. Referred 15.10.2024. https://rahanpesu.fi/documents/46317582/0/vuosikertomus-saavutettava.pdf/d8a4e937-429c-c865-1bf4-946d5c82ff86/vuosikertomus-saavutettava.pdf?t=1717418263260

PwC. 2023. Global Crypto Regulation Report. Referred 20.07.2024. https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf

Reuters. 2024. Russian regulator encourages use of crypto to counter sanctions. Referred 14.10.2024. https://www.reuters.com/business/finance/russian-regulator-encourages-use-crypto-counter-sanctions-2024-07-03/

Sanction Scanner. 2024. Most Well-Known AML Regulators. Referred 14.09.2024. https://www.sanctionscanner.com/blog/most-well-known-aml-regulators-764

The Cambridge Centre for Alternative Finance. 2024. Cambridge Bitcoin Electricity Consumption Index 2024. Referred 10.12.2024. https://ccaf.io/cbnsi/cbeci

TRM Labs. 2024. Crypto Crime in Russia: Ransomware, Sanctions Evasion, and Disinformation. Referred 10.12.2024. https://www.trmlabs.com/post/crypto-crime-in-russia-ransomware-sanctions-evasion-and-disinformation

United Nations. 2024. Money Laundering. Referred 18.12.2024. https://www.unodc.org/unodc/en/money-laundering/overview.html

United States Department of State. 2024. Anti-Money Laundering and Countering the Financing of Terrorism. Referred 18.12.2024. https://www.state.gov/anti-money-laundering-and-countering-the-financing-of-terrorism/

UNODC. 2024. Casinos and cryptocurrency: major drivers of money laundering, underground banking, and cyberfraud in East and Southeast Asia. Referred 14.07.2024.

https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf