TRABAJO FIN DE GRADO

Guarding Against Crypto-Criminals: The EU's Actions to Prevent Terrorist Financing through Cryptocurrencies

Author/Student: Michelle Anastasi

Tutor/Professor: Jorge Mestre-Jordá

Bachelor degree in International Relations

Academic Year 2022-2023

Acknowledgements

Throughout my university years I have grown and learned a lot, especially to appreciate the little things and to surround myself with people you can trust and who can support you in the good and in the bad moments. Fortunately, I was lucky enough to find myself in a class with amazing people and teachers, which I wanna thank for being not only amazing at an academic level but also on a personal one.

Especially, i want to acknowledge how grateful I am for some of my teachers, who have helped me through some difficult moments, and have always pushed me to be the best version of myself.

I want to say thank you to my parents for teaching me how to be an educated, mature, and independent person, and to have supported me since an early age, to study abroad and pursue my dreams. I wouldn't be the person I am today without them.

Lastly, I want to thank my sister Alissa for showing me how to never stop in front of nothing and no one, and to make me realize what a lucky person I am to have her in my life. You gave me the strength and determination I needed to create a great future for myself and for you.

Abstract

This study examines the role and effectiveness of the current European Union legal framework in the fight against money laundering and terrorism financing through cryptocurrencies. For this reason, this paper is structured by firstly defining terrorism and terrorist financing activities, then analyzing cryptocurrencies and the risks associated with it, mainly Anonymity. Subsequently the research will examine the current EU legal framework on Anti-Money Laundering and Countering the Financing of Terrorism, with the main institutions and actors responsible for a coherent application. As well, this investigation expresses the discrepancies and limitations of the Anti-Money Laundering Directives, and the lack of control over certain cryptocurrencies actors by the EU Framework, which results in the abuse of the cryptocurrency market by terrorist organizations to facilitate funds to engage in illicit activities. Additionally, the study cases of Hamas and The al-Qassam Brigades' Fundraising Camp, and Al-Qaeda,demonstrates that terrorism financing through cryptocurrencies is real, and the European Union needs to have better harmonization between Member States and a more legally binding framework to leave less room for interpretation and lead the way in the fight against money laundering and terrorism financing, so that our economy can be safe from similar attacks.

Keywords: European Union, Anti-money Laundering, Terrorism Financing, Cryptocurrencies

Resumen

Este estudio examina el papel y la eficacia del actual marco jurídico de la UE en la lucha contra el blanqueo de capitales y la financiación del terrorismo a través de las criptomonedas. Para ello, este trabajo se estructura definiendo en primer lugar las actividades de terrorismo y financiación del terrorismo y analizando a continuación las criptomonedas y los riesgos asociados, principalmente el anonimato. Posteriormente, la investigación examinará el actual marco jurídico de la UE en materia de Antilavado de dinero y Financiación de Terrorismo, con las principales instituciones y agentes responsables de una aplicación coherente. Esta investigación también expresa las discrepancias y limitaciones de las directivas contra el blanqueo de capitales, así como la falta de control sobre ciertos actores de la criptodivisa por parte del marco de la UE, lo que lleva al abuso del mercado de la criptodivisa por parte de organizaciones terroristas para facilitar fondos para realizar actividades ilícitas. Además, los casos estudiados de Hamás y las Brigadas al-Qassam y el campamento de recaudación de fondos de al-Qaeda,demuestran que la financiación del terrorismo a través de criptodivisas es real y que la Unión Europea necesita una mejor armonización entre los Estados miembros y un marco jurídicamente más vinculante para dejar menos margen a la interpretación y ser líder en la lucha contra el blanqueo de capitales y la financiación del terrorismo para que nuestra economía esté a salvo de ataques similares.

Palabras clave: Unión Europea, lucha contra el blanqueo de capitales, financiación del terrorismo, criptomonedas

Index

Abstract 3
List of figures 7
List of abbreviations 8
1. INTRODUCTION 10
1.1. Research Questions 11
1.2. Research Objective 11
1.3. Sustainable Development Goals 16 and 17 12
1.4. Methodology 13
2. OVERVIEW TERRORISM AND TERRORIST FINANCING 14
2.1. Global Anti-Terrorism Measures on Terrorism 15
2.2. EU approach to terrorism 17
2.3. Defining terrorist financing 18
2.4. Defining Money Laundering 19
2.5. Link between money laundering and terrorism financing 20
3. OVERVIEW OF CRYPTOCURRENCIES 21
3.1. Defining cryptocurrencies 21
3.2. Blockchain 23
3.3. Types of cryptocurrencies 25
3.4. Players involved in cryptocurrencies. 26
3.5. Weaknesses and risks of cryptocurrencies 31
3.5.1. Double spending 33
4. LEGAL STATUS OF CRYPTOCURRENCIES IN THE EUROPEAN UNION 35
4.1. The EU's Crypto-Terrorism Fighters: Meet the Protagonist 36
4.1.1. European Institutions involved in AML and CFT 37
4.1.2. Europol 38
4.1.3. Financial Action Task Force (FATF) 40
4.1.4. European anti-money laundering authority (AMLA) 42
4.2. Legal framework of cryptocurrencies in AML and CFT 47
4.2.1. MiCa: set standards for crypto regulation globally 48
4.2.2. EU single rulebook 51
4.2.3. Anti-Money Laundering Directives 51
4.2.4. FATF Travel Rule 54
4.3. Regulations towards key players in crypto market 55

5. CURRENT LIMITATIONS OF THE EUROPEAN REGULATORY FRAMEWORKS ON AML/CFT AND CRYPTOCURRENCIES 58
5.1.1. Member States Divergences on AML/CFT Framework 58
5.1.2. Regulatory Dilemma of Cryptocurrency's Anonymity 60
6. OVERVIEW OF THE CURRENT STATE OF MONEY LAUNDERING AND TERRORIST FINANCING THROUGH CRYPTOCURRENCIES 62
6.1. Terrorist use of money 63
6.2. Possible use of cryptocurrencies in money laundering and terrorism financing 66
6.3. Cases of terrorists use of cryptocurrencies 72
6.3.1. Hamas and The al-Qassam Brigades' Fundraising Camp 73
6.4. Case of Al-Qaeda 77
6.4.1. Leave an Impact Before Departure 79
6.4.2. Al Ikhwa 81
6.4.3. Malhama Tactical 82
6.4.4. Reminders From Syria 82
6.4.5. Al Sadaqah 83
7. DISCUSSION 85
8. CONCLUSION 91
BIBLIOGRAPHY 95
LEGAL DOCUMENTS 100

List of figures

Figure 1: Fundraising campaign al-Qassam Brigades 75

Figure 2: social media post of a BTC address for donations by al-Qassam Brigades 76

Figure 3: prices of military equipment to ask for donations 81

List of abbreviations

AEC:	Anonymity Enhanced Cryptocurrencies
AML:	Anti-Money Laundering
AMLA:	Anti-Money Laundering Authority
AMLD:	Anti-Money Laundering Directive
ANF:	Al-Nusrah Front
BTC:	Bitcoin
CDD:	Customer Due Diligence
CFT:	Combating the Financing of Terrorism
DeFi:	Decentralized Finance
EBA:	European Central Banking
ETH:	Ethereum
ESA:	European Supervisory Authorities
EU:	European Union
FATF:	Financial Action Task Force
FBI:	Federal Bureau of Investigation
FINCEN:	Financial Crimes Enforcement Network
GCTF:	Global Counterterrorism Forum
GDP:	Gross Domestic Product
HSI:	Homeland Security Investigations
HTS:	Hay'at Tahrir al-Sham
ICO:	Initial Coin Offerings
IMF:	International Monetary Fund
IRS:	International Revenue Service
IRS-CI:	International Revenue Service-Criminal Investigation's Cyber Crimes Units
ITMC:	Ibn Taymiyyah Media Center
MiCA:	Market in Cryptoassets

MSB:	Money Service Provider
MSC:	Mujahideen Shura Council in the Environs of Jerusalem
NFT:	Non-Fungible Tokens
OIC:	Organization of Islamic Cooperation
P2P:	Peer-to-peer
POW:	Proof of work consensus mechanism
SEO:	Selected obliged entities
STO:	Security token offerings
TFR:	Transfer of funds regulation
UN:	United Nations
US:	United States

1. INTRODUCTION

The rise of cryptocurrencies in the financial system has attracted the attention of the international community, due to the distinctive nature that they present, and for the fast adaptability of individuals to enter the crypto-market. Hence, as any other type of currency, criminals and terrorist organizations have considered using those to their advantage in order to carry out criminal activities and destabilize the financial system.

The European Union, since 1990, has developed multiple legislations addressing the financing of terrorism, and money laundering. However, only recently, it has included crypto-assets as a subject that should be regulated, with the 6th Anti-Money Laundering Directive. It has done so, because studies from Europol confirmed that the EU, since 2017, has lost around 1% of its GDP (Gross Domestic Product) to money laundering (European Commission, 2021). As a result, the interest in analyzing the effectiveness of the role of the European Union in the fight against money laundering and terrorism financing (AML/CFT), stems from the fact that this area has not received the attention it deserves.

This research paper includes the examination of the current European legal framework in AML/CFT and its limits. However, to better understand the functioning of the legal framework, the study provides a thorough analysis of cryptocurrencies and terrorism. Also, it was essential to analyze the roles and responsibilities of key institutions such as Europol, the Financial Action Task Force (FATF) and the European Anti-Money Laundering Authority (AMLA). The thesis has also identified the existing gaps in the European regulatory framework, such as: the differences between Member States' AML/CFT regimes and the regulatory dilemma regarding the anonymity of cryptocurrencies are identified as key issues that need to be addressed.

Additionally, it was worth noting the existence of real cases where terrorist organizations have used cryptocurrencies to finance illicit activities, such as the case of Hamas, and the Al-Qassam Brigades, and also the case of Al-Qaeda. Through which it can be demonstrated that terrorism financing is a real threat, and it should concern the European Union, to decrease the loopholes in the EU legal frameworks, and avoid being exploited by terrorist organizations for their own advantages.

1.1. Research Questions

The research questions addressed in this paper concern the effectiveness of combating money laundering, terrorist financing and tax evasion through cryptocurrency transactions at the European level. The first question is whether there is an appropriate mandate to address these issues at the European level, given the cross-border nature of cryptocurrency transactions. The second question is to assess whether the EU legal framework is sufficient to detect illicit activities and identify the actors involved.

Finally, the thesis explores the main gaps and weaknesses of the EU legal framework, focusing on areas for improvement in order to effectively regulate and detect illicit activities related to cryptocurrencies. By answering these research questions, this thesis aims to provide an understanding of the challenges and opportunities the EU faces in addressing the intersection of cryptocurrencies and illicit financial activities.

1.2. Research Objective

The goal of this final work is to demonstrate and gain a comprehensive understanding of how terrorist organizations use cryptocurrencies. By studying the way terrorist organizations operate, the study aims to highlight the evolution of the strategies they use to finance their illegal activities. Another main objective is to analyze the risks

posed by cryptocurrencies in the global fight against money laundering and terrorist financing.

Considering the unique characteristics of cryptocurrencies, including their anonymity and decentralized nature, the study will assess the challenges faced by law enforcement authorities in monitoring and identifying suspicious transactions.

One of the study's main objectives is to examine the EU's role in combating the use of cryptocurrencies for illicit purposes, particularly in preventing the financing of terrorism. It will assess the effectiveness of the EU's legal and regulatory framework to determine its ability to detect and prevent cybercriminals from attempting to use cryptocurrencies to finance terrorism. By examining the specific regulations and mechanisms developed by the EU, the study aims to determine whether the current legal framework is strong enough to detect and arrest individuals and organizations involved in these illegal activities.

In addition, by examining the strengths and weaknesses of the existing provisions, the study aims to identify the gaps and limitations that hinder the detection and prosecution of these criminals. Thus, the study aims to suggest improvements or enhancements to the EU's legal framework to improve its effectiveness in combating the financing of terrorism through cryptocurrencies.

Ultimately, by better understanding the use of cryptocurrencies by terrorist organizations, assessing the risks of anti-money laundering efforts, and evaluating the effectiveness of existing EU legislation, this research aims to introduce policymakers, law enforcement authorities, and stakeholders to the challenges and opportunities of addressing this pressing issue.

1.3. Sustainable Development Goals 16 and 17

SDG 16 "Peace, justice and strong institutions" and SDG 17 "Partnerships for the goals" are key to preventing money laundering and terrorist financing through cryptocurrencies in Europe. SDG 16 aims to build effective institutions, ensure transparency in financial transactions, and promote international cooperation. SDG 17 emphasizes the need for partnerships to combat these illicit activities. Cooperation between governments, financial institutions and stakeholders is needed to exchange information, share best practices, and develop common standards and principles. Strengthening institutions, promoting transparency, and building partnerships are key strategies to combat money laundering and terrorist financing through cryptocurrencies in Europe (Department of Economic and Social Affairs, 2023). Thus, the reason behind the choice of these SDGs is that they perfectly highlight the two main requirements that the European Union should consider, when countering terrorism financing and cryptocurrencies.

1.4.Methodology

To achieve the objectives of this investigation, the overall approach has been to gather qualitative data from legal and official resources such as: the European Union Anti-Money Laundering Directives, the Financial Action Task Force recommendations, and the legal framework that addresses the topic of terrorism and terrorism financing.

The study involved thorough research to better comprehend the current situation of terrorism financing and money laundering through cryptocurrencies, which has shed light in the lack of information over the matter, due to the fast-developing environment of cryptocurrencies, and the rapid adaptability of terrorist organizations to this new means of financing.

Also, this topic presents controversies because the European Union and the International community do not want to explicitly affirm the risks and weaknesses of cryptocurrencies, so that the technology would be limited in entering the financial markets. Hence, finding information over the approach of the EU in the matter was a complicated task.

Additionally, the need of creating a database where individuals and organizations could identify cases of terrorism financing through cryptocurrencies should be taken into consideration. Hence, collecting the necessary information to pursue this investigation has led us to have an extensive bibliography [1], in order to conduct our research properly.

[1] The electronic sources used in this thesis have all been last consulted in May of 2023. Also, the majority of these resources have been updated in the year 2023.

2. OVERVIEW TERRORISM AND TERRORIST FINANCING

Terrorism is a multifaceted and complex phenomenon that involves the use of violence and intimidation to achieve political, religious, or ideological objectives. It poses a significant threat to global security and stability and is a growing concern for governments, organizations, and individuals worldwide. Terrorism financing, on the other hand, refers to the provision of financial support or resources to individuals or groups involved in terrorist activities. It is crucial to understand what terrorism is when discussing terrorism financing, on the basis that financing is a vital component of terrorist operations and can enable them to carry out attacks, recruit members, and spread their message. Therefore, combatting terrorism financing is a crucial aspect of counterterrorism efforts.

Moreover, this section will briefly explain the phenomenon of money laundering and its connection to terrorism financing. Money laundering in the past was solely connected to the financial and banking systems, however, nowadays money launderers have become more sophisticated. They can penetrate many sectors, such as non-financial sectors, non-governmental organizations, and others. Terrorists and significant organized criminal organizations undermine the stability and integrity of financial systems by taking advantage of gaps in national anti-money laundering and combating terrorist financing (AML/CFT) frameworks. This has a severe impact on the stability of the markets, undermines public confidence in financial institutions, and increases the volatility of global capital flows. Additionally, the economy as a whole and foreign direct investment are both negatively impacted by these occurrences. For instance, Europol estimated that, since 2017 the European Union has lost around 1% of its GDP through money laundering, which basically makes up for the EU budget of the Multiannual Financial Framework, which is 1% of the GDP (European Commission, 2021). This shows the importance of tackling money laundering and terrorism financing (EU AML/CFT Global Facility, 2022).

2.1. Global Anti-Terrorism Measures on Terrorism

The international community has not yet reached agreement about a universal definition of terrorism. This is due to the conflicting view on what forms terrorism, and the confusion around the concept of people's right to self-determination[2]. In order to successfully tackle this issue, the United Nations (UN) has accepted the necessity for an international definition of terrorism. A foundation for international cooperation against terrorism has progressively been built since 1963 through a number of international treaties due to the lack of an agreed-upon definition. These accords construct a list of terrorist actions or activities that support terrorism, including hostage-taking, hijacking of passenger aircraft, nuclear terrorism, and funding of terrorism. States are compelled to extradite or punish anyone responsible for certain crimes.

Due to the objective of this investigation, the analysis of what regulates terrorism at a global level and how it is perceived throughout different countries will not be developed in depth. However, there are various international treaties, conventions and resolutions that are worth mentioning when referring to terrorism and terrorism financing.

The most relevant resolutions, conventions and treaties about terrorism and terrorism financing at global level are: The International Convention for the Suppression of the Financing of Terrorism of 1999 (United Nations, 1999); Resolution UN 1566 of 2004[3], Resolution UN 1373 of 2001, which urged member states to collaborate urgently to prevent and suppress terrorist activities (United Nations Security Council, 2001).

[2] The concept of self-determination derives from the US Declaration of Independence of 1776. Which affirmed that governments derive 'their just powers from the consent of the governed' and that 'whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it' (Oxford University Press, 2008).

[3] Declares that any acts that fall within the scope of and are defined in international conventions and protocols related to terrorism are unjustifiable by any political, philosophical, ideological, racial, ethnic, religious, or similar considerations.

Moreover, the United Nations Global Counter-Terrorism Strategy (A/RES/60/288)[4], introduced in 2006 and reviewed in 2008 and 2010, marked a crucial turning point in enhancing international cooperation against terrorism. The strategy focuses on measures to address conditions conducive to terrorism, strengthen state capacity, and ensure respect for human rights and the rule of law. Further, the objectives included in this strategy have been developed more in depth through other resolutions including Resolution 2178 (2014)[5]; Resolution 2195 (2014) and Resolution 2199 (2015), which propose additional steps to break the link between terrorism and transnational organized crime. Also, Resolution 2199 (2015), reiterates and enhances the provisions of Resolution 2161 (2014) by proposing additional restrictions against ISIL/Da'esh and al-Nusrah Front addressing direct or indirect trading with these groups, cultural heritage protection, arms proliferation, and asset freeze (United Nations Security Council, 2015). Additionally, the Global Counterterrorism Forum (GCTF) has reinforced these efforts by advocating best practices for dealing with overseas terrorist fighters, abduction for ransom, and effectively combating violent extremism (European Parliament, 2015).

2.2. EU approach to terrorism

The European Union position to combat terrorism is ratified in the Council Common Position 2001/931/CFSP[6] on the application of specific measures and the Council Framework Decision 2002/475/JHA[7] on combating terrorism. According to the Council Common Position, a "terrorist act" is any deliberate act that might significantly harm a nation or an international organization that is carried out with the goal of: (1) “Seriously

[4] See for more information: https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy#:~:text=The%20United%20Nations%20Global%20Counter,operational%20approach%20to%20fighting%20terrorism.

[5] Improving cooperation through increased information sharing, mutual legal assistance, and effective border controls, about countering the threat of foreign terrorist fighters.

[6] See also: European Council. (2001). COUNCIL COMMON POSITION of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0093:0096:EN:PDF

[7] See also: OPOCE. EUR-Lex - 32002F0475 - EN. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002F0475

intimidating a population, or (2) Unduly compelling a Government or an international organization to perform or abstain from performing any act, or (3) seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization" including in the third point "participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the group" (European Council 931/CFSP, 2001). The resolution goes on to define the entities and groups involved in terrorism as follows: (1) Individuals who engage and participate in, or aid the conduct of terrorist activities. (2) Groups and entities owned or controlled by terrorist organizations, directly or indirectly; individuals, groups, and entities acting on their behalf or under their direction; and earnings from assets managed directly or indirectly by such persons and affiliated individuals, groups, and entities (European Council 931/CFSP, 2001).

In addition, the Council of Europe adopted in 2005 the Convention on the Prevention of Terrorism (CETS No 196), which does not clearly provide a definition of terrorism but helps to strengthen member States' efforts to prevent terrorism in two main ways: by declaring certain actions criminal acts that could result in the commission of terrorist offenses, such as public incitement, recruitment, and training; and by enhancing international and domestic cooperation on prevention (through the modification of existing extradition and mutual assistance agreements and other means); and by using additional means (Treaty Office - CETS No 196, 2005).

Furthermore, in May 2015 the European Committee of Ministers adopted the Additional Protocol to the Convention. (Council of Europe Treaty Series - No.217, 2015). The objective of the Protocol is to criminalize engaging in terrorism, becoming trained to commit terrorism, visiting another state for terrorist-related activities, and giving or collecting money to support this kind of travel. On October 22, 2015, the Protocol was

signed by the EU and twelve other Member States. The Convention was signed on the same day by the EU's Luxembourg Presidency (European Parliament, 2015).

2.3. Defining terrorist financing

Based on a report from the International Monetary Fund (IMF), terrorism financing is described as the “solicitation, collection, or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources”. Funds to finance terrorist activities can come from legal and illegal assets (International Monetary Fund, 2011). Accordingly to the International Convention for the Suppression of the Financing of Terrorism[8] a person is guilty of financing terrorism "if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" a criminal act covered by the Convention (UNODC, 1999).

Moreover, terrorists generally tend to use traditional funding methods, although as explained in this research they are adapting to new ways to raise funds. Usually, they require considerably small amounts of money to pursue their objectives and they can acquire it significantly fast, making it challenging for jurisdictions to identify the individuals (EU AML/CFT Global Facility, 2022). In addition, a lack of funds will limit the ability of criminals to carry out their attack, meaning that preventing and disrupting financial flows for terrorism related activities can be considered one of the most effective ways to fight terrorism. Therefore, the main objective of terrorist organizations when they engage in money laundering is to conceal both the nature of the sponsored activities and not only the sources of the funds (International Monetary Fund, 2011).

[8] See also: International Convention for the Suppression of the Financing of Terrorism (New York, 9 December 1999)
https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf

2.4. Defining Money Laundering

Closely connected to terrorism financing is the activity of launder money. Money laundering is often used for activities such as human trafficking, drug trafficking, tax evasions and more. In simple terms, "money laundering" is the process by which the profits of criminal activities are hidden to conceal their illegal source. More precisely, the Vienna Convention (1988)[9] and the Palermo Convention (2001)[10] define money laundering as a process that includes three different types of criminal conduct: (1) the obfuscation or deception of the true nature, source, location, disposition, movement, ownership, knowing that such assets is the result of criminal activity; (2) the transformation or disposal, knowing that such property is the result of criminal activity; 3) the disguise or deceits of the true nature, ownership, or use of assets, knowing that such property is the result of criminal activity (International Monetary Fund, 2011).

In addition, the Financial Action Task Force (FATF) is responsible for developing a global standard to combat money laundering and the financing of terrorism. The FATF, comprising 33 members, was established in 1989 by the G-7 Summit in Paris. In partnership with other major international organizations such as the IMF, World Bank, United Nations, and regional bodies, the FATF strives to create a uniform anti-money laundering and anti-terrorism financing framework (International Monetary Fund, 2011).

2.5. Link between money laundering and terrorism financing

As mentioned above, money laundering is the process of hiding the origin of financial profits that come from crime, on the other hand, terrorism financing is the accumulation of funds for terrorist activities. The main difference stems from the fact that in the case

[9] See also: United Nations. (1988). United Nations Convention Against Illicit Traffic in Narcotic Drugs And Pyschotropic Substances. In United Nations. https://www.unodc.org/pdf/convention_1988_en.pdf

[10] See also: United Nations General Assembly. (2001). 55/25. United Nations Convention against Transnational Organized. In United Nations (A/RES/55/25). https://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

of money laundering, the source is always illicit, whereas funds for terrorist financing can originate from both legal and illegal sources (International Monetary Fund, 2011).

The link between the two lies in the similar methods used to carry out both activities. In both instances, the individual in question uses the finance sector in a fraudulent way. The processes of terrorist financing and money laundering are often very similar and are sometimes used interchangeably. It is important to recognize the need to address these two interrelated challenges, by preventing, detecting and punishing illicit financial flows into the financial system and limiting support for terrorists, their groups and their actions. This requires an effective framework that combines anti-money laundering (AML) and combating the financing of terrorism (CFT). In addition, AML and CFT approaches overlap in their efforts to combat criminal and terrorist organizations, and it is important to focus on their financial activities and use financial records to identify individual members of their networks (International Monetary Fund, 2011).

3. OVERVIEW OF CRYPTOCURRENCIES

Cryptocurrencies have entered the financial system for a couple of years, raising many questions on what they are, how they work and who is involved in the selling and purchase of those currencies. In this section, it will be analyzed what are cryptocurrencies, blockchain technology and who are the main actors to look into in the cryptocurrency environment. Moreover, it will explain some of the main weaknesses and limits that these currencies pose to the current financial system.

3.1. Defining cryptocurrencies

A cryptocurrency is a type of digital currency that uses data encryption to avoid fraud and double spending. The term "crypto" refers to the different cryptographic methods and encryption algorithms used to secure these transactions. Cryptocurrencies are

often decentralized networks powered by blockchain technology, a distributed ledger[11] maintained by numerous computer networks. The virtual assets are often not issued by any central authority, making them potentially immune to intervention from manipulation by governments. Also, cryptocurrencies make it possible to make safe online payments without the use of intermediaries, which make them much more attractive for potential illegal uses of the currency (Frankenfield J., 2023)

In addition, cryptocurrencies can be seen as a digital representation of a physical currency, can be used to purchase products online, and are very popular as trading and investment (Bitstamp., 2022). As there is no legal tender in any nation or administration, virtual assets cannot be compared to conventional currencies. Therefore, a group of users' agreement, or the so-called "mining process," determines the exchange value of virtual currency.

Moreover, mining cryptocurrencies is a crucial part of the growth of the blockchain ledger, it is how new bitcoins are added to circulation and how the network confirms new transactions. The process of "mining" involves the use of powerful hardware to resolve a challenging computational arithmetic problem, which allows computers to process the first block of Bitcoin and put it in circulation, creating a repeating cycle with the entries of new blocks. One block of bitcoin is limited to 1 MB, which is enough to store over 2000 transactions, however different blockchains have different block size limits (Hong E., 2022).

Furthermore, cryptocurrencies can be distinguished between “convertible”, which holds the same value as a real currency, or “non-convertible”, meaning that it cannot be exchanged for a real currency, but it is only used for a particular virtual domain as in the online gaming community. There are also cryptocurrencies that are part of centralized

[11] A ledger is a digital or physical log that records transactions associated with a financial system. *Ledger | Ledger*. (2022, December 9).

systems or decentralized systems. Centralized systems hold virtual currencies that have a single administering authority, instead, decentralized systems hold virtual currencies that are distributed through an open-source peer-to-peer (P2P) currencies with no central administration or authority (U.S. Department of Justice, 2020).

Cryptocurrencies can be exchanged in a variety of ways, the most common of which being direct person-to-person exchange, cryptocurrency exchanges, and other middlemen. Furthermore, while possessing cryptocurrencies, they ought to be kept in a "wallet." Having a wallet is similar to having a virtual account; these wallets create access keys that can be likened to a conventional bank account number, as well as a Pin code that can be used to transfer and receive cryptocurrency. These virtual wallets can be physically kept in a number of ways. Among the various forms there are: external devices, such as “hardware wallets”; downloaded it as a software, also called “software wallets”; can be stored into a personal computer referred as “desktop wallet”, or into the personal smartphone called “mobile wallets”; lastly can be stored in forms of public and private keys, called “paper wallets”, and also as an online account associated with a cryptocurrency exchange (U.S. Department of Justice, 2020).

Moreover, the above explanation varies depending on what type of cryptocurrencies we are referring to. The most known ones are Bitcoin (BTC), Ethereum (ETH), Litecoin, Monero, Zcash, and Dash. While bitcoin is functioning on Blockchain technology, the other mentioned cryptocurrency uses non-public or private blockchains, which increase the difficulty of tracing the transactions, and are known “anonymity enhanced cryptocurrencies” (AECs) (U.S. Department of Justice, 2020).

3.2. Blockchain

A fundamental technology to the functioning of Bitcoin and other cryptocurrencies, although not for each of the existing one, is Blockchain. A blockchain, as the name implies, is essentially a collection of linked blocks of data on an online ledger. Each

block contains a number of transactions that have been confirmed separately by each validator on a network. (Ravikiran A.,2023).

The way blockchain is structured allows it to store transactional records in a network connected through peer-to-peer[12] (P2P) nodes. It is in fact challenging to manipulate transaction histories because every time a block hits its maximum number of transactions, a new block is created that must first be checked before being confirmed. Basically, a network of individual nodes, or computers, which make up the ledger, must evaluate and approve the information included in the online ledger (Ravikiran A.,2023). As a result, all of the verified transactions are kept in the history of the public ledger, preventing double spending and counterfeiting by cryptographically recording every transaction (U.S. Department of Justice, 2020).

It is also vital to note that Blockchain is utilized for purposes other than cryptocurrency. Despite the fact that currencies like Bitcoin significantly rely on it, Blockchain is capable of supporting a variety of applications connected to many industries, including finance, supply chain, and manufacturing (Ravikiran A., 2023). It is in fact considered to have a lot of benefits. First of all, it is a considerably secure system that uses digital signature features to carry out transactions free from fraud, making it difficult, although not impossible, for other users to corrupt a person's data without a unique digital signature. Secondly, Blockchain is a decentralized system, meaning that to approve transactions there is no need to involve authorities like governments or banks. Transactions are accepted with the mutual consensus of users, making the latter much faster and safer. Thirdly, it is characterized by automation capability, meaning that the system can generate actions and payments automatically when certain sets of criterias are met (Ravikiran A.,2023). Basically, Blockchain constitutes an advancement in lowering transaction costs by streamlining payment processing, and enhancing

[12] “Peer-to-peer (P2P) networks are a type of decentralized network architecture that allows nodes to share and access resources directly without a central authority” (Abrol, 2023).

security by encrypting transactions in a digital database that is almost impossible to modify (JP Morgan Chase & Co., 2023). However, the technology still holds the risk of illicit uses of cryptocurrencies, which include selling and buying drugs, engaging in criminal financial transactions, soliciting funds to support terrorist activities, engage in money laundering, and even committing crimes directly implicating the cryptocurrency marketplace itself (U.S. Department of Justice, 2020).

3.3. Types of cryptocurrencies

There are several types of cryptocurrencies, each with its unique features and use cases. The most well-known cryptocurrency is Bitcoin, Bitcoin uses a proof-of-work (PoW)[13] consensus algorithm to validate transactions and secure the network. BTC was the first cryptocurrency to be created in 2009, by Satoshi Nakamoto, a pseudonym used by the creator or creators of Bitcoin. The identity of Satoshi Nakamoto is not publicly known (Sharma R., 2023).

Another popular cryptocurrency is Ethereum, which was created in 2015 and uses a proof-of-stake[14] consensus algorithm. Ethereum is known for its smart contract capabilities, which enable the creation of decentralized applications (DApps) on its blockchain (Frankenfield J., 2023). Other cryptocurrencies include Ripple, which is designed for international payments and settlement, Litecoin, which has faster transaction times and lower fees compared to Bitcoin, and Bitcoin Cash, which is a fork of Bitcoin and was created to address issues with Bitcoin's scalability. There are also privacy-focused cryptocurrencies such as Monero and Zcash, which use advanced cryptographic techniques to keep transactions private (Frankenfield J., 2023). In this investigation we will not focus on only one crypto currency, however, Bitcoin will be

[13] “Proof of work is a blockchain consensus mechanism in which computing power is used to verify cryptocurrency transactions and add them to the block chain” (Frankenfield, 2023).
[14] “Proof of stake is a cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain” (Frankenfield J., 2022).

mentioned in more instances due to its popularity within terrorist groups and cyber criminals. This does not exclude the fact that all the other cryptocurrencies have less risk of being abused by terrorist organizations.

Moreover, when discussing cryptocurrencies, it's important to distinguish between different types of coins. The five official categories are: Utility (e.g., XRP, ETH), Transactional (e.g., Bitcoin), Platform (e.g., Solana), Governance (e.g., Uniswap), and Security tokens (e.g., MS Token). Cryptocurrencies offer faster transactions, greater transparency, and decentralization. As new coins are developed, the crypto space continues to evolve, presenting opportunities for investors and developers (Frankenfield J., 2022)

3.4. Players involved in cryptocurrencies

The cryptocurrency's market has developed rapidly in the last years, with the new cryptocurrencies being created all the time, the crypto space continues to evolve, and with it the actors involved in it. As a result, Financial Intelligence Units (FIU) consider it very challenging to stay up to date with regulations regarding the constant developing protagonists of the cryptocurrency market. Hence, acknowledging these players is essential to then evaluate how they are being supervised, and assess the risk surrounding them. Later, paragraph 4.3 will cover how these actors are regulated in the European Union.

One of the first and most important players in the crypto-market is the cryptocurrency user. According to the 2014 *Financial Action Task Force (FATF) report on Virtual Currencies*, a cryptocurrency user is a natural person or legal entity, who acquires coins to use for three main purposes: 1. To purchase real or virtual goods or services. 2. To make P2P payments. 3. To use them for investment purposes (FATF , 2014).

The European central bank has briefly listed the main ways of how a user could acquire cryptocurrencies. The European Central Bank has summarized the primary methods for acquiring digital currencies. To begin, a user might purchase his coins on a cryptocurrency exchange with FIAT cash or another cryptocurrency. Assets can also be acquired directly from another cryptocurrency user, for example, through a P2P exchange or another trading platform. Second, if a cryptocurrency is built on a PoW consensus method, the user may be able to mine a new coin. In certain situations, a cryptocurrency user might get the coins through a coin offeror, either as part of a free initial coin offering or as part of a public sale organized by the coin offeror (for example, Ethereum was initially sold in a crowdsale to reduce development expenses). Third, if the user wants to offer products and services in return for Cryptocurrencies, he may be paid in crypto assets. Finally, a cryptocurrency user may receive coins as a gift or donation from a fellow cryptocurrency user (European Central Bank, 2015).

A second player in the cryptocurrency market is the miner. Cryptocurrency miners are individuals or entities that validate and add transactions to a blockchain network by solving complex mathematical problems using specialized computer hardware. Miners play a critical role in maintaining the security and integrity of the blockchain network, as they aim to prevent double-spending and ensure the accuracy of the ledger. In return for their efforts, miners are rewarded with newly mined cryptocurrency units and transaction fees (Hong E., 2022). However, miners could simultaneously be cryptocurrency users, or groups of people that have created a business out of mining coins to sell them for FIAT currency or in exchange of other cryptocurrencies. The “mining business” could represent a risk in the fight against terrorism financing and money laundering, which appears to be underestimated by governments (European Central Bank, 2015).

A third crucial group of actors are cryptocurrency exchanges. Cryptocurrency exchanges are entities or persons who provide exchange services to cryptocurrency users, generally without any commission, and they are used by cryptocurrency users to

sell and buy coins for FIAT currency and vice versa (FATF, 2014). The most known cryptocurrency exchanges are: Coinbase GDAX[15], Bitfinex[16], HitBTC[17], and Kraken[18] (Snyers, A., et al, 2018).

In addition, it is important to differentiate between *pure* cryptocurrency exchanges, which only accept cryptocurrencies as a form of payment, and *regular* cryptocurrencies exchanges that accept payments in FIAT currencies. It is worth noting that most of both types of exchanges operate as custodian wallet providers, as is explained further below (Snyers, A., et al, 2018).

Moreover, a broad range of payment methods, including wire transfers, PayPal transfers, credit cards, and other currencies, are generally available to customers of cryptocurrency exchanges. Some cryptocurrency exchanges additionally offer conversion services to businesses that accept cryptocurrency payments as well as information about the cryptocurrency market (such as trading volumes and coin volatility) (Snyers, A., et al, 2018). The so-called trading platforms also represent an important player in the exchange of cryptocurrencies. Trading platforms can be seen as marketplaces where cryptocurrency users interact directly with each other to buy or sell their coins (Snyers, A., et al, 2018). Generally trading platforms are referred to as “P2P exchanges” or “decentralized exchanges”[19]. They can be differentiated from cryptocurrency exchanges by two main reasons: 1. Trading platforms do not engage in the buying and selling of coins; 2. There is no entity nor company that supervises the transactions, but instead they are controlled by a software that is used to automatically connect buyers and sellers with each other (either online or physically), based on the

[15] See: https://www.coinbase.com
[16] See: https://www.bitfinex.com
[17] See: https://hitbtc.com
[18] See: https://www.kraken.com
[19]See: A. MARSHALL, “P2P Cryptocurrency Exchanges, Explained”, April 2017, https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained

terms they prefer. For instance, LocalBitcoins[20] is a well-known trading platform for Bitcoins (Marshall, 2017).

Furthermore, wallet providers constitute an important player in crypto-markets. Wallet providers are entities that provide digital or e-wallets that allow users to store and transfer coins (FATF, 2014). These wallets generate access keys (cryptographic keys) that can be compared to a regular bank account number and generate a Pin code used to send and receive cryptocurrencies. There are several types of wallet providers[21]:

1. *Hardware wallets providers*: A company that produces physical devices that are used to securely store and manage cryptocurrencies, which are necessary to access and authorize transactions on the blockchain. Hardware wallet providers offer users a more secure alternative to software wallets, which are vulnerable to hacking and malware attacks. By using a hardware wallet, users can store their cryptocurrency offline and away from potential threats.

2. *Software wallet providers:* A company or organization that offers software applications for the storage and management of cryptocurrencies. These wallets are accessible through a computer or mobile device and allow users to manage their cryptocurrency holdings through a user-friendly interface. However, they are generally considered less secure than hardware wallets, as they are more susceptible to hacking and malware attacks. Therefore, it is important for users to carefully choose a reputable software wallet provider and take necessary security precautions to protect their assets.

3. *Custodian wallet providers*: A company or financial institution that provides a service to securely store and manage cryptocurrencies on behalf of their clients.

[20] See: https://localbitcoins.com
[21] See also: Virtual Currencies and Terrorist Financing: assessing the risks and evaluating responses. In the European Parliament (PE 604.970).
https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

Custodian wallets are commonly used by institutional investors or high net worth individuals who may require a more secure solution for their cryptocurrency holdings. Custodian wallet providers typically offer advanced security measures such as multi-signature technology (eg. Coinbase)[22], which requires multiple parties to approve a transaction, and cold storage, which involves storing cryptocurrencies offline in secure vaults. They may also offer insurance protection to cover potential losses in the event of a security breach or other unexpected event. While custodian wallets offer a high level of security and peace of mind for users, they may also come with higher fees and require more trust in the custodian provider.

An additional player, who is fundamental to cryptocurrencies is the coin inventor. Coin inventors are people or groups who provide the technological groundwork for a cryptocurrency and define the original guidelines for its use, as implied by the name. Sometimes the identity of the creator is publicly known, such as in the cases of Litecoin, Ripple and Cardano, but in other cases, such as in the case of Bitcoin and Monero, the identity remained anonymous. Also, some creators decide to stay involved in the process of improving the cryptocurrency system and algorithm, while others cease to participate after having created the cryptocurrency (eg. Bitcoin) (European Central Bank, 2015).

Lastly, there are the coin offerors**.** Typically, they refer to entities that offer and sell digital assets, such as cryptocurrencies or tokens, to the public in exchange for other cryptocurrencies, FIAT currencies, or other assets. These offers may be made through initial coin offerings (ICOs), security token offerings (STOs), or other similar fundraising mechanisms. Typically, coin offerors do this to support the currency's early growth or development. Also, it is important to note that a coin offeror can be the same person as the coin inventor (Snyers, A., et al., 2018).

[22] See: https://www.coinbase.co

3.5. Weaknesses and risks of cryptocurrencies

Cryptocurrencies offer a range of benefits such as cheaper transactions, decentralization, and anonymity. However, the development of cryptocurrencies in the world of finance has brought various risks and challenges, especially in the fight against money laundering, terrorist financing and tax evasions. The role of cryptocurrencies in terrorism financing will be laid out in detail in paragraph 6, however it is first necessary to analyze the main risks and challenges that the nature of cryptocurrencies pose to the international arena of finance and politics.

One of the key issues that surround cryptocurrencies is the anonymity and pseudo-anonymity that characterizes them. The anonymity of cryptocurrencies allows cyber-criminals to avoid detection, opening opportunities to engage in illicit transactions that fall outside of the regulatory framework. As a matter of fact, anonymity represents one of the biggest challenges in combating money laundering and terrorism financing through Cryptocurrencies due to the difficulty of tracing back the transaction to a specific user or individual (Snyers, A., et al, 2018).

Furthermore, anonymity is a big obstacle in the sphere of tax avoidance. It is considered tax evasion when a user purchases a cryptocurrency that should be taxed but avoids doing so. However, because of the degree of anonymity at play, an authority cannot identify who engaged into the taxable transaction when attempting to track it back to an account. That is why cryptocurrencies are so appealing to tax evaders (He et al., 2016)

Although the majority of cryptocurrencies are anonymous, some of them are pseudo-anonymous, this means that with great challenges and effort, and often complex techniques, it could be possible for authorities to find out a user identity. Pseudo-anonymity can be of help in the fight against money laundering, terrorist

financing, however, it does not allow for the standardization of a legal approach to tackle money laundering, terrorist financing, and tax evasion more widely. Discovering identities is a significantly difficult and expensive process, and most importantly, not in every case will lead to a certain result, that is why a more structural regulatory approach is needed surrounding the characteristic of anonymity of cryptocurrencies (Snyers, A., et al., 2018).

In the second place, the cross-border nature of cryptocurrencies presents a significant challenge for regulators and financial institutions around the world (Snyers, A., et al, 2018). Due to their decentralized and global nature, cryptocurrencies can be easily transferred across borders without the need for intermediaries, making it difficult for governments to monitor and regulate their use. This lack of regulation also makes cryptocurrencies attractive to criminals who can use them for money laundering, terrorism financing, and other illicit activities.

According to a report by the Financial Action Task Force (FATF), "Virtual assets and virtual asset service providers present unique challenges that are not adequately addressed by traditional AML/CFT mechanisms." (FATF,2019). The research highlights that the decentralized structure of cryptocurrencies makes identifying and verifying users and transactions problematic, and that there is a lack of uniformity in rules across jurisdictions (FATF,2019).

To address these challenges, the FATF has developed a set of recommendations for countries to regulate virtual assets and virtual asset service providers, including requiring them to register with authorities, conduct customer due diligence, and report suspicious transactions. However, the effectiveness of these recommendations depends on their implementation and enforcement by individual countries, and these rules will only be adequate if taken at an international level (FATF,2019).

Another factor that challenges the fight against money laundering and terrorist financing is the absence of a central intermediary when exchanging cryptocurrencies, which makes it harder to find a subject of prime focus when creating regulations. The lack of a central intermediary represents a significant challenge when trying to understand which player in the crypto market the regulation should be aimed at. However, it could be possible to consider a crypto exchange system something similar to having a central intermediary, through which users, and criminals, buy and sell cryptocurrencies (Snyers, A., et al, 2018).

3.5.1. Double spending

Double spending is a major risk for cryptocurrencies, as attackers can fool merchants[23] into believing a transaction is confirmed while convincing the entire system to accept another transaction. This malicious action can cause merchants to suffer financial losses and lose merchandise. To solve this problem, a proof-of-work system was introduced that uses computers to confirm groups of transactions and create a blockchain. Transactions are organized into blocks that reference previous blocks through unique hashes and headers. These verified blocks form a tree structure, and the system considers the longest branch with the highest proof-of-work value to be a valid chain (Rosenfeld M., 2014).

In general, transactions are considered protected from double spending by sufficient verification. However, a successful double-spending attack involves several steps. First, the attacker reports the transaction to the platform when the affected merchant receives the payment. Second, the attacker secretly mines a branch that is currently connected to the last blockchain that contains competing transactions that forward the payments to

[23] A Cryptocurrency Merchant Account is a type of bank account that enables businesses to send and receive cryptocurrency and altcoins smoothly (Monneo, 2023).

the attacker. The attacker patiently waits for the transaction until the merchant receives sufficient confirmation that gives him the confidence to release the cryptoassets. If necessary, the attacker continues to extend the secret branch until it is longer than the public branch (the legitimate branch containing the transaction) and sends it to the network. Because of the length of the secret branch, the network confirms it as valid, replacing payment to the attacker with payment to the seller. (Rosenfeld M., 2014).

Understanding this type of process includes analyzing difficult mathematical assumptions, however, in this paper, we will simply summarize a successful double spending attack, as when the attacker succeeds in making his branch longer than the legitimate branch (already confirmed by the network), and manages to fool the merchant. Moreover, if an attacker has control of the majority of the branches, he could be able to reject and modify various blocks, which are not his own, and earn the entire amount of coins circulating in the chain at the time of the attack. The attacker could also be able to deny all the transactions, disrupting the entire operation. Basically, if the attack is successful, all the found blocks during the process will be confirmed as valid, and the attacker will be able to receive all of the rewards as if you had done it legitimately (Rosenfeld M., 2014).

In addition, although this analysis was based on the functioning of bitcoin, a double spending attack could happen in other networks that manage other cryptocurrencies, such as Ethereum and Monero.

4. LEGAL STATUS OF CRYPTOCURRENCIES IN THE EUROPEAN UNION

Analyzing the risks and weaknesses that cryptocurrencies present, arises the question of how to properly legislate them, and how to prevent their abuse by terrorist

groups and cyber criminals. Unlike the FIAT[24] currencies, which are controlled by the government or monetary authorities, cryptocurrencies are not backed up by any public or private entities.

Although cryptocurrencies have been a positive implementation in the strategic planning oriented toward building a digital economy, it has pushed some states to explore the legal nature of cryptocurrencies, as their legal status is necessary to take any steps further in legalizing them.

With respect to the legal nature of cryptocurrencies, there are two main approaches that can be taken. The first approach is to equate them with existing legal objects such as securities, currencies, or commodities and develop rules that specifically address the unique characteristics of cryptocurrencies as a relevant type of object. The second approach is to recognize cryptocurrencies as fundamentally new legal objects and create regulations from scratch. Currently, most countries in the world are struggling to regulate cryptocurrency relationships and address issues related to cryptocurrency transaction licensing, taxation, and the prevention of money laundering and terrorist financing through the proceeds of crime. (Bolotaeva et al,. 2019).

The European Union has acknowledged the risk that cryptocurrencies present in the fight against money laundering and terrorism financing and has recognized the need to consider cryptocurrencies as an asset that is distinct from anything that has ever entered the financial market before. That is why it has developed a new Anti-Money Laundering Directive (AMLD6) that includes the risks associated with digital assets such as cryptocurrencies and raises awareness about cybercrimes.

[24] Fiat money is a government-issued currency that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it (Chen, 2023).

Moreover, the European Union legal framework on AML/CFT mainly consists of Anti-Money Laundering Directives, the FATF recommendations, the new Anti-money Laundering Authority (AMLA), the EU Single Rulebook, and the new approved regulation MiCA (Markets in Crypto Assets). In cooperation with agencies such as Europol, the Financial Action Task Force, and the support of the European Parliament, the Council, and the European Banking institutions, the European Union aims to be a pioneer in the fight against money laundering and terrorist financing through cryptocurrencies.

The below paragraphs will better explain the role of the European Union in AML/CFT and the current legal framework in the matter.

4.1.The EU's Crypto-Terrorism Fighters: Meet the Protagonist

Many actors and institutions are involved in the policy-making process on cryptocurrencies and terrorist financing in the European Union. The European Commission, the European Parliament and the Council of the European Union are among the main institutions involved in the development of EU policy on cryptocurrencies and anti-money laundering and terrorist financing (AML/CFT). The Financial Action Task Force (FATF), an intergovernmental organization that sets global standards for combating money laundering and terrorist financing, also plays an important role in shaping the EU's approach to cryptocurrency regulation. In addition, national authorities in EU member states also play a role in implementing and enforcing EU rules related to cryptocurrencies and combating money laundering and terrorist financing. Moreover, in July 2021, the European Commission proposed to establish an Anti-Money Laundering Authority (AMLA), to counter money laundering and terrorism financing. The AMLA would serve as the hub of a unified framework made up of both the authority and the national agencies mandated with AML/CFT supervision. Additionally, it would develop a structure for collaboration amongst EU financial

intelligence units (FIUs) and assist them[25]. Additionally, the EU focus on the area of counterterrorism has rapidly increased over the years, resulting in higher cooperation with other security and judicial bodies, such as Europol, eu-LISA[26] and Eurojust[27].

4.1.1. European Institutions involved in AML and CFT

The list of European institutions involved in the fight against money laundering and terrorism financing is extensive, due to the cooperative nature of the fight for AML/CFT, however the main ones include: The European Commission, serving as the executive branch, and playing a crucial role in implementing policies and shaping them. The main tasks include proposing legislation, monitoring its implementation in Member States and coordinating efforts. Then, another essential actor is the European Parliament, which is the legislative body of the EU, and has the responsibility of reviewing and amending proposed legislation related to money laundering and terrorism financing. Also, it overviews the work and the effectiveness of the European Commission (European Commission, 2023).

Additionally, the Council of the European Union represents the EU member states' governments, and in collaboration with the Parliament provides its expertise on decision making of legislative proposals. Based on proposals from the European Commission, it adopts laws and regulations about AML/CFT (Council of the European Union – Role | European Union, 2023). Moreover, the European Banking Authority (EBA), which is an independent EU authority, ensures the effectiveness and the consistency of regulations

[25] Anti-money-laundering authority (AMLA): Countering money laundering and the financing of terrorism | Think Tank | European Parliament. (2022). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733645.

[26] The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (Discover eu-LISA, 2022)

[27] The Agency leads the judicial response to growing threats in Europe, enabling the Member States to keep one step ahead of criminals, mainly focusing on organized crime groups.

in the banking sector across the EU member states. In addition, it develops standards and guidelines on AML and CFT matters to increase cooperation and synchronization in the application of these standards (European Banking Authority, 2023). Similarly, the European Central Bank (ECB), has the responsibility of the monetary policies in Europe. It provides guidance to financial institutions under its jurisdiction and supervises the compliance of AML/CFT regulations (European Central Bank, 2022).

Furthermore, Financial Intelligence Units (FIUs), are national agencies with the job of receiving, analyzing, and spreading intelligence on suspicious transactions surrounding matters of money laundering and terrorism financing. FIUs, despite not being classified as institutions themselves, hold significant importance within the European anti-money laundering framework. In the European Union, FIUs collaborate via the FIU.net platform, which is facilitated by Europol, an essential institution in the fight of AML/CFT, which will be better explained below (Council of Europe, 2023)

4.1.2. Europol

Europol is a significant actor in Europe against the fight of money laundering and terrorist financing founded in 1998. The mission behind its establishment is to counter serious international threats, such as organized crime, cybercrime, and terrorism. Europol aims to support member states to deal with crimes that require international approach and cooperation between various countries, whether they are EU members or not (Europol,2023).

In order to support member states and increase cooperation, Europol has established a series of organizations, to provide specific expertise, information exchange, intelligence analysis, and many other tools to combat terrorism financing and money laundering. The most relevant agencies are: The European Serious Organized Crime

Center (ESOCC)[28]; The European Cybercrime Task Force (EC3)[29], which focuses on providing support to EU crisis management structures, and increases cooperation between FIU and Law enforcement agencies (LEAs); The European Counter Terrorism Center (ECTC), whose primary responsibilities are customized to each EU Member State, developed an approach that entails facilitating information exchange and cross-border cooperation, supporting and collaborating on investigations, reducing the use of social media for radicalization purposes, and having a strategic support capability; the European Financial and Economic Crime Center (EFECC)[30] for the integrity of the European financial system.

Basically, with the support of Europol Member States can counter the risks of terrorism financing and money laundering through cryptocurrencies much more efficiently, due to the cyber-crime expertise that is offered by the organization. Together with other factors explained in this research, and with the development and updating of regulations around cryptocurrencies, the strength of Europe against these challenges is surely increasing.

4.1.3. Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) plays a crucial role in the fight against money laundering and terrorism financing in Europe and around the world. It was established in

[28] During 2021 ESOCC provided extensive operational support to 742 Member States' serious and organized crime investigations. This led to the arrest of over 12 000 suspects and the seizure of over EUR 700 million in cash (European Serious and Organized Crime Centre - ESOCC | Europol, 2023.).

[29] EC3 was involved in the discovery of one of the most dangerous and long-lasting cybercrimes in history, called EMOTET. See for more in: https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action

[30] In September 2022, EFECC offered operational and analytical help in one of the biggest money laundering operations in Europe, referred to as Operation Whitewall. The suspects are suspected of laundering more than 200 million euros over the course of the inquiry (European Financial and Economic Crime Centre - EFECC | Europol, 2023).

1989 with the objective of creating and advancing regulations to effectively limit the activities of money laundering and the financing of terrorism. Also, the FATF is an intergovernmental body that aims to establish international AML/CFT standards and tracks the ability of countries to implement such requirements (FATF, 2012-2023).

The FATF has developed a series of guidelines that are intended to provide a uniform framework of measures that nations should take in order to combat money laundering, financing of terrorism, and other potential threats. In 1990 the FATF drew the original forty recommendations to counter the abuse of financial systems and money laundering. Further in 1996, the recommendations had been revised to extend their scope, and to stay up to date with new money laundering techniques. Later, in 2001 and 2003 the FATF Recommendations were reassessed again, to include measures about the financing of terrorism and create the Eight, later extended to Nine, Special Recommendations on Terrorist Financing. These recommendations have been agreed on by 180 countries and are considered the international standards for AML and CFT. The key actions covered by the Recommendations are: Recognize potential risks and create policies for domestic coordination; Take action against money laundering, terrorism financing, and proliferation financing; Implement preventive measures in the financial sector and other relevant areas; Define the responsibilities and authorities of investigative, law enforcement, and supervisory agencies; Increase transparency and access to information regarding beneficial ownership of companies and arrangements; Promote international collaboration. (FATF ,2012-2023).

Moreover, due to the challenge that terrorism financing and money laundering pose to national and international security, the FATF has dedicated a special section specifically for terrorism financing. Respectively are:

1. *Terrorist financing offense:* Adopting a risk-based approach enables countries to implement measures that are tailored to the level of risk and comply with FATF guidelines, resulting in more effective resource allocation and the application of proportionate preventative measures to effectively target risks.
2. *Targeted financial sanctions related to terrorism and terrorist financing:* Nations must adhere to UN Security Council resolutions that aim to prevent and combat terrorism and its financing by implementing targeted financial sanctions regimes. These measures require immediate freezing of the assets of any person or entity designated under Chapter VII of the UN Charter, including resolutions 1267 (1999) and its successors, or designated by the nation under resolution 1373 (2001). Furthermore, nations should prevent designated individuals or entities from accessing any resources, including financial resources, directly or indirectly.
3. *Targeted related financial sanctions related to proliferation:* To comply with U.N. Security Council resolutions on preventing the proliferation of weapons of mass destruction and their financing, countries must implement targeted economic sanctions. These resolutions require countries to freeze the assets of any natural or legal person designated by the UN Security Council under Chapter VII of the UN Charter and to ensure that no funds or assets are made available, directly or indirectly, for their benefit.
4. *Non-profit organizations:* Countries need to assess whether their laws and regulations concerning non-profit organizations can prevent terrorist financing abuse. These organizations can be at risk of being exploited for such purposes, and so it is important to implement measures that are appropriate to the level of risk, in accordance with the risk-based approach. These measures should protect non-profit organizations from being used by terrorist groups posing as legitimate entities or using them as a means of bypassing asset-freezing measures. Additionally, they should also prevent the covert diversion of funds intended for lawful purposes towards terrorist organizations (FATF,2012-2023).

Furthermore, the FATF in accordance to risk-based approach, suggests that countries evaluate the level of risk of money laundering and terrorism financing within their borders to properly adopt the measures recommended by the FATF, and be able to modify each measure in order to target in the most effective way the nature of the risks.

4.1.4. European anti-money laundering authority (AMLA)

The establishment of the AMLA was proposed in 2021, by a proposal for "Regulation of the European Parliament and of the Council" to establish the Authority for Anti-Money Laundering and Terrorism Financing, redrafting the Regulations (EU) 1093/2010[31], (EU) 1094/2010[32], (EU) 1095/2010[33]. In the proposal it is mentioned that currently the AML/CFT legal framework of the European Union mainly consists of the Anti-Money Laundering Directives (AMLD)[34], and the Funds Transfer Regulation[35]. However, this proposal had the objective to extend the scope of the EU legislation and submitted three additional proposals within the same document. These are: the creation of a Single Rulebook for AML/CFT; a new AML/CFT Directive (AMLD6); a revision of Regulation 2015/847 on the disclosures corresponding transfer of funds. In accordance with the Commission Action Plan on AML/CFT of May 7, 2020, this package of four legislative initiatives is taken as one unit. Aiming at establishing a new and stricter enforcement framework for AML/CFT regulations in the Union (European Commission, 2021).

---

[31] Establishing a European Supervisory Authority (European Banking Authority) in 2010. (European Parliament & Council of Europe, 2010)

[32] Establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority) (European Parliament & Council of Europe, 2010b).

[33] Establishing a European Supervisory Authority (European Securities and Markets Authority) (European Parliament & Council of Europe, 2010c)

[34] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amended by Directive (EU) 2018/843 of the European Parliament and of the Council (OJ L 156, 19.6.2018, p. 43-74).

[35] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance), (OJ L 141, 5.6.2015, p. 1-18).

Moreover, according to the proposal, anti-money laundering would be the focus of an integrated system consisting of the Authority itself and national authorities. It would also support EU financial intelligence units (FIUs) and establish a cooperation mechanism between them. Basically, the AMLA delivers "A partial centralization of AML/CFT supervision (...) with direct and indirect supervisory powers through an "integrated system composed of the AMLA and national supervisors (...) to grant effectiveness for the future integrated system to act as a 'mechanism' " (Remeur C., 2023). It is important to note that the AMLA was not established to be a FIU, but more a FIU's support and coordination mechanism that could provide standards and assistance to FIU in cases of detecting suspicious activities or transactions connected to money laundering and terrorist financing (Remeur C., 2023)

Eva Maria Poptcheva, a member of the European Parliament, and co-rapporteur of the proposals[36] explained in an interview that the Parliament agreed, with a sweeping majority, on a legislative package that is made of three instruments: two of them are regulations and directives, that will basically make up the Rule Book on AML and CTF, and one is the creation of the AMLA. The Council subsequently reached semi-partial political agreement on the proposal on June 29, 2022, and the rapporteurs issued a joint report in May 2022. The proposal was then voted on by the Committee on Economic and Monetary Affairs and the Committee on Civil Liberties, Justice and Home Affairs, and adopted in March 2023. The report was adopted by 102 votes to 11, with 2 abstentions (Remeur C., 2023).

The AMLA will bring many changes in the fight against money laundering and terrorist financing. It is intended to supervise various sectors around money laundering

[36] Eva Maria Poptcheva, Renew Europe Group, Partido de la Ciudadania Spain, co-rapporteur of: Anti-money-laundering authority (AMLA): Countering money laundering and the financing of terrorism | Think Tank | European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733645

and terrorism financing, such as “selected obliged entities” (SEO) and increase cooperation between national supervisors to increase the effectiveness of the AML legislations. The AMLA will closely monitor and issue motions regarding “selected obliged entities” in the financial industry operating in certain Member States that are at high risk of AML and CFT by their national supervisor. The selection process of these entities will be revised every three years and will be carried out by Joint Supervisory Teams (JSTs), directed by the members of the AMLA, and in cooperation with national supervisors. In 2026, SEOs will be subject to EU-level regulation, and on-site inspections will be a common occurrence since the supervision is carried out by a joint team leader that will be based in a specific Member State where a selected entity has its headquarters. For direct monitoring, AMLA would have the authority to impose legal obligations and administrative penalties (Remeur C., 2023).

On the other hand, for non-selected obliged entities, the primary level of AML and CFT would remain at the national level, leaving the responsibility of overviewing the entities by national supervisors. However, AMLA would assist and coordinate national supervisors in becoming more successful in upholding the Single Rulebook and assuring consistent and more effective risk assessments procedures (Remeur C., 2023).

Also, AMLA would conduct independent assessments of non-financial supervisors and investigate potential violations or incorrect applications of EU law by non-financial supervisors, such as public authorities managing self-monitoring bodies, in order to improve surveillance procedures and implement AML/CFT measures with greater efficiency in the non-financial sector. Additionally, the AMLA would have the authority to grant permission to financial and non-financial supervisors to use their authority to regulate and provide them instructions on how to do so for indirect supervision (Remeur C., 2023).

Furthermore, in addition to indirect and direct supervision the AMLA is in charge of various tasks that involve the development and updating of the AML/CFT database, which is currently controlled by the European Banking Authority (EBA), to evaluate the risk and challenges in connection to the selected obliged entities, and would carry out periodic reviews to ensure that national supervisors have the resources to do their job in the best manner (Remeur C., 2023).

In addition, the AMLA would be responsible for establishing a supervisory system focused on a risk-based approach. It would coordinate peer reviews of the procedures and standards of supervisory authorities outside the financial sector, such as self-regulatory organizations, and would seek to investigate violations of rules applicable to obligated entities. Sanctions and other possible solutions will also be considered. AMLA will work with financial intelligence agencies to conduct joint investigations of cross-border cases and provide services, information technology and artificial intelligence tools for secure information exchange, including hosting the fiu.net website (Remeur C., 2023).

Moreover, AMLA's governance structure will consist of a General Council and an Executive Council. The General Council, composed of representatives from all EU Member States, will be responsible for governance and decision-making in two different configurations: one composed of the heads of government authorities responsible for AML/CFT oversight and the other composed of the heads of the Member States' FIUs. The Board of Directors, composed of the President of the Authority and five full-time independent members appointed by the General Council, will be responsible for making all decisions regarding Obligated Entities or individual supervisors (European Commission, 2021).

In order to avoid conflicts of competence between EU authorities, adjustments are foreseen in the three regulations establishing the ESAs (European Supervisory Authorities). The AMLA will cooperate with the ESAs and may participate in their meetings as a permanent non-voting member. The President will represent the Authority and chair the general meetings of the Board, while the Executive Director will be responsible for the day-to-day management and administrative responsibility for budget execution, resources, personnel, and procurement. Finally, the Management Board will be responsible for examining appeals against binding decisions of the Authority in the statutory areas under its direct control and its decisions will be subject to review by the Court of Justice of the European Union (European Commission, 2021).

It is important to recognize that the effectiveness of anti-money laundering legislation varies depending on the resources and practices of each EU member state, as anti-money laundering legislation is based on a national framework. According to a report by the European Banking Authority, the competent authorities have made progress in monitoring money laundering and terrorist financing, but not all are able to cooperate effectively with national and international actors. There are differences in the methods used to define and implement a risk-based approach to supervision, and some risks affect the entire EU financial system, not just one country (European Banking Authority, 2022). Member States agree on the need for a common and consistent methodology for assessing and identifying risks, as indicated in the public consultation on the Action Plan adopted on May 7, 2020. The EBA also notes that some national AML/CFT supervisory authorities may not be using the full range of powers available to them, resulting in insufficient supervision at the national level and inadequate supervision of cross-border financial service providers, which may pose risks to the domestic market as a whole. A recent report by the European Court of Auditors confirms these findings[37]. As a result, the establishment of the AMLA is essential to

[37] ECA special report 'EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficient':
https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_EN.pdf

address the shortcomings of AML and CFT in the European Union, and to ensure the effectiveness of supervision and practices of all Member States (European Commission, 2021).

4.2. Legal framework of cryptocurrencies in AML and CFT

As previously mentioned, there is a growing concern in the European Union, about the role and risks of cryptocurrencies in terrorism financing and money laundering. Hence, in recent years there have been multiple advancements in the EU legal framework to extend the scope of the already existing Anti-Money Laundering Directives to include definitions of digital assets and include cryptocurrencies as a potentially means of terrorism financing and money laundering.

Just recently, in April of 2023, the European Parliament approved the MiCA, to improve standards that regulate AML/CFT in the EU and include cryptocurrencies and its main actors under the scope of the regulation. Moreover, the EU has implemented the 6th AMLD, which included the EU Single Rulebook, and a proposal for the creation of the AMLA.

Moreover, the EU legal framework has been influenced by the FATF recommendations, specifically the FATF Travel Rule, which expands the list of obliged entities that should comply with the European Union legislations in AML/CFT.

4.2.1.MiCa: set standards for crypto regulation globally

MiCA, or Markets in Crypto assets Regulation, is the new European regulation supervising the issue and delivery of services for stablecoins and digital assets. MiCA, which the European Parliament approved on April 20, 2023, is a pioneering piece of

legislation that sets the standard for other countries. The regulation will go into effect somewhere between the middle of 2024 and the beginning of 2025 (Yianni, 2023).

MiCA is meant to deliver a uniform regulatory framework that supports investor protection, market integrity, and financial stability. The rule imposes strict regulations to prevent fraud and other financial crimes, as well as licensing requirements, operating standards, and transparency requirements for issuers of digital assets. In conjunction with the Anti-Money Laundering regulations, MiCA aims to remodel the crypto industry in the European Union, imposing rules on issuers, crypto service providers and investors (Yianni, 2023). As a matter of fact, a member of BBVA's Digital Regulation team has stated that: "MiCA is a pioneering legislative text in terms of regulating crypto markets. It undoubtedly places the European Union as a global pacesetter." (BBVA, 2023).

MiCA was created to provide a regulatory framework for cryptocurrencies that use decentralized ledger technology (DLT). The regulation clarifies which kinds of digital assets are covered under its authority and introduces a more detailed definition to distinguish between crypto-assets[38], Asset Referenced Token[39] (ART), E-money token (EMT), and Utility token[40].

Although the inclusion of the assets mentioned above represents a big step forward, MiCA failed to include other Cryptoassets, such as assets in the DeFi industry and non-fungible tokens (NFT). The reason for leaving out of the scope of the regulation's

[38] "A digital representation of value or rights which may be transferred and stored electronically, using Decentralized Ledger Technology (DLT) or similar technology." (BBVA, 2023).
[39] "A type of crypto-asset which is meant to maintain a stable value by referring to the value of several currencies that are legal tender (FIAT currencies), one or several commodities, or one or several crypto-assets, or a combination of such assets" (Ibidem, 2023).
[40] A type of crypto asset which "provides digital access to a good or service available on DLT and is only accepted by the issuer of that token." They do not fall into the category of financial instruments under security legislation of the majority of countries (Ibidem, 2023).

assets such as NFT, and DeFi derives from the fact that they have very specific features and variables, so creating a regulatory framework would need a deep analysis of the risks that those pose, raising many new challenges for financial stability in the European Union. However, MiCA leads the way to minimizing the risks surrounding cryptocurrency and towards a stronger consumer protection (BBVA, 2023).

For the purpose of this research, we will focus on the area of the legislation that covers illicit flows in Crypto Assets, and how these regulations will limit the use of cryptocurrencies from criminals and terrorists. For instance, Ernest Urtasun, a rapporteur for the Economic and Monetary Affairs Committee on crypto-assets transfers stated that: “Currently illicit flows in crypto-assets are moved swiftly across the world, with a high chance of never being detected. The Recast of the TFR (Transfer Funds Regulation) will oblige crypto-asset service providers to detect and stop criminal crypto flows and also ensure that all categories of crypto companies are subject to the full set of anti-money laundering obligations. This will close a major loophole in our AML framework and implement in the EU the most ambitious travel rule legislation in the world so far, in full compliance with international standards.” (European Parliament, 2023).

The articles that concern the misuse of cryptocurrencies for terrorist financing included in the “Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA) are: Article 16.2.ea (application for authorization); Article 16.3.a; Article 19.2.c; Article 56.1.ea; Article 56.2.a; Article 61.7; Article 82.4.b (Powers of competent authorities); Article 83.2.a (refusal of cooperation)” (Council of the European Union, 2022).

The purpose of these articles is to regulate the use of cryptocurrencies by cryptoasset service providers and token issuers in connection with assets in order to

prevent money laundering and terrorist financing. To this end, the laws require these providers to have effective systems, procedures, and mechanisms in place to detect and prevent these criminal activities. In addition, issuers must demonstrate that their management team has no criminal record in the relevant areas of law.

Moreover, the competent authorities have the power to refuse or revoke authorization if the issuer's business model poses a serious threat to financial stability, payment systems or market integrity, or if there is a risk of money laundering and terrorist financing. In addition, the competent authorities are empowered to cooperate with other authorities, including those responsible for the prevention of money laundering and terrorist financing. However, competent authorities may refuse to cooperate if the disclosure of relevant information could endanger national security, in particular the fight against terrorism and other serious crimes. These articles establish a legal framework to ensure the safe use of cryptocurrencies and prevent the misuse of these digital assets for criminal activities.

4.2.2. EU single rulebook

As previously mentioned, the EU single rulebook is a fundamental mechanism included in the proposal for the establishment of the AMLA, to combat the financing of terrorism and money laundering. Apart from the AMLA, the EU single rulebook is a central element in the proposal, since it replaces some rules of the AMLD, such as regulations regarding the obliged entities, openness of information regarding individual owning or managing the clients of such businesses. Also, it addresses the exploitation of anonymous instruments, hence cryptocurrencies. Additionally, the EU single rulebook, in accordance with the FATF Recommendations, aims at extending the list of selected obliged entities to include all crypto-asset service providers and harmonize beneficial ownership requirements across the EU. Most importantly, it will limit transactions that surpass €10,000, both in receiving and sending processes. Lastly, it

included the objective of coordinating European policies towards third world countries to decrease the gaps in their AML/CFT regimes (Bąkowski P.,2023).

4.2.3. Anti-Money Laundering Directives

The purpose of the EU Money Laundering Directive is to prevent money laundering and terrorist financing and to establish a harmonized legal and regulatory framework in the EU. This is achieved by addressing the money laundering and terrorist financing crisis and eliminating inconsistencies in compliance with money laundering laws. The EU Money Laundering Directive has been regularly adopted by the European Parliament since 1990, and each member state has a set deadline to implement it into national law. The most important Anti-Money Laundering Directives include: AMLD1, 1991: to criminalize money laundering; AMLD2, 2001: wider range of criminal activities and introduced customer due diligence (CDD) for financial institutions; AMLD3, 2005: stricter record keeping requirements, establish national AML supervisory authorities, introduce risk-based approaches to AML; AMLD4[41], 2015: introduce risk-based approach to AML and CDD, required member states to establish beneficial ownership registers, and extended the scope of the directive to include virtual currencies; AMLD5, 2018: introduced new requirements for identification and verification of beneficial owners, and required member states to establish central registers of beneficial ownership information.

The latest EU AML Directive is the 6th AMLD, released on the 3rd of December 2020, and was transposed into domestic legislation across all member states by the 3d of June 2021. The 6th EU AML Directive replaces the previous fourth and fifth directive.

[41] Directive (EU) 2015/849 (4th Anti-Money Laundering Directive, 4AMLD) “aims to combat money laundering* and the financing of terrorism* by preventing the financial market from being misused for these purposes. It seeks to extend and replaces the previous Directive (EC) 2005/60 (3rd Anti-Money Laundering Directive, 3AMLD) that entered into force in 2007”. (EUR-Lex - 230804_1 - EN - EUR-Lex, 2021)

Every directive adds to or updates regulatory obligations on member state governments. Each directive enhances the previous one and provides further guidance on any existing or new risk involving money laundering and terrorist financing. The 6th AMLD focuses on four key areas: the expansion of regulatory scope; improved harmonization; cooperation among member states; and stricter criminal penalties (European Commission, 2021).

Respectively, the expansion of regulatory scope, refers to the fact that the 6th AMLD gives more clarity to the definition of money laundering and ensures there is more consistency across the EU member states at the time of interpreting what money laundering means as a crime. Whereas under the previous rules only individuals and organizations that directly benefited from money laundering were prosecuted, under the new directive anyone who facilitates financial crime will be held responsible. Therefore, all those who facilitate money laundering, or the financing of terrorism are guilty of the same offense. The directive will also apply to anyone caught attempting to launder money, whether or not the attempt is successful (European Commission, 2021).

Second, as part of the harmonization improvements, the sixth AMLD includes a list of 22 offenses that are legally viewed as money laundering. This extensive list includes human trafficking, tax offenses, cybercrime and terrorist financing. It should be noted that this is the first time that cybercrime is included in the scope of the AML Directive (European Commission, 2021).

Third, the Sixth AML Directive promotes cooperation between Member States in combating money laundering crimes. For example, when money laundering takes place across the borders of two countries, both Member States will need to cooperate in identifying, prosecuting, and convicting the offenders involved in the illegal activity. This

will decentralize justice and ensure that the same penalties are imposed throughout the EU (European Commission, 2021).

Fourth, money laundering can be a dual crime, the principle that a crime is committed in one jurisdiction and then its financial resources are laundered in another jurisdiction. In addition, the minimum custodial sentence for persons convicted of money laundering offenses was increased from one to four years in order to increase consistency of sentences across member states, although many EU member states have set much higher maximum sentences than those provided for in the Directive (European Commission, 2021).

4.2.4. FATF Travel Rule

An important legislation to consider in the fight against money laundering and terrorism financing is the FATF Travel Rule, which is part of the AMLD new proposal, and it is incorporated in the MiCA. The FATF Travel Rule represents a significant step in the fight against AML/CFT because it expands the scope of entities that are obliged to comply with the AML framework: such as financial institutions engaged in the exchange of virtual currencies, and Virtual Asset Service Providers (VASP)[42]. Additionally, depending on certain conditions, the FATF Travel Rule also includes decentralized services and P2P platforms (Sav D., 2023). However, regulations on VASP may be different depending on the jurisdiction, although between member states there is an increasing effort for standardizing definitions and rules surrounding these types of entities.

[42] A service is considered VASP if it provides: Exchange of virtual assets and fiat currencies; exchange of one or more forms of virtual assets; transfer of virtual assets; custody and/or management of virtual assets or assets that allow control of virtual assets; participation in and provision of financial services to an issuer in connection with the offering and/or sale of virtual assets. (Sav, D. 2023)

In addition, the FATF Travel Rule is considered key in the fight against money laundering and terrorist financing as they require VASPs to store and disclose information about the senders and recipients of virtual asset transfers. The name of the rule comes from the fact that when a transaction takes place, the personal data of the parties involved moves with it. This allows financial institutions and virtual payment service providers to conduct sanction checks and identify suspicious transactions so that appropriate action can be taken.

As a result, requiring financial institutions and VASP to share more information[43] about the sender and recipient of transactions, the possibility of being successful in targeting anonymity of crypto transactions could lower, and thus prevent money laundering and terrorism financing through virtual assets (Sav D., 2023).

4.3. Regulations towards key players in crypto market

In the above paragraphs we have analyzed the key players in the crypto market, and identified the ones that are included in the list of obliged entities in the AMLD package (4th, 5th, 6th directives), which are custodian wallet providers and virtual currency exchanges. When speaking about terrorism financing and money laundering, including only those two entities could result in a lack of control over other players that are present and very much active in the crypto market. The key players are: users, miners, cryptocurrency exchanges, trading platforms, wallet providers, coin inventors, and coin offerors. Various of these players are included in the Anti Money Laundering Directives, but others are still being left out. Users are not obliged entities under AMLD 4-5-6, due to the fact that the legal framework of the AMLD focuses more on intermediaries. However, this could represent a risk in the fight against terrorism financing in the long

[43] VASP must collect: Sender's name; Sender's account number (e.g., wallet address) used to process the transaction.; Sender's physical (geographic) address, national identification number, customer identification number (not transaction number) or place and date of birth used to uniquely identify the sender to the originating authority; the name of the recipient; beneficiary account number of the account used to process the transaction (e.g., a wallet address) (Sav D., 2023).

term (Snyers, A., et al., 2018). Also, not considered obliged entities are the Miners, for two main reasons. Firstly, they are technical service providers rather than intermediaries between the crypto market and the physical one. Secondly, the majority of miners are located in China, meaning that enforcing any type of legislation would be almost impossible. Also, it is important to note that miners could be cryptocurrency users or might be individuals that create a business out of mining cryptocurrencies, and then becoming coin offerors, which will be analyzed further below (Sav D., 2023).

Consequently, it might be possible that criminals would start a mining business as well. In fact, not including miners as obliged entities can be considered a risk due to the fact that it is an attractive activity for criminals or terrorists. With the development of technology in remote areas from where terrorists usually operate, the possibility of terrorist groups to start a mining business and then convert cryptocurrencies into FIAT money is a real and present risk. Underestimating miners as a possible actor to include under the scope of AML Directives, or in the MiCA, leaves a blind spot in the European Union's fight against money laundering and terrorist financing (Snyers, A., et al., 2018).

As previously explained in this work, cryptocurrency exchanges are one of the most important players in the crypto market, as they allow users to buy and sell cryptocurrencies with FIAT money and vice versa. Because of the nature of cryptocurrency exchanges they are considered obliged entities under the scope of the Anti Money Laundering Directives. However, pure cryptocurrency exchanges do not fall into the scope of the legislation because they only accept payments with cryptocurrencies, so they do not deal with FIAT currency. Leaving these cryptocurrency exchanges out of the scope of AMLD creates opportunities for terrorists to finance their activities while adding an extra layer of anonymity, and disguising the origin of the cryptocurrencies (Snyers, A., et al., 2018).

Another exchange that creates opportunities for terrorist financing is the atomic swap[44], which does not need a third-party intermediary. The lack of a middleman makes it significantly hard to include this exchange under the scope of AMLD, thus leaving a blind spot in the fight against money laundering and terrorist financing (Snyers, A., et al., 2018).

Other important players are trading platforms, which allow users to interact directly when buying and selling cryptocurrencies. They are referred to as “P2P exchanges” or “decentralized exchanges”, and they are not the same as cryptocurrency exchanges. Trading platforms are controlled by softwares, meaning that there is no central authority operating them, hence it is very hard to regulate them and include them in the list of obliged entities. Similarly, to the pure cryptocurrency exchanges, excluding trading platforms from the scope of AMLD leaves a blind spot in the fight against money laundering and terrorist financing (Snyers, A., et al., 2018).

As already explained previously in paragraph 3.4, there are three main types of wallet providers, respectively: hardware wallet providers, software wallet providers and custodian wallet providers. Between all of them, only custodian wallet providers, defined as organizations that offer services to protect secret cryptographic keys on behalf of their clients, are obliged entities under the package of AMLD. On the other hand, hardware wallet providers and software wallet providers do not keep the cryptographic keys on behalf of their customers, but just provide some services that help the customer protect their cryptographic keys. As a result, individuals using software or hardware wallet providers can get away from Anti Money Laundering regulations, as long as they do not engage in cryptocurrency exchanges to convert their crypto into FIAT money. Consequently, this can be considered another deficiency in the fight against money laundering and terrorist financing (Snyers, A., et al., 2018).

[44] An atomic swap is a cryptocurrency exchange between two parties that wish to exchange tokens from different blockchains (Frankenfield, 2022a)

It goes without saying that coin inventors are also identified as key players as they create and set the rules for the cryptocurrency in question. Usually, the identity of the coin inventor is unknown, which makes it harder for policy makers to establish a target when creating a legislation. However, the European Union policy makers do not consider them a priority to be listed as an obliged entity. Although, if a terrorist organization would acquire the skills to invent a coin, it could start posing various risks to the stability of the crypto market (Snyers, A., et al., 2018).

Lastly, coin offerors are not obliged entities under Anti Money Laundering Directives. As previously explained, coin offerors are entities or individuals that offer coins to cryptocurrency users, when a cryptocurrency is released. Once more this creates a loophole in the fight against money laundering and terrorist financing (Snyers, A., et al., 2018).

5. CURRENT LIMITATIONS OF THE EUROPEAN REGULATORY FRAMEWORKS ON AML/CFT AND CRYPTOCURRENCIES

The European Union has made great efforts and advancements in the field of the fight against money laundering and terrorism financing, with the introduction of MiCA, the Single Rule Book and the 6th AMLD. However, the environment of cryptocurrencies, terrorism financing, and money laundering is so vast, that there are loopholes and challenges in the practical application of the directives. Among the main issues are: member states divergences on AML/CFT, and the dilemma of anonymity that characterizes some cryptocurrencies and technologies, which challenge the effectiveness of law enforcement in AML/CFT.

5.1.1. Member States Divergences on AML/CFT Framework

The current regulatory frameworks of the European Union on AML/CFT and cryptocurrencies, presentes various flaws that could cause the decrease in effectiveness of the EU legislations in this matter. The divergences between Member States' legal frameworks and the cross-border challenges are among the main issues, which require better harmonization and better applicability of the AMLD frameworks.

The European Anti-Money Laundering Directives are set out as standards that Member States should follow and comply with, however they do not impose on countries how they should achieve these standards. Basically, the responsibility to implement the directives in the national legislations falls onto each Member State. However, in cases related to AML and CFT, this more "free" type of implementation creates a lack of harmonization and opportunities for criminals to exploit the financial system. For instance, based on Canestri[45] there are various areas where it is possible to identify a lack of harmonization between Member States, such as:

1. *Asset seizure methods*: some countries confiscate assets without needing to have a previous conviction related to the individual, others instead sequester assets only if there is a criminal conviction already put in place.
2. *Tools and mechanisms for enforcement*: some Member States have access to more resources than others to pursue a criminal investigation of AML/CFT, either in the EU or abroad, which leads to an incoherent effort between Member States.
3. *Different definitions on what is money laundering*: the difference in interpretation of what is money laundering between Member States represent a significant limitation. Although FATF recommendations defined what type of offenses are considered money laundering, not every country has implemented those into

[45] Canestri, D. (2015). Fourth EU AML Directive: What is Missing? Section 319 PATRIOT Act and the New EU AML Directive. European Journal of Crime, Criminal Law and Criminal Justice, 23(3), pp. 214–240.

domestic legislations. As a result, a transaction could be allowed in one Member State, but be considered an illicit activity in another.

4. *Different application of sanctions:* each Member State has substantial differences in how they sanction money laundering and terrorism financing crimes. The variety of definitions on these types of crimes offer criminal opportunities to exploit the system of some Member States to their advantage (Unger et al., 2014).

Furthermore, it is worth noting that contrary to regulations (directly applicable), directives take much longer time to be implemented into the political processes of each Member State. For example, based on a study made by Edward Elgar (2014) on The Economic and Legal Effectiveness of Anti-Money Laundering Policy[46], there have been significant delays in the implementation of AML/CFT policies in Europe. As an example, France was three years late in implementing the Third AMLD, similarly, Ireland, Spain, and Belgium, exceeded the deadline by more than two years. Also, for the Fourth AMLD, countries such as Romania, Spain, Netherlands, and Greece had an average of 15 months delay in implementing the directive. As a justification to their delays Member States have declared that the main difficulties in implementing the directives were: legal, social, political, long parliamentary procedures, limits of internal supervision, and others (Unger et al., 2014).

Consequently, the biggest limitations and weaknesses of the AMLD frameworks lies in the lack of direct applicability and harmonization between Member States, which makes the fight against money laundering and terrorism financing much harder to tackle. And also, the lack of the European Union lacks extraterritorial powers, which could be a significant consideration to apply to AMLD to better target the financing of

[46] Unger, B., Ferwerda, J., van den Broek, M., Deleanu, I. (2014) The Economic and Legal Effectiveness of Anti-Money Laundering Policy, Edward Elgar 2014 and L. Rossel, B. Unger, J. Batchelor, F. Vallejo AML Tools http://coffers.eu/.

terrorism through cryptocurrencies. However, this could have made the process of AMLD approvals more difficult to achieve (Unger et al., 2014).

5.1.2. Regulatory Dilemma of Cryptocurrency's Anonymity

Furthermore, one of the most important limitations of the European Union framework on AML/CFT is the difficulty of targeting the anonymity of cryptocurrencies. Although MiCA and the 6th AMLD have extended their scope on what and who is considered an obliged entity, they still did not manage to cover all of the potential categories that could still pose a risk to the financial system. For instance, not all of the activities of DeFi is included under any type of legislation due to its lack of central entity nature. The technology has such unique characteristics, mainly the lack of a central intermediary/entity, that lawmakers need to conduct further research to develop a regulatory framework that adequately addresses the existing issues, specifically anonymity. As a result, without an intermediary, or someone to be identified, it is significantly challenging to understand to whom the regulations should apply (Born A., 2022).

Moreover, cryptocurrencies such as Monero, DCash, and ZCash present features that make it almost impossible to unveil the anonymity of the user that would exchange them. The problem generates, because when dealing with those cryptocurrencies, every time there is the need to make a transaction, especially Monero, a new stealth address[47] is being created, and then the money is sent to the wallet. As a result, the address of the wallets of both the sender, and the recipient, remains anonymous and protects their identities very well. Since there is no wallet address to identify, managing to unveil who is behind the transactions is almost impossible, making the characteristic

[47] A wallet address that is cryptographically tied to the recipient's public address, but that is only revealed to the parties transacting (Marcobello M., 2023)

of Anonymity one of the biggest challenges tha cryptocurrencies pose in the fight against terrorism financing and money laundering (Daniels N., 2023).

As it is possible to see in the following cases, in some occasions anonymity can be revealed, however cryptocurrencies have still been attractive for terrorist groups to finance their activities, and without great cooperation between FIU and countries, this limits should be crucial to address to have a more efficient legal framework surrounding AML/CFT and cryptocurrencies.

6. OVERVIEW OF THE CURRENT STATE OF MONEY LAUNDERING AND TERRORIST FINANCING THROUGH CRYPTOCURRENCIES

The use of cryptocurrencies for terrorist financing has been a debated topic in recent years. Since their inception, terrorist groups have been adapting to the new ideological and financial system, so the question of shifting from traditional means of financing towards cryptocurrencies has been a real risk for law enforcement agencies and governments. The level of anonymity and speedy transactions that cryptocurrencies offer, could be very appealing to terrorist organizations. As a matter of fact, it has been challenging to identify in how many instances terrorist groups have adopted cryptocurrencies, both in Europe and internationally, due to various limits that the technology presents, such as anonymity (the capacity of hiding the identity of the user), usability (the simplicity with which a user may deal and control their own money), security (level of security of cryptocurrencies infrastructures), acceptance (level of acceptance by user community), reliability (how users refer to the speed and availability of transactions), and volume (cumulative transaction volume over time in the cryptocurrency ecosystem). For this reason, it is indispensable to acknowledge the type of activities terrorists would use cryptocurrencies for, to better tackle the risks.

According to a RAND (Research and Development) report on *terrorist use of cryptocurrencies,* there are five main activities of terrorist organizations' finance activities: fundraising, illegal drug and arms trafficking, remittance and transfer of funds, attack funding and operational funding (Dion-Schwarz et al., 2019).

For this reason, in this section, we will look into the potential reasons of why they would need to use cryptocurrencies, and if the current cryptocurrencies regime would allow these groups to illegally finance their activities. However, first it is worth mentioning for what purpose terrorist organizations usually use FIAT money.

6.1.Terrorist use of money

Firstly, in order to understand why terrorist organizations would consider shifting to cryptocurrencies to finance their activities, it is necessary to consider how terrorist groups use money and identify any severe financial limitations that might require the employment of other techniques, like digital currencies (for instance, due to pressure from law enforcement). According to the RAND report, there are three main activities for which terrorists use money: receipt, management, and spending (Dion-Schwarz et al., 2019).

In the first place, terrorist groups' main objective is to accumulate and receive money through a variety of sources, including state sponsors, illegal activities such as drug trafficking and extortion, and donations from sympathizers. According to the Financial Action Task Force (FATF), cash remains the primary method of financing for terrorist groups. However, the use of cryptocurrencies could potentially make it easier for terrorist groups to receive and move funds without detection. For instance, due to the increase of AML and CFT regulations terrorist groups supporters do not donate nor support as much as they did in the past, so it is possible that if a cryptocurrency offers a terrorist organization enough security, and less risk of being caught, it could re-enable

donations as a significant source of terrorist financing. Supporters might, for instance, give their own cryptocurrency or send it through intermediaries (Dion-Schwarz et al., 2019).

Once the money is received by the terrorist group, they must manage it. In the case of the money not being yet under direct control of the group or if it is difficult to transfer it because of security reasons, terrorists will usually proceed to launder money or to use other transfer mechanisms. Terrorist groups often use a variety of methods to manage and transfer their money, including using informal money transfer systems known as hawalas, smuggling cash across borders, and using money service businesses to conceal their activities. Generally, this aspect is more crucial for terrorist organizations that rely on external financial sources and less crucial for groups like ISIS that are primarily territorial (Dion-Schwarz et al., 2019).

Furthermore, due to the increased effort of AML frameworks it is significantly harder for terrorist organizations to rely on traditional banking systems, meaning that they could shift to cryptocurrencies to move funds without detection. However, the issue with utilizing cryptocurrencies for moving and transferring funds is that large transactions of money in the form of virtual currencies could be detected by authorities due to the factor of transaction volume, and the FATF Travel Rule standards[48] (Dion-Schwarz et al., 2019).

[48]Taking as an example Bitcoin, its daily volume of transactions corresponds to $1 billion, and most of the transactions occur in specific countries and are done between known parties. Therefore, if a large movement of Bitcoin would be put forward, it would be most likely detected. However, if funds are moved in smaller amounts incrementally, it would be plausible to be successful. Also, if the terrorist organization would find a cryptocurrency that best fits all the criteria to achieve a successful movement of funds, it will be more likely that cryptocurrencies will be used as a method of terrorism financing. However, it is necessary to note that large terrorist organizations rely on robust and secure financial infrastructures, and cryptocurrencies do not represent the most robust option, especially if there is a lack of technological expertise within the group (Dion-Schwarz et al., 2019).

Moreover, once the terrorist organization seizes the money, it aims to spend it on "operating expenses" or "violence-producing expenses." Both operations are generally funded through the same mechanism. Depending on their needs and goals, different terrorist organizations will allocate their funds differently, and depending on the decisions made, operations to detect and disrupt the activities of these organizations will have different results. Because of the lack of knowledge and close ties between these activities, and especially because legal activities provide incentives and disincentives for illegal acts, it is difficult to distinguish between clearly legal costs such as salaries and services and clearly illegal costs such as terrorist recruitment and training . For example, the category of operating expenditures includes: salaries, propaganda activities, and recruitment, which indirectly contribute to the terrorist group's ability to produce violence, and so terrorist finance operations also focus on these types of activities (Dion-Schwarz et al., 2019).

In this case, cryptocurrencies could serve as an attractive alternative to escape CFT regulations and control. However, due to the limited acceptability of cryptocurrencies in areas where usually terrorists operate, it could be hard to "cash out" [49]. Only a few Bitcoin ATMs exist in the Middle East, so it can be difficult to exchange Bitcoin for FIAT currencies. However, there are many other types of cryptocurrencies that could be used by the organization and, if managed to be converted into FIAT currencies, cryptocurrencies can serve as a useful means to finance terrorist activities (Dion-Schwarz et al., 2019). Due to the wide acceptance of FIAT currencies, terrorist groups could potentially use cryptocurrencies to transfer funds to different parts of the world, and then convert them into FIAT currencies to finance their activities. This would make it harder for law enforcement agencies to track the movement of funds and detect illicit activities.

[49] Cashing out means selling crypto coins or tokens in exchange for fiat money and then withdrawing the money to a bank account (Kriptomat, 2023).

Also, it is important to add that terrorist groups like Al Qaeda, similarly to ISIS, have independent cells that operate overseas, and aid the group to possibly organize attacks in different parts of the world. As a result, access to cryptocurrencies and the possibility to convert them to traditional money could increase, as well as the risk of its illicit use for terrorism financing (Dion-Schwarz et al., 2019).

6.2. Possible use of cryptocurrencies in money laundering and terrorism financing

The question of whether terrorist groups would use cryptocurrencies as a form to finance their terrorist activities depends on the type of activities they would need to finance. Based on the RAND report used above, five categories of terrorist organizations finance have been identified: fundraising, illegal drug/arms trafficking, transfer, attack funding, and operational funding. Using the limitations of cryptocurrencies mentioned above (anonymity, usability, security, acceptance, reliability, and volume) each activity for financing terrorist groups will be analyzed to understand if terrorist organizations can find opportunities and advantages in using cryptocurrencies as a source of funding terrorist activities (Dion-Schwarz et al., 2019).

Firstly, fundraising is a crucial component in terrorism financing to support all types of activities, such as purchasing weapons, salaries, financing attacks, and other daily activities. Fundraising can come from various sources, even form nation-states and individual donors, and charities. For instance, ISIS, defined as one of the world's best-funded terrorist groups by U.S. officials, relies on different types of sources. Foreign terrorist fighters that gather money for travel, travel with finances, or get funding from outside supporters as well as rich, private, regional benefactors have all contributed to the organization.

Also, terrorist groups started to recognize the importance of social media and crowdfunding to create new mechanisms for soliciting funds. For example, a user

created a Facebook account that published food recipes, to support a fighter in Syria. Through this account the user was asking money for cooking utensils and gave a German bank account details to receive the funds. This shows how easy it can be to use the internet to support terrorist-activities, without anyone suspecting it. Another similar method is crowdfunding. Groups like Al-Qaeda have made effective use of crowdfunding to collect donations and expand their networks. Usually, the real objective of a crowdfunding is hidden, so that the individual contributing to the terrorist organizations, thinks that he or she is actually helping a real charity or humanitarian activity (Goldman et al., 2017).

Both fundraising and crowdfunding can be achieved through cryptocurrencies. In this case anonymity provides donors and recipients a level of security from being caught by authorities. According to Yaya Fanusie of the Foundation for Defense of Democracies, jihadists are innovating their financing techniques by soliciting cryptocurrencies to raise funds. For instance, in 2016 the online media unit of the Mujahideen Shura Council in the Environs of Jerusalem (MSC), known as the Ibn Taymiyyah Media Center (ITMC), created an online campaign to receive funds[50]. The MSC has been recognized as a foreign terrorist organization by the US State Department for targeting Israel and giving support to the Islamic State[51]. The online campaign was called “Jahezona” translated to “equip us” in Arabic, in which details on how to transfer Bitcoins were posted. When the campaign was discovered, only a little amount of Bitcoin had been received (0.929 BTC), amounting to $540. But as of March 2018, the associated Bitcoin address had received about 1.46 Bitcoin, which, due to the sharp increase in Bitcoin's price, amounted to roughly $8,000.[52] (Goldman et al., 2017).

[50] Fanusie, Yaya, ‘The New Frontier in Terrorist Financing,’ The Cipher Brief, 24 August 2016, https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin.
[51] US Department of State, ‘Terrorist Designation of the Mujahidin Shura Council in the Environs of Jerusalem (MSC),’US Department of State website, Terrorism Designations Press Releases 19 August 2014, https://www.state.gov/j/ct/rls/other/des/266549.htm.
[52] According to a Bitcoin blockchain analysis, the Jahezona account is linked to 14 other Bitcoin addresses that, as of March 2018, have collectively received about 10.4 Bitcoin (or about USD 80,000). The motivation of these connected transfers is unknown, but given their proximity to one another, it

Additionally, drugs and arms trafficking is one of the biggest income sources for terrorist organizations. When engaging in both activities achieving a level of anonymity and high security is essential. In this context usability is less important than the other components, because only a few individuals will be engaged in the transaction. As a result, widespread acceptance is also not too necessary if only a couple of people are participating in the transaction process.

However, reliability is important when, for instance, two partners that are exchanging either drugs or arms do not trust each other, so having a reliable exchanging infrastructure can be useful and make the transaction more efficient. Finally, volume in this case has less importance, because actors engaging in arms and drugs transactions might be smart enough to hide large transactions in a chain of smaller ones (Dion-Schwarz et al., 2019).

In recent years there have been some cases of cyber criminals trying to exploit the “dark web” markets, to buy and sell drugs and weapons with cryptocurrencies. In this context, the criminal does not need to convert cryptocurrencies into FIAT currencies, because he or she can simply re-use them for future transactions. For instance, the cryptocurrency Monero has been called the “drug dealer’s cryptocurrency of choice” because of the level of anonymity that it offers (Greenberg A., 2017). In 2016, the dark web market started to accept Monero as an alternative to Bitcoin, due to its capability of hiding big amounts of transactions and the identity of the users. As of 2017, Monero's adoption in online criminal markets increased its value by 27 times (Greenberg A., 2017).

---

appears that they are being managed by the same organization as the Jahezona campaign. The blockchain intelligence company Elliptic gave the study's authors access to this data.

Moreover, it is important to highlight the creation of software such as *Dark Wallets,* that allow users to improve the anonymity of Bitcoin and other cryptocurrencies, so that the transactions are obfuscated, and it is almost impossible to identify the user details behind a transaction. As a matter of fact, Monero has many features of Dark Wallet built into its infrastructure (Frankenfield J., 2021).

Similarly, to fundraising, transfer activities require a good level of anonymity and a high level of security, to avoid being detected by authorities. Security is one of the most important components when transferring funds, due to the presumably big amounts of money being moved and the possibility of someone detecting it or stealing it. On the other hand, usability and wide acceptance are less important factors when using cryptocurrencies due to the small amount of people needed for the transaction to take place. However, the components of volume and reliability should be considered necessary when moving funds, because being able to assure the transfer of large sums is the most important requirement for terrorist organizations (Dion-Schwarz et al., 2019).

As a matter of fact, there is a growing concern in the use of cryptocurrencies to transfer funds for trade in child sexual abuse, ransomware payments and fraudulent trading schemes. Child sexual abuse is an increasing threat and although there is not a lot of evidence of transferring money through cryptocurrencies for this cause, it still poses a high threat for the possible consequences of the activity. Also, dedicated marketplaces and dark web forums are the main means of dealing with this type of activity, allowing transactions to happen solely by cryptocurrencies (EUROPOL,2021).

Another issue is the evolution of ransomware[53] payments, which has been closely connected to the increase in price of BTC and other cryptocurrencies. A growing number of incidents also involve the theft and storage of data used to blackmail the

[53] The use of malware to encrypt computer systems or data, followed by a demand for payment in return for the decryption key, is known as ransomware (Custer et al., 2020).

victims; a practice known as double-extortion. Bitcoin is the most common cryptocurrency used for ransomware payments (Custer et al., 2020). The victim is typically required to pay a Bitcoin ransom to get their system unlocked. When a financial institution complies with this request, FIAT money is withdrawn in order to buy the desired cryptocurrency. The money is subsequently sent to the wallet address that the criminal actor gave. For instance, in 2017 the hackers who created the Wannacry ransomware[54] began taking money out of the three Bitcoin wallets linked to their criminal activity. Then, to convert Bitcoins into Monero and prevent traceability, they sent the money to the exchange Shapeshift.io (open-source platform)[55] (EUROPOL,2021).

Lastly, fraudulent trading schemes have also created a new opportunity for criminal actors to transfer and move their funds or collect them. Fraudsters set up websites dedicated to cryptocurrency investments or promote profitable investments, luring customers to register on trading websites. For instance, a criminal organization created several trading websites that promoted high profits from investments in cryptocurrencies[56]. Through advertisements on social media and search engines, the criminal organization lured victims to at least four of these legitimate-looking trading platforms. By contacting victims through the call center they had set up, members of the criminal organization posed as experienced stockbrokers. To demonstrate the profitability of the investments and encourage victims to continue investing, the suspects used modified software. The scam, orchestrated mainly by Israeli nationals, was spread through call centers operating in Bulgaria and northern Macedonia. The criminal network defrauded individuals across Europe of approximately EUR 30 million (EUROPOL,2021).

---

[54] WannaCry is one of the first examples of a worldwide ransomware attack. It began with a cyber attack on May 12, 2017, that affected hundreds of thousands of computers in as many as 150 countries, including systems in the National Health Services of England and Scotland, FedEx, University of Montreal and Honda (Rosencrance, 2021).

[55] See also: https://shapeshift.com/

[56] See also: Trading scheme resulting in €30 million in losses uncovered: https://www.europol.europa.eu/media-press/newsroom/news/trading-scheme-resulting-in-%e2%82%ac30-million-in-losses-uncovered

In the case of activities related to attack funding, the anonymity of the actors involved, especially the anonymity of the attacker is significantly important. Likewise, security is considered very important, in order to not be caught prior the execution of the attack. On the other hand, the factor of usability can be useful in this case, however, it is not necessary. Based on the RAND Report, attackers might be able to acquire the skills necessary to deal with crypto currencies for funds destined to terrorist activities. Additionally, wide acceptance is an important component, due to the fact that access to the cryptocurrency infrastructures would be restricted in the case of lack of acceptance in the area where the terrorist organization operates. Reliability is also significantly important because cryptocurrencies are sensitive to time, causing their prices to be highly volatile, and possibly resulting in the disruption of the transferring of funds to support the attacks. Lastly, volume is not of high importance because terrorist attacks usually require small amounts of people, and can be low-cost (Dion-Schwarz et al., 2019). Some concrete examples of attack funding through cryptocurrencies will be further elaborated below.

Furthermore, operational funding is basically the funding of daily activities of terrorist organizations. Due to the methods used to make transactions on a daily basis, which are usually more or less legal, the factor of anonymity is not of high importance in this case, although it is convenient to stay unidentified. Similarly, usability has less importance due to the limited number of users that would be involved in the transaction, who can rapidly acquire the skills to work with cryptocurrencies. The report notes that the security of the transactions and the management of the funds are of paramount importance. This is because the amounts involved are relatively significant and the structure of the organizational funding would reveal the scale and scope of the transaction. Acceptance is necessary since operational finance would include dealings with other organizations that offer basic needs like food and communications. In order to encourage confidence among transaction partners and maintain budget consistency, especially with unpredictable pricing, the reliability of the cryptocurrency and its

infrastructure would also be somewhat important. Finally, volume is critical since transaction support is often the organization's biggest continuing expenditure and costs a lot of money (Dion-Schwarz et al., 2019).

6.3. Cases of terrorist's use of cryptocurrencies

This section will concretely show how terrorist organizations have used cryptocurrencies to finance their activities. As a study case, the investigation included the cases of Hamas and The al-Qassam Brigades, the case of Al-Qaeda and its affiliated terrorist organizations. Although, this paper is based in the role of the European Union in AML/CFT, the chosen cases have taken place outside of the EU, but due to their impact and also for being one of the biggest of most dangerous terrorist organizations, it was necessary to examine these cases and acknowledge the scale of the abuse of cryptocurrencies for terrorist financing.

However, there have been a couple of identified cases that took place in Europe, although they haven't been analyzed in depth. For instance, in 2018, Europol discovered that multiple organized crime groups have utilized Bitcoin ATMs to conceal transactions for cocaine shipments coming from Colombia. The investigations proved that the chain of payments started in Europe, where criminals have exchanged laundered Euros to Bitcoin through ATMs. After having exchanged the coins the BTC were transferred from a digital wallet supervised by the money-laundering syndicate in Europe, and then moved to Colombian digital wallets. The transactions amounted to around $20,000, which were moved in smaller parts to avoid being identified by law enforcement (Couvée K., 2018). As a result, of the transfer of the Bitcoins to Colombia, European law enforcements do not really have control over the case, however it raised significant concerns in the European financial system, and has pushed for new legislations, like the ones already mentioned above.

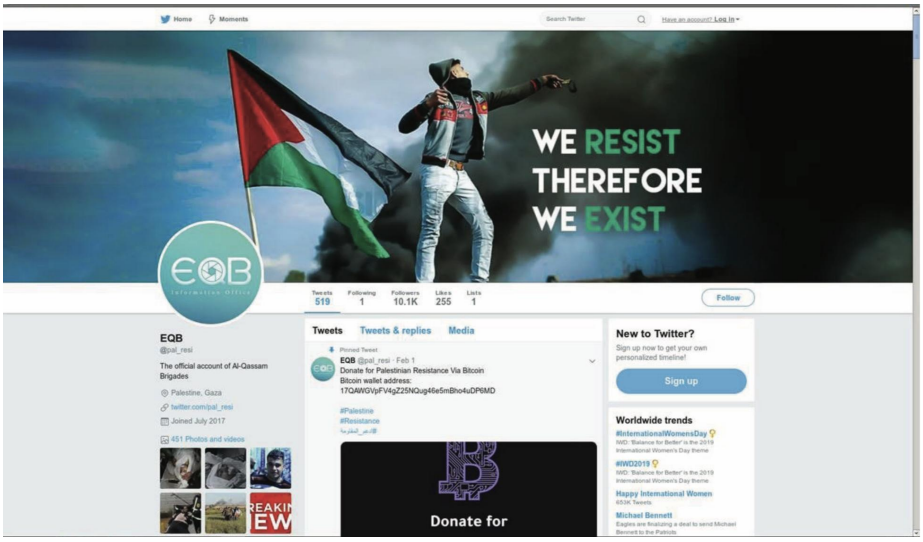
6.3.1. Hamas and The al-Qassam Brigades' Fundraising Camp

The first case of abuse of cryptocurrencies for terrorist financing has as a protagonist the Al-Qassam Brigades. In 1997, the United States Secretary of State designated Hamas as a Foreign Terrorist Organization (FTO), and in 2001 the organization was designated as a Specially Designated Global Terrorist under Executive Order 13224[57]. Included in the designation were the various aliases used by Hamas, such as: Izz Al-Din Al-Qassam Brigades, Izz Al-Din Al-Qassim Forces, Izz Al-Din Al Qassim Battalions, Izz al-Din Al Qassam Brigades, Izz al-Din Al Qassam Forces, and Izz al-Din Al Qassam Battalions (Harvey, 2020).

The case of Hamas and The al-Qassam Brigades' Fundraising Camp, has been described in the *Affidavit in support of an application for a criminal complaint and arrest warrant* against defendants Mehmet Akti and Hüsamettin Karatas[58]. In January of 2019, a fundraising campaign on social media was created by the Al-Qassam Brigades to solicit BTC donations. The organization set up various cryptocurrency accounts to receive BTC donations, including an account starting with 17QAW, a recognizable code that was already publicly posted by the group on its social media accounts. As shown in the image below, the fundraising campaign asked supporters to send BTC to the account (Harvey M., 2020).

[57] Executive order 13224 "provides a means by which to disrupt the financial support network for terrorists and terrorist organizations by authorizing the U.S. government to designate and block the assets of foreign individuals and entities that commit, or pose a significant risk of committing, acts of terrorism"(Executive Order 13224 - United States Department of State, 2023).
[58] See also: AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT AND ARREST WARRANT https://www.justice.gov/opa/press-release/file/1304276/download

Figure 1: *Fundraising campaign al-Qassam Brigades*



(Harvey M., 2020).

After the discovery of this campaign, law enforcement analyzed transactions published in the public ledger of Bitcoin, to try to identify the individual behind the account. Although the nature of cryptocurrencies makes it significantly challenging to discover the identity of the BTC owner, by analyzing public transactions ledger law enforcement was able to discover not only the identity of the owner but also all the other accounts that were controlled by the same individual, in total there were 10 other accounts. The clustering of all the accounts is referred in the Affidavit as “Hamas Account 2” (Harvey M., 2020).

Hamas Account 2 received multiple donations for the terrorist fundraising campaign, however, Al-Qassam Brigades transferred the fundraising to its official websites: “alqassam.net” and “alqassam.ps”. To decrease the possibility of being tracked by

authorities, the campaign relied on unique BTC addresses that were generated for each individual trying to donate, as illustrated by the image below (Harvey M., 2020).

Figure 2: *social media post of a BTC address for donations by al-Qassam Brigades*

(Harvey M., 2020).

In addition, their website would offer detailed instructions on how to make donations and keep the identity of the user anonymous. However, the donations were not anonymous and law enforcement agencies, such as the IRS, FBI, and HSI, were able to discover and seize around 150 cryptocurrency accounts that served the purpose of laundering funds to and from the Al-Qassam brigades' accounts (Harvey M., 2020).

Law enforcement managed to discover the identity of defendant Mehmet Akti, by analyzing the movements of cryptocurrencies through a blockchain analysis. Law enforcements were able to establish that the accounts usually converted the cryptocurrency into FIAT money, exchanged it for valuable objects, or sent it to other accounts. By using blockchain analysis, they were able to trace transactions from Hamas Account 2 to Akti's account at VC A (VC Account 1). By analyzing transaction

records, law enforcements were able to reveal that the account was registered under Akti's name in 2017 (Harvey M., 2020).

Furthermore, when entering cryptocurrencies exchanges and dealing with larger sums of money, the United States Financial Crimes Enforcement Network (FINCEN), requires the user to be registered as a Money Service Provider (MSB[59]), defined as " any person doing business, whether or not on a regular basis or an organized business concern,in one or more of the following capacities: Currency dealer or exchanger, Check casher, etc…" [60]. However, records show that Akti was never properly registered, but he still operated a fruitful cryptocurrency account as an MSB from his account. VC Account 1 showed that the individual was not only dealing with BTC but managed to receive 2,328 BTC, 2,296 ETH, and US dollar transfers estimated to an amount of $82.8 million. Moreover, they were able to discover that the money transfers in US dollars were coming from a Turkish bank account under the name of Deniz Royal Dis Ticaret Limited Sirketi, also Deniz Royal. As a result of the nature of bank transactions, the wires from Turkey entered the US and subsequently returned to the planned destination. Analysis made by law enforcement showed that the US dollar wires were then used to purchase other virtual currencies, mainly Bitcoin and Ethereum (Harvey, 2020). Furthermore, around 11,228 BTC, 7,063 ETH, 957,109 XRP, and 118,008 EOS were among the significant quantities of virtual currency Akti withdrew from VC Account 1 within the same time frame. Notably, these withdrawals comprised transactions totaling over $90 million and were delivered to over 250 different cryptocurrency wallet addresses, which suggests that Akti had hundreds of clients for whom he transferred money as an unregistered MSB (Harvey M., 2020).

---

[59] FINCEN uses the term "money service business" or MSB, to "denote the companies that must register with the agency. Per its own definition, MSBs include "money transmitting businesses" and, specifically, those companies regulated by 18 U.S.C § 1960.", https://www.justice.gov/opa/press-release/file/1304276/download

[60] See also: https://bitaml.com/2018/10/29/cryptocurrency-msb/#:~:text=According%20to%20the%20Financial%20Crimes,(2)%20Check%20casher

Additionally, part of the investigation shows that after Akti's deposed a statement in March 2019, he transferred the totality of his virtual assets to other wallets, and a few weeks later were moved to another account at VC A (VC Account 2), under the name of Hüsamettin Karatas, the second defendant part of this investigation. When he opened VC Account 2, law enforcements were able to identify that the amount of funds in the account were almost the same exact amount as when Akti liquidated VC Account 1, respectively: 42.2 BTC, 2,465 ETH, 123,500 XRP, and 70,055 EOS[61], which was estimated to be $803,712 altogether (Harvey M., 2020).

In addition, when law enforcement interviewed Karatas he stated that he was not connected to Akti and were not business partners. However, the investigation proved otherwise. Karatas was indeed behind VC Account 2, and apart from the cryptocurrencies received from Atki's VC Account 1, between April 2019 and July 2019 Karatas received around $2.1 million dollars in cryptocurrencies and FIAT currencies, including $500.000 transfer from Deniz Royal. Also, in the same timeframe the defendant exchanged his cryptocurrencies with a value of $2.3 million dollars from 17 different wallet addresses[62] (Harvey M., 2020).

6.4. Case of Al-Qaeda

The second case arises from an investigation made by the International Revenue Service- Criminal Investigation's Cyber Crimes Units (IRS-CI), the FBI and the HSI. The case is connected to foreign terrorist organizations in Syria that are affiliated with Al-Qaeda, including the al-Nusrah Front (ANF) and Hay'at Tahrir al-Sham (HTS), who committed several federal crimes of terrorism against the United States, its inhabitants

[61] "The EOS coin is the native token of EOSIO network, which is a type of blockchain technology that is positioning itself as a decentralized operating system", at https://www.abra.com/cryptocurrency/eos/#:~:text=What%20is%20EOS%3F,build%20and%20scale%20decentralized%20applications.

[62] As a result of the investigation both defendants, Akti and Karatas were proved guilty for violating 18 U.S.C § § 1960 and 1956(h) (Harvey, 2020).

or citizens, as well as against any foreign assets that may be used to give someone power over any such body or organization (Sherwin et al,. 2020).

Since 1999, the US Secretary of State included AL-Qaeda as an FTO both as a Specially Designated Global Terrorist ("SDGT") under Section 1(b) of Executive Order 13224 and under Section 219 of the Immigration and Nationality Act. The Osama Bin Laden Network, the Osama Bin Laden Organization, "the Base," the Islamic Army for the Liberation of the Holy Places, the World Islamic Front for Jihad Against Jews and Crusaders, the Islamic Salvation Foundation, and The Group for the Preservation of the Holy Sites were also added by the Secretary of State to the list of FTOs. AQ is still a recognized FTO as of right now. In 2004, the alias of AL-Qaeda in Iraq (AQI), was also added as an FTO, Moreover, in 2012, the Secretary of State designated as an FTO and SDGT the Jam'at al Tawhid wa'al-Jihad to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant. In 2018, the Secretary of State requested to add the include the following names as aliases of ANF: Hay'at Tahrir al-Sham, also known as Hay'et Tahrir al- Sham, also known as Hayat Tahrir al-Sham, also known as HTS, also known as Assembly for the Liberation of Syria. As of today, HTS and ANF are still appointed as FTOs (Sherwin et al., 2020).

Through the investigation, in 2019 law enforcement agencies discovered that Al-Qaeda and affiliated terrorist organizations controlled a Bitcoin money laundering network by using Telegram and other social media apps, to ask for BTC donations to fund their terrorist activities. The Telegram channels were being promoted as charities; however, they were in fact collecting funds for the mujahideen (Al-Qaeda fighters or soldiers). In April of 2019, the Telegram group called "Tawheed & Jihad Media", published a Bitcoin address initiating with 37yrx7 (Defendant property AQ1) as a reference for Al-Qaeda donations. In the same time frame, in the group chat users were advertising fundraising campaigns to collect money for fighters. For instance, in May of

the same year, an unidentified user posted a photo with the caption “FINANCE BULLETS AND ROCKETS FOR THE MUJAHIDEEN”, and also added “for donations and details: please message @TawheedJihadMedia”. As stated in the *civil complaint* by the US District Court For the District of Columbia, in the Telegram groups there were pictures and content related to both Ansar al-Tawheed, a jihadist organization founded in or around March 2018, and Wa Haredh al-Moemeneen (Incite the Faithful), an Al-Qaeda supporter organization of which Ansar al-Tawheed is a part of. The group Wa Haredh al-Moemeneen was created in 2018 to resist negotiations with the Syrian regime, and in 2019, the same period of when the first BTC transaction had been solicited through the Telegram group, conflicted with the government forces of Syria and their allies (Sherwin et al., 2020).

Furthermore, during these months the funds that had been collected by the account Defendant Property AQ1, were then transferred to other 2 virtual currency exchange accounts: Defendant Property AQ2 and Defendant Property AQ3. This method of sending funds back and forth from one account to the other is known as *layering,* a common technique used in money laundering. However many other virtual currencies accounts had been identified connected to Al-Qaeda funding activities, which were operated by other terrorist organizations and movements, such as the *Leave an Impact Before Departure* organizations, the *Malhama Tactical,* the telegram channel *Al Ikhwa,* the *Reminders from Syria,* and *Al Sadaqah* (Sherwin et al,. 2020).

6.4.1. Leave an Impact Before Departure

One of the organizations helping Al-Qaeda to collect funds was a Syrian based group that in English translates to “Leave an Impact Before Departure”, who was asking people to donate BTC through “charities for humanitarian work”, but in fact was asking for funds for military equipment. As a matter of fact, the group had posted images on

Telegram showing the different prices for military equipment that was needed to fighters located in Syria (as shown below) (Sherwin et al., 2020).

Figure 3: *prices of military equipment to ask for donations*

(Sherwin et al., 2020).

As it shows, the donations were destined for terrorist related activities, and the group was also advertising an account (Defendant Property 4) to which individuals could send donations. Through records, law enforcement discovered that Defendant Property 4 received many transactions between March and December of 2019, including seven transactions of a value of 0.73060999 BTC from Defendant Property AQ2. In addition, Defendant Property AQ2 transferred funds to a cluster of 29 BTC addresses (Defendant Property 5 - Defendant Property 33) that proved the connection of these organizations working to raise funds for illicit use (Sherwin et al., 2020).

6.4.2. Al Ikhwa

A second connection to the funding activities of Al-Qaeda has been made by the discovery of a Telegram channel named @Al_ikhwa_official, which appeared online around June of 2018. The group's account description mentioned that they were "independent charity on the ground in Syria" and that they were not part of any terrorist organizations or activity. However, the investigation confirmed that posts on social media and transactions were made, which proved otherwise (Sherwin et al., 2020).

Through its social media, the group asked for donations that could've been made through Western Union, PayPal and anonymous payments with Bitcoin. The Al Ikhwa administrator published 11 BTC addresses (Al Ikhwa Cluster) to which donors could have sent funds. The 11 BTC addresses were referred to as Defendant property 34 until Defendant property 44. Thanks to the Blockchain analysis, law enforcements were able to prove that at least half of the BTC received the Al Ikhwa Cluster work coming from Defendant Property AQ2, this was around October 2018 and September 2019. Al Ikhwa was also controlling a Facebook account where other four BTC addresses were published, two part of Al Ikhwa Cluster and the other two part of a cluster of six BTC addresses addressed as Al Ikhwa Facebook Cluster. The six Facebook addresses represent Defendant Property 45 through Defendant Property 50 (Sherwin et al., 2020).

Additionally, the investigation was able to prove that Al Ikhwa was allegedly trying to hide the identity of the actors behind the accounts to obfuscate the source of BTC. As a matter of fact, Al Ikhwa posted on telegram, a statement destined to the donors saying "our Syria IP addresses are Turkish because our Internet comes from Turkey. So if they try to trap someone and say you sent money here by showing an IP address, you say they are liars and you did business in Turkey…cause the IP address is Turkish." Finally, Blockchain analysis proved that Al Ikhwa money laundering network send, and receive

the money from Defendant Property 1, Defendant Property 4, and Defendant Property AQ2 (Sherwin et al,. 2020).

6.4.3. Malhama Tactical

After further investigations Al Ikhwa has been linked to Malhama Tactical, described as a Jihadists military organization that trains Hay'at Tahrir al-Sham (HTS) fighters and has asked for Bitcoin donations to support HTS activities in Syria. Malhama Tactical is referred to as a "Jihadist private military company" that has soldiers coming from the Russian Caucasus and Uzbekistan. The founding leader of the group, Abu Salman Belarus, was described in the official organization's Twitter page as the "commander of Malhama Tactical", the page also mentioned that "we are military instructors, we've been teaching rebels who to fight and provide emergency aid on the battlefield since 2013". During the years of 2019 and 2020, Malhama Tactical was undressing for weapons and military equipment, including drones. Additionally, the Twitter account of Malhama Tactical's founder published two BTC addresses, stating that people could support the organization without being discovered by using Bitcoin wallets. The two addresses were part of a cluster of 23 addresses named MT Cluster, which from July 13 to November 22, 2019, received 15 transactions totaling around 0.19501359 BTC. These 23 BTC addresses stand in for Defendant Properties 51 through 73. On or around October 9, 2018, the MT cluster transmitted around 0.03839 BTC to the cluster 3Jb1M, which had previously sent BTC to Defendant Property AQ2 (Sherwin et al., 2020).

6.4.4. Reminders From Syria

Similarly, to the previous case, the Al Ikhwa telegram network raised suspicions about the @ReminderFromSyria (RFS) channel. Apparently both accounts were publishing each other's contents, including BTC addresses. The RFS had stated that

they were not linked to any terrorist groups in Syria, however, various donation requests, radical extremist statements, and threat to the United States, proved the contrary (Sherwin et al,. 2020).

As part of the investigation, an Homeland Security Investigations (HSI) undercover agent managed to contact the administrator of the account, asking for the BTC addresses to donate funds. After the conversations between the two parties, the law enforcement agent understood that the cluster of BTC addresses were representing Defendant Property 74 to Defendant Property 78. Additionally, a Blockchain analysis proved that funds were moved throughout these accounts, and Defendant Property 78 had the same virtual currency exchange as Defendant Property 1 (Sherwin et al,. 2020).

6.4.5. Al Sadaqah

Al Sadaqah, which means "charity" in Arabic, is a Syrian group that manages social media profiles on various platforms with the intention of using BTC solicitations to fund terrorism. They identified themselves as "an independent charitable organization that is assisting and supplying the Mujahideen in Syria with weapons, financial help, and other jihad-related operations" and claim that Bitcoin is a secure and safe way to make donations (Sherwin et al., 2020).

As a matter of fact, Al Sadaqah publicly requested donations via BTC to an address beginning with 15K9Z (Defendant Property 79, which was grouped with Defendant Property 80) on its Telegram account. The address referred to as Defendant Property 79, was used in a post made by the group claiming to support "the mujahideen in Syria with weapons, financial aid, and other projects assisting the jihad." (Shown below) (Sherwin et al., 2020).

(Sherwin et al., 2020).

Subsequently after deep Blockchain analysis, law-enforcement was able to prove that 155 cryptocurrency accounts were related to these groups[63] and were aimed at financing terrorist activities in Syria and in the United States (Sherwin et al., 2020)

[63] The civil complaint document where this cases are described in detail, confirms that the Defendant Properties:*"Are subject to forfeiture to the United States, pursuant to 18 U.S.C. § 981(a)(1)(G)(i), as assets of a foreign terrorist organization engaged in planning or perpetrating any federal crime of terrorism (as defined in section 2332b(g)(5)) against the United States, citizens or residents of the United States, or their property, and as assets affording any person a source of influence over any such entity or organization"* (Sherwin et al,. 2020).

7. DISCUSSION

In this research paper we have discussed how cryptocurrencies are facilitating the financing of terrorism and the laundering of money, to fund illicit activities, which represent a big challenge for law enforcements to detect and suppress. The main question of this research is to understand the effectiveness of the role of the European Union to decrease the amount of cases of terrorism financing through cryptocurrencies, and if the current legal framework is good enough to bring to light the actors that engage in these activities.

Terrorism is a complex phenomenon that poses a significant threat to global security, and after the Twin Tower attack of 2001, has been one of the most growing concerns between governments, organizations, and individuals. With the advent of technology, terrorist groups have become much more sophisticated on how they finance their activities, and although their main means of financing remains a cash-based economy, cryptocurrencies have opened a variety of opportunities for them to exploit the financial system and continue with their terrorist activities without being detected. The characteristic of anonymity of cryptocurrencies has been one of the main reasons for terrorist groups to engage in this new way of financing. As a matter of fact, Europol has stated that the European Union has lost 1% of its GDP through money laundering, which is a significantly big part of the EU economy, and it creates an alarming concern on how terrorist organizations and criminals can be stopped before it is too late.

It is worth noting, that the European Union actually supports the advance of the Blockchain technology, on which cryptocurrency runs on, because its scope is much wider and can be applied to a variety of sectors. Specifically, Blockchain technology could represent an advancement in trade and commerce, governance, health sector, and others. That is why it is important to dissociate Blockchain from cryptocurrency and

understand that just because some terrorist organizations have exploited the system, it does not mean that it should be discouraged and stopped from being implemented in the European economy. This would mean dissociating from future innovations, and in today's world it is significantly important to stay up to date with these technologies and instead of rejecting them, we should consider just better implementing regulations in order to limit the illicit use of these systems by terrorist groups.

In connection to this, the effectiveness of the current European Union Framework is essential, because if cryptocurrencies are being known to be insecure and exploited by terrorist groups, they will lose their credibility, and the technology will not advance in the European economy. This could show that the EU does not have the proper capacity to control new advancement in the economy, nor has the capacity to tackle the characteristic of anonymity of cryptocurrencies.

For this reason, we have analyzed the limitations that the European Union legal Framework on AML/CFT present, towards the financing of terrorism through cryptocurrencies. Firstly, a significant underestimation of the EU is the role of the mining business in cryptocurrencies. Miners, depending on the activities they engage with, could fall into or outside the scope of the AMLD. If they become cryptocurrencies providers, then they could be legislated by the new EU framework, however, in most cases, miners stay in the dark and just mine coins for other entities. Also, miners could simultaneously be cryptocurrency users, which could create big risks and challenges for law enforcements. The problem derives from the fact that, if a terrorist organization manages to become a miner, and create new coins, it could just start a financing system between its members with newly mined coins and pursue its terrorist activities without being detected.

Secondly, the new AML/CFT framework has failed to include all of the entities that engage in cryptocurrency transactions, mainly because some cryptocurrencies offer a higher level of anonymity, such as Monero, which makes impossible to identify who is behind an account or a group of transactions. Also, although MiCA extended its scope on more actors in the cryptocurrency market, it still missed the mark in including certain cryptocurrencies that work on Decentralized Finance. This stems from the fact that there is no central entity or intermediaries, to whom a regulation should be aimed at. Hence, terrorist organizations have found this loophole in the EU AML/CFT framework, and exploited it to their own advantage, to finance their activities, create fundraising campaigns without the risk of being identified.

Moreover, the lack of regulation around the anonymity of cryptocurrencies makes other legislation less effective. For instance, the current EU framework on tax avoidance which relates, among other things, to exit taxes in the context of assets transfers by businesses, misses the target when it comes to cryptocurrencies (Council of the European Union, 2016). The tax administration must be aware of the taxable framework in order to be able to collect taxes, and with regard to cryptocurrencies, this is merely very challenging (Snyers, A., et al, 2018).

Another example in connection to the gaps of the EU framework, is related to the freezing and confiscation of property. It can be argued that cryptocurrencies are already included in the relevant European rules, which define property as any type of corporeal or incorporeal, movable or immovable asset, including legal documents. Cryptocurrencies could be seen as a type of incorporeal movable property. However, these rules have limited success in practice. The reason for this is the difficulty in identifying when a criminal possesses cryptocurrencies due to the anonymity surrounding these transactions. Therefore, the key issue is how to reveal the anonymity associated with cryptocurrency transactions in order to track illegal activities (Snyers, A., et al, 2018).

Moreover, the evolving objectives of the system to combat money laundering and terrorist financing are undermined by institutional overload and growing coordination problems. Cryptocurrencies and other technological developments are not only accelerating the anti-money laundering and counter-terrorist financing agenda, but also highlighting the limitations of a purely intergovernmental response. In fact, although mechanisms to combat money laundering and terrorism financing have been put in place, there is a growing challenge in having a coherent legal framework in each of the EU Member States. As already mentioned earlier, the lack of harmonization between Member States is among one of the main issues in the detection of terrorism financing and money laundering through cryptocurrencies. The main problem is that the EU AML/CFT framework is mainly based on Directives, which are not directly applicable into national legislations, contrary to regulations. This leaves a freedom to Member States to decide how to implement these directives, and results in a divergence between how EU Member States act on activities related to money laundering and terrorism financing, both through cryptocurrencies and FIAT currencies. Also, the lack of direct applicability undermines the efficiency of the directives themselves, due to the fact that by the time EU Member States might implement them, the risks and challenges around terrorism financing through cryptocurrencies, will develop differently, and new risk will arise that will not be included in the Directives. Hence, the reality of the risks that cryptocurrency pose, will not be up to date with the issues addressed in the AMLD. However, leaving interpretative freedom to EU Member States on Directives, has also its positive sides, because each country has a different level of risk of money laundering and terrorism financing, but as we saw in earlier paragraphs, this leads to an incoherent approach of Member States in this matter.

Furthermore, it is critical to strike a balance between safeguarding privacy, cybersecurity, and data protection while simultaneously allowing authorized law enforcement access to information for criminal investigations. On the basis that, it is common practice for individuals and organizations to utilize encryption (intensively used

in the context of cryptocurrencies), as a line of defense against IT-related crimes including fraud, identity theft, hacking, and unauthorized exposure of sensitive information. However, encryption may also be used by criminals to carry out operations like money laundering or financing terrorism, making it challenging for law enforcement officials to undertake investigations into crimes (Snyers, A., et al, 2018).

Moreover, the creation of the AMLA, although being one of the biggest steps forward in the AML/CFT legal framework, by increasing cooperation and supervision in Member States, it still does not address the problem of subsidiarity in EU countries. It also does not address one of the biggest challenges of terrorism financing through cryptocurrencies, which is its cross-border nature. The European Union, contrary to the United States, lacks extraterritorial power in AML/CFT. The United States has in fact a much more effective approach because it can prosecute and sanction non-US institutions that engage in money laundering and terrorist financing through US dollars, no matter if it was held inside or outside the US. The United States has the power to control all the transactions that happen with the US currency, that is because all of these transactions have to be cleared by the Federal Reserve, in New York. Having extraterritorial powers is one of the most effective tool in stopping terrorism financing through cryptocurrencies, however there are various limits in Europe that do not allow to have extraterritorial powers, such as: the lack of a centralized clearing system that controls all Euro transactions, lack of political awareness, and egoistic national legislations that prioritize each EU Member States necessities, and also the fact that AMLD only addresses EU Member States and leaves the decisions of extraterritorial powers to each one of them (Unger et al., 2020).

Consequently, as we have seen in the cases of the Hamas and The al-Qassam Brigades' Fundraising Camp, and Al-Qaeda, terrorist organizations are being up to date more than regulations are. They have adapted to the fast developing digital financial system, and have strategically understood how to finance their illicit activities without

being detected, or at least by being less under the radar. In both cases, the groups have created social media accounts, or websites, where they would open a fundraising campaign, through which sympathizers could donate cryptocurrencies. Between both cases the amount of laundered cryptocurrencies amounts around $150 millions, which shows how important cryptocurrencies have become for the financing of terrorist activities, and should raise big concerns in Europe and globally, to how effectively detect these types of transactions.

Furthermore, although the main focus of this investigation is the European Union, it was considerably hard to find cases related to terrorism financing through cryptocurrencies in the European Union, which shows that the European legal framework on AML/CFT is still insufficient to bring into light the actors involved in these activities. As a result, we believe that the European Union should take some inspiration from the United States AML/CFT framework, and consider implementing the factor of extraterritoriality in AMLD. Also, we think that making the AMLD at less risk of freedom of interpretation could result in a much more effective and coherent framework to target the financing of terrorism and money laundering through cryptocurrencies.

8. CONCLUSION

With the advent of cryptocurrencies in the financial system, many risks and challenges have risen for law enforcement, not only in the European Union but internationally. In 2009, Bitcoin was created, and has opened new opportunities for terrorist organizations to fund their activities. With the development of technology, many more cryptocurrencies have been created, such as Monero and DCash, which offered much more anonymity to the cryptocurrency user, and have canceled the necessity of having a central intermediary to exchange virtual assets to FIAT money, which further attracted cyber criminals in the crypto market.

Today, the crypto market has many different types of actors, such as: cryptocurrencies users, miners, cryptocurrencies exchanges, trading platforms, wallet providers, coin offerors, and coin inventors. The variety of actors has negatively impacted the efficiency of the EU AML/CFT legal framework, due to the fact that sometimes identifying the target to whom a certain regulation should be aimed at is very difficult. A lack of a central entity makes it almost impossible to understand who to target when creating a legislation.

Moreover, as we have examined in this research, the threat of terrorism is a real and growing concern, which has led us to analyze the European approach towards this issue. The European Council definition of terrorist acts acknowledges the threat that using cryptocurrencies to finance terrorist activities poses to the European financial stability, and could be a significant risk to human security as well.

The weaknesses of cryptocurrencies have demonstrated that anonymity and double spending create new methods of terrorist financing, without the risk of being under law enforcement’s radar. As well, the cross-border nature of cryptocurrencies pose a serious

challenge to the European Union due to the EU's lack of extraterritorial power. Moreover, due to the distinctive characteristics that cryptocurrencies have, such as their decentralized nature, lawmakers have had a significantly difficult time understanding how to properly address these issues, and target the actors involved in illicit activities through cryptocurrencies.

Additionally, the European Union has acknowledged the risks that the launder of cryptocurrencies to fund terrorist activities could pose to our continent and to the rest of the world. Which resulted in the creation of various legal mechanisms to better address the matter. The establishment of the AMLA, and the MiCA, can be considered one of the biggest steps ever made in Europe to counter the financing of terrorism and money laundering. They have extended the list of selected obliged entities that fall under the scope of the EU AMLD, such as VASPs, and any institutions that serve as a cryptocurrencies provider. Which will obligate them to share information about the identity of users with law enforcement agencies responsible for supervising the environment of money laundering and terrorism financing, such as Europol, the European Banking Authority, and the FATF.

Moreover, the fast adaptability of terrorist organizations to cryptocurrencies, has resulted into a intergovernmental overload on the current EU legal framework, which has created some limits in the effectiveness of the AMLD, and the other AML/CFT mechanisms. The main limits include the difference in application between EU Member States. This can be seen in the divergences of asset seizure methods, the dissimilarity of access to resources to pursue criminal investigations of AML/CFT, the various interpretations on what is money laundering, what could constitute a terrorist finance offense, and also the substantial differences in the application of sanctions. Each Member State has the freedom to interpret the AMLD, as they consider fit to the risk assessment within their borders. This stems from the fact that the EU AMLD is not directly applicable in national legislations, which consequently increases the

divergences between Member States on how to counter terrorism financing and money laundering. As we have seen in some cases, some states have taken a long time to actually implement the AMLD in their countries, such as France, who surpassed the deadline of the 3AMLD by three years. As a result, considering making the AMLD a binding legal instrument could change the level of effectiveness on how European countries counter terrorism financing and money laundering.

In conclusion, the cases of Hamas and the Al-Qassam Brigades, and Al-Qaeda, show that terrorism financing and money laundering through cryptocurrencies is real, and they have in fact managed to launder over $150 millions, by creating social media accounts and fundraising campaigns. Through this means, they asked donors to finance their illicit activities, and have managed to move funds from one virtual account to another to then proceed to finance criminal acts with the purpose of destabilizing the government, and the economy of the United States. Although these study cases did not take place in Europe, cryptocurrencies transactions do not have borders. As a matter of fact many of those payments were based in Turkey, while the accounts holders were from Syria, which demonstrates that solely limiting the EU AML/CFT framework within the European Union's Member States could only further open more opportunities for terrorist organizations to exploit our financial system, and possibly increase the loss of the EU GDP through money laundering.

Finally, as a result of this research we can conclude that the European Union needs to better address and analyze more in depth the current different actors that participate in cryptocurrencies transactions, that could increase the risk of terrrorism financing and money laundering through cryptocurrencies, such as the miners. Moreover, a deepening in the understanding of cryptocurrency's anonymity is necessary, to better target which cryptocurrencies present a higher risk for the fight against AML/CFT, and to potentially ban those cryptocurrencies that make it almost impossible to reveal the identity of the user. In conclusion, the EU Member States should work on having better harmonization,

and potentially transform the Anti-Money Laundering Directives into a more legally binding instrument, to properly decrease the risk of laundering cryptocurrencies for terrorism purposes, and to increase the efficiency of the European Union legal framework on Anti-money Laundering and terrorism financing.

BIBLIOGRAPHY

About Europol | Europol. (2023). Europol. https://www.europol.europa.eu/about-europol

Abrol, A. (2023, March 10). What is Peer to Peer Network, and How does it work? Blockchain Council. https://www.blockchain-council.org/blockchain/peer-to-peer-network/

Academy, B. (2023, February 21). What Is Uniswap and How Does It Work? Binance Academy. https://academy.binance.com/en/articles/what-is-uniswap-and-how-does-it-work

BBVA. (2023, April 19). EU Markets in Cryptoassets (MiCA) Regulation: What is it and why does it matter? NEWS BBVA. https://www.bbva.com/en/innovation/eu-markets-in-cryptoassets-mica-regulation-what-is-it-and-why-does-it-matter/#

Bitstamp. (2022, August 17). What is block size? - Bitstamp Learn Center. Learn Center. https://www.bitstamp.net/learn/crypto-101/what-is-block-size/

Born, A. (2022, July 11). Decentralised finance – a new unregulated non-bank system? European Central Bank. https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html

Chen, J. (2023, March 28). Fiat Money: What It Is, How It Works, Example, Pros & Cons. Investopedia. https://www.investopedia.com/terms/f/fiatmoney.asp

Coinbase. (2023). What is a crypto wallet? Coinbase. https://www.coinbase.com/learn/crypto-basics/what-is-a-crypto-wallet

Could Blockchain Have as Great an Impact as the Internet? (n.d.). https://www.jpmorganchase.com/news-stories/could-blockchain-have-great-impact-as-internet

Couvée, K. (2018). European Traffickers Pay Colombian Cartels Through Bitcoin ATMs: Europol Official. Acams.

https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/

Custers, Bart and Oerlemans, JanJaap and Pool, Ronald, Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies (June 16, 2020). Custers, B.H.M., Oerlemans, J.J., Pool, R. Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies, European Journal of Crime, Criminal Law and Criminal Justice, 28 (2020), p. 121-152. https://ssrn.com/abstract=3694282

Daniels, N. (2023). The 7 Most Private Cryptocurrencies For You to Consider in 2023. VPNOverview.com. https://vpnoverview.com/privacy/finance/private-cryptocurrencies/

Discover eu-LISA - 2022. (n.d.). https://www.eulisa.europa.eu/SiteAssets/Discover/default.aspx/home

EU AML/CFT Global Facility. (2022, February 11). Money laundering and terrorist financing: global AML/CFT context. https://www.global-amlcft.eu/global-anti-money-laundering-and-countering-terrorism-financing-context/

European Banking Authority. (2022, March 22). Anti-money laundering and countering the financing of terrorism. European Banking Authority. https://www.eba.europa.eu/anti-money-laundering-and-countering-financing-terrorism-supervision-improving-not-always-effective

European Commission, official website. (2023). European Commission. https://commission.europa.eu/index_en

European Cybercrime Centre - EC3 | Europol. (2023.). Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

European Financial and Economic Crime Centre - EFECC | Europol. (2023.). Europol. https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc

Eurojust. (n.d.). What we do. https://www.eurojust.europa.eu/about-us/what-we-do?pk_source=website&pk_medium=link&pk_campaign=homepage-bloc%E2%80%A6

European Serious and Organised Crime Centre - ESOCC | Europol. (2023.). Europol. https://www.europol.europa.eu/about-europol/european-serious-and-organised-crime-centre-esocc

Frankenfield, J. (2021). Dark Wallet. Investopedia. https://www.investopedia.com/terms/d/dark-wallet.asp

Frankenfield, J. (2022a). Atomic Swap: Definition, How It Works With Cryptocurrency Trade. Investopedia. https://www.investopedia.com/terms/a/atomic-swaps.asp

Frankenfield, J. (2022b, September 27). What Does Proof-of-Stake (PoS) Mean in Crypto? Investopedia. https://www.investopedia.com/terms/p/proof-stake-pos.asp

Frankenfield, J. (2023, February 9). What Is Proof of Work (PoW) in Blockchain? Investopedia. https://www.investopedia.com/terms/p/proof-work.asp

Frankenfield, J. (2023, February 4). Cryptocurrency Explained With Pros and Cons for Investment. Investopedia. https://www.investopedia.com/terms/c/cryptocurrency.asp

Global Counterterrorism Forum (GCTF) - Home. (n.d.). https://www.thegctf.org/

Goal 16 | Department of Economic and Social Affairs. (2023.). https://sdgs.un.org/goals/goal16

Goal 17 | Department of Economic and Social Affairs. (2023.). https://sdgs.un.org/goals/goal17

Goldman, Z. K., Maruyama, E., Rosenberg, E., Saravalle, E., & Solomon-Strauss, J. (2017). Terrorist use of Virtual currencies. CNAS. https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies

Greenberg, A. (2017, January 25). Cryptocurrency Monero Is Skyrocketing Thanks to Darknet Druglords. WIRED. https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/

Harvey, M. G. (2020). Affidavit in support of an application for a criminal complaint and arrest warrant. United States District Court for the District of Columbia. https://www.justice.gov/opa/press-release/file/1304276/download

Hong, E. (2022, May 5). How Does Bitcoin Mining Work? Investopedia. https://www.investopedia.com/tech/how-does-bitcoin-mining-work

International Monetary Fund (2011, December 14) Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) - Topics. https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

Kriptomat. (2023.). How To Cash Out Your Crypto Safely and Easily - Kriptomat. https://kriptomat.io/cryptocurrencies/how-to-sell-cryptocurrency/guide/#:~:text=Cashing%20out%20means%20selling%20crypto,money%20to%20your%20bank%20account.

Ledger | Ledger. (2022, December 9). Ledger. https://www.ledger.com/academy/glossary/ledger

Ledger. (n.d.). Why choose Ledger. Retrieved from https://www.ledger.com/why-choose-ledger

Marcobello, M. (2023, March 26). What Are Stealth Addresses? Decrypt. https://decrypt.co/resources/what-are-stealth-addresses

Marshall, A. (2017). P2P Cryptocurrency Exchanges, Explained. Cointelegraph. https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained

Monneo. (2023). Merchant Accounts for Cryptocurrency Businesses | Monneo. https://www.monneo.com/cryptocurrency-merchant-account/

Mstoken.art. (2023, January 28). Home - mstoken.art. mstoken.art - a Fine Art Security Token. https://mstoken.art/

Policy department for citizens' rights and constitutional affairs. (2018). Virtual Currencies and Terrorist Financing: assessing the risks and evaluating responses. In European Parliament (PE 604.970). https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

JP Morgan Chase & Co. (2023). Could Blockchain Have as Great an Impact as the Internet? https://www.jpmorganchase.com/news-stories/could-blockchain-have-great-impact-as-internet

Ravikiran A. S. (2023, January 29). What is Blockchain Technology? How Does Blockchain Work? [Updated]. Simplilearn.com. https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology

Rosencrance, L. (2021). WannaCry ransomware. Security. https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware

Rosenfeld, M. (2014). Analysis of hashrate-based double-spending. ArXiv. https://arxiv.org/pdf/1402.2009.pdf

Sav, D. (2023). What is the FATF Travel Rule? The Ultimate Guide to Compliance (2023). Sumsub. https://sumsub.com/blog/what-is-the-fatf-travel-rule/#

Sharma, R. (2023, February 5). 3 People Who Were Supposedly Bitcoin Founder Satoshi Nakamoto. Investopedia. https://www.investopedia.com/tech/three-people-who-were-supposedly-bitcoin-founder-satoshi-nakamoto/#:~:text=Key%20Takeaways,continues%20to%20decline%20the%20claim

Solana (SOL) Price, Charts, and News | Coinbase: solana price, solana, sol price. (n.d.). https://www.coinbase.com/price/solana

The cipher brief. (2017, July 25). The New Frontier in Terror Fundraising: Bitcoin. The Cipher Brief. https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin

Trading scheme resulting in €30 million in losses uncovered | Europol. (2021.). Europol. https://www.europol.europa.eu/media-press/newsroom/news/trading-scheme-resulting-in-%E2%82%AC30-million-in-losses-uncovered

LEGAL DOCUMENTS

Bąkowski, P. (2023). EU anti-money laundering (AML) and combating the financing of terrorism (CFT) single rule book - Q1 202. In European Parliament. https://www.europarl.europa.eu/legislative-train/carriage/eu-amlcft-single-rule-book/report?sid=6901

Bolotaeva O. S., et al. (2019). IOP Conference Series: Earth and Environmental Science. The Legal Nature of Cryptocurrency. Retrieved from https://iopscience.iop.org/article/10.1088/1755-1315/272/3/032166/meta

Commonwealth Secretariat. (2015). Commonwealth Working Group on Virtual Currencies. The commonwealth.org. https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/press-release/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf

Council of Europe. (2015). Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168047c5ea

Council of Europe. (2023). Financial Intelligence Units - Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - www.coe.int. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. https://www.coe.int/en/web/moneyval/implementation/fiu

Council of the European Union. (2016). COUNCIL DIRECTIVE (EU) 2016/1164 of 12 July 2016 laying down rules against tax avoidance practices that directly affect the functioning of the internal market. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1164&from=EN

Council of the European Union – role | European Union. (2023). European Union. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/council-european-union_en

Dion-Schwarz C., et al. (2019). Terrorist Use of Cryptocurrencies. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

European Banking Authority. (2023). Anti-Money Laundering and Countering the Financing of Terrorism. European Banking Authority. https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism

European Commission. (2017). Report from the Commission to the European Parliament and to the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border situations. European Commission. https://eur-lex.europa.eu/resource.html?uri=cellar:d4d7d30e-5a5a-11e7-954d-01aa75ed71a1.0001.02/DOC_1&format=PDF

European Commission. (2021). REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010. In European Commission (2021/0240(COD)). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0421

European Council. (2001). COUNCIL COMMON POSITION of 27 December 2001 on the application of specific measures to combat terrorism (2001/931/CFSP). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:344:0093:0096:EN:PDF

European Court of Auditors. (2021). EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficient. In European Court of Auditors. https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_EN.pdf

EUR-Lex - 230804_1 - EN - EUR-Lex. (n.d.). https://eur-lex.europa.eu/EN/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes.html#:~:text=Directive%20(EU)%2

02015%2F849%20(4th%20Anti%2DMoney,being%20misused%20for%20these%20purposes.

European Parliament & Council of Europe. (2010). Regulation (EU) NO 1093/2010 of the European Parliament and of the Council. In Official Journal of the European Union (L 331/12) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:331:0012:0047:EN:PDF

European Parliament & Council of Europe. (2010b). REGULATION (EU) No 1094/2010 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. In Official Journal of the European Union (L 331/48). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010R1094

European Parliament & Council of Europe. (2010c). REGULATION (EU) No 1095/2010 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 November 2010. In Official Journal of the European Union (L 331/84). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:331:0084:0119:EN:PDF

European Parliament. (2015). Understanding definitions of terrorism. https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/571320/EPRS_ATA(2015)571320_EN.pdf

European Parliament. (2023). Crypto-assets: green light to new rules for tracing transfers in the EU | News | European Parliament. https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu

European Parliament, Directorate-General for Internal Policies of the Union, Snyers, A., Houben, R. (2018). Cryptocurrencies and blockchain – Legal context and implications for financial crime, money laundering and tax evasion, European Parliament. https://data.europa.eu/doi/10.2861/280969

Europol (2021), Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union,

Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Executive Order 13224 - United States Department of State. (2023, April 12). United States Department of State. https://www.state.gov/executive-order-13224/

FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

FATF (2021), Guidance on Risk-Based Supervision, FATF, Paris, www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html

FATF (2012-2023), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html

Full list - Treaty Office - www.coe.int. (2005). Treaty Office. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=196

Oxford University Press. (2008). Self determination. Oxford Public International Law. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e873

Remeur, C. (2023). Anti-money-laundering authority (AMLA): Countering money laundering and the financing of terrorism | Think Tank | European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733645

S/RES/2199 (2015) | United Nations Security Council. (2015). https://www.un.org/securitycouncil/content/sres2199-2015

Sherwin, M. R. (2020). United States' verified complaint for forfeiture in REM. United States District Court for the District of Colombia. https://www.justice.gov/opa/press-release/file/1304296/download

Unger, B., Alshut, F., Jerosch Herold Da Costa Reís, J., & Blokland, G. (2020). Improving Anti-Money Laundering Policy. In European Parliament (PE 648.789). https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648789/IPOL_STU(2020)648789_EN.pdf

United Nations. (1988). United Nations Convention Against Illicit Traffic in Narcotic Drugs And Pyschotropic Substances. In United Nations. https://www.unodc.org/pdf/convention_1988_en.pdf

United Nations. (1999). International convention for the suppression of the financing of terrorism. United Nations. https://treaties.un.org/doc/db/Terrorism/english-18-11.pdf

United Nations General Assembly. (2001). 55/25. United Nations Convention against Transnational Organized. In United Nations (A/RES/55/25). https://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

United Nations Global Counter-Terrorism Strategy (A/RES/60/288) | Office of Counter-Terrorism. (n.d.). https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy#:~:text=The%20United%20Nations%20Global%20Counter,operational%20approach%20to%20fighting%20terrorism

United Nations Security Council. (2001). Resolution 1373 (2001). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement

United Nations Security Council. (2004). Resolution 1566 (2004). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement

United Nations Security Council. (2014). Fact Sheet: UN Security Council Resolution 2178 on Foreign Terrorist Fighters. https://www.justice.gov/file/344501/download#:~:text=Resolution%202178%20requires%20countries%20to,have%20laws%20to%20prosecute%20FTFs.

United Nations Security Council. (2014). Resolution 2195. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/708/75/PDF/N1470875.pdf?OpenElement

United Nations Security Council. (2014). Resolution 2161 (2014). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/432/98/PDF/N1443298.pdf?OpenElement

United Nations Security Council. (2015). Resolution 2199 (2015). In United Nations Security Council (S/RES/2199(2015)). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/040/28/PDF/N1504028.pdf?OpenElement

United States Department of Justice. (2020). United States of America v. Mehmet Akti & Hsamettin. https://www.justice.gov/opa/press-release/file/1304276/download

UNODC. (1999). International Convention for the Suppression of the Financing of Terrorism (New York, 9 December 1999). https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf

U.S. Department of Justice. (2020). Cryptocurrency Enforcement Framework. Retrieved April 7, 2023, from https://www.justice.gov/archives/ag/page/file/1326061/download

Virtual Currencies: Key Definitions and Potential AML/CFT Risks. (2014). https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html

Yianni, A. (2023, March 17). An Overview of the MiCA Regulation: What you need to know! - European Institute of Management and Finance. European Institute of Management and Finance. https://eimf.eu/an-overview-of-the-mica-regulation-what-you-need-to-know/