ISCTE Business School
Instituto Universitário de Lisboa

THE IMPACT OF BLOCKCHAIN TECHNOLOGY ON ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING MANAGEMENT BY FINANCIAL INSTITUTIONS

Sofia Antunes da Silva Cabral

Dissertation submitted as partial requirement for the conferral of

Master in Management

Supervisor:

Prof. Luís Miguel da Silva Laureano, Assistant Professor, ISCTE Business School, Department of Finance

October 2019

ISCTE Business School
Instituto Universitário de Lisboa

THE IMPACT OF BLOCKCHAIN TECHNOLOGY ON AML/CFT MANAGEMENT BY FINANCIAL INSTITUTIONS

Sofia Antunes da Silva Cabral

“Blackbird singing in the dead of night

Take these broken wings and learn to fly

All your life (...)”

The Beatles, 1968.

Abstract

Money laundering and financing of terrorism are serious criminal offences that contribute to the parallel economy and harm the overall society wellbeing, as they generate further crime. The ever-evolving technological field makes it so that ML/FT schemes are becoming increasingly complex and dynamic, hindering the efforts conducted by regulators and authorities to suppress these events. Financial institutions, being an attractive vehicle for this type of criminal offences, also play an important role in fighting ML/FT. Hence, financial entities must ensure adequate controls and procedures to comply with the prevailing AML/CFT legislation.

Blockchain technology first arose in the context of cryptocurrencies. However, its inherent characteristics and flexibility make it suitable for numerous areas, including the financial services industry.

The goal of this dissertation is to assess the overall impact of the adoption of blockchain based solutions by financial institutions in compliance with AML/CFT legal requirements, particularly when the use case directly affects the AML/CFT process. Moreover, a comprehensive academic research was conducted to gain an in-depth understanding of both topics beforehand. Due to the lack of quantitative data available, literature review alongside with practical know-how were the basis used to reach the conclusions.

The results show that the impact of the adoption of blockchain based solutions by financial institutions on AML/CFT management is positive in the context of private or hybrid networks. Public blockchains, on the other hand, are not compliant with AML/CFT standards. Nonetheless, legislation on the matter is required and each use case must be addressed independently.

Keywords: Blockchain, Anti-Money Laundering and Counter-Terrorism Financing, Financial Institutions, Innovation

JEL Classification: G280, M150

Resumo

O branqueamento de capitais e financiamento do terrorismo são atos criminosos graves que contribuem para a economia paralela e prejudicam o bem-estar da sociedade. A evolução constante do ramo tecnológico, faz com que os crimes de BC/FT se tornem cada vez mais complexos e dinâmicos, dificultando os esforços conduzidos pelos reguladores e autoridades competentes. As instituições financeiras, veículos atrativos para este tipo de crimes, também desempenham um papel fundamental no combate ao BC/FT. Assim, estas devem dispor de controlos adequados, de forma a assegurar o cumprimento com os requisitos legais.

A tecnologia blockchain surgiu no contexto das criptomoedas. No entanto, as propriedades e flexibilidade de que dispõe, permitem que esta seja utilizada nas mais diversas áreas, incluindo na indústria dos serviços financeiros.

O objetivo desta dissertação passa por avaliar o impacto da adoção de soluções tecnológicas baseadas na blockchain por parte das instituições financeiras no cumprimento dos requisitos legais em termos de PBC/FT, especialmente em cenários que afetem diretamente o referido processo. Devido à escassez de dados quantitativos relevantes, as conclusões foram geradas com base em revisão literária sobre ambos os tópicos, juntamente com conhecimentos práticos.

Os resultados mostram que o impacto da adoção de soluções tecnológicas baseadas na blockchain por parte das instituições financeiras na gestão do PBC/FT é positivo no contexto de redes privadas ou híbridas. Por outro lado, as redes públicas não cumprem com os requisitos legais de PBC/FT. Não obstante, é necessária a produção de legislação específica e cada caso particular deverá ser analisado individualmente.

Palavras-chave: Blockchain, Prevenção do Branqueamento de Capitais e Financiamento do Terrorismo, Instituições Financeiras, Inovação

Classificação JEL: G280, M150

Acknowledgments

Some might consider the thesis itself as a journey, instead, I see it as a closure of the cycle that is academic life. Hence, I must thank everyone who stood by my side throughout this journey – those who have always been there, those who I met along the way and those with whom I will cross the finish line.

Family first. I would like to star off by thanking my grandparents for the unconditional support, for asking me 4862 times "*are you done yet?*" and for worrying about my eating and sleeping habits. To my father, for reading my thesis, for providing useful and unbiased feedback and for being excited about my topic choice since day one. Finally, to my mother, for the unhealthy amounts of coffee and candy provided in these last weeks, for the home cooked meals, for reading about a third of my thesis, for ensuring that I always benefited from high education standards, for everything.

They say that friends are the family you choose. Although I might not always make the wisest choices, I am proud to say that these ones I got right. To my best friend Mariana, for the kindness and for always making me laugh. To my friend Henrique, who never failed to provide words of encouragement despite being quite a few kilometers away. To my dear friend Guilherme who kindly took the time to read my thesis, not because I am his child, but because he was interested in the content. To Jana, Miranda and Vera, who I met in my freshman year and I will keep for life, for bearing with all the "*I'm sorry I can't make it.*" texts. To Marta, Jorge and Pedro for sharing this experience with me, I am sure your dissertations are outstanding.

I must thank the Compliance department of *Financeira El Corte Inglés* for the flawless reception and integration, for bearing with my typical Monday zombie looks and for listening to all the nonsense that regularly comes out of my mouth. Thank you to my work family, Claudia and Rita, for the friendship, for laughing it out with me and for always having my back. To Catarina, for introducing me to AML/CFT and for sharing SAS and Excel tricks with me (*#teamPBC*). To my eternal boss, Bruno, for the knowledge, for leading by example, for always pushing me forward without ever letting me fall.

Thank you to my supervisor, Prof. Luís Miguel da Silva Laureano, for guiding me in the right direction and for understanding my busy schedule.

Finally, I have to thank Guilherme for understanding my absence in these last months, for the kindness and for always wanting to see me thrive.

Glossary

AML/CFT - Anti-Money Laundering/Combating the Financing of Terrorism

BC/FT –Branqueamento de Capitais e Financiamento do Terrorismo

CDD – Customer Due Diligence

CMVM – Comissão do Mercado de Valores Mobiliários

CPU – Central Processing Unit

DCIAP – Departamento Central de Investigação e Ação Penal

DLT – Distributed Ledger Technology

EBA – European Banking Authority

EU – European Union

FATF – Financial Action Task Force

KYC – Know Your Costumer

ML/FT - Money Laundering/Financing of Terrorism

PBC/FT – Prevenção do Branqueamento de Capitais e Financiamento do Terrorismo

PEP – Politically Exposed Person

RCBE – Registo Central do Beneficiário Efetivo

UIF – Unidade de Informação Financeira

Table of Contents

List of Figures

1. Introduction

1.1. Topic

The theme I chose to address on this thesis is related to my current job position as an AML/CFT analyst. I find this topic extremely interesting and complex enough to serve as a basis for academic research. However, exclusively addressing AML/CFT management would be too broad and there is already a solid amount of information on the topic. Whereas innovation and technology are two of my favorite topics, I started looking into future trends that might have implications on the matter. Given the increasing popularity of blockchain technology and its various applications, I thought it would be useful to understand the implications of such technology on ML/FT prevention efforts by financial institutions. Moreover, the goal of this dissertation is to weight the pros and cons of the adoption of blockchain by financial institutions in terms of AML/CFT and conclude weather the overall impact is positive or negative.

Money laundering is not a recent issue, in fact it has been around for over 2 000 years. Chinese merchants were the pioneers of this criminal offense, by trying to cover up funds from government officials (O'Connell, 2019). To do so, they would engage in a series of complex transactions to hinder traceability of their income sources. However, it was in 20th century that the authorities began paying closer attention to money launderers, in an attempt to fight ever-increasing organized crime. When it comes to the financing of terrorism, awareness towards this crime rose after the terrorist attack that took place on September 11 of 2001. Countries started realizing the need to implement tight controls and corresponding legislation on the matter. Besides, nations became aware of the dimension of money laundering and financing of terrorism, concluding that international efforts and joint forces were needed to fight these issues globally. The European Union, for instance, has released five anti-money laundering and counter terrorist financing directives so far (European Commission, 2018). Financial institutions, being an attractive vehicle for this type of criminal offences, have been increasing their efforts to remain compliant with legislation and prevent ML/TF as much as possible. As it will be further discussed on the thesis, ML/FT can seriously jeopardize the functioning of financial entities associated with such crimes, imposing reputational, operational, legal and concentration risks. Despite the efforts of both

regulators and financial institutions themselves, ML/FT crimes are becoming increasingly complex and dynamic, mostly due to the constant evolutions within the technological field. Besides, criminals tend to act in tentacular networks, which are extremely difficult to unveil. Thus, regulators and organizations must be on top of the latest technology breakthroughs so that they can anticipate which features might be leveraged by individuals with mischievous intentions.

Blockchain is commonly known for being the technology behind Bitcoin. Although Bitcoin was indeed the first practical application of blockchain technology, its properties make it flexible enough to be used in different fields – ranging from healthcare to government services. Furthermore, the financial services industry is among the strong candidates for the development of solutions based on the distributed ledger technology. Within the financial services industry, there are various possible blockchain applications. Thus, it is necessary to understand the impact that those applications will have on AML/CFT management by financial institutions, particularly on the use case in which the traditional AML/CFT process will be affected.

1.2. Research Problem

The purpose of this thesis is to understand how the impact of the implementation of blockchain technology by financial institutions will impact AML/CFT management. Furthermore, the main objective is to study the ways in which financial entities will leverage blockchain practicalities in their core activity and services provided alongside with the resulting impact on AML/CFT efforts. For this purpose, current legislation regarding AML/FT will be examined, more specifically in the Portuguese context, to assess the main duties and obligations that all financial institutions must fulfill to be compliant with the applicable legal parameters. Then, it is necessary to understand if the new practices allowed by the technology at hand fall into the previously referred legal standards, or if new challenges will arise. Moreover, the aim of this thesis is to understand pros and cons of blockchain based strategies in terms of compliance with AML/CFT requirements.

To channel the academic research towards the issue above mentioned, a research question was elaborated. Thus, the content presented on this thesis will be focused on providing an answer for the following research question:

RQ1: *"What will be the overall impact of blockchain technology adoption by financial institutions on AML/CFT management?"*

1.3. Methodology

The adoption of blockchain technology is still in the early stages, hence, it was not possible to find significant data on the topic of this dissertation. Moreover, the research conducted was mostly based on scientific articles, academic papers, books, electronic journals, newspapers and official reports and statements, particularly from audit and consulting firms. The last source of information provided relevant insights on how the industry actors are tackling the various adoption possibilities supported by the distributed ledger technology and what are the predominant future trends, upcoming challenges and concerns on the subject. In addition, pieces of legislation and regulation were also a crucial source of information, not only when addressing AML/CFT, but also when tackling other critical subjects, namely data privacy and security.

The literature review conducted on the second chapter of the dissertation provided the necessary knowledge base to build a realistic scenario of how the structure of financial entities would look like after having implemented blockchain based solutions. Subsequently, the overall impact of such solutions on AML/CFT management was addressed on the third chapter. To do so, current legislation on the matter alongside with AML/CFT best practices by financial institutions were used as a basis. The latter stemmed not only from the research process conducted, but also from the practical knowledge acquired through my current job position as an AML/CFT analyst.

At last, the main conclusions deriving from the bundling of chapters two and three were drawn on the forth chapter of the dissertation.

2. Literature Review

The dissertation addresses two equally complex and yet very distinct topics. Hence, the literature review will be divided in two sub chapters, one for each theme. The first sub chapter focuses on AML/CFT, with a particular emphasis on the prevailing legislation on the subject. Since money laundering and financing of terrorism are criminal offences, a detailed analysis of legislation is vital to understand not only the actions that financial institutions must undertake in order to be compliant with the law, but also the consequences they might face if they fail to comply. Since there will be several references regarding Portuguese legislation, it is important to clarify that all the translations present on the thesis were conducted by the author.

The second sub chapter regards blockchain technology. First, the general properties of the technology are explained, followed by the specificities that make the distributed ledger such a versatile a useful tool. Then, the different types of blockchains are presented, so that the benefits and drawbacks of each one are clearly understood and can later be compared. The section ends with an outline of the main blockchain applications, particularly in the financial sector.

2.1. Money Laundering and Financing of Terrorism

Money laundering consists of introducing illicitly obtained cash funds in the legal economy so that earnings appear to come from a legitimate source (Schott, 2005: I-1). According to the Financial Action Task Force, FATF, the *dirty* money comes from criminal activities such as drug and human trafficking, the sale of illegal weapons, fraud, corruption, extortion, bribery or gambling. Moreover, money laundering can be considered a secondary crime, as it presupposes the existence of a prior crime. (FATF, n.d.)

FATF states that the process of laundering money can be divided in three phases – placement, layering and integration. The first involves inserting the illicit cash funds in the financial system, which is usually done through banks and other financial institutions. Funds are then converted in monetary or financial instruments, including currency, debit and credit

cards, bank checks, securities, bonds and stocks. The layering stage has the intent of hindering traceability of the source of funds. For this purpose, launderers perform a series of movements, such as buying and selling financial products or conducting several bank transfers to different accounts. The last stage regards the integration of the illicit money in the economy. Common methods of integration include buying and selling assets, conducting investments and making false loans to associates or their own firms. (FATF, n.d.)

Money laundering practices can be quite complex and difficult to detect, especially as we move further in the stages of the *cleansing* process (Demetis, 2017). It is, therefore, crucial that companies, particularly in the financial industry, develop adequate strategies to unveil money laundering attempts as early as possible.

Financing of terrorism, on the other hand, consists on raising funds from licit or illicit activities to finance terrorism related practices. Unlike money laundering, the funds used often come from legitimate sources and the amounts transferred tend to be small, making it increasingly difficult to detect and prevent the financing of terrorism. Furthermore, the main difference between the two concepts is that money laundering involves concealing the real origin of the funds, while terrorism financing is about covering up the intended usage of the funds. (*Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo*, n.d.)

Money laundering and financing of terrorism are not only crimes *per se*, as they generate further crime and corruption, contributing to the deterioration of economic development and the solidity of the financial system.

2.1.1. Regulators and Supervisory Authorities

2.1.1.1. International Level

At an international level, the FATF is the inter-governmental body whose objective is to implement a comprehensive strategy to fight money laundering and the financing of terrorism. The activity carried out by this body involves the analysis of ML/FT techniques and trends, understanding of the actions already undertaken at national or international

levels, monitoring compliance with prevailing measures and defining new ones whenever necessary. In 1990, the FATF published forty recommendations that serve as an action plan to prevent ML/FT as well as the proliferation of weapons of mass destruction. The referred set of recommendations was subsequently revised in 1996, 2001, 2003 and 2012. The prevailing version is regularly revised in order to be as up to date as possible, thus, the last update was conducted in June 2019. (FATF, 2012-2019)

2.1.1.2. European Level

With the intent of bringing European legislation closer to the international standards and recommendations issued by the FATF, the European Union established Directive 2015/849/EU of the European Parliament and of the Council on the 20 of May of 2015 on the prevention of the use of the financial system for ML/FT purposes. In addition, the European Banking Authority, EBA, supervises the European banking sector. The work developed by EBA focuses on the standardization of prudential rules throughout European financial institutions, aiming for a harmonization of practices. (EBA, n.d.)

2.1.1.3. National Level

In Portugal, the prevailing piece of law in terms of AML/CFT is *Lei n.º 83/2017*, of August 18, which stems from the partial transposition of two EU directives - Directive 2015/849/EU of the European Parliament and of the Council of 20 of May of 2015 and Directive 2016/2258/EU of the Council of 6 of December of 2016. *Artigo 81.º*, *Lei n.º 83/2017*, of August 18, defines *Departamento Central de Investigação e Ação Penal*, part of *Procuradoria-Geral da República*, of the *Ministério Público*, *DCIAP*, as the authority responsible for the development of measures to prevent ML/FT. Furthermore, in accordance with *Artigo 82.º*, *UIF* (*Unidade de Informação Financeira*, part of *Polícia Judiciária*) has the competence to receive, analyze and disseminate information resulting from the communication of operations and activities suspicious of being related with ML/FT crimes,

as well as information stemming from other sources when associated with criminal activities from which funds or other property arise. At last, *Artigo 84.º* lists the supervisory authorities responsible for ensuring that financial institutions are complying with the duties and obligations stated on *Lei n.º 83/2017*, of August 18. The referred authorities include *Autoridade de Supervisão de Seguros e Fundos de Pensões* (*Artigo 84.º, a)*), the Bank of Portugal, *Comissão do Mercado de Valores Mobiliários, CMVM*, (*Artigo 84.º, b)*) and *Inspeção Geral das Finanças* (*Artigo 84.º, c)*).

2.1.2. Sanctions Framework

The violation of AML/CFT duties defined by law results in criminal liability. As previously referred on this thesis, there are several types of crimes that may be ML/FT related, with penalties varying depending on the crime involved. *Lei n.º 83/2017*, of August 18, states three situations of non-compliance with the AML/CFT rules that cause criminal liability - illegitimate disclosure of information to third parties, violating the duty of non-disclosure (*Artigo 157.º*), revelation of the identity of the individual responsible for providing relevant pieces of information for the investigation (*Artigo 158.º*), disobedience to orders or warrants defined by the sectorial authorities (*Artigo 159.º*).

Lack of compliance with the prevailing law is severe, as both violations of the law and negligent behaviors are considered offenses punishable as misconducts. Moreover, the financial institution may have to pay a fine and/or be subject to an ancillary sanction. Depending on the severity of the misconduct, the entity may be accused of committing a financial crime and will be condemned to follow through with the resulting penalties.

The financial institution is responsible for the payment of any fines and costs concerning the conviction of directors, agents, representatives or other employees (*Artigo 162.º*, *Lei n.º 83/2017*, of August 18). However, individual agents are not excluded from being held accountable for their actions, in addition to the disciplinary procedures in which they may incur. If, when given the opportunity, the members of the administration board do not oppose to the practice of an infraction, they are liable for the payment of the

corresponding fine and court fees. The members of the administration board are subject to the penalty imposed on the author of the misconduct. The sanction can be attenuated when, cumulatively, the members of the administration board are not directly responsible for the area where the infraction was committed and their responsibility is based solely on the fact that, having the obligation of knowing the practice of the infraction, they have not immediately taken the appropriate measures to put an end to it. (*Artigo 163.º, Lei n.º 83/2017*, of August 18)

In addition to the fines predicted in *Artigo 170.º* and *Artigo 171.º, Lei n.º 83/2017*, of August 18, depending on the severity of the conduct practiced, the following ancillary penalties might be applied:

a) *"Loss, in favor of the State, of the object of the infraction and of the economic benefit obtained*
b) *Closing, for up to two years, of the establishment where the activity took place*
c) *Interdiction up to three years, from the exercise of the profession or activity*
d) *Inhibition of up to three years, from the exercise of social positions or functions of administration, direction, leadership, supervision, representation, and mandate in financial entities and non-financial entities, and may be included in the prohibition entities that are in a domain or group*
e) *Publication of the final decision or the one transit in rem judicatam"*

Ancillary sanctions can be as harmful or even more so to entities when compared to financial penalties.

2.1.3. Preventive Duties

According to *Artigo 11.º* of *Lei n.º 83/2017*, of August 18, obliged entities, listed in *Artigo 3.º* and *Artigo 4.º*, in which financial institutions are included, are subject, in their performance, to the fulfillment of the following preventive duties:

a) Duty of control;

b) Duty of identification and diligence;

c) Duty of communication;

d) Duty of abstention;

e) Duty of refusal;

f) Duty of conservation;

g) Duty of examination;

h) Duty of collaboration;

i) Duty of non-disclosure;

j) Duty of training.

2.1.3.1. Duty of Control

Lei n.º 83/2017, of August 18, introduced a series of obligations deriving from the duty of control, imposing the requirement to define and ensure internal policies and procedures adequate to the fulfillment of all the duties above mentioned and to guarantee the prevention and combat of ML/FT, through internal control, risk assessment, risk management and internal audits.

The execution of the control duty by the financial entities is overseen by the Bank of Portugal and it is based on three pillars - internal control system (*Artigo 12.º*), compliance function (*Artigo 16.º*) and effectiveness tests (*Artigo 17.º*). Each of these will be further explained on the next section.

The predominant reason for implementing an internal control system is to ensure compliance with the prevailing legislation on AML/CFT and ultimately avoid being involved in crimes of such nature. The extent of the policies and procedures governing the internal control system shall be adequate and proportional to the size, nature and complexity of the organizational structure and activity conducted, as well as to the nature and magnitude of the risks it faces and the degree of centralization of authority established. The policies and

procedures must be composed in a written form and the corresponding physical documents kept for a period of seven years.

Artigo 3.º, *Aviso n.º 2/2018*, of November 25, of the Bank of Portugal, stipulates that the designated management body must have the suitability, professional qualification and performance guarantee of its assigned duties independently and with the necessary decision-making autonomy. Top management must have unrestricted and timely access to all relevant internal information and cannot be subject to potential functional conflicts. However, if the nature, size and complexity of the activity pursued by the financial institution allows, the assignment of non-conflicting roles is not required. Nevertheless, additional controls shall be established to mitigate the potential conflicts and increased emerging risks. According to *Artigo* 7.º, *Aviso n.º 2/2018*, of November 25, of the Bank of Portugal, it is considered that the compliance function shall be segregated from others whenever the number of employees, excluding administrators, is equal to or greater than six and the operating income in the last financial year is equal to or greater than 1.000.000€.

Financial institutions are required to maintain an independent, permanent and effective compliance function, to monitor the fulfillment of AML/CFT legal requirements. The responsible for the compliance department shall be involved in the definition and monitoring of the internal control system as well as in the assessment of the adequacy and efficacy of the inherent policies and procedures. The goal is to ensure that information is shared across all business areas of the financial institution and that the communications to the competent authorities are done properly. The compliance function ensures that information on the internal control system and on the respective standards and instrumental procedures is made available to relevant employees of the organization. Besides issuing opinions on internal policies and procedures aimed at preventing ML/FT and preparing que corresponding effectiveness tests, the internal training policy on the subject is also defined, monitored and evaluated by this department. Furthermore, the compliance unit plays the interlocutor role of judicial, police and supervisory authorities, whilst also coordinating the preparation of periodic reports to the Bank of Portugal regarding AML/CFT.

Periodically, financial institutions are obliged to carry out effectiveness tests to the AML/CFT internal control system. The effectiveness tests take place once a year or every

two years, in the case of business areas or financial institutions less exposed to ML/FT risks. The tests are performed by the internal audit function, external auditors or a third-party entity qualified to do so. *Artigo 8.º* of *Aviso n.º 2/2018*, of November 25, of the Bank of Portugal, lists the components that shall be evaluated on the effectiveness tests.

Reports produced as a result of the effectiveness tests and monitoring procedures, alongside with all supporting documentation, shall be kept on paper or another durable format for at least seven years. All the documentation shall be kept in a place that allows immediate access, so that those responsible for the compliance or internal audit functions, external auditors, judicial, police and supervisory authorities are able to access them promptly.

Artigo 8.º also states that financial institutions in which the existence of the internal audit function is not feasible due to the nature, size and complexity of the activity carried out, which have a number of employees, excluding top management, inferior to thirty and where the operating income in the last financial year is below 20.000€, have to adopt additional monitoring procedures proportional to the dimensions of the organization, designed to assess the effectiveness of their internal system.

Lei n.º 83/2017, of August 18, requires special attention when it comes to operations likely to promote anonymity, but also operations deriving from newly introduced products, commercial practices or technologies (*Artigo 15.º*). Furthermore, a risk analysis must be carried out before the launch of new products, practices or technologies, by analyzing the specific ML/FT risks associated with them. Entities shall also anticipate and adopt specific procedures to mitigate the risks associated with the innovation at hand. Again, the documentation supporting the risk analysis must be kept for a period of seven years and available for sectorial authorities whenever requested.

2.1.3.2. Duty of identification and diligence

Identification

Financial entities are required to verify the identity of their customers and the corresponding beneficial owners, if they have any. The process of identity verification is commonly referred to as Know Your Customer, KYC. In addition, institutions often perform customer due diligence proceedings, CDD, which go beyond identity verification. CDD involves obtaining additional information either by analyzing supplementary documents provided by the client or by looking for supplementary data in external sources, such as the Internet. Depending on the situation, standard measures, simplified measures or enhanced measures may be applied.

As mentioned on *Artigo 23.º, Lei n.º 83/2017,* of August 18, identification proceedings must be carried out whenever a business relationship is established, occasional transactions involving an amount equal to or greater than 15.000€ are made, regardless of whether the transaction is carried out through a single or several operations. Additionally, the referred diligences also apply in cases in which a transfer of funds greater than 1.000€ takes place. Nonetheless, if a particular operation appears to be related with ML/FT, the client will be asked to provide a proof of identity, independently of the amount at stake. An operation or set of operations may be regarded as suspicious due to its nature, frequency, complexity, place of origin or destination of the funds, inconsistency with the profile and history of the client's activity, amount at stake or the chosen payment method.

Aviso n.º 2/2018, of November 25, of the Bank of Portugal requires financial entities to keep a centralized and computerized record containing at least the full name, number and type of identity document, the date and value of the transaction as well as of all the occasional transactions regardless of the amounts, to identify the fractionation of operations. Data must be updated whenever a new occasional transaction is made. In order to ensure an efficient flow of information, the record must be available to the entire organization, as well as its agents, distributors and third parties responsible for carrying out operational functions related with payment services and the issue of electronic money.

In cases where the client acts on behalf of a third party, the beneficial owner must be identified so that appropriate due diligence measures are taken, according to the corresponding ML/FT risk held by that stakeholder. The identity documents of the beneficial owner must also be requested if the client is a legal person or collective interest center without legal personality or whenever it is suspected that the client does not act on his own account.

The assessment of the quality of beneficial owner can be carried out through any document, measure or diligence deemed appropriate and sufficient depending on the level of risk of the client.

The *Registo Central do Beneficiário Efetivo, RCBE*, consists on a database where the identification elements of the beneficial owners of all national and international entities operating in Portugal are kept (*Registo Central do Beneficiário Efetivo*, n.d.). Financial institutions, besides being obliged entities themselves, they might have clients which are also under the obligation to register the corresponding beneficial owners on the referred platform. Thus, *Artigo 34.º, Lei n.º 83/2017,* of August 18, predicts that the financial institution must consult the information featured on the *RCBE* and conduct periodic consultations according to the client's ML/FT risk. On the occasion that the institution detects that the obligation to register in the RCBE is not fulfilled, the *Instituto dos Registos e do Notariado* must be immediately notified of any discrepancies or omissions between the *RCBE* and the information provided by the client. In this circumstance, the financial entity would refuse to establish or maintain the business relationship or occasional transaction. In case the client is not obliged to register its effective beneficiaries in Portugal, the financial institution must check the information present in an equivalent mechanism established in another jurisdiction. Alternatively, if access to these records is not possible or cannot be made in a timely manner, the entity shall obtain such information from the client.

In order to verify the identity of the beneficial owner, the entity might conduct simplified measures (*Artigo 35.º*, *Lei n.º 83/2017*, of August 18). The standard measures presuppose proof of the identifying elements of the beneficial owners based on documents, data or information from independent and credible sources. In this case, a copy of the identity document may be collected on physical or digital media. If the ML/FT risk is considered low, sectorial regulation may allow the identification of the beneficial owner identification

elements based on a statement issued by the client or by the corresponding legal representative. Financial entities shall conduct the validation of the beneficial owner's identifying elements in the same manner as they would for the actual client. According to *Aviso n.º 2/2018*, of November 25, of the Bank of Portugal, alternative validation means or procedures that offer identical security levels, are also legitimate, if performed by individuals with the adequate competences and qualifications (*Artigo 22.º*). One example would be identification via videoconference as it allows the verification of several identifying elements including photograph, full name, signature, date of birth, nationality, type, number, expiration date and issuer of the identification document, taxpayer identification number or equivalent issued by a competent foreign authority. In addition, other elements, such as occupation and employer, permanent and tax address, and other nationalities not included in the identification document. All proceedings undertaken to identify the beneficial owners must be preserved for a period of seven years and kept available for the sectorial authorities.

Regarding business relationships, financial entities may complete proof of identity after the relationship is established if and only if the ML/FT risk is low and there is no legal or regulatory rule that prevents it (*Artigo 35.º*, *Lei n.º 83/2017*, of August 18). Nonetheless, the described scenario shall only occur in exceptional circumstances and it demands appropriate measures to manage the risk inherent to the situation - by limiting the number, type or amount of operations that can be carried out in these terms. Regardless, the identity verification process must be completed as soon as possible. Whenever changes in AML/CFT legislation or regulations take place, financial institutions must ensure that the identification and due diligence procedures are adequate, sufficient and up to date considering the new legal requirements. In case any deficiencies are identified, they have to be promptly tackled.

Diligence

Financial institutions must perform due diligence processes both for new and existing clients, on a regular basis. The corresponding level of risk will determine the extent of the monitoring of the business relationship, the frequency of the updates of the identity elements obtained, the collection of information considered relevant and the implementation of measures deemed appropriate to comply with the prevailing legislation.

Due diligence procedures include gathering information about the purpose and intended nature of the business relationship as well as the origin and destination of the funds at hand. When the client's risk profile or the characteristics of the operation justify it, financial entities maintain a continuous monitoring of the ongoing client activity, ensuring that the transactions carried out in the course of the business relationship are consistent with their usual activity and risk profile.

Simplified identification and due diligence measures

Whenever a business relationship, occasional transaction or operation appears to hold a lower risk in terms of ML/FT, financial institutions are allowed to apply simplified identification due diligence measures.

Artigo 35.º, Lei n.º 83/2017, of August 18, mentions a few examples of simplified measures that organizations might apply to clients that present a potentially lower ML/FT risk. As previously mentioned, when addressing the duty of identification, the identity of the client and, if applicable, of the respective beneficial owner, can be confirmed *a posteriori* of the establishment of the business relationship. In addition, identification elements and other documents that might seem reasonable to collect in diligence procedures, do not have to be updated as often as if the client held a higher risk of ML/FT. Naturally, lower risk profiles do not require continuous monitoring, nor an in-depth analysis of the operations conducted, if these do not involve substantial amounts of money. However, monitoring can only be simplified up to an extent since regular checks of client activity are still necessary to account for the detection of suspicious behaviors.

Enhanced identification and due diligence measures

Enhanced identification and due diligence measures shall be implemented if a potentially higher ML/FT risk is identified in the business relationships, occasional transactions or operations carried out, by the financial entities themselves or by the sectorial authorities. *Artigo 36.º, Lei n.º 83/2017*, August 18, lists a few examples of common due diligence measures. To better understand the likelihood of a certain business relationship,

transaction or operations being ML/FT related, financial institutions usually demand additional information or documentations when fulfilling the duty of identification of the client and the corresponding beneficial owner, if there is one. Plus, additional controls shall be performed in order to check the veracity and authenticity of the data and documentation provided by the client. Although entities are required to monitor all customer activity, those subject to enhanced due diligence measures require a continuous monitoring and more frequent updates of the identification elements as well as additional documentation that might have been requested in the course of the due diligence process. The payment methods used by clients that present a higher ML/FT risk, preferably shall allow for traceability of the origin of the funds, even if the financial institution has to impose this requirement.

Despite the controls above mentioned, all business relationships, occasional transactions and single operations are subject to the approval of top management.

High-Risk Third Countries

According to the Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 and the Commission Delegated Regulation (EU) 2018/105 of 27 October 2017, high-risk third countries are those that do not possess adequate and sufficient AML/CFT strategies, making them more vulnerable to this type of crimes. Therefore, when managing relationships with jurisdictions belonging to the group above mentioned, financial entities shall adopt an enhanced diligence measure that is effective and proportional to the identified risk. The law does not specify a specific procedure to deal with this matter, leaving entities free to choose an appropriate strategy. Regardless, financial institutions must ensure enhanced identification and due diligence measures whenever a new relationship, occasional transaction or operation is established with a client from a high-risk third country. The countries that fall upon this category are identified by the FATF, sectorial authorities or other credible sources of information.

Distance Hiring

Technology allows for business relationships or occasional transactions to take place without the client or its representative being physically present. Thus, the identification duty shall be assured preferably through the usage of electronic means that allow for the identification and validation of the identifying elements. Nonetheless, financial institutions are required to perform additional steps to confirm the validity of the information obtained in the identification process and, if needed, request additional information or documentation to corroborate the data provided by the client. (*Artigo 38.º, Lei n.º 83/2017*, of August 18)

Politically Exposed Person

Artigo 39.º, Lei n.º 83/2017, of August 18, disposes that financial institutions shall regularly check sources of information that allow for the detection of the quality of Politically Exposed Person (PEP), both before and throughout the course of the contractual relationship. When this quality is detected, the intervention of an element of top management is required both for the approval of the business relationship and its maintenance or the execution of occasional transactions. Whether the quality of PEP is detected before or in the course of the business relationship, additional measures shall be implemented to gain knowledge and verify the origin of the client's assets and funds. Moreover, business relationships with PEPs have to be constantly monitored, even after the individual has left the position that classified him as PEP for an additional period of twelve months or longer if the client exhibits suspicious behaviors that require enhanced due diligence.

The procedures mentioned in the previous paragraph are not exclusively applied to PEPs, as their applicability is extensible to their close relatives or individuals close to them as well holders of other political or public positions. Thus, identification and due diligence measures are also applied to clients, representatives or beneficial owners that possess these qualities.

Life Insurance Contracts

Artigo 69.º, *Lei n.º 83/2017*, of August 18, requires obliged entities to pay special attention to beneficiaries of life insurance contracts and the eventual beneficial owners. A life insurance beneficiary constitutes a source of an increased ML/FT risk in the case of a legal person or collective bargaining center without legal personality. Therefore, enhanced due diligence measures must be applied, including the adoption of measures to verify the identity of the beneficial owner of the insurance as well as the quality of PEP, up to the moment of payment of the benefit or of the assigned value, whether the payment is total or partial. In case the beneficiary is a PEP or another source of increased ML/FT risk is identified, top management must be informed before the capital payments agreed upon the contract takes place. Plus, the business relationship shall be monitored attentively.

Correspondent Relationships

The concept of correspondent relationships is defined by *Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo* (n.d.) as *"The provision of services by a bank, financial entity or other similar service provider (the correspondent), a bank, financial entity or other equivalent entity that is a customer of the financial institution (the respondent), including the provision of a checking account or other account that generates an obligation and related services, such as cash management, transfer processing of funds and other respondent payment services, check clearing, payable-through accounts, foreign exchange and securities transactions."*

The enhanced due diligence measures that financial entities are forced to apply, differ depending on whether the entity acts as correspondent or respondent, *Lei n.º 83/2017*, of August 18, addresses these measures on *Artigo 70.º* and *Artigo 71.º*, respectively. Aviso n.º 2/2018, of November 25, of the Bank of Portugal also describes these measures on *Artigo 32.º* and *Artigo 33.º*, respectively.

Identification and due diligence procedures may be performed through credit intermediaries, promoters and other intermediation relationships or through outsourcing.

2.1.3.3. Duty of Communication

Depending on the results of the examination duty, financial institutions might suspect that an ML/FT related operation has taken place, is under way or has been attempted. If so, according to *Artigo 43.º, Lei n.º 83/2017*, of August 18, the compliance function has to report the operation to *DCIAP* and *UIF*. The communication of the suspicious incident shall be made as soon as it is detected and it must include a description of the factors that contributed to the transaction being considered ML/FT related, all the evidences portraying the operation at hand as well proof of the analysis conducted. Additionally, the entity must include the data obtained as part of the identification proceedings, alongside with all the information regarding the activity of the parties involved in the suspicious incident. Under no circumstances can top management interfere with the decision made by the compliance unit.

Financial institutions must adopt the necessary procedures in their organizational structure to comply with the duty of communication, namely by ensuring the confidentiality of the identity of employees who internally detect and report suspicious transactions. To facilitate the analysis and reporting of suspicious incidents, a simplified and agile flow of the information is recommended, composed by the minimum possible number of actors. (*Artigo 44.º, 2.*)

2.1.3.4. Duty of Abstention

On the previous section, it was mentioned that any activity apparently related with ML/FT crimes must be reported to the competent authorities. However, financial institutions also have the obligation to abstain from performing operations that seem suspicious. (*Artigo 47.º, Lei n.º 83/2017*, of August 18).

The duty of abstention implies the fulfillment of other duties, namely the duty of communication. Moreover, every time an entity refuses to follow through with a certain operation, *DCIAP* and *UIF* must be immediately informed.

Nevertheless, there are some exceptional circumstances under which the operation might be completed (*Artigo 47.º, 5.*). If, for some reason, the organization is incapable of putting

an end to the operation, or *DCIAP* or *UIF* consider that stopping the transaction could actually harm the ongoing investigation, the financial institution can proceed with the operation and deliver the corresponding information to the referred bodies. Also, in case *DCIAP* fails to notify the entity within six working days of the date of the communication, the operation can be performed.

2.1.3.5. Duty of Refusal

Financial institutions might not be able to obtain certain client data required to follow through with the establishment of a business relationship, occasional transaction or single operation. Thus, as stated on the first point of *Artigo 50.º, Lei n.º 83/2017*, of August 18, the entity is obliged to refuse the execution of either of the referred activities, if it is unable to gather identification elements from both the client and the beneficial owner, if applicable, or information that justifies the nature and purpose of the business relationship as well as the origin and destination of the funds. Overall, the consequences for a client who does not provide the required documents or information, range from not starting or terminating the business relationship, refusing to perform the occasional transaction or conduct a specific operation or set of operations. As soon as the organization decides to terminate the business relationship, all movements of funds or other assets associated with the business relationship shall be put on hold. The repayment of these funds may be conducted via bank transfer to an account of the financial entity held by the client, or another legally authorized, as long as it is subject to procedures of identification and diligence foreseen in the law and is not located in a high-risk third country. In any case, the motive of the transfer shall be clearly stated. Alternatively, the funds may also be returned in cash if the client does not have any account legally entitled to receive the transfer of the amount at stake. (*Artigo 39.º, Aviso n.º 2/2018*, of November 25, of the Bank of Portugal)

Additionally, financial entities shall analyze the possible reasons for not providing the required elements and, if justifiable, communicate the suspicious behavior to the competent authorities. (*Artigo 50.º , 3., c*)

2.1.3.6. Duty of Conservation

According to *Artigo 51.º, Lei n.º 83/2017*, August 18, every document, whether it is an original or a copy, every piece of information or data collected from the client for identification and due diligence purposes, every element or analysis regarding operations, every account file, must be kept in a durable support, preferably by means of an electronic support, for a period of seven years after the execution of the operations or the end of the business relationship. The goal is to be able to reconstruct a particular operation at any given time, if requested by *UIF*, the judicial or sectorial authorities, police or the national tax and customs authority, namely *Autoridade Tributária e Aduaneira*. Therefore, it is of outmost importance that the records are kept in good condition and in a known location.

2.1.3.7. Duty of Examination

Artigo 52.º, Lei n.º 23/2017, of August 18, refers that conducts, activities or operations which, due to its inherent characteristics, pose a higher risk of being ML/FT related, have to be carefully studied and analyzed by a qualified and diligent professional. Because oftentimes there is no actual evidence nor documentation supporting the hypothesis of a certain behavior being indeed ML/FT related, it is extremely important to ensure that analysts receive the adequate training and exhibit diligent traits, as it will be further explained when addressing the duty of training.

The outcome of the examination process could be one of two – the entity either decides to communicate the suspicious conduct, activity or operation to the competent authorities, or the entity concludes that the occurrence does not hold the grounds to be considered suspicious and opts for not communicating the incident. If the chosen pathway is the latter, all documents and registries containing the basis behind the conclusion that the event does not present concrete risk of being linked with ML/FT practices, must be kept for a period of seven years. In case there was any informal contact with UIF or the judicial and police authorities, all records available, dates during which the communications took place as well as the used means shall be kept registered.

2.1.3.8. Duty of Collaboration

The duty of collaboration is the obligation to promptly provide the cooperation required by *DCIAP*, *UIF*, other judicial, sectorial and police authorities and *Autoridade Tributária e Aduaneira*, namely by ensuring direct access to information and by providing documents or records. The second point of *Artigo 53º, Lei n.º 83/2017*, of August 18, states the specific obligations under de duty of collaboration.

2.1.3.9. Duty of Non-disclosure

The duty of non-disclosure concerns the obligation of the organization's employees and external service providers not to disclose to the client or third parties any information related to communications made to the competent authorities, not even the single fact that a suspicious operation was reported. (*Artigo 54.º, Lei n.º 83/2017*, of August 18)

The duty of non-disclosure does not cover the disclosure of information to judicial, sectorial and police authorities and *Autoridade Tributária e Aduaneira*, to financial entities and other entities of equivalent nature located in an EU Member State (regardless of the existence of a group relationship), between institutions that are part of the same group and are located in EU Member States or equivalent third countries in what concerns AML/CFT legislation and practices. Another exception of the non-disclosure duty is the exchange of information with another entity of a similar nature established in an EU Member State or in a third country with equivalent AML/CFT requirements, with whom the financial institution has a client or operation in common with - as long as the entity belongs to the same professional category and is subject to equivalent obligations regarding professional secrecy and personal data protection. Auditors, certified accountants, tax consultants, lawyers, solicitors, notaries and other independent legal professionals, constituted in a company or in individual practice, are also among the exceptions of the non-disclosure duty, as long as established in an EU Member State or in a third country with similar AML/CFT legislation.

Moreover, the procedures performed to comply with the duties of communication, abstention and collaboration do not constitute a breach of the duty of non-disclosure, nor do they imply responsibilities of any kind to those who perform those procedures.

2.1.3.10. Duty of Training

Artigo 55.º, Lei n.º 83/2017, of August 18, compels the training of managers and employees with relevant functions in AML/CFT so that they are aware of the legal obligations and the applicable legislation. The goal is for employees to be able to recognize operations that appear to be suspicious of being related with ML/FT crimes and subsequently act accordingly. Thus, financial entities must define and apply both an initial and continuous training policy, keeping records and proof all the training sessions. Again, all records must be kept for a period of seven years in a location easily accessible whenever requested by the compliance or internal audit functions, external auditors or competent authorities. The content presented on each session must be adequate to the specific functions of the employees present, considering that they perform relevant role in the process of prevention of ML/FT. *Artigo 43.º, Aviso n.º 2/2018*, of November 25, of the Bank of Portugal dictates that all data and information presented in the training sessions must be up-to-date and shall include a "*description of the current and applicable legal framework, the policies and procedures defined and implemented within the institution , guidelines, recommendations and information from judicial authorities, police authorities, supervisory authorities or associations representing the sector, techniques and trends used for ML / FT, the vulnerabilities of the existent business areas, products, services and operations made available by the entity, as well as the distribution channels of these products and services and the means of communication used to interact with customers, reputational risks and consequences of a non-regulatory nature resulting from non-compliance with ML/FT preventive duties, specific professional responsibilities regarding AML/CFT and the operational procedures associated with compliance with preventive duties."*

The definition of the training policy, the monitoring of its implementation and the evaluation of its effectiveness shall have the direct participation of top management and the director of the compliance function.

Financial institutions using credit intermediaries in their consumer credit operations must provide information concerning the internal AML/CFT procedures. In this case, all evidences of compliance with the training duty must be kept for at least seven years after the contractual relationship with the credit intermediary ceases.

2.1.4. ML/FT Risks and Consequences to Financial Institutions

The association with ML/FT crimes leaves financial institutions exposed to different sorts of risk, namely reputational, operational, legal and concentration risks. (Basel Committee on Bank Supervision, *Customer due diligence for banks*, 2001)

2.1.4.1. Reputational Risk

The negative publicity arising from the association of an entity with ML/FT crimes, results in a loss of trust in the integrity of the institution (Schott, 2006: II-5). Inevitably, clients and investors will refrain from incurring in business relationships with an institution whose reputation is impaired by ML/FT suspicions or allegations. Reputational risk has a serious impact in all sorts of organizations but particularly when it comes to financial entities. Consequences for financial institutions include a reduction in the profitability of operations conducted, an increase in the risk of the credit portfolio and ultimately a loss of clients. In the case of banks, liquidity issues can also arise as money launderers tend to withdraw large amounts of funds from their accounts.

2.1.4.2. Operational Risk

The operational risk derives from the inadequacy of internal procedures, the poor performance of employees or control systems, or by negative external events, causing

institutions to incur in higher costs with financing, interbank services or bank correspondence. (Schott, 2006: II-5).

2.1.4.3. Legal Risk

Association with ML/FT related practices can originate lawsuits, fines, penalties and unfulfilled contracts, resulting in increased expenses for the institution. In case legitimate clients suffer financial losses due to ML/FT events, the institution needs to ensure an adequate compensation. Ultimately, the financial entity might not have enough resources to cover all the referred additional expenses, culminating in its closure. (Schott, 2006: II-5).

2.1.4.4. Risk of Concentration

The risk of concentration arises when a financial institution is dependent on a single client or group of clients, particularly when it comes to the provision of credit or loans. The entity faces an increased potential risk of concentration if there is a lack of information about a particular client, the operations and transactions conducted by such individual or the relationship with other clients. (Schott, 2006: II-5).

The risks above mentioned are all interrelated and have costs associated, including the loss of business, the loss of customers, liquidity problems, cancellation of bank correspondence agreements, costs with fines and compensations, apprehension of assets and a decrease in the stock value of financial institutions. (Basel Committee on Bank Supervision, *Customer due diligence for banks*, 2001)

2.1.5. Risk-based Approach

The first of the forty recommendations of the FATF, regards the adoption of a risk-based approach by countries, so that the measures adopted to prevent ML/FT are not only compatible, but derive from the risks identified. (FATF**,** 2012-2019)

Furthermore, the extent of the procedures to which financial entities are obliged to varies depending on the specific ML/FT risk of each entity. The degree of risk of an organization is calculated based on the type of products and services commercialized, transactions conducted, used distribution channels, customer profiles and served geographic locations.

An important part of a risk-based approach is the risk assessment process, which consists on measuring the threat, vulnerability and consequence vectors of an organization. First, a set of threats, vulnerabilities, risks or risk factors related with ML/FT are identified. Then, an analysis is performed to assess the nature, sources, likelihood and potential consequences of the risks or risk factors identified on the previous stage. The risk analysis can be carried out in different degrees of detail, depending on the type of risk and the purpose of the assessment. The extent of the analysis is also dependent on the information, data and resources available. Ultimately, the risk assessment shall culminate in the definition of the priorities to be taken into account in the risk mitigation strategy.

A solid risk assessment methodology allows financial institutions to obtain the rating of ML/FT of each business unit as well as the global distribution of such risk. Furthermore, having an adequate risk assessment will allow organizations to identify and quantify the risks derived from the different business lines, consequently determining those that, due to their criticality, shall be addressed immediately. However, an efficient risk assessment process also detects external emerging risks, allowing institutions to identify cases in which the inherent risks must be mitigated through the strengthening of established controls and implementation of new ones if necessary, whether the inherent risks come from an internal or external source. Thus, this methodology provides an accurate evaluation of the effectiveness of the controls applied by the financial entity.

The outcome of the risk assessment shall be communicated to top management, making it a useful summary of the organization’s risk situation.

The ML/FT risk management model must be reviewed annually and kept in the form of a written document or register. The model must detail the risks of the activity carried out by the institution, how the institution identified and evaluated those risk, the prevailing means and control procedures and their adequacy on mitigating existing risks. (*Artigo 4.º, Aviso n.º 2/2018*, of November 25, of the Bank of Portugal).

2.1.6. Information Systems

Artigo 18.º, Lei n.º 83/2017, of August 18, demands financial institutions to adopt tools or information systems that consolidate records related to business relationships, occasional transactions or transactions in general, performed on behalf of the institution itself or its clients, including documents collected as part of the fulfillment of the duty of identification and diligence. These tools must allow the registration of all customer related data as well as information concerning their representatives and beneficial owners. In addition, information systems must be parametrized with the adequate scenarios and variables so that they are capable of detecting circumstances that justify the updating of the existing data elements as well as changes in the behavior and activity pattern of clients. Information systems must be capable of identifying indicators of ML/FT practices, automatically blocking suspicious transactions. Moreover, the system must identify weather the client or the beneficial owner possess the quality of Politically Exposed Person, family member or strictly associated person of a PEP. In addition, the system must be parametrized to detect if either of the referred parties belong to a list of individuals identified by sectorial authorities as being obliged to fulfill enhanced due diligence procedures, or to a group of persons or entities subject to restrictive measures imposed by The United Nations Security Council or EU rulings.

The definition and updating of the risk profile associated with clients, business relations, occasional transactions and operations in general, alongside with the monitoring of customers and operations according to the corresponding risks, are also crucial functionalities of an AML/CFT information system. At last, the system must allow for the timely extraction

of reliable and comprehensible information which supports analysis and decision-making, as well as the exercise of legally stipulated communication and collaboration duties.

The treatment of all ML/FT related data and information shall be performed in restricted access databases, built in a way that prohibits deleting, sharing or disclosing information, within the financial entity itself or to third parties.

2.2. Blockchain

2.2.1. Blockchain technology

Blockchain technology was first introduced in 2008 by the creator of Bitcoin, Satoshi Nakamoto. Bitcoin is a cryptocurrency based on a peer-to-peer network, with a decentralized structure, secured by consensus protocols and public-key encryption (Nakamoto, n.d.). Blockchain, the technology behind Bitcoin, is a public data base of records that "*combines mathematical cryptography, open source software, computer networks and incentive mechanisms*" (Davidson, Filippi and Potts, 2018). The chain itself is made up from chronological blocks which are all linked together, each one containing a bundle of records, ranging from contracts, transactions, or any other sort of information.

Whenever a new record is added, all the nodes within the network must validate the new entry, rather than a single hierarchically superior node. In other words, the blockchain is a decentralized network, meaning that all nodes are free to take action. Furthermore, the redundancy present in the blockchain storage system implies that the information flow differs from the information flow of a centralized structure. On the latter, the central authority is responsible for the transmission of information to the members of the network. Thus, without the presence of a central figure, nodes of a decentralized network must pass the information to their peers. This process is called *Gossiping* (Tasca and Tessone, 2019). To ensure trustworthiness, decision making is based on consensus mechanisms, which will be further explained on this thesis.

Traditional ledgers typically consist of centralized networks, where management is attributed to a central node which holds the power of making decisions and managing the

whole network. Naturally, centralized authority leaves more room for power abuses and disruptions in the network, if the central node has malicious intentions. Another advantage of the blockchain, is that once a record is added to the network, it is extremely difficult to alter it, since all records are secured by hash functions. A hash is a code with the exact same length of the original file composed by numbers and letters. The reason why this type of code is so effective in ensuring the inalterability of the original input, is because any minimal alteration in the original record will generate a completely different hash, therefore, the alteration can be easily traced. Given that all blocks in the network are interconnected, a change in one hash would require the calculation of the remaining hashes, otherwise the chain would break. Recalculating every hash is highly demanding and time consuming, dissuading malicious actors from hacking the network.

2.2.2. Features of the Blockchain

2.2.2.1. Immutability

Each block is identified with a timestamp, a ten-digit hash code belonging to the previous block of the chain and the transactions corresponding to that block (Blockchain Technologies, 2016). The timestamp ensures that blocks follow a chronological order, while also allowing for an accurate traceability of all transactions conducted, thus avoiding the double-spending issue that could arise in the case of cryptocurrencies (Nakamoto, n.d.). The hash code, on the other hand, is generated using a hash function, meant to transform the data used as an input – usually called the *message*, in a bit string of a predetermined size – the *message digest*, in the case of blockchain it corresponds to ten digits. The hash function provides a solid level of security since it is a one-way function, meaning that it is practically impossible to reverse it (as in trying to convert the hash code originated by the function to the input data). Each message is represented by a unique message digest, therefore, if the content of the message is altered the resulting message digest will be different (Mohanty, Sarangi and Bishi, 2010). Moreover, the hash function provides three important features – data is secured, any alterations on the message are easily identified and it avoids overlapping information. Since each block contains a hash code belonging to the previous block, all

blocks on the chain are connected. If one block (*n*) suffers an alternation, even if minor, the following block on the chain (*n+1*) will stop matching the previous one, breaking the chain. To alter a single block, one would have to go ahead and manually change the ones that follow, which not only takes a tremendous amount of work and computer power but is also extremely difficult due to consensus mechanisms. Therefore, it is possible to conclude that the blockchain is immutable.

2.2.2.2. Distributed Computation

Blockchain is a type of distributed ledger technology (DLT). Walport, the Chief Science Advisor of the United Kingdom Government, defines the distributed ledger technology as it follows: "*A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within the network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or seconds*." (Walport, 2015).

Rauchs *et al.* (2018: 22) indicate that the main differences between distributed ledgers and traditional distributed databases is the capacity to support data and maintain data integrity in the presence of malicious actors within the network, what the authors define as an adversarial environment. According to the authors, a distributed ledger technology has to possess certain properties, namely shared recordkeeping, multi-party consensus, independent validation - so that each member is able to confirm their own transactions as well as the overall integrity of the network, and finally tamper evidence and resistance, which prevent non-consensual changes that can easily be detected by any participant, while hindering the capability of a single party unilaterally altering a transaction already performed. Therefore, whilst traditional distributed databases are based on trust, centralized on an authority figure, blockchain is based on multi-party consensus.

2.2.2.3. Consensus

Bonneau *et al.* (2015) defined consensus as "*the set of rules and mechanics that allows to maintain and update the ledger and to guarantee the trustworthiness of the records in it, i.e., their reliability, authenticity and accuracy*." Moreover, consensus is not only a crucial property for the blockchain to function and ensure data quality, but it also secures all the information present on the chain, without the need to save duplicates and backups of the data. There are a few mechanisms that can be used to establish consensus on the blockchain.

Proof-of-Work

Proof-of-Work is the consensus mechanism behind Bitcoin. The reasoning behind this mechanism consists on computing new hash values resulting from the combination of the components that are already a part of the block (the hash code from de previous block and the transactions conducted) and an additional nonce added to the block, resulting in a new value for the block's hash code, which must start with a specific number of zero bits. Since all blocks of the chain are connected, the blocks that follow the one that was used as the basis of Proof-of-Work will be altered as well. Furthermore, if one wanted to change the block afterwards, Proof-of-Work would have to performed all over again.

The Proof-of-Work voting method uses CPU as the counting unit (each CPU equals one vote), instead of using IP addresses (one vote per IP address), which could lead to a scenario of concentration of power if one actor of the chain were able to allocate a large number of IP addresses. The so called honest or longest chain – the chain in which more Proof-of-Work was conducted and, consequently, the chain with more blocks validated, is the chain to which the majority to decide is provided. To surpass the honest chain, a hacker would have to repeat the Proof-of-Work of the first block of the chain and all the ones that follow. Nakamoto proves that the probability of an attacker being able to successfully surpass the honest chain decreases exponentially as the more blocks are added to the chain. (Nakamoto, n.d.).

Depending on the size of the chain, satisfying Proof-of-Work can take a considerable amount of computing power. In the case of Bitcoin, the electricity spending is massive and

the machines necessary to perform these tasks are expensive due to the substantial size of the blockchain (O'Dwyer and Malone). In the long run, this downside can lead to a centralization of the mining power (Tasca and Tessone, 2019), contradicting the concept of decentralized network.

Proof-of-Stake

According to Proof-of-Stake, the more digital assets a member has, the more qualified they are to validate and verify transactions (Tasca and Tessone, 2019). This method serves as an alternative to Proof-of-Work as it provides validation without the need to acquire expensive machines and spend a great amount of electricity resources. However, Proof-of-Stake is based on the assumption that the larger the share of a member, the more trustworthy they are. Unfortunately, this might not always be the case. Oftentimes individuals are not altruistic and those who hold a high share might benefit if they act in a malicious manner. The same factors that make Proof-of-Stake a good alternative to Proof-of-Work, also constitute one of the downsides of this consensus method – because expensive devices and vast computer power are not requirements to validate transactions, the members of the chain who hold the higher shares will be tempted to perform actions that leave them better off, even if they harm the network as whole, for instance by voting for several blockchain-histories (Tasca and Tessone, 2019).

Proof-of-Authority

Proof-of-Authority is a modified form of Proof-of-Stake, in which the actors responsible for validating blocks are chosen beforehand. This type of consensus mechanism is typically used in private blockchains, such as networks that need to be regulated by the competent authorities (Tasca and Tessone, 2019). In this example, the authorities would be the nodes with permission to conduct the validation of blocks, through the means of a digital signature. In other words, if a block is *signed* by one of the trusted actors, it means that the transactions were verified and, consequently, the block was validated. The main difference between Proof-of-Authority and the previously described consensus methods regards the

revelation of the actual identity of the person behind the node. Whilst in Proof-of-Work and Proof-of-Stake all members of the chain remain anonymous, Proof-of-Authority requires the identity of the trusted signers to be known. Having their identity revealed brings about a common constraint that keeps individuals from coming unlawfully acts – reputational concerns (POA Network, 2017). In addition, networks using this consensus mechanism tend to choose the trusted signers carefully, in order to avoid undesired scenarios. Despite the referred advantages, the risk of power abuse by a single actor or group of actors is still a threat, particularly when the list of authorized nodes for validation is small.

2.2.3. Types of Blockchains

The first version of the blockchain, brought about by Satoshi Nakamoto, is naturally a public network since it was meant to serve the exchange of a cryptocurrency, Bitcoin. However, the flexibility of blockchain created room for the technology to be used with other purposes. Whenever enterprises adopt blockchain based technologies, they opt for private or semi-private networks, due to confidentiality concerns.

2.2.3.1. Public

A public blockchain, such as Bitcoin, can be accessed by anyone, without any restrictions. Moreover, anyone can perform transactions on the chain, although the validation of those transactions is still dependent of approval through the prevailing consensus mechanisms. Permissionless public blockchains are considered to be fully decentralized networks (Sultan, Ruhi and Laknani, 2018: 53) given that any member of the blockchain is allowed to validate transactions, in other words, all actors are provided with both read and write permissions. Thus, the consensus process is secured by all the actors belonging to the blockchain, without the need to centralize power on an authority figure. The influence level of each member of the blockchain varies in accordance with the adopted consensus mechanism. In public networks, Proof-of-Work and Proof-of-Stake tend to be the most common mechanisms used.

Permissioned public blockchains consist on a less decentralized version of a strictly public network. As mentioned above, the latter allows all participants to read and write content on the blockchain. A permissioned public network, on the other hand, restricts write permissions to a specific set of nodes, nominated beforehand. Read access is still available to all members (Guegan, 2017).

2.2.3.2. Private

Private networks arose from the implementation of blockchain based technologies on organizations. The most common scenario consists on allowing all actors of the blockchain to read its content but restricting writing capabilities to specific actors of the network. Whilst write permissions are typically kept within the enterprise, read permissions may be public or subject to some restrictions, depending on the nature of the organization and the established internal rules on information sharing.

Unlike public blockchains, private networks do not possess a fully decentralized structured, in fact, decision-making is not based on consensus but on trust, given that read permissions are often centralized on the enterprise. Because only specific actors validate the transactions, this type of blockchain tends to be more efficient in terms of the number of transactions processed as well as the costs associated (Buterin, 2015). In addition, validation of transactions can be performed more easily and without spending as much time and electricity resources when compared to public networks secured by consensus mechanisms, such as Proof-of-Work or Proof-of-Stake. Although the immutability principle is clearly hindered on this case, the capability to perform alterations is exclusively delegated to those who hold the write permission, which tend to be trustworthy actors belonging to the organization. Besides, the increased level of privacy arising from restricting not only write but also read permissions is very significant.

2.2.3.3. Hybrid

Hybrid or Consortium blockchains are similar to private blockchains but instead of having the consensus process assigned to a single organization, it is assigned to a group of organizations. However, it is not mandatory that all the entities belonging to the blockchain are given the permission to validate blocks. For instance, if the blockchain is constituted by twenty institutions, each one corresponding to a node of the chain, it can be predetermined that only fourteen of them are authorized to validate transactions.

Consortium blockchains are somewhat of a middle ground between public and private networks. Although these are not fully decentralized structures, like public blockchains, decision-making is not solely centralized on a single party, as in private networks. According to Sultan, Ruhi and Laknani, hybrid blockchains can be considered a micro version of public blockchains, since they exhibit a decentralized structure but only within a limited network of participants (Sultan, Ruhi and Laknani, 2018: 53).

2.2.4. Applications of the blockchain technology

Although cryptocurrencies, are among the most recognized uses of the blockchain technology, the properties of such technology make it flexible and transversal to other fields, very distinct from one other.

Blockchain Technologies lists the areas in which the blockchain technology can be successfully applied – financial services, governance, healthcare, identity, Internet-of-Things (IoT), insurance, music, real estate, supply chain and contracts (Blockchain Technologies, 2016).

Although the blockchain technology arose in 2008, in most industries it is still in the early adoption stage. Being a new and potentially revolutionary technology, there are risks and barriers that organizations will naturally face if they wish to adopt such technology. However, the pre-adoption process is of outmost importance - executives must guarantee that employees are educated about the technology and that the necessary investments for implementation are made (Iansiti and Lakhani, 2017). The authors suggest a humble start,

developing small applications within certain lines of the organization, to obtain the necessary know-how to grow.

Despite the flexibility and the numerous possibilities blockchain provides, not all enterprises will benefit from blockchain based solutions, especially at the current stage where there is still a lot of uncertainty and a lack of successful use cases.

Nevertheless, organizations are interest in implementing blockchain related projects, with the majority of them being at the research and development stage (PwC's Global Blockchain Survey, 2018). When it comes to the leading industries, the financial services sector is at the forefront of the blockchain adoption, followed by the manufacturing industry, energy and utilities, healthcare, government and retail and consumer goods (PwC's Global Blockchain Survey, 2018).

2.2.5. Applications in the financial sector

Before looking into the applications of blockchain on the financial sector, particularly in banking, it is important to look back and understand how we got to the financial sector as we know it today.

Centralized Banking

The traditional banking industry follows a centralized structure. In its primary and most basic form, it consists on individuals using banks to store their fiat money. Naturally, banks provide other useful services, but deposit accounts are among the first and most important features of the banking activity. Having a third-party managing one's funds and transactions is obviously subject to the payment of service fees. So, why do individuals submit themselves to the payment of these fees, instead of storing their financial assets themselves? The answer is as simple as a cost-benefit analysis – the benefits of using centralized banking are superior to the costs of doing so.

Magnr concludes that there are three primary advantages regarding the use of centralized banking, the first being security. In case individuals stored their funds at their homes or if they chose to carry their monetary assets around with them, there would be some

risks associated – natural disasters or theft could easily make one's money disappear. In fact, not claiming funds can, in some cases, be considered a tax evasion or a money laundering crime. The second reason why individuals choose to place their funds in a bank is because, so far, it is the most efficient way to store and manage money. Banks facilitate everyday life tasks, such as paying bills, transferring money to other individuals and purchasing goods or services. Besides, accessing personal finances has become increasingly easier with online banking and mobile applications that allow individuals to check their accounts and balances through their mobile devices. At last, banks generate added value to their clients by rewarding them with interests. Even if the interest rates are low, clients are better off with interest than without (Magnr, 2016).

Decentralized Banking

Until the creation of Bitcoin, there was no alternative to centralized financial services. Digital banking was not a reality because there was always the double-spending issue. However, Bitcoin appeared as the first cryptocurrency that did not allow for double spending, thus making digital banking a feasible reality. Blockchain allows users to convert fiat money in cryptocurrency, without the need for an intermediary. Also, due to the technology's decentralized structure, peer-to-peer transactions can take place without the permission of a central figure, such as a bank, since validation of transactions is performed through consensus mechanisms.

The high security level provided by blockchain is greatly caused by the immutability principle. As previously referred on the thesis, it is extremely difficult to alter any data embodied on the blockchain, as it would require a great amount of time, effort, and computing power. Additionally, every piece of information is encrypted with the use of an hash function which is a one-way function, meaning that the hash code cannot be reverted to the data initially converted in code. The decentralized structure of the technology implies that blockchains cannot be altered from a single computer, since they are not located on a single location, but distributed across peer-to-peer networks. Therefore, for a single party or group of entities to gain control over the blockchain, an extraordinary amount of computing power would be necessary to access and alter simultaneously a minimum of 51% of the blockchain

(Miles, 2017). The 51% attack is more common in public networks that use Proof-of-Work to validate transactions. In the case of cryptocurrencies, malicious actors aim to double spend coins. The security level of a blockchain varies depending on whether the network is public or private. Public networks can be accessed by anyone with an internet connection, but actors of the blockchain remain anonymous. Thus, public blockchains, such as Bitcoin or other cryptocurrencies, present a higher risk due to the lack of access restrictions – anyone can be a part of the network without having to through any kind of control system beforehand. In a private setting, access is restricted, usually to the members of an organization. Here the principle of anonymization does not hold because the organization controls read and write permissions. Moreover, all participants are required to identify themselves to gain access to the network (Arunkumar and Muppidi, 2019). Miles defends that the potential security issues of private networks, coming from insiders with malicious intentions, can be solved with a highly secured infrastructure. According to the author, such infrastructure must prevent unauthorized parties from accessing sensitive data - even root users and system administrators, deny any attempts to alter information within the blockchain that might look illicit and save encryption keys to prevent them from ever being misappropriated (Miles, 2017).

When compared to centralized systems, blockchain provides increased efficiency in what concerns cross border transfers and transactions. In a traditional banking structure, cross border transfers are subject to a longer validation process than national transfers, taking longer, often a few days, until the transfer is concluded. Blockchain does not have a distinct procedure to validate national or cross border transactions. Therefore, the process to verify cross border transactions is more efficient with blockchain, which is an important feature given the importance of global trade nowadays.

As previously mentioned, banks have service fees associated with their range of financial products. These fees are necessary so that banks can cover their costs and go on with their activity. On the other hand, financial institutions also reward clients with interests. When it comes to costs, a blockchain network, once established, does not require additional expenses on the account of the members, only regular maintenance costs. In the case of

cryptocurrencies, incentives are provided so that participants are rewarded for validating transactions on the network, as previously explained when addressing Proof-of-Work.

After analyzing the pros and cons of centralized and decentralized banking in terms of security, efficiency and added value for the user, the extinction of traditional banks is not at stake, even in the long run (Blockchain Technologies, 2016). It is reasonable to imagine a future with both centralized and decentralized banking. From a customer point of view, having both options available is positive, as there are more alternatives to manage one's finances. However, from the financial institutions point of view, decentralized banking constitutes a new competitor. Furthermore, it is of outmost importance that financial entities develop adequate strategies to deal with this new reality. In fact, banks shall adopt blockchain based structures themselves to leverage the advantages of the technology. On the following section, there will be presented some areas in which the adoption of blockchain by financial institutions might be beneficial.

2.2.5.1. Instant Clearing and Settlement

The traditional asset trading process can be divided in three distinct phases – execution, clearing and settlement. The first occurs whenever the individual or organization selling the security finds a party willing to purchase it. Once the counterparties agree on the conditions of the ownership exchange, the proceedings involving the transfer of the security ownership to the buyer and the payment to the seller. Those proceedings are part of clearing, the most complex of the three stages (Fronda, 2019) as it includes netting, calculating margins, novation and managing the risks associated with the transaction (Rodgers, 2019). At last, settlement takes place once the transaction is completed, meaning that the security ownership is fully assigned to the buyer and the money is available on the seller's account. According to Benos, Garratt and Gurrola-Perez from the Bank of England, the traditional asset trading process, namely clearing and settlement stages, can be quite consuming in terms of time and money. To ensure that the risks inherent to the exchange are managed and mitigated, there are several parties and procedures involved. Consequently, trading costs are

high, and settlement can take up to three day to be completed (Benos, Garratt and Gurrola-Perez, 2017: 2-5).

Blockchain eliminates the need for the intervention of third parties when exchanging securities, since the payment goes directly to the seller's wallet, and vice versa. Thus, the costs associated with having multiple parties conducting the exchange are substantially reduced. Distributed ledger technology also decreases the settlement time from an average of two to three days to seconds or a few minutes, at the maximum. However, real time settlement is only possible if a cryptocurrency is used as the payment method, otherwise banks are required to convert fiat money in the chosen cryptocurrency to follow through with the transaction. Due to currency volatility, this process might be challenging. McKinsey suggests *stable coins* as a solution for the volatility problem, as the value of these coins is pegged to real-world assets. Nonetheless, an intermediary is still required to perform the conversion (Higginson, Hilal and Yugac, 2019).

2.2.5.2. Cross-border Payments

Similarly to asset trading, cross-border transactions are also associated with high costs as well as inefficiencies when it comes to settlement time. Thus, distributed ledger technology could be a fitter alternative. However, the conversion and volatility are more significant when it comes to cross-border payments since each transaction entails at least three distinct currencies: the national currency of the sender, the cryptocurrency to which the fiat money must be converted to in order to be a part of the blockchain, and the national currency of the recipient. Compared to asset trading (holding the assumption that the buyer and seller are from the same country), each transaction requires at least two currency conversions, instead of one. The volatility issue also escalates when dealing with an additional currency. Nevertheless, some companies were able to counter these setbacks and develop adequate blockchain based cross-border payment systems.

IBM created *IBM Blockchain World Wire,* a platform that allows instant clearing and settlement of cross-border payments. It works by converting the fiat currency of the sender in a digital asset, central bank cryptocurrency or stable coin, which is then converted in the

fiat currency of the recipient. The two institutions are free to decide beforehand which intermediate digital asset they wish to use. Basically, *World Wire* is the intermediary responsible for converting the agreed upon digital asset into the recipient's fiat currency (IBM, 2018).

In the financial sector, Santander was the pioneer in the development of a cross-border payment service based on distributed ledger technology. On the 12th of April of 2018, the Spanish bank launched *Santander One Pay FX*. The technology behind it is *xCurrent*, a distributed ledger technology developed by Ripple. The service allows for international transfers to be settled on the same day in the majority of case, or latter in the following day. Besides, senders can visualize beforehand the exact amount that the counterparty will receive in the destination currency, in case they follow through with the transfer (Santander, 2018).

2.2.5.3. Record Keeping and Auditing

Auditors oftentimes face some challenges in their activity, especially when auditing large companies, which frequently have a multinational scope. Information is dispersed through different databases within the organization, making it difficult to look at the big picture and detect eventual flaws. Blockchain would allow for standardization of bookkeeping and data storage in general, while providing a consolidated view of all customer activity in a single repository. The transparency and immutability features, inherent to this technology, make it attractive for auditors and regulators. Because all transactions on the blockchain are endowed with a time stamp, it is possible to conduct a frictionless audit trail, since auditors can easily trace and reconstruct the track record of all transactions.

The quality and veracity of the records kept by financial institutions is another prevailing issue that not only makes auditing a long lasting and difficult process, but also harms the daily activity of financial entities. By design, all transactions must be validated and verified in order to be a part of the blockchain. Regardless of the chosen consensus mechanism, veracity of the records kept on the distributed ledger is ensured.

2.2.5.4. Digital Identity and Data Privacy

Although privacy and transparency appear to be opposite concepts, a distributed ledger technology allows for both attributes to seamlessly coexist. However, the extent to which one overcomes the other varies depending on the type of blockchain. In public networks, the degree of privacy is higher when compared to the degree of transparency, since members are allowed to choose which identity elements they reveal to the network – because data on the blockchain is cryptographically secured, individuals can act in an anonymous matter if they wish to do so. On the other hand, in private blockchains not all members have the same permissions. If regulators belong to the network, they might be given the permission to unveil the identity of the remaining members of the blockchain, whilst another element, for instance a client of a financial institution, will not be granted such access. Hence, transparency surpasses privacy on this case. However, if permissions are correctly and carefully attributed, privacy can still be preserved will providing the necessary transparency for regulators and supervisory authorities to act upon.

2.2.6. Barriers to Blockchain Adoption

Despite the advantages offered by the distributed ledger, there are a few obstacles keeping organizations from adopting blockchain based strategies. Between February and March of the current year, Deloitte conducted a blockchain survey to sample composed by 1.386 senior executives of different organizations alongside with 31 emerging disruptors of the technology, at an international level. Respondents named regulatory concerns (30%), replacement of legacy systems (30%), potential security threats (29%) and lack of internal knowledge and skills on the matter (28%[1]) as the main barriers to further adoption and investment in blockchain technology. Nevertheless, 86% of respondents agreed that blockchain is scalable enough to attain mainstream adoption, with 83% of the surveyed entities pursuing blockchain as a compelling business case (Deloitte 2019 Global Blockchain Survey, 2019).

[1] Percentages total more than 100% because respondents were given the opportunity to select more than one answer, if they wished to (Deloitte 2019 Global Blockchain Survey).

PwC conducted a similar survey in 2018. The sample used was much smaller when compared to Deloitte's sample size, but it was still significant as it included 600 executives from 15 different territories. Respondents listed similar barriers to adoption of the distributed ledger, namely, regulatory uncertainty (48%[2]), lack of trust among employees (45%) and ability to benefit from network effects (44%). The authors of the study predict that by 2030 the distributed ledger technology will generate an annual business greater than three trillion US dollars (PwC's Global Blockchain Survey, 2018).

2.2.6.1. Regulatory Uncertainty

According to Deloitte's 2019 Global Blockchain Survey, as mentioned on the previous section, 30% of respondents named regulatory concerns as a barrier to further adoption and investment in blockchain technology. Moreover, half of the respondents claimed privacy to be the primary regulatory issue of concern for their organizations or projects, followed by money transmission (41%), KYC/AML (39%) and reporting (39%).

Blockchain is an innovative technology, flexible enough to be presented in numerous forms and to be applied to different industries. Additionally, it implies moving from a centralized to a decentralized system. Although public, private and consortium blockchains each provide different levels of decentralization, the elimination of a centralized authority is still a massive shift that might leave regulators unsure how to act upon these circumstances.

On July 2019, the European Parliament Research Service issued a study on the compatibility of blockchain with European data protection law, in which three policy recommendations were elaborated (European Parliament Research Service, 2019). The author starts by clarifying that the compatibility between distributed ledgers and GDPR is not black and white. General Data Protection Regulation is intended to be technologically-neutral, so that it can be applied to several technologies, regardless of individual specificities. However, the legal uncertainties and lack of concrete definitions of certain GDPR concepts, hampers its applicability not only to blockchain, but also to other technologies. Thus, the first

[2] Once again, percentages total more than 100% because respondents were given the opportunity to select more than one answer, if they wished to (PwC's Global Blockchain Survey, 2018).

policy suggested regards regulatory guidance with further enlightenments on the applications of GDPR concepts to blockchain use cases. Given the various forms and potential applications of blockchain, each use case will have to be analyzed individually. Moreover, one cannot conclude whether blockchain *per se* is compliant or non-compliant with data protection legislation. Nevertheless, organizations implementing blockchain based projects could provide regulators important insights on the characteristics of the technology. The author believes joining forces between regulators and the private sector would be beneficial for both parties, namely through the development of certification mechanisms and codes of conduct – which constitutes the second policy recommendation. The EU Cloud Code of Conduct, produced to achieve compliance of cloud computing with GDPR, can be used as an example of a successful. The third and last policy suggested aims to go beyond the synergies of knowledge sharing between the private sector and regulators. The policy comprises funding for interdisciplinary research, so that the two parties can work together in building blockchain based systems that, by design, offer the required features to ensure compliance with GDPR. Again, the outcome would bring advantages both for the private organizations, by promoting valuable technological developments without regulatory barriers holding back innovation, and for regulators as it would allow for the production of adequate legislation on the matter.

When it comes to compliance with data protection law, private blockchains are more likely to be set up in a way that does not harm data privacy. Unlike public networks, private blockchains allow for the restriction of read and writing permissions to specific actors, therefore, not all members of the network have access to personal information. Because only pre-selected actors are granted permission to treat and manage data, responsibility can be easily accounted for. Immutability is another inherent property of distributed ledger technology that does not appear to be aligned with data protection. Articles 16 and 17 of GDPR imply that data can be altered or erased at any given time, although the meaning of erasure defined in the latter article is not clear for the author. By design, it is extremely difficult to alter or eliminate any data inserted on the blockchain, especially when it comes to public networks, due to the great amount of manual work and computing power it would require (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016). Again, private blockchains are more compliant with GDPR as the attribution of

distinct permissions to the actors of the network hinders the immutability feature, making it easier for the authorized parties to conduct alterations and eliminate data from the network whenever necessary.

2.2.6.2. Replacement of Legacy Systems and Scalability

The implementation of a distributive technology, such as blockchain, not only requires a high initial cost, but it implies substantial alternations in the way the organization conducts its activity. McKinsey's 7-S Framework identifies seven organizational spheres that shape and define its capacity to change, namely, strategy, structure, systems, style, staff, skills and shared values (Peters and Waterman, 1982). The identified areas are all interconnected, therefore, if change occurs in one of the areas the remaining ones are all affected as well. In the case of the adoption a distributed ledger technology, the change would take place in the "systems" sphere, but its impact would be transversal to the six remaining fields. This goes to show the magnitude of the implementation of blockchain on organizations.

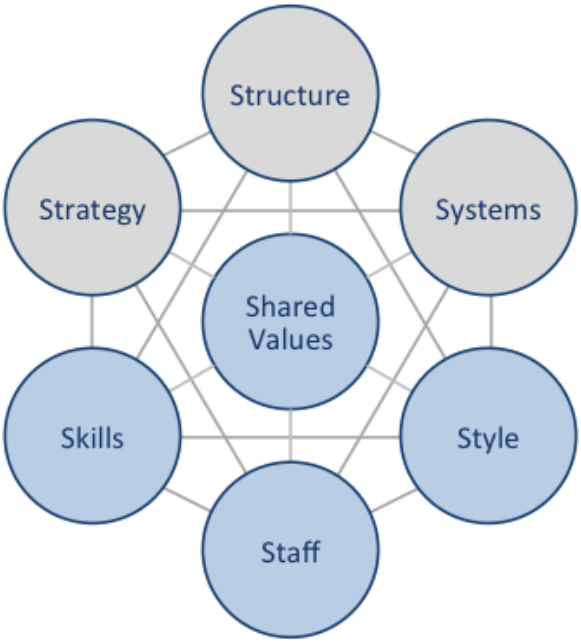

Figure 1: McKinsey's 7-S Framework (Dudovskiy, 2016)

Change, even if positive for the organization, generates resistance (Kotter and Schlesinger, 2008). Even though employees might be able to perceive the positive outcome of such change, they will inevitably experience feeling of loss and uncertainty about the future. Furthermore, moving from a centralized system to a distributed ledger, is far from being just a minor alteration, which can be overwhelming to some individuals. The reactions can be aggravated if employees are not familiarized with the new system. Top management must take time to share their vision rather than just imposing it (Jalagat, 2016). Thus, it is of outmost importance that all members of the enterprise are presented with the necessary knowledge about the new technology *a priori* of its establishment. If individuals know beforehand the reasons behind the change, how the new system will impact their daily tasks, how can they take advantage of it and what are the expected outcomes, they will be more prone to accept the change.

On the previous paragraphs, only the implementation of the new technology was referred. However, replacing legacy structures goes beyond the implementation of the substitute system. Naturally, decision makers also look at the long-term effects, both in terms of the cost structure evolution as well as in what concerns scalability and efficiency. Public blockchains reveal a decrease in efficiency as the number of nodes increases, since transactions require more time and computing power to be validated due to the permissionless consensus process through which transactions are verified. Private networks, on the other hand, perform better in terms of efficiency, since there are fewer actors responsible for validating the transactions. Therefore, private blockchains are more efficient in terms of time and electricity resources spent on transaction validation, proving to be more prone to scalability compared to public networks.

2.2.6.3. Security Concerns

As previously mentioned, when addressing decentralized banking services, blockchain possesses inherent properties that ensure good security levels. However, like any other technology, there are some flaws that can be exploited by malicious actors. In January of 2019, the cryptocurrency Ethereum Classic suffered a 51% attack in which the malicious

actor was able to perform consecutive double spending of the coin by gaining control of a large percentage of the computing power of the public network (Orcutt, 2019). Bitfinex, a Hong-Kong based exchange platform for Bitcoin, was also a victim of a cyber-attack, incurring in a loss of 73 million US dollars (Baldwin, 2016). From 2017 to the early 2019, the loss of cryptocurrency to attackers equaled two billion US dollars (Orcutt, 2019).

Arunkumar and Muppidi from IBM state that security can be achieved with proper risk management, thus, understanding and classifying the potential risks associated with blockchain is a crucial first step. The authors divide the underlying risks in three categories – business and governance, process and technology risks. The first group includes policy definition, management of access permissions, financial risks associated with fraud and loss of important data as well as compliance, legal and audit issues that might arise with the use of the technology. Process risks have to do with vulnerabilities on the code used to program the system or on the infrastructures in which it is built upon, non-secure communication within the system and management of identity keys. The last category refers to underlying technology risks, related with storage, poor performance of the identity keys and transaction tokens, malfunctioning of the authentication or consensus process and flaws in smart contracts (Arunkumar and Muppidi, 2019). KPMG elaborated a blockchain risk assessment model based on a maturity scale composed by five stages (*adhoc*, reactive, proactive, service, value), covering all the risk areas of the distributed ledger and allowing firms to understand where the main vulnerabilities are located. The robustness of the system as one moves across the stages. For instance, the first level implies deficiencies in the validation of members of the blockchain, moving to the next level supposes that those deficiencies have been solved, meaning that the security level increased consequently. The fifth and last stage of the maturity scale, the value level, includes processes that ensure solid security controls in the present but also predict future network events and how to the mitigate the associated risks that might arise (KPMG, 2018).

Before defining the adequate risk mitigation strategies, Arunkumar and Muppidi recommend the construction of a threat model as a way to perform an in-depth analysis of the vulnerabilities present in the blockchain based solution at hand. The goal of the threat model is to present an overall picture of all the threats the organization faces, including the

usual threats deriving from the cores activity of the company, the new ones stemming from blockchain adoption and the threats resulting from the convergence of legacy systems with the distributed ledger.

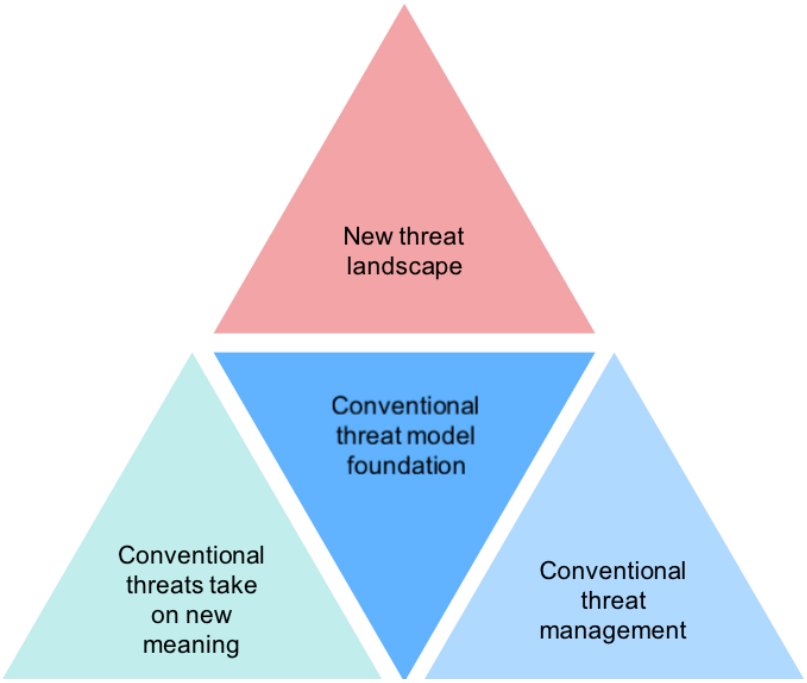

Figure 2: Threat Model in a Blockchain Solution (Arunkumar and Muppidi, 2019)

Arunkumar and Muppidi believe that the main challenges associated with such technology derive from the variety of actors and individual components it possesses. Therefore, it is of outmost importance that all the actors of the network are continuously monitored in order to promptly detect structured attacks, organized by colluding malicious actors, and act accordingly towards a fast recovery of the resulting losses. Given the decentralized nature of the technology, attackers are more likely to succeed if the chosen target is the infrastructure or application supporting the blockchain. Additionally, firms also have to account for traditional threats that might escalate further with blockchain or any other newly implemented technology, such as data leaks and spiteful transactions.

Following the development of a risk and a threat model, organizations have the necessary base to assess which proceedings shall be adopted to properly mitigate the security breaches that might arise in the decentralized network. The authors consider that the chosen mitigation proceedings shall be a combination of blockchain specific controls as well as traditional and business-related controls. Again, the goal is not only to account for inherent features of the technology, but also for the ways in which such technology will influence the company's core activity. Given the flexibility of blockchain, it is essential to consider these two spheres because the solutions might be very different depending on the blockchain use case.

3. The Impact of Blockchain on AML/CFT

The literature review conducted on the second chapter of the dissertation, allowed me to acquire essential knowledge on the concepts under analysis – AML/CFT and blockchain technology. The information collected from credible sources and authors, provided the solid knowledge base required to understand the relation between the two topics.

Furthermore, the following section will address the impact of blockchain technology on the prevention of money laundering and counter terrorism financing by financial institutions, particularly in a context that supposes the adoption of such technology by financial entities in ways that affect the AML/CFT process. To do so, I will analyze how blockchain based solutions for financial entities affect the major components of ML/FT prevention, namely – KYC and CDD, data quality, reporting to regulators, security and data privacy.

3.1. KYC & CDD

An effective KYC process is of outmost importance when it comes to preventing ML/FT related crimes. The personal client data collected as a part of the KYC serves as a basis for the calculation of the corresponding ML/FT risk level of each client. Therefore, a flawless and complete KYC ensures that the client is placed in the appropriate ML/FT risk

category, in line with the information and documentation provided. Having the customer portfolio placed in the right risk category, depending on each individual profile, is vital for financial entities because the level of customer due diligence applied to each client derives from the corresponding ML/FT risk. As previously seen on section 2.1.2.3., when addressing the identification and diligence duty, financial institutions might apply simplified or enhanced identification and due diligence measures, depending on the risk associated with the client profile or activity conducted. In an extreme scenario, a weak KYC can lead to the placement of a high-risk individual – with an increased likelihood or probability of being involved in ML/FT crimes, in a lower risk level. This would imply the application of simplified identification and due diligence instead of enhanced measures that would allow the entity to gather more documentation and customer data. Unlike, enhanced CDD, simplified proceedings do not ensure a close and continuous monitoring of the client activity, which would for a better prevention or earlier detection of ML/FT related behaviors.

Financial institutions understand the importance of having a robust KYC process and regulators drew specific demands that must be fulfilled. Because entities want to ensure the quality of KYC, it often becomes an extensive process, with client data and documentation being validated by different departments. Although it provides a good way to guarantee the validity of the information provided by the client, thus contributing to an accurate customer profiling, it harms efficiency. Additionally, documentation might be lost in the validation process.

Blockchain can be a solution for the inefficiencies of the traditional KYC process. The technology allows for the creation of a digital identity, built with the personal information provided by the client as part of onboarding. Each digital identity is unique and unreplaceable, in simple terms, it works as a sort of digital fingerprint. Given the sensitivity of the data at hand, a public blockchain would not be the most appropriate solution. A private network, on the other hand, would support and efficient onboarding process, while ensuring the that the sensitive information stays inside the financial institutions network. Moreover, it would for accurate customer profiling based on the information and documents provided by the client – all gathered in the digital identity, thus ensuring and adequate assessment of the client's risk in terms of ML/FT. Again, an appropriate risk assessment is crucial for the

prevention of malicious behaviors by applying the proper identification and due diligence level. Alternative to a private network, a consortium blockchain could also be a beneficial solution for financial institutions, allowing them to leverage network benefits when it comes to KYC. If a client as an account on Bank X, having completed the regular onboarding proceedings, and chooses to open another account on Bank Y, Bank X can share the client's digital identity with Bank Y, eliminating the need for the client to provide personal data once again. A consortium blockchain brings advantages both to the client, providing a simplified and faster onboarding when opening the account on Bank Y, as well as to the financial institutions – in this case, Bank Y will save time and resources by receiving the information provided by Bank X. Looking at the example, one might think that, although the client and Bank Y benefit from the exchange of information, Bank X is does not. Why would Bank X want to offer Bank Y sensitive client data without anything in return? Afterall Bank X spent valuable time and resources collecting and processing the data provided by the client, why give it away for free? Oftentimes leveraging network benefits requires looking at the big picture. Although Bank X helped Bank Y on this occasion, the opposite might occur. If a client from Bank Y decides to open a second account on Bank X, the latter would appreciate the collaboration. Of course, this scenario, although advantageous for all parties involved, is not black and white. Firstly, financial institutions joining the consortium must ensure the compatibility of internal data management systems with blockchain, so that data can be promptly extracted and managed. Then, the client would have to authorize the exchange of information. Finally, financial institutions must focus on the overall benefit, instead of acting upon selfish ways.

Financial institutions monitor all client activity, particularly the activity of those subject to enhanced due diligence measures. The distributed ledger technology would allow for a better control over transactions, particularly in a hybrid network. With traditional centralized systems, a financial entity can only control the activity an individual conducts using the accounts of that same entity. However, blockchain would provide an aggregated view of all transactions performed by an actor, throughout their unique digital identity. Whenever one of the financial institutions identified a suspicious behavior severe enough to be reported the competent authorities, if the authorities were members the network, they would have access to all the transactions performed by a certain individual, regardless of the

financial institution used an intermediary to conduct those transactions. Of course, this permission would be exclusive to the competent authorities, to avoid data privacy breaches. By having all individual activity gathered in one single source, the authorities would not spend time collecting and putting together data from disparate sources, increasing the response time and preventing further malicious behaviors.

3.2. Data Quality

ML/FT detection and prevention are highly dependent on data – customer identification data and data regarding transactions. When it comes to AML/CFT related data, it is not as simple as the more the merrier. Quantity must not be prioritized over quality. Large amounts of data are useless if they are inaccurate, which can actually lead to imprecise decision making. Moreover, the lack of data quality harms AML/CFT management by financial institutions, as it sabotages the prevention and detection of ML/FT related behaviors.

Nowadays, data collection by organizations goes beyond internal databases and spreadsheets, external sources of data, such as the Internet, are also frequently used. External data is naturally more costly to manage, as it comes from disparate sources in different formats. Thus, raw external data must be treated beforehand so that it is converted to a standardized format, so that it becomes compatible with internal analytics and storage systems and comparable with internal data (Marr, 2017: 85-86). According to Bernard Marr, the most valuable outcome derives from the combination of internal and external data. Nevertheless, the risk of poor data quality becomes increasingly higher as the volume and complexity of data collected and stored by an organization increases (Watts & Shankaranarayanan, 2009).

The way data is stored on the blockchain allows for a certain level of standardization, useful when dealing with large volumes of data coming from various sources. The immutability property contributes to the integrity of the data present on the network, by impeding malicious actors from altering information for their individual benefit. Although this property brings important advantages when it comes to data integrity and fraud

prevention, full immutability is not desirable in an organizational context, in which adjustments might have to be made at some point. On a private or consortium blockchain, however, the immutability principle is not absolute, leaving room from for correcting data incorrectly inserted on the distributed ledger. In terms of compliance with GDPR, a fully immutable system is also not ideal, since it does not support the alteration or elimination of information. Furthermore, a private or hybrid blockchain allows financial institutions to leverage the perks of offered by the immutability principle, namely the standardization and traceability of all registries and subsequent alterations, while also enabling the possibility to alter or delete data from the network. While this last feature is important, not every member of the blockchain has be awarded with the permission to conduct alterations or eliminate information. Financial entities shall manage read and write permissions in a way that is compatible with their core business and still provides a strong level of protection of the sensitive business and costumer data.

In the context of a consortium blockchain, standardization allows for valuable information sharing between the members of the consortium. As mentioned on the previous section, financial institutions, regulators and clients can benefit from the collaboration fostered by the network. Considering financial institutions individually, the harmonization of data throughout the whole organization eliminates efficiencies caused by the different ways each department chooses to treat and present the data. Also, the decentralized nature of blockchain solves the issue of duplicate entries of the data by different business areas – once information is introduced in the system by one department, all the other ones will have access to it, if provided the necessary permissions.

Summing up, blockchain ensures a hefty level of data quality, particularly private or hybrid networks. High data quality standards guarantee the veracity and trustworthiness of KYC, CDD and transaction information, giving compliance officers a solid foundation for their analysis. Accurate data leads to accurate customer profiling and ML/FT risk assessment. Consequently, if a financial entity has a flawlessly segmented customer portfolio in terms of ML/FT risk, it will succeed in preventing and identifying suspicious behaviors. In addition, the distributed ledger deters fraud by providing traceability of all transactions performed on the network. If an insider with malicious intentions committed a fraudulent act, blockchain

would allow for a complete reconstruction of all the steps taken to do so, tracing them back to the author of the transgression.

3.3. Reporting to Regulators

The activity conducted by financial institutions is supervised by regulators, who demand frequent reports. In what concerns AML/CFT, the Bank of Portugal demands an extensive annual report on the matter – *Relatório de Prevenção do Branqueamento de Capitais e do Financiamento do Terrorismo*, with the corresponding guidelines contemplated in *Instrução n.º 5/2019*. Besides, in line with the duty of communication, financial entities, namely the Compliance department, must report any dubious events that might be detected in the diligences carried out by the AML/CFT analysts or any other employee to the competent authorities, *DCIAP* and *UIF*. The communication of the incident shall be made as soon as it is detected and it must include a description of the factors that lead to consider the behavior suspicious, all the evidences portraying the operation at hand as well proof of the analysis conducted. Additionally, the entity must include the identification and all the information regarding the activity of the person or persons involved in the suspicious incident. Financial institutions are also required to provide immediate access to any information, documents or records requested by *DCIAP*, *UIF*, other judicial, sectorial and police authorities and *Autoridade Tributária e Aduaneira* as part of the duty of collaboration.

To fulfill these duties, a simple and agile information flow is recommended, composed by the minimum possible number of actors. The decentralized structure of blockchain allows for a smooth flow of information, without the need for the intervention of unnecessary parties, which often occurs in traditional centralized systems. If regulators belong to the network, communication with financial institutions becomes easier and faster. Plus, financial institutions will spend less time collecting and putting together all the pieces of information requested by regulators under the duty of collaboration or the evidence concerning the reported incident under the duty of communication. In a consortium blockchain setting, regulators will benefit from the harmonization of how data is presented and reported by the different financial entities belonging to the network. As for now

regulators receive information from the numerous institutions under their supervision, in all sorts of formats, apart from mandatory reports, such as the report above mentioned (*Relatório de Prevenção do Branqueamento de Capitais e do Financiamento do Terrorismo)*, which usually have a predefined template. The data harmonization will allow regulators to effectively compare the information sent by the various financial entities. Thus, regulators can assess more accurately which institutions are compliant with prevailing law and regulations, and which ones are not. Looking at a scenario in which Bank A and Bank B are peers, meaning that they are about the same dimension, conduct a similar activity and their core product is equivalent. After analyzing the reported data and information by both banks, Regulator C concludes that while Bank A is compliant with AML/CFT legislation, Bank B presents some deficiencies on crucial matters for AML/CFT. Both banks reported data in a similar manner, making it clear for Regulator C to understand the main differences between the two entities. Since both entities are overall quite identical, Regulator C can recommend a few of Bank A's best practices to Bank B, so that it becomes fully compliant. Bank B will therefore receive recommendations proportional and adequate to its dimension and activity. Once Bank B implements those best practices, it will become compliant. The example shows that standardized reporting helps regulators not only in performing a rigorous evaluation of the compliance level of financial institutions, but also in suggesting measures that are adequate to the reality of each entity, considering the individualities of each one of them. Moreover, blockchain promotes an increase in the number of compliant entities, which in turn decreases the likelihood of ML/FT crimes taking place.

3.4. Security and Data Privacy

AML/CFT involves the collection and management of very sensitive data, ranging from personal client information, to sanctions lists, lists of politically exposed persons, transaction history or documentation regarding the origin of the client's funds. Therefore, security is a must in any AML/CFT information system. Customers have become increasingly aware of data privacy concerns with the proliferation of GDPR. Moreover, an AML/CFT management system must ensure both strong security levels as well as compliance with data privacy regulation.

On section 2.2.6.3., regarding the security concerns associated with blockchain, it was concluded that attacks are more likely to succeed if the chosen target is the infrastructure or application supporting the blockchain due to the decentralized nature of the technology. Plus, firms also need to account for traditional threats that might escalate further with blockchain, as they would with any other newly implemented technology, such as data leaks and fraudulent transactions. The decentralized nature of the distributed ledger eliminates the need for onboarding client information, in which KYC data is included, having to go through several departments of the financial institution in order to be validated. Having a more efficient information flow, decrease the chances of client data being lost in the process. If financial entities choose to become part of a consortium blockchain, institutions might be able to share information, in case they have clients in common and the clients agree with the information exchange beforehand. If the exchange takes place, the client will be spared from providing sensitive personal data again, thus decreasing the probability of having conflicting data about the same individual alongside with the probability of information and documentation being lost.

When addressing the regulatory uncertainty associated with blockchain technology, the data privacy field was analyzed, more specifically on section 2.2.6.1. of the thesis. It was concluded that private blockchains were more compliant with GDPR than public networks. Firstly, private blockchains are usually permissioned, meaning that not every member is allowed the read all contents present on the network, nor are they able to write and validate them. Therefore, read and write permissions can be exclusively granted to those, due to their functions, are strictly required to access and manage the sensitive personal information. In a financial institution, compliance officers might be granted access to KYC/CDD data so that they can perform the necessary AML/CFT analysis and diligences. On the other hand, credit risk analysts will only have access to the information and documents required to perform a regular credit risk analysis. Client H from Bank A will be able to visualize the personal data provided to Bank A as well as his corresponding account movements, but Client H will not be able to access the personal information and transactions of Client J from the same bank or Client K from Bank B, even if they all belong to the same consortium blockchain. Furthermore, each actor of the blockchain shall only be granted access to the data needed to conduct its function on the network. Articles 16 and 17 of GDPR imply that data can be

altered or deleted at any given time. Therefore, a fully immutable blockchain, which would be the case of a public network, is clearly non-compliant with these two articles. Once again, private or hybrid blockchains perform better when it comes to compatibility with data protection law and regulation. Despite possessing the immutability feature, private and consortium networks are not one hundred per cent immutable. The fact that these two types of blockchains can be permissioned, instead of permissionless like public ones, implies that data on the blockchain can be altered or eliminated by those with the permission to do so. In the case of consortium blockchains, if Client H, who is a client of Bank A, wishes to open a new account on Bank B, Bank A will transfer Client H's KYC information to Bank B, only and only if Client H explicitly authorizes Bank A to do so. If the client does not consent the information exchange between the two banks belonging to the same consortium blockchain, Bank B will only be able to read the hash functions resulting from the encryption of Client H's information by Bank A. It is important to remember that a hash function is a one-way function, making it practically impossible to revert the hash code in its original content.

4. Conclusion

After analyzing the information gathered about each main topic as part of the literature review, it was possible to reach some conclusions concerning the impact of blockchain based solutions on AML/CFT management by financial institutions, thus answering the research question (RQ1). Moreover, the third chapter of the dissertation consisted off a gap analysis of the overall effect of blockchain based systems on the four main factors contributing to a strong AML/CFT strategy. The dimensions addressed, namely, KYC and CDD, data quality, reporting to regulators, security and data privacy, were chosen based on theoretical knowledge obtained while conducting the literature review as well as practical knowledge deriving from what I have learned so far as an AML/CFT analyst. The KYC and CDD processes are of outmost importance because they are the main vehicles used by financial institutions to gather personal client information, which serves as a basis for costumer profiling and individual risk assessment. Data quality is inherently correlated with a solid KYC and CDD process – if the data is not authentic, all the proceedings that follow, including costumer profiling and placement in the corresponding risk category, will be made

based on incorrect facts, thereby leading to inaccurate decision making. A proper reporting of AML/CFT data is beneficial for the financial institution, for regulators and for society as a whole, as it leads to a reliable evaluation of compliance with AML/CFT legal standards. When organizations receive a trustworthy feedback from regulators, they can take the necessary measures to start or maintain the compliant behaviors, thereby decreasing the risk of ML/FT crimes taking place. Again, data quality is key for incisive reporting. Lastly, strong data privacy and security levels are required to avoid data leaks and attacks from malicious actors. Besides, the information handled in the AML/CFT proceeding consists of sensitive personal client data, which implies that compliance with GDPR is of outmost importance.

The research question (RQ1) aims to clarify the general impact of blockchain on AML/CFT. However, given the flexibility of the distributed ledger technology it is not possible to conclude whether the overall impact is negative or positive, as it greatly depends on the use case. On the thesis, the focus was directed towards use cases that directly affected the AML/CFT process. Nonetheless, the answer is still not straightforward. Here, the main differences come from the type of blockchain at stake. As mentioned on section 2.2.3., there are three types of blockchains – public, private and hybrid. The results from the gap analysis conducted on the third chapter of the thesis, show that private and hybrid blockchains perform better in terms of compliance with AML/CFT standards. Public blockchains, on the other hand, fail to provide the required features to be adopted by a financial institution. As the name suggests, public networks can be accessed by anyone with Internet connection, which is not ideal considering the amounts of sensitive and private internal data present on a financial entity systems. Additionally, public blockchains are fully immutable – once a piece of data is inserted on the network, it cannot be altered nor deleted. Full immutability is not desirable in an organizational context, in which data inserted on systems might suffer posterior alterations. Besides, a fully immutable network is not compliant with GDPR. Clients need to be able to exert their rights, which implies having the possibility to alter or erase personal data from the institutions systems, if they wish to do so. Unlike public networks, private and hybrid blockchains are capable of being compliant with AML/CFT legal requirements. Both types of blockchain allow for the attribution of read and write permissions, so that only the required parties are given access to sensitive data. On a private setting, the information would stay within the financial institutions – basically, a private

blockchain would act as an internal system. On a consortium blockchain, the information would be available to the members of the consortium. Again, the possibility to attribute different read and write permissions implies that not all participants will have access to the same content. Private and consortium blockchains do not exhibit full immutability. Hence, financial institutions can leverage the benefits of the immutability feature inherent to blockchain technology, namely the standardization and traceability of all registries and subsequent alterations, while also having the possibility to alter or delete data from the network. Therefore, compliance with GDPR is ensured. In terms of efficiency and scalability, private and hybrid blockchains also outweigh public versions of the distributed ledger. Public blockchains must undergo Proof-of-Work, the most popular consensus mechanism for this type of network, every time a transaction takes place. As the size of the network increases, the longer Proof-of-Work will take and the more computer power it will require. Private and hybrid blockchains are more prone to being scalable. Since there are fewer actors responsible for validating the transactions, increasing the network size will not have a significant impact in terms of time and energy efficiency.

Furthermore, it is possible to conclude that private and hybrid blockchains are a better fit for financial institutions. Consortium blockchains provide an additional perk – network effects. Considering the financial industry context, financial institutions and regulators would be good candidates for being a part of the consortium, as long as the members of the consortium are included in the exceptions of the duty of non-disclosure. Network effects are mostly related with the information sharing a consortium blockchain allows. Financial institutions, by being able to share information with their peers would have more valuable information available, become more efficient - as they would be able decrease onboarding time and costs and diminish the possibility of client data and documentation being lost, thus increasing data quality. Regulators would benefit from the smooth information flow, standardized reporting and easy access to data whenever necessary. Globally, the fight against ML/FT would be more efficient. Nonetheless, financial institutions would have to be willing to work together, which implies a great mindset change. Organizations are used to think of their peers as competitors and not allies.

In conclusion, blockchain based solutions are capable of bringing advantages to financial institutions, particularly when it comes to private or hybrid blockchains. Whilst the latter provides greater benefits, it also implies overcoming more barriers. Either way, organizations must perform a cautious cost-benefit analysis before adopting distributed ledger technology. Replacing legacy systems requires not only a significant investment, but also a change in the company structure. Adopting blockchain implies moving from a centralized system to a decentralized one, which *per se* is already a considerable change. As a result, the organizations might have to undergo a few alterations – processes might look different with the new technology, new departments might have to be created and employees will certainly be required to have new technical skills. If the company fosters a culture where change is perceived as positive, the transition will be smoother. However, if employees are not prepared to deal with change, the transition will surely take more time and require more efforts from top management. Moreover, financial institutions implementing blockchain based solutions must provide their employees with proper training beforehand. Ideally, the content of the training sessions shall cover technical skills as well as the reasons behind the adoption of the new technology, how it will impact employees' usual tasks and what are the expected benefits. Regulatory uncertainty is the main reason holding organizations back in adopting the distributed ledger technology. Therefore, clear regulation on the matter would not only be an incentive for financial institutions to start tackling blockchain use cases, but also an effective way for regulators to ensure that entities are compliant with legislation from the start.

5. References

Arunkumar S. & Muppidi S. 2019. Secure your blockchain solutions. Retrieved September 10, 2019, from https://developer.ibm.com/articles/how-to-secure-blockchain-solutions/

Autoridade de Supervisão de Seguros e Fundos de Pensões. (n.d.). Missão, Atribuições e Competências. Retrieved July 24, 2019, from https://www.asf.com.pt/NR/exeres/4BF1F468-F99E-40FD-A3CC-8A47F5C7F099.htm

Baldwin C. 2016. Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong. ***Reuters***. Retrieved September 28, 2019 from https://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP

Banco de Portugal. (n.d. a). Missão e funções – Supervisão prudencial. Retrieved July 24, 2019, from https://www.bportugal.pt/page/missao-e-funcoes?mlid=808

Banco de Portugal. (n.d. b). Missão e funções – Supervisão comportamental. Retrieved July 24, 2019, from https://www.bportugal.pt/page/missao-e-funcoes?mlid=808

Banco de Portugal. 2018. Aviso do Banco de Portugal n.º 2/2018. Retrieved August 10, 2019, from https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/329407737_5.docx.pdf

Banco de Portugal. 2019. Instrução n.º 5/2019. Retrieved October 28, 2019, from https://www.bportugal.pt/sites/default/files/anexos/instrucoes/348104873_1.docx.pdf

Basel Committee on Banking Supervision. 2001. Customer due diligence for banks. Retrieved September 20, 2019, from https://www.bis.org/publ/bcbs85.pdf

Benos E., Garratt R. & Gurrola-Perez P. 2017. ***The economics of distributed ledger technology for securities settlement***. Staff Working Paper no. 670, Bank of England. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement

Blockchain Technologies. 2016, a. Blockchain Applications in Financial Services. Retrieved September 2, 2019, from https://www.blockchaintechnologies.com/applications/financial-services/

Blockchain Technologies. 2016, b. The Ultimate Guide to Understanding Blockchain Technology. Retrieved August 26, 2019, from https://www.blockchaintechnologies.com/blockchain-technology/

Blockchain Technologies. 2016, c. The Ultimate Guide to Understanding Blockchain Applications. Retrieved September 2, 2019, from https://www.blockchaintechnologies.com/applications/

Bonneau J., Miller A., Clark J., Narayanan A., Kroll J. A. & Felten E. W. 2015. ***SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies***. Paper presented at the 2015 IEEE Symposium on Security and Privacy, 104–121. Retrieved from https://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf

Buterin V. 2015. On Public and Private Blockchains. Retrieved August 28, 2019 from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, (n.d.). Financiamento do Terrorismo. Retrivied July 20, 2019, from http://www.portalbcft.pt/pt-pt/content/financiamento-do-terrorismo

Comissão de Coordenação de Políticas de Prevenção e Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, (n.d.). Relações de correspondência. Retrieved August 14, 2019, from http://www.portalbcft.pt/pt-pt/content/outros-conceitos

Comissão do Mercado de Valores Mobiliários. (n.d.). Apresentação – O que é a CMVM? Retrieved July 24, 2019, from https://www.cmvm.pt/pt/CMVM/Apresentacao/Pages/Apresentacao-o-que-e-a-CMVM.aspx

Davidson S., Filippi P. & Potts J. 2018. Blockchains and the economic institutions of capitalism. ***Journal of Institutional Economics, Cambridge University Press (CUP)***, 14 (4): 5. Retrieved from https://hal.archives-ouvertes.fr/hal-01850927/document

Deloitte. 2019. ***Deloitte 2019 Global Blockchain Survey***. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

Demetis, D. S., 2017. Fighting money laundering with technology: a case study of Bank X in the UK. ***Elsevier***, December 2017: 96-98. Retrieved from https://paperdownload.me/wp-content/uploads/2018/01/7403-fighting-money-laundering-technology-bank-uk.pdf

Diário da República Eletrónico. 2017. Lei n.º 83/2017. Retrieved August 10, 2019, from https://dre.pt/home/-/dre/108021178/details/maximized

Dudovskiy J. 2017. IKEA McKinsey 7-S Model. Retrieved October 6, 2019, from https://research-methodology.net/ikea-mckinsey-7s-model/

European Banking Authority. EBA at a glance. Retrieved July 20, 2019, from https://eba.europa.eu/about-us/eba-at-a-glance

European Commission. 2018. Anti-money laundering and counter terrorist financing. Retrieved October 28, 2019, from https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en

European Parliament Research Service. 2019. ***Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection***

law? Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Financial Action Task Force. 2012-2019. ***International standards on combating money laundering and the financing of terrorism & proliferation***. Paris, France: FATF. Retrieved from www.fatf-gafi.org/recommendations.html

Financial Action Task Force. How is money laundered? Retrieved July 18, 2019, from https://www.fatf-gafi.org/faq/moneylaundering/

Fronda A. 2019. The future of clearing and settlement. Retrieved September 14, 2019, from https://www.theglobaltreasurer.com/2019/02/15/the-future-of-clearing-and-settlement/

Guegan D. 2017. ***Public blockchain versus private blockchain***. Working paper no. ANR-10-LABEX-0095, University Paris 1 Panthéon-Sorbonne, and labEx ReF. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01524440/document

Higginson M., Hilal A. & Yugac E. 2019. Blockchain and retail banking: Making the connection. Retrieved September 14, 2019, from https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection

Iansiti M. & Lakhani K. R. 2017. The truth about blockchain. ***Harvard Business Review***, January–February 2017 issue: 118–127. Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain

IBM. 2018. ***Transform cross-border payments with IBM Blockchain World Wire***. Retrieved from https://www.ibm.com/blockchain/solutions/world-wire

Inspeção Geral das Finanças. (n.d.). A IGF. Retrieved July 24, 2019, from https://www.igf.gov.pt/institucional1/apresentacao111/a-igf.aspx

Instituto dos Registos e do Notariado. (n.d.). Quem somos. Retrieved August 12, 2019, from https://irn.justica.gov.pt/Sobre-o-IRN/Quem-somos

Jalagat, R. 2016. Job Performance, Job Satisfaction and Motivation: A Critical Review of Their Relationship. ***International Journal of Management and Economics***, 5(6): 36-43. Retrieved from https://www.researchgate.net/publication/310498763_Job_Performance_Job_Satisfaction_and_Motivation_A_Critical_Review_of_Their_Relationship/link/5830553508ae004f74c0d709/download

Kotter J.P. & Schlesinger L.A. 2008. Choosing strategies for change. Harvard Business Review, July–August 2008 issue. Retrieved from https://hbr.org/2008/07/choosing-strategies-for-change

KPMG, 2018. ***Realizing Blockchain's potential – Introducing KPMG blockchain technology risk assessment solution***. Retrieved from

https://home.kpmg/content/dam/kpmg/co/pdf/2018/09/kpmg-realizing-blockchains-potential.pdf

Magnr. 2016. Centralized vs Decentralized Banking. Retrieved September 10, 2019, from https://medium.com/@Magnr/centralized-vs-decentralized-banking-5c2a657e94b7

Malone D. & O'Dwyer K.J. (2014). ***Bitcoin mining and its energy footprint***. Paper presented at the 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014). Retrieved from file:///C:/Users/Sofia/Downloads/DM-Bitcoin.pdf

Marr B. 2017. ***Data Strategy – How to profit from a world of Big Data, analytics and the Internet of Things***. FGreat Britain and United States: Kogan Page Limited.

Miles C. 2017. Blockchain security: What keeps your transaction data safe? Retrieved September 10, 2019, from https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

Ministério Público Portugal. (n.d.). Departamento Central de Investigação e Ação Penal – Quem somos. Retrieved July 24, 2019, from http://dciap.ministeriopublico.pt/pagina/quem-somos-33

Mohanty R. Sarangi N., and Bishi S. (2010). ***A secured cryptographic hashing algorithm***. Working paper, Veer Surendra Sai University of Technology, Burla, Orissa, India. Retrieved from file:///C:/Users/Sofia/Downloads/A_secured_Cryptographic_Hashing_Algorithm%20(1).pdf

Nakamoto S. (n.d.). Bitcoin: a peer-to-peer electronic cash system. Retrieved August 26, 2019, from https://bitcoin.org/bitcoin.pdf

O'Connell B. 2019. What Is Money Laundering and What Is Its History? Retrieved October 28, 2019, from https://www.thestreet.com/personal-finance/education/what-is-money-laundering-14897715

Official Journal of the European Union. 2015. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015. Retrieved July 24, 2019, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

Official Journal of the European Union. 2016, a. Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016. Retrieved September 20, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1675&from=EN

Official Journal of the European Union. 2016, b. Council directive (EU) 2016/2258 of 6 December 2016. Retrieved July 24, 2019, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2258&from=en

Official Journal of the European Union. 2016, c. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Retrieved September 20, 2019 from

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Official Journal of the European Union. 2018. Commission Delegated Regulation (EU) 2018/105 of 27 October 2017. Retrieved September 22, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0105&from=EN

Orcutt M. 2019. Once hailed as unhackable, blockchains are now getting hacked. ***MIT Technology Review***. Retrieved from https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Peters T. J. & Waterman Jr. R. H. 1982. ***In Search of Excellence***. New York, Harper & Row.

POA Network. 2017. Proof of Authority: consensus model with Identity at Stake. Retrieved August 28, 2019, from https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

Polícia Judiciária. (n.d.). Unidade de Informação Financeira. Retrieved July 24, 2019, from https://www.policiajudiciaria.pt/uif/

PwC. 2018. ***Global Blockchain Survey***. Retrieved from https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html

Rauchs M., Glidden A., Gordon B., Pieters G., Recanatini M., Rostand F., Vagneur K. & Zhang B. (2018). Distributed Ledger Technology Systems: A Conceptual Framework. ***SSRN Electronic Journal***, 10: 22. Retrieved from file:///C:/Users/Sofia/Downloads/2018-08-20-conceptualising-dlt-systems%20(1).pdf

Registo Central do Beneficiário Efetivo. (n.d.). Retrieved August 12, 2019, from https://rcbe.justica.gov.pt/

Rodgers D. 2019. A Primer About Clearing and Settlements. Retrieved September 14, 2019, from https://www.thebalance.com/a-primer-about-clearing-and-settlements-1290415

Santander. 2018. ***Santander launches the first blockchain-based international money transfer service across four countries***. Retrieved from https://www.santander.com/csgs/Satellite/CFWCSancomQP01/en_GB/Corporate/Press-room/Santander-News/2018/04/12/Santander-launches-the-first-blockchain-based-international-money-transfer-service-across-four-countries-.html

Schott, P. A. 2006. Money laundering and terrorist financing: definitions and explanations. In The International Bank for Reconstruction and Development/The World Bank/ The International Monetary Fund (Eds.), ***Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: Second Edition and Supplement on Special Recommendation IX***: 1-3. Washington, DC: World Bank.

Sultan K., Ruhi U. & Lakhani R. (2018). ***Conceptualizing blockchains: characteristics & applications***. Paper presented on the 11th IADIS International Conference Information Systems 2018. Retrieved from https://arxiv.org/ftp/arxiv/papers/1806/1806.03693.pdf

Tasca, P., Tessone, C. (2019). A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. ***Ledger***, 140. Retrieved from http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/140

Walport M. 2015. ***Distributed Ledger Technology: beyond blockchain.*** A report by the UK Government Chief Scientific Adviser. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Watts S., Shankaranarayanan G. & Even A. 2009. Data quality assessment in context: A cognitive perspective. ***Elsevier***, 48(1): 202-2011. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167923609001766?via%3Dihub

6. Appendix

Appendix 1: Summary table of the AML/CFT Preventive Duties

Duty	Definition	How can financial institutions comply with the duty?
Duty of Control	Defining and ensuring internal policies and procedures adequate to the fulfillment of all the preventive duties.	• Strong and adequate internal control system; • Independent, permanent and effective compliance function; • Conducting periodic effectiveness tests.
Duty of identification and diligence	**Identification** Identifying customers and the corresponding beneficial owners, if applicable.	**Identification** • Complete KYC process; • Keeping an updated and computerized record containing personal client data as well as the history of all transactions performed; • The record must be available to the entire organization, and any agents, distributors or other third parties responsible for carrying out operational functions.
	Diligence Gathering information about the purpose and intended nature of the business relationship as well as the origin and destination of the funds at hand.	**Diligence** • Defining adequate standard, simplified and enhanced due diligence measures; • Solid risk assessment so that each client is placed in the right ML/FT risk category; • Guaranteeing that the monitoring of the business relationship, the frequency of the KYC and CDD information updates, the collection of additional information considered relevant and the application of measures deemed appropriate are in line with the ML/FT risk profile of the client.
Duty of communication	The Compliance function must report any operation	• The communication of the suspicious incident shall be made as soon as possible, and it must include a

	that appears to be related with ML/FT crimes to *DCIAP* and *UIF*.	description of the factors that contributed to the transaction being considered ML/FT related, all the evidences portraying the operation at hand as well proof of the analysis conducted; • The identity of the employee(s) who detected and reported the suspicious occurrence must be kept anonymous; • Ideally, the flow of information shall be simple and agile.
Duty of abstention	Abstaining from performing suspicious operations.	• The duty of abstention implies the fulfillment of the duty of communication – every time a financial entity decides not following through with an operation, *DCIAP* and *UIF* must be immediately informed.
Duty of refusal	Refusing the establishment of a business relationship, occasional transaction or single operation, in case the client does not provide the required information and documents.	• Whenever a client does not provide the required documents or information, the consequences can range from not starting or terminating the business relationship, refusing to perform the occasional transaction or conduct a specific operation or set of operations; • If the business relationship is ceased, all movements of funds or other assets associated with the business relationship shall be put on hold. • Once again, if justifiable, the event must be reported to the competent authorities.
Duty of conservation	Every document, whether it is an original or a copy, every piece of information or data collected from the client for KYC and CDD purposes, every element or analysis regarding	• Internal systems must provide enough storage capacity to keep the referred data available and in proper conditions; • The main goal of the duty of conservation is the possibility to reconstruct any operation that took place in that timeline.

	operations, every account file, must be kept in a durable support, preferably by means of an electronic support, for a period of seven years after the execution of the operations or the end of the business relationship.	
Duty of examination	Events posing a higher risk of being ML/FT related, must be carefully analyzed.	• In case the outcome of the examination leads to the conclusion that the event is indeed suspicious, it must be communicated to the competent authorities.
Duty of collaboration	Cooperation with *DCIAP*, *UIF*, other judicial, sectorial and police authorities and *Autoridade Tributária e Aduaneira*.	• Ensuring immediate and direct access to the information and documents or records requested by the competent authorities.
Duty of non-disclosure	Non-disclosure to the client or third parties of any information regarding communications made to the competent authorities. The procedures performed to comply with the duties of communication, abstention and collaboration do not constitute a breach of the duty of non-disclosure.	Exceptions include: • Judicial, sectorial and police authorities and *Autoridade Tributária e Aduaneira*; • Financial entities and other entities of equivalent nature located in an EU Member State (regardless of the existence of a group relationship); • Institutions that are part of the same group and are located in EU Member States or in equivalent third countries; • Entities of a similar nature established in an EU Member State or in an equivalent third country, with whom the financial institution has a client or operation in common;

		• Auditors, certified accountants, tax consultants, lawyers, solicitors, notaries and other independent legal professionals, constituted in a company or in individual practice, if established in an EU Member State or in an equivalent third country.
Duty of training	Training of managers and employees with relevant functions in AML/CFT.	• Definition of a training program • Its implementation and the evaluation of its effectiveness shall have the direct participation of top management and the director of the Compliance function.