Universidade do Minho
Escola de Direito

Elif Nazli Birgi

AML/CFT Regulations of EU in the Age of Virtual Currency

April 2018

Elif Nazli Birgi **AML/CFT Regulations of EU in the Age of Virtual Currency**

UMinho | 2018

Universidade do Minho
Escola de Direito

Elif Nazli Birgi

AML/CFT Regulations of EU in the Age of Virtual Currency

Master Dissertation
LL.M. in European and Transglobal Business Law

Work conducted under the guidance of
Professor Miguel Pedro Freitas

April 2018

STATEMENT

Name:Elif Nazlı Birgi

Email:elifnazlibirgi@gmail.com Telephone number: 938140456

Identification card number: U14966444

Title of dissertation: AML/CFT Regulations of EU in the Age of Virtual Currency

Adviser: Pedro Miguel Freitas

Year of completion: 2018

Designation of the Master's degree: LL.M. in European and Transglobal Business Law

University of Minho, ____ / ____ / _____

Signature: _____

Acknowledgments

Firstly, I would like to express my gratitude to my supervisor Professor Pedro Miguel Freitas for the continuous support of my thesis research, for his professionalism, immense knowledge and commitment throughout the orientation process.

I would also like to express my very great appreciation to Professor João Sérgio Ribeiro for his valuable and constructive suggestions and availability throughout the LL.M. Program.

Mother, father, brother, your unconditional support was particularly decisive for me in completing my studies and this work. Thank you for your continual support of my academic endeavours and for your patience.

Anneanne, dede, bana olan sonsuz güveniniz için teşekkür ederim. Benim üzerimde emeğiniz büyük.

André, I cannot thank you enough for your patience, support and understanding. Thank you for encouraging me throughout this experience and for believing in me in difficult moments.

Ultimately, I would like to thank Dina, Jorge and Gustavo for always being there for me.

Thank you University of Minho, for this unforgettable journey.

Abstract

Global consideration on money laundering has its origins in narco-trafficking of 1980s which raised public awareness and took international regulatory body's attention. Throughout time, due to the socio-economic and political context, legislations on money laundering were transformed in order to introduce an efficient response to new issues. As a need in the aftermath of 9/11, counter-financing of terrorism (CFT) was included in the scope of anti-money laundering (AML) legislations, due to the intertwined nature of these two criminal matters.

A new challenge to the AML/CFT legislations was introduced by the technological developments and the emergence of virtual currency. Appearing as an alternative, fast, easy and cheap non-cash payment method, its relation with criminal activities, widespread usage and unregulated operations raised concerns. When traditional approaches to the fight against money laundering and financing of terrorism were circumvented by pseudo-anonymous and decentralized nature of new transaction methods, existing legislations were forced to be transformed once more.

European Union, taking its powers for regulating criminal matters from the Treaty of the Functioning of European Union (TFEU), proposed an amendment to the 4th AML, with the purpose of reducing anonymity of virtual currency. Not being accepted yet, its ability to produce an adequate respond to challenges, due to the special nature of virtual currency, is questionable.

This thesis analyse European Union's current Anti-Money Laundering legislation and its responsiveness to the characteristics of virtual currency that are attributable to the risks, with particular attention to crypto-currency, through a critical perspective. It aimed to raise awareness of the subject matter and contribute to the future of AML/CFT reuglations of the EU.

Key Words: Virtual Currency, Cryptocurrency, Anti-Money Laundering, Combating Financing of Terrorism, EU Law, Judicial Cooperation in Criminal Matters

Resumo

A preocupação internacional com o branqueamento de capitais está ligada ao narcotráfico da década de oitenta. Ao longo do tempo e devido ao contexto sócio económico e político, a legislação relacionada com o branqueamento de capitais foi sendo adaptada, permitindo introduzir uma resposta mais eficiente aos novos desafios. Isto foi particularmente visível na sequência dos ataques de 11 de setembro, momento a partir do qual a prevenção do financiamento do terrorismo passou a estar incluída no domínio do branqueamento de capitais, atendendo à ligação próxima entre estes dois fenómenos.

Um novo desafio à legislação sobre branqueamento de capitais surgiu como desenvolvimento tecnológico, nomeadamente com o aparecimento de cripto-moedas. As moedas virtuais surgiram como uma alternativa rápida, fácil e pouco dispendiosa, para realizar pagamentos. Porém, a sua associação a atividades criminosas, uso generalizado e ausência de regulamentação própria conduziram a fortes preocupações por parte das entidades reguladoras. As abordagens tradicionais de combate à lavagem de dinheiro e financiamento do terrorismo tornaram-se obsoletas perante a natureza descentralizada e pseudoanónima destes novos métodos de transações, demandando uma reforma célere da legislação existente.

A União Europeia, utilizando o Tratado sobre o Funcionamento da União Europeia como forma de fundamentar os seus poderes, propôs uma alteração à diretiva 4.ª AML, com o objetivo de reduzir o anonimato das cripto-moedas. Não tendo sido ainda aprovada, a capacidade desta alteração produzir a resposta adequada aos desafios apresentados pela natureza especial das moedas virtuais é, no mínimo, questionável.

O trabalho aqui apresentado analisa a atual legislação europeia contra o branqueamento de capitais e a sua capacidade de responder às características das moedas virtuais, às quais se atribui um elevado risco. Tem também como objetivo salientar questões relativas a esta temática e despertar maior interesse, assim como contribuir para o futuro da regulamentação AML/CFT da União Europeia.

Palavras Chaves: Moedas Virtuais, Cripto-moedas, Anti-Branqueamento de Capitais, Combate ao Financiamento do Terrorismo, Lei Europeia, Cooperação Judicial em Assuntos Criminais.

Table of Contents

Abbreviations

AML - Anti-Money Laundering

AMLD- Anti-money Laundering Directive

BaFin- The Federal Financial Supervisory Authority

BTC – Bitcoin

CDD – Customer Due Diligence

CFT- Counter Financing of Terrorism

CNAS – Center for a New American Security

COE – Council of Europe

DTL – Distributed Ledger Technology

EBA – European Banking Authority

ECB – European Central Bank

ECON – The Commission for Economic Policy

EDD – Enhanced Due Diligence

EMD – Electronic Money Directive

FATF – Financial Action Task Force

FBF – French Banking Authority

FBI – Federal Bureau of Investigation

FIU – Financial Intelligence Unit

IMCO – Committee on Internal Market and Consumer Protection

KYC – Know Your Customer

PAD – Payment Account Directive

PEP – Politically Exposed Person

PSD – Payment Services Directive

SAR – Suspicious Activity Report

SDD – Simplified Due Diligence

TEU – Treaty on European Union

TFEU – Treaty on the Functioning of the European Union

UBO – Ultimate Beneficial Owner

VC – Virtual Currency

Introduction

World Wide Internet is considered a valuable communication channel which allows individuals to interact with each other (peer-to-peer communication) from one place to another, instantly. While in its first times, there were very few contents that you could find on the internet, it transformed into the primary source of information with its wide range of content and of communication allowing people to conduct peer-to-peer communication. Innovations in information and communications technologies, including the mobile phones and internet, changed the way of conducting business and revolutionize commerce, marketing and the economy.

E-commerce emerged as a result of the innovations in information technologies which made business-to-consumers (B2C) sales and business-to-business (B2B) commerce possible through electronic market platforms. It allowed a better access to markets and products, reduced the time for market research and made the transactions faster for the consumers and businesses. Nowadays buyers can access the wide range of products from the stores all over the world, choose and buy the one that suits them the best at their homes. E-commerce, in a very short-time, became one of the milestones of the world economies and global retail e-commerce sales is expected to reach $4.5 Trillion by 2021[1].

Widespread usage of the electronic market platforms (online shopping) and electronic banking forced traditional payment systems (using checks or cash) to change and they eventually were replaced by the "electronic payment systems to pay for goods and services electronically through an electronic medium"[2]. PayPal is one of the most popular electronic systems which allows users "to send and receive money and to make an online payment"[3] through their PayPal digital wallet. Online payment methods include bank transfers, credit and debit card requiring intermediaries as well as the alternative payment services and service providers that are emerged recently such as Bitcoin removing the third trusted party.

[1] Orendorf A. (2017), "*Global Ecommerce Statistics [Infographic] and 10 International Growt Trends You Need to Know*". Retrieved from https://www.shopify.com/enterprise/global-ecommerce-statistics. [Accessed on 01.02.2018].

[2] SecurionPay, "*What is an E-payment System?". Retrieved from* https://securionpay.com/blog/e-payment-system/. [Accessed on 23.02.2018].

[3] PayPal, Home Page. Retrieved from https://www.paypal.com/uk/webapps/mpp/home. [Accessed on 23.02.2018].

Virtual currency, more specifically cryptocurrency[4], emerged as a peer-to-peer electronic payment system eliminating the electronic medium. Its creation was a result of the financial crises of 2008 which reduced individual confidence on financial institutions and the services they provide.

Bitcoin is the most prominent cryptocurrency with $160B market capacity, allowing transactions to occur between any two parties. Due to the removal of the intermediary, transaction does not require a bank account, gains speed and proceeds without being subjected to any fee or arbitrary limits of transfer. The technology behind it, called Blockchain prevents double-spending that is based on cryptographic proof rather than trust.[5]

Usage of virtual currencies, more specifically cryptocurrency, has grew in numbers due to its easy, fast and cheap nature comparing with traditional payment methods. Along with its benefits, the system is not invulnerable to risks, namely money laundering and terrorist financing abuses, since it allows greater anonymity than traditional electronic payment systems and monitored by no authority. Despite the transparency of the transfer of funds, sales through anonymous digital wallets enables launderers to conceal the origins of illegally obtained money and hardens the surveillance of the money flow. Besides, its international transmissibility allowing access through internet and cross-border transfers increases the risks related to money laundering and terrorist financing.

Despite its widespread usage and invulnerability to risks, it operated free from regulation for a long time. However regulators took a notice on the issue after facing with various cases namely Liberty Reserve, Silk Road and Western Express International, involving the usage of virtual currency for the purpose of criminal activities, namely drug trafficking, armament and fraud.

Furthermore, some Bitcoin wallets were found that were related to some terrorist groups in Gaza Strip and to Daesh to fund their activities. Responses were various and distinct to these risks, while some countries opted to ban trade in virtual currency (China), some

[4] A type of virtual currency which can be used to purchase real goods and services of the market. The way of operation of crpytocurrencies are decentralized, hence there is no authority that issues, controls and monitors the currency. Furthermore, the currency allows users to keep themselves anonymous.

[5] Nakamoto, S. (2008), "*Bitcoin: A Peer-to-Peer Electronic Cash System*", p.1.

opted to issue licenses to the virtual currency exchangers[6] (New York State Department of Financial Services- BitLicense), subjecting them to specific requirements with the purpose of reducing client anonymity.

The European Union, on the other hand, adopted an incremental approach. Despite, the need of the European Regulation on virtual currency was raised for the first time in 2012, the European Union dealt with the issue on a theoretical level only, until 2016. An amendment to the 4th AML Directive was proposed on June 2016 as a part of Commission Action Plan against terrorist financing, following the Paris terrorist attack, aiming to bring virtual currencies under the scope of the Directive, requiring virtual currency exchangers to comply with customer due diligence and know your client (KYC) methods as it requires from financial institutions among others. Having not been accepted yet, its adequacy in responding to virtual currencies is questioned due to the special characteristics of virtual currencies.

Technology is faster than law making. When law seeks to regulate only a decade old technology, which might be still unfamiliar to many regulators, firstly the unique and distinct characteristics of that technology should be understood and embraced. Since it is a "new" reality, a wide spectrum of issues that might arise from that technology should be thought carefully. Moreover, along with its risks, benefits should be kept in mind not to hinder further development. Without taking all these factors mentioned above into account, regulations could be unable to fight effectively the abuses of that technology.

This thesis aims to study EU's Anti-Money Laundering Legislation and its application to Virtual Currency, with particular attention to cryptocurrency due to its decentralized and universal nature. In order to carry out research, the thesis is based on the main research question: "Is current AML/CFT Law of the European Union adequate in dealing with virtual currency?".

Assessment will be done by taking special characteristics of virtual currencies attributable to the risks into account; anonymity, international transmissibility and decentralization, and answering the question of whether these characteristics received a response from the proposal directive on AML or not. Instead of solely defining what virtual currency is and how it is regulated, the present investigation seeks to adopt a critical approach against

[6] According to the definition of FATF Report, exchanger is a person or entity engaged as a business in the exchange of virtual currency for real currency.

current AML/CFT regulations of EU, highlighting its strengths and inadequacies. When needed, it will propose a solution to for the transformation of virtual currency into a AML-compliant electronic payment system.

Part I. Money Laundering and Formation of International Anti-Money Laundering Regime

1. International Money Laundering

i. Basic Concepts

The concept of Money Laundering refers, in general terms, to the process of cleaning the illegal earnings (dirty money) that are obtained from criminal activities such as corruption and bribery, drug-trafficking, extortion, human smuggling, illegal gambling, tax evasion, weapon smuggling and terror financing.

Holding great amount of dirty money, mostly obtained in cash, can be held as the proof of a criminal offence. Linkage between the crime and the criminal would become more evident and take the notice of authorities. In order to prevent prosecution, criminals wish to create an appearance in which the proceeds of crime seem to have its origins in legal sources. Therefore, by transferring dirty money through legitimate channels into the clean accounts, they disguise the illegal origins. By laundering the proceeds of crime, the criminals mainly aim to accomplish two things: to be distanced from the predicate offence and to be able use the illegally obtained money in the mainstream market without being caught by the authorities.

The concept of Money Laundering is as old as the money. The historian Sterling Seagrave, in his book *Lords of the Rim*[7], has written how Chinese merchants hid their wealth 3000 years ago from the rulers because they were afraid that the rulers would take away the profits and assets deriving from trade. Hence they developed techniques such as converting money to removable assets and investing on businesses that were out of Chinese jurisdiction.

Despite the fact that money laundering is as old as the money itself, it was not criminalized until a very recent date. Previously what mattered was the criminalization of the predicate offence that lies under the money laundering and the prosecution of that offence.

It is believed that the concept of money laundering is originated in the time of Prohibition (1920-1933) in the United States, where the production, importation and sales of alcoholic beverages were banned by the constitution. It is believed that enormous amounts of money were laundered in that time[8], by gangsters, including Al Capone. Criminals

[7] Seagrave, S. (2012), "*Lords of the Rim*". Corgi.

[8] Muller, W. H. & Kalin, C. H. & Goldsworth, J. G. (2006), "*Anti-Money Laundering: International Law and Practice*". John Wiley & Sons Ltd, p.3.

benefitted from the Prohibition and generated enormous amounts of cash by smuggling alcohol. Cash generated from the organized crime[9] was hidden through investments in legitimate businesses like cash-only laundromats in order to disguise the origin of the source and consequently to avoid criminal prosecution. Since then the laundry analogy is commonly accepted and used[10], for the processes of cleaning dirty money.

One should not be confused by the wording of the concept as what is laundered cannot be limited only by money. It includes all the assets that are obtained by carrying out a criminal offence. If earned as a result of an offence, luxury cars, jewelry, luxury watches and properties are considered as proceeds of crime. Anything of value can be laundered.[11]

ii. The Process of Money Laundering

Money laundering is a complex process that can be realized by using various methods, all containing three phases: placement, layering and integration. It should be kept in mind that there is always a primary offence or offences before the money laundering process which gives rise to the illegal funds.[12]

Placement is the initial phase to start to the money laundering procedure. After obtaining illegitimate funds from criminal activities, the fund has to be transferred from its original form, mostly cash, to another form. Aim of this phase is to place the dirty money into the legitimate financial system. This stage of the money laundering can be carried out by various methods such as purchasing of paintings or antiques, acquisition of stamps and coins, buying chips at a casino, acquiring shares in private companies or placing funds into a banking system.

For example, a government official received a bribe of €10000 in cash. In order to not get caught and charged by corruption offences, he buys shares from a company. He successfully places his money in the legitimate financial system. The profits derived from the shares would have a legitimate source since he is receiving dividend as a shareholder, from a legitimate business.

[9] Not by only smuggling alcohol but also through prostitution, extortion and illegal gambling.

[10] Turner, E. J. (2011), "*MONEY LAUNDERING PREVENTION, Deterring, Detecting, AND Resolving Financial Fraud".* John Wiley & Sons, Inc., p.2.

[11] Sullivan, K. (2015), "*Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business*".Apress, p.16.

[12] Cox, D. (2014), "*Handbook of Anti Money Laundering".* WILEY, p.7.

Another example would be if a drug dealer visits a casino and buys chips in exchange of illegally obtained money. After playing at different tables for couple of hours, he returns the chips that are remaining in his hand and leaves the casino. By doing this, he would place the dirty money into the legitimate financial system (placement) and distance the money from its origins (layering).

Layering phase is the second stage of the money laundering process and the most complex one. In this stage, the criminal's objective is to distance the funds from their origins. Launderers can use various methods to disguise the origin of the money. One of the most applied method is the movement of funds between various bank accounts in jurisdictions where the Bank Secrecy Laws are very strict such as Cayman Islands, British Virgin Islands and Panama. It is known that, in a sophisticated layering stage, funds can spin up to 10 times before the last stage.[13]

In the aftermath of the layering phase the relation between the origin of the funds and the current position of the funds becomes ambiguous. The audit trail is so obscured that the investigation on the source of the money becomes harder. Hence, during or in the aftermath of the initial stage, authorities have higher chances to detect the launderer than in the aftermath of the second stage, layering.

Additional to the movement of funds internationally, the launderer may opt to purchase paintings, antiques and precious gems at shops, auctions or flea markets and properties. However since various authorities are involved in the process of purchasing a property like lawyers, holding activities individually would be less risky for the launderer. For instance, if the criminal purchases a valuable painting at an auction or an antique store, there will be no party involved in the process that has the obligation of carrying out anti-money laundering measures.

The final phase of the money laundering, called integration refers to the re-entry of the cleaned money into the mainstream economy. Cash being placed in the economy and layered, returns to the launderer as a legitimate earning to be used in any purpose. Launderer then can purchase luxury items.

In order to carry out a successful integration phase, the cleaned money must appear to be derived from a legitimate source and purchases done by the launderer must not draw

[13] Cox, D. (2014), "*Handbook of Anti Money Laundering".* WILEY, p.17.

attention. The launderer might invest the money into a legitimate business and claim payments by creating fake invoices for the services that were not provided or were provided for less amount of money.

iii. Money Laundering Schemes and Methods

There are various methods of money laundering which are constantly evolving to circumvent the existential money laundering laws. Criminals develop new techniques every other day to avoid prosecution. While it is impossible to provide an exhaustive list of schemes, most commonly used methods are highlighted below, including laundering through financial institutions and non-financial businesses and/or professions.

Cash Smuggling

Cash smuggling is one of the most frequent method that is used by the launderers which refers to the shipment of large sums of cash across borders, to where the Bank Secrecy Laws are strict. Since every country has its threshold of carrying cash legally across the border, launderers hide the bulk of cash in a cargo, boat or on a person. Due to the strict border controls, criminals have been developing new techniques to smuggle money across borders without being noticed. Cars that have hidden compartments called 'traps' are one of the most applied shipment tools when it comes to cash smuggling. Once the cash is taken offshore, the launderer can deposit it to a bank (placement) and proceed to the second phase.

As mentioned previously, a person might carry the large sums of cash on her, hidden in a personal belonging. A unique case of cash smuggling occurred in 2014 where a 40-year-old woman was arrested by Dominican Republic Officials, who was carrying more than $70K in her stomach and more $69K in her suitcase which was believed to be linked to drug trafficking[14].

Drug Enforcement Administration (DEA), in 2015's National Drug Threat Assessment, reported that, "Currently, bulk cash smuggling is still the most widely-reported method used by [transnational criminal organizations, or TCOs] to move illicit proceeds."[15]

[14] New York Post News. (2014), "*Woman arrested with over $70,000 in her stomach". Retrieved from* http://nypost.com/2014/10/25/woman-arrested-with-over-70000-in-her-stomach/. [Accessed on 10.11.2017].

[15] U.S. Department of Justice Drug Enforcement Administration, DEA Strategic Intelligence Section. (2015), "*National Drug Threat Assessment Summary"*.

According to the report, over 4000 bulk cash seizures were held in 2014 with the total over $383M.

Casinos

Casinos are great places for money launderers which could be used both for the placement and the layering phase. The technique is very easy: the launderer places his illegally obtained money into the financial system by buying chips from legitimately operating casinos and cashes them back in the check-out. If any financial institution raises doubts on the origin of the money, the launderer would have a reasonable answer. Having various accounts in different casinos located in different jurisdictions would furthermore help him/her to distance the funds from their criminal origin.

Structuring (Smurfing)

Structuring refers to the act of splitting large sums of cash into smaller amounts below the currency reporting threshold. It is also called smurfing due to the fact that the launderer sometimes hires individuals (smurfs) to deposit the money from different places in small amounts to the same account. Structuring is a method of the placement phase. Once the total amount it deposited to the bank without being reported, the launderer can proceed to the second stage.

Wire Transfers

Wire transfers refers to the electronic transfers of money through banks or credit unions. While being a great part of a legitimate business' day to day operation, it is commonly used by launderers for the layering phase. Wire transfers are used by launderers in the conjunction of offshore accounts and shell companies.[16]

Offshore Bank Accounts

Offshore bank account refers to the accounts opened at a bank located in jurisdictions that have less controlling legal regulations and strict banking secrecy laws. By providing privacy, easy access to deposits, protection against investigation, low or non-taxation rates, they attract investors. Offshore financial centers (OFCs) have an important role for

[16] Sullivan, K. (2015), "*Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business*".Apress.

Cox, D. (2014), "*Handbook of Anti Money Laundering".* WILEY, p.19.

hiding identity and the ownership of the assets.[17] These accounts are used by the criminals in the layering stage, in order to obscure audit trail. The most popular offshore banking centers are Cayman Islands, Panama and British Virgin Islands.

Shell Companies

"Shell companies are businesses without substance or commercial purpose and incorporated to conceal the true beneficial ownership of business accounts and assets owned"[18], in the countries that have lax anti-money laundering regulations. Despite the fact that the incorporation of these companies is not illegal they are mostly associated with shady business practices such as tax evasion, money laundering and to criminals who wish to circumvent international sanctions.

The process starts with setting up a company in one of those abovementioned countries. An offshore financial service provider that offers financial secrecy to its client registers the company without disclosing the information on the ownership. To ensure the safety, the launderer may opt to create series of companies that are registered in different countries with each one owning the previous one. In this context, the complex chain of ownership would distance the beneficial owner from the ownership of the companies. Once the company is set, it can act as a real natural entity, as it may purchase goods and services on the behalf of the owners, open a bank account or hold assets. Upon the formation of the company, the dirty money can be deposited to the shell company's bank account. Replaced money then can be used to buy luxury goods, be transferred to the launderer's illegitimate business for further purchases or to a terrorist group to finance violence, and to promote an election campaign. Since the ownership information is not disclosed by the tax haven, the owner of the assets can avoid income tax, tax on capital gains or corporation tax of the residency company.

On April 2016, 11.5 million documents were leaked from a Panamanian law firm Mossack Fonseca, containing information on how the global law firms and banks were helping their clients to evade tax, launder money and circumvent trade sanctions by providing them financial secrecy through offshore services such as shell companies and

[17] European Parliament, DIRECTORATE GENERAL FOR INTERNAL POLICIES, ECONOMIC AND SCIENTIFIC POLICY, Economic and Monetary Affairs. (2017), "*Offshore activities and money laundering: recent findings and challenges*".

[18] European Parliament, DIRECTORATE GENERAL FOR INTERNAL POLICIES, ECONOMIC AND SCIENTIFIC POLICY, Economic and Monetary Affairs. (2017), "*Offshore activities and money laundering: recent findings and challenges*". p.20.

offshore accounts. Panama Papers revealed the names of head of states, politicians, celebrities and billionaires from all around the world and proved again the corrupted and criminalized nature of the offshore world.[19]

Paradise Papers[20] furthermore made it clear that as long as the beneficial owners[21] of all companies are not disclosed, corrupt politicians, tax evaders and the other criminals will continue to use offshore companies to conceal their identity and to move their money across the globe.

Fake Invoices

Money Launderers commonly use generation of fake invoices in the layering phase of money laundering program. Export and import businesses are mainly benefitted for the laundering offence. Both high valued and low valued invoices are used by the criminals.

For instance, a criminal purchases phones with the illegally obtained money and he exports these phones through an importer to another country. Despite the fact that the shipment has the value of $700K, it was invoiced at the value of $100K. When the importer sells the phones in the receiver country, it sells it for its real value and profit $600K from the sales, which represents the laundered money. This way, the source of importer's profit would appear to be legitimate while the exporter pays tax only on the income that he claims to generate.

Underground Banking

Underground banking refers to any financial operation outside the traditional regulated banking sector, consequently outside of the supervisions of governments. It is known by different names in different parts of the world. While in India it is called Hundi, in Asia it is called Hawala which means "transfer" in Arabic. Operations are always conducted in cash but there is no actual movement of the money to be tracked.

[19] The Panama Papers (2016) "*Giant Leak Of Offshore Financial Records Exposes Global Array of Crime and Corruption. Retrieved from* https://panamapapers.icij.org/20160403-panama-papers-global-overview.html. [Accessed on 12.11.2017].

[20] Second biggest data leakage in history published in November 2017.

[21] FATF defines beneficial owner as "the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate eff active control over a legal person or arrangement." *See* FATF. (2012), "*INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION, The FATF Recommendations".* P. 110. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf. [Accessed on 10.11.2017].

For example, John wishes to send €1,000 to Mary who resides in another country. John finds a hawala broker, Tom, and give him €1,000, in cash, to be received by Mary. Tom contacts with another hawaladar, Jane, in the country of Mary and asks her to give €1,000 to Mary. Mary gets the money from Jane minus a commission. In the end of the transaction Tom owes €1,000 to Jane. All credit and debit transactions are recorded in a book by hawala dealers and settled afterwards.

As one may see, the system, unlike traditional remittance networks, is solely based on trust in hawala network. Despite its common usage for legitimate reasons, it has been attributed to tax evasion, money laundering and terrorist financing based on its anonymity and untraceable nature.

2. Formation of International Standards for Anti-Money Laundering Laws

Despite the fact that money laundering operations have been carried out for more than 3,000 years, it was not considered as a crime in any jurisdiction until the United States Money Laundering Control Act of 1986. The Act was a response to the growing numbers of money laundering cases and its undeniable linkage to drug cartels. By concealing the existence of illegal gains and legitimizing the source, money laundering schemes were making the prosecution of the criminals harder. Furthermore, enormous profits generated by the criminals and government's inability to seizure those profits were contributing to the expansion of criminal activity and to the increase in the life span of criminal groups.[22]

Criminalization of the money laundering was adopted as an instrument to fight against its predicate offence which in the context of the late 1980s was narco-trafficking. It was a part of the policy on "War on Drugs" of United States, declared during the Nixon administration.

In June 1980, the Council of Europe published a recommendation on measures against the transfer and the safekeeping of funds of criminal origin[23], warning the Member States

[22] Gurule, J. (1995), "*The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity?*" Scholarly Works, Paper 21, p. 824. Retrieved from https://scholarship.law.nd.edu/law_faculty_scholarship/21/?utm_source=scholarship.law.nd.edu%2Flaw_faculty_scholarship%2F21&utm_medium=PDF&utm_campaign=PDFCoverPages. [Accessed on 15.10.2017].

[23] COUNCIL OF EUROPE, COMMITTEE OF MINISTERS. (1980), "*RECOMMENDATION No. R (80) 10 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON MEASURES AGAINST THE TRANSAFER AND THE SAFEKEEPING OF FUNDS OF CRIMINAL* ORIGIN". Retrieved from https://rm.coe.int/16804f6231. [Accessed on 09.08.2017].

on the issue and recommending them to take important steps to ensure that their financial institutions are adopting such measures. This led to the adaptation of the similar laws in various member states such as France[24], United Kingdom[25] and Portugal[26].

Not long after, it became evident that confronting with the challenges posed by money laundering by just relying on unilateral domestic measures was not sufficient. In the advent of the globalization, financial systems were so intertwined that money laundering was transformed into a transnational criminal activity. National governments that had already criminalized money-laundering pressed the international community to act on this context[27], with the purpose of strengthening cooperation across national boundaries and fighting with the criminal offences more effectively and efficiently. National Laws, outlawing money laundering, assisted agencies across the globe and contributed to the formation of international standards of anti-money laundering (AML) laws.

International efforts to fight with money laundering and its predicate offence started to be held by the late 1980s. It aimed to form international standards, containing prohibitory and preventative measures.[28] Their objective was to protect the stability and the integrity of the financial system; to provide a disincentive to economically motivated crimes through the reduction of profit and to decrease the inflow of illegal money that can finance further crimes; and to provide effective tools for the prosecution of money laundering and predicate offences.[29]

[24] Loi n° 87-1157 du 31 Décembre 1987 relative à la lutte contre le trafic de stupéfiants et modifiant certaines dispositions du code penal and Loi n° 88-1149 du 23 Décembre 1988 de Finances pour 1989 . Retrieved from https://www.legifrance.gouv.fr/. [Accessed on 08.10.2017].

[25] UK Drug Trafficking Offences Act 1986. Retrieved from https://www.legislation.gov.uk/ukpga/1986/32/introduction. [Accessed on 08.10.2017].

[26] Decreto-lei n.° 15/93 de 22 de Janeiro 1993, Legislação de Combate à Droga. Artigo 23.°, Conversão, transferência ou dissimulação de bens ou produtos. Retrieved from http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=181&tabela=lei_velhas&nversao=1&so_miolo. [Accessed on 08.10.2017].

[27] Hülsse, R. (2007), "*Creating Demand for Global Governance: The Making of a Global Money-Laundering* Problem". pp.166.

[28] Alldridge, P. (2008), "*Money Laundering and Globalization*". Journal of Law and Society, Vol. 35, No. 4 (Dec., 2008), pp.442. Retrieved from https://www.jstor.org/stable/40206861?seq=1#page_scan_tab_contents. [Accessed on 21.10.2017].

[29] Ioannides, E. (2014), "*Fundamental Principles of EU Law Against Money Laundering*". Ashgate Publishing Company, pp.7.

Foundations of the AML laws were laid respectively by 1988 UN Vienna Convention[30], 1990 Council of Europe Strasbourg Convention[31], 2004 UN Palermo Convention[32], 2005 Council of Europe Warsaw Convention[33], and 1990, 1996, 2004 and 2012 Recommendations of the Financial Action Task Force. While formed around the same objective, each Convention and Recommendation were held to respond a distinct concern. With the introduction of every new challenge to the combatting of money laundering, the international regime on anti-money laundering laws has changed to respond effectively to those challenges.

Having its origins on narco-trafficking, scope of AML laws was broadened in accordance with the social and political concerns of the time. By the 1990s, some non-drug related offences were incorporated into the AML laws. It was considered crucial to include them into the context of the AML laws due to their transnational nature and severity. Those offences were considered as serious crimes which is controlled and carried out by powerful groups of criminals in a large scale and for long period of times, such as arms trafficking and human smuggling. In the early 2000s, the scope was broadened once again. The fear of and the concern on terrorism, in the aftermath of 9/11, led to the incorporation of the terrorism offences such as the funding of terrorism, into the AML Laws. 2012, FATF identified a new challenge to the combating of money laundering. Technological developments and the emergence of virtual currency was found to be the contributing factor for criminals to circumvent the existing AML laws. Identification of the new challenge, just like the previous ones that appeared, forced national and regional legislative bodies to transform their anti-money laundering laws once again.

The evolution of international anti-money laundering laws is examined below in an historical order starting from 1980s. It aims to highlight the nexus between the concerns (social, political and economic) of the era and the transformation of the AML laws. The criteria used for assessment is the scope of AML laws, which divides the evolution into four distinctive periods; narco-trafficking and AML, organized crime and AML, funding

[30] The United Nations (1998), "*The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*".

[31] Council of Europe (COE) (1990), "*Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds of Crime*". ETS NO:141.

[32] United Nations (2004), "*United Nations Convention Against Transnational Organized Crime*".

[33] Council of Europe (COE) (2005), "*Council of Europe Convention on the Prevention of Terrorism*". ETS NO:196.

of terrorism and AML and the new challenges introduced by the technological developments to AML.

i. Narco-Trafficking and Anti-Money Laundering

Growing demand on narcotic drugs, its illicit production and trade were the main political and social concerns of 1970s and 1980s. The popularity of illicit production and trade of narcotic drugs was rising due to its profitability. Various criminal groups involved themselves into these activities to benefit from the demand and to fund their criminal activities further. Political arena not only considered the increase in drug related crimes a threat to the human life but also a threat to the economic, cultural and political foundations of society.[34] Large profits generated by illegal trafficking were inclined to undermine legitimate economies, corrupt the structures of the governments and degrade the principles that society were based on, which led governments to wage war on drugs.

Large sums of proceeds of crime had to be monitored and be subjected to seizure to prevent the financing of further crimes and to provide a disincentive for economically motivated crimes. However, control of the money flow could only be done if the money was found. No prosecution can be held against a criminal without the proof of the criminal's involvement, which is the proceeds of the crime.

At this point, we observe why and how the money laundering became a dear tool for the criminals. It helps criminals to disguise the true nature, the source and the ownership of the criminal proceeds, obscures the audit trail, consequently hardens the supervision of the money flow and complexes the prosecution procedure.

The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, known as 1988 UN Vienna Convention was implemented as a consequence of the 1980s political and social environment. It is the first multinational response embracing the link between illicit trafficking and money laundering which is emphasized in the introduction section of the convention as the following: "The Parties to this Convention are *aware* that illicit traffic generates large financial profits and wealth enabling transnational criminal organizations to penetrate, contaminate and corrupt the structures of government, legitimate commercial and financial business and society at all

[34] The United Nations (1998), "*The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*".pp.10.

its levels, are *determined* to deprive persons engaged in illicit traffic of the proceeds of their criminal activities and thereby eliminate their main incentive for so doing."[35]

With the purpose of preventing the money flow and eliminating obstacles for governments to investigate the proceeds of crime, convention regulates money laundering in two aspects: criminalization of money laundering and allowing for the confiscation of the proceeds of drugs related crimes.

Article 3 subparagraph 1(b) of the UN Convention regulates the criminalization of money laundering. The Article states that "each party shall adopt such measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally: the conversion of transfer of property, knowing that such a property is derived from any offence[36] or from an act of participation in such offence, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence to evade the legal consequences of his actions; the concealment or disguise of the true nature, source, location, disposition, movements, or ownership of property, knowing that such property is derived from an offence..."[37].

Allowance for the confiscation of the proceeds of drugs is regulated in Article 5 of the UN Convention. According to the Article, each party is obliged to identify, trace and free or seize proceeds, property, or instrumentalities for the purpose of eventual confiscation.[38] For this purpose, no party shall try to justify declining to act with the provisions of bank secrecy law.[39] Each party, if the proceeds are situated in their territory, is obliged to submit the request to obtain an order of confiscation to its competent authorities and to submit to its authorities an order of confiscation issued by the requesting party.[40]

[35] The United Nations (1998), "*The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*".pp.10.

[36] A list of offences are stated in Article 3 subparagraph 1 (a). The offences that are regulated in the Convention are all drug related crimes.

[37] The United Nations (1998), "*The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*".

[38] Article 5(2).

[39] Article 5(3).

[40] Article 5(4)(a).

Despite the fact that UN Convention mainly aimed to tackle with the international illicit drug rather than money laundering, it laid down the foundations for international anti-money laundering measures[41].

In response to the growing political concern of the misuse of financial systems by criminals laundering drug money, money laundering became the major issue in 1989 at Paris G7 Summit. The participants, recognizing the threat posed to the banking system and to financial institution[42] , established the Financial Action Task Force (FATF) which aimed to deter and disrupt criminal finance[43]. The Financial Action Task Force was given the responsibility to examine money laundering techniques and new challenges, to establish comprehensive measures to combat money laundering globally, to monitor the countries' progress in implementing the FATF Recommendations.

Since 1989, FATF Recommendations are endorsed to be international standards[44] for the fight against money laundering. By setting out international standards, FATF does not only assist governments to implement coherent, comprehensive and efficient anti-money laundering laws but also contributes to the convergence of AML laws across the globe in national and regional levels[45]. Strengthened global cooperation and approximation of laws produce a more solid weapon against a transnational crime that does not recognize boarders, makes monitoring and reporting of unusual patterns of transactions more efficient.

FATF Recommendations, first issued in 1990, have been revised in 1996, 2001, 2003 and 2012 in cooperation with the regional bodies under the observation of international organizations including the World Bank, the International Monetary Fund and the United Nations. Revision addresses the new challenges anti-money laundering laws are facing with and sets out measures that are relevant and necessary to combat with the introduced threat.

[41] [41] Ioannides, E. (2014), "*Fundamental Principles of EU Law Against Money Laundering*". Ashgate Publishing Company, pp.13.

[42] Zagaris, B. (2015), "*International White Collar Crime, Cases and Materials*". Berliner, Corcoran & Rowe, Washington, DC, 2nd Edition, pp.59.

[43] [43] Ioannides, E. (2014), "*Fundamental Principles of EU Law Against Money Laundering*". Ashgate Publishing Company, pp.12.

[44] FATF produces 'soft law' that contributes to the implementation of 'hard laws'. It creates the best practice with the expectation of compliance.

[45] [45] Ioannides, E. (2014), "*Fundamental Principles of EU Law Against Money Laundering*". Ashgate Publishing Company, pp.12.

The revision's applicability is universal. The differences in the legal and financial systems are identified by the FATF and does not oblige the parties to implement the anti-money laundering framework identical to one another.[46] The principles of the framework allows some extend of flexibility as measures that are used for implementation can be shaped in accordance with the constitutional and regulatory standards of that particular country. This way countries are able to produce and apply more effective measures to combat money laundering.

ii. Serious Offences, Transnational Organized Crime and Anti-Money Laundering

Council of Europe (COE) Convention on Laundering, Search, Seizure and Confiscation of Proceeds of Crime, known as the Strasbourg Convention of 1990, was created with the objective of fighting against serious crime which was considered as an international problem. Whereby the huge profits were considered to contribute to the life span of criminal activities, its method of combat was stated in its Preamble as "to deprive criminals of the proceeds of the crime, achieved through a well-functioning system and fortified international cooperation"[47].

Although it shares the same objective with UN Vienna Convention, The Strasbourg Convention diverges from it since it does not limit the predicate offence solely to drug-related crimes. The Convention extends the scope of money laundering by stating that "predicate offence means any criminal offence as a result of which proceeds were generated that may become the subject of a laundering offence"[48]. While an exhaustive list of predicate offences is not provided by COE, Article 6 (4)[49] gives each jurisdiction the flexibility to identify and determine the offences in accordance with that jurisdiction's perception and categorization of a predicate offence.

The Strasbourg Convention brings a new aspect to the international cooperation by implementing 'spontaneous information' on Article 10. In that context, spontaneous

[46] FATF on Money Laundering (1996), "*The Forty Recommendations*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201996.pdf. [Accessed on 23.10.2017].

[47] Council of Europe (COE) (1990), "*Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds of Crime*". ETS NO:141, p.1.

[48] Article 1 (e).

[49] Article 6(4) of the Convention states that "Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by declaration addressed to the Secretary General of the Council of Europe declare that paragraph 1 of this article applies only to predicate offences or categories of such offences specified in such declaration." *See COE ETS NO:141.*

information means that, if a party considers that a disclosure of an information might assist another party in initiating or carrying out investigations, it may forward that information prior to any request.

Another document that one would find it influential on the extension of the scope of the anti-money laundering regime is the 1990 and 1996 Recommendations of FATF. While Recommendation from 1990 invites each country to consider extending the criminalization of money laundering based on any other crimes, the revised Recommendation of FATF from 1996 obliges parties to extend the scope of the criminal offence of money laundering based on all serious offences. The Recommendation allows some extend of flexibility for countries to identify the serious crimes that are characterized as money laundering predicate offence. However in the Recommendation from 1990, it is also expressed that money laundering offences should be applicable to all serious crimes and to crimes that generate great amount of profits.

The reason of this expansion again can be found in the political and social concerns of that time frame. It was understood that not only narco- traffickers were undermining the financial systems through money laundering. Instead, it was embraced that money laundering became a tool for all criminals to sustain their activities and avoid any prosecution. By broadening the scope, authorities aimed to render existing anti-money laundering laws applicable in various scenarios in which the criminals undermine the financial systems through money laundering and to prevent crimes in a larger scale.

The United Convention against Transnational Organized Crime was published in 2002. The United Nations were concerned by the damaging social and economic effects of organized criminal activities[50]. They highlighted the need to strengthen international and regional cooperation to combat such activities and consequently the Convention, also known as the Palermo Convention, broadened the scope of the international regime.

[50] Organized crime refers to the offences that are controlled and carried out by powerful criminal groups in a large scale, for a long period of time. Trafficking of drugs, human smuggling and arms trafficking were identified as some of the many forms that organized crime could take by the Palermo Convention.

iii. Terrorism and Anti-Money Laundering

Terrorism is the use of violence or threat of violence targeting civilians. They use the fear to accomplish their political, ideological or religious aims. A comprehensive definition adopted at the international level is important for the effective combatting mechanism, however the consensus among the international community has not been reach yet. Different bodies define it distinctively, yet containing the same elements: the use of violence against civilians to accomplish a certain change.

According to the Directive on combatting terrorism of the EU[51], " 'terrorist group' means a structured group of more than two persons, established for period of time and acting in concert to commit terrorist offences"[52]. The Directive criminalizes the offences related to a terrorist group and of offences related to terrorist activities.[53] Offences include receiving training for terrorism[54], to travel for the purpose of terrorism, to provide training and recruit for terrorism offences[55]. Furthermore, committing or contributing to a terrorist offence and collecting or providing funds for terrorism related reasons[56] are punishable under the Directive.

Terrorist groups, in order to build an appropriate environment to carry out their activities, to sustain their position and to expand their reach, raise funds through legitimate sources as from charities, businesses and self-funding and illicit sources as from illegal goods trafficking, human smuggling, credit card fraud and extortion.[57] At this point, the link between terrorism and transnational organized crime cannot be ignored.

September 11th of 2001, the world witnessed the most deadly terrorist attack in the history. The terrorist group, Al-Qaeda held 4 coordinated attacks through four hijacked commercial planes. They were respectively crashed into North and South towers of the World Trade Centre, into Pentagon where the headquarters of the United States

[51] European Union (2017), "*Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing the Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*".

[52] Article 2 (3).

[53] Recital 6.

[54] Recital 11.

[55] Recital 16.

[56] Recital 12.

[57] FATF (2008), "*FATF Terrorist Financing Typologies Report*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf. [Accessed on 03.11.2017].

Department of Defense was located and into Pennsylvania and caused the death of nearly 3,000 individuals.

In the aftermath of the attacks, the overriding imperative of the authorities was to identify and determine the methods to effectively combat with terrorism in the global level. Upon the identification of the importance of terrorist financing networks for the continuation of terrorist groups, authorities included disruption of these networks into their political agenda. Controlling the money flow became the most important tool to combat terrorism.

Despite the fact that terrorism financing and money laundering processes are completely different, same overriding imperative in both cases - to control the money flow- brought combatting of money laundering and financing of terrorism under the same regulations.

In this context, in 2001 the Financial Task Action Force was rendered responsible to introduce measures to deal with the issue of financing of terrorism and assist the countries to implement comprehensive laws. Eight Special Recommendations[58] on Terrorist Financing was published to complete the international standards on combatting of money laundering and financing of terrorism. Integration of the special recommendations produced a stronger set of standards.[59]

COE Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, also known as Warsaw Convention of 2005, was held recognizing the fact that the acts of terrorism by their nature pose a great danger to the fundamental political and socio-economic structures of the countries.[60] In order to prevent any future attack and, if the attack could not be prevented, to prosecute the criminals some measures were implemented. Parties were not only obliged to criminalize the acts of terrorism but also the funding of the terrorism. Financing of terrorism was thought to be mitigated through advanced surveillance system carried out by the financial institutions across the globe. The rationale behind it was to constraint the

[58] FATF (2001), "*FATF Standards, FATF IX Special Recommendations*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf. [Accessed on 23.11.2017].

[59] Cox, D. (2014), "*Handbook of Anti Money Laundering".* WILEY, pp.22.

[60] Council of Europe (COE) (2005), "*Council of Europe Convention on the Prevention of Terrorism*". ETS NO:196.

terrorist groups from their financing tools which would consequently limit their capabilities and their reach and render them vulnerable[61].

Being the first international treaty that obliges its parties to take all the necessary measures for the prevention of both money laundering and the financing of terrorism, the Warsaw Convention structured the most recent international standard for AML laws. With the entrance of the combatting of the financing of terrorism into the scope of AML laws, currently the law is called AML/CFT Laws.

However, some critics have been questioning whether the financial institutions should be bothered to tackle with the issue of terrorist financing or not. Dionysios S. Demetis in his book *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach* supports this argument illustrating some facts on the costs of terrorist attacks. He indicates that amount of money involved in the funding of terrorism varies greatly in which some of the terrorist attacks cost so less that it would be impossible for financial institutions to detect within the pool of daily transactions.[62] Efficiency produced by including financing terrorism into the money laundering agenda can be questioned. Yet, for the purpose of this thesis, the discussion is not carried out further.

iv. Virtual Currency and Anti-Money Laundering

The recent expansion of the scope of AML/CFT Law coincides with the emergence of virtual currency, more specifically cryptocurrencies such as Bitcoin, which introduced an alternative remittance method. It attracted individuals across the globe by providing its users a system that is not centralized on any authority and an online transaction method that is cheaper and relatively faster than the traditional methods. Anonymity[63] that it allows for its users in their transactions facilitated to the realization of its widespread usage.

FATF issued a report in 2014 on *Virtual Currencies, Key Definitions and Potential AML/CFT Risks* which elaborated the virtual currency and its characteristics. Emergence of the virtual currencies was considered a financial innovation in the report, recognizing its potential to improve payment efficiency and to benefit the existing online payment

[61] FATF (2008), "*Terrorist Financing*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf. [Accessed on 13.10.2017].

[62] Demetis, S. D. (2010), "*Technology and Anti- Money Laundering, A Systems Theory and Risk-Based* Approach". Edward Elgar Publishing Limited, ISBN 978 1 84844 5567, pp.33.

[63] Virtual Currency and its characteristics is examined further in Part III.

systems.[64] However, the virtual currency was not found to be beneficial only but also potentially vulnerable to money laundering and terrorist financing abuses due to its particular characteristics: decentralized nature, anonymity and international transmissibility. The report intended to raise awareness of the national and regional authorities on understanding the new technology, so regulatory bodies could develop measures to combat with it more effectively.

On 2015, FATF published a guidance for a risk-based approach to virtual currency. The purpose of the Guidance was stated in subparagraph 6 as "to identify the entities involved in Virtual currency services; and to clarify the application of the relevant *FATF Recommendations* to convertible virtual currency exchangers."[65] FATF expected countries to assess risks related to the virtual currencies and to implement regulatory measures in conjunction with those risks. By guiding the national and regional bodies, the FATF intended to get similar regulatory responses for the purpose of enhancing the international AML/CFT standards.

In the aftermath of the FATF Report and the Guidance, virtual currencies officially took their place in Money Laundering and Terrorist Financing Schemes and Methods next to the traditional tools such like shell companies, underground remittance services and wire transfers.

Regulatory bodies of some jurisdictions have already implemented or are still in the process of implementing laws to prevent criminals to use virtual currency to circumvent existing AML/CFT Laws in compliance with the guidelines set out by FATF. On the other hand, while some of the jurisdictions are still studying to raise a better understanding of Virtual Currency and monitoring its development to set out more effective laws, some are simply banning the usage and the trading of it.

Sufficiency of the regulatory responses or banning could be questioned, however one thing is certain, concentrated efforts have always been the primary imperative for the world to tackle with the transnational crime. Thus without some level of harmonization

[64] FATF (2014), "*FATF Report, Virtual Currencies Key Definition and Potential AML/CFT Risks*". pp.9. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. [Accessed on 18.07.2017].

[65] FATF (2015), "*GUIDANCE FOR A RISK-BASED APPROACH, VIRTUAL CURRENCIES*". pp.3. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. [Accessed on 02.08.2017].

in the laws that are aiming to reduce the risks posed by virtual currency, efficiency of the AML/CFT, in global level, is questionable.

For the purpose of this thesis, it is found important to briefly touch upon the international standards on anti-money laundering and the combatting of terrorism. The international regime is structured around three policies: criminalization of the money laundering offences, introducing prevention measures and the focus on the financial intelligence.

Part II. European Union Anti-Money Laundering Laws

1. Fundamentals

Money laundering, terrorism financing and organized crime are considered to be significant problems threatening the integrity, stability and reputation of the financial system, as well as the single market of the European Union.[66] Money launderers and other criminals involved in financial crimes benefit from the free movement of capital and the services that the European Union single market provides to its member states. Launderers benefit from the intertwined nature of the financial systems at the EU level and ease their program of money laundering and funding of terrorism. For the prevention of such interference with the financial systems and to mitigate abusive activities against the EU financial interests, the union enacts legal acts.[67]

Collaborative actions between the member states of the EU are recognized to be necessary for the implementation of stringent rules. By proposing a minimum level of combating mechanism through legal instruments, the EU aims to approximate the definition of crimes, the sanctions of the offences and the scope of liabilities of the obliged entities across the union. Some level of harmonization in the rules related to the AML/CFT across the EU hinders criminals benefitting from the existing differences in domestic laws of the member states and presents a system of laws in which the union as a whole deals with the issue in the same manner. Furthermore, approximation of the law and regulations facilitates cooperation for the cases of money laundering crossing the borders.

Approximation at the EU level is not the only objective of the European Union. It embraces the cross-border nature of money laundering whose domain is beyond the EU border. In order to produce effective combatting measures, the EU acknowledges the need to follow the path of the concentrated international efforts. Therefore, EU utilizes the international standards on AML/CFT measures introduced through a joint action of the United Nations, the Council of Europe and the Financial Action Task Force (FATF). Soft law that is introduced by that joint action is used as a framework law when materializing the hard law at the EU level.

---

[66] European Union (2015), "*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 purpose of money laundering or terrorist financing*", the 4th AML Directive.

[67] *See* two additional legal acts enacted aiming to protect the financial interests of the EU. The Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of European Public Prosecutor's Office, having regard to the TFEU, and in particular Article 86. And The Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by the means of criminal law, having regard to the TFEU, and in particular Article 83(2).

Revised versions of the recommendations that are published by FATF are important sources for the EU. The EU amends its AML laws in conjunction with the revised versions of the Recommendations in order to respond to new challenges against combatting of money laundering and terrorism financing. As the FATF acknowledges the diverse nature of the legal, operational and administrative frameworks[68], it confers the right to the national and regional bodies to tailor the standards in line with the existing domestic and regional laws. As a consequence, the recommendations taken as a model, the EU adjusts and tailors its AML/CFT laws in accordance with the existing EU treaties and the national laws of the member states.

The AML laws of the EU contains three elements: the criminalization of the money laundering and the financing of terrorism, prevention of money laundering and terrorism financing through obligations imposed on entities, and the utilization of financial intelligence units to enhance cooperation between the entities in exchanging information and analysing reports.

The First AML Directive[69] of the European Union dates back to 1991, following the FATF Recommendations. Its main objective was the prevention of the usage of financial and credit institutions to launder the proceeds of crime, the protection of the financial system and the European single market from the detrimental nature of predicate crimes and money laundering. It criminalized money laundering and imposed obligations to certain private sector entities for the prevention of money laundering. Despite the fact that the outcome it produced was limited, compared to the recent sophisticated AML/CFT laws, the First AML structured the base for the Second, Third and the Fourth AML Directive of the European Union.

Second AML Directive[70] amended and revised the First Directive on the prevention of the use of the financial system for the purpose of money laundering in 2001. Its aim was to enact a more consistent law by utilizing the FATF Recommendations and to eliminate the inconsistencies of the First Directive leading to a limited outcome. It extended the

[68] Nechaev, V. (2014), "*Setting and Implementing Global Standards against Money Laundering and Terrorist Financing*". Speech at Institute of International and European Affairs, Dublin Ireland. Retrieved from http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-iiea-nechaev-feb2014.html. [Accessed on 09.08.2017].

[69] European Union (1991), "*Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering*". 1st AML Directive.

[70] European Union (2001), "*Directive 2001/97/EC on prevention of the use of the financial system for the purpose of money laundering- Commission Declaration*". 2nd AML Directive.

scope of the required entities and broadened the definition of the predicate offence. Inclusion of the authority of identification, tracing, freezing, seizing and confiscations of instrumentalities and the proceeds from crimes was the most important feature of the Second AML.

Third AML Directive[71] was enacted as a response to the political, social and economic concerns of the period in the aftermath of 9/11 terrorist attacks. It took into account the FATF's revised 40 Recommendations and the 8 Special Recommendations related to anti-money laundering and counter terrorist financing standards from 2003. By the implementation of the Third AML/CFT Directive, the scope of the obliged entities were broadened to the legal or natural persons acting in the exercise of their professional activities[72] which were not obliged before, such as the lawyers. By comparing the Second and the Third AML Directives, one may easily observe the transformation of the EU anti-money laundering regime into more comprehensive and a consistent law.

The most recent AML/CFT law at the EU level is the Fourth AML Directive[73] enacted in 2015 with the purpose of improving the uniformity and of responding to the inconsistencies of the AML/CFT rules at the EU level. The modifications that it made on the Third AML Directive can be observed in the areas of customer due diligence (CDD), politically exposed persons (PEPs), ongoing monitoring, risk-based approach and the third party equivalence.[74] The Fourth AML Directive is aligned with the FATF Recommendations from 2012 and the EU charter of fundamental rights.

It is important to mention that there are various instruments implemented by the EU for advancing the agenda to fight against money laundering and terrorism financing. These instruments have a complementary character to the AML/CFT Directive of the EU. Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the community is one of these instruments. Due to the application of the AML Directive to the transactions held through

[71] European Union (2005), "*Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*". Third AML Directive.

[72] Article 2 (3) of Directive 2005/60/EC.

[73] European Union (2015), "*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 purpose of money laundering or terrorist financing*", the 4th AML Directive.

[74] Deloitte (2015), "*The Fourth EU Anti Money Laundering Directive*". Retrieved from https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Laundering_Directive_Deloitte_Ireland.pdf. [Accessed on 19.09.2017].

financial and credit institutions, the cash movements occurring outside of the authority of the financial and credit institutions were found to have the tendency to increase in numbers. Thus in order to prevent it from happening, the regulation targets the cash movements for illegal purposes. Regulation obliges persons entering or leaving the union to declare the amount of cash they are carrying to the competent authorities, whom are obliged to share that information with other authorities in other countries. Passengers are subjected to such obligation if the amount that they carry exceeds the threshold determined in the Regulation. In the context of the Regulation (EC) 1889/2005, that threshold is determined as €10,000 and above.

Another complementary instrument is the Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union. The objective of the Directive is to deprive criminals from their financial gains obtained through illicit activities. In the context of the Directive, financial gains include all proceeds of crime such as the direct gains or benefits from the illegal activities and previously laundered instrumentalities. The purpose of the Directive is to render criminal business methods more risky to provide a disincentive for the criminals and to decrease the number of criminals involved in such activities.

Regulation (EU) 2015/847 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006[75] is another complementary legislative act to the AML Directive. It targets the anonymous transfers which may occur through the payment service providers. The regulation allows the information on the payer and the payee to be provided to the payment service providers for the assessment of the risk level related to a specific transfer. The payment service providers are obliged to check the completeness of the information required on the payer and the payee. They are given the authority to determine whether to execute, reject or suspend a transfer in which the information of the payee and the payer is either missing or incomplete. Furthermore, the regulation obliges the service providers to report suspicious transactions to the competent authorities in conjunction with the reporting requirements regulated under the Directive (EU) 2015/849 (4th AML/CFT) and with the national measures transposing that Directive.[76]

[75] Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds is no longer in force.

[76] European Union (2015), "*Regulation (EU) 2015/847 on the information accompanying transfers of funds repealing Regulation (EC) No 1781/2006*", Recital 24.

Measures in combating the AML/CFT abuses are introduced after a long process of identifying, assessing and understanding the risks. Regulatory bodies take every step carefully to produce such measures to target a specific risk that is previously identified. It is found important, for the purpose of this thesis, to briefly touch upon the current AML/CFT framework at the EU level in order to highlight the measures implemented targeting the identified AML/CFT risks.

Prior to the examination of the 4th AML/CFT Directive, the paper assesses the source of the European Union's power to regulate AML/CFT laws as a part of the EU Criminal Law, taking into consideration the Treaty of the Functioning of the EU and the EU Charter of the Fundamental Rights.

2. EU Powers to Regulate Anti-money Laundering and the Financing of Terrorism

i. European Criminal Law and the AML

The European Union was formed as a community, based on cooperation, to bring peace and prosperity to Europe in the aftermath of the World War II. Throughout its deepening and enlargement process, the EU extended its domain from solely monetary policies to social and political policies. Thus its nature has changed throughout time to build "ever closer union among the peoples of Europe"[77].

Criminal Law of the European Union is relatively a new field of the European Union Law, developed as a consequence of the integration process and still continuing to be developed. The criminal law of the member states are not harmonized fully but some level of approximation has been achieved. The formation of EU Criminal Law can be observed in distinct three periods, from Maastricht Treaty of 1993 until the Amsterdam Treaty of 1999, from 1999 to the Lisbon Treaty of 2009 and from 2009 to onwards.

Maastricht Treaty, dated back to 1993, was the first time in the European Union history where the cooperation in the fields of Justice and Home Affairs was mentioned. The treaty consisted of two separate treaties, Treaty Establishing the European Community (TEC) and the Treaty on European Union (TEU). It structured a pillar system (III Pillar System) that classified the powers of the EU under three groups. The pillars were dedicated respectively to European Communities, Common Foreign & Security Policy and Justice

[77] European Union, Council of the European Communities, Commission of the European Communities (1992), "*Treaty on European Union*". Maastricht Treaty, ISBN 92-824-0959-7. Article A.

and Home Affairs. While the first pillar was subjected to supranational cooperation, the other two pillars were found to be too sensitive to national sovereignty for the supranational cooperation. Hence, those matters were handled with the intergovernmental method laid down respectively in the Title V and VI of the TEU.

Cooperation in the fields of Justice and Home Affairs was acknowledge to be crucial for the success of the single market and the safety the peoples of the Union. It covered the areas of combating terrorism, serious international crime, international fraud, judicial cooperation in criminal and civil matters, controlling illegal immigration and the common asylum policy. In this pillar, unlike the European Communities pillar, the European Union did not have exclusive powers to regulate the abovementioned matters. Under the intergovernmental method, the European Commission and the member states had the equal right to initiative, where the decision making was dependent on the achievement of unanimity at the Council, as stated in Article 42 of the TEU[78].

Pursuant to Article K.6 of the Treaty of European Union, The European Parliament only had a consultative role where the powers of European Court of Justice were limited. In order to strengthen the intergovernmental cooperation, the treaty created a system to exchange information between national police forces known as the European Police Office (Europol).[79]

Under the Maastricht Treaty, the legal instruments were specific to each of the pillars. The instruments to be utilized under the second and third pillar (intergovernmental method) were different than the instruments under the first pillar which were the regulations, directives and decisions. Pursuant to Article K.3 of the TEU[80], the legal instruments for the third pillar were divided into three: joint positions, joint actions and conventions.

Various conventions, which are international treaties governed by the international law, were enacted in the area of criminal law such as the CEO Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime of 1990, Criminal Convention

[78] European Union, Council of the European Communities, Commission of the European Communities (1992), "*Treaty on European Union*". Maastricht Treaty, ISBN 92-824-0959-7. Article 42.

[79] European Union, Council of the European Communities, Commission of the European Communities (1992), "*Treaty on European Union*". Maastricht Treaty, ISBN 92-824-0959-7. Title VI, Article K.1 (9).

[80] European Union, Council of the European Communities, Commission of the European Communities (1992), "*Treaty on European Union*". Maastricht Treaty, ISBN 92-824-0959-7.

on Corruption of 1999 and CEO Convention on the Prevention of Terrorism of 2005. Influence of these conventions in introducing an appropriate legal framework in European Criminal Law was limited since many countries have signed but not ratified the Treaty. In time, closer ties between the member states required a stronger cooperation and consequently implementation of a more effective legal instruments under the third pillar to produce. Criminal law across the EU had to be more harmonized in order to prevent utilization of the diversities in criminal laws of the member states. With the Treaty of Amsterdam of 2009, even though the decision-making process remained intergovernmental, the legal instruments specific to the third pillar gained a more supranational character.

Framework Decisions, stated in the Article 34[81] in the consolidated version of the EU, were introduced to be utilized by the Council in order to approximate the laws and regulations of the member states in Police and Judicial Cooperation in Criminal Matters[82]. Framework Decisions, in their nature, carry similar characteristics with the Directives that are governed by Article 249 of the TEC. They are binding upon the member States as to the results to be achieved but choice of method and form to be applied is left to the member states. However, they do not entail direct effect in any case and it is where they are differentiate from the first pillar community directives.

Direct effect is a principle of EU that was stated by the European Court of Justice in the judgement of *Van Gen den Loos- Case 26/62* of 1963. Direct effect confers rights on individuals and enables them to invoke a provision before a national or European Court.[83] A judge is obliged to interpret a national law in conformity with that particular directive, the EU Law. On the other hand, since the TEU excludes direct effect in Article 34, the framework decision does not directly entails rights and obligations to the individuals.

Pursuant to Article 35, framework decisions under the TEU were only subject to the preliminary rulings to be interpreted by the ECJ. The ECJ did not have jurisdiction to review the validity, proportionality of operations carried out[84], to review the legality of

[81] European Union (1997), "*Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, signed at Amsterdam 2 October 1997*". TEU Consolidated (1997), ISSN 0378-6986. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1997:340:FULL&from=EN. [Accessed on 07.09.2017].

[82] Name of the third pillar was changed with the Amsterdam Treaty.

[83] European Union, "*The Direct Effect of European Law*". Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14547. [Accessed on 07.11.2017].

[84] TEU Consolidated (1997). Article 35(5).

framework decisions and decisions in actions brought by a member state or the Commission on grounds of lack of competence, infringement of any procedural requirement[85] and to rule on any dispute between member states regarding the interpretation or application of acts[86]. In another words, non-compliance due to failure to transpose or non-transposition could not give rise to any sanctions on the member states. Furthermore, the Commission was not given the power to monitor the implementation of the framework decisions. Pursuant to Article 36(2) Commission was to be fully involved in the area of police and judicial cooperation but does not hold the power to act upon infringement.

Until 2009, the Treaty of Lisbon, many Framework Decisions were adapted in the third pillar based on the principle of mutual recognition[87]. The Principle was established in the Tampere meeting of the European Council on 1999 and is considered as one of the main contributors for a stronger cooperation in police and judicial matters. By adopting this principle, centralized policies were abandoned and mutual recognition in the decisions of member states was enhanced.

Mutual recognition means that a decision taken by a member state on a specific case may be applied by another member state, when faced with a particular criminal case similar to the case decided previously. The principle does not only contain the recognition of judgements but also recognition of the definition of the offence, recognition of the offender and offence, recognition of the legal liabilities and the recognition of the penalties. Hence, mutual recognition in criminal law creates standard combatting mechanism and brings the criminal laws of the member states closer to one another.

With the implementation of Framework Decisions in conformity with the principle of mutual recognition and the Charter of Fundamental Rights of the EU, the EU criminal law started to be shaped. From the Amsterdam Treaty and onwards, the third pillar, Police and Judicial Cooperation gained a more supranational character. However, due to the nature of the framework decisions, especially the lack of sanctions for non-implementation, the framework decisions were also not sufficient to provide a

[85] TEU Consolidated (1997). Article 35(6).

[86] TEU Consolidated (1997). Article 35 (7).

[87] Mutual recognition was first applied to the economic sphere of the EU Law. It enables the sales of a product in a member states, if that product is lawfully sold in one member state of the EU. It promotes the free movement of goods and guarantees the market access for all products even if there is no harmonization related to that particular product.

harmonized legal framework at the EU level. To provide an adequate response, the Lisbon Treaty was adopted and new measures were introduced.

The three pillar structure, as well as the different legal instruments under each pillar was abolished by the Treaty of Lisbon in 2009. It amended the Treaty on the European Union and the Treaty Establishing the European Community and gave EU a single legal personality. The amendment, the Treaty of the Functioning of the European Union (TFEU), harmonized the legislative instruments in the area of criminal law where the framework decisions and the conventions were replaced by the directives and regulations. By changing the legal instrument regarding the criminal matters, the legal acts created consistency in the common legal system of the EU and strengthened the combat against serious crimes which has a transnational nature.

The decision making process along with the method of cooperation in criminal matters have gained a supranational character with the enactment of the TFEU. The sovereignty of the member states was limited to regulate the criminal matters while the power of the European institutions was extended.

Unlike in the previous legal acts, with the enactment of the TFEU the Commission is conferred the sole right of initiative, rather than sharing that right with the member states. Decision making process regarding the criminal matters remained in the competence of the Council but the rights of the European Parliament was extended in a way that the Parliament attained the power to suspend a proposal. By conferring rights to the European Parliament, the process of regulating criminal matters gained a democratic character. Unanimity rule in decision making procedure on the other hand was replaced by the qualified majority voting which ruled out the possibility of a simple veto to bring a proposal to an end as a consequence of the departure from intergovernmental method of cooperation.

Since the enactment of the TFEU, the Commission is conferred the power to monitor the implementation of the provisions by the member states. Following the Article 258 of the TFEU, if the Commission considers that a Member State has failed to fulfil an obligation under the Treaties, it may initiate an infringement action against that member state and bring the matter to the ECJ.

Furthermore, ECJ does not have a limited role in regulating the criminal matters. Pursuant to Article 220, when the Commission brings a case before the Court, if the ECJ finds that

Member State has failed to fulfil an obligation under the Treaties and infringed the EU law, the ECJ has the right to impose a penalty payment on the member state. Thus the Court ensures the uniformity of the implementation of the Union Laws and compliance.

Chapter 4 of the TFEU regulates the judicial cooperation in criminal matters between Articles 82 to 86. According to the Article 82 of the TFEU, principle of mutual recognition of judgments and judicial decisions lies in the core of the judicial cooperation in criminal matters. The European Parliament and the Council are given the responsibility to establish minimum rules by means of the directives related to mutual admissibility of evidence between member states; the rights of individuals in criminal procedure; the rights of victims of crime and the any other aspects of criminal procedure identified by the Council.[88] The directives do not restrain member states to adopt stricter provisions, as long as the minimum rules are met.

There are various legal legislations that are adopted under the TFEU aiming to harmonize the criminal laws and regulations of the member states for the appropriate protection of the Union policies. As regard to the Article 83, it is European Union's competence to regulate criminal matters regarding the certain areas in combatting with serious crimes with a cross-border dimension. Areas of crime are non-exhaustively listed in Article 83 where its domain may be extended by the Council due to the developments in crime. Indicated areas of crime include terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug and arms trafficking, corruption, money laundering, counterfeiting of means of payment, computer crime and organized crimes. Whenever the nature of the crime or the effect of the crime leads to the need to combat in common grounds[89], the European Parliament and the Council together may utilize one of the instruments such as a directive, in accordance with the ordinary legislative procedure regulated in Article 294.

In accordance with the Article 83 of the TFEU, it is European Union's competence to regulate matters related to money laundering and the financing of terrorism since the nature of the crime and the effect of the crime lead to the need to combat in common grounds. AML/CFT laws are a part of the criminal law of the European Union, regulated

[88] European Union (2012), "*Consolidated Version of the Treaty on the Functioning of the* EU". The Lisbon Treaty, Article 82(2).

[89] TFEU, Article 83.

to protect the financial interests of the European Union and to produce appropriate measures to prevent the misuse of the financial system.

ii. Fundamental Rights and Freedoms and the AML

In the treaties of the EC, the Fundamental Rights were neither explicitly included nor was made legally binding other than in few articles such as the Article 7 of the EEC treaty prohibiting discrimination on the grounds of nationality or the Article 119 of the EEC ensuring the equal payment for men and women.[90] It was solely a declaratory document which had no legally binding effect. As a consequence, it was leading to the problem of having two levels of fundamental rights within the EU regarding the rights of the criminal and the victim. By the enactment of the TFEU and the enhancement efforts to harmonize the laws and regulations of the member states, the Charter of Fundamental Rights[91] became a part of the European Treaties.

The Charter have become legally binding upon the EU institutions as the primary EU law. Thus, whenever the EU institutions are legislating new laws for the realization of the union policies and member states are acting within the scope of the EU law, fundamental rights and freedoms, as well as the rule of law must be complied.

Incorporation of the Charter into the Treaties led to the elimination of the differences in the level of rights and freedoms within the EU and the enhancement of the application of the principle of mutual recognition in criminal law. Furthermore, since the Charter became legally binding for EU institutions in enacting laws, it was easier for Member States to limit their sovereignty in the area of law that intervenes with the internal matter such as the criminal law.

Preventive measures in fighting with money laundering and the financing of terrorism may appear to be violating the fundamental rights and freedoms indicated in the Charter since it limits some of the rights and freedoms. The rights and freedoms of individuals that the AML laws intervene with are the right to respect for private and family life, home and communications[92] due to customer due diligence measures carried out by the obliged

[90] European Parliament, European Parliamentary Research Service (2015) "*Fundamental Rights in the European Union, The role of the Charter after the Lisbon* Treaty". ISBN 978-92-823-6749-0. Retrieved from http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf. [Accessed on 09.07.2017].

[91] European Union (2012), "*Charter of Fundamental Rights of the European Union 2012/C 326/*02". Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT. [Accessed on 12.08.2017].

[92] Article 7.

entities, right to the protection of personal data[93] due to storage and transferring of personal data between the financial units and freedom to conduct a business[94]. It is important to highlight that these limitations do not have an arbitrary character. The contrary, it has its basis in the rule of law.

In accordance with the Article 52 of the Charter of the Fundamental Rights of the EU, the EU law may limit the fundamental rights and freedoms to an extent. The Article states that if any limitation is brought against the fundamental rights and freedoms it should be proven necessary for the overriding general interest or the protection of another individual recognized by the law. Measures adopted should not go beyond what is needed to for the attainment of the objectives of the law and should respect to the principle of proportionality.

Regarding the limitations led by the application of the AML/CFT, it is important to remark the overriding European general interest against fundamental rights and freedoms. Money laundering is detrimental for the economic, financial and social segments of the society, which threatens the security and safety of the peoples, states and the democratic institutions at the national, regional and global level by fuelling the activities of criminals involved in illicit narco-trafficking, illegal arms deals, corruption and the terrorism. It helps criminals to operate and expand their criminal enterprises which leads to the manipulation of the financial system, erosion of the integrity of the financial institutions and the creation of unfair competition between legal and illegal businesses. Hence, limitations are justified by the European general interest such as the protection of the integrity of the financial institutions, the legal businesses from unfair competition, economic prosperity and the security of the peoples.

3. AML/CFT Framework at the EU Level

The EU has put forward the 4th AML Directive in 2015, taking into account the FATF Standards published in 2012. The directive has been transposed into the judicial systems of the Member States by 26th June 2017. Being the current AML/CFT legislation adopted at the EU level, it approximates the criminal laws of its Member States in the area of combating money laundering and terrorist financing and produces a more sophisticated combatting mechanism.

[93] Article 8.

[94] Article 16.

The objective of the Directive was stressed out in Article 1 (1) as "to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing"[95]. The Directive introduced the minimum standards for the member states to transpose into their judicial system, where the Member States were given the flexibility to adopt stricter provisions within the limits of the Union law including the Charter of the Fundamental Rights.

The Member States are obliged to implement the Directive in full compliance with the Union laws and the principle of proportionality[96] as the application of the directive should not go further than what is intended to be achieved. Additionally, since the Directive involves the requirements of collection, processing, storage and the transfer of the personal data, member states should ensure to adopt all necessary measures to prevent any violation of the data protection law[97] and the fundamental rights.

As stated in the Recitals of the Directive, "the Directive respects the fundamental rights and observes the principles recognized by the Charter, in particular the right to respect for private and family life, the right to the protection of personal data, the freedom to conduct a business, the prohibition of discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of defence."[98]

For the purpose of this thesis, the relation between the AML/CFT laws and the data protection law is not assessed further. However the key highlights of the 4th AML Directive in fighting with the money laundering and terrorist financing are examined below.

The Directive obliges member states to prohibit and criminalize money laundering and terrorist financing and obliges member states to implement the necessary measures for the prevention of money laundering and for the enhancement of the financial intelligence. As a prevention method, the Member States are rendered responsible to ensure that the sufficient instruments are made available to the obliged entities[99] in carrying out

[95] Directive 2015/849, Article 1(1).

[96] TEU Consolidated, Article 5(1).

[97] European Union (2016) , "*Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*". General Data Protection Regulation.

[98] Directive 2015/849, Recital 65.

[99] Obliged entities are the intermediaries of the transfer of funds.

particular AML/CFT requirements, such as customer identification and verification, investigation and reporting of the unusual and suspicious activities.

Money Laundering is considered as the conversion or transfer of property which is derived from criminal activity for the purpose of disguising the true nature of the source. In the context of the Directive, "'property' means assets of any kind whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents of instruments in any form including electronic or digital, evidencing tile to or an interest in such assets"[100].

Under the Directive, definition of the criminal activity is applicable to all serious crimes including the drug-related offences, the activities of criminal organizations, fraud affecting the EU's financial interests, corruption and all other offences which are punishable by deprivation of liberty[101], including tax crimes related to the direct and indirect taxes[102].

Considering all the facts above, one may easily observe that the Directive, by defining "property" and "criminal offence" in a broad way, increases the number of the cases for which the Directive is applicable. Taking into consideration the provision of the Directive, -any property, meaning assets of any kind that is derived from any criminal offence being transferred to disguise the origin of the source would be enough to qualify the person as an offender of money laundering.

As a part of the prevention policy, the Directive puts forward the entities who are obliged to carry customer due diligence (CDD) and know your client (KYC) measures. As a part of the CDD and KYC, these entities are responsible for the identification and verification of its customers and the investigation of the transactions and business relationships. Furthermore, if any transfer of funds is found to be suspicious, these entities are obliged to report to the Financial Intelligence Units (FIUs).

Obliged entities are stated in Article 2(1) as the credit institutions, financial institutions and the natural or legal persons acting in the exercise of their professional activities, including estate agents, legal professionals, auditors and providers of the gambling

[100] Article 3(3).

[101] Article 3(4).

[102] Differing from the previous AML Directives, the 4th AML Directive includes tax crimes in the scope of predicate offences.

services[103]. It is important to highlight once more that what laundered is not only the money as well as through whom it is laundered is not solely financial or credit institutions. Any property attained through illegal ways and is transferred through lawyers, real estate agents or gambling services to disguise its nature is considered as laundering. Therefore, it is highly crucial for the authorities to think of and consider all possible middle man who may take a part in money laundering and the financing of terrorism in order to mitigate the risks as much as possible. The Fourth AML, incorporating all possible middle man who are identified to have a high risk profile and obliging those entities to carry out CDD and KYC, introduces a strong and a sophisticated AML/CFT.

FIUs are central national authorities who collect and assess the information provided by the obliged entities on suspicious transactions, accounts and business relationships and on other information related to money laundering, financing of terrorism and any predicate offences. FIUs are a part of the Egmont Group (Expert Group on Money Laundering and Terrorist Financing) which is an international exchange platform of financial intelligence situated at the core of the global efforts in combatting money laundering and the financing of terrorism.[104]

As highlighted at the recitals[105] of the Directive, the coordination and the cooperation between the member states FIUs, as well as between the FIUs and other third country financial intelligence units, are crucial for efforts to combat money laundering and terrorist financing due to its transnational nature. The exchange of information should be encouraged and made available to the bodies of the other countries, for the timely management of the risks. Member States of the EU, under the directive are obliged to provide necessary instruments to the FIUs for the information to be exchange freely whether spontaneously or upon request.

Aligned with the 2012 FATF Recommendations, the 4th AML enhances the risk-based approach in assessing each case of money laundering and terrorist financing. It highlights the importance of a supranational approach, consisted of various Union, international and national based bodies including the Egmont Group and the Financial Intelligence Units

[103] The inclusion of the entire gambling sector in the scope of the obliged entities is one of the key points of the 4th AML Directive while only the casinos were subjected to specific requirements under the 3rd AML Directive.

[104] Egmont Group, "*About". Retrieved from* https://egmontgroup.org/en/content/about. [Accessed on 15.09.2017].

[105] Directive 2015/849, Recital 55-56.

in identification, understanding and mitigating the risks related to money laundering and terrorist financing.[106] As a part of the risk-based approach the member states are required to put forward the documents proving that they assessed the risks related to money laundering and the financing of terrorism and took sufficient measures to mitigate those risks.[107]

Transparency in the identity of the ultimate beneficial owner (UBO) of a legal entity is one of the most important factor in the success of AML/CFT laws. The Directive acknowledges it and stresses out the importance of the identification and verification of the beneficial owners in tracking the criminals who are hiding their identity behind legal entities through the utilization of offshore financial services, offshore bank accounts and shell companies. According to the provisions of the Directive, in order to make identification and the surveillance of the client more transparent and to prevent the misuse of the legal entities, member states are obliged to "ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held"[108] and to ensure that the collected information is available for all the competent authorities, obliged entities and the FIUs.[109]

As a part of the policy that adopts a risk-based approach, the cash-payment threshold for obliged entities to carry out CDD is decreased from € 15,000 to €10,000[110] and the conditions to carry out Enhanced Due Diligence (EDD) was changed. EDD is regulated under Article 18 and refers to the cases where the obliged entities are dealing with the natural or legal persons located in a high-risk third country[111], or when the customer profile or the status of the transaction is considered to carry high risk[112]. In addition to the basic information, the Directive obliges entities to examine a greater domain of information[113] under the EDD. Obliged entities with majority-owned subsidiaries or

[106] Directive 2015/849, Recital 24.

[107] Directive 2015/849, Recital 22.

[108] Directive 2015/849, Article 30 (1).

[109] Directive 2015/849, Article 30 (5).

[110] Directive 2015/849, Recital 6.

[111] The European Commission is delegated to determine the high-risk third countries whose AML/CFT laws are deficient. *See* European Union (2016), "*Commission Delegated Regulation (EU) 2016/1675 of 14 of July supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies*".

[112] Whether a transaction is considered risky or not is based on evidence.

[113] Directive 2015/849, Article 18 (2).

branches located in the high-risk countries are obliged to meet with the requirements of the Directive at those subsidiaries or branches. After the risk assessment process, the EDD may be carried out when dealing with those branches or subsidiaries.[114]

With the 4th AML directive, again as a part of the enhanced risk-based approach, the obliged entities were invited to reconsider the way that they manage their cash-intensive clients. While previously the customers located in the EU/EEA, or in a jurisdiction that imposes equivalent requirements, were automatically granted with Simplified Due Diligence (SDD) status, the 4thAML conditioned the allowance of SDD status upon proof. According to the Article 15 (2) "before applying SDD measures, obliged entities shall ascertain that the business relationship or the transaction presents a lower degree of risk." In another words, without the proof indicating the low risk profile of the transaction, a business relationship or a client, the SDD status cannot be granted automatically. Application of the SDD status should be backed up by the documentation.

Adoption of the risk-based approach also lead to the broadened definition of the politically exposed persons[115] (PEPs). In the context of the 4th AML, foreign politically exposed persons, as well as the domestic PEPs, are subjected to EDD measures performed by the obliged entities. Specific requirements laid down by the directive related to the PEPs do not have a criminal nature, rather have a preventive nature. A person who is politically exposed cannot be considered automatically as being a criminal.[116] Further assessment is required to prove the high-risk profile of that person.

Considering all the characteristic of the AML/CFT framework indicated above, one may easily say that the anti-money laundering and terrorist financing laws are based and dependent greatly on the cooperation of the trusted third parties. These entities are the source of intelligence that are rendered responsible to monitor abnormal money flow, identification and verification of the natural and/or legal persons who are transferring funds and reporting of the suspicious business activities or transactions. In the traditional remittance systems, no transaction can be made and verified without passing from these parties, thus they are the gatekeepers of any transaction for the prevention of money laundering and terrorism financing offences. Taken out of the equation, the system does

[114] Directive 2015/849, Article 18 (1).

[115] Under Article 3 (9) of the Directive 2015/849, politically exposed persons are referred as "a natural person who is or who has been entrusted with prominent functions". The list consisted of the politically exposed persons are indicated under Article 3(9).

[116] Directive 2015/849, Recital 33.

not function properly since there is no intelligence provided to catch the criminals. The remittance system that eliminates the trusted third party becomes short in combating with the money laundering and the financing of terrorism.

Transparency is another catalyst for the system to work properly which is ensured by these trusted third parties, the obliged entities in the context of the Directive. Trusted third parties by identifying and continuously monitoring the natural persons and the beneficial owners of the legal entities, enable the authorities to go back in the audit trail and detect the criminal. Without transparency, the system would fail to track the natural or legal persons, the laundered money and the fund that benefitted a terrorist group. Thus, a system that is structured around anonymity would help the audit trail to be obscured and make detection of the criminals way harder than it is.

As it is put forward in the next chapter, two features of virtual currency, more specifically cryptocurrency, render the existing AML/CFT laws incapable of responding and mitigating the risks. Being pseudo-anonymous and eliminating the trusted third parties, cryptocurrency forces regulatory bodies to identify, assess and understand the new challenges and to transform the existing AML/CFT laws to tackle with those challenges.

FATF report on the Virtual currencies Key Definitions and Potential AML/CFT Risks from 2014 and the FATF guidance for a risk-based approach on virtual currencies from 2015 led European Union Commission to propose an amendment to the 4th AML Directive, to bring Virtual Currencies into the scope of Directive (EU) 2015/849.[117]

The proposal of revision was presented upon the terrorist attacks of Paris and the Panama Papers exposure, as a part of the European Commission's Action Plan for Strengthening the Fight against Terrorist Financing announced in February 2016. The proposal obliges virtual currency platforms to perform the same CDD and KYK methods as the financial institutions and non-financial businesses and professions. Assessment of the proposal is curial for the determination of whether the virtual currencies are sufficiently dealt under the proposed AML/CFT law.

Prior to the critical assessment of the proposed AML/CFT on whether it sufficiently deals with the potential abuses caused by the usage of virtual currency, it is important to put

[117] European Commission (2016), "*Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*".

forward the basic concepts related to the virtual currencies and its characteristics that are likely to abuse AML/CFT regulations.

Part III. Virtual Currency and Blockchain

1. Basic Concepts

i. Virtual Currency

There is no definition of virtual currency that is internationally accepted. Various institutions defined it differently. European Central Bank in 2012 defined it as "a type of unregulated, digital money, which is issued and usually controlled by its developer, and used and accepted among the members of a specific virtual community."[118] Meanwhile the U.S. Treasury defined it as a "medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[119]

Despite the lack of a uniform definition and classifications on legal status[120], one should avoid confusion between virtual currency and fiat currency, virtual currency and electronic money and virtual currency and digital currency. Fiat currency, also known as national currency, is issued and controlled by a country. It is put into circulation by central authorities and recognized as a medium of exchange. In contrast to fiat currency, virtual currency is a medium of exchange and/or a unit of account or store of value that does not have a legal tender status. Thus a creditor is not obliged by law to accept virtual currency as a form of payment to extinguish a private or public debt. Additionally, virtual currency is not always administrated or issued by a central authority.

The nature of it, on the other hand, is distinct from electronic money (e-money). Article 2 of the Electronic Money Directive 2009/110 defines electronic money as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions… which is accepted by a natural or legal person other than the electronic money issuer."[121] While some elements of virtual currency coincide with electronic money, there are significant differences. E-money is a digital representation of fiat currency and maintains its unit of account and legal tender status. It is equal to an amount

[118] European Central Bank (2012), "*Virtual Currency Schemes*". pp.5.

[119] Department of the Treasury Financial Crimes Enforcement Network, FinCEN (2013), "*Application Of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*". FIN-2013-G001, pp.1. Retrieved from https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf. [Accessed on 06.09.2017].

[120] There is an ongoing debate on the legal status of Virtual Currency, more specifically cryptocurrency on whether it is a currency, an asset or something else. Jurisdictions treat it differently.

[121] European Union (2009), "*Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money* institutions". Retrieved from http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0110. [Accessed on 06.09.2017].

of fiat currency exchanged into electronic form by a central authority. On the other hand, unit of account changes for the virtual currencies.

Distinction between virtual currency and digital currency comes from the division between digital economy and the virtual economy. While digital economy describes all the business operating in digital arena (online), selling and providing physical goods and services, virtual economy represents the un-real economy which only exist in a virtual world. However the distinction between digital currency and virtual currency became unclear with the introduction of a type of virtual currency, cryptocurrency.

ii. Categorization of Virtual Currency

Virtual currencies can be divided into categories based on their use and the way of operation.[122] Based on their use virtual currencies divide into two groups: community based, e.g. World of Warcraft Gold, Amazon Coins and Microsoft Points; and universal virtual currencies, e.g. Bitcoin, Ethereum and WebMoney. And virtual currencies operate in two ways, based on a central authority or without a central authority.

a. Community-related Virtual Currency

Virtual communities are computer-generated environments in which the members or users of the community interact with each other through their virtual characters (avatars) and pursue one mutual goal. These worlds can be reached simultaneously by great amounts of individuals from anywhere in the world. Networking websites such as Instagram, Twitter and Facebook, chatrooms and online games like World of Warcraft and League of Legends are examples of a virtual domain.

Every community related virtual currency is developed to be specific to one particular virtual world. These currencies can only be spent in that virtual domain through members' interactions. It serves as a form of payment while the user purchases specific virtual items or services within the world. For instance, World of Warcraft Gold, whose subunits are Silver and Copper, is used as a medium of exchange within that cyberspace.

Community related virtual currencies differ in a way on how a participant obtains it. While some of them can be acquired by purchasing with legal tender such as Amazon Coins and abolished Microsoft Points, some of them can only be obtained by carrying out

[122] ECB has a different classification – closed, bidirectional, unidirectional. *See* European Central Bank (2012), "*Virtual Currency Schemes*".

a particular task as it is the case for World of Warcraft Gold. However none of these community related virtual currencies can be converted back to legal tender.

In their nature, all community related virtual currencies are centralized, having a single authority of administration. The central authority issues the currency, administers the transactions, determines the rules and monitors the currency flow.

b. Universal Virtual Currency

The use of universal currencies is not limited to a specific computer-generated world but they can be used to purchase real goods and services of the market. Not only one can obtain these universal virtual currencies with legal tender but also convert it back into a legal tender. They function like a real currency with its convertibility and exchange rates. Examples of this type are Bitcoin, being the most prominent, Ethereum and other *"altcoins"*[123].

Regarding the way of operation, universal currencies may be centralized (WebMoney) or decentralized (Bitcoin and Ethereum). Decentralized universal currencies are not issued by a central authority (put into circulation), thus not subjected to any central monitoring or to any rules established by a central authority. Furthermore, it cannot be withdrawn from circulation. These decentralized currencies are called cryptocurrencies[124], transferred from an information system to another, for example, from computer to computer.

2. Cryptocurrency, Bitcoin and the Bitcoin Protocol

i. Bitcoin

Bitcoin is the first decentralized convertible virtual currency, cryptocurrency. This electronic cash system was designed by an anonymous individual or a group of individuals called Satoshi Nakamoto as a pseudo-anonymous system. The system consists of four innovations, a de-centralized peer-to-peer network (bitcoin protocol), a public transaction ledger (the Blockchain), a de-centralized mathematical currency issuance (distributed mining) and a de-centralized transaction verification system (transaction script).[125] Introduction of Bitcoin was done by Satoshi Nakamoto's self-published paper,

[123] Bitcoin alternatives.

[124] Cryptocurrency is a medium of exchange that uses cryptography to secure transactions rather than trusted third party.

[125] Antonopoulos, A. M. (2014), "*Mastering Bitcoin*". O'Reilly Media, First Edition, ISBN 978-1-449-37404-4.

"*Bitcoin: A Peer-to-Peer Electronic Cash System"*[126] in 2008 which was a response to financial crises of 2008 that reduced individual confidence on financial institutions dramatically.

In the paper, an electronic payment system that would allow two parties to directly transmit value without a trusted third party, is claimed as a need based on various reasons. It was first argued that the sector of commerce on internet is growing and financial institutions remain the sole, indispensable actors of e-commerce transactions. These actors of non-cash transactions (electronic transactions) are unable to avoid mediating disputes and leading to the rise of transaction costs, to the limitation in the minimum amount to be transferred and to the prevention of irreversible transactions for irreversible goods and services. In order to overcome the weakness of the system, it proposes a network that is not dependent on trusted third party based on cryptographic proof[127] instead of trust.[128]Despite the invention of other cryptocurrencies since 2008, Bitcoin remained the most prominent one.

Classification of Bitcoin's legal status has been posing a great challenge for countries and regulatory bodies. While there is no unanimously decided status, classification is crucial for the determination of the applicable laws and regulations. There are two main arguments on determining the class of Bitcoin, bitcoin as a currency and bitcoin as an asset. Its usage is considered sometimes to be the determinative factor. If used to purchase or sell goods and services, Bitcoin is more similar to a currency. However if used for investment purposes to generate profit, it functions more like an asset. This paper does not aim to determine the nature of bitcoin but briefly touches upon the ongoing arguments on the legal status of Bitcoin.

As mentioned previously, currency is characterized as a medium of exchange, a unit of account and a store of value which is designed as a legal tender that circulates in the country of issuance[129]. Real or fiat currencies are issued to be scarce that does not hold

[126] Nakamoto, S. (2008), "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Retrieved from https://bitcoin.org/bitcoin.pdf. [Accessed on 05.06.2017].

[127] Cryptographic proof relies on private and public keys which are used in the process of transfer of value from a payor to a payee. These digital signatures ensure the security of the system.

[128] Nakamoto, S. (2008), "*Bitcoin: A Peer-to-Peer Electronic Cash System*". pp.1.

[129] FATF (2014), "*FATF Report, Virtual Currencies Key Definition and Potential AML/CFT Risks*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

intrinsic value. Despite the similarities of Bitcoin and real currency, it does not fulfil all the criteria.

Germany considers Bitcoin as a units of account which is not expressed in the form of legal tender, however it does not classify it as a real currency but rather a "private money".[130]

Another argument has been held on whether Bitcoin can be considered as a commodity money such as gold and silver which are naturally scarce currencies that are not issued by any central authority whose value are derived from the material.[131]

On 2014, Danish Central Bank stated that Bitcoin is not a currency because it does not have an intrinsic value compared to silver and gold.[132] Its value is dependent on individuals and on how much they are willing to pay.

Jurisdictions seeing bitcoins as assets based their claims on the usage of bitcoin as an investment tool. Norway, one of the jurisdictions that rejected to treat bitcoins as a currency, classifies bitcoin as a capital property.[133] Jeffry Dorfman, however differentiates Bitcoins from other assets and classifies bitcoin as a "speculative asset". Economics Professor from University of Georgia, writing in Forbes, in May 2017 claimed that Bitcoin is not a plausible currency or an investment tool due to its unstable value that changes nearly 50% months where the exchange rate between the USD and the Euro only changes 3% monthly. He furthermore argued that bitcoin has no underlying usage as gold does, usage for investment.[134]

---

[130] CNBC, Clinch, M. (2013), "*Bitcoin recognized by Germany as 'private money'*". Retrieved from https://www.cnbc.com/id/100971898. [Accessed on 24.08.2017].

[131] Baur, D. G. & Hongik, K. H. & Lee, A. D. (2015), "*Bitcoin: Currency or Asset?*". Pp.3. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736020. [Accessed on 29.09.2017].

[132] DENMARKS NATIONALBANK (2014), "*BITCOIN ER IKKE PENGE".* Retrieved from http://www.nationalbanken.dk/da/presse/Documents/2014/03/PH_bitcoin.pdf#search=Bitcoin. [Accessed on 03.09.2017].

[133] LIBRARY OF CONGRESS, Global Legal Monitor, Hofverberg, E. (2013), "*Norway: Bitcoins Are Capital Property, Not Currency, Says Norwegian Tax Authority"*. Retrieved from http://www.loc.gov/law/foreign-news/article/norway-bitcoins-are-capital-property-not-currency-says-norwegian-tax-authority/. [Accessed on 01.09.2017].

[134] Forbes, Dorfman, J. (2017), "*Bitcoin Is An Asset, Not A Currency".* Retrieved from https://www.forbes.com/sites/jeffreydorfman/2017/05/17/bitcoin-is-an-asset-not-a-currency/#7669eb222e5b. [Accessed on 13.10.2017].

Figure 1. Bitcoin Volatility Over Time (%)[135]

Considering all the arguments touched upon, one may easily say that, the hybrid nature of Bitcoin prevents authorities to decide on its legal status and remains to be an issue for the regulation purposes. In order to deal effectively with this issue, Canada and Australia adopt a hybrid approach where Bitcoin is classified as both asset and currency depending on specific situations.[136]

Bitcoin's market capacity, at the moment of the writing, 10th of March 2018, is approximately $160B (depending on the exchange rate of the day) with almost 17M Bitcoins in circulation. As mentioned above, there is no central authority that puts Bitcoin into circulation. The network creates a Bitcoin every 10 minutes (in average) and guarantees that supply of the Bitcoin to never exceed 21 Million (to be reached in 2140), where each unit can be broken into subunits. Its exchange rate varies (due to user demand) which may differ $500 in a 12 hours period. Since its invention, exchange rate of Bitcoin reached to the highest of $20,052.60 in December 2017, with the rate of $9,423.00 at the moment of writing. The largest Bitcoin transaction so far was 194,933 Bitcoins, worth, at the moment of the transaction, $150M.

Bitcoin as a universal virtual currency, can be used to purchase physical goods and services, to make payments to anyone or any organization or to sell goods and services. In this sense one could say that Bitcoin is more of a digital currency than a virtual currency

[135] The Bitcoin Volatility Index, Bitcoin Volatility Over Time. Retrieved from https://bitvol.info/. [Accessed on 10.03.2018].

[136] Litwak, S. (2015), "*Bitcoin: Currency or Fool's Gold: A Comparative Analysis of the Legal Classification of* Bitcoin". 29 Temp. Int'l & Comp. L. J., pp.345.Available online at www.heinonline.com.

since it is used in the real world for physical goods and services. Companies or businesses who accepts Bitcoin as a payment method for the provided good or service, are increasing in number, rapidly and are expected to spread all around the world.[137]

Its extra-territorial nature is one of the biggest contributor for Bitcoin becoming very successful along with the accelerated payments, removal of high fees and arbitrary limits of transfer. Neither has it required a user to possess a bank account nor to wait for the working hours to make a payment. The system is always open and the transactions occur mostly in short times.[138]

The Bitcoin software is public, can be downloaded for free by anyone in the purpose of storing, receiving and transferring Bitcoin. As mentioned above, Bitcoins can be obtained against other currencies and converted back at particular exchange rates. Exchange is held by various exchange services with many national currencies like United States Dollar (USD), Euro (EUR), Swedish Krona (SEK), Turkish Lira (TL), British Pound (GBP) and etc. When exchanged to Bitcoins are completely virtual. Meaning that, Bitcoins are not available in a physical or a digital form.

ii. How to acquire Bitcoin?

Being a participant in bitcoin network is easy and for free. All a user has to do is to download a virtual currency wallet[139] to its computer, smart phone or to use an online version of a wallet (Coinbase, Bitcoin Wallet, Multibit). When it's downloaded, the account is created without the need of an individual to disclosure any information related to personal identification. Participant's identity is only linked to a Bitcoin address.

Acquiring bitcoin/cryptocurrency is no different than buying foreign currencies from exchange kiosks, banks or online banking systems. Unlike foreign currencies, for Bitcoin a merchant should go to a special exchange office, web platform or a bitcoin ATM that sells cryptocurrencies. Bitstamp for European (EUR), Coinbase (coinbase.com) for USD

[137] List of Entities accepting Bitcoin. Retrieved from https://en.bitcoin.it/wiki/Trade. [Accessed on 25.09.2017].

[138] Average confirmation times for Bitcoin transactions vary due to the Blockchain transaction traffic caused by software's limitation on the block size of just 1MB. Increase in total transactions per day and fees paid to miners for transactions causes delays since total amount of transactions exceeds the number of overall space. *See* Coin Telegraph (2016), "*Why is My Bitcoin Transaction Taking So Long? Here's Why*". Retrieved from https://cointelegraph.com/news/why-is-my-bitcoin-transaction-taking-so-long-heres-why. [Accessed on 23.11.2017].

[139] Virtual currency wallet is defined by FATF as means (software application or other mechanism/medium) for holding, storing and transferring bitcoin or other virtual currency. *See* FATF (2014), "*FATF Report, Virtual Currencies Key Definition and Potential AML/CFT Risks*". pp.7.

based currency market are the largest Bitcoin brokers where merchants can buy and sell cryptocurrencies. Depending on the national jurisdiction, cryptocurrency exchange offices are subjected to regulations as Know Your Client (KYC) and Customer Due Diligence (CDD) that has to be taken into account when buying. Depending on the requirements, obtaining bitcoins may take some time.

On the other hand, there are alternative ways to acquire bitcoin such as buying it from a local system participant or a friend directly in exchange with cash or transfer of money. Furthermore, a merchant may sell a good or a service in its Brick and Mortar or online store for Bitcoin or altcoins.[140] Additionally, by mining process, one may alternatively acquire Bitcoin.

iii. Bitcoin Protocol and Blockchain

Bitcoin, along with being the name of a cryptocurrency, is the name of a protocol, a peer-to-peer network. Unlike the traditional banking systems, any transaction occurs between two information systems, from computer to computer or from smart-phone to another without a central authority monitoring the network.

The system introduces a non-conventional solution for the problems that electronic transactions faces with: verification of the authenticity of the money and the double spending. Authenticity and double spending problems are dealt by central authorities who are given responsibility to handle all electronic transactions. However the removal of the authorities leads these problems to be remained. Cryptographic digital signature integrated with distributed computation systems serve as a solution for both of the problems under Bitcoin software.

Upon the creation of a bitcoin wallet, each user is given two keys as a requirement of public-key cryptography[141]. One of them is a private key that functions as a personal password or a hand-writing signature and is used to authorize a transaction. The other is a public key, which can be shared with other users and serves as a bitcoin address. Bitcoin address has an encrypted structure which is a long code of letters and numbers. Even though it operates as an e-mail address, a user may create a new address as many time as

[140] Antonopoulos, A. M. (2014), "*Mastering Bitcoin*". O'Reilly Media, First Edition, ISBN 978-1-449-37404-4. pp.10.

[141] Brito, J. & Castillo, A. (2013), "*BITCOIN A Primer for Policymakers*". MERCATUS CENTER, George Mason University, pp.5.

it wishes which will be connected to the user's wallet[142]. With the keys assigned, a user can prove ownership of value, transfer value or access and control its account.

Figure 2.. Public and Private Key [143]

When user X wishes to transfer bitcoins to user Y, all X has to do is to type in the bitcoin address of Y, enter the amount of bitcoin to be sent and to authorize the transaction by signing it digitally with its private key in the transfer page.

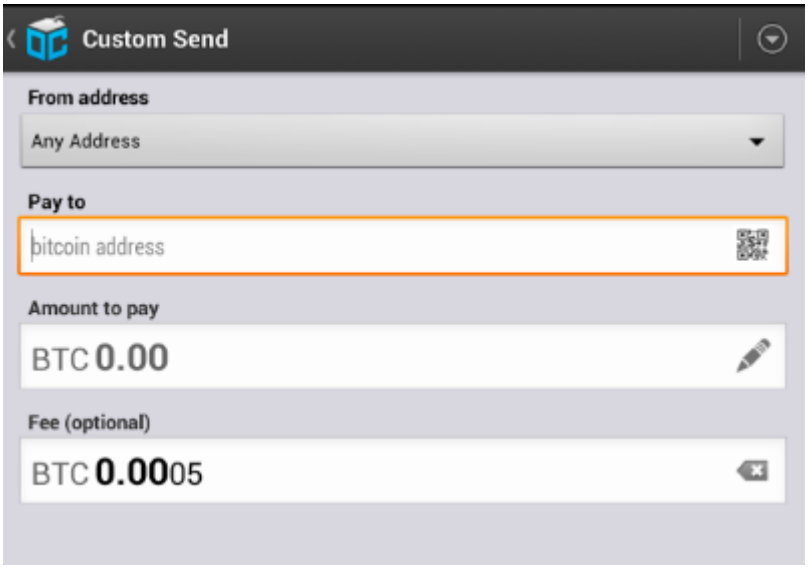

Figure 3. Bitcoin Mobile Wallet- Send Bitcoin Screen [144]

[142] *"A wallet is simply a collection of addresses and the keys that unlock funds within." See* Antonopoulos, A. M. (2014), "*Mastering Bitcoin*". O'Reilly Media, First Edition, ISBN 978-1-449-37404-4. pp.9.

[143]National Bitcoin ATM Helpdesk (2016), "*How do I use/send the bitcoin I just bought with my receipt?". R*etrieved from http://help.nationalbitcoinatm.com/support/solutions/articles/6000080051-how-do-i-use-send-the-bitcoin-i-just-bought-with-my-receipt-. [Accessed on 17.10.2017].

[144] Antonopoulos, A. M. (2014), "*Mastering Bitcoin*". O'Reilly Media, First Edition, ISBN 978-1-449-37404-4. pp.12.

By the public-key cryptography, verification of ownership (authenticity of the coin) can be proved. However it solely cannot verify if a coin is not spent doubly (double-spending problem).

Blockchain technology in the core of the system solves this problem by registering every single Bitcoin transaction in a distributed public ledger. Every participant keeps the copies of their ledger. Thus everyone in the system is able to see one other's balance. The maintenance of the public ledger (Blockchain) is performed by communication network through computers which are not under the control of any centralized entity, called maintainers. These high performance computers are expected to solve a sophisticated algorithm and reach to a math-based consensus on the true record of all previous transactions (chain of sequence of events). Once the chain is created by proof of work it is true and irreversible which is used for the next transactions to prevent double-spending of a coin.

For instance, when payer X sends q amount of bitcoins to payee Y, the transaction is broadcasted to the whole network with attached information; bitcoin address of X and Y and the amount of bitcoin sent. If the transaction has a valid signature, every computer (maintainer) in the system updates their ledger. However, fraudulent activity or traffic in the system might lead to differences in the ledger. In order to decide on the true sequence of events (true ledger), system requires the maintainers to vote by solving an algorithm based on their version of the ledger. The race between the maintainers is not for numbers but is to find the true sequence of data.[145] There is no need to create unanimity on the true version of the ledger, however a consensus is needed. The more people are trying to solve the algorithm based on their version of the ledger, the faster the algorithm to be solved. Thus as long as the majority of the computers are honest and generating true entries regarding the sequence of events, any fraudulent activity or a mistake is dealt within the system.[146] When a maintainer solves the mathematical problem, it announces the "true" version and others update their copies of the ledger accordingly.

[145] Brito, J. & Castillo, A. (2013), "*BITCOIN A Primer for Policymakers*". MERCATUS CENTER, George Mason University. pp.6.

[146]Nakamoto, S. (2008), "*Bitcoin: A Peer-to-Peer Electronic Cash System*". pp.5.

New transactions are constantly flowing into the network and every 10 minutes[147] create a block that contains the algorithm to be solved. When the process successfully ends and a true ledger is announced by a participant, the block attaches to the previous blocks of transactions which all together creates a Blockchain. This process, called Proof-of-Work, happens, averagely, every 10 minutes and each solution creates a block that will be attached to the preceding blocks containing entire history of commerce of bitcoin (blockchain - public ledger - sequence of events).

iv. Distributed Mining and Issuance of Bitcoin

Any person may perform the responsibility of a maintainer yet, not without being subjected to maintenance costs which grow as more maintainers participated to the bitcoin network. Involvement to Proof-of-Work, solving a problem, consumes a lot of electricity since the computer has to work 24/7, without being turned off. On the other hand, one can join but cannot remain in the bitcoin network as a maintainer with a normal computer. Possessing a high performance machine is a necessity. Thus being a maintainer is costly. In order to encourage people to join the network and to contribute to the verification of transactions, the bitcoin network awards the participant who solves the mathematical problem first (verifies first), with Bitcoins. Award is given to compensate the costs of maintenance. Due to the issuance of bitcoin after every verification, the maintainers are also called bitcoin miners.

Bitcoins are issued at a fixed and a decreasing rate. Satoshi Nakomoto declared that "total circulation will be 21,000,000 coins. It'll be distributed to network nodes when they make blocks, with the amount cut in half every 4 years. first 4 years: 10,500,000 coins next 4 years: 5,250,000 coins next 4 years: 2,625,000 coins next 4 years: 1,312,500 coins etc. …"[148] While the first 4 years 50 Bitcoin was the reward of each block, the amount diminished to 25 Bitcoin in November 2012 and finally to 12,5 Bitcoin in 2016. [149]

As mentioned previously, the system is built to ensure that the issuance of a bitcoin will take place at a time that was determined in the software. If every block contained 50 Bitcoin, then 10.500.000 coins were issued from 210.000 (4 * 365 * 144) blocks in the

[147] Interval between blocks is not always exactly 10 minutes. While many takes less than that, some takes much more than it, with the average interval of 10 minutes.

[148] Satoshi Nakamoto Institute (2009), "*Bitcoin v0.1 released"*. Retrieved from http://satoshi.nakamotoinstitute.org/emails/cryptography/16/. [Accessed on 28.09.2017].

[149] Antonopoulos, A. M. (2014), "*Mastering Bitcoin*". O'Reilly Media, First Edition, ISBN 978-1-449-37404-4. pp.178.

first 4 years, which makes averagely 144 blocks per day. By looking at the equation given above, one can easily confirm that every block is created in 10 minutes (average) and the software guarantees that the interval will remain the same.

Blockchain technology that lies under the Bitcoin network introduces a security technology. The Blockchain, is considered as one of the most secured systems against cyberattacks, since a successful attack has to be carried simultaneously from the majority of the computers connected to the system. Research on the applicability of Blockchain technology to other systems is already been carried out, some being implemented and some waiting in the line to be realized. Self-executing smart contracts, fraud-free voting systems and protection of IP rights are some of the applicable systems. Yet for the purpose of this paper, non-virtual currency applications of the Blockchain Technology will not be assessed further.

3. Vulnerability to Risks

Usage of virtual currencies has grew in numbers due to its easy, fast and cheap nature comparing with the traditional payment methods. Along with its benefits, the system is not invulnerable to risks related to the users, the market and the investors.[150] Risks related to the users are observed as losses incurring due to wallet theft, fraudulent exchanges and value fluctuations which were considered as the most possible scenarios to be realized[151]. On the other hand investor concern is linked mainly to the volatility of the currency. Market concern, maybe the most acknowledged one, is linked to risks of financial integrity including money laundering and terrorist financing, risk of financial crime such as trade of illegal commodities or ability to avoid seizure of assets and commodities and tax evasion.[152] For the purpose of this paper, risks and regulatory measures other than money laundering and terrorist financing are not assessed further.

Among all virtual currencies, cryptocurrency has the highest risk potential due to its pseudo-anonymous nature, decentralized network and easy international transmissibility. Despite its widespread usage and vulnerability to risks, it operated free from any regulation for a long time. However regulators took notice on the issue and incentives for regulation increased in order to protect the stakeholders and the market. Responses were

[150] Vandezande, N. (2017), "*Virtual currencies under EU anti-money laundering law*". Computer Law & Security Review 33, KU Leuven Centre for IT & IP Law, pp.342. Available online at www.sciencedirect.com.

[151] European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". pp.21-22.

[152] European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". pp.33-35.

various and distinct to these risks, while some countries opted to ban trade in virtual currency (China), some opted to issue licenses to the virtual currency exchangers[153] (New York State Department of Financial Services- BitLicense), subjecting them to specific requirements with the purpose of reducing client anonymity.

Action at European Union level adopted an incremental approach. Despite, the need of the European Regulation on virtual currency was raised for the first time in 2012, the European Union dealt with the issue on a theoretical level only until 2016. An amendment to the 4th AML Directive was proposed on June 2016 as a part of Commission Action Plan against terrorist financing, following the Paris terrorist attack, aiming to bring virtual currencies under the scope of the Directive, requiring virtual currency exchangers to comply with customer due diligence (CDD) and know your client (KYC) methods as it requires from financial institutions among others, which have not been accepted yet.

i. Virtual Currency in Money Laundering and Terrorist Financing Schemes

Virtual currencies took their place in Money Laundering and Terrorist Financing Schemes and Methods next to the traditional tools such as offshore banking, alternative underground remittance services (hwala[154]) and use of international wire transfers.

a. Money Laundering

Benefitting from Virtual Currencies for money laundering purposes could occur in two different ways. Firstly, dirty money obtained from illegal activities as drug trafficking, human-trafficking or sale of various illicit commodities, could be exchanged through a virtual currency exchanger into a virtual currency (placement). And criminals by involving into multiple transactions and purchases could obscure the origin of funds (layering). Funds that are distanced from their origin then could be integrated into the mainstream economy (integration). In the second scenario, virtual currency obtained through criminal activity could be converted to a fiat currency and go through the same layering process to distance funds from their origin.

The first case to take public attention to the potential of virtual currency to facilitate crime is the *Liberty Reserve* case. In May 2013, a Costa Rica based online payment system that

[153] According to the definition of FATF Report, exchanger is a person or entity engaged as a business in the exchange of virtual currency for real currency.

[154] Hwala is a method of transferring money without an actual movement, done through Hwala brokers. *See* Part I.

issued its own centralized virtual currency (Liberty Reserve Dollars/Euros backed by real dollars or euros) was prosecuted by US authorities with the charges of laundering $8B by more than 50 million transactions combined of credit card and identity theft.[155] The system was allowing criminals to make financial activity on Liberty Reserve in a completely anonymous way. Customers were asked to provide names and addresses, however none of them were obliged to verify the information given with official documents. Hence the transactions were untraceable. Completely anonymous and untraceable transactions were the source of attention of criminals.

Silk Road was the name of another case brought by the U.S. authorities. Silk Road was an online market known for selling illegal commodities including drugs, armament, stolen credit card numbers, fake licenses and passports[156]. It was providing its customers a monitoring free and an anonymous browsing by requiring payments to be made by Bitcoin and by limiting the accession of the website which could be only done through an anonymizing network, Tor[157]. From its creation in 2011 until its seizure in 2013, the website operated without legal enforcement due to its method of operation.[158] When the Federal Bureau of Investigation (FBI) shut down the website and convicted Ross Ulbricht, the founder of Silk Road, of money laundering, computer hacking and drug trafficking crimes, the reputation of virtual currency and Bitcoin being contributors of crime began to be acknowledged by the media and regulators.

b. Funding of Terrorism

Virtual currencies as a threat for counter terrorism efforts were dealt with different responses. While the National Terrorist Financing Risk Assessment of the U.S. considers virtual currencies as a *potential* threat to financing of terrorism[159], the European Banking

[155] Carlisle, D. (2017), "*Virtual Currencies and Financial Crime, Challenges and Opportunities*". Royal United Services Institute for Defence and Security Studies, ISSN 2397-0286, pp.15.

[156] FBI, U.S. Attorney's Office (2013), "M*anhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*". Retrieved from https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website. [Accessed on 13.09.2017].

[157] The Onion Router (Tor) is an open and free software designed to conceal the real IP addresses of computers which prevents people from locating the users. *See* The Onion Router at https://www.torproject.org/.

[158] Brill, A. & Keene, L (2014), "*Cryptocurrencies: The Next Generation of Terrorism Financing?*" Defence Against Terrorism Review, Vol. 6, No. 1, Spring&Fall 2014, ISSN: 1307-9190, pp.20.

[159] Department of the Treasury, Washington DC. (2015), "*National Terrorist Financing Risk Assessment*". Retrieved from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf. [Accessed on 28.01.2018].

Authority considers Virtual Currency remittance systems as a high risk development for the efforts against funding of terrorism.[160]

According to the report of CNAS of 2017, virtual currencies became a threat recently for counter-terrorism measures due to its regulatory challenges[161]. They have not been used in a large scale yet, but authorities should not ignore the risks and should bring virtual currencies under law enforcement.[162]

Unlike the money laundering cases, reports of terrorism funding by virtual currencies remains anecdotal.[163] There are reports from various intelligence services and governmental authorities containing information that terrorist groups in Gaza have been using Bitcoin to fund their activities, while some other reports claim that various Bitcoin wallets were found to be owned by Daesh militants. Recently, Bitcoin and terrorism link was claimed by the Indonesian government in January 2017. Indonesian authorities declared that they have evidence on Daesh operatives, using Bitcoin to transfer money to other operatives. One of the names appeared in reports, Bahrun Naim is an Indonesian operative of Islamic State, who is claimed to be the person behind the Jakarta attack of 2016.[164]However as mentioned above, there are no official evidence proving that terrorists have been using virtual currencies to fund their activities.

Incidents and intelligence reports mentioned above proved once again the need to regulate virtual currency in order to mitigate the risks related to money laundering and financing of terrorism. Various countries proposed different solutions as European Union member states adopted diversified initiatives. For the purpose of this thesis, only European Union level AML/CFT regulations will be introduced and assessed with a critical approach.

In order to assess existing regulations, to highlight its inadequate and sufficient points and, if needed, to propose an effective regulation, characteristics of cryptocurrencies that

[160] European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'".

[161] These challenges are introduced under the topic "Characteristics related to AML/CFT Abuses" in this Part.

[162] CNAS (2017), "*TERRORIST USE OF VIRTUAL CURRENCIES, Containing the Potential Threat".* Energy, Economics & Security, pp.1.

[163] Carlisle, D. (2017), "*Virtual Currencies and Financial Crime, Challenges and Opportunities*". Royal United Services Institute for Defence and Security Studies, ISSN 2397-0286. pp.18.

[164] Coindesk, Rizzo, P. (2017), "*Indonesia's AML Watchdog Links Bitcoin to Islamic State".* Retrieved from https://www.coindesk.com/indonesias-aml-agency-links-bitcoin-islamic-state-terrorism/. [Accessed on 08.07.2017].

makes them attractive to be used for money laundering and as a tool for global terrorist funding are addressed first.

ii. Characteristics Related to AML/CFT Abuses

a. Anonymity

Great deal of anonymity provided by the Bitcoin network to its users is one of the reasons why Bitcoin is linked to money laundering and terrorist financing, why criminals are encouraged to use and why media and regulators are giving a great deal of attention to it. Despite the fact that sales through anonymous digital wallet enables launderers to conceal the origins of illegally obtained money and hardens the surveillance of the money flow, anonymity of bitcoin transaction is a widely misunderstood concept. In order to eliminate the misunderstanding, the paper compares two existing system of transaction with the cryptocurrency transactions, PayPal[165] or traditional electronic transfers and payment with cash.

When an individual wishes to create a bank account, since mediating party is involved, she/he is subjected to disclosure of personal information that identifies the user. Therefore, whenever the account holder transfers money electronically to another account holder, identity of the payer and the payee appears in the system and transaction is recorded in the ledger. Likewise, payments done through PayPal, since a user's PayPal account is attached to their bank account, are fully transparent as the financial institution monitors the flow of money between its two system participants. On the other hand, payments done with cash are completely anonymous, whereby there is no institution (mediating party) to witness or supervise the transaction. Transactions through Bitcoin network are different than the realities mentioned above and yet carries some of their characteristics.

As mentioned above, a person is not required to disclosure his/her identity or any other information when obtaining a bitcoin account, unlike creating a bank account through financial institutions. Hence, the system provides privacy to its users. The public key given to the user is not attributable to any specific individual or to any personal information. Neither a third party nor the payee can know the identity of the payer or the

[165] "PayPal is only a payment service provider whose main business is the issuance of E-money and the provision of services closely related to the issuance of e-money." *See* Guadamuz, A. (2004), "*PayPal: The legal status of C2C payment systems".* Computer Law & Security Report, pp.2-4. Available online at www.researchgate.net. PayPal is covered under the scope of e-money directive 2009/110/EC.

identity of the payee. Thus, like in the transaction scenario of cash, identity of the payer and the payee are also anonymous in a bitcoin transaction.

Bitcoin differs from cash and appears to be more similar to traditional electronic transactions due to the transparency of bitcoin addresses. All transactions of a bitcoin address, from the first ever bitcoin transaction to the last, are recorded in the public ledger. Hence, one can look to the public ledger (Blockchain) and see all transactions associated with the particular bitcoin address, the public key.[166] Publicly shared ledger makes these payments pseudo-anonymous rather than completely anonymous as cash payments.

However, upgrading personal security for the usage of cryptocurrency is possible through cryptocurrency mixing services/tumblers such as Helix, Bitcoin Blender and Ethereum Mixer. These services offer protection of privacy by mixing funds with others to hide where cryptocurrency came from originally and clean user's coin (layering phase). These systems function similar as one moves its funds through financial institutions located in countries that have strict bank secrecy laws such as Panama, Philippines, Cayman Islands and Curacao.[167]

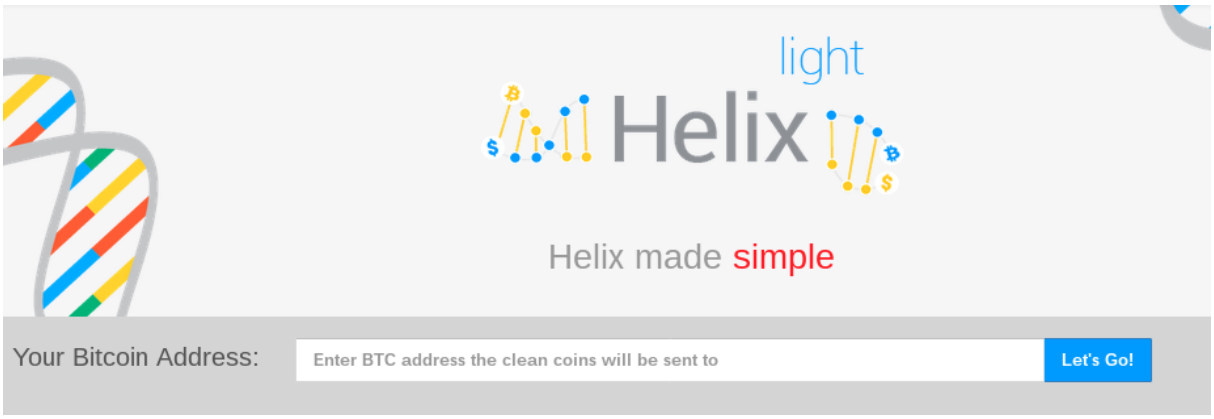

Figure 4. Helix Mixer – Cleaning Screen[168]

So one can easily say that, permitting some level of anonymity and existence of cryptocurrency mixing services or tumblers to upgrade user anonymity makes

[166] Brito, J. & Castillo, A. (2013), "*BITCOIN A Primer for Policymakers*". MERCATUS CENTER, George Mason University, pp.8.

[167] United States Department of State Bureau for International Narcotics and Law Enforcement Affairs (2014), "*International Narcotics Control Strategy Report, Volume II, Money Laundering and Financial Crimes". pp. 36.*

[168] Helix Mixer. Accessed from mixerrzpzcbjj2kl.onion. [Accessed on 05.10.2017]

cryptocurrency, including bitcoin, highly desirable for money launderers, terrorists and others who carry out illegal schemes (criminal activities).

b. Easy, Cheap, Fast and Irrevocable International Transmissibility

Another reason why bitcoin is perceived as a potential money laundering and terrorist financing tool is linked with its cheap, quick and easy international transmissibility. A transaction is permitted to be sent from any place to anywhere, at any time and in any amount. For instance, a person located in Country A may initiate a transaction through an online exchanger located in Country B in order to acquire cryptocurrency with the national currency of Country C. Obtained cryptocurrency can be transmitted to a receiver located in Country D. Receiver may convert his/her cryptocurrency to the fiat currency of Country E, through an exchanger in Country F.

Additionally, while the costs of international transaction are much lower for peer-to-peer network than fees required trusted third parties (financial institutions), its transfer is completed within minutes instead of waiting for days. Moreover, surveillance of a transaction by financial institutions is not possible, so there is no authority to report and stop a suspicious transaction that contains abnormal money flow or to require a registration of cross-border transactions exceeding certain value threshold. Cash transactions are also characterized by being irreversible. Once made, there is no way it to be reversed by a financial institution or the user. But there is one factor that makes bitcoin an ideal payment method comparing with cash, which is the complexity of carrying large amounts of cash around the world. [169] It is too weighty and burdensome to transfer large amounts of money without the attention of authorities. Cryptocurrency, on the other hand, has no physical existence as a coin or a banknote. It faces with no transfer obstacle.

c. Non-centralized Institutions

Cryptocurrencies are popular due to their de-centralized nature. They are not backed by any public or private authority. Thus there is no central institution for monitoring purposes. Traditionally what hardens operations of money launderers, terrorists or persons who are involved in illegal activities, is the control mechanism carried out by the financial institutions through a system that allows transactions and group actions to be tracked. By carrying out due diligence, know your client mechanisms and reporting

[169] Mimic, M. (2014), "*REGULATORY CHALLENGES OF ALTERNATIVE E-CURRENCY, COMPARATIVE ANALYSIS OF BITCOIN MODEL IN US AND EU JURISDICTIONS".* Central European University, pp.27.

suspicious transactions those institutions ensure the functionality of AML/CFT and mitigate the risks. Yet, in a peer-to-peer electronic transaction network, there is no central institution to ensure a functioning AML/CFT mechanism.

Up to a certain level, exchangers may operate as a control mechanism. They can subject their clients to CDD and minimize the anonymity of a user. Nonetheless, exchangers can never fully function as financial institutions since international transactions of cryptocurrency take place without any central channel, where the value is not transmitted through exchangers. In their case observing a transaction, not to mention reporting a suspicious transaction, will be impossible. Considering all the factors highlighted above, it is obvious to understand why criminals are attracted to this system.

Despite all the captivating features for money launderers and terrorist financers that are highlighted above, bitcoin has setbacks which limits its usefulness. These unattractive features are: unpredictable changes in the value of cryptocurrency, volatility of the currency, potential cryptocurrency wallet theft, failure to convert fiat currency to cryptocurrency or vice versa due to supply, demand and cost issues and rising regulatory awareness.[170]

[170] Brill, A. & Keene, L (2014), "*Cryptocurrencies: The Next Generation of Terrorism Financing?*" Defence Against Terrorism Review, Vol. 6, No. 1, Spring&Fall 2014, ISSN: 1307-9190, pp.15.

Part IV. EU AML/CFT Directive in the Age of Virtual Currency

1. The European Union Takes a Notice

Identified risks related to the anonymity and decentralized nature of the virtual currency and its tendency to be used by criminals to conceal the source of the illegal gains raised concerns of regulators all over the world. Jurisdictions adopted different approaches to mitigate the risks related to the trade and usage of the decentralized virtual currency.

The European Union followed an approach in which the issues related to virtual currency was treated at the theoretical level only, from 2012 to 2016 when the Commission presented a draft regulation amending the Fourth AML/CFT Directive in connection with the reveal of Panama Papers and the terrorist attacks in Paris in 2015.

At the European Union level the first report to be released on virtual currency was held by the European Central Bank on 2012[171], followed by the second report in 2015[172]. The aim of the first report was to conduct a research on virtual currency to create an understanding of the new reality and to pave the way for further discussion. The second report conducted a more detailed study on the examination of virtual currency, its disadvantages in general as well as the advantages over traditional payment systems.[173] In this recent report it seemed that the ECB was still questioning whether a regulation was needed or not, by arguing that the usage of virtual currency as a payment method is still very limited, thus the risks it poses to the banking operations are not materialized yet.

The warning for the first time at the EU level, though, came from the European Banking Authority on 2013, whose objective is regulated in Article 1 (5) of the Regulation establishing the EBA as "to protect the public interest by contributing to the short, medium and long-term stability and effectiveness of the financial system, for the Union economy, its citizens and businesses."[174] The EBA published a document named as "Warning for the consumers on virtual currency"[175] to raise the awareness of the risks related to the buying, holding and trading in virtual currencies, giving specific attention

[171] European Central Bank (2012), "*Virtual Currency Schemes*". Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. [Accessed on 23.09.2017].

[172] European Central Bank (2015), "*Virtual Currency Schemes – A Further Analysis"*. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf. [Accessed 21.09.2017].

[173] European Central Bank (2015), "*Virtual Currency Schemes – A Further Analysis"*.pp.33.

[174] European Union (2010) , "*Regulation (EU) No 1093/2010 of the European Parliament and of the Counsil of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC*". Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010R1093-20160112. {Accessed on 17.09.2017].

[175] European Banking Authority (2013), "*Warning to consumers on virtual* currencies".

to the new generation virtual currencies, cryptocurrency. The warning invited consumers to be cautious when being a part of the Bitcoin system by taking their attention to its high volatility, vulnerability to attacks, tendency to be used for criminal activities and the lack of protection that could be offered from any authority.

A comprehensive report was released by the EBA on 2014 which identified economic and individual benefits as well as various risks related to the users, non-user market participants, financial integrity, payment systems and payment service providers in FCs and regulatory authorities. Unlike the ECB reports, the EBA embraced the urgency of a regulation by arguing that some risks have already been materialised[176] and recommended a possible long and short term regulatory approach taking into consideration the risks drivers. Until a more comprehensive regulatory regime is adopted, the report recommended that "the national supervisory authorities discourage credit institutions, payment institutions, and e-money institutions from buying, holding or selling VCs, thereby 'shielding' regulated financial services from VCs"[177] and the virtual currency exchangers to be subjected to AML/CFT requirements as obliged entities under anti-money laundering and counter terrorist financing laws.[178]

For a consistent and a successful legislation European Banking Authority highlighted the need of a harmonized response at the EU level by putting forward the disadvantages of a segregated legislation due to the peer-to-peer nature and the international transmissibility of the virtual currency. It furthermore justified its argument by expressing that the non-coordination would lead to different regimes and eventually to forum shopping for the most favourable approach.[179]

Following the terrorist attacks in Paris at the fall of 2015, the European Commission highlighted the need for European Union to work on policies to fight against terrorism and to prevent the movement of funds to be used for used for terrorist activities. Financial and technological innovations were stressed out to be the reason for the need of a policy update. As a consequence of this need and the reveal of the Panama Papers, the European Commission adopted an "Action Plan to strengthen the fight against the financing of

[176] European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". pp.44. Retrieved from https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf. [Accessed on 23.08.2017].

[177] European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". pp.44.

[178] European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". pp.44.

[179] European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". pp.46.

terrorism"[180] in order to prevent and fight terrorism[181]. The gaps identified were: cash and trade in artefacts, virtual currency and the anonymous pre-paid cards.[182] In the Communication, the Commission not only recommended various actions to be taken under existing laws but also recommended a legislative proposal to amend Fourth AML Directive in the points of: "enhanced due diligence measures/countermeasures with regards to high risk thirds countries; virtual currency exchange platforms; prepaid instruments; centralised bank and payment account registers or electronic data retrieval systems, the access of Financial Intelligence Units to, and exchange of, information."[183]

In the Action Plan, the Commission acknowledges the fact that the virtual currencies are not regulated currently under the EU law, thus there is no authority to monitor and control the suspicious transactions.[184] Furthermore, the real issue related to virtual currency was found to be its nature of anonymity.[185] Hence, the Commission proposed in the Action Plan "to bring anonymous currency exchanges under the competent authorities by extending the scope of the AMLD to include virtual currency exchange platforms, and have them supervised under Anti-Money Laundering/ countering terrorist financing legislation at national level"[186]. With the amendment, the users of the virtual currency would be subjected to due diligence requirements whenever they wish to exchange their virtual currency for "fiat currency", and vice versa, through the exchange platforms and deduce the level of anonymity related to virtual currency transactions. Application of the

[180] European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*". Retrieved from http://eur-lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0002.02/DOC_1&format=PDF. [Accessed on 31.10.2017].

[181] European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*". pp.2.

[182] European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*".

[183] European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*". pp.9.

[184] European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*". pp.3.

[185] "New financial tools such as virtual currencies create new challenges in terms of combatting terrorist financing. Highly versatile criminals are quick to switch to new channels if existing ones become too risky. For innovative financial tools, it is critical to be able to manage the risks relating to their anonymity, such as for virtual currencies. Critical to this question is less the forms of payment themselves, but rather whether they can be used anonymously." *See* European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*".pp.3.

[186] European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*". pp.5.

rules under the Payment Services Directive related to licensing and supervision to the virtual currency exchange platforms was considered by the Commission as a policy option to be assessed further along with the regulation of the virtual currency "wallet providers".[187] The Commission presented its proposal for "amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC"[188] on July of 2016.

Recently, on February 2016, the European Parliament's Committee on the Economic and Monetary Affairs issued a draft report on virtual currencies[189]. The Committee adapted a neutral approach when examining the virtual currency and the Blockchain Technology. The report exhibited that the Committee is willing to consider the new ideas and is unprejudiced against the widespread usage of both virtual currency and distributed ledger technology.

The report by touching upon many factors created a deep understanding of the virtual currencies as well as the Blockchain technology (Distributed Ledger Technology - DTL) that lies under the Bitcoin system. The draft report stressed that the virtual currency comparing with the traditional online payment systems is indeed cheaper, faster and provides high degree of privacy but does not operates without vulnerabilities related to the pseudo-anonymity[190], the existence of mixing services, lack of safeguards for consumers and lack of legal certainty.[191] Furthermore, high exchange rate volatility, expensive operational costs of the virtual currencies due to the consumption of electricity were indicated in the report as the disadvantages. The consumers and the Member States were informed with the objective of raising awareness.

---

[187] European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*". pp.5.

[188] European Commission (2016), "*Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*".

[189] European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))". Retrieved fromt* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0168+0+DOC+XML+V0//EN. [Accessed on 31.10.2017].

[190] Creating tendency to be used on the black market, for money laundering, tax evasion and for financing of terrorism.

[191] European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))". pp.6.*

Along with the comprehensive information regarding the disadvantages, the report stressed the potential benefits of the utilization of distributed ledger technology not only in the context of virtual currency but also of financial technology and beyond such as smart contracts and the registration of intellectual property rights. The report encouraged the investment in Distributed Ledger Technology for the optimization of various day to day operations at the financial[192] and governmental services. The draft report recommended a possible regulation[193], which in one hand accommodates the further innovation and avoid any "pre-emptive and heavy-handed regulation that would stifle growth"[194]. On the other hand it suggested regulators to develop sufficient laws to respond the risks before they become systemic[195].

The ECON report welcomed the European Commission's Action Plan to amend the Fourth AML Directive to bring the virtual currencies under AML/CFT laws scope and to render virtual currency exchange providers "obliged entities", in ending the anonymity associated with the virtual currency operations.[196] The ECON did not only considered the need of an amendment of the AML laws of the EU but recommended to the Commission to assess the all possible risks related to the virtual currency and accordingly to revise other relevant legislations when needed, including the Electronic Money Directive (EMD), Payment Services Directive (PSD) and the Payment Accounts Directive (PAD).[197] Furthermore, the ECON report called for the creation of a task force (TF DLT) consisting of experts to further investigate virtual currency and to revise existing European regulation if found necessary to tackle with the challenges.[198]

---

[192] BNP Paribas is exploring the private use of Blockchain Distributed Ledger Technology since 2016 in order to make the sharing of collateral valuation (involving manual reconciliation for the unsecured transactions involving multiple parties) less complex and less-time consuming. *See* BNP Paribas (2017), "*CO-CREATION, CLIENTS AND BLOCKCHAIN: MYCOLLAT".* Retrieved from https://cib.bnpparibas.com/adapt/co-creation-clients-and-blockchain-mycollat_a-2-1041.html. [Accessed on 27.01.2017].

[193] The report suggested a smart regulation towards fostering innovation and safeguarding integrity. *See* European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))", pp.*8.

[194] European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))".* pp.8.

[195] European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))".* pp.9

[196]European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))".* pp.8.

[197] European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))".* pp.8.

[198] European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))".* pp.9.

In addition to the Committee on Economic and Monetary Affairs, the Committee on the Internal Market and Consumer Protection (IMCO) presented its opinion on virtual currencies[199] for the Committee on Economic and Monetary Affairs to consider as a responsible committee, in April 2016. In the report, the Committee highlighted the need of an effective regulatory responses by recognizing the risks related to virtual currencies in relation to criminal activities as financial crimes (tax fraud, tax evasion, financing of terrorism, etc.) which does not prevent further innovation due to the benefits that it may offer in the future.[200] IMCO asked Commission to "develop a coherent and comprehensive strategy at EU level"[201] and to consider the revision of the Fourth AML Directive[202].

Considering the different approaches mentioned above, one may easily conclude that the European Parliament has been cautious in approaching the virtual currencies. On one hand, it highlights the need of regulation keeping in mind the risks, and on the other hand by acknowledging the economic and technological benefits offered by the virtual currencies, the Parliament has been recommending smart policies.

2. National Responses to Virtual Currency in the EU

The usage of virtual currencies, particularly Bitcoin as a math-based, decentralized virtual currency (cryptocurrency), grew in numbers and still has been growing. It attracted thousands for various and differentiated reasons and became a widespread phenomenon despite the bad reputation that it gained starting from the reveal of the Silk Road and Bitcoin's involvement in it as the facilitator of money laundering and drug trafficking. Despite some that think that the "virtual currencies are the wave of the future for payment systems"[203], for many the Bitcoin remained associated with the criminals or "sanction evaders to move and store illicit funds, out of the reach of law enforcement and other

[199] European Parliament, Committee on the Internal Market and Consumer Protection (2016), "*OPINION on virtual currencies (2016/2007(INI))". Retrieved from* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-577.006%2b02%2bDOC%2bPDF%2bV0%2f%2fEN. [Accessed on 22.11.2017].

[200] European Parliament, Committee on the Internal Market and Consumer Protection (2016), "*OPINION on virtual currencies (2016/2007(INI))".* pp. 3-5.

[201] European Parliament, Committee on the Internal Market and Consumer Protection (2016), "*OPINION on virtual currencies (2016/2007(INI))".*pp.4.

[202] European Parliament, Committee on the Internal Market and Consumer Protection (2016), "*OPINION on virtual currencies (2016/2007(INI))".*pp.5.

[203] FATF (2014), "*FATF Report, Virtual Currencies Key Definition and Potential AML/CFT Risks*". pp.3.

authorities"[204]. The prosecution of the case in New York State and other cases that followed the first one, took attention of the regulators all over the world and signalled the need of a proper legislation.

Regulating a decade old technology is not easy. Drafting a regulation requires expertise in the subject matter. All the relevant aspects of the technology should be worked on and understood well in order to set forward a legislation that both recognizes and responds to the risks and does not put limitations to the benefits that this technology would offer in the future. This was the case that the regulators faced with when revising the relevant laws in line with new challenges. In this case the challenge was a decentralized and pseudo-anonymous virtual currency, Bitcoin.

The first issue as mentioned in the previous chapter was the determination of the legal status of Bitcoin. For many, it did not fulfil the requirements of being neither a currency nor a money. Lack of legal status created complexities in regulating the subject matter and differences between the national laws. While the EU, as a regional body, did not set forward a harmonized response towards the virtual currencies until the Commission proposal amending the Fourth AML Directive and solely published opinions aiming to raise awareness of the users and the national authorities, different Member States of the EU followed different methods in responding the issue.[205] The differences in approaches raised from the differences in the legal and institutional framework and the interpretation differences.[206] While some Member States solely gave a warnings about Bitcoin in reference to EBA warnings such as UK, Malta and Slovenia, some subjected the Bitcoin exchanges to specific requirements such as France, Germany and Sweden by consulting the EBA, ECB and FATF reports and opinions on virtual currency.[207]

In order to show the variety, the paper draws attention to the responses of Germany, France and Spain to Bitcoin/virtual currency below.[208]

[204] FATF (2014), "*FATF Report, Virtual Currencies Key Definition and Potential AML/CFT Risks*". pp.3.

[205] Responses are mainly directed to Bitcoin due to its prominent status among other virtual currencies as a decentralized, pseudo-anonymous cryptoccurency.

[206] Lexology, WH Partners (2017), "*Virtual currencies in Malta. The brave new world Bitcoin*". Retrieved from https://www.lexology.com/library/detail.aspx?g=3627fc49-6219-4fce-92bc-4ddc42efb9e7. [Accessed on 06.01.2018].

[207] European Central Bank (2015), "*Virtual Currency Schemes – A Further Analysis"*.pp.34-37.

[208] Country Specific responses can be found in European Central Bank (2012), "*Virtual Currency Schemes*", pp.34-37.

i. Germany

Federal Financial Supervisory Authority (BaFin) of Germany, under the consumer protection matter, released a warning document "Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer" (Bitcoins: Supervisory assessment and risks to users) in December 2013[209], providing a comprehensive assessment of the Bitcoin for the public. The attention is given to Bitcoin, however the publication explicitly indicates that the article is applicable to other decentralized virtual currencies as well.

In order to supervise the exchanges of Bitcoin, BaFin classifies Bitcoin as a unit of account that does not hold a legal tender conforming with the German Banking Act (Kreditwesengesetz- KWG) section 1 (11).[210] It is explicitly stated that the Bitcoin differs from e-money which is regulated under "German Payment Services Supervision Act" (Zahlungsdiensteaufsichtsgesetz- ZAG) since there is no authority that issues Bitcoin unlike e-money.[211] By the German Law, Bitcoin is considered as a private money that functions as a means of payment in private transactions. Thus the debt cannot be paid by Bitcoin unless the debtor and the creditor agrees on using Bitcoin as the means of payment.

According to BaFin, the buying, selling, mining and usage of Bitcoin is not subjected to authorization and a license is not required for these activities to be carried out. However, BaFin also specifies particular circumstances in which the authorization might be asked from the seller, miner, buyer or the users. Authorization requirement applies in situations "where it is not only the case that BTC are mined, purchased or sold to participate in an existing market but in addition a special contribution is paid to create or preserve such market"[212]. One of those situations occurs when a market participant buys, sells and mines Bitcoin for merely commercial purposes in which the economic advantages arise for a third party. That market participant is considered as a broker under the German Law and is subjected to an authorization to operate. Other participants that are subjected to an

[209] Federal Financial Supervisory Authority (BaFin) (2014), "*Bitcoins: Supervisory assesment and risks to users*". Retrieved from https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html. [Accessed on 21.01.2018].

[210] Federal Financial Supervisory Authority (BaFin) (2014), "*Bitcoins: Supervisory assesment and risks to users*". pp.2.

[211] Federal Financial Supervisory Authority (BaFin) (2014), "*Bitcoins: Supervisory assesment and risks to users*". pp.2.

[212] Federal Financial Supervisory Authority (BaFin) (2014), "*Bitcoins: Supervisory assesment and risks to users*". pp.3.

authorization are the participants who buys or sells Bitcoin in exchange of fiat currencies (broking and proprietary trading) and who operates a multilateral trading platform.[213]

ii. France

The French Banking Federation organized a working group to work on virtual currencies in June 2014 in order to recommend policy options to prevent the usage of virtual currencies for fraudulent purposes and money laundering.[214] The working paper was a warning for the users, highlighting the sources of risks namely the presence of unregulated participants, lack of transparency and extraterritoriality.

The lack of legal classification of Bitcoin refrains it both from being treated under the existing laws and from being regulated. Yet, there are no French laws regulating virtual currency. However, according to the French Banking Federation (FBF) revenues of the sales of Bitcoins through a bank account may require the bank to file a declaration to the French anti-money laundering agency.[215]

iii. Spain

Virtual currencies are not classified as legal currency under the Spanish laws due to their decentralized nature.[216] The legal definition of Bitcoin in Spain was put forward by Pablo Fernández Burgueño in its Article called "12 Cosas Deberías saber antes de usar Bitcoins (Le ley y el Bitcoin)"[217] , "*12 Things You Should Know Before Using Bitcoins (Law and Bitcoin)*". According to the article "A Bitcoin is an intangible digital asset, functions as a unit of account created by and transferred through a computer system which cannot be copied"[218].

[213] Federal Financial Supervisory Authority (BaFin) (2014), "*Bitcoins: Supervisory assesment and risks to users*". pp.3-4.

[214] Republique Française, Ministère des Finances et des Comptes Publics, Virtual Currencies Working Group (2014), "*Regulating Virtual Currencies. Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering".* Retrieved from https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf. [Accessed on 07.01.2018].

[215] Coindesk, Adamowski, J. (2014), "*France: Bitcoin Revenues Must be Declared to Tax Authorities"*. Retrieved from https://www.coindesk.com/france-bitcoin-revenues-must-declared-tax-authorities/. [Accessed on 07.01.2018].

[216] European Central Bank (2012), "*Virtual Currency Schemes*". pp.35.

[217] Burgueño, P. F. (2013), "12 Cosas Deberías saber antes de usar Bitcoins (Le ley y el Bitcoin)". Retrieved from https://www.abanlex.com/2013/11/12-cosas-que-deberias-saber-antes-de-usar-bitcoins/. [Accessed on 07.02.2018].

[218] Burgueño, P. F. (2013), "12 Cosas Deberías saber antes de usar Bitcoins (Le ley y el Bitcoin)".

Under Spanish laws, virtual currency is not regulated. However a judgment of Provincial Court of Asturias[219] of 2015 raised the question of whether the sale and exchange of Bitcoins was subjected to the AML legislation[220] of Spain.

The case includes Meetpays, a service provider for buying Bitcoins with credit cards, and Caja Laboral, a credit institution. After entering into an affiliation agreement to systems of Mastercard and Visa which included the installation of Point of Sale (POS)[221], Meetpays sued Caja Laboral for not fulfilling its contractual obligations. The defendant argued that the POS operation was never activated thus the contract never became effective due to the fact that it could not guarantee the requirements of diligence since the payments could be done in Bitcoin, anonymously, without being subjected to any fees, worldwide and without the disclosure of the source of funds. Article 16 of the Law 10/2010 was referred in the judgment which obliges financial institutions to draw attention to risks of money laundering related to new technologies and services allowing anonymity.[222]

The court furthermore referred to the Article 7.3 of the Spanish AML Act stating that "the cases in which the obliged entities cannot guarantee the measures of diligence under the law, they have the right to not establish a business relationship or may terminate the execution of the operation". Upon the referral, the court dismissed the claims of the plaintiff and decided in favour of the defendant, Caja Laboral.

What can be said about the Spanish AML Law is that, it does not regulate the virtual currency or oblige virtual currency exchanger to comply with AML laws regarding the KYC and CDD measures explicitly. However, it indirectly by the Article 16 of the Law 10/2010 obliges entities to take necessary measures to carry out due diligence. Hence, the virtual currency falls under the scope of Spanish AML Act.

---

[219] LAW & BITCOIN (2015), "*Judgement of the Court of Asturias. Judgment No: 00037/2015*". Retrieved from http://lawandbitcoin.com/en/judgment-of-the-provincial-court-of-asturias/. [Accessed on 07.01.2018].

[220] Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Available online at https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737.

[221] "A point of sale system encompasses the hardware, software, and support that manage that transaction, including credit card processing, and the post-transaction operations that lead to customer fulfillment, whether in a retail or restaurant setting." Available at https://pos.toasttab.com/what-is-pos.

[222] LAW & BITCOIN (2015), "*Bitcoin and Anti-Money Laundering Part I*". Retrieved from http://lawandbitcoin.com/en/bitcoin-and-anti-money-laundering-part-i/. [Accessed on 05.02.2018].

Examples given above regarding the differences in legal frameworks and actions taken towards virtual currency/Bitcoin put forward the current situation of the virtual currency in EU. The regime is not harmonized at the EU level which creates disadvantages for the anti-money laundering and counter financing of terrorism policies of the EU. The lack of a harmonized action and differences in the national regimes create insufficiencies in accomplishing the objectives of preventing the usage of virtual currencies for fraudulent purposes and money laundering. The current situation prevents the large scale success of the policies and renders the national actions inadequate due to the international transmissibility of the virtual currency. Furthermore, it leads criminals to the "virtual currency industry shopping"[223], where they benefit from the most favourable regulation, create different levels of protection for the system participants and differences in the liabilities of the legal persons.

Therefore, for the achievement of the objectives; mitigation of financial crimes and fraudulent activities and the protection of the system participants, internal market and the financial stability, an action at the EU level is crucial and necessary. To establish a minimum level of combating mechanisms through criminal law and a harmonized regime at the EU level, the Commission proposed to amend the Fourth AML/CFT Directive in 2016. Haven't been accepted yet, its adequacy to tackle with the money laundering and financing of terrorism risks related to virtual currency, particularly cryptocurrency, is questionable. The next section is dedicated to the changes brought to the Fourth AML Directive in regards to virtual currency. The clauses added to the Directive are assessed in order to answer the main question of this paper; whether the proposal provides sufficient combating mechanisms against the risks related to virtual currency or not. The evaluation is done by taking the characteristics of cryptocurrency giving rise to the risks into account.

3. Commission Proposal to Amend 4th AML/CFT Directive and Virtual Currency

As a conclusion of the Justice and Home Affairs Council of November 2015, the Economic and Financial Affairs Council of December 2017, the European Council of December 2015 and as the part of the Action Plan to strengthen the fight against financing of terrorism, the Commission revised Anti-Money Laundering rules and proposed an

[223]European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". pp.46.

amendment of the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC on July 2016.[224]

The revision was drafted in line with the recommendations of the European institutions such as EBA, ECB and ECOFIN Council, as well as the international policy guidance published by the Financial Action Task Force to form an international standard and to fill the gaps in the existing regimes to tackle with the new challenges introduced by the advances in technology and communications that blurs the transparency of financial transactions. In the explanatory memorandum of the proposal, it is indicated that the primary objective of the revision is to "prevent the large-scale concealment of funds which can hinder the effective fight against financial crime, and to ensure enhanced corporate transparency so that true beneficial owners of companies or other legal arrangements cannot hide behind undisclosed identities."[225]

The proposal is drafted in compliance with the principles of proportionality and subsidiarity regulated in Article 5 of the TFEU, the personal data protection laws of the EU; Directive (EU) 2016/680[226] and Regulation (EU) 2016/679[227]. Fundamental rights particularly the right to private and family life set out in Article 7, the protection of personal data set out in Article 8 and the freedom to conduct business set out in Article 16 of the Charter of the Fundamental Rights are recognized in accordance with the Article 6(1)[228] of the TEU.

---

[224] European Commission (2016), "*Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*".pp.3.

[225] European Commission (2016), "*Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*". pp.2.

[226] European Union (2016), "*Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*".

[227] European Union (2016) , "*Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*". General Data Protection Regulation.

[228] Article 6(1) of the TEU states that "The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."

Points that were amended in the proposal in regards to the virtual currencies are as follows:

Article 1 (1) of the Proposal amends the Directive (EU) 2015/849 Article 2(1), regulating the obliged entities whom are subjected to specific requirements under the Directive. The scope of the obliged entities who are natural or legal persons acting in the exercise of their professional activities (point 3 of Article 2(1)) was extended to include point (g) and (h) to cover exchange platforms of the virtual currency and the wallet providers offering custodial services. The matter is regulated as the following: "(g) providers engaged primarily and professionally in exchange services between virtual and fiat currencies; (h) wallet offering custodial services of credentials necessary to access virtual currencies."[229]

By the inclusion of the custodial wallet providers and the virtual currency exchange platforms to the obliged entities, the system participants who buy or sell their virtual currencies through these service providers are rendered to disclose their identity through Know Your Client and are subjected to due diligence measures regulated in Chapter II Section 1,2 and 3. The sale, purchase and usage of the virtual currencies can be monitored by the competent authorities which would increase transparency in the transactions of virtual currency. Extending the scope of the Directive makes virtual currency exchange platforms and custodial service providers the gatekeepers of the Anti-money laundering and counter financing of terrorism laws, as well as the authority who controls the access to virtual currency.

The circumstances in which the due diligence is required to be carried out is set out in Article 11 of the Fourth AML Directive. In regards to these service providers, the circumstances are as the following; "(a) when establishing a business relationship; (b) when carrying out an occasional transaction that amounts EUR 15000 or more, constitutes a transfer of funds exceeding EUR 1000; (c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more; (e) when there is a suspicion of money laundering and terrorist financing, regardless of any derogation, exemption or threshold; and (f) where there are doubts about the veracity or adequacy of previously obtained customer identification data."[230]

[229] Article 1(1).

[230] Article 11.

Another change to be brought to the Fourth AML Directive is within Article 3 setting out the definitions to apply for the purpose of the Directive. Point (18) is added to define virtual currencies with the purpose of reducing complexities in defining virtual currency and consequently adopting measures tailored for the characteristics of virtual currency.

According to Article 3 (18) of the proposal " 'virtual currencies' means a digital representation of value that is neither issued by a central bank of a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically."[231] In this regard the definition of the virtual currency may seem to carry similarities with the German Law regulating Bitcoin like a 'private money'. It functions as a means of payment as long as the parties involved, natural or legal persons accept it as one.

The proposed amendment to the Fourth AML Directive requires virtual currency exchange providers and custodian wallet providers to be licensed or registered, which is set out in Article 1, point 16 of the proposal. Article 47(1) is replaced by the following clause; "Member States shall ensure that providers of exchanging services between virtual currencies and fiat currencies, custodian wallet providers, currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated."[232] This is a complementary clause in achieving the control over exchange services providers and the custodian wallet services and ensuring that they will oblige with the requirements set out in the Directive. Additionally, registration of these platforms allows authorities to monitor transactions of virtual currency. Business licenses of virtual currency are regulated and issued by some jurisdictions already. One of the first licenses granted was by the New York State Department of Financial Services. Being issued in New York State, the license only covers those platforms operating in that area. The law prohibits exchange platforms who does not hold business license to operate.[233]

The changes mentioned above are the clauses which directly regulates virtual currency to mitigate the money laundering and financing of terrorism risks. There are clauses that are

[231] Article 1(2).

[232] Article 1(16).

[233] New York State Department of Financial Services, New York Codes, Rules and Regulations (2015), "*Title 23. Department of Financial Services, Chapter I. Regulations of the Superintendent of Financial Sevices Part 200. Virtual Currencies*".pp.7. Retrieved from https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf. [Accessed on 10.08.2017].

indirectly linked to virtual currency, exchange service and custodial wallet providers. According to Article 1(11) section (a) and (b) of the proposal, Article 32 of the Fourth AML Directive is amended. Section (a) adds a paragraph 9 to the Article 32 stating that "In the context of its functions, each FIU shall be able to obtain from any obliged entity information…"[234] In this regard, the reporting and the monitoring agency for the virtual currency exchange providers and the custodial wallet providers are determined as Financial Intelligence Units, as it is for the financial institutions. Pursuant to Article 33 of the Directive (EU) 2015/849, those platforms related to virtual currency are obliged to monitor transactions and to carry out necessary investigations to understand the nature of the transaction and if found suspicious, to make a suspicious activity report (SAR) to the FIU of the member state, "on their own initiative"[235] or by "request"[236].

By analysing the changes to be brought to the Fourth AMLD in relation to virtual currencies, we can observe that the proposal offers set of rules that are promising, as it takes steps towards the characteristics of cryptocurrencies giving rise to AML risks. A detailed argument on the measures and their effect will be carried below.

4. Analysis of the Proposal

We can conclude by analysing the responses given by the European Union that even though virtual currency was given attention to before, terrorist attacks along with the concerns on tax evasion following the offshore scandals alarmed European Commission towards virtual currencies that are facilitating criminal activities through anonymous transactions.[237] And here, as it has been the case since 1980, the AML law was forced once again to evolve to be responsive towards new challenges. This time for the virtual currencies.

It is possible to say that bringing virtual currency exchange platforms and the custodial wallet providers under the due diligence and know your client requirements will contribute to the achievement of the objectives of this proposal which are obtaining

[234] Article 1 (11) (a).

[235] Article 33(1) (a) of Directive (EU) 2015/849.

[236] Article 33 (1) (b) of Directive (EU) 2015/849.

[237] BITCOIN MAGAZINE (2016), "*EU State-By-State Regulation of Bitcoin, Digital Currencies: What Are the Implications?*". Retrieved from https://bitcoinmagazine.com/articles/eu-state-by-state-regulation-what-are-the-implications-1480975527/. [Accessed on 07.01.2018].

transparency in the transfer of funds, mitigating the anonymity of the system participants and monitoring the virtual currency transactions.

The argument takes place below, where 3 characteristics of virtual currency, more specifically cryptocurrency will be assessed in the light of the proposal.

i. Anonymity

As mentioned in the previous Chapter, pseudo-anonymity is one of the major factor why the criminals are attracted to cryptocurrencies. Non-disclosure of the identity works too well for the criminals and ease their operation. Naturally, regulators gave full attention to tackle with the anonymous nature of the cryptocurrencies. Subjecting virtual currency exchange providers and custodial wallet providers to CDD and KYC requirements will help to de-anonymize the users who are trading Bitcoin for a fiat currency and vice versa and whose wallets are under the custody of an agency (custodial wallet provider). Thus, if the proposal is adopted, whenever an individual wishes to obtain cryptocurrency through an exchange service platform, he/she will be subjected to some requirements pursuant to of the Directive. These providers would know their clients through the information collected and they will be able to observe the activities of their clients. The same will apply for the users who keep their cryptocurrency in a custodial wallet where the BTC, or any other cryptocurrency is held by an agency on the user's behalf.[238] Consequently, as the AML/CFT system requires, there will be now a trusted third party, an intermediary for a virtual currency transaction serving like an informant.

Throughout their operations, they will have to report suspicious transactions, the abnormal flow of funds, to the FIUs. However, the factors which render a transaction abnormal or suspicious are unclear.

Virtual currency is relatively a new phenomenon and the transaction patterns are still unknown. Therefore, a comprehensive study should be done in order to understand what is considered as a normal transfer of fund and what is not to help exchange service and custodial wallet providers who are mostly start-ups. The factor of determination of suspicion could be in geographical basis. Jurisdictions considered as high-risk countries by law could be the focal point of the investigations. By this, anytime a fund flows through a high-risk country the system could alert the authorities and be subjected to a

[238] Coinsutra (2017), "*Bitcoin Wallter: Everything a Beginner Needs to know".* Retrieved from https://coinsutra.com/bitcoin-wallet/. [Accessed on 09.01.2018].

thorough investigation. Another factor could be in threshold basis determined in line with the profile of the client. If the client excesses the threshold and cannot prove the rationale behind it, these entities would report it to FIUs. If these remain imprecise, FIUs would be overwhelmed by the amount of the suspicious reports delivered by the exchangers, and left in a position where they cannot distinguish false and true hits.

After the elaboration done above, it is not unusual to say at this point that the proposal would not achieve its objectives to its fullest due to various factors. First of all, it misses the point that the exchangers are not the only means to obtain virtual currency. As mentioned in the previous chapter, users have other options in obtaining virtual currency in exchange of cash (from a local system participant or a friend) or through mining. These alternative ways are as easy as going to a Bitcoin ATM or to an exchanger. And maybe even simpler and faster if the proposal is to be adopted, since no information is required to be disclosed. Within such an exchange, the third trusted party or the intermediary would not be present to function as a financial service. And the AML/CFT Directive will still be not applicable to those circumstances.

Another limitation of the amendment arises from the definition of the exchange services. The exchange services covered by the proposal are the "providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies"[239], obviously it does not cover the exchange services between virtual currencies and other virtual currencies, for instance Ethereum to Bitcoin and vice a versa. Consequently, once again the new Directive will be in short to eliminate anonymous nature of the virtual currency transactions within this context.

Wallets contains private keys[240] of the particular virtual currency address. The user may choose "a wallet based on connectivity[241], the custodianship of keys[242] and wallets related to a specific device[243]"[244]. Custodial wallet providers, covered by the proposal, are the agencies who hold the private keys of the BTC address and exchange on the behalf of the true owner of that currency. According to the proposal, these agencies will have to subject their customers to CDD requirements. They will be obliged to know the identity of the

[239] Article 1 (1) of the Proposal.

[240] Antonopoulos, A. M. (2014), "*Mastering Bitcoin*". O'Reilly Media, First Edition, ISBN 978-1-449-37404-4.pp.84.

[241] Wallets based on connectivity are divided into two types, online and offline wallets.

[242] Custodial and non-custodial wallets depending on whether the user is responsible for its own funds or not.

[243] Device related wallets are the hardware wallets, mobile wallets, desktop wallets and the web wallets.

[244] Coinsutra (2017), "*Bitcoin Wallet: Everything a Beginner Needs to know".*

user and understand their business operations and patterns. As the exchange providers, these entities will be obliged to report to the FIUs whenever they have a reasonable ground to suspect that the transaction is held to benefit a criminal activity.

Until this point, it seems that the virtual currency will be compatible with the AML/CFT laws, since a gatekeeper is restored within the system. But one should not ignore wallets that are taken care by their true owners, the beneficial owners of the account. For those cases, a trusted third party is not present as it was not before the proposal to amend Fourth AMLD. Therefore there no trusted third party to identify the user, monitor, investigate and report the suspicious transactions. And, yet the proposal will not sufficiently eliminate risks related to anonymity for the wallet users who take the responsibility of their own wallets.

It is highlighted above that the proposal will help to de-anonymize only the users who exchange their virtual currency with fiat currency and vice a versa. While it is always questionable how accurate and reliable the information collected would be, the availability of the mixing services/tumbler should not be forgotten. These services offer protection of privacy by mixing funds with others to obscure the origin of funds and clean the coin of the user. Because of the availability of such methods, no matter how detailed, up to date, accurate and reliable the KYC documentation is, the user would still be able to circumvent CDD through these services.

On the other hand, as long as there are jurisdictions that do not regulate cryptocurrency and no limitation is put on the international transmissibility of the coin, criminals could just simply acquire cryptocurrency against fiat currency, or the other way around, in other jurisdictions and use it within EU for the purposes of laundering money or finance terrorism.

The last but not the least, all the measures set forward by the AML/CFT laws regarding the virtual currency, efforts to de-anonymize cryptocurrency users, would be inapplicable and obsolete if the usage of Bitcoin or any other cryptocurrency becomes widespread. Even though it is unlikely for the close future, there is a great possibility that virtual currency will be the future of the traditional payment systems. In such scenario, no one would feel the need to go to an exchange platform to acquire cash against virtual currency simply because they can buy and sell goods and services in exchange of a decentralized virtual currency. Under these circumstances, the money launderers and the financers of

terrorism would be freed from going through KYC and CDD and carry out their operation in ease. Naturally, this payment system would still be a threat for many jurisdictions who are incapable of inserting a trusted third party for virtual currency transactions.

To introduce a more effective and an efficient solution for the de-anonymization process the European Commission seems to consider establishing a mandatory database for the virtual currency holders to self-declare to the authorities[245] -changing the possible plan for a self-declaration system on a voluntary basis[246] as stated in the proposal. However, even the regulator "forces" users of the de-centralized virtual currency, like Bitcoin, no one can actually be enforced to do so since there is no authority having control over the de-centralized system. And without such control, it is too naive to believe that such measure actually would pay off. There is no doubt that in the event of money laundering and terrorism financing, such registry would contribute to the AML/CFT policy but it is way too utopic to believe that a criminal would actually register to this database.

ii. Easy, Cheap, Fast and Irrevocable International Transmissibility

Another reason why Bitcoin is perceived as a potential money laundering and financing of terrorism tool is because of its comparative advantage against the traditional payment systems relating to its speed, the amount of transaction fees and the international transmissibility which is supported by the Bitcoin Protocol. While the proposal may seem to be incapable to have a direct effect on those characteristics[247], it is true that it actually may influence.

Virtual currency exchange platforms subjected to AML/CFT responsibilities, like financial institutions, will find themselves in a situation where the law compliance will be too burdensome due to the costs[248]. No one can be sure but there is a great change for those compliance and administration costs, rising up dramatically, to find a reflection on the transaction fees put on the customers.

On the other hand, since the on-boarding of a client has to be compatible with the law and all necessary documentation should to be obtained from the customer speed of obtaining

[245] Paraskevopoulos, I. (2017), "*THE THREAT OF MONEY LAUNDERING IN INTERMEDIATED SECURITIES SYSTEMS AND BITCOIN TRANSACTIONS".* International Helleniic University, School of Economics, Business Administration&Legal Studies.pp44.

[246] Recital 7 of the Proposal.

[247] Unless the Bitcoin protocol is changed.

[248] Gathering information, record-keeping, risk assesment, suspicious activity reporting and etc.

cryptocurrency and/or transferring would be affected. Consequently, the comparative advantage of cryptocurrencies would be gradually diminished and some users would be discouraged by the rising costs, slowed and hardened transactions. However these repercussions are still not enough for such currencies to disappear. As long as Bitcoin-like-coins are internationally transmissible and decentralized, there is no regulation that can stop users to benefit from the exchange service platforms in other jurisdictions who operate without being obliged to comply with any regulation. Unless a protocol change is accomplished, those characteristics cannot be altered by anyone or any law.

As mentioned before, peer-to-peer transaction network is similar with the transactions held by cash due to the fact that payments are irrevocable. In the case of wire transfers, fund flowing from or flowing to a suspicious entity would alert the financial institutions and may result in the confiscation of assets generated by criminal activities, which is an important tool to prevent and fight with crime that deprives criminal from its profits. If proceeds of crime is identified and traced in the traditional electronic transaction networks, pursuant to the Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union[249] member states are given rights and tools for the freezing and confiscation of proceeds of crime.[250] However, transactions carried through a decentralized peer-to-peer networks are irrevocable and the nature of Bitcoin makes seizure impossible.

A way, a possibility of confiscation of Bitcoin was mentioned in the FBI released Article "Virtual Currency: Investigative Challenges and Opportunities"[251]. According to the article seizure of Bitcoin could be done through gaining access to the user's wallet which can be kept "on a laptop, thumb drive, or server"[252] as well as on a paper wallet. The paper argues furthermore that prosecutors may use the asset forfeiture laws to seize

[249] European Union (2014), "***Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union*". Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042#ntr4-L_2014127EN.01003901-E0004**. [Accessed on 23.01.2018].

[250] Currently there is a proposal for a Regulation of the European Parliament and of the Council on mutual recognition of freezing and confiscation orders. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0819.

[251] Coin Telegraph, Cohen, B. (2015), "*Governments Seize the Opportunity to Control Bitcoin".* Retrieved from https://cointelegraph.com/news/governments-seize-the-opportunity-to-control-bitcoin. [Accessed on 12.09.2017].

[252] FBI, LEB, Nigh B. & Pelker A. (2015), "*Virtual Currency. Investigative Challenges and Opportunities".* Retrieved from https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities. [Accessed on 18.10.2017].

Bitcoin as a proceeds of crime. However, existence of back-up wallets and volatility of Bitcoin makes the procedure problematic as long as the Bitcoin system remains the same.

iii. Non-centralized Institutions

The Bitcoin protocol and the Ethereum Protocol using consensus to regulate transactions and to prevent double-spending ensure the decentralization of the software.[253] If any individual or a governmental body wishes to shut down all the system, freeze and confiscate the funds that are suspected, it is simply impossible since there is no centralized server.[254]

In the contemporary systems, money moves and the transaction is concluded only if the permission has been given by the financial institution. The system in its nature limits the individual by dictating it to have a bank account and to use a specific fiat currency if he/she wishes to participate to the financial system. On the other hand, peer-to-peer electronic transaction system based on the Blockchain technology gives the society a chance to opt out for the utilization of a centralized service, which is why so many people are interested in this innovation and perceives it as the beginning of a new era for electronic transactions.

Whether the proposal introduces any measures in order to implement a central authority of control and management or not is a question whose answer is already given above. In a Blockchain based, a peer-to-peer transaction network, there is no central institution to ensure a functioning AML/CFT mechanism no matter how stringent the obligations are for the intermediaries, if intermediaries exist. Therefore, no regulation would be good enough to tackle with such technical aspect unless a protocol change is accomplished.

[253] Gencer, A. E. & Basu, S. & Eyal, I. & van Renese, R.& Sirer, E. G. (2018) "*Decentralization in Bitcoin and Ethereum Networks"*.pp.2. Retrieved from https://arxiv.org/pdf/1801.03998.pdf. [Accessed on 01.02.28018].

[254] While decentralization is ensured by the system, it is true that the mining pools where the miners work cooperatively and share the reward, consititute a threat to the decentralization of the system. Especially due to the fact that the top 4 mining pools control more than %50 of the computing power of the whole system. *See* Kaspersky, Malanov, A. (2017), "*Six Myths about blockchaion and Bitcoin: Debunking the efectiveness of the technology".* Available online at https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/.

5. A Possible Long-term Solution

It is clear that the proposal, if to be adopted, will mitigate the risks at some level due to its focus on de-anonymization. However it does not stand as a long-term solution for the problem as it cannot sufficiently tackle with the characteristics attributable to risks.

The most prominent cryptocurrency, which is at the moment is Bitcoin, may lose its attention which it has been getting from all over the world and consequently its value. Even so, certainly there will be more to come in the future as it benefits the users by low transaction fees, no requirement to hold a bank account, giving independency and privacy in transactions. Moreover, because of the technology behind the Bitcoin network, the Blockchain Technology, since it introduces a secure system allowing further innovation in many areas such as self-executing smart contracts, fraud-free voting systems, protection of IP rights and collateral management. Regulators should give full attention to the utilization of the benefits that this technology may present. Accordingly they should not simply ban cryptocurrencies worldwide or implement too stringent rules which would discourage further innovation. On the other hand, they should endorse vulnerability of the system to risks related to money laundering and financing of terrorism and take steps to prevent and fight against possible criminal usage on the basis of an overriding public interest in restoring financial and territorial security. Taking negative and positive aspects of virtual currencies into account, legislations should be drafted in a way that balances promotion of technology and prevention of criminal usage.

While the European Commission's short-term solution stands, the need of a comprehensive long-term solution remains problematic. However, utilization of Blockchain technology to end anonymity and to bring transparency to the system could be the answer.

The possibility of an AML compliant protocol was argued by Gunnar Nordseth Signicat in his article, "Will regulation be a blessing or a blow for Bitcoin?"[255]. According to the article, issue of anonymity could be tackled by using the technology behind Bitcoin itself. "The answer might lie with the Blockchain itself: a distributed ledger would enable

[255] Bankingtech, Signicat, G. N. (2016), "*Will regulation be a blessing or a blow for Bitcoin?*". Retrieved from http://www.bankingtech.com/2016/04/will-the-4th-aml-directive-be-a-blessing-or-a-blow-for-bitcoin/. [Accessed on 15.02.2018].

identity to be built up based on individual ID credentials – their driving license, bank account, government ID, and so on."[256]

Without going technical in the subject matter, what is suggested is a replacement of Bitcoin platform with a new software, also called hard fork protocol change[257]. In hard forks the software simply creates a fork in the Blockchain and splits the previous version of the public ledger from the newest version.[258] Implementation of codes (AML-compliant codes) in this new Bitcoin protocol or creation of AML compliant protocols for new virtual currencies could restore the thrusted third parties and give them the authority to monitor, control, investigate and report all transactions within that Blockchain.

Within the new system whenever the system receives a new participant through the issuance of addresses (public and private keys), the third trusted party would carry KYC and CDD, requiring all the documentation needed for identification of the users and his/her risk profile. Identities and identifying information would be encoded in the system therefore would allow authorities to investigate a transaction whenever that address receives or sends funds.

It is necessary for the new software to recognize abnormal patterns of transactions. In traditional systems a computer-based software carries out risk assessment in line with encoded patterns of abnormality and indicators of suspicion (threshold, watch-list, geographical identifiers). "Pattern recognition software searches millions of bank, brokerage and insurance accounts and review trillions of dollars' worth of transactions each day"[259] To that end, indicators such as threshold, based on the client profile, geographical identifiers and watch lists should be encoded within the new protocol which would allow the system to automatically warn the authorities whenever a threshold is excessed and/or a high risk country client, PEPs, known criminals or terrorists are involved in the transaction. Thanks to the encoded identities and documentation gathered in on-boarding (attribution of public and private keys) of the system participant, the

[256] Bankingtech, Signicat, G. N. (2016), "*Will regulation be a blessing or a blow for Bitcoin?*".

[257] Ethereum went through a protocol change (hard fork protocol change) after DOA drained tokens. By the hard fork, transaction which drained tokens could be reversed. *See* Coindesk, Siegel, D. (2016) "*Understanding The DAO Attack*". Available online at https://www.coindesk.com/understanding-dao-hack-journalists/.

[258] Investopedia, "*Hard Fork*". Retrieved from https://www.investopedia.com/terms/h/hard-fork.asp. [Accessed on 08.02.2018].

[259] Romney, M. B. & John, P. & Mula, J. M. & McNamara, R. P. & Trevor, T. (2013), "Accounting Information Systems". First adaptation Edition, Pearson, pp.354.

responsible person could easily carry out investigation in the basis of risk-based approach and report the suspicious activity to the FIUs. Pursuant to Fourth AML/CFT Directive, FIUs would be able to require information from any obliged entity (in this case, it would be the third trusted party inserted through hard fork protocol change) for the purpose of the prevention the usage of the system for criminal purposes.

Freezing and confiscation of funds is an essential concept in AML and CFT policies, if irrevocability of the transactions is kept in the protocol, rendering criminal businesses unprofitable could not be achieved and consequently further activities could not be discouraged. To that end, an AML-compliant protocol change should contain a feature which allows FIUs to stop a transaction and freeze and confiscate criminal assets when is necessary to do so.

Possible solution argued above is conflicting with the rationale and ideology behind the creation of peer-to-peer electronic transaction systems as the Bitcoin Protocol, without a doubt. It takes away the right to privacy of the user and make them dependent on the system which was proved to be vulnerable by the Financial Banking Crises of 2008.

However, if virtual currency is to be regulated fully and is to coexist with AML/CFT laws, a hard-fork protocol change for the transformation and creation of AML-compliant protocols seem to be the only solution for now, if to be achieved for every single cryptocurrency, considering the fact that there are more than 1000 cryptocurrencies in existence and more to come.[260]

[260] The Motley Fool, Frankel, M. (2018), "*Bitcoin, Ethereum, and Ripple are just the beginning*". Retrived from https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx. [Accesed on 16.03.2018].

Conclusion

Anti-money laundering laws emerged as a tool to cope with transnational narco-trafficking evolved throughout time due to social, economic and political concerns of the era respectively to deal with organized crime and terrorism. Regulatory bodies, international and regional organizations formed international standards to criminalize and prevent money laundering that undermines financial stability, regional and international economy as well as security. This thesis addressed the need of a change in AML/CFT regulations for the purpose of responding to technological developments undermining the current laws, facilitating criminals to conceal the origins of illegal gains and hide behind the emerging technology.

Revision of laws was proposed to be made by acknowledging the distinct characteristics of virtual currency attributable to criminal activities such as decentralized nature, international transmissibility and pseudo-anonymity, as well as the technology behind virtual currency and its possible non-bitcoin applications that would benefit day-to-day activities of financial institutions and intellectual property rights.

In order to answer whether the current AML/CFT laws of the European Union adequately deal with virtual currency or not, this thesis analysed the characteristics of cryptocurrency attributable to the money laundering and terrorism financing offences and examined the Commission proposal amending the Fourth AMLD in the light of those characteristics with the purpose of answering the main research question "Is current AML/CFT Law of the European Union adequate in dealing with virtual currency?".

It was concluded that the proposal to amend Fourth AML Directive remains short in mitigating the AML/CFT risks posed by centralized, pseudo-anonymous nature of cryptocurrency, as well as its international transmissibility. It was argued that even though the amending directive seeks to de-anonymize system participants it does not introduce a sufficient and a comprehensive mechanism as it ignores alternative ways of acquiring cryptocurrency, the existence of mixing services, non-custodial wallet users and the possibility to spend cryptocurrency in real life purchases.

Finally, even though the possibility of achieving for all cryptocurrencies in existence and for the ones to come is questionable, a hard-fork protocol change is proposed as a possible solution to make virtual currency AML-compliant.

Bibliography

Books/Reviews

Antonopoulos, A. M. (2014), "*Mastering Bitcoin*". O'Reilly Media, First Edition, ISBN 978-1-449-37404-4.

Brito, J. & Castillo, A. (2013), "*BITCOIN A Primer for Policymakers*". MERCATUS CENTER, George Mason University.

Cox, D. (2014), "*Handbook of Anti Money Laundering".* WILEY.

Demetis, S. D. (2010), "*Technology and Anti- Money Laundering, A Systems Theory and Risk-Based* Approach". Edward Elgar Publishing Limited, ISBN 978 1 84844 5567.

Hülsse, R. (2007), "*Creating Demand for Global Governance: The Making of a Global Money-Laundering* Problem".

Ioannides, E. (2014), "*Fundamental Principles of EU Law Against Money Laundering*". Ashgate Publishing Company.

Muller, W. H. & Kalin, C. H. & Goldsworth, J. G. (2006), "*Anti-Money Laundering: International Law and Practice*". John Wiley & Sons Ltd.

Paraskevopoulos, I. (2017), "*THE THREAT OF MONEY LAUNDERING IN INTERMEDIATED SECURITIES SYSTEMS AND BITCOIN TRANSACTIONS".* International Helleniic University, School of Economics, Business Administration&Legal Studies.pp44.

Romney, M. B. & John, P. & Mula, J. M. & McNamara, R. P. & Trevor, T. (2013), "Accounting Information Systems". First adaptation Edition, Pearson.

Seagrave, S. (2012), "*Lords of the Rim*". Corgi.

Sullivan, K. (2015), "*Anti-Money Laundering in a Nutshell: Awareness and Compliance for Financial Personnel and Business*".Apress.

Turner, E. J. (2011), "*MONEY LAUNDERING PREVENTION, Deterring, Detecting, AND Resolving Financial Fraud".* John Wiley & Sons, Inc.

Zagaris, B. (2015), "*International White Collar Crime, Cases and Materials*". Berliner, Corcoran & Rowe, Washington, DC, 2nd Edition.

Electronic Sources

Alldridge, P. (2008), "*Money Laundering and Globalization*". Journal of Law and Society, Vol. 35, No. 4 (Dec., 2008), p.442. Retrieved from https://www.jstor.org/stable/40206861?seq=1#page_scan_tab_contents.

Brill, A. & Keene, L (2014), "*Cryptocurrencies: The Next Generation of Terrorism Financing?*" Defence Against Terrorism Review, Vol. 6, No. 1, Spring&Fall 2014, ISSN: 1307-9190.

Baur, D. G. & Hongik, K. H. & Lee, A. D. (2015), "*Bitcoin: Currency or Asset?*". Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736020.

Carlisle, D. (2017), "*Virtual Currencies and Financial Crime, Challenges and Opportunities*". Royal United Services Institute for Defence and Security Studies, ISSN 2397-0286.

CNAS (2017), "*TERRORIST USE OF VIRTUAL CURRENCIES, Containing the Potential Threat".* Energy, Economics & Security.

Gencer, A. E. & Basu, S. & Eyal, I. & van Renese, R.& Sirer, E. G. (2018) "*Decentralization in Bitcoin and Ethereum Networks".*Retrieved from https://arxiv.org/pdf/1801.03998.pdf.

Gurule, J. (1995), "*The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity?*" Scholarly Works, Paper 21, p. 824. Retrieved from https://scholarship.law.nd.edu/law_faculty_scholarship/21/?utm_source=scholarship.law.nd.edu%2Flaw_faculty_scholarship%2F21&utm_medium=PDF&utm_campaign=PDFCoverPages.

Guadamuz, A. (2004), "*PayPal: The legal status of C2C payment systems".* Computer Law & Security Report. Available online at www.researchgate.net.

Mimic, M. (2014), "*REGULATORY CHALLENGES OF ALTERNATIVE E-CURRENCY, COMPARATIVE ANALYSIS OF BITCOIN MODEL IN US AND EU JURISDICTIONS".* Central European University,

Litwak, S. (2015), "*Bitcoin: Currency or Fool's Gold: A Comparative Analysis of the Legal Classification of* Bitcoin". 29 Temp. Int'l & Comp. L. J., pp.345.Available online at www.heinonline.com.

Vandezande, N. (2017), "*Virtual currencies under EU anti-money laundering law*". Computer Law & Security Review 33, KU Leuven Centre for IT & IP Law, pp.342. Available online at www.sciencedirect.com.

Legislations

Decreto-lei n.° 15/93 de 22 de Janeiro 1993, Legislação de Combate à Droga. Artigo 23.°, Conversão, transferência ou dissimulação de bens ou produtos. Retrieved from http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=181&tabela=lei_velhas&nversao=1&so_miolo.

European Commission (2016), "*Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*".

European Commission (2016), "*Proposal for a Regulation of the European Parliament and of the Council on the mutual recognition of freezing and confiscation orders".* Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0819.

European Union, Council of the European Communities, Commission of the European Communities (1992), "*Treaty on European Union*". Maastricht Treaty, ISBN 92-824-0959-7.

European Union (1997), "*Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, signed at Amsterdam 2 October 1997*". TEU Consolidated (1997), ISSN 0378-6986. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1997:340:FULL&from=EN.

European Union (2012), "*Consolidated Version of the Treaty on the Functioning of the* EU". The Lisbon Treaty.

European Union (2012), "*Charter of Fundamental Rights of the European Union 2012/C 326/*02".Article 7. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

European Union (2017), "*Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combatting terrorism and replacing the Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*".

European Union (2017), "*Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office".*

European Union (2017), "*Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law*".

European Union (1991), "*Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering*". 1st AML Directive.

European Union (2001), "*Directive 2001/97/EC on prevention of the use of the financial system for the purpose of money laundering- Commission Declaration*".2nd AML Directive.

European Union (2005), "*Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*". Third AML Directive.

European Union (2015), "*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 purpose of money laundering or terrorist financing*", the 4th AML Directive.

European Union (2015), "*Regulation (EU) 2015/847 on the information accompanying transfers of funds repealing Regulation (EC) No 1781/2006*".

European Union (2016) , "*Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*". General Data Protection Regulation.

European Union (2016), "*Commission Delegated Regulation (EU) 2016/1675 of 14 of July supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies*".

European Union (2009), "*Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money* institutions". Retrieved from http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32009L0110.

European Union (2010) , "*Regulation (EU) No 1093/2010 of the European Parliament and of the Counsil of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC*". Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010R1093-20160112.

European Union (2016), "*Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*".

European Union (2014), "*Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union*". Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0042#ntr4-L_2014127EN.01003901-E0004**.**

Loi n° 87-1157 du 31 Décembre 1987 relative à la lutte contre le trafic de stupéfiants et modifiant certaines dispositions du code penal and Loi n° 88-1149 du 23 Décembre 1988 de Finances pour 1989 . Retrieved from https://www.legifrance.gouv.fr/.

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Available online at https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737.

New York State Department of Financial Services, New York Codes, Rules and Regulations (2015), "*Title 23. Department of Financial Services, Chapter I. Regulations of the Superintendent of Financial Sevices Part 200. Virtual Currencies*".pp.7. Retrieved from https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

UK Drug Trafficking Offences Act 1986. Retrieved from https://www.legislation.gov.uk/ukpga/1986/32/introduction.

Online Sources

Bankingtech, Signicat, G. N. (2016), "*Will regulation be a blessing or a blow for Bitcoin?*". Retrieved from http://www.bankingtech.com/2016/04/will-the-4th-aml-directive-be-a-blessing-or-a-blow-for-bitcoin/.

Burgueño, P. F. (2013), "12 Cosas Deberías saber antes de usar Bitcoins (Le ley y el Bitcoin)". Retrieved from https://www.abanlex.com/2013/11/12-cosas-que-deberias-saber-antes-de-usar-bitcoins/.

BITCOIN MAGAZINE (2016), "*EU State-By-State Regulation of Bitcoin, Digital Currencies: What Are the Implications?*". Retrieved from https://bitcoinmagazine.com/articles/eu-state-by-state-regulation-what-are-the-implications-1480975527/.

BNP Paribas (2017), "*CO-CREATION, CLIENTS AND BLOCKCHAIN: MYCOLLAT".* Retrieved from https://cib.bnpparibas.com/adapt/co-creation-clients-and-blockchain-mycollat_a-2-1041.html.

Coin Telegraph, Cohen, B. (2015), "*Governments Seize the Opportunity to Control Bitcoin".* Retrieved from https://cointelegraph.com/news/governments-seize-the-opportunity-to-control-bitcoin.

Coindesk, Rizzo, P. (2017), "*Indonesia's AML Watchdog Links Bitcoin to Islamic State".* Retrieved from https://www.coindesk.com/indonesias-aml-agency-links-bitcoin-islamic-state-terrorism/.

Coindesk, Adamowski, J. (2014), "*France: Bitcoin Revenues Must be Declared to Tax Authorities"*. Retrieved from https://www.coindesk.com/france-bitcoin-revenues-must-declared-tax-authorities/.

Coindesk, Siegel, D. (2016) "*Understanding The DAO Attack*". Available online at https://www.coindesk.com/understanding-dao-hack-journalists/.

Coin Telegraph (2016), "*Why is My Bitcoin Transaction Taking So Long? Here's Why*". Retrieved from https://cointelegraph.com/news/why-is-my-bitcoin-transaction-taking-so-long-heres-why.

Coinsutra (2017), "*Bitcoin Wallter: Everything a Beginner Needs to know".* Retrieved from https://coinsutra.com/bitcoin-wallet/.

CNBC, Clinch, M. (2013), "*Bitcoin recognized by Germany as 'private money'*". Retrieved from https://www.cnbc.com/id/100971898.

Deloitte (2015), "*The Fourth EU Anti Money Laundering Directive*". Retrieved from https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/investmentmanagement/ie_2015_The_Fourth_EU_Anti_Money_Laundering_Directive_Deloitte_Ireland.pdf.

Egmont Group, "*About". Retrieved from* https://egmontgroup.org/en/content/about.

Forbes, Dorfman, J. (2017), "*Bitcoin Is An Asset, Not A Currency".* Retrieved from https://www.forbes.com/sites/jeffreydorfman/2017/05/17/bitcoin-is-an-asset-not-a-currency/#7669eb222e5b.

Helix Mixer. Accessed from mixerrzpzcbjj2kl.onion.

Investopedia, "*Hard Fork*". Retrieved from https://www.investopedia.com/terms/h/hard-fork.asp.

Kaspersky, Malanov, A. (2017), "*Six Myths about blockchaion and Bitcoin: Debunking the efectiveness of the technology".* Available online at https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/.

Lexology, WH Partners (2017), "*Virtual currencies in Malta. The brave new world Bitcoin*". Retrieved from https://www.lexology.com/library/detail.aspx?g=3627fc49-6219-4fce-92bc-4ddc42efb9e7.

LAW & BITCOIN (2015), "*Judgement of the Court of Asturias. Judgment No: 00037/2015*". Retrieved from http://lawandbitcoin.com/en/judgment-of-the-provincial-court-of-asturias/.

LAW & BITCOIN (2015), "*Bitcoin and Anti-Money Laundering Part I*". Retrieved from http://lawandbitcoin.com/en/bitcoin-and-anti-money-laundering-part-i/.

Nakamoto, S. (2008), "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Retrieved from https://bitcoin.org/bitcoin.pdf.

National Bitcoin ATM Helpdesk (2016), "*How do I use/send the bitcoin I just bought with my receipt?". R*etrieved from http://help.nationalbitcoinatm.com/support/solutions/articles/6000080051-how-do-i-use-send-the-bitcoin-i-just-bought-with-my-receipt-.

New York Post News. (2014), "*Woman arrested with over $70,000 in her stomach". Retrieved from* http://nypost.com/2014/10/25/woman-arrested-with-over-70000-in-her-stomach/.

List of Entities accepting Bitcoin. Retrieved from https://en.bitcoin.it/wiki/Trade. [Accessed on 25.09.2017]

Orendorf A. (2017), "*Global Ecommerce Statistics [Infographic] and 10 International Growt Trends You Need to Know*". Retrieved from https://www.shopify.com/enterprise/global-ecommerce-statistics.

PayPal, Home Page. Retrieved from https://www.paypal.com/uk/webapps/mpp/home.

Satoshi Nakamoto Institute (2009), "*Bitcoin v0.1 released"*. Retrieved from http://satoshi.nakamotoinstitute.org/emails/cryptography/16/.

SecurionPay, "*What is an E-payment System?". Retrieved from* https://securionpay.com/blog/e-payment-system/.

The Bitcoin Volatility Index, Bitcoin Volatility Over Time. Retrieved from https://bitvol.info/.

The Onion Router. Accessed from https://www.torproject.org/.

The Panama Papers (2016) "*Giant Leak Of Offshore Financial Records Exposes Global Array of Crime and Corruption. Retrieved from* https://panamapapers.icij.org/20160403-panama-papers-global-overview.html.

The Motley Fool, Frankel, M. (2018), "*Bitcoin, Ethereum, and Ripple are just the beginning*". Retrived from https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx.

Other Sources

Council of Europe (COE) (1990), "*Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds of Crime*". ETS NO:141.

Council of Europe (COE) (2005), "*Council of Europe Convention on the Prevention of Terrorism*". ETS NO:196.

COUNCIL OF EUROPE, COMMITTEE OF MINISTERS. (1980), "*RECOMMENDATION No. R (80) 10 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON MEASURES AGAINST THE TRANSAFER AND THE SAFEKEEPING OF FUNDS OF CRIMINAL* ORIGIN". Retrieved from https://rm.coe.int/16804f6231.

DENMARKS NATIONALBANK (2014), "*BITCOIN ER IKKE PENGE".* Retrieved from http://www.nationalbanken.dk/da/presse/Documents/2014/03/PH_bitcoin.pdf#search=Bitcoin.

Department of the Treasury, Washington DC. (2015), "*National Terrorist Financing Risk Assessment*". Retrieved from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

Department of the Treasury Financial Crimes Enforcement Network, FinCEN (2013), "*Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*". FIN-2013-G001. Retrieved from https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

European Banking Authority (2014), "*EBA Opinion on 'virtual* currencies'". Retrieved from https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

European Banking Authority (2013), "*Warning to consumers on virtual* currencies".

European Central Bank (2012), "*Virtual Currency Schemes*". Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

European Central Bank (2015), "*Virtual Currency Schemes – A Further Analysis"*. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

European Commission (2016), "*Communication From the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against the financing of terrorism*". Retrieved from http://eur-lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5-01aa75ed71a1.0002.02/DOC_1&format=PDF.

European Parliament, Committee on Economic and Monetary Affairs (2016), "*Report on virtual currencies (2016/2007(INI))". Retrieved from*t http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0168+0+DOC+XML+V0//EN.

European Parliament, European Parliamentary Research Service (2015) "*Fundamental Rights in the European Union, The role of the Charter after the Lisbon* Treaty". ISBN 978-92-823-6749-0. Retrieved from http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf.

European Parliament, DIRECTORATE GENERAL FOR INTERNAL POLICIES, ECONOMIC AND SCIENTIFIC POLICY, Economic and Monetary Affairs. (2017), "*Offshore activities and money laundering: recent findings and challenges*".

European Parliament, Committee on the Internal Market and Consumer Protection (2016), "*OPINION on virtual currencies (2016/2007(INI))". Retrieved from* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-577.006%2b02%2bDOC%2bPDF%2bV0%2f%2fEN.

FBI, U.S. Attorney's Office (2013), "M*anhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*". Retrieved from https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website.

FBI, LEB, Nigh B. & Pelker A. (2015), "*Virtual Currency. Investigative Challenges and Opportunities".* Retrieved from https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities.

FATF (2012), "*INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION, the FATF Recommendations". P. 110. Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.*
Federal Financial Supervisory Authority (BaFin) (2014), "*Bitcoins: Supervisory assesment and risks to users*". Retrieved from https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html.

FATF on Money Laundering (1996), "*The Forty Recommendations*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201996.pdf.

FATF (2008), "*FATF Terrorist Financing Typologies Report*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

FATF (2001), "*FATF Standards, FATF IX Special Recommendations*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.

FATF (2008), "*Terrorist Financing*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf.

FATF (2014), "*FATF Report, Virtual Currencies Key Definition and Potential AML/CFT Risks*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FATF (2015), "*GUIDANCE FOR A RISK-BASED APPROACH, VIRTUAL CURRENCIES*". Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

LIBRARY OF CONGRESS, Global Legal Monitor, Hofverberg, E. (2013), "*Norway: Bitcoins Are Capital Property, Not Currency, Says Norwegian Tax Authority"*. Retrieved from http://www.loc.gov/law/foreign-news/article/norway-bitcoins-are-capital-property-not-currency-says-norwegian-tax-authority/.

Nechaev, V. (2014), "*Setting and Implementing Global Standards against Money Laundering and Terrorist Financing*". Speech at Institute of International and European Affairs, Dublin Ireland. Retrieved from http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-iiea-nechaev-feb2014.html.

Republique Française, Ministère des Finances et des Comptes Publics, Virtual Currencies Working Group (2014), "*Regulating Virtual Currencies. Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering".* Retrieved from https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf.

The United Nations (1998), "*The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*".

The United Nations (2004), "*United Nations Convention against Transnational Organized Crime*".

U.S. Department of Justice Drug Enforcement Administration, DEA Strategic Intelligence Section. (2015), "*National Drug Threat Assessment Summary"*.

United States Department of State Bureau for International Narcotics and Law Enforcement Affairs (2014), "*International Narcotics Control Strategy Report, Volume II, Money Laundering and Financial Crimes".*