

# **Anti-Money Laundering and Counter-Terrorism Financing methodology for cryptocurrency exchanges in the European Union**

Master's Thesis project for MSc in Business Administration and Information Systems program

Anrijs Valts Bebris  
anbe15ah@student.cbs.dk

Supervisor:  
Raghava Rao Mukkamala  
rrm.digi@cbs.dk

Date of submission: 15.05.2018

Number of characters (incl. spaces): 213 282

Number of pages: 80

Copenhagen, 2018

# Table of contents

Abstract .....	3
Acknowledgment .....	4
1. Introduction .....	4
1.1. Research topic and relevance .....	5
2. Research methods .....	6
2.1. Literature review .....	6
2.2. Participant observation.....	7
2.3. Interviews.....	8
2.4. Collaboration.....	8
3. Cryptocurrency.....	9
3.1. Bitcoin.....	11
3.1.1. Blockchain .....	13
3.1.2. Mining.....	15
3.1.3. Transactions .....	16
3.2. Other cryptocurrencies .....	18
3.2.1. Ethereum .....	18
3.2.2. Ripple (XRP).....	20
3.3. Summary .....	22
4. Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) .....	23
4.1. Money laundering .....	23
4.2. Terrorist financing.....	24
4.3. Directives and organizations in the European Union.....	25
4.3.1. The 4 <sup>th</sup> AML Directive.....	25
4.3.2. The 5 <sup>th</sup> AML Directive.....	26

4.3.3. Organizations .....	27
4.4. AML/CTF measures .....	29
4.4.1. Risk assessments and Risk-Based Approach (RBA) .....	29
4.4.2. Know Your Customer (KYC) .....	37
4.4.3. Policies and procedures.....	43
5. Cryptocurrency exchanges .....	47
5.1. Market landscape of cryptocurrency exchanges .....	49
5.2. Customer data that already is being collected by cryptocurrency exchanges .....	50
6. AML/CTF measures in cryptocurrency exchanges .....	56
6.1. Enterprise-wide ML/TF risk assessment of a financial institution .....	57
6.2. Customer ML/TF risk assessment.....	61
6.3. Customer due diligence (CDD).....	64
6.4. Transaction monitoring (TM) .....	67
6.5. Sanctions screening.....	70
6.6. Governance .....	71
6.7. Reporting.....	73
6.8. Administration of data and information.....	73
6.9. Training.....	74
6.10. Research framework .....	75
7. Discussion .....	78
8. Conclusion .....	79
9. Reflections and limitations.....	80
10. References .....	81
11. Appendix.....	87

## Abstract

In the light of rising popularity of the cryptocurrency, an increasing amount of revolutionary applications to the technology are being invented. However, in addition to all of the beneficial applications to the cryptocurrency, the technology has brought some unintended consequences as well – easier and safer approach for criminals to launder money and evade international sanctions. Having recognized the risks of the technology to the financial sector and the lack of regulations in the European Union concerning cryptocurrencies, an amendment to the directive “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing” has been proposed. One of the key additions of the proposed amendment is the inclusion of virtual currency, including cryptocurrency, exchange and digital wallet service providers as obliged entities under the directive. This inclusion will require all of the mentioned virtual currency service providers to design and implement some certain anti-money laundering and counter-terrorist financing (AML/CTF) measures as, for example, customer due diligence, customer money laundering and terrorist financing risk assessment, and reporting of suspicious activities. However, the directive or the amendment to the directive does not provide clear guidelines to the design and implementation of the AML/CTF measures.

This paper aims to provide suggestions for the adjustments to the AML/CTF measures that could be made in order to adapt the measures to the specific circumstances of the cryptocurrency exchanges. The paper begins with the explanation of the underlying technological and conceptual principles of the cryptocurrencies through the Bitcoin cryptocurrency platform. Next, the information that is available on the specific design and implementation principles regarding the AML/CTF measures is aggregated and all of the required AML/CTF measures are described in depth based on the information available in the regulations and official guidelines. Afterwards, the registration process for cryptocurrency exchanges is researched in order to acquire information on the current situation of the cryptocurrency exchanges. At the end, based on all of the collected and analyzed information, specific suggestions are provided regarding the adjustments to each of the AML/CTF measures that could be made in order to facilitate the unique circumstances of the cryptocurrency exchanges, while remaining compliant with the regulations. Additionally, a research framework was developed that summarizes all of the regulations, guidelines, software tools and methodologies for each of the AML/CTF measures.

# Acknowledgment

I would like to express my gratitude to the people that supported this research. Especially I would like to emphasize the help I received from my supervisor, Raghava Rao Mukkamala. He helped me throughout the whole writing process by holding weekly meetings and providing me with valuable insights, while ensuring that the research is being done according to the planned schedule. Additionally, I would like to thank the employees of Deloitte Latvia for providing the core understanding of the AML/CTF related issues as well as verifying my understanding of the AML/CTF processes and the adjustment ideas I had regarding them. Another person that provided valuable insights for the research was the CEO of a Latvian Fintech company (it was asked not to reveal his or the company's identity); thus I would like to thank him as well. Finally, the largest support I received was from my family; thus the greatest gratitude goes to them.

## 1. Introduction

*“Asked how the blockchain industry has changed in the last few years, an animated Hartej Singh Sawhney, co-founder of the auditing and security firm Hosho, says, “If I played a drinking game, and I took a shot every time Bitcoin was mentioned on CNBC, I’d be really [drunk]””* (Nick Statt, 2018).

The popularity of cryptocurrency has experienced a significant increase over the last year, which has been reflected in the recent increase of the Bitcoin's price (John W. Schoen, 2017). However, while the cryptocurrency has been seen as a revolutionary technology that could revolutionize the financial sector and substitute the slow and expensive transactions of fiat currencies, cryptocurrency have caused some unintended consequences as, for example, enabled easier and safer way for the criminals to launder money and evade international sanctions (Joshua Fruth, 2018).

At the same time, the European Union (EU) has recognized the lack of oversight regarding the virtual currencies, including cryptocurrencies, and the risks to the financial sector that the technology poses. To mitigate the risks it has proposed an amendment to the EU directive “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing” (European Commission, 2015), which stipulates a requirement to classify virtual currency exchange and digital wallet service providers as obliged entities under the directive and thus requiring the implementation of different Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) measures. While the design and

implementation of the AML/CTF measures is required by the amendment, no detailed instructions have been provided (European Commission, 2016).

## 1.1. Research topic and relevance

Since the proposed amendment to the directive, mentioned in the previous section, has provided description of the goals that should be achieved – the implementation of different AML/CTF measures - rather than the specific steps to take in order to achieve the necessary goals, the specific approach for achieving the required goals is left for the obliged entities to design and implement. Cryptocurrency exchanges being one of the mentioned obliged entities in the proposed amendment will be required to design and implement AML/CTF measures as well. In order to succeed with the design and implementation of the required AML/CTF measures different elements will have to be considered. This paper will aim to research the requirements for AML/CTF measures stated in the EU regulations and provide suggestions for the possible adjustments of the measures for cryptocurrency exchanges. Thus the research question is as follows:

***How the different Anti-Money Laundering and Conter-Terrorist Financing measures could be adjusted to the specific circumstances of cryptocurrency exchanges, while complying with the European Union regulations?***

In order to answer the research question, first, the research methods will be described in the next chapter. Next, the foundational technological and conceptual principles of the cryptocurrency will be introduced. After explaining the underlying technological and conceptual principles of the cryptocurrency, the AML/CTF measures that are required by the EU regulations will be presented and described in depth. Afterwards, the main characteristics of the cryptocurrency exchange market landscape will be presented as well as the process of registration at several cryptocurrency exchanges will be analyzed from the customer's point-of-view. Then additional information regarding the different software tools and complementary methodologies that could be used in the cryptocurrency exchanges for the implementation of AML/CTF measures will be provided together with suggestions for AML/CTF measure adaptation for cryptocurrency exchanges. Additionally, a research framework will be developed based on the information described throughout the paper. At last, the research framework as well as all of the other suggestions will be discussed and a conclusion provided.

## 2. Research methods

In order to answer the posed research question several different methods were used for data collection as well as for the construction of suggestions regarding the implementation of AML/CTF measures in cryptocurrency exchanges. Each of the research methods will be described further in this section.

### 2.1. Literature review

As explained in the introduction, the aim of this paper is to provide suggestions of possible adjustments to the AML/CTF measures that could be made for cryptocurrency exchanges in order to comply with the EU regulations. Since one of the requirements for the suggestions is compliance with the EU regulations, a thorough research of the requirements that are stipulated by the EU regulations as well as any guidelines to the implementation of the AML/CTF measures should be conducted. Thus the literature review was chosen as the primary research method.

*“A literature review is a particular kind of library search. It summarizes the major findings of scholars and researchers who have conducted research in the area you are interested in investigating. To do a literature search, you search through the library (including databases and the Internet) for articles, research reports, journals, and books on your subject and offer a summary about what has been done in the particular area you are investigating”* (Arthur Asa Berger, 2014: 39).

First, the literature review will be used to research the requirements stipulated in the EU regulations. This will provide the necessary foundational understanding of the elements that the AML/CTF measures consists of as well as knowledge of the processes that definitely have to be included, when designing the AML/CTF program for an organization. The whole research will be primarily based on the found requirements that are stipulated in the EU regulations during the literature review of the regulations.

Second, the same method will be used to review relevant guidelines that have been developed by organizations that specialize in the field of AML/CTF. This will enable to acquire additional understanding of the AML/CTF measures and the process of designing them; thus complementing the stipulated requirements in the regulations.

Third, the literature review will be used to collect additional information on the different software tools and methodologies that could be used specifically in cryptocurrency exchanges in order to ensure the compliance with the regulations as well as to improve the effectiveness of the AML/CTF measures in the cryptocurrency exchanges. The findings from the literature review of the research work done by other

authors will enable to complement the suggestions of possible adjustments of the AML/CTF measures for cryptocurrency exchanges with additional methods and software tools that could significantly improve the effectiveness of the implemented measures.

Lastly, the approach of reviewing papers that have been written by other authors will be used to research the underlying technological and conceptual principles of cryptocurrencies as well as to provide overview of the different differentiations cryptocurrencies can have. Thus ensuring increased understanding of not only AML/CTF related issues, but also the issues regarding the different cryptocurrencies. This understanding of the technological working principles of cryptocurrencies will arguably increase the quality of suggested adjustments to the AML/CTF measures for cryptocurrency exchanges.

The use of papers that have been written by other researchers or authors to conclude something about a research topic or to argue for something is called a secondary research. *“In essence, this kind of research is a form of editing, in which quotations (and sometimes summaries, paraphrases, and synthesis of the material read) from this scholar and that scholar are collected to produce an essay or article that makes its argument”* (Arthur Asa Berger, 2014: 39).

## 2.2. Participant observation

In addition to the information that could be collected through the literature review an understanding of the internal processes of the cryptocurrency exchanges would be required in order to provide valuable suggestions to the adjustments of the AML/CTF measures for the cryptocurrency exchanges. However, due to not having access to the internal processes of cryptocurrency exchanges or the employees of any of the exchanges, as the second best option a research of the processes of cryptocurrency exchanges from the customer’s point-of-view was chosen.

In order to research the cryptocurrency exchanges for the point-of-view of customer, a research method called participant observation was employed. The method has been defined as follows:

*[I]t is a qualitative research technique that provides the opportunity to study people in real-life situations. It is a form of field research in which observations are carried out in real settings and where there is a lack of the kind of control and structure you have in experiments, for example. In participant observation, as the name suggests, researchers become involved in the group, organization, or entity they are studying”* (Arthur Asa Berger, 2014: 216).



In the case of this paper, instead of being involved in the company, the researcher will be involved in the process of opening an account in cryptocurrency exchanges. And instead of studying people, the registration process and the required information to open an account will be studied. This approach will provide an opportunity to complement the theoretical information gathered through literature review with a view on the actual situation in the cryptocurrency exchanges.

### 2.3. Interviews

While through the method of participant observation a point-of-view of the researcher on the customer data collection in the cryptocurrency exchanges will be acquired, it could be argued that it would be beneficial to complement this information with additional views. Thus another research method – interviews - was employed.

*“[Interviews] enable researchers to obtain information they cannot gain by observation alone. Perhaps the simplest way to describe an interview is a conversation between a researcher (someone who wishes to gain information about a subject) and an informant (someone who presumably has information of interest on the subject)”* (Arthur Asa Berger, 2014: 159).

There are types of interviews that are used for research – informal interviews, unstructured interviews, semistructured interviews, and focus groups (Arthur Asa Berger, 2014). In order to provide a structure for the interviews and at the same time provide an opportunity for the conversation to lead the way of the interview; thus possibly leading to even more valuable information compared to what was initially supposed, a semistructured type of interview was chosen. Semistructured interview has been defined as a type of interview when *“the interviewer usually has a written list of questions to ask the informant but tries, to the extent possible, to maintain the casual quality found in unstructured interviews”* (Arthur Asa Berger, 2014: 160).

### 2.4. Collaboration

Besides all of the mentioned research methods that are going to be employed for the research, a collaboration between the researcher and the employees of Deloitte Latvia will be maintained as well. The collaboration with the employees of Deloitte Latvia primarily will be employed to gain additional knowledge regarding the issues related to the field of AML/CTF as well as to verify the understanding of the AML/CTF processes. Deloitte Latvia can be viewed as a great partner due to having extensive expertise in the field of AML/CTF. This expertise already have proved to be valuable in the past, since

the research have had previous collaboration with the company, which equipped the researcher with a foundational knowledge and understanding of the AML/CTF processes and measures. Additionally, Deloitte Latvia will provide informal guidance in form of verifying the ideas made by the researcher. However, none of the interactions with the Deloitte Latvia will be recorded, since mainly the collaboration will be used for verification purposes as well as the collaboration will be executed through informal communication with the employees of the company.

### 3. Cryptocurrency

The digitization of assets that were previously available in physical form (e.g. books, magazines, notes) has enabled development of electronic money and digital (virtual) currencies. According to the European Banking Authority (EBA) virtual currencies can be defined as *“a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically”* (European Banking Authority, 2014: 11). In contrast, electronic money *“means electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer”* (European Banking Authority, 2014: 11). Thus the main difference between the virtual currency and electronic money according to the EBA is that virtual currency is not attached to any fiat currency – the value is not fixed to the fiat currency. The value of the virtual currency is based solely on the trust by the currency users that it has some value (European Banking Authority, 2014). Electronic money is not going to be further discussed in this paper.

Virtual currency can differ from other virtual currencies in certain different ways. Some virtual currencies in addition to the digital representation of value can have physical representation as well in form of printouts, engagements in some object or other physical forms. The physical representation does not change that the currency primarily exists in the digital environment. It only enables additional ways of transferring the value from one individual to another (European Banking Authority, 2014).

Next, virtual currencies can be designed to be used among limited number of individuals on private networks or open for the whole public. For example, companies can develop their own internal virtual currency that could be used for purchases of internal services or internal transfers of value. In contrast,

publicly available virtual currencies can act similarly to fiat currencies and allow to pay for products and services in stores or transfer money from one person to another, if such actions are accepted by the public. In addition, a publicly available virtual currency could be converted to fiat currencies in currency exchanges, if the exchanges accept the virtual currency (European Banking Authority, 2014).

Virtual currencies can be either centralized or decentralized (European Banking Authority, 2014). Centralized virtual currencies have some central body that manages the issuance of the currency, currency transfers and other parts of the virtual currency. Thus there is always a single point of passage that has to be passed in order to transfer the money or interact with the virtual currency in any other way. In contrast, decentralized virtual currencies have no central body or mandatory point of passage. The network is organized in nodes, where each of the nodes is connected to several other nodes. This enables peer-to-peer money transfers and reduces the vulnerability of the virtual currency network, since there is no center of the network or single connection that could be compromised (Satoshi Nakamoto, 2018).

As mentioned above, there are different types of virtual currencies, which can differ from each other across several different characteristics. One type of virtual currency that has become very popular in recent years – adding more than 100 000 users every day to the currency exchanges according to Joseph Young (Joseph Young, 2018) – is cryptocurrency. The main characteristic that differentiates cryptocurrencies from the other virtual currencies is the use of cryptography.

*“Cryptocurrencies are decentralized digital currencies. The decentralization is achieved by the p2p architecture. The cryptography is used for decentralized confirmation of transactions. New cryptocurrency units are usually (but not always) put into circulation as a reward for using the computer’s computing power for solving complicated mathematic problems which are used by participants on the system to confirm new transactions among participants”* (Jan Lansky, 2018: 19).

In addition to the definition, Jan Lansky in his paper “Possible State Approaches to Cryptocurrencies” has defined six characteristics that a cryptocurrency has to meet:

- “(1) The system does not require a central authority, distributed achieve consensus on its state.*
- (2) The system keeps an overview of cryptocurrency units and their ownership.*
- (3) The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.*
- (4) Ownership of cryptocurrency units can be proved exclusively cryptographically.*

*(5) The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.*

*(6) If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them” (Jan Lansky, 2018: 19).*

As explained by Satoshi Nakamoto in his paper “Bitcoin: A Peer-to-Peer Electronic Cash System” there are several technological components to the foundational design of cryptocurrencies – blockchain, cryptography, mining, “proof of work”, general ledger - that allow them to satisfy the aforementioned six characteristics of cryptocurrencies as well as achieve pseudo-anonymity (Satoshi Nakamoto, 2008). All of the main components and working principles of a cryptocurrency will be presented and explained in the next chapter. For the description of cryptocurrency main structure principles the Bitcoin will be used as an example, since it is the first cryptocurrency, has enabled other cryptocurrencies to evolve (Jan Lansky, 2018), and has the largest market cap by far compared to other cryptocurrencies (CoinMarketCap). Additionally, to present the different variations cryptocurrency can have other cryptocurrencies will be presented and their main operating principles will be explained.

### 3.1. Bitcoin

*“Bitcoin is a decentralized digital currency payment system that consists of a public transaction ledger called Blockchain. The essential feature of Bitcoin is the maintainability of the value of the currency without any organization or governmental administration in control” (Yli-Huumo J. et al., 2016: 2).*

The main principles and technologies that are the foundation of the Bitcoin were introduced in the paper “Bitcoin: A Peer-to-Peer Electronic Cash System” written by Satoshi Nakamoto (Satoshi Nakamoto, 2008). The paper introduced concepts as blockchain, proof-of-work, mining, transaction inputs and outputs, not necessarily with the exactly same names, but the same operating principles (Satoshi Nakamoto, 2008). Bitcoin was the first cryptocurrency ever made. It was launched on 3rd of January, 2009 and it was based on the principles explained in the Satoshi Nakamoto’s paper (Jan Lansky, 2018).

The operation of Bitcoin cannot be controlled by a single entity and there is no single point of failure, since it is decentralized and peer-to-peer connected – run by a large network of computers (nodes), where each of the nodes are directly connected to several other nodes in the network; thus ensuring that there will always be multiple connections to reach any of the nodes in the network. Anybody can become a

node in the Bitcoin network by simply downloading on their computers a specialized software and providing computational resources through the software (Reuben Grinberg, 2011)

Each node in the network is participating in maintenance of the general ledger – a complete list of all of the transactions ever made. The ledger is publicly available and can be viewed by anybody. However, to maintain some degree of anonymity, the only information that can be seen in the ledger regarding the transactions are the public keys (a seemingly random string of numbers and letters) of both counterparties and the total amount of bitcoins transferred between the counterparties. Additionally, to ensure that nobody can change the information regarding transactions in the general ledger, the transactions in the ledger are recorded in a chain of blocks (blockchain), where each of the blocks contain a reference to the previous block in the chain; thus changing any part of the information stored (even one letter or number) in the ledger or substitution of any of the blocks with a new one would cause the blockchain to automatically discard any changes made due to mismatch of the information (will be explained in more detail in the next section) (Hari K. Ramachandran et al., 2015).

The general ledger is not stored on a centrally controlled server, but it is distributed all across the network of the Bitcoin nodes. Each node in the network stores the complete list of all of the transactions ever made. New transactions to the general ledger are added in batches of transactions in form of blocks. A new block can only be added, if a consensus among the majority of the Bitcoin nodes can be reached – majority of the nodes agree about the correctness of the transactions included in the block. The process of reviewing the information of new transactions and adding them in a block is called mining, which is going to be explained in more detail further in the paper (Hari K. Ramachandran et al., 2015).

The bitcoins can be acquired in two ways – either by exchanging other currency for them through cryptocurrency exchanges or by mining. The process of bitcoin mining not only ensures the maintenance of the general ledger, but also serves as a way for issuing and distributing the currency. The Bitcoin has been set to stop the issuance of new bitcoins after reaching 21 million bitcoins. All of the bitcoins either mined or exchanged are stored on digital wallets (Hari K. Ramachandran et al., 2015). Digital wallets can be either web-based (available online by logging in into user's account) or locally stored (a software installed on a personal computer that is not necessarily connected to the internet) (Wim Raymaekers, 2014).

In the next sections, the main elements of the Bitcoin will be explained in more detail to provide a better understanding of the technological and mathematical foundation of the cryptocurrencies.

### **3.1.1. Blockchain**

The blockchain is one of the core technologies of the Bitcoin. It has made possible the elimination of the central body that verifies and controls transactions that are made by the users. This has been achieved by the combination of the different elements of the blockchain (M. Nofer et al., 2017).

*“Blockchain is a distributed database solution that maintains a continuously growing list of data records that are confirmed by the nodes participating in it. The data is recorded in a public ledger, including information of every transaction ever completed. Blockchain is a decentralized solution which does not require any third party organization in the middle. The information about every transaction ever completed in Blockchain is shared and available to all nodes”* (Yli-Huumo J. et al., 2016: 2).

The blockchain’s name comes from the fact that it consists of blocks that are linked together in a chronological sequence. Each of the blocks consist of several elements (see Appendix 1). First, it contains the reference to the previous block – a hash value of it. *“A hash algorithm turns an arbitrarily-large amount of data into a fixed-length hash. The same hash will always result from the same data, but modifying the data by even one bit will completely change the hash”* (Bitcoinwiki Hash: 1). Having included the hash value of the previous block it creates a linkage to the block. This method makes it almost impossible to alter the information in the blocks, since even a small change in the block would result in a completely different hash value and would break the chain of the next blocks in the blockchain (M. Nofer et al., 2017). In addition, the information of a block in a blockchain includes a merkle root, which is a hash value of all of the previous blocks in the blockchain; thus providing additional security (Bela Gipp et al., 2015).

Second, a block in a blockchain contains transactions and information regarding them – who is sending bitcoins to whom and how many bitcoins. Even though all of the transactions are publicly available on the general ledger, the counterparties are only represented by a seemingly random sequence of numbers and letters (the public key); thus breaking the flow of information and making the transactions anonymous (Satoshi Nakamoto, 2018). The transactions in a block are not added automatically one by one, but are compiled by the participants in the bitcoin network through process of mining, which is

going to be explained in more detail in the next chapter. The mining process ensures that all of the transactions in the block have been verified and are authentic (M. Nofer et al., 2017).

Third, the block contains different administrative information – timestamp and software version. In the timestamp field the time, when the particular block was created, is recorded. Next, the software version field presents the version title of the software that was used for the creation of the block; thus making it possible for the peer-to-peer network to make sure that no altered versions of the software, which could enable some fraudulent activity, were used for the block creation. Both of the administrative information elements are used in the hash function, when the hash value of the block is created; thus making these two pieces of information unalterable as well (Bitcoinwiki Block hashing algorithm).

At last, in addition to all other information that the blocks contain, a nonce. Nonce is a random number, which is combined with the hash value of the previous block, the hash value of the merkle root, and a timestamp to form a hash value of the block. Nonce is changed in order to change the hash value of the block and achieve the required hash value of the block (see more in chapter about mining) (Ghassan O. Karame et al., 2012).

The combination of the blocks in blockchain forms a list of all of the transactions ever made by every user of Bitcoin – ledger. The ledger is not stored in one particular place or computer, but its exact copies are stored on computers of the users of Bitcoin; therefore it is called distributed ledger. Having the copies of the ledger stored on many computers in different places ensures that the information of it cannot be easily changed and used for fraudulent activities, because the information then would have to be changed in all of the distributed ledgers and, if not, the changed ledger would simply be rejected by the network of the Bitcoin users as invalid and unusable for the validation of any further transactions. Additionally, if any of the ledger holders disconnect from the network, there are plenty of other ledger holders that can continue validating transactions and recording them in the ledger (M. Nofer et al., 2017).

The operation of the blockchain in Bitcoin is deeply integrated with the process called mining, which is going to be explained in the next chapter.

### **3.1.2. Mining**

*“Mining is the integral process wherein generation, transmission and validation of transactions of cryptocurrencies is done. It ensures stable, secure and safe propagation of the currency from the payer to payee”* (Hari K. Ramachandran et al., 2015: 1).

In addition to being a core process for transaction validation and maintenance of the general ledger (blockchain), bitcoin mining process is responsible for new bitcoin emission as well. By participating in the process of validating and maintaining the general ledger, bitcoin miners are rewarded with a completely new bitcoin in addition to the fee that is paid by the bitcoin senders. The bitcoin emission is designed to gradually decrease the amount of bitcoins issued through increased difficulty of the mining process and halving the rewarded amount of bitcoins approximately every four years. However, the emission of new bitcoins is forecasted to end around year 2040, when the total amount of bitcoins will reach 21 million, which through the technical design of Bitcoin has been set as the maximum amount of bitcoins that can exist. After the bitcoin cap will be reached, the Bitcoin miners will only be incentivized by receiving the fees from the transactions they have processed (Hari K. Ramachandran et al., 2015).

The process of mining is similar to solving a puzzle. First, the miner collects a number of the most recent transactions that have been broadcasted to all of the nodes in the network and forms a block. Next, in order for the miner to be able to add the block to the blockchain, several operations have to be performed in advance. Each of the added transactions to the block are validated through the use of the previous blocks in the blockchain – the existence of sufficient funds for the bitcoin transfer is validated by comparing the information of the origin of the funds with the information recorded in the blockchain; thus tracking the funds all the way to the initial origin of the bitcoins. When this task is completed, the transactions can be added to the block. Next, the information in the block is hashed through SHA-256 hash function. By changing a nonce number in the block a hash that satisfies a specific requirement (e.g. to have a hash function that starts with five zeros) is guessed. As mentioned before, a small change in the object of the hash function changes the hash function completely. The miner then iterates through many nonce numbers (more than 100 000 iterations) before a hash value that satisfies the requirement is found. It is argued to be impossible to just calculate what nonce number will be needed to achieve a hash value that satisfies the requirement; thus many iterations of guesses are needed (Hari K. Ramachandran et al., 2015). The achieved hash value in combination with the nonce value is used as a proof-of-work;



thus implementing a distributed timestamp of the blocks and providing additional security against double spending of the bitcoins – spending twice the same bitcoin. *“To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes”* (Satoshi Nakamoto, 2008: 3). Only when the nonce that gives the required hash value has been found, the block is ready to be added in the block chain. However, since there are many participants in the mining process, only the first miner that guesses the right nonce number can add the block to the blockchain. This ensures that all of the participants are working on the same blockchain; thus having the same information about the historical transactions available. Only when the block is actually added to the blockchain by winning the guessing competition, the miner is awarded with the completely new bitcoin and the fees from each of the transactions included in the block. The Bitcoin has been designed in a way that the requirement difficulty for guessing the hash value is adjusted dynamically in order to a block would be added in the blockchain every 10 minutes; thus ensuring a stable process of new bitcoin emission. All of the bitcoin mining steps presented in this chapter are not executed manually, but they are done by computers and a Bitcoin software (Hari K. Ramachandran et al., 2015).

### **3.1.3. Transactions**

*“We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership”* (Satoshi Nakamoto, 2008: 2).

Thus instead of actually transferring a physical or digital object from one person to another, only the ownership is transferred from one owner to the next one. The security of transactions has been ensured through asymmetric cryptography – by using pairs of public and private keys and signing each of the transactions with them (see Appendix 2).

*“Cryptography is an algorithmic process of converting a plain data to a cipher text, a form that is unreadable by an unauthorized person (eavesdropper). This technique is usually achieved with the use of an encryption key to alter the message based on the key bits resulting in a cipher text (encrypted data)”* (Adedeji Kazeem and Ponnle Akinlolu, 2016: 308).

*“[A]symmetric key cryptography technique [employs] two keys for encryption and decryption process. In this system, one key called the secret key is used for encryption while the other key called the public key is used for decryption”* (Adedeji Kazeem and Ponnle Akinlolu, 2016: 308).

Signing the transaction with the sender's secret key provides a proof of the bitcoin ownership and ensures that the bitcoin a user is receiving has definitely been sent by the user it has been signed by and no fraud can be committed, since the transaction can be verified by applying the sender's public key to the transaction and confirming that the pair of public and private keys match (Satoshi Nakamoto, 2008).

*“Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender”* (Satoshi Nakamoto, 2008: 5).

This means that for a Bitcoin user in order to transfer bitcoins (make an output) from his/her wallet to another user's wallet, previously received bitcoins (inputs) that add up to the amount of the outgoing transfer of bitcoins (output) have to be provided. Thus ensuring that no bitcoin transfer can be made, if the specific wallet has not received enough bitcoins previously or has already spent the received bitcoins. There can be two outputs, as mentioned above. First output is the actual transfer of bitcoins. The second, output is the part of bitcoins that were not used for the transfer and that are sent back to the sender (Satoshi Nakamoto, 2008). For example, if a user wants to send 10 bitcoins to another user, but the sender has previously received 2 bitcoins, 3 bitcoins and 6 bitcoins. This means that the combined amount of received bitcoins add up to 11 bitcoins and there is no way how to combine them in order to get 10 bitcoins without any change. In this case, all of the three bitcoin inputs (11 bitcoins in sum) would be used for the transfer, but 1 bitcoin would be sent back to the sender; thus there would be two outputs – 10 bitcoins as a transfer to the other user and 1 bitcoin as a change, which is sent back to the sender.

To sum up, the foundation of Bitcoin does not consist simply of one technology or one principle, but it rather consists of a combination of different technologies and principles that have been connected in order to ensure protection from different fraudulent activities or thefts as well as eliminate the need for a third person for ensuring the correctness of transactions made by users. This goal has arguably made the Bitcoin into complicated system that consists of different components, which are very intertwined with each other and thus cannot be separated. Even though the Bitcoin system seems complicated and very rigid there are many different ways how the system can be altered in order to enable additional or different functionality. There are many different cryptocurrencies that use the underlying the same principles and

technologies as the Bitcoin, but have been slightly or even greatly modified and repurposed. Two cryptocurrencies that differ from the Bitcoin will be explained in more detail in the next chapter.

## 3.2. Other cryptocurrencies

According to the “coinmarketcap.com” there are more than 1500 active cryptocurrencies available for purchase and the global market cap of the cryptocurrencies is rapidly increasing – in the beginning of 2018 reaching more 700 billion USD. Based on the market cap, the top three cryptocurrencies in descending order are Bitcoin, Ethereum and Ripple (XRP) (CoinMarketCap). Both of the top two (besides the Bitcoin) cryptocurrencies use the same underlying principles and technologies when compared to Bitcoin. However, there are some differences between them and the Bitcoin. The top cryptocurrencies will be introduced in the next sections of this chapter and the differences between them and Bitcoin briefly explained.

### 3.2.1. Ethereum

*“The intent of Ethereum is to create an alternative protocol for building decentralized applications [...] Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions”* (Vitalik Buterin, 2013: 13).

While Bitcoin was developed to solely support transfer of funds in form of cryptocurrency (bitcoin) through decentralized network of computers (nodes) and act as a substitution to the traditional FIAT currencies, Ethereum has exploited the same underlying technologies and concepts – blockchain, mining, cryptography etc. – to develop a more sophisticated and flexible platform that supports additional features beyond transactions of a virtual currency (Vitalik Buterin, 2013).

The main differentiator of Ethereum, when compared to Bitcoin, is that it can execute computer code called “smart contracts” in addition to the cryptocurrency transactions. Smart contracts are a set of rules that specify actions that are automatically executed (e.g. transfer of specific amount of funds) based on some external information or programmed algorithms. For example, two persons can set a bet on the temperature for a specific date and whoever guesses the closest gets paid automatically. These smart contracts ensure that there will be no cheating and that the winner will definitely get paid, since once the

code is uploaded it cannot be edited. This is just one use case from infinite number of possible use cases of the smart contracts (Vitalik Buterin, 2013).

Additionally, Ethereum supports development of decentralized software applications “Dapps” that can be executed on Ethereum Virtual Machine (EVM), which is Turing complete and is run on each Ethereum network node. Turing completeness means that the EVM is capable of executing many different types of functions – e.g. loops – and thus is less restricted than Bitcoin. In comparison, Bitcoin is not capable of executing loops. Dapps can be developed by anyone and passed on to the decentralized Ethereum network, where the applications are executed by the connected computers (nodes). This configuration means that there is no need for centralized server that executes the application code as in usual web based applications; thus making Dapps less susceptible to hacker attacks (Vitalik Buterin, 2013).

However, the execution of application code on Ethereum network is not for free. The use of computational power for the execution of application code has to be compensated. Ethereum has integrated their own cryptocurrency “ether” in the Ethereum network, which is used to pay for the computational power as well as a typical cryptocurrency for transfers of funds. In order to measure how expensive in terms of ether the execution of the specific application code will be, a unit called “gas” is employed in Ethereum. Before sending the application code to the Ethereum network for execution, a user has to set the limit of how much gas the user is willing to spend on this particular application code (“gasLimit”) and how much the user is willing to pay for each computational step (“gasPrice”). Each computational step uses certain amount of gas depending on the complexity and resource capacity that is needed for the execution of the step. If the execution of application reaches set gas limit before the code execution has been completed, the execution stops. The execution of application then reverts back to the initial state, but the node, which provided the computational power and resources, receives the payment for resource provision either way. This has been implemented in order to prevent malicious activities on the network and infinite loops that could crash or corrupt the computer that the application code is executed on (Gavin Wood, 2014).

Ethereum is organized in accounts. There are two types of accounts – externally owned accounts and contract accounts. While externally owned accounts does not contain any computer code to be executed and are controlled by the private key, contract accounts hold computer codes that can be executed on the Ethereum network and are only controlled by the computer code. Externally owned accounts can create

contract accounts for application code storage and execution. Accounts consist of nonce, ether balance, contract code (if present), and storage, which is empty by default. When a new block is added in blockchain, the state of each of the accounts (the state of the accounts parameters) is recorded and the application code contained in the accounts is executed. It is done by each of the nodes to ensure that each of them would get the same result as others. Thus the process of mining in Ethereum not only updates the general ledger of the state in the blockchain network, but also executes the application code (Vitalik Buterin, 2013).

As mentioned in the previous chapter, in the Bitcoin a new block is added to the blockchain on average every 10 minutes. In Ethereum the process is accelerated to adding a new block on average every 15 seconds. In addition, the issuance of ether in the Ethereum network is not limited to a specific number as Bitcoin (21 million will be issued in total, as mentioned above), but rather the rate of issuance will gradually slow down over time (Vitalik Buterin, 2013).

### **3.2.2. Ripple (XRP)**

It could be argued, that Ripple in many ways is similar to Bitcoin and in many ways the exact opposite of Bitcoin. Similarly to Bitcoin, Ripple is a decentralized platform that supports peer-to-peer transfer of funds in form of cryptocurrency (XRP), a common consensus has to be reached on the network before the transfer is accepted, it utilizes blockchain technology to ensure secure transactions between the users, and the transactions are verified by cryptographical signatures. All of the transactions on Ripple network are recorded on a publicly available general ledger that is duplicated across a network of nodes that are verifying the transactions (Frederik Armknecht et al., 2015). Besides the mentioned similarities between Bitcoin and Ripple there are many differences.

First, Ripple is not completely open platform and is centrally controlled (Jon Martindale, 2018). While on Bitcoin and Ethereum anyone can become a part of a large node network and mine the cryptocurrencies by simply downloading the necessary software; thus maintaining the blockchain and recording the transactions in the general ledger (described above), on Ripple only particular entities that have been accepted by the Ripple Labs Inc. can become “gateways” that constitute the decentralized node network and validate transactions. In order to become a gateway on the Ripple network, an entity has to comply with different rules and regulations from different regulators as, e.g. OFAC, FinCEN

(Gateway guide). On the Ripple network there is no mining like in the Bitcoin and nodes do not have to provide proof-of-work, instead each node validate the transactions themselves (Jon Martindale, 2018).

Second, while cryptocurrencies in general are thought to be usable as a substitute to a traditional state issued and controlled currency (Jan Lansky, 2018), Ripple has been characterized as a “bridge currency” (Gateway guide) and primarily is used to increase the speed and reliability for international payments that are performed through payment institutions as, e.g., banks (XRP The Digital Asset for Payments). XRP was not developed to serve as a standalone currency, but rather as a part of a larger platform – Ripple – where it provides a common and liquid way of settling balances between payment institutions (Gateway guide).

Third, due to a tight collaboration between Ripple and payment institutions Ripple network is being strongly controlled to comply with all of the payment institution requirements. The supervision of the network is ensured by the Ripple and all of the gateways of the Ripple network (Gateway guide). For example, the gateways can freeze accounts or transactions, if suspicious activity is identified (Gateway guide). On the contrary, the Bitcoin is not controlled by anybody. None of the nodes in the network can singlehandedly impact the processes on the Bitcoin network (explained above).

Forth, the Bitcoin, as described in the previous section, has been developed to gradually issue new bitcoins in the network through the process of mining until the total amount of bitcoins issued will reach 21 million. The ether issuance process on the Ethereum platform is similar to the Bitcoin’s, but it does not have an upper limit. There is no gradual XRP issuance process. All of the 100 billion XRPs were issued and distributed among the different participants of the network, when the platform was launched and around 60 billion XRPs were kept by the Ripple itself; thus the XRP can be strongly controlled by Ripple (Jon Martindale, 2018).

While Ripple’s XRP is different from the Bitcoin and Ethereum in several major ways, it is still considered a cryptocurrency (Jon Martindale, 2018). Besides being used by the financial institutions for settling balances between them, the XRPs can be bought by anybody and they are available on a number of cryptocurrency exchanges – Bitstamp, Kraken, Bitso, Coincheck etc. (How to Buy XRP).

### 3.3. Summary

As showed in the previous chapters, cryptocurrencies can differ from each other even in some major ways. In order to provide a comprehensive overview of the differences between the Bitcoin, Ethereum and Ripple the differences will be described across several different dimensions and arranged in a table (see Table 1 below).

The first dimension is the “Level of decentralization”, which refers to two characteristics – how distributed is the network and whether there is some central body that to some extent controls the cryptocurrency network. The second dimension is “Primary purpose and functionality”. This dimension briefly presents the main use cases of the particular cryptocurrencies and additional functionality in comparison to the Bitcoin. Third dimension “Issuance of the cryptocurrency” provides brief information regarding the mechanism behind the issuance of new cryptocurrency units and distributing them in the network. The last dimension “Transaction validation” mentions the validation mechanism that is used in each of the cryptocurrencies.

Dimensions	Cryptocurrency platforms		
	Bitcoin	Ethereum	Ripple
<b>Cryptocurrency</b>	<ul style="list-style-type: none"> <li>▪ bitcoin</li> </ul>	<ul style="list-style-type: none"> <li>▪ ether</li> </ul>	<ul style="list-style-type: none"> <li>▪ XRP</li> </ul>
<b>Level of decentralization</b>	<ul style="list-style-type: none"> <li>▪ Completely decentralized and distributed among large number of nodes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Completely decentralized and distributed among large number of nodes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Not fully decentralized</li> <li>▪ Distributed among nodes that have been selected by the Ripple</li> </ul>
<b>Primary purpose and functionality</b>	<ul style="list-style-type: none"> <li>▪ Transfer cryptocurrency peer-to-peer to any user of the network without third party</li> </ul>	<ul style="list-style-type: none"> <li>▪ Transfer cryptocurrency peer-to-peer to any user of the network without third party</li> <li>▪ Execute computer code (smart contracts and dapps) on the network</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ensure almost instant bank balance clearing, when international transfers are made – bridge currency</li> <li>▪ Transfer cryptocurrency peer-to-peer to any user of the network without third party</li> </ul>
<b>Issuance of the cryptocurrency</b>	<ul style="list-style-type: none"> <li>▪ Through the mining process;</li> <li>▪ Market cap – 21 million bitcoins.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Through mining process;</li> <li>▪ No market cap.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Distributed by the Ripple company itself;</li> <li>▪ No mining process – all of the 100 billion XRPs were issued when the currency was launched.</li> </ul>
<b>Transaction validation</b>	<ul style="list-style-type: none"> <li>▪ By proof-of-work</li> </ul>	<ul style="list-style-type: none"> <li>▪ By proof-of-work</li> </ul>	<ul style="list-style-type: none"> <li>▪ Each of the nodes validates the transactions themselves</li> </ul>

*Table 1 – Summary of cryptocurrencies*

As it can be seen in the Table 1, the cryptocurrencies differ from each other in some major ways across different dimensions. It can be argued that there is almost unlimited number of combinations of the cryptocurrency elements that the cryptocurrencies can adopt. Thus it is impossible to describe how all of the cryptocurrencies function in detail. However, it can be said that there are several technologies and principles that are used in most of the cryptocurrencies as, for example, blockchain, cryptography and distributed network of nodes.

## 4. Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF)

This chapter will start by defining crimes of money laundering and terrorist financing. Next, the main measures for combating the money laundering and terrorist financing in the European Union – directives and organizations – will be briefly presented. Finally, the AML/CTF measures that the financial institutions, which are located in the European Union, are required to develop and implement will be described in depth.

### 4.1. Money laundering

The Financial Action Task Force (FATF), an inter-governmental organization that helps to set standards and develop guidelines for AML/CTF measures, has described money laundering as a three stage process of covering up the source of unlawfully acquired financial resources. According to the FATF, these resources can come from many different illegal activities as, for example, organized crime, drug trafficking, bribery, computer fraud (FATF: What is Money Laundering?). The need for money laundering has been explained as follows:

*“[w]hen a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention”* (FATF: What is Money Laundering?).

In 2011, United Nations Office on Drugs and Crime (UNDOC) released research report “Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes”, where it was estimated that in 2009 there were around 1.6 trillion USD laundered globally, which is around 2.7



percent of the Global Domestic Product (GDP) and only less than 1 percent of the global flows of unlawful funds are seized or being frozen (UNDOC, 2011).

The process of money laundering starts with the placement stage, where the unlawfully acquired profits are inserted into the financial system through application of various different methods as, for example, *“by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location”* (FATF: What is Money Laundering?). In the first stage, *“the funds are usually processed relatively close to the underlying activity; often, but not in every case, in the country where the funds originate”* (FATF: What is Money Laundering?).

In the second stage – layering – the profits are converted and moved around in order to obscure actual sources of the funds. This stage again can be executed through different methods – by purchasing investment instruments and selling them, by sending the funds through series of different accounts that are located in different countries and masking the transfers as payments for products and services (FATF: What is Money Laundering?). *“With the layering phase, the launderer might choose an offshore financial centre, a large regional business centre, or a world banking centre – any location that provides an adequate financial or business infrastructure”* (FATF: What is Money Laundering?).

The main purpose of the third stage – integration – is to place the funds back into the legal economy. *“The launderer might choose to invest the funds into real estate, luxury assets, or business ventures”* (FATF: What is Money Laundering?). By investing into legitimate assets, the value can be then easily moved around in from of the legitimate assets and turned back into legitimate money without raising any suspicions to the authorities. *“[A]t the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities”* (FATF: What is Money Laundering?).

## 4.2. Terrorist financing

In the European Union directive “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing” terrorist financing has been described as *“the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the*

*knowledge that they are to be used, in full or in part, in order to carry out any of the offences”* (European Commission, 2015: 83) in connection to terrorist financing. The funds that are transferred to the terrorists or terrorist organizations not necessarily have to be acquired through illicit activities. The funds can be completely legally obtained, but the use for financing activities that are connected with terrorists and require financing make them illegal (European Commission, 2015).

*“Terrorist financing requirements fall into two general areas: (1) funding specific terrorist operations, such as direct costs associated with specific operations and (2) broader organizational costs to develop and maintain an infrastructure of organizational support and to promote the ideology of a terrorist organization”* (FATF, 2008: 7).

### 4.3. Directives and organizations in the European Union

Money laundering and terrorist financing is a real threat and can make a significant impact to the stability and reputation of the financial sector as well as to confidence in the financial system. In order to prevent the possible impact the money laundering and terrorist financing could have on the European Union’s financial sector, a directive “on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing” was developed (European Commission, 2015). The directive has also been called 4<sup>th</sup> AML Directive (4AMLD) (Deloitte, 2017), since it is the fourth directive that has been developed in order to prevent money laundering and it *“constitutes the main legal instrument in the prevention of the use of the Union’s financial system for the purposes of money laundering and terrorist financing”* (European Commission, 2016: 21).

#### 4.3.1. The 4<sup>th</sup> AML Directive

4AMLD was enacted on 25<sup>th</sup> of June, 2015 and came into force on 26<sup>th</sup> of June, 2017. It *“sets out a comprehensive framework to address the collection of money or property for terrorist purposes by requiring Member States to identify, understand and mitigate risks related to money laundering and terrorist financing”* (European Commission, 2016: 21). The main purpose of the directive is to provide consistent requirements to all member states of the European Union and thus ensure increased efficiency in prevention of money laundering and terrorist financing (European Commission, 2015). *“Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even at Union level, without taking into account international coordination and cooperation, would have very limited effect”* (European Commission, 2015: 74). The 4AMLD

stipulates a requirement for different processes and rules to be implemented by the subjects of the directive in their procedures, policies and IT systems. Subjects of the 4AMLD are credit institutions, financial institutions and various natural or legal persons providing professional services as, for example, auditors, tax consultants, external accountants, independent legal professionals, providers of gambling services (European Commission, 2015).

#### **4.3.2. The 5<sup>th</sup> AML Directive**

*“Recent terrorist attacks have brought to light emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations. Certain modern technology services are becoming more and more popular as alternative financial systems and remain outside the scope of Union legislation or benefit from exemptions that may no longer be justified. In order to keep pace with evolving trends, further measures to improve the existing preventive framework should be taken”* (European Commission, 2016: 21).

On 5<sup>th</sup> of July, 2016, European Commission proposed amendments regarding 4AMLD. This proposal has been called 5<sup>th</sup> AML Directive (5AMLD) even though it is not a completely new version of the directive, but rather an addition to already existing rules (Samantha Sheen, 2016). *“On December 20, 2017, EU ambassadors confirmed that agreement had been reached between the European Parliament and the Council regarding the latest amendments to the Anti-Money Laundering Directive (AMLD 5) proposed by the European Commission in July 2016”* (KPMG, 2017). Even though only political agreement has been reached and the proposed amendment still has to be adopted, the adoption most likely will happen, according to Nejc Novak (Nejc Novak, 2018). The most significant changes to the 4AMLD that 5AMLD introduces are that virtual currency exchange service providers between virtual currencies and fiat currencies as well as custodian wallet providers will become subjects under the directive, the virtual currency exchanges and wallet providers will have to be licensed and registered, additionally the information on company beneficiary owners will have to be publicly available in interconnected register systems, and, in case of dealing with natural persons or companies that are residents of or registered in third countries of high risk, a minimal requirements of the enhanced due diligence procedure has been provided (European Commission, 2016).

Both 4AMLD and 5AMLD have to be transposed into national law of the member states based on the requirements provided in the directives. This provides a certain adaptability to the circumstances of each

of the EU member states, while ensuring a certain level of coherence among the regulations of the member states (European Commission, 2015).

While 5AMLD provides some additional requirements, the core elements as well as the processes that have to be implemented within subjects of the directive have been left unchanged from the 4AMLD; thus in order to understand the main requirements the 4AMLD has to be reviewed. 4AMLD stipulates a requirement for several core processes that are mandatory for the subjects as, for example, money laundering and terrorist financing (ML/TF) risk assessment of the financial institution, client ML/TF risk assessment, customer due diligence (CDD), transaction monitoring, and suspicious activity reporting (SAR) to the Financial Investigation Units (FIUs) (European Commission, 2015). Each of the core measures that are required by both of the directives to be developed and implemented will be described in the next section of this chapter.

### **4.3.3. Organizations**

In addition to the 4AMLD and its amendment, 5AMLD, there are several organizations that work in the Europe Union and outside of it to advance the AML/CTF measures and provide financial institutions with recommendations and guidelines regarding the AML/CTF measures and their implementation. The organizations are the Financial Action Task Force (FATF), the Wolfsberg Group, the Basel Committee on Banking Supervision (BCBS), and the European Supervisory Authorities (ESA). All of these organizations will be briefly introduced in this section.

#### **4.3.3.1. Financial Action Task Force (FATF)**

The Financial Action Task Force has been one of the leading developers and promoters of the Anti-Money Laundering and Counter-Terrorism measures in the European Union.

*“The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system”* (FATF: Who we are).

The FATF is known for their forty recommendations described in a paper titled “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation”, where they “*set out a comprehensive and consistent framework of measures which countries should implement in order to*

*combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction” (FATF, 2018: 6). Besides the FATF forty recommendations, the organization has developed other guidelines as well on topics as, for example, Risk-Based Approach, which will be introduced further in this paper (FATF Risk-Based Approach).*

*“The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse” (FATF: Who we are).*

#### **4.3.3.2. The Wolfsberg Group**

The Wolfsberg Group is *“an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies” (The Wolfsberg Group Mission).* Contrary to other organizations, the Wolfsberg Group was established to provide an industry perspective on risk management from point-of-view of the financial institutions. Over the years the Wolfsberg Group has published a significant number of AML/CTF related papers in forms of Principles, Guidelines, Frequently Asked Questions and Statements (The Wolfsberg Group Mission).

*“The Wolfsberg Group does not advocate that FIs simply adopt each publication, but rather each FI should consider the risks described, the applicable regulatory standards and their own defined risk management strategy. The materials published by the Wolfsberg Group offer a perspective through which FIs may identify gaps or new insights and consider to what extent these gaps or insights require attention” (The Wolfsberg Group Mission).*

#### **4.3.3.3. Basel Committee on Banking Supervision (BCBS)**

The Basel Committee on Banking Supervision (BCBS) is a committee that sets global standards for banks, including in the field of AML/CTF, but has no legal force (Basel Committee Charter). *“Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability” (Basel Committee Charter).* The members of BCBS are organizations that has direct authority on bank supervision as well as central banks.

*“The BCBS expects full implementation of its standards by BCBS members and their internationally active banks. However, BCBS standards constitute minimum requirements and BCBS members may decide to go beyond them. The Committee expects standards to be incorporated into local legal*

*frameworks through each jurisdiction's rule-making process within the pre-defined time frame established by the Committee.” (Basel Committee Charter).*

#### **4.3.3.4. European Supervisory Authorities (ESA)**

The Joint Committee of European Supervisory Authorities (ESA), which consists of European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA), *“works in the areas of micro-prudential analyses of cross-sectoral developments, risks and vulnerabilities for financial stability, retail investment products, supervision of financial conglomerates, accounting and auditing, and measures combating money laundering”* (Joint Committee of European Supervisory Authorities: About Us). Additionally, *“[t]he ESAs, within the Joint Committee, jointly explore and monitor potential emerging risks for financial markets participants and the financial system as a whole”* (Joint Committee of European Supervisory Authorities: About Us). Existence of the committee ensures that the practices are coordinated and consistent across the members of the committee (Joint Committee of European Supervisory Authorities: About Us).

### **4.4. AML/CTF measures**

In this section each of the AML/CTF measures that are required according to the directives – 4AMLD and 5AMLD – will be presented and described in depth. The directives will be used as a foundation for the descriptions. However, different guidelines that have been developed by the different organizations mentioned in the previous section will be used to complement the information provided in the directives and provide additional information in terms of process steps that have to be executed in order to ensure compliance with the requirements stipulated in the directives. The descriptions of the AML/CTF measures will be divided in three groups – risk assessments, Know Your Customer (KYC), and policies and procedures.

#### **4.4.1. Risk assessments and Risk-Based Approach (RBA)**

In the 4AMLD it is stipulated that *“a holistic, risk-based approach should be used. [...]It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively”* (European Commission, 2015:76). The first recommendation of the FATF’s “International Standards on Combating Money

Laundering and the Financing of Terrorism and Proliferation” explains that the risk-based approach means that risks of money laundering and terrorist financing should be assessed and resources to mitigate the risks should be allocated in accordance to the identified risk areas – more resources to the areas with higher ML/TF risk and less resources to the areas that pose less ML/TF risk (FATF, 2018). Additionally, in the “Guidance for a Risk-Based Approach. The Banking Sector” written by the FATF it is stated that the “*RBA to AML/CFT means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively*” (FATF, 2014: 6). Thus the ML/TF risks not only has to be identified, the risks are supposed to be understood and acted upon accordingly. According to the 4AMLD, the money laundering and terrorist financing risks should be assessed on four levels – supranational (European Union), national, financial institution and client. Supranational as well as national ML/TF risk assessments are not conducted at a company level and the companies of the EU member states are not responsible for them; thus these two types of risk assessments will not be discussed any further in this paper (European Commission, 2015).

#### **4.4.1.1. Enterprise-wide ML/TF risk assessment of a financial institution (FI)**

*“Member States shall ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. Those steps shall be proportionate to the nature and size of the obliged entities”* (European Commission, 2015: 90).

While the risk factor segments – customer, geographic, product or service, transaction and delivery channel – are clearly defined in the 4AMLD, the specific approach of how the risk assessment should be conducted and what methodologies should be utilized have not been stated; thus providing a possibility for variation in approaches (European Commission, 2015).

The ESA in “The Risk Factors Guidelines” have described the ML/TF risk assessment of financial institution as follows:

*“Business-wide risk assessments should help firms understand where they are exposed to ML/TF risk and which areas of their business they should prioritise in the fight against ML/TF. [...] [F]irms should identify and assess the ML/TF risk associated with the products and services they offer, the jurisdictions they operate in, the customers they attract and the transaction or delivery channels they use to service their customers. The steps firms take to identify and assess ML/TF risk across their business must be*

*proportionate to the nature and size of each firm. Firms that do not offer complex products or services and that have limited or no international exposure may not need an overly complex or sophisticated risk assessment” (ESA, 2017: 11).*

In order to clarify various questions regarding the enterprise-wide risk assessment and the approach used to conduct it, the Wolfsberg Group in 2015 issued a paper called “Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption”. In this paper the association provided answers to various risk assessment related questions as, for example, “[w]hat is the purpose of a risk assessment?” (The Wolfsberg Group, 2015: 3), “[h]ow should a risk assessment be organised?” (The Wolfsberg Group, 2015: 4), and “[w]hat software/systems can be used to conduct a risk assessment?” (The Wolfsberg Group, 2015: 16). Additionally, the standard methodology for conducting enterprise-wide risk assessment was described (The Wolfsberg Group, 2015).

According to the Wolfsberg Group “[t]he risk assessment should cover the entirety of the FI’s business, though may be conducted in parts, or as part of a rolling cycle, to focus on separate areas, such as divisions, units or specific business lines, countries and/or legal entities” (The Wolfsberg Group, 2015: 7). The standard methodology for conducting enterprise-wide risk assessment is divided in three phases (see diagram in Appendix 3):

*“Phase 1: Determine the Inherent Risk;*

*Phase 2: Assess the Internal Control Environment (both design and operating effectiveness); and*

*Phase 3: Derive the Residual Risk” (The Wolfsberg Group, 2015: 7).*

The inherent risk can be defined as a collection of different risk factors that the company is exposed to and it can vary significantly across different companies depending on the size and other business specifics. However, the risk factor categories that should be used for the risk assessment remain the same for all of the companies (The Wolfsberg Group, 2015). The Wolfsberg Group has stated five risk categories that are slightly different from the ones stated in the 4AMLD:

*“1. Clients*

*2. Products and Services*

*3. Channels*

*4. Geographies*

*5. Other Qualitative Risk Factors” (The Wolfsberg Group, 2015: 8).*



While the listed risk factor categories should cover almost all of the possible ML/TF risk factors, the categories do not exclude considering other factors outside of the provided categories (The Wolfsberg Group, 2015). *“The categories of risk faced by an organisation can be very broad. These broad risk categories are then sub-divided into inherent risk factors that are derived from regulatory guidance or expectations as well as leading industry practices, and include a mix of both qualitative and quantitative criteria”* (The Wolfsberg Group, 2015: 8).

The risk factors in the client risk category could be, for example, the number of domestic and international clients, the number of clients that are engaged in high risk economic activity, the number of different type of clients (individuals and entities). Next, when considering the products and services the company is providing to its clients the following example of factors could be taken into account – the number of increased risk products and services the company offers, the increased risk types of transactions that have been carried out (cash transactions, transactions flagged as unusual or suspicious). There are different product or service provision channels that can increase the risk of money laundering or terrorist financing as, for example, non face-to-face business relationship establishment or third party (e.g. agent) involvement. In order to assess the geographical risk the following risk factors could be taken into account – number of clients located in high risk countries, the location of the company or business unit itself, the number of clients with their main economic activity located in high risk countries. At last, the risk category of other qualitative risk factors refers to risk factors that could not be quantified - represented by numbers. The category can contain risk factors as, for example, the stability of client base, the level of IT system integration, reliance on third party software or IT system providers (The Wolfsberg Group, 2015).

Based on the assessed factors in each of the risk factor categories a risk rating in terms of risk level (at least low, medium, and high) should be provided for each of the business units in the company and each of the risk factor categories. Additionally, there should be an option to obtain risk rating for the company as a whole, in order to gain a holistic overview of the inherent risk situation in the company (The Wolfsberg Group, 2015).

In the second phase, assessment of internal controls, the *“internal controls must be evaluated to determine how effectively they offset the overall risks. Controls are programmes, policies or activities put in place by the FI to protect against the materialisation of a ML risk, or to ensure that potential risks*

*are promptly identified*” (The Wolfsberg Group, 2015: 10). The internal controls are assessed through two dimensions – the design and operating effectiveness of controls – and most commonly across the following categories:

- “- AML Corporate Governance; Management Oversight and Accountability*
- Policies and Procedures*
- Know Your Client (“KYC”); Client Due Diligence (“CDD”); Enhanced Due Diligence (“EDD”)*
- Previous Other Risk Assessments (local and enterprise-wide)*
- Management Information/Reporting*
- Record Keeping and Retention*
- Designated AML Compliance Officer/Unit*
- Detection and SAR filing*
- Monitoring and Controls*
- Training*
- Independent Testing and Oversight (including recent Internal Audit or Other Material Findings)*
- Other Controls/Others”* (The Wolfsberg Group, 2015: 11).

Each of the specific controls can be rated with one of the three possible states – satisfactory, needs improvement or deficient. The information on the states of each of the specific controls could be collected through self-assessments conducted in each of the business units or parts of the company as well as through some other sources as, for example, audits, business risk reviews. When each of the controls have been rated, a guidance on how to improve the design or effectiveness of the control or how to sustain high effectiveness of the control should be provided. In case, if the control has not yet been implemented, an action plan of how to remedy the situation should be issued and acted upon as soon as possible (The Wolfsberg Group, 2015).

*“As with inherent risk factors above, the response to each area under examination is assigned a score, which, when aggregated, reflects the relative strength of that control. Each area can then be assigned a weighting based on the importance that the institution places on that control. For example, it may be expected that Client Due Diligence carries a larger weighting than Record Keeping and Retention within the risk assessment”* (The Wolfsberg Group, 2015: 12).

Additionally, in the enterprise-wide risk assessment there should be an option to override the acquired ratings of the inherent risk and controls effectiveness as well as in some cases even the residual risk ratings should be overridden. Any utilization of the override function should be well documented and approved by somebody with the authorization. The override function is needed due to a possibility of low quality of data that has been used for the assessment or some other instances, when additional information regarding the inherent risks and controls has been acquired and it provides a sufficient argumentation for the need of changing the ratings. A frequent use of the override function could signal for significant weaknesses in the risk assessment methodology (The Wolfsberg Group, 2015).

The third and last phase in the enterprise-wide risk assessment is calculating the residual risk. *“Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML risks within the FI are being adequately managed”* (The Wolfsberg Group, 2015: 12). For rating the residual risk of the company different scales can be used as, for example, three point scale (low, medium, high), five point scale (low, low to medium, medium, medium to high, high). There are different ways of configuring the parameters that are used to assign the residual risk based on the assessments of the inherent risk and control effectiveness. Two of the possible configurations can be seen in the Appendix 4. Results of the risk assessment should be viewable in different views and sorted in different views as, for example, the residual risk ratings should be viewable for each of the inherent risk areas, for each of the business units or parts of the company, for each of the geographies (The Wolfsberg Group, 2015).

In order to provide a higher level of adaptability for enterprise-wide risk assessment’s methodology, a weight can be assigned to each of the inherent risk and control categories based on the circumstances and environment of the financial institution. Example of the possible weighting distribution across the inherent risk and controls categories can be found in the Appendix 5. This enables the methodology to increase the importance of certain risk areas and controls for residual risk calculations and decrease for others; thus increasing the correspondence with the business model and other circumstances the financial institution experiences (The Wolfsberg Group, 2015).

*“For example, if the focus of a business division within a FI is correspondent banking and a proportion of its client base is in different international jurisdictions, geography, therefore, may be considered of higher relevance (and therefore receive higher weight) than client type for that business division.*

*Similarly, certain controls have a more direct impact on the mitigation of ML risk, such as front line controls where client due diligence is weighted more heavily than controls around independent testing” (The Wolfsberg Group, 2015: 13).*

The results of the enterprise-wide risk assessment should be used to understand the deficiencies in the overall AML/CTF program and design corresponding mitigation plan as well as accordingly to the risk areas with increased residual risk set up client transaction monitoring system and customer due diligence procedures. The enterprise-wide risk assessment should be used as the foundation to all of the other ML/TF risk mitigating measures (The Wolfsberg Group, 2015).

#### **4.4.1.2. Customer ML/TF risk assessment**

4AMLD stipulates that the obliged entities are required to assess not only the ML/TF risk of the financial institution itself, but also the ML/TF risk of customers it provides services to. The risk assessment of customers has to be performed when the client establishes a business relationship with the financial institution as well as while the client is in the business relationship with the financial institution on an ongoing basis. The customer ML/TF risk assessment provides risk level of money laundering and terrorist financing to each of the customers of the financial institution; thus enabling application of different levels of the customer due diligence measures (will be discussed further in this paper) and allocate appropriate amount of resources to each of the customers – using the RBA. However, there should be rigid and comprehensive procedures in place that describe and explain the level of customer due diligence that should be applied for each of the customer risk levels (European Commission, 2015). *“Member States shall ensure that obliged entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified” (European Commission, 2015: 92).*

While in the 4AMLD a requirement for customer ML/TF risk assessment is stated, there is no description or instruction of how it should be done, except the requirement for including in the risk assessment a number of factors that lower the risk of ML/TF (see Appendix 6) and factors that increase the risk (see Appendix 7) (European Commission, 2015). However, FATF has provided several guidelines for Risk-Based Approach application in different sectors as, for example, Money or Value Transfer Services (MVTs), banking sector, life insurance sector, legal professionals, casinos and virtual currencies. In their guidelines FATF has provided high-level recommendations on the implementation of the RBA in the

obliged entities across different sectors and what are the unique risk factors that the obliged entities are exposed to and are recommended to consider, when conducting ML/TF risk assessment (FATF Risk-Based Approach).

According to The Risk Factors Guidelines, in order to conduct customer ML/TF risk assessment, the first step is to identify the ML/TF risks and then assess each of the identified risks. The guidelines of ESA provides a non-exhaustive list of possible risk factors that the entity should consider when assessing ML/TF risks. The risk factors are divided in segments similar to the ones mentioned in the 4AMLD – customer risk factors, countries and geographical areas, products, services and transactions risk factors, and delivery channel risk factors (ESA, 2017).

Next, after the firm has identified all of the relevant risk factors across the different risk factor segments, each of the risk factors has to be assessed based on their relative importance. The importance of each of the risk factors is distributed by assigning weights to the risk factors – assigning higher numerical score to risk factors that potentially would pose higher risk to the firm and assign lower numerical score to risk factor that poses lower risk.

*“When weighting risk factors, firms should ensure that:*

- *weighting is not unduly influenced by just one factor;*
- *economic or profit considerations do not influence the risk rating;*
- *weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;*
- *the provisions of Directive (EU) 2015/849 or national legislation regarding situations that always present a high money laundering risk cannot be over-ruled by the firm’s weighting; and*
- *they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately”* (ESA, 2017: 22).

By summarizing the scores of the risk factors that have been identified for the specific customer the ML/TF risk score for the customer can be acquired. Additionally to acquiring the risk score for the customer, the risk score should be categorized. Most commonly the risk scores are categorized as high, medium or low level of ML/TF risk. However, the obliged entities can choose to categorize the ML/TF risk scores in different categories than the mentioned three (ESA, 2017).

The last step is to assign appropriate customer due diligence measures to each of the ML/TF risk level categories while taking into account other circumstances as, for example, customer type, the country of residency or registration. This allows companies to focus more resources on the riskier customers and less resources to less risky customers. The companies have to be able to clearly explain and show to the competent authorities how the different risk factors impact the level of applied customer due diligence (ESA, 2017).

#### **4.4.2. Know Your Customer (KYC)**

*“Supervisors around the world are increasingly recognising the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost”* (Basel Committee on Banking Supervision, 2001: 2).

By collecting information on the customers that are being serviced by the financial institution as well as getting to know the customer base of the organization and the specific ML/TF risks associated with it, enable companies to understand ML/TF risks associated with the customers and provide corresponding risk mitigation controls (Basel Committee on Banking Supervision, 2001). Thus *“[s]ound KYC policies and procedures are critical in protecting the safety and soundness of banks and the integrity of banking systems”* (Basel Committee on Banking Supervision, 2001: 2).

It could be argued that there are three essential KYC measures that have to be implemented into the financial institution in order to collect enough information about its customers, to be able to mitigate the risks associated with the customers and satisfy the requirements stipulated by the regulations. The three measures are customer due diligence (CDD), transaction monitoring (TM), and sanctions screening. Each of the mentioned key measures will be described in detail further in this paper.

##### **4.4.2.1. Customer due diligence (CDD)**

As mentioned before, different anti-money laundering and counter-terrorist financing measures should be designed and adjusted based on the outcomes of the four ML/TF risk assessments – supranational risk assessment, national risk assessment, enterprise-wide risk assessment and customer risk assessment. One of the measures that should be affected by the results of the risk assessments is customer due diligence – collection of information regarding the customer with an aim of identification of the individual or entity

as well as assessment of the ML/TF risk associated with the customer (European Commission, 2015). In the 4AMLD it is stipulated that “[c]ustomer due diligence measures shall comprise:

- (a) *identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;*
- (b) *identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;*
- (c) *assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;*
- (d) *conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date”* (European Commission, 2015: 92).

Even though CDD is one of the key measures that ensure effective AML/CTF program in financial institutions, it does not have to be applied to all of the transactions and customers. 4AMLD stipulates rules for when it has to be carried out (see Appendix 8). Most notably, the rules state that the CDD should always be applied when establishing a business relationship between customer and the financial institution as well as they set thresholds for the requirement to apply CDD based on the type of transaction that has been carried out. Additionally to applying CDD measures when the business relationships are being established, CDD measures have to be applied on an ongoing basis as well, especially, if some circumstances of the business relationship change (European Commission, 2015).

In addition to the standard CDD measures, there are two additional types of the CDD described in the 4AMLD – simplified customer due diligence (SCDD or SDD) and enhanced due diligence (ECDD or EDD). Each type of CDD differs from the others by the depth of the customer due diligence that has to be applied and the circumstances in which each of the types can be applied (European Commission, 2015).

According to the 4AMLD, in certain cases financial institutions are allowed to apply SCDD - customer due diligence with reduced depth – while ensuring adequate transaction and business relationship monitoring. The “Article 15” of the 4AMLD states that the SCDD can be applied only in cases, when there is a sufficient evidence of the customer or transaction having low level of ML/TF risk; thus a proper

assessment of the possible ML/TF risk has to be performed before deciding to apply SCDD (see description of the customer ML/TF risk assessment above). To provide additional information on the SCDD, the “Article 17” of 4AMLD directs to “The Risk Factors Guidelines” written by the ESA (European Commission, 2015). The guidelines of the ESA state that “*SDD is not an exemption from any of the CDD measures; however, firms may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they have identified*” (ESA, 2017: 23). There are several dimensions, which, in accordance to ESA, can be adjusted to simplify customer due diligence procedure – timing of the application of CDD measures (e.g. the CDD measures could be applied later in time during the business relationship), amount of information collected for identification, verification or transaction monitoring, quality of the information or sources the information was collected from (e.g. trusting that the customer provides correct information without verifying it), frequency of the application of CDD measures during the business relationship, and frequency and depth of transaction monitoring (e.g. instead of monitoring all of the transactions, monitor only the transactions that exceed certain thresholds) (ESA, 2017).

Next, the 4AMLD stipulates a requirement for performing the ECDD and a minimum number of measures that should be applied when performing ECDD in certain cases – when establishing correspondent relationships with a third-country institution, when providing services politically exposed persons (PEPs), when providing services to family members or close associates with politically exposed persons etc. (European Commission, 2015). 5AMLD supplements the requirements stated in the 4AMLD with additional and more precise ECDD measures that should be applied when dealing with customers coming from or related to high-risk third countries (European Commission, 2016). Similarly to the previously described SCDD, the “Article 18” from the 4AMLD directs to the ESA’s Risk Factor Guidelines for more information on the ECDD (European Commission, 2015).

*“Firms must apply EDD measures in higher risk situations to manage and mitigate those risks appropriately. EDD measures cannot be substituted for regular CDD measures but must be applied in addition to regular CDD measures”* (ESA, 2017: 25). The Risk Factor Guidelines describe the different ECDD measures that should be applied in certain higher-risk cases (the cases mentioned in the previous paragraph) as, for example, when dealing with PEPs the financial institution should determine the source of wealth and funds, and verify the information through independent and reliable information, obtain



approval from the senior management when establishing or continuing business relationship with this customer, and apply increased level of transaction monitoring (ESA, 2017).

In addition to the description of CDD, SCDD, and ECDD measures The Risk Factor Guidelines have described and listed different risk factors for each of the risk factor segments (see section above) as well as have provided a list of risk factors specific to different sectors as, for example, retail banks, wealth management, investment firms, and money remitters (ESA, 2017).

#### **4.4.2.2. Transaction monitoring (TM)**

The 4AMLD stipulates a requirement for a financial institution to monitor the customer and its transactions during the business relationship with the financial institution in order to detect unusual and suspicious transactions as well as to detect any deviations from the usual behavior of the customer and its risk profile. While the 4AMLD has mentioned the requirement for an ongoing monitoring of the customers and their transactions, it has not provided any description of how should the monitoring system be developed and implemented (European Commission, 2015).

In the guidelines titled “Sound management of risks related to money laundering and financing of terrorism” written by the BCBS is stated that the ongoing monitoring is an essential part of the ML/TF risk management. *“A bank can only effectively manage its risks if it has an understanding of the normal and reasonable banking activity of its customers that enables the bank to identify attempted and unusual transactions which fall outside the regular pattern of the banking activity”* (Basel Committee on Banking Supervision, 2016: 10). While all of the transactions and business relationships should be monitored, the extent of the monitoring and the applied measures should be determined by the risk assessments and information collected on the customer through application of the CDD measures (Basel Committee on Banking Supervision, 2016)

The main purpose of the transaction monitoring is to detect unusual and suspicious transactions or activities of a customer that do not make any economic sense. It is done through establishing scenarios that signal for possible money laundering or terrorist financing. *“In establishing scenarios for identifying such activity, a bank should consider the customer’s risk profile developed as a result of the bank’s risk assessment, information collected during its CDD efforts, and other information obtained from law enforcement and other authorities in its jurisdiction”* (Basel Committee on Banking Supervision, 2016:

10). The TM system can be set to recognize complex scenarios that pose ML/TF risk and alert employees of the financial institution regarding them or simply set to alert when limits of certain category of activity have been exceeded as, for example, exceeding transaction amount limit of the international transactions (Basel Committee on Banking Supervision, 2016).

Next, based on the scenarios the TM system should be able to filter out the suspicious or unusual transactions, which should be further analyzed by the employee of the financial institution in order to separate false positives from genuinely suspicious or unusual transactions (Basel Committee on Banking Supervision, 2016). For the analysis purposes the employees should be provided with *“all the available information on that customer relationship including transaction history, missing account opening documentation and significant changes in the customer’s behaviour or business profile and transactions made through a customer account that are unusual”* (Basel Committee on Banking Supervision, 2016: 10). After the analysis, the false positives can be discarded by providing detailed enough description of the reasons why the suspicions can be discarded, but the genuinely suspicious transactions or customers have to be reported to the local FIUs by filing a SAR (will be described in the next chapter in more details) (Basel Committee on Banking Supervision, 2016).

#### **4.4.2.3. Sanctions screening**

*“Without prejudice to the right of Member States to provide for and impose criminal sanctions, Member States shall lay down rules on administrative sanctions and measures and ensure that their competent authorities may impose such sanctions and measures with respect to breaches of the national provisions transposing this Directive, and shall ensure that they are applied”* (European Commission, 2015: 107).

Sanctions serve as an important measure for combating repeated and serious breaches of the requirements set by the 4AMLD. However, the breaches can differ in their magnitude, duration, caused losses etc. as well as the obliged entities differ from each other across various characteristics – e.g. size, nature of business – thus the range of applicable sanctions have to be sufficiently broad in order to take into account all of the differences and apply the appropriate intensity of sanctions. In addition to the legal entities, the sanctions can be imposed to natural persons and countries as well (European Commission, 2015).

One of the minimum requirements for the sanctions is *“a public statement which identifies the natural or legal person and the nature of the breach”* (European Commission, 2015: 108). At least the personal data of the responsible persons (legal or natural) together with the information on the nature and type of

the breach have to be published on the official website of the competent authority right after the sanctions have been imposed (European Commission, 2015). *“Competent authorities shall ensure that any publication in accordance with this Article shall remain on their official website for a period of five years after its publication”* (European Commission, 2015: 109).

While the 4AMLD does not explicitly state a requirement for regular screening of the obliged entity’s customer base and comparison of the customer information (including personal data and connection to countries) against the sanctions lists with a goal of possibly finding a match, it could be argued that the process of sanction screening is essential part of the AML/CTF measures. First, It has been stated in the “Annex III” of the 4AMLD that when assessing the ML/TF risk of customers a connection to *“countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations”* (European Commission, 2015: 115) should be considered as a risk increasing factor. Thus the fact there have been certain sanctions imposed on a country should be taken into account, when assessing the overall risk of a financial institution or a customer.

Second, the BCBS in the “Sound management of risks related to money laundering and financing of terrorism” under the section “Ongoing monitoring” has stated that *“The bank should screen its customer database(s) whenever there are changes to sanction lists. The bank should also screen its customer database(s) periodically to detect foreign PEPs and other higher risk accounts and subject them to enhanced due diligence”* (Basel Committee on Banking Supervision, 2016: 10). Additionally, the BCBS has mentioned sanctions as a risk increasing factor as well.

Third, the breach of sanctions in the EU is punishable with penalties and according to the “EU Best Practices for the effective implementation of restrictive measures” published by the Council of the European Union the specific penalties for the breaches of the sanctions are not set on the European Union level, but each of the EU member states have to set them individually. In addition to setting sanctions on the EU level, the member states have to be capable to set sanctions on the national level as well (Council of the European Union, 2016).

In certain cases – e.g. when the financial institution has branches in the US – the European financial institutions are obliged to comply additionally with the US sanctions regulations – Bank Secrecy Act (BSA) and Office of Foreign Assets Control (OFAC) regulations (BANK SECRECY ACT, ANTI-

MONEY LAUNDERING, AND OFFICE OF FOREIGN ASSETS CONTROL). However, US regulations are out of scope of this paper; thus will not be discussed any further.

### **4.4.3. Policies and procedures**

In addition to the risk assessments and KYC measures the financial institution has to be organized in a certain way in order to ensure effective execution of the AML/CTF measures as well as compliance to the requirements stated in the 4AML and 5AML. The 4AML stipulates that the obliged entities should develop internal policies and procedures that at least cover topics as governance, administration of data and information, reporting and employee training (European Commission, 2015). Each of the listed topics will be described in depth further in this section.

#### **4.4.3.1. Governance**

The 4AML directive stipulates a requirement for establishing certain governance measures. For example, 4AML requires that *“obliged entities identify the member of the management board who is responsible for the implementation of the laws, regulations and administrative provisions necessary to comply with this Directive”* (European Commission, 2015: 104). The “Sound management of risks related to money laundering and financing of terrorism” paper written by the BCBS mentions a three lines of defense in addition to the already mentioned identification of the responsible board member.

*“As part of the first line of defence, policies and procedures should be clearly specified in writing, and communicated to all personnel. They should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the bank in compliance with regulations. There should be internal procedures for detecting and reporting suspicious transactions”* (Basel Committee on Banking Supervision, 2016: 5).

The primary focus regarding the first line of defense is on providing a proper training to all of the new and existing employees of the financial institutions. The training programs should be tailored towards each of the specific roles and responsibilities in order to provide specific enough training and ensure adequate understanding on the execution of the policies and procedures implemented within the obliged entity (Basel Committee on Banking Supervision, 2016).

The second line of defense should be realized by appointing, in addition to the responsible board member, a chief AML/CTF officer that is going to be responsible for ensuring the compliance with all of the AML/CTF requirements. Furthermore, the officer would be the main contact person regarding all of the

AML/CTF issues internally and externally. Additionally, the duties of chief AML/CTF officer should include reporting to either the senior management or the board as well as reporting suspicious activities to the corresponding FIUs (Basel Committee on Banking Supervision, 2016).

The third line of defense is internal audit. Internal audit *“plays an important role in independently evaluating the risk management and controls, and discharges its responsibility to the audit committee of the board of directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with AML/CFT policies and procedures”* (Basel Committee on Banking Supervision, 2016: 5). During the internal audits several AML/CTF elements should be reviewed – the sufficiency of the policies and procedures of the financial institution in mitigating the identified ML/TF risks, the capability of the financial institution’s employees to implement the policies and procedures, sufficiency of the quality control and overview of the AML/CTF overall measures, and the adequacy of the employee training program to each of the specific roles (Basel Committee on Banking Supervision, 2016).

#### **4.4.3.2. Reporting**

In the 4AMLD two types of reports that have to be supported by the financial institution’s internal procedures and policies have been mentioned. The first type of report should enable employees and persons in comparable position to report breaches committed within the financial institution regarding the AML/CTF measures to the respective authorities. The reporting procedure should provide an independent and anonymous mean of alerting competent authorities of possible or already performed breaches (European Commission, 2015). The reporting procedures should also ensure *“protection of personal data concerning both the person who reports the breaches and the natural person who is allegedly responsible for a breach”* (European Commission, 2015: 110).

The second type of reports that are required by the 4AMLD are Suspicious Activity Reports (SARs). SAR is a report that is used to inform FIUs of customer’s activity *“where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing”* (European Commission, 2015: 99). As mentioned before, the SARs should be filed in cases, when some suspicious activity has been identified during transaction monitoring. However, the employees should be enabled to file a SAR in other circumstances as well (European Commission, 2015). *“Information on suspicions that funds are*

*the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group, unless otherwise instructed by the FIU” (European Commission, 2015: 103).*

#### **4.4.3.3. Administration of data and information**

Throughout the 4AMLD it is stipulated that the obliged entities are required to have adequate data and information administration policies and procedures in place. The obliged entities are required to address activities as data and information sharing between the branches of the obliged entity, other obliged entities and FIUs, collection, storage, usage and retention of data and information and other activities (European Commission, 2015). These data and information related activities will be explained in more depth further in this section.

According to the 4AMLD, obliged entities are required to develop and implement policies and procedures that address data and information sharing on three levels – between the financial institution and its branches, between the financial institution and other obliged entities, and between the financial institution and FIUs. Regarding the information sharing between the financial institution and its branches the 4AMLD requires that *“obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes”* (European Commission, 2015: 103). Next, according to the 4AMLD the information regarding whether the data concerning a customer has been sent or is going to be sent to the FIU for further investigation as well as whether ML/TF analysis are being performed or are going to be performed should be shared between the obliged entities for AML/CTF purposes. Thus signaling to other obliged entities that some certain customers or transactions might be suspicious and might need an extra attention as well as enabling obliged entities to have more complete overview of the ML/TF risks their customer bases pose (European Commission, 2015). Regarding the sharing of information between the financial institutions and FIUs the 4AMLD states the following:

*“In order to be able to respond fully and rapidly to enquiries from FIUs, obliged entities need to have in place effective systems enabling them to have full and timely access through secure and confidential channels to information about business relationships that they maintain or have maintained with specified persons. In accordance with Union and national law, Member States could, for instance, consider putting in place systems of banking registries or electronic data retrieval systems which would provide FIUs with access to information on bank accounts without prejudice to judicial authorisation where applicable. Member States could also consider establishing mechanisms to ensure that competent*

*authorities have procedures in place to identify assets without prior notification to the owner”* (European Commission, 2015: 81).

*“The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of this Directive and personal data should not be further processed in a way that is incompatible with that purpose. In particular, further processing of personal data for commercial purposes should be strictly prohibited”* (European Commission, 2015: 79).

It is required that the obliged entities before establishing a business relationship with a new customer or executing an occasional transaction inform the customer about the legal obligation for the financial institution to collect and process personal data for the AML/CTF purposes. Overall the processing of personal data for the AML/CTF purposes has been considered as a matter of public interest; thus the customers should not need any additional incentives to provide the required personal information. In addition to collection of data and information directly from the customer, financial institutions should be able to collect the relevant information on the customer’s UBOs from a central register database, which has been established by the respective EU member state. The information regarding UBOs should be adequate, accurate and current (European Commission, 2015). *“Timely access to information on beneficial ownership should be ensured in ways which avoid any risk of tipping off the company concerned”* (European Commission, 2015: 76). When the 5AMLD will come into force these central register databases will have to become publicly available (European Commission, 2016), in contrast to what 4AMLD stipulates – the databases should be accessible by authorities, obliged entities and other persons or organizations, which can provide legitimate reason for a need to access the information (European Commission, 2015).

The 4AMLD stipulates that the information that has been collected through CDD measures and the data on transactions should be retained for at least five years for the purposes of prevention, detection or investigation of ML/TF related issues, while ensuring a proper level of security and access rights to the stored personal data. While the data subject should have access rights to the personal data that is being processed for the AML/CTF measures, the data subject should not have access to any information regarding SARs, where the customer’s personal data has been used, or any other AML/CTF processes in order to ensure the effectiveness of these processes and measures (European Commission, 2015).

#### 4.4.3.4. Training

In order to ensure an adequate level of understanding of the AML/CTF processes and the need for them as well as provide awareness of the compliance requirements regarding the AML/CTF and data protection to the employees of the financial institution, the 4AMLD stipulates a requirement of *“participation of their employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases”* (European Commission, 2015: 104). As mentioned before, when describing the first line of defense, the trainings should be customized to suit the needs of each of the specific roles and functions (Basel Committee on Banking Supervision, 2016).

### 5. Cryptocurrency exchanges

As mentioned in the previous chapter, in the 5AMLD the *“providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies”* (European Commission, 2016: 30) as well as the *“wallet providers offering custodial services of credentials necessary to access virtual currencies”* (European Commission, 2016: 30) have been added to the list of obliged entities; thus required to comply with the requirements stated in the 4AMLD and the amendments to the 4AMLD stipulated in the 5AMLD (the main requirements of the directives are described in the previous chapter). The cryptocurrencies, as explained in the third chapter of this paper, are a type of virtual currency; thus the cryptocurrency exchanges and custodial wallet service providers according to the 5AMLD are obliged entities as well and have to comply with all of the requirements in the same way as any other obliged entity (European Commission, 2016). While the 5AMLD proposes to make both virtual currency exchanges and custodial wallet providers as obliged entities, to narrow down the scope of this paper only the virtual currency exchanges will be further discussed in this paper, since it could be argued that the virtual currency exchanges pose higher risk for the financial sector of the EU due to the possibility to exchange funds with high degree of anonymity (virtual currency) for a fiat currency (e.g. euro) and thus enabling to execute the third stage of money laundering – integration of illicitly acquired funds back into the legal financial system. Additionally, the FATF in their guidelines titled *“Guidance For a Risk-Based Approach to Virtual Currencies”* have stated that *“AML/CFT controls should target convertible VC nodes—i.e., points of intersection that provide gateways to the regulated financial*



*system—and not seek to regulate users who obtain VC to purchase goods or services. These nodes include third-party convertible VC exchangers” (FATF, 2015: 6).*

*“Transactions with virtual currencies benefit from a higher degree of anonymity than classical financial fund transfers and therefore entail a risk that virtual currency may be used by terrorist organisations to conceal financial transfers. Possible further risks relate to the irreversibility of transactions, means of dealing with fraudulent operations, the opaque and technologically complex nature of the industry, and the lack of regulatory safeguards” (European Commission, 2016: 12).*

Since the transactions of virtual currency are not monitored by the authorities in the EU in any way, it is crucial to provide regulatory framework for the gatekeepers that enable the public to access virtual currencies – virtual currency exchanges – in order to mitigate the ML/TF risks that virtual currencies pose; thus the amendments to the 4AMLD were proposed in form of the 5AMLD. While the regulatory framework that includes virtual currency exchanges is needed, the framework should not hinder the innovation (European Commission, 2016).

*“In respect of designing providers of exchange services between virtual currencies and fiat currencies as obliged entities, the proposed amendments respect the proportionality principle. In order to allow competent authorities to monitor suspicious transactions with virtual currencies, while preserving the innovative advances offered by such currencies, it is appropriate to define as obliged entities under the 4AMLD all gatekeepers that control access to virtual currencies, in particular exchange platforms” (European Commission, 2016: 7).*

It is argued in the 5AMLD that defining virtual currency exchanges as obliged entities will not only decrease the overall ML/TF risk, but also increase the public trust in the virtual currencies and thus improve the opportunity for the virtual currency market to grow (European Commission, 2016).

However,

*“[t]he inclusion of virtual exchange platforms and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without exchange platforms or custodian wallet providers. To combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to associate virtual currency addresses to the identity of the owner of virtual currencies. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed” (European Commission, 2016: 22).*

Besides proposing that virtual currency exchanges should be defined as obliged entities, the 5AMLD additionally proposes the requirement for the virtual currency exchanges to be licensed or registered;

thus providing additional means of regulation and increasing public trust in the virtual currency exchanges (European Commission, 2016).

In order to complement the described regulatory requirements and circumstances, the current market landscape of the cryptocurrency exchanges as well as the information that is already being collected by some of the existing cryptocurrency exchanges will be described in the proceeding sections of this chapter.

## 5.1. Market landscape of cryptocurrency exchanges

*“Exchanges were one of the first services to emerge in the cryptocurrency industry: the first exchange was founded in early 2010 as a project to enable early users to trade bitcoin and thereby establish a market price. The exchange sector remains the most populated in terms of the number of active entities. One data services website alone lists daily trading volumes for 138 different cryptocurrency exchanges, which suggests that the total number of operating exchanges is likely considerably higher”* (Garrick Hileman and Michel Rauchs, 2017: 30).

In 2017, a “Global Cryptocurrency Benchmarking Study” written by Garrick Hileman and Michel Rauchs was published. The research stated that *“[t]he data demonstrate that the exchange market is dominated by a handful of exchanges that are responsible for the majority of global bitcoin trading volumes”* (Garrick Hileman and Michel Rauchs, 2017: 32). According to the CryptoCoinCharts, cryptocurrency exchanges that have the largest market shares are “Bitfinex”, “Binance”, “Coinbase GDAX”, “Kraken”, “coinone”, “HitBTC”, and “Bitstamp”. At the time of writing this paper, 5<sup>th</sup> of May 2018, there are 193 cryptocurrency exchanges listed on the CryptoCoinCharts with a total 24 hour exchange volume of 6.62 billion USD (CryptoCoinCharts). In addition to the large volumes of exchanges, the market size of cryptocurrencies is growing rapidly. *“The combined market capitalisation (i.e., market price multiplied by the number of existing currency units) of all cryptocurrencies has increased more than threefold since early 2016 and has reached \$27 billion in April 2017”* (Garrick Hileman and Michel Rauchs, 2017: 16).

It was found that almost half of the cryptocurrency exchanges support exchanging cryptocurrencies for EUR, but more than half – for USD. Additionally, 53% of the exchanges support other fiat currencies than the USD, EUR, GBP, JPY, and CNY; thus providing local currency support for different smaller markets and enabling increased accessibility to the cryptocurrency markets for the local citizens.

Furthermore, the support of more than one cryptocurrency is not that uncommon for the cryptocurrency exchanges (Garrick Hileman and Michel Rauchs, 2017).

*“While 39% of exchanges solely support bitcoin, 25% have two listed cryptocurrencies, and 36% of all entities enable trading three or more cryptocurrencies. We observe that 72% of large exchanges provide trading support for two or more cryptocurrencies, while 73% of small exchanges have only one or two cryptocurrencies listed. 6% of survey participants also provide cryptocurrency-based derivatives, and 16% are offering margin trading”* (Garrick Hileman and Michel Rauchs, 2017: 32).

Garrick Hileman and Michel Rauchs in their global study found that on average cryptocurrency exchanges employ 24 people, *“with the largest employing around 150 people”* (Garrick Hileman and Michel Rauchs, 2017: 34). The study also showed that almost half of the exchanges employ less than 11 employees; thus demonstrating that most of cryptocurrency exchanges are small companies. Additionally, the data showed that 20% cryptocurrency exchanges employ less than 5 employees, but 9% - more than 50 employees (Garrick Hileman and Michel Rauchs, 2017).

It could be argued that the cryptocurrency exchange market is significant considering the total number of active exchanges, the total 24 hour exchange volume, the total market capitalization of cryptocurrencies, the number of different fiat currencies and cryptocurrencies the exchanges support and the average number of employees employed within the exchanges; thus any regulations concerning cryptocurrency exchanges have a potential to make an impact on a significant scale. This indicates that regulations regarding cryptocurrency should be designed with caution.

As stated in the previous section of this chapter, the 5AMLD stipulates a requirement for virtual currency exchanges to comply with the regulations outlined in the 5AMLD as well as 4AMLD (European Commission, 2016). One of the requirements that the virtual currency exchanges will have to comply with is the obligation to conduct customer due diligence at the point of opening an account with the financial institution (European Commission, 2015). While at the moment there is no requirement for cryptocurrency exchanges to conduct customer due diligence, there is certain information already being collected by the exchanges, which will be described in detail in the next section.

## 5.2. Customer data that already is being collected by cryptocurrency exchanges

In order to understand what additional AML/CTF measures will have to be developed and implemented into the policies and procedures of the cryptocurrency exchanges, currently existing processes of the

exchanges should be researched. To gain an accurate overview of the current practices in the cryptocurrency exchanges one would require a full access to at least a few exchanges, their internal processes and employees. Due to lack of access to any of the cryptocurrency exchanges another approach was required.

Since almost all of the AML/CTF measures are heavily information reliant, especially information on the customers (see section 4.4.), it could be argued that it would be beneficial to identify the data that is already being collected on the customers of cryptocurrency exchanges; thus gaining an insight into the information that the exchanges already are collecting and have access to, and utilize these insights, when developing AML/CTF measures for cryptocurrency exchanges. Not having an access to any of the cryptocurrency exchanges and their internal processes restricted the research of the data that is being already collected to exploration solely from the customers' point-of-view.

The information for the research was acquired through two sources – through an interview with CEO of a company that had a recent experience with setting up corporate accounts in three cryptocurrency exchanges at the same time (see Appendix 9) and through a hands-on registration of both personal (see Appendix 10) and corporate accounts (see Appendix 11) for the three exchanges. This approach enabled to determine the information that is collected on both corporate and individual customers as well as gain additional insights regarding the registration process from the experience of the FinTech company; thus arguably acquiring an extensive overview of the information that is being processed by the cryptocurrency exchanges during the registration process. Each of the data collection approaches as well as the insights will be discussed further in this section.

First, an interview was arranged with a CEO of a Latvian FinTech company, which was possible due to some common acquaintances. However, the CEO asked to not disclose his identity as well as the name of the company due to the nature of the information provided during the interview. It was known that a few weeks earlier the FinTech company had gone through a registration processes in three cryptocurrency exchanges at the same time; thus possibly gaining an extensive experience regarding the registration process. The interview was conducted in the office of the FinTech company on the 23<sup>rd</sup> of March, 2018. In order to increase the quality of the discussion the interview was conducted in Latvian language. The interview was 1 hour long and during it some part of the registration process was showcased on the computer by the CEO. Unfortunately, no pictures could be taken due to security

concerns. However, the whole interview was recorded, transcribed and translated to English language (see Appendix 9).

During the interview it was found that the three cryptocurrency exchanges that the FinTech company were trying to register with were Bitstamp, Mistertango and Globitex. The provided reasons for the particular choice were the close proximity of the offices (Globitex - Latvia and Mistertango - Lithuania) and the previous experience (Bitstamp). It was said that the close proximity provides additional safety and convenience, since the offices could be visited at any time in case of any issues arising (Appendix 9).

In the interview the registration process was described in great detail; thus providing several insights. First, the CEO mentioned that he had noticed that the questions and process were adjusted to different types of customers, for example, financial institutions were asked different questions when compared to other types of legal entities. Since their company is a financial institution, he thinks that they had to go through more thorough process of due diligence – they had to answer to more questions and more documents had to be uploaded - when compared to other types of legal entities (Appendix 9).

Second, according to the CEO, as a convenience in the registration process was considered, if most of the questions were asked at the beginning of the process, instead of asking the questions in multiple iterations, since each iteration could take up a lot of time. This was the case with Globitex - the company only had to answer to three additional questions after filling in the initial questionnaire and providing all of the required documents. The CEO mentioned that they were forced to ask one of the exchanges to move forward them in the queue, since it was said that it could take up to three months to finish the registration in a normal case. The long waiting lists were explained with the high demand and, most probably, manual processes that had to be executed and thus took a lot of time (Appendix 9).

Third, it was argued that overall the questions that were asked were in similar amount or even more than in banks and of similar nature as well. However, this observation relates only to corporate accounts, since the registration process for personal accounts arguably was simple and straight forward. It was guessed in the interview, that the cryptocurrency exchanges have implemented a due diligence process due to having banks as partners, who are pressuring them to comply with the AML/CTF regulations as well, or due to having acquired a license for electronic money service provider (Appendix 9).

Fourth, besides the questionnaires and document uploading, the CEO had encountered other identification method in one of the exchanges – transferring money to the exchange in order to verify the identity. This verification method was deemed to be necessary due to some new SEPA standards. While this method provides a more advanced way of verifying the identity, it was mentioned that evidently the exchanges do not have a clear understanding of how to adequately organize the identification process, especially considering the new regulations that will come into force (Appendix 9).

Lastly, through the interview it was found that that the limits of the amount that the customers are allowed to exchange in the cryptocurrency exchanges could not be easily found and that it requires to exchange large amounts in order to attract attention of the cryptocurrency exchange. It was said that one of the exchanges stated that they only start asking additional questions, if the sum of the transfer exceeds 100 000 euro (Appendix 9).

In order to complement the information that was gathered in the interview, it was decided to create both personal and corporate accounts in the same three cryptocurrency exchanges – Bitstamp, Mistertango, and Globitex. While the process for personal account opening could be finished, the process for opening a corporate account could not be; thus only the initial questionnaire was assessed. The whole registration process was documented with screenshots (see Appendix 10 and Appendix 11). Additionally, the information that was asked from the customer was aggregated and divided in three sections – personal/company data, additional information and documents (see table 2).

Based on the information collected during the registration processes, it could be seen that, similarly to the observations of the CEO, the questionnaires and the documents that had to be uploaded were adjusted for different customer types – in this case individuals and legal entities. The amount of information that is being collected on the customers that are opening a corporate account is significantly larger than the amount that is being collected on the customers that are opening a personal account. This arguably corresponds to the required customer due diligence activities, including adequate identification of the customer, identification of the beneficial owner and determining the reason for creation of the account, explained previously in this paper.

Additionally, it could be argued that the information that it is being collected by the cryptocurrency exchanges on their customers could be used for customer ML/TF risk assessment as well. The information that is collected on the customers could be used to cover all of the risk factor segments

mentioned in the 4AMLD – customer risk, geographical risk, product and service risk, transaction risk and delivery channel risk (European Commission, 2015).

To sum up, based on the insights acquired from the interview and the first-hand experience with registration process, it could be argued that the cryptocurrency exchanges already have some part of the AML/CTF measures implemented, even though there is no specific regulation that requires it. The extent of the AML/CTF measures that have been implemented could not be tested due to not having an access to any of the internal process of the cryptocurrency exchanges. However, it could be argued the information that is being collected on the customers would be enough to comply with the customer due diligence requirements.

Personal Account (Appendix 10)			Corporate account (Appendix 11)			
	Bitstamp	Mistertango	Globitex	Bitstamp	Mistertango	Globitex
Personal/Company data	First Name; Last Name; E-mail; Address (Street name, Postal code, City, Country); Nationality; Birth date.	First Name; Last Name; E-mail; Phone number; Nationality; Birth date.	Given/Other name(s); Last Name; E-mail; Residence address (Street name, Postal code, City, Country); Phone number; Nationality; Birth date; Gender; Country of birth (only for Advanced and Unlimited accounts); Personal identification number (only for Advanced and Unlimited accounts); Identification number country (only for Advanced and Unlimited accounts).	First Name; Last Name; E-mail; Company name; Company number; Company website; Tax ID; Registered address (Street name, Postal code, City, Country); Office address (Street name, Postal code, City, Country).	First Name; Last Name; E-mail (natural person); Phone number; Nationality; Birth date; Company name; Company code; VAT code; Phone number; E-mail (company); Country where the company is registered; Registration address.	Given/Other name(s) of representatives; Last Name of representatives; E-mail; Position of representatives; ID number of representatives; Residential address of representatives; Representative role; Company name (incl. in original language); Legal form of entity; Registration date; Registration number; Tax residence country; Tax ID; Registered address (Street name, Postal code, City, Country); Business address (Street name, Postal code, City, Country); Business phone number; Business e-mail address.
Additional information	Whether the person is US citizen, US resident alien, or US tax person for any other reason; Current occupation; Annual income; Net worth; Source of funds; Annual deposit estimation; Annual transaction number estimation; Intended activities on the platform; Whether the person intends to cash out at Bitstamp.		Whether the person is a tax resident (only for Unlimited account); Tax residence country (only for Unlimited account); Tax ID number (only for Unlimited account); Whether the person is a beneficial owner (only for Unlimited account); Purpose of account (only for Unlimited account); Estimated annual deposit (only for Unlimited account); Occupation (only for Unlimited account); Source of wealth (only for Unlimited account); Whether the person is a PEP (only for Unlimited account).	The main purpose of the corporate account; The channels the company's customers typically use to reach the company; Whether the company is publicly listed on a recognized stock exchange; List of company shareholders (incl. the percentage of shares each holds); Detailed description of company's business activity; Whether the company is AML regulated; Source of funds; Name, address and SWIFT code of the bank that the company uses; Estimated monthly volumes, amounts (in USD and BTC) and frequency; The type of trading that will be conducted through the account of Bitstamp; Whether the company already has an account with any other bitcoin exchange.	Description of the company's business; Whether the company is planning to send or receive payments to cryptocurrency exchanges; Official public source, where information about the company can be found; Purpose of opening the account.	Purpose of account; Origin of funds; Estimated annual deposit; Description of the company's business activities; Whether the company's business requires a licence; Whether the shares of the company are listed on a stock exchange; Whether any of the representatives, UBOs or shareholders is PEP; Whether the company is a part of group of companies or a holding company; Whether the company is a financial institution.
Documents	ID document with photo; Proof of residence document (e.g. bank account statement, utility bill, tax statement, certificate of residency).	ID document with photo (passport or ID card).	ID document (only for Advanced and Unlimited accounts); Proof of funds (only for Unlimited account); Proof of residence (only for Unlimited account).	Certificate of Incorporation; Memorandum and Articles of Association; Annual return (incl. directors and beneficial owners of the last fiscal year); Resolution of the Board of Directors to open an account with Bitstamp; List of authorized persons to operate the account (if applicable); Authorization for other persons to manage your account (if applicable); Recently issued bank account statement addressed to your company name and office address; High resolution images of the international passport and proof of residency document of at least two members of the board of directors; High resolution images of the international passport and proof of residency document of all owners with a company share of 10% or higher; Membership ID (if company publicly listed); AML policy (if AML regulated).	ID document with photo (passport or ID card) for natural person; Certificate of Incorporation Articles of association (Statute); List of shareholders; Official extract from the commercial register not older than 3 months (incl. name of the company, address of the company, director of the company, shareholders of the company); AML and KYC procedure (if the company's activity is related to financial services or cryptocurrency exchange); Power of attorney document signed by the director and director's ID (if the account has not been opened by the director); Information about ultimate beneficiary owners who have more than 25 percent of shares (incl. UBO IDs).	Proof of funds; ID copies of representatives; Incorporation documents; Directors resolutions; List of company shareholders (incl. name, ID, share percentage, and address); List of UBOs (incl. name, ID, owned percentage, address).

Table 2 – Summary of the data collected by cryptocurrency exchanges



## 6. AML/CTF measures in cryptocurrency exchanges

While the requirement for development and implementation of the AML/CTF measures that were introduced in the chapter 4 of this paper is stipulated in the 4AMLD, the specific rules for development and implementation of most of the measures are not described in the regulation (European Commission, 2015). This leaves obliged entities with a lot of possible development and implementation options. Fortunately, there are different guidelines that have been developed by different organizations that specializes in the AML/CTF to support the process of development and implementation of the AML/CTF measures (see chapter 4 of this paper). As it could be observed in the chapter 4 of this paper, while the guidelines provide valuable advices, there are still many aspects of the measures that have to be adjusted to each of the specific companies and their businesses as well as to each of the business sectors.

In this section the possible adjustments to each of the introduced AML/CTF measures will be described to conform to the business circumstances and environment of the cryptocurrency exchanges, while ensuring a compliance to the 4AMLD and 5AMLD. It could be argued that there are many additional methods and ways how the effectiveness of the AML/CTF measures could be adjusted and improved. However, it is more important for obliged entities to be compliant to the regulations. Thus the suggestions for adjustments of the AML/CTF measures will be primarily based on the regulations and guidelines mentioned in the chapter 4 of this paper as well as some additional guidelines that were not included in the chapter.

Additionally, different software tools and methodologies that would support the AML/CTF measures in cryptocurrency exchanges will be introduced. As presented in the previous chapters, there are many different cryptocurrencies available. While the adjustments for the AML/CTF measures described further in this chapter should be appropriate for all of the cryptocurrency exchanges that offer exchange services between cryptocurrencies and fiat currencies regardless of the specific currencies they offer to exchange, the Bitcoin will be used as a foundation for the proposed adjustments. At last, the information provided in this paper will be aggregated and based on it a research framework will be developed and introduced in the last section of this chapter.

## 6.1. Enterprise-wide ML/TF risk assessment of a financial institution

As explained in the section 4.4.1.1. of this paper, the enterprise-wide ML/TF risk assessment of a financial institution is a crucial AML/CTF measure that helps to identify different risk areas that the company is exposed to and does not have sufficient controls for mitigation of those risk areas; thus providing a list of areas, where improvements should be made in order to improve the company's overall AML/CTF program. While it could be argued that the process phases of enterprise-wide ML/TF risk assessment – identification of inherent risk, assessment of internal controls and calculation of residual risk – as well as the risk categories of the inherent risk – clients, products and services, channels, geographies and other qualitative risks – that were introduced by the Wolfsberg Group (The Wolfsberg Group, 2015) could be left unchanged for the ML/TF risk assessment of cryptocurrency exchanges, the risk factors used for identification of inherent risk should be adjusted in accordance to the specific circumstances and distinctive risk factors that the cryptocurrency exchanges are exposed to. Examples of risk factors that could be used in addition to others to assess the ML/TF risk of a cryptocurrency exchange, in particular exchange that exchanges between bitcoins and fiat currency, will be provided further for each of the mentioned inherent risk categories.

First, *“by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity”* (FATF, 2014: 9). While, as it was observed in the previous chapter, the researched cryptocurrency exchanges already were collecting significant amount of information on their customers and thus would not have any issues in assessing the AML/CTF risks of their customer base, there might be cryptocurrency exchanges that are not collecting as much information, since it has not been required by the current EU regulations. Therefore the exchanges that are collecting less information might experience issues regarding the assessment of their customer bases due to the built-in anonymity of the cryptocurrency platforms as, for example, Bitcoin platform. In particular, it would be difficult to divide the customer base in, for example, domestic and foreign customers, types of customers (legal or individual), the business activities that the customers are engaged in, whether the customers are PEPs. However, arguably one possible solution to this issue might be the inclusion of a separate customer type – unidentifiable customers – in the risk assessment and

ensuring that this category significantly increases the ML/TF risk of the particular inherent risk category. Thus the more unidentified customers the exchange would service, the higher the inherent risk would be, and high customer risk would mean that the cryptocurrency exchange would have to increase the level of KYC measures it is performing.

Next, in order to assess the inherent risk level of the second category, products and services, each of the products and services that the cryptocurrency exchanges offer to their customers would have to be listed and a ML/TF risk level would have to be assigned to each of them, similarly to the example that the Wolfsberg Group had provided (The Wolfsberg Group, 2015) (see Appendix 12). Based on the assigned ratings to each of the products and services that the cryptocurrency exchange offer, the total inherent risk could be calculated for this risk category by summarizing the number of products and services that have been offered to the customers and have the respective ML/TF risk - low, medium or high.

Arguably the risk ratings of the same products and services could differ between different cryptocurrency exchanges due to their business models or other circumstances and thus individual assessment of the products and services that each of the cryptocurrency exchanges offer would be required. For example, it could be argued that for cryptocurrency exchanges, which in addition to exchange service offer a digital wallet services as well, transactions of cryptocurrency from one account to another account would be considered to pose low or medium ML/TF risk, if no other suspicious characteristics would be identified, since that would be one of the core services that they offer to their customers. However, for the cryptocurrency exchanges that do not offer such services transactions, where cryptocurrency is taken from an account that is owned by one person, exchanged for a fiat currency and then transferred to an account that is owned by another owner, could be argued to be a transaction of a higher risk, since it could be used for the second stage of money laundering mentioned previously in this paper.

Additionally, the fact that in different guidelines (for other sectors than cryptocurrency exchanges) some particular products and services have been considered to have a high ML/TF risk, does not mean that, when assessing the ML/TF risk of cryptocurrency exchanges, a high risk should be assigned to the same products and services. For example, while in other industries the exchanging of cryptocurrencies would be considered as a high risk service, for the cryptocurrency exchanges that is the core business activity and thus should have advanced AML/CTF measures in place for the specific service and should not be considered as a high ML/TF risk activity.

Similarly to the ML/TF risk of services and products, having some channels considered as posing a high ML/TF risk in guidelines for other sectors does not mean that they should be considered as a high risk channels, when assessing the ML/TF risk of cryptocurrency exchanges as well. For example, according to the “Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption” written by the Wolfsberg Group the provision of services to the customers through non-face-to-face channels should be considered to pose high risk (The Wolfsberg Group, 2015). This would mean that all of the services that are provided by the cryptocurrency exchanges that solely exist on the internet would have to be considered as having high inherent ML/TF risk. Additionally, these exchanges, when assessing the ML/TF risks, would have only one channel to consider. Thus it could be argued that it might be beneficial to divide the non-face-to-face channel into more detailed groups as, for example, having or not having an involvement of a third person for the service provision, dividing the non-face-to-face channels based on the technology used – telephone, e-mail, website etc. The division arguably would increase the variation in the risk assessment and thus increase the granularity of the ML/TF risk assessment results.

The assessment of geographical risks in terms of ML/TF, according to the Wolfsberg Group, is to a great extent linked to two risk factor groups – the location of the financial institution itself and its branches as well as the geographical distribution of the customer’s nationalities, residences, transaction counterparties. For the assessment purposes the number of customers that are linked in any way (residence, citizenship etc.) to high, medium, or low risk countries should be counted and summarized to acquire the ML/TF risk assessment score. Similar actions should be executed for assessing the geographical risk for the locations of the financial institution and its branches (The Wolfsberg Group, 2015). While the information for geographical risk assessment of the cryptocurrency exchanges and its branches could be collected easily (the exchanges would already possess the information), the information on the geographical distribution of the customers and their transaction counterparties would not be available for the assessment in case, if appropriate customer due diligence and transaction monitoring measures have not been implemented. Thus, similarly to customer risk category, when assessing the geographical distribution of the customer base, additional group – unidentified – could be dedicated and a high risk level assigned to it in order to arguably mitigate the lack of information a cryptocurrency exchange might have.

At last, the cryptocurrency exchanges could include other qualitative risk factors in the ML/TF risk assessment. *“Additional risk factors can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML controls. Qualitative risk factors directly or indirectly affect inherent risk factors”* (The Wolfsberg Group, 2015: 10). Some of the qualitative risk factors, according to the Wolfsberg Group, might include the following *“Client base stability, Integration of IT systems, Expected account/client growth, Expected revenue growth, Recent AML Compliance employee turnover, Reliance on third party providers”* (The Wolfsberg Group, 2015: 10). It could be argued that any of the mentioned qualitative risk factor examples could be directly implemented in the ML/TF risk assessment of a cryptocurrency exchanges, since none of them are industry-specific.

While there were different examples of possible ML/TF risk factors mentioned, it should be added that besides these examples there are a lot of other possible risk factors that could be included in the risk assessment categories. And, as mentioned previously in this paper, there are no restrictions regarding the risk categories as well – any other categories can be added, if deemed to be necessary.

It was mentioned that for the assessment of customer risk and geographical risk categories a risk factor titled “unidentifiable customers” or “unidentified”, respectively, should be introduced due to possible lack of information regarding the customer base of the cryptocurrency exchanges. While initially that should be allowed, ultimately for cryptocurrency exchanges that comply with all of the AML/CTF requirements always should be available at least this kind of information on their customers; thus there would be no need for the categories of “unidentifiable customers” and “unidentified”.

Overall, the whole process of inherent risk assessment and calculating the inherent risk level arguably should remain the same as described in the section 4.4.1.1. of this paper. Likewise, it could be argued that the second and third phases should remain the same as described in the previous chapters of this paper as well. The AML/CTF controls should be evaluated across the same categories as mentioned by the Wolfsberg Group (The Wolfsberg Group, 2015) and introduced in the section 4.4.1.1., since all of the obliged entities, according to the 4AMLD, are required to comply with the same requirements and thus develop and implement the same set of AML/CTF measures (European Commission, 2015). Additionally, it could be argued that there is no need for cryptocurrency exchanges to adjust the

methodology for the determination of the residual risk, since the methodology itself is not industry-specific.

*“Some FIs may find it useful to utilise systems or software when conducting a risk assessment. Determining the best system or software to use can be one of the more challenging aspects of conducting a risk assessment. The software employed by FIs varies widely, from customized templates built in standard spreadsheet software to sophisticated database systems built in-house or purchased from vendors. Each approach has relative strengths and weaknesses, and selecting the right tool will depend on various factors, including the size and complexity of the FI (and the corresponding complexity of the assessment itself), the number and geographic distribution of participants in the assessment process, the extent of quantitative metrics/key risk indicators underlying the assessment, the required management information regarding the results of the assessment and the level of dynamic, ongoing changes to the assessment that are anticipated”* (The Wolfsberg Group, 2015: 16).

It could be argued that based on the aforementioned factors the cryptocurrency exchanges in most of the cases should be able to conduct the enterprise-wide ML/TF risk assessment by utilization of a spreadsheet software, since, as mentioned in the previous chapter, the “Global Cryptocurrency Benchmarking Study” found that on average the cryptocurrency exchanges employed 24 employees (Garrick Hileman and Michel Rauchs, 2017), which arguably does not signal for a need of a special risk assessment software. Additionally, it could be argued that there is no need for complementary methodologies to the one already discussed in this section, since all of the required information for the risk assessment the cryptocurrency exchanges should already possess and the methodology itself is fully adaptable to suit the unique circumstances of cryptocurrency exchanges.

## 6.2. Customer ML/TF risk assessment

The quality of ML/TF risk assessment of a customer is arguably deeply linked with the quality and amount of information regarding customers that is available to the obliged entity, in this case, cryptocurrency exchange. As mentioned in the previous section, there might be occasions due to the anonymity element of cryptocurrency, when no information is available about the customer and thus the risks that the customer poses to the exchange could not be assessed. It could be argued that these customers should be assessed as having the highest level of ML/TF risk. Additionally, this arguably would be the first sign that would signal for a need of a more enhanced transaction monitoring for the particular customer. While it was mentioned in the previous chapters that for high risk customers an ECDD should be performed, for cryptocurrency exchanges there might be situations, when it is impossible to perform ECDD due to being unable to gather any information on the customer; thus the

only measure that could be performed would be transaction monitoring to determine patterns of suspicious activity, flag the respective customer as being of a high risk and report it to the authorities, if any suspicions are detected. However, it could be argued that in cases, when the cryptocurrency exchange is compliant with the EU AML/CTF regulations, a situation, when there is no information available for the assessment of the ML/TF risk of a customer, should not be possible, since significant part of the required AML/CTF measures consists of gathering information on the customers. Thus this possibility will not be further discussed.

Similarly to the enterprise-wide ML/TF risk assessment there are certain risk categories that have to be assessed in order to calculate the final customer risk score and categorize the score as being a part of some particular ML/TF risk level. However, before the ML/TF risk of all of the risk categories can be assessed, according to the ESA, the financial institution has to identify the different risk factors that would be part of each of the risk categories and assess the importance of each of the risk factors, while taking into account the specific circumstances of the financial institution. The risk factors categories that are mentioned in the “The Risk Factors Guidelines” are customer risk, geographical risk, products, services and transactions risk, and delivery channel risk (ESA, 2017). Most of the risk factors that have been mentioned in the guidelines arguably could be directly applied to the customer risk assessment in the cryptocurrency exchanges as well. However, in order to adjust the ML/TF risk assessment to cover the possible ML/TF risks in the cryptocurrency exchange sector, the exchanges could implement risk factors that are unique to their industry and thus have not been mentioned in the guidelines. Examples of the possible unique customer ML/TF risk increasing factors will be provided further.

*“The underlying protocols on which almost all decentralised VCPSS are currently based do not require or provide identification and verification of participants. Moreover, the historical transactions records generated on the blockchain by the underlying protocols are not necessarily associated with real world identity”* (FATF, 2015: 11). As mentioned previously, the cryptocurrency exchanges that comply with the AML/CTF regulations should be collecting enough information on their customers to be able to link the cryptocurrency wallet addresses with the real world identity. However, since there are many different entities that are part of the cryptocurrency network and that are not necessarily subjected by any AML/CTF regulations; thus not having a requirement to link the cryptocurrency addresses with real world identity, it could be argued that during the customer risk assessment in addition to checking the

reputation of the customer and its close associates or beneficial owners, as mentioned in the guidelines provided by the ESA (ESA, 2017), the cryptocurrency exchanges should also check whether the cryptocurrency addresses known to be owned by the customer or its close associates (incl. beneficial owners) are not publicly known to be linked to some illegal activities. This could be done by, for example, using an online tool titled “Bitcoin Who's Who - Bitcoin Address Lookup”, which allows its users to report scams for specific Bitcoin addresses and to check whether there has been any reports made for some particular Bitcoin address (Bitcoin Who is Who). Additionally, it could be argued that until the 5AMLD will come into force there will be some database maintained by governmental institution that contains addresses of different cryptocurrency wallets that have been known to have connections with illegal activities or any other kind of bad reputation. This risk factor should be included in the customer risk category.

In terms of products and services that the customer has used, it could be argued that another risk increasing factor that is unique to the cryptocurrency exchanges is a regular use of services as mixer and anonymiser or usage in the past. *“Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address”* (FATF, 2015: 28). *“Anonymiser (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. (Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer))”* (FATF, 2015: 28). A known regular use of any of these services by a customer or use of them in the past arguably would increase the suspicions of the customer’s intentions, when using cryptocurrencies; thus increase the risk of ML/TF.

One methodology that could be used to uncover whether the customer has used a mixer or anonymiser would be to employ a machine learning. The specific approach has been explained in the academic paper titled “Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning”. In the paper it is demonstrated how supervised machine learning can be used to categorize Bitcoin addresses in different categories, including mixing services (Mikkel Alexander Harlev et al., 2017). It could be argued that based on this method cryptocurrency exchanges would be able to identify mixer services that their customers have used and thus increase the ML/TF risk level of their



customers. This method could be used during the customer ML/TF risk assessment and transaction monitoring. The use of the method in transaction monitoring will be described in the proceeding sections.

It could be argued that apart from reconsidering the risk factors that are used for the customer ML/TF risk assessment and adjusting them according to the unique circumstances of the cryptocurrency exchanges, the process of risk assessment should remain the same as described previously - the relative importance of each of the risk factors should be assessed and based on the assessments weights to each of the risk factors assigned. The methodology of how to properly assess the importance of each of the risk factors and assign weights accordingly is out of scope of this paper; thus will not be further discussed. Additionally, in order to acquire the final risk score and determine the customer ML/TF risk level it could be argued that the same approach as described in the ESA's "Risk Factors Guidelines" (ESA, 2017) should be applied in cryptocurrency exchanges as well.

While it was argued that for the enterprise-wide ML/TF risk assessment a risk assessment model built in a simple spreadsheet software might be enough due to the relative simplicity of most of the cryptocurrency exchanges and the frequency of performing the enterprise-wide ML/TF risk assessments, having the requirement to assess the ML/TF risk for each customer and reassess it on ongoing basis arguably would demand that cryptocurrency exchanges implement automated software solutions. Additionally, it could be argued that the automated software should be integrated with the database, where all of the information gathered during CDD has been stored.

### 6.3. Customer due diligence (CDD)

*"CDD is an essential measure to mitigate the ML/TF risks associated with convertible VC [- virtual currency]. In accordance with the FATF Standards, countries should require convertible VC exchangers to undertake customer due diligence when establishing business relations or when carrying out (non-wire) occasional transactions using reliable, independent source documents, data or information. (FATF, 2015: 12).*

It was shown in the previous chapter that the cryptocurrency exchanges already are collecting arguably an extensive amount of information on their customers. However, all of the information that was shown to be collected by the exchanges was asked directly to the client and was done through the internet instead of face-to-face; thus relying solely on the customer's honesty to provide accurate information. While it might be that the cryptocurrency exchanges are collecting more information on their customers than the one that is directly asked for customers to provide, it could not be tested during this research due to not

having an access to the internal processes of cryptocurrency exchanges. However, the FATF has provided several suggestions that could augment the already collected information as well as verify it.

*“In light of the nature of VCPSS, in which customer relationships are established, funds loaded and transactions transmitted entirely through the internet, institutions must necessarily rely on nonface-to-face identification and verification. These, to the extent applicable, include: corroborating identity information received from the customer, such as a national identity number, with information in third party databases or other reliable sources; potentially tracing the customer’s Internet Protocol (IP) address; and searching the Web for corroborating activity information consistent with the customer’s transaction profile, provided that the data collection is in line with national privacy legislation”* (FATF, 2015: 12).

In addition to collecting the identification and other customer related data that has been required by the regulations and recommended by the guidelines mentioned earlier in this paper, arguably cryptocurrency exchanges should collect and store data that is unique to the cryptocurrencies as well. For example, in case of Bitcoin, the bitcoin addresses that are known or have been indicated by the customer to belong to the specific customer. The addresses then could be compared against different lists and tested whether any of them have been known to be involved in any scams or any other illegal activities. Additionally, the whole transaction history that is stored on the public general ledger could be reviewed during the CDD process in order to find some suspicious patterns or transactions executed in the past. For this purpose Michele Spagnuolo, Federico Maggi, and Stefano Zanero have designed and tested a framework called “BitIodine”.

*“BitIodine is a modular framework to parse the Bitcoin blockchain, cluster addresses likely to belong to a same entity, classify such entities and labels them, and visualize complex information extracted from the Bitcoin network. BitIodine can label users and addresses (semi-)automatically thanks to scrapers that crawl the Web and query exchanges for information, thus allowing to attach identities to users and trace money flowing through Bitcoin. BitIodine supports manual investigation by finding (reverse) paths between two addresses or a user and an address”* (Michele Spagnuolo, Federico Maggi, and Stefano Zanero, 2014: 467).

This framework would enable obliged entities to collect more information regarding the customer’s past activities on the cryptocurrency network in a easy to read format; thus decreasing the ML/TF risks that cryptocurrencies pose due to their anonymity aspect by enabling proper assessment of the customer.

Another possibility for cryptocurrency exchanges to collect additional information on their customers or verify the already collected information would be the central register of beneficial owners of

organizations that is going to be required by the 5AMLD, when it comes into force (European Commission, 2016).

*“The personal data of beneficial owners referred to in paragraph 1 [- the name, the month and year of birth, the nationality and the country of residence of the beneficial owner as well as the nature and extent of the beneficial interest held -] shall be disclosed for the purpose of enabling third parties and civil society at large to know who are the beneficial owners, thus contributing to prevent the misuse of legal entities and legal arrangements through enhanced public scrutiny. For this purpose the information shall be publicly available through the national registers and through the system of interconnection of registers for no longer than 10 years after the company has been struck off from the register”* (European Commission, 2016: 40).

It could be argued that cryptocurrency exchanges should ensure a direct connection to the national registers and automatic updating of the information regarding beneficial owners of the organizations that are part of their customer base, since manual collection or verification for each of the customers of the exchange would be inefficient and most probably inaccurate as well. Additionally, if the cryptocurrency exchanges would be able to establish a direct connection to all of the national registers of beneficial owners in the EU, it could be argued that there would be no need for the customers to provide the information by themselves, but rather the information could be collected automatically through the national registers; thus making the registration process significantly less complicated and reduce the total time it takes to complete the registration process.

Besides the standard CDD, the 4AMLD stipulates a need for two additional types of CDD – SCDD and ECDD. The cases, when each of the CDD types are applied should be documented in detail. The use cases should depend on the transaction type and the results of customer ML/TF risk assessment (European Commission, 2015). The same requirements apply directly to the cryptocurrency exchanges as well due to being included as an obliged entity in the 5AMLD (European Commission, 2016). The design of the SCDD and ECDD measures, as explained in the previous chapters, should rely completely on the circumstances of each of the specific companies and require adjustments across various different dimensions. Since, there are many ways of how to design the SCDD and ECDD measures, the specific design of them is outside of the scope of this paper.

To sum up, it could be argued that the overall design of CDD, SCDD, and ECDD measures in the cryptocurrency exchanges should be similar to the ones that have been described earlier in this paper. However, as mentioned above, to compensate for the nature of cryptocurrency exchanges – most of the

business being conducted on the internet rather face-to-face – and cryptocurrencies – a high level of anonymity on the cryptocurrency network itself – as well as to utilize the unique circumstances of the exchanges, the cryptocurrency exchanges arguably should collect additional information on the customers through other sources that might be unavailable to obliged entities in other industries or information that is unique for the cryptocurrencies, while at the same time complying with the privacy regulations. This arguably would enable cryptocurrency exchanges to cover the unique ML/TF risks that they are exposed to compared to other, more conventional financial institutions.

According to the 4AMLD, the obliged entities are required to retain records that include *“a copy of the documents and information which are necessary to comply with the customer due diligence requirements [...] for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction”* (European Commission, 2015:101). Thus besides keeping records of the information that has been gathered on the existing customer during the process of CDD, the cryptocurrency exchanges should have systems and policies in place to ensure the retention of the relevant information regarding their former customers as well.

In terms of software, it could be argued that for the CDD process per se no special tools would be required besides a database and a data input interface, since no automation is required and, as showed in the previous chapter, some cryptocurrency exchanges allow their customers to provide the information about themselves in form of e-mails or by uploading the information filled out in word documents. The database should ensure data retention for five years as required by the 4AMLD (European Commission, 2015) as well as integration with other software tools that are used in other AML/CTF measures, since, as mentioned before, the information regarding the organization’s customer base serves as a foundation for other AML/CTF measures. However, it could be argued that some specialized software would be required to acquire data that is unique to the cryptocurrency exchange industry. For example, software for acquisition of the customer’s IP address, software for the Bitlodge framework, or software to integrate with the national registers of beneficial owners.

#### 6.4. Transaction monitoring (TM)

*“Transaction monitoring is a key risk mitigant in the convertible VC space because of the difficulty of non-face-to-face identity verification and because it is only recently that decentralised convertible VC technology allows certain risk mitigants that may be available for NPPS to be built into decentralised VCPSS in order to restrict functionality and reduce risk. For instance, multisignature (multi-sig)*

*technology now enables VCPPTS to effectively build in loading total wallet value, and value/velocity transaction limits into decentralised VCPPTS. However, current decentralised VC technology does not make it possible to effectively build in geographic limits; limit use to the purchase of certain goods and services; or prevent person-to-person transfers” (FATF, 2015: 13).*

The 4AMLD stipulates a requirement for obliged entities to monitor all of the transactions of its customers that have been serviced by the obliged entities. The obliged entities are required to identify any suspicious or unusual transactions through their transaction monitoring measures and report them to the authorities – FIUs (European Commission, 2015). As mentioned in the previous chapters, the suspicious or unusual transactions are identified by comparing them to different scenarios or limits. If any of the scenarios or limits have been reached, the transaction should be flagged as suspicious and further analyzed by an analyst.

According to the BCBS, obliged entities “*should be able to identify transactions that do not appear to make economic sense, that involve large cash deposits or that are not consistent with the customer’s normal and expected transactions”* (Basel Committee on Banking Supervision, 2016: 10). Additionally, the ESA in their guidelines have provided the following characteristics of unusual transactions:

- “• they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;*
- they have an unusual or unexpected pattern compared with the customer’s normal activity or the pattern of transactions associated with similar customers, products or services; or*
- they are very complex compared with other, similar, transactions associated with similar customer types, products or services”* (ESA, 2017: 27).

While there is no requirement for obliged entities to monitor transactions that the entities are not servicing, it could be argued that for cryptocurrency exchanges it would be beneficial to not only screen the transactions that the exchange is servicing, but also some part of the transactions on the cryptocurrency network in order to detect transactions that are suspicious and would require additional attention. For example, in case, if a customer wants to exchange its bitcoins for euro, while the customer itself would be assessed as having a low ML/TF risk and would have a legitimate reason for owning the bitcoins, it might be that the bitcoins have recently been used for some illegal activities and thus should be reported. If the exchanges would not extend their monitoring outside of the firms boundaries, they might not be able to identify the suspicious transaction and thus become facilitators of some illegal activities.

Malte Moser, Rainer Bohme, and Dominic Breuker in their paper “Towards Risk Scoring of Bitcoin Transactions” have described methodology of how by using a set of predictors and the information available on the Bitcoin general ledger one could assesses the risk of a bitcoin being involved in some thefts in the past and thus possibly could be blacklisted by the government (Malte Moser, Rainer Bohme, and Dominic Breuker, 2014). It could be argued that this methodology could be used during the transaction monitoring in order to assess the risk of each of the transactions and determine the probability of any of them being involved in any thefts or scams in the past. Thus ensuring the utilization of publicly available information on all of the cryptocurrency transactions. Any of the transactions that would reach a certain level of probability that the specific bitcoins involved in the transaction have been involved in a scam or a theft in the past would have to be analyzed in detail by the analysts.

Additionally, as mentioned in the section about CDD measures, the classification method explained in the paper “Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning” could be used in the transaction monitoring as well. As it was mentioned, the methodology employs supervised machine learning to classify different wallet addresses on the Bitcoin network. The classification groups include exchanges, merchant service providers, gambling service providers, mixers and other service providers (Mikkel Alexander Harlev et.al., 2017). Arguably this method could be used for classification of the counterparties that the customers of a cryptocurrency exchanges are conducting business with on the Bitcoin network. It could provide additional information to the cryptocurrency exchanges regarding their customers and thus enable them to identify suspicious or unusual activities more effectively.

It could be argued that, in addition to different pattern detection, cryptocurrency exchanges would also need to have different thresholds that would be used to monitor transactions and identify any unusual transactions that are not consistent with the customer’s normal behavior or the normal behavior of similar customers, and thus require ECDD. For example, different thresholds could be set for the amounts that are being exchanged by a customer in some period of time or in a single transaction, the frequency of performed exchanges by a customer in different periods of time, and the total number of transactions performed in a certain period of time. According to Umberto Lucchetti Junior, different thresholds should be set for different groups of customers in order to decrease amount of false positives as well as ensure that the thresholds are closer to the reality. The customers should be divided in groups based on the

information gathered during the CDD – for example, based on the disclosed annual income or revenue (legal entity) of the customer – or customer ML/TF risk assessment – for example, based on the overall risk that the customer pose to the company. Additionally, Umbretto has provided a description of tuning the thresholds in order to increase the efficiency of the transaction monitoring (Umberto Lucchetti Junior, 2013). However, further introduction of this method is out of scope of this paper.

*“A bank should ensure that they have appropriate integrated management information systems, commensurate with its size, organisational structure or complexity, based on materiality and risks, to provide both business units (eg relationship managers) and risk and compliance officers (including investigating staff) with timely information needed to identify, analyse and effectively monitor customer accounts. The systems used and the information available should support the monitoring of such customer relationships across lines of business and include all the available information on that customer relationship including transaction history, missing account opening documentation and significant changes in the customer’s behaviour or business profile and transactions made through a customer account that are unusual”* (Basel Committee on Banking Supervision, 2016).

It could be argued that not only banks require information systems for transaction monitoring, but also cryptocurrency exchanges due to the fact that, as showed in previous chapter, there is a large volume of USD exchanged through cryptocurrency exchanges every 24 hours, and thus requires an information system to monitor all of the exchanges serviced by the cryptocurrency exchange and identify any suspicious or unusual activities. It could not be done manually. Additionally, an integration of the previously described methodology for rating the risk of the bitcoins that are contained in the transactions being involved in a theft or scam in the past would require a software that analyses the general ledger of the Bitcoin network and determines the risk level automatically.

## 6.5. Sanctions screening

It has been reported that OFAC, US department that administrates and imposes sanctions based on US foreign policy (OFAC: About), may include cryptocurrency wallet addresses on their Specially Designated Nationals (SDN) list next to the names of people and organization against whom certain sanctions have been imposed (Nikhilesh De, 2018). While there are no news regarding the inclusion of cryptocurrency wallet addresses in sanctions lists that apply to the obliged entities in EU, it could be argued that until the 5AMLD will come into force the cryptocurrency wallet addresses will be added to the relevant sanctions lists as well. Thus enabling and arguably most probably requiring for the cryptocurrency exchanges to screen not only the names of customers or countries that the customers are

connected with against the sanctions lists, but the cryptocurrency wallet addresses as well. This additional information to use for screening the customers against the sanctions lists arguably would benefit in identification of suspicious activities as well as suspicious customers by ensuring that, for example, seemingly low risk customers that own Bitcoin wallet addresses that have been known to be involved in terrorist financing activities and thus have been sanctioned would be identified during the CDD procedures or transaction monitoring; therefore would not implicate cryptocurrency exchanges that services the currency exchange transactions for the customer.

As mentioned in the previous chapters, the process of sanctions screening should be conducted together with CDD and transaction monitoring measures in order for the obliged entities to be able to identify any possible connections to sanctions lists and thus evade any possible sanctions breaches. Based on the information provided in the previous chapters as well as in the beginning of this section, it could be argued that the cryptocurrency exchanges should screen the names, countries and cryptocurrency wallet addresses that are associated to their customers. Additionally, it could be argued that while during the CDD the process of sanctions screening could be performed manually by the employees, during the transaction monitoring it should be linked to the information system that has been used for the transaction monitoring in order to ensure a timely detection of possible sanctions breaches.

## 6.6. Governance

As stipulated by the 4AMLD, obliged entities are required to appoint a board member that is going to be responsible for the AML/CTF measures and other AML/CTF related issues (European Commission, 2015). This requirement will apply to the cryptocurrency exchanges as well, when the 5AMLD will come into force (European Commission, 2016). Next, it was mentioned in the previous sections that the BCBS has proposed three lines of defense that should be implemented by the obliged entities (Basel Committee on Banking Supervision, 2016).

The first line of defense relates to the employees of the company. The BCBS mentions the need for the obliged entities to design clear procedures and policies presented in writing and communicated to the employees in order to provide them with instructions for complying with the AML/CTF requirements (Basel Committee on Banking Supervision, 2016). It could be argued that, while the core part of the policies and procedures could remain similar to, for example, the banks, different additional requirements should be included in the AML/CTF policy for cryptocurrency exchanges. The core part could remain



the same for cryptocurrency exchanges due to having to comply with the same AML/CTF regulations as any other obliged entities, including banks, mentioned in the 4AMLD and 5AMLD. The additional requirements described in the AML/CTF policy could be, for example, descriptions of the unique AML/CTF measures for the cryptocurrency exchanges introduced in this chapter. There the different requirements and instructions for the employees to ensure the compliance with AML/CTF requirements could be described. Additionally, it could be argued that the instructions for employees described in the AML/CTF policies in cryptocurrency exchanges could be more technologically advanced than the ones in the banks due to the nature of the business. Thus an appropriate technical training might be required to the personnel whose responsibilities are related to the AML/CTF measures in any way. However, the training requirements for cryptocurrency exchanges will be discussed in different section further in this chapter.

The second line of defense, as described before, relates to the appointment of chief AML/CTF officer that would serve as the key person in the organization regarding any internal or external issues related to the AML/CTF. It could be argued that the second line of defense could be ensured by the cryptocurrency exchanges without additional adjustments – appointing an adequate chief AML/CTF officer that would be responsible for the compliance with the AML/CTF requirements.

It could be argued that in order for the third line of defense, internal audit, to be effective in cryptocurrency exchanges the additional tools and methodologies that could be used to enhance different AML/CTF measures and were mentioned in the previous chapters should be tested as well, additionally to all of the functions that were mentioned by the BCBS (Basel Committee on Banking Supervision, 2016). Arguably testing of the tools that are unique to the AML/CTF measures of cryptocurrency exchanges would involve specific knowledge and software; thus either the employees of the cryptocurrency exchanges should possess such capabilities or the testing could be outsourced to some reliable third party. However, no further considerations regarding these software tools or capabilities will be discussed in this paper due to being out of scope.

Overall, it could be argued that no specific software tools or complementary methodologies would be required for cryptocurrency exchanges to comply with the governance requirements and to implement the three lines of defense, except from the discussed additional software tools and capabilities for internal auditing, if such process would be implemented at all within the exchange.

## 6.7. Reporting

As stipulated by the 4AMLD, obliged entities are required to establish two types of reporting processes within the organization – reporting of internal breaches and reporting of suspicious activities to the local FIUs (European Commission, 2015). While arguably the reporting process of internal breaches should not be any different from the reporting process implemented in any other types of obliged entities, it could be argued that the process of reporting suspicious activity should involve several differences. First, the information that is provided in the SAR and reported to the respective authorities should contain additional information that is unique to the sector of cryptocurrency exchanges as, for example, cryptocurrency wallet addresses of the entities mentioned in the SAR. This would enable FIUs to conduct more thorough investigations outside and inside the cryptocurrency network.

Second, it could be argued that in case, if the cryptocurrency exchange has implemented in the transaction monitoring measure the previously mentioned method of monitoring transactions that have been performed on the cryptocurrency network by the customers that the exchange is servicing, the cryptocurrency exchange should report any suspicious activities identified on cryptocurrency network as well. Thus enhancing the effectiveness of AML/CTF measures on the union level by enabling authorities to identify cryptocurrency transactions and wallet addresses that could be connected to some illegal activities as well as to collect more information on the participants of different cryptocurrency networks.

It could be argued that for the implementation of reporting measures in the cryptocurrency exchanges there would be no need for any complementary methodologies or software tools. Arguably the procedures for both of the mentioned types of reports that have to be implemented in the obliged entities could be performed manually – by using report templates that are filled out by the analysts or employees of the organization and sent to the respective authorities. However, software tools could be used to facilitate and increase efficiency for the both of the mentioned reporting requirements.

## 6.8. Administration of data and information

*“At a minimum, financial institutions and DNFBP should be required to maintain transaction records that include: information to identify the parties; the public keys, addresses or accounts involved; the nature and date of the transaction, and the amount transferred. The public information available on the blockchain provides a beginning foundation for record keeping, provided institutions can adequately identify their customers. Countries should require institutions to be attentive to the type of suspicious activity they are in a position to detect” (FATF, 2015: 13).*

While it could be argued that the cryptocurrency exchanges should collect and retain information that is specific to the particular industry additionally to the required information that is mentioned in the section 4.4.3.3., all of the other requirements on the data processing, sharing and retaining described in the previous sections should be directly applied in the cryptocurrency exchanges as well. The data and information administration procedures and policies should be described in the AML/CTF policy of the cryptocurrency exchange.

It could be argued that there is no need for separate software tools that enable for the cryptocurrency exchanges to share and retain the collected information on customers and their transactions. These functionalities should be already integrated in the systems that are used to facilitate other AML/CTF measures described in this paper. Additionally, it could be argued that this AML/CTF measure primarily relates to the policies and procedures that should be developed and written down as a guidance for the employees to be able to comply with the AML/CTF requirements instead of implementing separate systems or processes.

## 6.9. Training

As stipulated in the 4AMLD, obliged entities are required to provide training to their employees in order to increase their understanding of the AML/CTF measures as well as increase their capability to identify possible suspicious activities (European Commission, 2015). It could be argued that in order for the trainings to be effective they should be significantly adjusted to the circumstances of cryptocurrency exchanges. Additionally, they arguably should provide not only the knowledge regarding the AML/CTF measures and requirements, but the conceptual and technological foundation of cryptocurrency to a certain degree as well. This would enable employees to acquire better understanding of the connection between AML/CTF measures and the cryptocurrency itself; thus enabling them to identify suspicious activities more effectively.

Additionally, it could be argued that it would be beneficial for the cryptocurrency exchanges to provide their employees with opportunity to acquire certificates from the Association of Certified Anti-Money Laundering Specialists (ACAMS) (About the Association of Certified Anti-Money Laundering Specialists), including the “Virtual Currency and Blockchain training Certificate”, which would provide employees with in-depth knowledge regarding the risks that cryptocurrencies pose as well as some practical examples (A Cost-Effective Solution to Obtaining Virtual Currency and Blockchain Training).

*“ACAMS is the largest international membership organization dedicated to advancing the professional knowledge, skills and experience of those dedicated to the detection and prevention of money laundering around the world, and to promote the development and implementation of sound anti-money laundering policies and procedures”* (About the Association of Certified Anti-Money Laundering Specialists).

In addition to certification, ACAMS provides trainings in form of seminars, conferences and online seminars; thus the organization can choose the most appropriate form and topic of the AML/CTF trainings (The Global Leader in Financial Crime Conferences & Education).

The training plans and requirements as well as all of the other AML/CTF measures mentioned in this chapter should be described in the AML/CTF policy of the organization; thus providing a clear overview of all of the internal requirements for the employees that have to be followed in order to comply with the AML/CTF requirements as well as providing authorities with a description of the implemented measures for ML/TF risk mitigation.

## 6.10. Research framework

In addition to all of the recommendations provided in the previous sections of this chapter, a research framework was developed (see Table 3). Information that has been provided throughout this paper has been used as a foundation for the development of the research framework. The research framework contains all of the mentioned AML/CTF measures (on the horizontal axes) grouped in the three respective categories – risk assessments, Know Your Customer (KYC), and policies and procedures. The dimensions to AML/CTF measures that are relevant for cryptocurrency exchanges are listed on the vertical axis. The dimensions are regulations, guidelines, software tools, and complementary methodologies and guidelines. Each of the research framework dimensions will be described next.

Information regarding the first two dimensions – regulations and guidelines – can be found in the chapter 4 of this paper, where they are introduced in context of each of the AML/CTF measures. Regulations dimension refers to the different regulations applicable in the EU that require design and implementation of the described AML/CTF measures. This dimension mainly consists of two regulations – the 4AMLD and 5AMLD – since these are the main regulations in the European Union that stipulate the requirement for development and implementation of AML/CTF measures, as explained previously in this paper. They serve as the foundation for all of the AML/CTF measures discussed in this paper. While the regulations

that are applicable to the cryptocurrency exchanges operating in the EU were included in the dimension, these regulations stipulate the same requirements for other types of organizations as well.

Next, guidelines refer to the different guidance materials for the design and implementation of the AML/CTF measures that have been developed by different international organizations that specialize in AML/CTF related issues. These guidelines provide additional information and recommendations on how the AML/CTF measures that have been required by the aforementioned regulations should be designed and implemented. Similarly to the regulations dimension the guidelines included in this dimension apply to other types of organizations as well in addition to the cryptocurrency exchanges.

Furthermore, the information on the two last dimensions of the research framework – software tools and complementary methodologies and guidelines – can be found in the chapter 6 of this paper together with different suggestions regarding the design and implementation of the required AML/CTF measures. These two dimensions refer specifically to the cryptocurrency exchanges and are not applicable to any other types of organizations.

Software tools dimension refers to the different information systems that arguably could facilitate the implementation and execution of the AML/CTF measures. The information contained in this dimension provides an overview of the technology related needs for implementation and execution of the AML/CTF measures. As it could be seen, not all of the AML/CTF measures require sophisticated software tools or information systems.

At last, the complementary methodologies and guidelines dimension refers to the different methodologies that could be implemented in the cryptocurrency exchanges in order to facilitate the execution of the AML/CTF measures as well as to the guidelines that can help to increase the understanding of the AML/CTF related issues in context of the cryptocurrency exchanges. The methodologies mentioned in this dimension have been introduced by other researches. However, the additional guidelines have been provided by organizations that specializes in AML/CTF related issues.

The research framework as well as the suggestions provided in this chapter will be discussed further in the next chapter.

Dimensions to AML/CTF Measures for Cryptocurrency Exchanges	AML/CTF Measures								
	Risk Assessments		Know Your Customer (KYC)			Policies and Procedures			
	Enterprise-wide ML/TF risk assessment of a financial institution	Client ML/TF risk assessment	Customer Due Diligence (CDD)	Transaction Monitoring (TM)	Sanctions screening	Governance	Reporting	Administration of data and information	Employee training
<b>Regulations</b>	- The 4th AML Directive; - The 5th AML Directive.	- The 4th AML Directive; - The 5th AML Directive.	- The 4th AML Directive; - The 5th AML Directive.	- The 4th AML Directive; - The 5th AML Directive.	- The 4th AML Directive; - The 5th AML Directive; - The Bank Secrecy Act (applicable only in particular cases).	- The 4th AML Directive; - The 5th AML Directive.	- The 4th AML Directive; - The 5th AML Directive.	- The 4th AML Directive; - The 5th AML Directive.	- The 4th AML Directive; - The 5th AML Directive.
<b>Guidelines</b>	- Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption (The Wolfsberg Group, 2015); - The Risk Factors Guidelines (The Joint Committee of ESA, 2017).	- RBA approaches for different sectors (FATF); - The Risk Factors Guidelines (The Joint Committee of ESA, 2017).	- Customer due diligence for banks (Basel Committee on Banking Supervision, 2001); - The Risk Factors Guidelines (The Joint Committee of ESA, 2017).	- Sound management of risks related to money laundering and financing of terrorism (Basel Committee on Banking Supervision, 2016).	- Sound management of risks related to money laundering and financing of terrorism (Basel Committee on Banking Supervision, 2017).	- Sound management of risks related to money laundering and financing of terrorism (Basel Committee on Banking Supervision, 2017).	- No additional guidelines have been provided.	- No additional guidelines have been provided.	- Sound management of risks related to money laundering and financing of terrorism (Basel Committee on Banking Supervision, 2017).
<b>Software tools</b>	- Spreadsheet software.	- Bitcoin Address Lookup online tool for testing whether any of the Bitcoin wallet addresses associated with a customer have bad reputation (Bitcoin Who is Who); - Automated software solutions.	- Database with data input interface and possibility to integrate with other software tools used for other AML/CTF measures; - Specialized software tools for acquisition of information that is unique to cryptocurrency exchanges.	- Information system that performs transaction monitoring automatically and can be integrated with other systems as well.	- Could be conducted manually during the CDD; - Would need integration with the information system used for transaction monitoring to screen customers automatically during the monitoring of transactions.	- Specialized software tools for internal auditing of the AML/CTF measures unique to the cryptocurrency exchanges (if internal audit is implemented).	- No software tools required (would be needed only to increase efficiency).	- No software tools required.	- No software tools required.
<b>Complementary methodologies and guidelines</b>	- Virtual Currencies Key Definitions and Potential AML/CFT Risks (FATF, 2014)	- Guidance for a Risk-Based Approach: Virtual Currencies (FATF, 2015); - Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning (Mikkel Alexander Harlev et al., 2017).	- Guidance for a Risk-Based Approach: Virtual Currencies (FATF, 2015); - BitIodine: Extracting Intelligence from the Bitcoin Network (Michele Spagnuolo, Federico Maggi, and Stefano Zanero, 2014).	- Guidance for a Risk-Based Approach: Virtual Currencies (FATF, 2015); - Towards Risk Scoring of Bitcoin Transactions (Malte Moser, Rainer Bohme, and Dominic Breuker, 2014); - Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning (Mikkel Alexander Harlev et al., 2017); - AML Rule Tuning: Applying Statistical and Risk-Based Approach to Achieve Higher Alert Efficiency (Umberto Lucchetti Junior, 2015).	- US Could Put Crypto Wallets on OFAC Sanctions List (Nikhilesh De, 2018).	- No complementary methodologies or guidelines are required.	- No complementary methodologies or guidelines are required.	- Guidance for a Risk-Based Approach: Virtual Currencies (FATF, 2015).	- ACAMS Virtual Currency and Blockchain Certificate; - ACAMS Training - seminars, conferences, web seminars.

Table 3 – Research Framework

## 7. Discussion

The research framework, presented in the previous chapter, could be used both by the academics and the cryptocurrency exchanges. The academics could use the research framework to gain an overview of the AML/CTF measures that have been stipulated by the regulations and guidelines as well as to gain an overview of the different methodologies and software tools that could be used to complement the AML/CTF measures. The framework could serve as a foundation for further research on each of the specific AML/CTF measures or on the issues that relates to the design and implementation of AML/CTF measures in cryptocurrency exchanges. This could inspire whole range of different researches; thus contributing to the understanding of AML/CTF measures from the academic point of view.

Next, the cryptocurrency exchanges could use the research framework as a first step in understanding the requirements regarding the implementation of specific AML/CTF measures that are stipulated by the EU regulations. The research framework could serve as an overview of all of the AML/CTF measures that are required as well as would provide a guide of where to find more information regarding the specific AML/CTF measures. Additionally, the framework could help to explore the different methodologies that could improve the effectiveness of the AML/CTF measures and the software tools that would be required to ensure a proper execution of the measures. This could serve as the starting point for the cryptocurrency exchanges, when designing or implementing the required AML/CTF measures as well as when starting to explore the requirements and the different options regarding the measures.

Major part of the information that was collected for the development of the research framework was taken from the regulations or different guidelines that have been developed by different organizations that specialize in the issues related to the AML/CTF. While none of the guidance acquired from the regulations and guidelines were specifically tailored for the cryptocurrency exchanges, the information ensured that the adjustments to the AML/CTF suggested for the crypocurrency exchanges will compliant to the regulations, since that is one of the main concerns, when discussing AML/CTF measures.

While it was demonstrated that currently there are no guidelines that are specifically developed for crypotcurrency exchanges, it could be argued that until the proposed amendments to the 4AMLD will come into force at least some guidelines will be developed that will address specifically the unique circumstances of the cryptocurrency exchanges. However, at this point in time only guidelines for different sectors than the crypocurrency exchanges are available and thus for the design and

implementation of the AML/CTF measures the guidance provided in the guidelines have to be adapted to suit the cryptocurrency exchanges as well as the unique circumstances.

It was demonstrated in this paper that the core parts of the AML/CTF measures could be implemented directly in the cryptocurrency exchanges. However, it was also showed that different adjustments could be made to the AML/CTF measures in order to suit the cryptocurrency exchanges better and would be more effective. For example, different software tools and methodologies could be utilized in order to collect additional information that is unique to the cryptocurrency exchanges. It could be argued that there could be many more adjustments made to the AML/CTF measures in addition to the ones already presented in this paper to improve the effectiveness even further. However, as already mentioned before, a compliance to the regulations is a major requirement that should be taken into account when redesigning the AML/CTF measures; thus the regulations and official guidelines should be used as a foundation for the any of the AML/CTF measures.

## 8. Conclusion

In this paper, it was demonstrated how the AML/CTF measures that are required by the EU regulations could be adjusted for the cryptocurrency exchanges in order to ensure effective mitigation of ML/TF risk, while at the same time remaining compliant with the regulations. First, the underlying technological and conceptual principles of the cryptocurrency were explained as well as it was argued that cryptocurrencies can be very diverse. Second, the AML/CTF measures that are required by the EU regulations were presented and described in depth based on the stipulated requirements of the regulations as well as guidelines that were developed by organizations that specializes in issues related to AML/CTF. Third, the market landscape of the cryptocurrency exchanges was described and an overview of the customer information that is being collected by the cryptocurrency exchanges was provided. It was argued that the cryptocurrency exchanges already are collecting a significant amount of information on their customers and that the customers could be properly identified and the customer ML/TF risk assessed based on this information. Fourth, different recommendations regarding the possible adaptations of the AML/CTF measures for cryptocurrency exchanges were provided. Additionally, different software tools and methodologies that could facilitate the AML/CTF measures were mentioned. At last, a research framework that contains the different guidelines, software tools and methodologies was proposed. While



some of the elements from the research framework could be applied to other obliged entities as well, the research framework is specifically designed to be applied for cryptocurrency exchanges.

It could be argued that the contribution of this research is two-fold. First, the main AML/CTF measures that are required by the EU regulations were described in detail taking into account both the requirements stipulated in the EU regulations and relevant guidelines. Thus a comprehensive description of the required AML/CTF measures was provided and it could be used not only in the context of cryptocurrency exchanges, but also for any other obliged entities. Second, different suggestions were provided specifically for cryptocurrency exchanges regarding the adjustments of AML/CTF measures. These suggestions could further be used by the cryptocurrency exchanges, when implementing AML/CTF measures due to the requirement of the 5AMLD. To the author's best of knowledge this is the first research that aimed to adapt AML/CTF measures for cryptocurrency exchanges.

## 9. Reflections and limitations

The research that was described in this paper, instead of being an extensive description of all of the adjustments that should be made to the AML/CTF measures for cryptocurrency exchanges, should be considered as a starting point for further research that would do a more in-depth review of each of the particular AML/CTF measures and provide even more precise description of the possible design options for cryptocurrency exchanges, for example, in a form of developing a detailed model of the customer ML/TF risk assessment. Additionally, a research of the current internal processes, procedures and policies of cryptocurrency exchanges could lead to even better understanding of the circumstances that the cryptocurrency exchanges are exposed to. This could be another direction for further research, since this direction was arguably under-researched in this paper.

## 10. References

- Nick Statt (2018). This year's SXSW was all about blockchain dreamers, cryptocurrency scammers, and everything in between. Available at: <https://www.theverge.com/2018/3/16/17130532/blockchain-bitcoin-cryptocurrency-scams-fraud-sec-sxsw-2018> [Accessed on 15/05/2018]
- John W. Schoen (2017). This chart shows bitcoin's meteoric rise over the last 6 years. Available at: <https://www.cnbc.com/2017/11/29/this-chart-show-bitcoins-meteoric-rise-over-the-last-6-years.html> [Accessed on 15/05/2018]
- Joshua Fruth (2018). 'Crypto-cleansing:' strategies to fight digital currency money laundering and sanctions evasion. Available at: <https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I> [Accessed on 15/05/2018]
- European Commission (2015). DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849> [Accessed on 02/05/2018]
- European Commission (2016). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0450> [Accessed on 02/05/2018]
- Arthur Asa Berger (2014). Media And Communication Research Methods Third Edition. SAGE.
- CoinMarketCap. All Cryptocurrencies. Available at: <https://coinmarketcap.com/all/views/all/> [Accessed on 25/03/2018]

- Jan Lansky (2018). Possible State Approaches to Cryptocurrencies. JOURNAL OF SYSTEMS INTEGRATION 2018/1 19
- European Banking Authority (2014). EBA Opinion on ‘virtual currencies’. Available at: <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> [Accessed on 24/03/2018]
- Joseph Young (2018). Exponential Growth: Cryptocurrency Exchanges Are Adding 100,000+ Users Per Day. Available at: <https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day> [Accessed on 24/03/2018]
- Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- Yli-Huomo J., Ko D., Choi S., Park S., Smolander K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 11(10).
- Reuben Grinberg (2011). Bitcoin: An Innovative Alternative Digital Currency.
- Wim Raymaekers (2014). Cryptocurrency Bitcoin: Disruption, challenges and opportunities. Journal of Payments Strategy & Systems Volume 9 Number 1.
- Hari Krishnan Ramachandran, Sai Saketh, and Marichetty Venkata Teja Vaibhav (2015). Bitcoin Mining: Transition to Cloud. International Journal of Cloud Applications and Computing, 5(4), 56-87.
- Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun (2012). Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin.
- Bitcoinwiki. Hash. Available at: <https://en.bitcoin.it/wiki/Hash> [Accessed on 14/04/2018]
- M. Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck (2017). Blockchain. Springer Fachmedien Wiesbaden 2017.
- Bitcoinwiki. Block hashing algorithm. Available at: [https://en.bitcoin.it/wiki/Block\\_hashing\\_algorithm](https://en.bitcoin.it/wiki/Block_hashing_algorithm) [Accessed on 14/04/2018]
- B. Gipp, N. Meuschke, and A. Gernandt (2015). Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. In Proceedings of the iConference 2015 (to appear), Newport Beach, CA, USA, Mar. 24 - 27, 2015.

- Adedeji Kazeem and Ponnle Akinlolu (2016). Improved Image Encryption for Application over Wireless Communication Networks using Hybrid Cryptography Technique. Indonesian Journal of Electrical Engineering and Informatics (IJEI) Vol. 4, No. 4, pp. 307-318.
- Vitalik Buterin (2013). A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM.
- Gavin Wood (2014). ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.
- Frederik Armknecht, Ghassan O. Karame, Avikarsha Mandal, Franck Youssef, and Erik Zenner (2015). Ripple: Overview and Outlook.
- Jon Martindale (2018). What is Ripple? Available at: <https://www.digitaltrends.com/computing/what-is-ripple/> [Accessed on 01/04/2018]
- Gateway guide. Available at: <https://ripple.com/build/gateway-guide/> [Accessed on 01/04/2018]
- XRP The Digital Asset for Payments. Available at: <https://ripple.com/xrp/> [Accessed on 01/04/2018]
- How to Buy XRP. Available at: <https://ripple.com/xrp/buy-xrp/> [Accessed on 01/04/2018]
- FATF: Who we are. Available at: <http://www.fatf-gafi.org/about/> [Accessed on 12/04/2018]
- FATF: What is Money Laundering? Available at: <http://www.fatf-gafi.org/faq/moneylaundering/> [Accessed on 12/04/2018]
- UNDOC (2011). Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes. Available at: [http://www.unodc.org/documents/data-and-analysis/Studies/Illicit\\_financial\\_flows\\_2011\\_web.pdf](http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf) [Accessed on 12/04/2018]
- FATF (2008). Terrorist financing. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf> [Accessed on 12/04/2018]
- Deloitte (2017). 4th Anti-Money Laundering Directive (4AMLD) came into effect on 26th of June 2017. Available at: <https://www2.deloitte.com/ro/en/pages/risk/articles/4th-anti-money-laundering-directive.html> [Accessed on 12/04/2018]

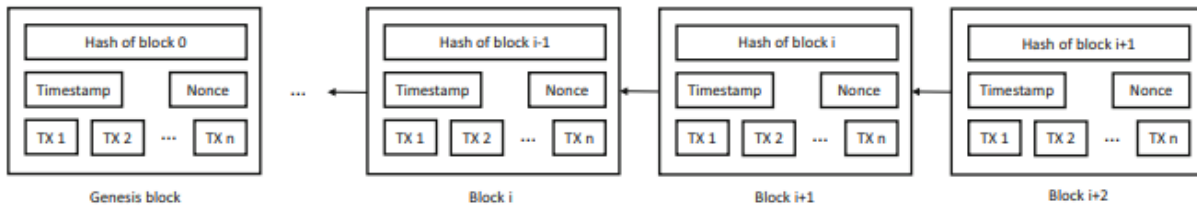
- Samantha Sheen (2016). What is the 5th Anti-Money Laundering Directive? Available at: <https://www.acams.org/aml-resources/samantha-sheens-blog/5th-anti-money-laundering-directive/> [Accessed on 13/04/2018]
- KPMG (2017). Agreement on 5th Anti-Money Laundering Directive. Available at: <https://home.kpmg.com/xx/en/home/insights/2017/12/etf-351-amld5-and-ubo-agreement.html> [Accessed on 13/04/2018]
- Nejc Novak (2018). EU Introduces Crypto Anti-Money Laundering Regulation. Available at: <https://medium.com/@nejcnovaklaw/eu-introduces-crypto-anti-money-laundering-regulation-d6ab0ddedd3> [Accessed on 13/04/2018]
- FATF (2018). INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION The FATF Recommendations. Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> [Accessed on 14/04/2018]
- FATF (2014). GUIDANCE FOR A RISK-BASED APPROACH THE BANKING SECTOR. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf> [Accessed on 14/04/2018]
- FATF Risk-Based Approach. Available at: [http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc\(fatf\\_releasedate\)](http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate)) [Accessed on 14/04/2018]
- ESA (2017). The Risk Factors Guidelines. Available at: <https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf> [Accessed on 14/04/2018]
- Basel Committee Charter. Available at: <https://www.bis.org/bcbs/charter.htm> [Accessed on 14/04/2018]
- Basel Committee on Banking Supervision (2016). Sound management of risks related to money laundering and financing of terrorism. Available at: <https://www.bis.org/bcbs/publ/d353.pdf> [Accessed on 14/04/2018]

- The Wolfsberg Group Mission. Available at: <https://www.wolfsberg-principles.com/about/mission> [Accessed on 14/04/2018]
- The Wolfsberg Group (2015). The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption. Available at: [Accessed on 14/04/2018]
- Basel Committee on Banking Supervision (2001). Customer due diligence for banks. Available at: <https://www.bis.org/publ/bcbs85.pdf> [Accessed on 22/04/2018]
- Council of the European Union (2016). Update of the EU Best Practices for the effective implementation of restrictive measures. Available at: <http://data.consilium.europa.eu/doc/document/ST-15530-2016-INIT/en/pdf> [Accessed on 03/05/2018]
- BANK SECRECY ACT, ANTI-MONEY LAUNDERING, AND OFFICE OF FOREIGN ASSETS CONTROL. Available at: [https://www.ffiec.gov/bsa\\_aml\\_infobase/documents/fdic\\_docs/bsa\\_manual.pdf](https://www.ffiec.gov/bsa_aml_infobase/documents/fdic_docs/bsa_manual.pdf) [Accessed on 03/05/2018]
- Joint Committee of European Supervisory Authorities: About Us. Available at: <https://esas-joint-committee.europa.eu/about-us> [Accessed on 04/05/2018]
- FATF (2015). GUIDANCE FOR A RISK-BASED APPROACH VIRTUAL CURRENCIES. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> [Accessed on 05/05/2018]
- Garrick Hileman and Michel Rauchs (2017). GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY. Available at: [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf) [Accessed on 05/05/2018]
- CryptoCoinCharts. Cryptocurrency Exchanges / Markets List. Available at: <https://cryptocoincharts.info/markets/info> [Accessed on 05/05/2018]
- Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review

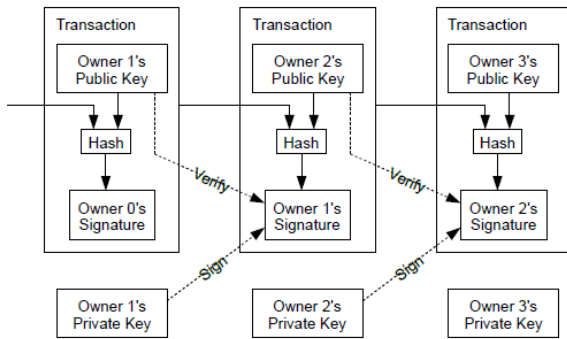
- FATF (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks. Available at: <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> [Accessed on 02/04/2018]
- Bitcoin Who is Who. Available at: <http://bitcoinwhoswho.com/> [Accessed on 02/04/2018]
- Mikkel Alexander Harlev, Haohua Sun Yin, Klaus Christian Langenheldt, Raghava Rao Mukkamala, and Ravi Vatrapu (2017). Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning.
- Michele Spagnuolo, Federico Maggi, and Stefano Zanero (2014). BitIodine: Extracting Intelligence from the Bitcoin Network. International Financial Cryptography Association 2014.
- Malte Moser, Rainer Bohme, and Dominic Breuker (2014). Towards Risk Scoring of Bitcoin Transactions.
- Umberto Lucchetti Junior (2013). AML Rule Tuning: Applying Statistical and Risk-Based Approach to Achieve Higher Alert Efficiency. ACAMS.
- OFAC: About. Available at: <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx> [Accessed on 03/05/2018]
- Niklesh De (2018). US Could Put Crypto Wallets on OFAC Sanctions List. Available at: <https://www.coindesk.com/treasury-department-says-to-not-transact-with-rogue-nations-crypto-users/> [Accessed on 03/05/2018]
- About the Association of Certified Anti-Money Laundering Specialists. Available at: <https://www.acams.org/about-acams/> [Accessed on 03/05/2018]
- A Cost-Effective Solution to Obtaining Virtual Currency and Blockchain Training. Available at: <https://www.acams.org/virtual-currency-and-blockchain-training/> [Accessed on 03/05/2018]
- The Global Leader in Financial Crime Conferences & Education. Available at: <https://www.acams.org/aml-training-and-conferences/> [Accessed on 03/05/2018]

# 11. Appendix

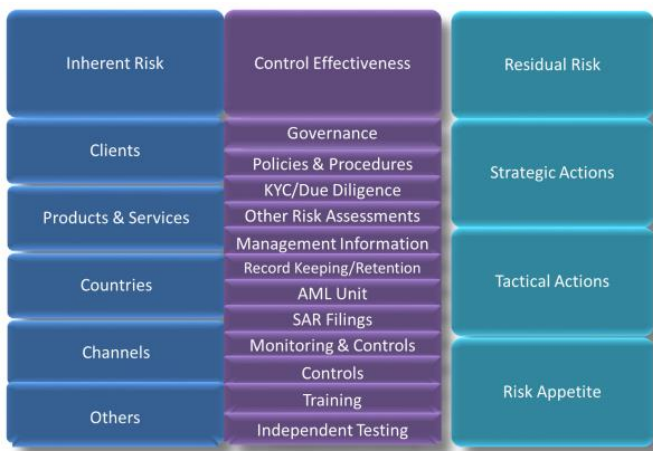
## Appendix 1 – Example of a blockchain (M. Nofer et al., 2017: 184)



## Appendix 2 – Transaction verification (Satoshi Nakamoto, 2008: 2)



## Appendix 3 – Diagram of the conventional/standard ML risk Assessment methodology (The Wolfsberg group, 2015: 7).



## Appendix 4 - Example Calculation of Residual Risk (The Wolfsberg group, 2015: 28)



**3-tier Residual / Risk Rating Approach**

Example Calculation of Residual Risk		
Inherent Risks	Controls Strength	Residual Risks
Low	90-100%	Low
	89-80%	Moderate
	<80%	High
Moderate	90-100%	Low
	89-80%	Moderate
	<80%	High
High	90-100%	Low
	89-80%	Moderate
	<80%	High

**5-tier Residual Risk Rating Approach**

Example Calculation of Residual Risk		
Inherent Risks	Controls Strength	Residual Risks
Low	95-100%	Low
	90-94%	Low to Moderate
	85-89%	Moderate
	80-84%	Moderate to High
	<80%	High
Moderate	95-100%	Low
	90-94%	Low to Moderate
	85-89%	Moderate
	80-84%	Moderate to High
	<80%	High
High	95-100%	Low
	90-94%	Low to Moderate
	85-89%	Moderate
	80-84%	Moderate to High
	<80%	High

**Appendix 5 - Example Factor Weightings (The Wolfsberg group, 2015: 27)**

**Inherent Factor Weighting Examples**

Inherent Factor Weighting Examples	
Inherent Factor	Inherent Weighting
Channels	5-10%
Clients	25-35%
Country / Geography	20-30%
Products & Services	20-30%
Other Qualitative Risk Factors	10-15%

**Control Factor Weighting Examples**

Control Factor Weighting Examples	
Control Factor	Control Weighting
KYC (incl. All requirements)	20-30%
Monitoring & Controls	20-30%
Policies & Procedures	10-15%
Other Risk Assessments	10-15%
AML Corporate Governance; Management Oversight & Accountability	5-10%
Management Information / Reporting	5-10%
Record Keeping & Retention	5-10%
Designated AML Compliance Officer / Unit	5-10%
Detection and SAR Filing	5-10%
Training	5-10%
Independent Testing & Oversight	5-10%
Other Controls / Others	5-10%

**Appendix 6 – factors that lower the risk of ML/TF (European Commission, 2015: 114)**

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 16:

(1) Customer risk factors:

- (a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- (b) public administrations or enterprises;
- (c) customers that are resident in geographical areas of lower risk as set out in point (3);

(2) Product, service, transaction or delivery channel risk factors:

- (a) life insurance policies for which the premium is low;
- (b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
- (c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
- (d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
- (e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);

(3) Geographical risk factors:

- (a) Member States;
- (b) third countries having effective AML/CFT systems;
- (c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
- (d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money

laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

## **Appendix 7 – factors that increase the risk of ML/TF (European Commission, 2015: 115)**

### ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

(1) Customer risk factors:

- (a) the business relationship is conducted in unusual circumstances;
- (b) customers that are resident in geographical areas of higher risk as set out in point (3);
- (c) legal persons or arrangements that are personal asset-holding vehicles;
- (d) companies that have nominee shareholders or shares in bearer form;
- (e) businesses that are cash-intensive;
- (f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(2) Product, service, transaction or delivery channel risk factors:

- (a) private banking;
- (b) products or transactions that might favour anonymity;
- (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
- (d) payment received from unknown or unassociated third parties;
- (e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(3) Geographical risk factors:

- (a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- (b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
- (c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
- (d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

## **Appendix 8 – 4AMLD Article 11 on application of customer due diligence (4AMLD: 91)**

### Article 11

Member States shall ensure that obliged entities apply customer due diligence measures in the following circumstances:

- (a) when establishing a business relationship;
- (b) when carrying out an occasional transaction that:
  - (i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or
  - (ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (1), exceeding EUR 1 000;
- (c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

- (d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- (e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- (f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

## **Appendix 9 – Interview with CEO of a Latvian FinTech company**

**Anrijs:** Hi! I am currently writing my Master Thesis, where I am trying to show how cryptocurrency exchanges could develop and implement AML/CTF measures in order to comply with the upcoming regulations, while taking into account the different guidelines and other advancements in the field of AML/CTF. Regarding this project I wanted to talk to you about your experience regarding cryptocurrency exchanges. Maybe you could start by describing your experience?

**CEO:** Hi! Yes, sure. So couple of weeks ago we were looking for new investors for our FinTech start-up company. We were lucky to find one. However, the catch with him was that all of the money he wanted to invest in our company was stored in his virtual wallet in cryptocurrency. He did not want to pay all of the exchange fees and deal with authorities that might be interested to tax the money at the point of exchange; thus the deal was that he would send us all of the investment sum in corresponding amount of cryptocurrency and we could do whatever we want with it. Of course, we needed to exchange it to euro. Otherwise, we would not be able to use it for supporting the company. Then we started to look for exchanges that we could use to convert the cryptocurrency. The time was very crucial for us, since we really needed to get the money as soon as possible to cover our liabilities. We ended up with three – Mistertango, Bitstamp and Globitex. Next, we proceeded to creating corporate accounts in all of the three cryptocurrency exchange service providers in order to see, who will be the quickest to conclude our registration. We knew that it might take some time to do it and thus we needed to have some backup options, in case if we would get stuck during the registration process. That is pretty much the story.

**Anrijs:** Thank you for the great introduction! May I ask why did you choose these specific three cryptocurrency exchanges?

**CEO:** First of all, we chose Globitex, because it is a Latvian company. We thought that it might be quicker and easier to quickly create account there, since any issues could be resolved by simply visiting their office. The next closest exchange that we found was Mistertango. They are located in Lithuania. And Bitstamp was chosen, because they are large and I had a previous experience with them, which was good; thus we thought that they might have a good and quick registration process. Plus they are large; thus we could trust them.

**Anrijs:** Sounds like a good strategy. Could you please tell me more about the registration process you encountered in these exchanges?

**CEO:** The process of registration was quite straight forward. You go to their website and click on the registration button. Next, you are required to fill out a form with various details about you and answer to some questions. Then you might be asked to answer to some additional questions. At last, when they have received all of the necessary information and probably also verified it, you receive a confirmation message. Then you are good to go.

If we compare the registration process of the different exchanges, Bitstamp had the most complex and longest process of registration. At least, it was for us. They started to ask questions that obviously were gravitating towards the notion that we might use their exchange for the needs of our clients. They started asking for our AML/CTF policies and procedures, since we are financial institution. Most probably, if we would not be a financial institution, they would not have been asking so many questions. Thus I tried to lead the conversation in a direction that would show them that we will only use the service for our own needs, instead of servicing our clients through their exchange. At last, by providing them with our agreement with the investor, they accepted our story.

We had the same issue, when we tried to register for Mistertango. During the registration process, they started asking for the AML/CTF procedures as well. And I quickly replied that *“No, we are not going to use the account to facilitate transactions of our clients. We only need the account for ourselves to receive an investment from our investors”*. They were ok with our response, but then they asked for the

investment agreement. Similarly to the Bitstamp, when I provided them the agreement, there were no more questions, except from that they asked us to get a notarial approval for some documents.

There was one interesting thing with Mistertango that we noticed. While all of the other exchanges had an option to create a corporate account from the beginning, in the Mistertango you have to create an account for a natural person before you can create a corporate account. In a sense, this might be even more advanced than the option to create a corporate account from the beginning, since then you have only one login for you and your company, instead of having to make one for your company and yourself. However, in terms of registration process, it just seemed to be more complicated.

With Globitex we had the least problems. When I had sent answers and documents to all of the required questions that you get at the beginning, we got back only three additional questions, which was significantly less than in other exchanges. Overall the registration process was very similar to all of the other exchanges. The difference between Globitex and the other exchanges was that they asked a full history of the company already in the beginning. When registering to the other exchanges, I uploaded the history in advance together with other documents, even though they did not ask for it. I had a hunch that they might ask for it at some point in the process; thus I had prepared a print out of the full history of the company from Lursoft. I would guess that the reason for why Globitex was the only one that asked for the history of the company might be that, since Globitex is a Latvian company, they might have a better idea of what to ask, when they saw that our company is also from Latvia.

One advantage of Globitex's registration process is that, you receive the full list of questions at the beginning of the whole registration process. Globitex had some questions that you had to answer online and some question that had to be answered after downloading them and then you had to upload the answers back. If I remember correctly, there were two such questionnaires. Additionally, what I noticed was that if you answer that you are a financial institution, when opening a corporate account in Globitex, you will see that they will ask you more questions than when opening a standard corporate account; thus it can be seen that they have adjusted the questionnaires to different types of customers, instead of just asking the same questions to all of their customers.

Additionally what I like about Globitex is that it is a local exchange; thus, if anything happens, it is much easier to reach them. In situation, if some transaction would not go through, we could easily drive to them and ask what other information they need in order to finish executing the transaction, while, for

example, Bitstamp does not provide such convenience. We even tried to do a Skype call with the employees of Bitstamp, but nobody would even consider such possibility, they just acted as I did not suggest anything. We tried the same with Mistertango, but they also did not want to do any video calls. It probably is because of the large demand they are experiencing. Therefore they simply does not have the capacity to perform video calls with their customers. Thus we chose to do the first exchanges through Globitex, even though we already had an account in Bitstamp.

**Anrijs:** Ok. Thank you for the great insights into the registration process! Did you encounter any additional means of identification besides filling out forms and uploading documents?

**CEO:** What we discovered was that Mistertango does not allow to use many bank accounts for one exchange account. For the Mistertango I additionally had to send 1 or 10 euro for the identification purposes and to assign the bank account we are going to be using for the exchange services. This ensured that we will not use the account to service some third parties. The third party servicing is one of the risks that the exchanges could be exposed to, since the new SEPA standard does not require comparing the names of the bank account holders with the bank account numbers. If the bank account numbers are correct, the money has to be transferred. This means that the only way how they can make sure of the account holders identity is to ask for a transfer of money.

**Anrijs:** How much time it took for each of the exchanges to finalize the registration process?

**CEO:** Globitex was the fastest in terms of accepting the creation of account. We got an acceptance in one day after the first round of conversation through e-mails.

Regarding Mistertango, we have not yet concluded the registration process. It is still in progress. It is due to the communication, which has been the slowest. At one moment they disappeared for one week and did not respond to any of our e-mails.

With the Bitstamp we were able to arrange that they move us forward in the waiting list for the account opening. Currently, in a normal situation, people have to wait in lines for up to three months just to begin the registration process. The situation is the same even for natural persons. Since we had arranged the accelerated process of registration, we received the initial list of questions in a couple of days after filling out a form with personal information and after that pretty much every day we received new questions that we had to answer; thus the iterations were very quick. Of course, sometimes we could not give an



answer at the same day of receiving the question, since we had to wait for notarial confirmations for some of the documents.

**Anrijs:** Why do you think they have these very long waiting lists?

**CEO:** Because they are receiving so many registration requests that they simply cannot process them in time due to the collection of customer data.

**Anrijs:** So they are probably processing all of the customer identification data manually?

**CEO:** It seems so. At least from the information that I got from one of the exchanges, it seems that they do not have much of an understanding of how to properly organize identification processes and what specific data should be collected for the identification purposes. It seems that they are learning by doing at this point.

**Anrijs:** Is it that they have implemented too rigid identification measures or the opposite?

**CEO:** It is more regarding the new regulations that will come into force and they do not know what will relate to them and what will not; thus they do not know how to proceed further. However, I would argue that the questions that we were asked could be even more detailed than you get asked at the banks, when you open account there. If not more detailed, then at least in less structured manner definitely; thus reducing the user-friendliness. In banks at least some of the information would be gathered automatically through other sources and would not be asked directly to the customer. Additionally, in banks there is an employee that you can talk to and explain who you are and why you would like to open a bank account. And instead of you receiving a list of question that you have to answer to, you are interviewed by the employee and give or receive the response immediately, which definitively makes the whole process easier.

However, if you are signing up for a private account, there are not that many questions asked and the process is quite simple. I could compare it to signing up for Revolut or N26 account. Overall, as far as I have had an experience with different exchanges as a natural person, usually the process is very simple – you fill out a form with some personal information and send a utility bill or other document to verify the information and that is it.

**Anrijs:** Do you think that they were asking all of the questions due to some regulations?

**CEO:** I do not know. However, I would guess it is because of the pressure from the banks they are collaborating with. In order for them to be able to comply with the AML regulations, their business partners would have to comply as well. But at this point it is just a guess. What I have heard is that some exchange service providers choose to acquire a license for electronic money; thus they have to comply with the AML/CTF regulations. Additionally, it serves them as a way to conduct their business seemingly legally.

**Anrijs:** What about any additional documentation? Did you have to provide any when you performed large transactions? If I remember correctly, you told me that you had done some transactions with amount of more than 10 000 euro.

**CEO:** Since Globitex was the first one to accept our registration, we wrote them a question whether we are allowed to exchange cryptocurrency to euro in amount of 20 000 euro. The support gave as an answer that it is completely fine and they only start asking additional questions when the amount reaches 100 000 euro.

**Anrijs:** How about limits for the exchanges? Did you encounter any? Were you able to indicate the average amount that you are planning to exchange over some specific period of time?

**CEO:** We did indicate in the answers to the Bitstamp's initial questions that we will do transactions around 650 000 USD in a year. However, there is no place, where you could find the set limits; thus there is no way to know how much you are allowed to transact. In my personal account it was showed that the limit is 100 000 USD in a month or a week, I cannot remember, but the issue is that I have no idea whether I can exchange them easily in one transaction, or I need to separate them in multiple transactions, and what additional information they will ask for. I have no idea.

**Anrijs:** Ok. Thank you very much for your time and answers! I think that they will be very helpful for my thesis. For now, I think, it is going to be enough information. Have a great day!

**CEO:** Thank you! You too!

## **Appendix 10 – Customer data collection for natural persons in cryptocurrency exchanges**

# Bitstamp

### Open your free account


First Name  
Type here

Last Name  
Type here

E-Mail  
Type here

Country  
Select country...

I agree to Bitstamp's [Terms of Use](#) and [Privacy Policy](#)

I'm not a robot 

**REGISTER**

[Already registered? Log in.](#)

### Registration Complete

An email containing your customer ID and password has been sent to your e-mail address.

You should change your password as soon as you log in for the first time.

Welcome to Bitstamp News

Bitstamp <noreply@bitstamp.net> to me 3:27 PM (1 minute ago)

### Bitstamp

Dear Anrijs Daniels,





Thank you for registering at Bitstamp exchange service! At this point you have just contributed a great deal to future of decentralized monetary market. If you are not already a bitcoin user please read about the benefits that bitcoin is offering to modern society. Feel free to invite your friends and family members to Bitcoin community and learn about advantages that bitcoin is offering to users.

Please write down the following login information  
Client ID: ██████████  
Password: ██████████

The above password has been automatically generated. You should change it as soon as you log in for the first time.

If you have any questions regarding Bitstamp exchange service please read our FAQ or use our support form (<https://www.bitstamp.net/support/>). Our support staff will be more than happy to assist you.

Don't forget to follow us on your favorite social network.

Yours sincerely,  
Bitstamp team

### CHANGE PASSWORD

**YOUR PASSWORD IS TOO OLD. PLEASE CHANGE IT NOW.**

Current Password:

New Password:

Repeat New Password:

**CHANGE PASSWORD**

You can disable this password change prompt here.

### CHANGE PASSWORD

**YOU HAVE SUCCESSFULLY CHANGED YOUR PASSWORD.**

**TO VERIFY YOUR ACCOUNT PLEASE CLICK HERE**

Current Password:

New Password:

Repeat New Password:

**CHANGE PASSWORD**

You can disable this password change prompt here.

## VERIFY ACCOUNT

STATUS: UNVERIFIED

Are you an individual? Then click "Personal Account Verification".

Are you representing a company or institution? Then click "Corporate Account Verification".

PERSONAL ACCOUNT VERIFICATION

CORPORATE ACCOUNT VERIFICATION

## PERSONAL ACCOUNT VERIFICATION < Back

**PERSONAL INFORMATION:**

**IMPORTANT: Enter your name into the fields exactly as it appears on your identity document (full first name, any middle names/initials, and full last name(s))**

First Name:  Last Name:

Address:

Postal Code:  City:

Address:

Postal Code:  City:

Country:  Nationality:

Birth Date:

Under the Foreign Account Tax Compliance Act (FATCA) foreign financial institutions are obliged to report financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

In order to comply, we kindly ask you to provide the information below.

I hereby declare: ?

I am a US citizen  Yes  No

I am a US resident alien  Yes  No

I am a US tax person for any other reason  Yes  No

**ID DOCUMENT:**

Please make sure that your submitted documents are:

**HIGH QUALITY** (colour images, 300dpi resolution or higher).  
**VISIBLE IN THEIR ENTIRETY** (watermarks are permitted).  
**VALID**, with the expiry date clearly visible.

**Please do not submit the identity document as your proof of residence.**

Photo ID Document: ?

Please make sure that your submitted documents are:

**HIGH QUALITY** (colour images, 300dpi resolution or higher).  
**VISIBLE IN THEIR ENTIRETY** (watermarks are permitted).  
**VALID**, with the expiry date clearly visible.

**Please do not submit the identity document as your proof of residence.**

Photo ID Document: ?

No file chosen

Back Side Photo ID Document:

No file chosen

ID Document Issue Date:    ID Document Expiration Date:

ID Document Number:  ID Document Type:

ID Document Number:  ID Document Type:

**PROOF OF RESIDENCE DOCUMENT:**

To avoid delays when verifying your account, please make sure:

Your **NAME, ADDRESS, ISSUE DATE** and **ISSUER** are clearly visible.  
 The submitted proof of residence document is **NOT OLDER THAN THREE MONTHS**.  
 You submit color photographs or scanned images in **HIGH QUALITY** (at least 300 DPI)

**Do not resubmit identity document as proof of residence.**

**AN ACCEPTABLE PROOF OF RESIDENCE IS:**

- A bank account statement.
- A utility bill (electricity, water, internet, etc.).
- A government-issued document (tax statement, certificate of residency, etc.).

**We cannot accept the address on your submitted identity document as a valid proof of residence.**

The submitted proof of residence document is **NOT OLDER THAN THREE MONTHS**.  
 You submit color photographs or scanned images in **HIGH QUALITY** (at least 300 DPI)

**Do not resubmit identity document as proof of residence.**

**AN ACCEPTABLE PROOF OF RESIDENCE IS:**

- A bank account statement.
- A utility bill (electricity, water, internet, etc.).
- A government-issued document (tax statement, certificate of residency, etc.).

**We cannot accept the address on your submitted identity document as a valid proof of residence.**

Proof Of Residence: ?

No file chosen

SUBMIT VERIFICATION REQUEST

## VERIFY ACCOUNT

STATUS: PENDING

THANK YOU FOR SUBMITTING YOUR REQUEST. UNFORTUNATELY, WE ARE CURRENTLY EXPERIENCING HIGH VOLUMES OF VERIFICATION REQUESTS, CAUSING BACKLOGS OF UP TO 2 WEEKS BEFORE THEY ARE PROCESSED. WE ARE WORKING VERY HARD TO APPROVE YOUR REQUEST AS QUICKLY AS POSSIBLE. THANK YOU FOR YOUR PATIENCE.

We recommend that you fill in our [KYC questionnaire](#) while you wait for your account to be verified. The questionnaire will enable us to process your future fiat transactions faster.

### ADDITIONAL INFORMATION

Please help us better understand your intended Bitstamp account usage by providing the information requested below, as a part of our AML/CTF regulatory obligations. Make sure the submitted information is correct and up to date, as this may result in faster processing of your transactions.

**FINANCIAL**

Your current occupation:

Your annual income:

Your annual income:

Your net worth:

Your source of funds:

Your annual deposit estimation:

Your annual transaction number estimation:

**ACTIVITY**

What are your intended activities on our platform?

- Arbitrage
- Investing
- Trading
- Reselling (Broker / Dealer) related activities
- Online gambling related activities
- Buying/Selling goods or services

Do you intend to cash out at Bitstamp?  
 Yes  No

- Investing
- Trading
- Reselling (Broker / Dealer) related activities
- Online gambling related activities
- Buying/Selling goods or services

Do you intend to cash out at Bitstamp?  
 Yes  No

**SUBMIT**

### ADDITIONAL INFORMATION

Please help us better understand your intended Bitstamp account usage by providing the information requested below, as a part of our AML/CTF regulatory obligations. Make sure the submitted information is correct and up to date, as this may result in faster processing of your transactions.

Your current profession:

Accountancy	Education
Administrative	Emergency services
Agriculture	Financial services - Banking
Arts/Entertainment/Media	Financial services - Insurance
Broker/Dealer	Financial services - Other
Catering/Hospitality/Tourism	Government
Construction/Real Estate	Health care/Medical
<b>Education</b>	Information technology
Emergency services	Legal
Financial services - Banking	Manufacturing
Financial services - Insurance	Marketing
Financial services - Other	Military
Government	Pensioner
Health care/Medical	Retail sales
Financial services - Other	Financial services - Other
Your annual income:	Your annual income:
From \$10,000 to \$50,000	From \$10,000 to \$50,000
Your net worth: ?	Your net worth: ?
Up to \$50,000	Up to \$50,000

**FINANCIAL**

Your current occupation:

Employed

Up to \$10,000

**From \$10,000 to \$50,000**

From \$50,000 to \$150,000

From \$150,000 to \$300,000

More than \$300,000

From \$10,000 to \$50,000

Your net worth: ?

Up to \$50,000

Your current profession:

Financial services - Other

Your annual income:

From \$10,000 to \$50,000

Your net worth: ?

Up to \$50,000

**Up to \$50,000**

From \$50,000 to \$200,000

From \$200,000 to \$500,000

From \$500,000 to \$1,000,000

More than \$1,000,000

Salary

- Dividends
- Inheritance
- Savings
- Investment
- Gift
- Mining
- Real estate
- Loan

Salary

Your annual deposit estimation:

Up to \$10,000

Your annual transaction number estimation:

Select

Your annual transaction number estimation:

Select

Select

- Less than 5
- 5 to 10
- 10 to 20
- 20 to 50
- More than 50

- Reselling (Broker / Dealer) related activities
- Online gambling related activities
- Buying/Selling goods or services

Do you intend to cash out at Bitstamp?

- Trading
- Reselling (Broker / Dealer) related activities
- Online gambling related activities
- Buying/Selling goods or services

Do you intend to cash out at Bitstamp?

Yes  No

What is the origin of your crypto assets?

- Investment / Trading proceeds
- Mining proceeds
- ICO proceeds
- Salary / Dividends received in crypto
- Gambling / Gambling proceeds
- CSGO proceeds

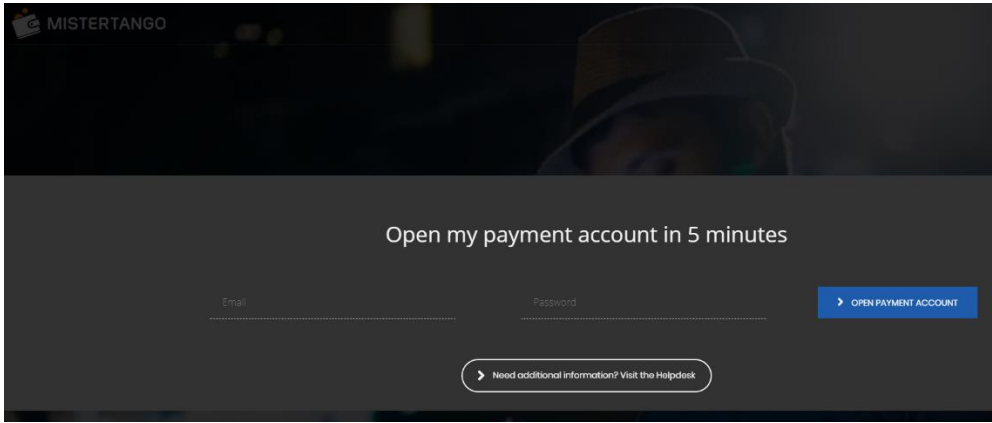
- Trading
- Reselling (Broker / Dealer) related activities
- Online gambling related activities
- Buying/Selling goods or services

Do you intend to cash out at Bitstamp?


Yes  No

**SUBMIT**

**Mistertango**



Mistertango: Account verification Inbox x

 **Mistertango** <no-reply@mistertango.com>  
to me



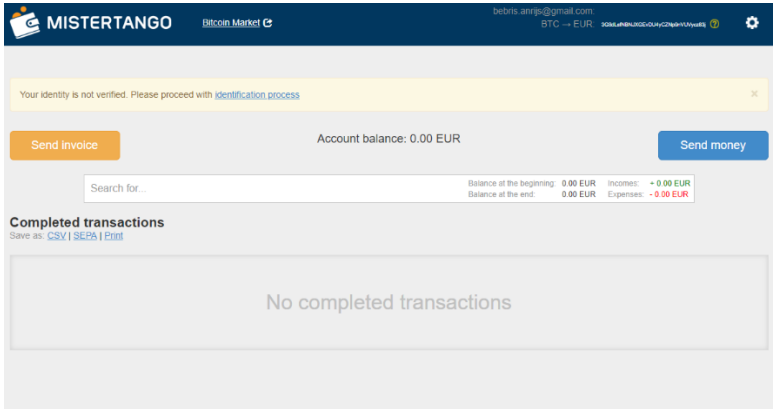
Dear customer,

In order to verify your email please click this link:  
<https://bank.mistertango.com/en/profile/verify>

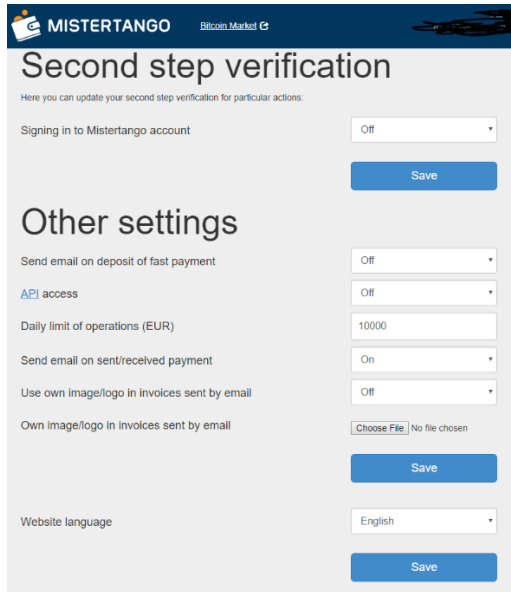
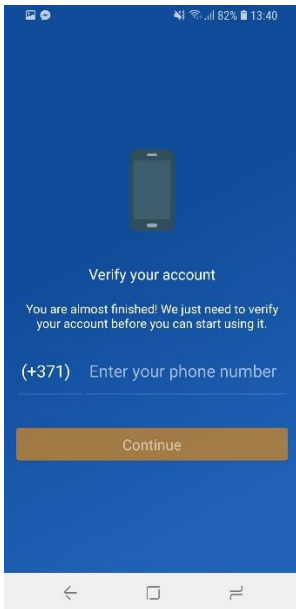
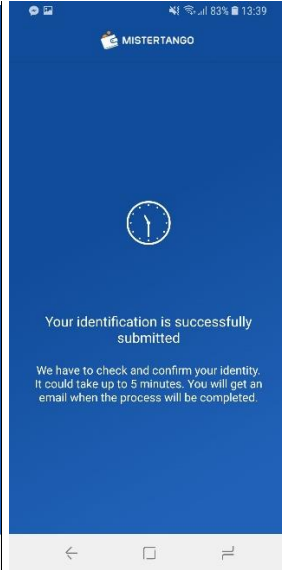
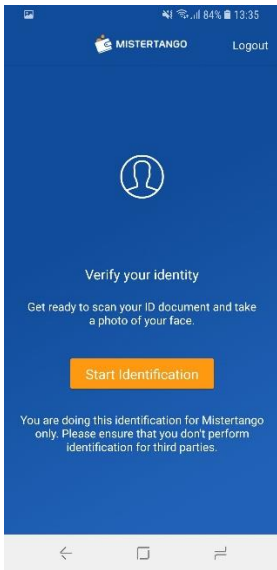
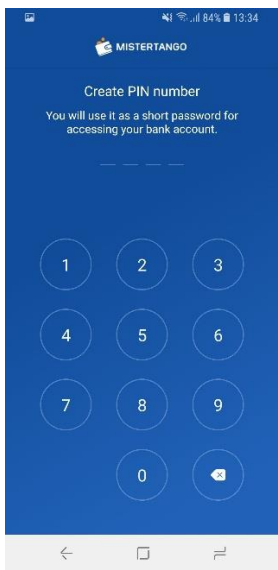
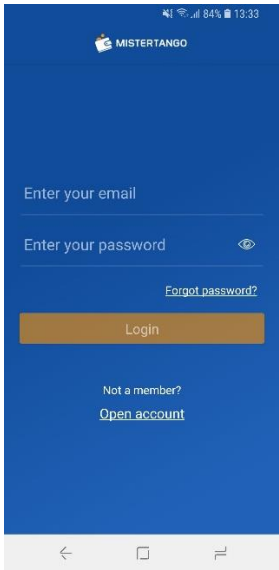
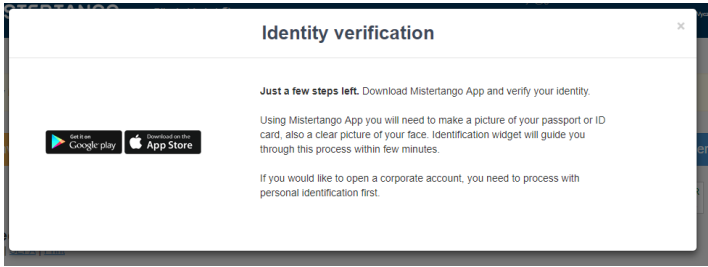
Verification link is valid for 1 hour.  
Date created: 2018-05-07 00:50:02.

Sincerely,  
Mistertango Team  
<https://mistertango.com>

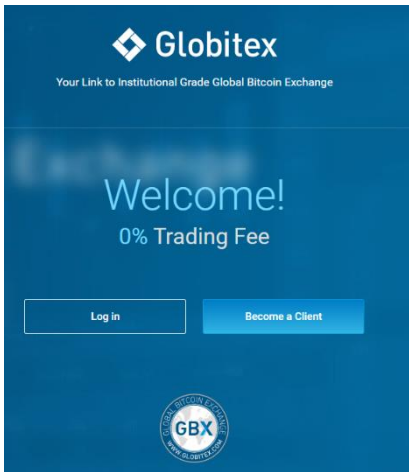
P.S. Payment accounts: <https://mistertango.com/en/bank-account/>  
MasterCard payment card: <https://mistertango.com/en/mastercard/>  
Payment card acquiring for your e-shop: <https://mistertango.com/en/credit-card-processing/>  
Automate your payments with API: <https://mistertango.com/en/api/>







Globitex



Registration Form

New Client | E-mail Verification | Phone Number Verification | 2-Factor Authenticator

New Client

Email address

Username

Password

Password confirmation

Submit

Registration Form

E-mail Verification | Phone Number Verification | 2-Fa

E-mail verification

An e-mail with a verification code has been sent to [redacted]@gmail.com. Please check and enter the code below.

Enter e-mail verification code

Registration Form

New Client ✓ | E-mail Verification ✓ | Phone Number Verification | 2-Factor Authenticator

Phone number verification

LV +371 Country calling code

Phone number

Submit

Registration Form

New Client ✓ | E-mail Verification ✓ | Phone Number Verification | 2-Factor Authenticator

← Phone number verification

An SMS with a verification code has been sent to +371 [redacted]. Please check and enter the code below.

Enter code

Resend code | Submit

2-Step Verification

Use Google Authenticator App



Scan the QR Code or enter the Secret Key manually





DNMEMQJRRXLHUHKX  
Secret Key

Enter one-time password

Submit Need help?

Choose account type

  
**Personal account**  
For private individual

  
**Corporate account**  
For representative of a legal entity

← Submit compliance data

Personal info ↓ Collapse

Given / Other name(s) ⓘ

Surname ⓘ

Date of Birth > ⓘ

Gender ⓘ

Country of citizenship ⓘ

+ Add one more citizenship

Residence address ↓ Collapse

Country ⓘ

Address ⓘ

City / Place ⓘ


State / Province ⓘ

Postal code / ZIP ⓘ

Accept General Terms

Submit

Success



Application submitted

Ok

Account Status

Net Asset value (NAV): EUR 0

Activity during last 12 months

Deposits: XBT 0

Withdrawals: XBT 0

Your account is ready for business.

Tutorials

- Exchange Tutorial: Learn here how the exchange platform works
- Accounts Tutorial: Coming soon
- Reports Tutorial: Coming soon

Trading Fee Schedule

Account Level Upgrade

Advanced

Limits  
EUR 15 000

Requirements  
Basic information disclosure

Upgrade

Unlimited<sup>∞</sup>

Limits  
Unlimited

Requirements  
Full personal information disclosure

Upgrade

Accounts

All accounts | All currencies | Total balance in EUR

View recent payments in Reports

Account	Currency	Pay-in	Pay-out	Available	Reserved	Total	Total in EUR
[Redacted]	BCH	↓	↑	0.00000000	0.00000000	0.00000000	0.00
	EUR	↓	↑	0.00	0.00	0.00	0.00
	XBT	↓	↑	0.00000000	0.00000000	0.00000000	0.00

+ Create new account

Submit compliance data for Unlimited account

Personal information

Country of birth

Personal identification number

Identification number country

Are you USA tax resident?

Tax residence country

Tax ID number

Financial data

Are you beneficial owner?

Purpose of account:

- Saving
- Investment
- Trading
- Speculation
- Hedging
- Other

Estimated annual deposit (EUR)

Occupation

- Source of wealth:
- Employment
  - Self-employment
  - Retirement / pension / social benefits
  - Inheritance
  - Interest
  - Real estate / rental income
  - Trading & Investments
  - Unemployment
  - Savings
  - Other

Are you politically exposed person?

Identity document

Select document type

Upload identity document file

Description of uploaded identity document...

Proof of funds

Select proof of funds

Upload proof of funds document file

Description of uploaded proof of funds document...

Proof of residence

Select proof of residence

Upload proof of residence document file

Description of uploaded proof of residence document...

Accept General Terms

[Submit compliance data for Advanced account](#)

Personal information ↑ Collapse

Identity document ↑ Collapse

[Upload identity document files](#)

[Accept General Terms](#)

## Appendix 11 - Customer data collection for legal entities in cryptocurrency exchanges

### Bitstamp

Open your free account


First Name

Last Name

E-Mail

Country

I agree to Bitstamp's [Terms of Use](#) and [Privacy Policy](#)

I'm not a robot 

[Already registered? Log in.](#)

**Registration Complete**

An email containing your customer ID and password has been sent to your e-mail address.

You should change your password as soon as you log in for the first time.

### Bitstamp

Dear Anrijs Debris,

Thank you for registering at Bitstamp exchange service! At this point you have just contributed a great deal to future of decentralized monetary market. If you are not already a bitcoin user please read about the benefits that bitcoin is offering to modern society. Feel free to invite your friends and family members to bitcoin community and learn about advantages that bitcoin is offering to users.

Please write down the following login information

Client ID: [REDACTED]  
Password: [REDACTED]

The above password has been automatically generated. You should change it as soon as you log in for the first time.

If you have any questions regarding Bitstamp exchange service please read our FAQ or use our support form (<https://www.bitstamp.net/support/>). Our support staff will be more than happy to assist you.

Don't forget to follow us on your favorite social network.



Yours sincerely,  
Bitstamp team

## CHANGE PASSWORD

YOUR PASSWORD IS TOO OLD. PLEASE CHANGE IT NOW.

Current Password:

New Password:

Repeat New Password:

You can disable this password change prompt [here](#).

## CHANGE PASSWORD

YOU HAVE SUCCESSFULLY CHANGED YOUR PASSWORD.

TO VERIFY YOUR ACCOUNT PLEASE CLICK [HERE](#).

Current Password:

New Password:

Repeat New Password:

You can disable this password change prompt [here](#).

## FORMATION

and your intended Bitstamp account usage by providing the information for our AML/CTF regulatory obligations. Make sure the submitted information is accurate and complete to avoid any result in faster processing of your transactions.

## VERIFY ACCOUNT

STATUS: UNVERIFIED

Are you an individual? Then click "Personal Account Verification".

Are you representing a company or institution? Then click "Corporate Account Verification".

Your annual transaction number estimation:

Select

**ACTIVITY**

What are your intended activities on our platform?

Arbitrage

Investing

Trading

Reselling (Broker / Dealer) related activities

Online gambling related activities

Buying/Selling goods or services

Do you intend to cash out at Bitstamp?

Yes  No

**SUBMIT**

Do you intend to cash out at Bitstamp?

Yes  No

What is the origin of your crypto assets?

Investment / Trading proceeds

Mining proceeds

ICO proceeds

Salary / Dividends received in crypto

Gambling / Gambling proceeds

CSGO proceeds

**SUBMIT**

**CORPORATE ACCOUNT VERIFICATION** ← Back

**COMPANY INFORMATION:**

General Information:

Company Name:  Company Number:

Company Website (URL):  Tax ID:

(If Applicable) (If Applicable)

Registered Address:  Office Address:  Same As Registered Address:

Address:

City:

State:  State:

(Of Applicable) (Of Applicable)

Select state...  Select state...

Postal Code / Zip Code:  Postal Code / Zip Code:

Country:  Country:

Select country...  Select country...

**What is The Main Purpose Of Your Corporate Account?**

Accepting or converting payments from customers for services rendered or goods sold.

Depositing or withdrawing funds to business bank accounts.

Managing funds of other individuals.

Any other business activity (specify):

Click submit and a dedicated account representative will be in contact with you to process your application.

**SUBMIT VERIFICATION REQUEST**

Thank you for your interest in opening a corporate account at Bitstamp.

In order to continue with your corporate account verification, please provide company-related documents and information specified below.

Kindly note that the specified documents are the general documents that are required. If the documentation for your company is named differently than the documents we specify, please provide documents that disclose the ownership and management structure applicable to your company type.

**Documents**

(i) Certificate of Incorporation.

(ii) Memorandum and Articles of Association; OR any other relevant founding documents.

(iii) Annual return, listing company directors and beneficial shareholders of the last fiscal year. OR similar documents confirming company ownership and management.

(iv) Resolution of the Board of Directors to open an account with Bitstamp.

(v) List of authorized persons to operate the account (if applicable).

(vi) Authorization for other persons to manage your account (if applicable).

(vii) Recently issued bank account statement addressed to your company name and office address.

(viii) High resolution images of the international passport and proof of residency document of at least two members of the board of directors.

(ix) High resolution images of the international passport and proof of residency document of all owners with a company share of 10% or higher.

Proof of residency is a scanned image of a physical document such as a:

bank statement (credit card statements not accepted),

utility bill for utilities consumed at the applicant's home address,

tax return or council tax,

certificate of residency issued by your respective government or a local government

authority.

related document that verifies your residence: government-issued documents, judicial authority-issued documents, documents issued by a public agency / authority, utility services company documents, or similar regulated service-providing companies.

**IMPORTANT:** Please provide high resolution document images. We only accept PDF, JPEG or PNG format.

Please also provide the following additional information:

1. How do your customers typically reach you?

2. Is your business publicly listed on a recognized stock exchange?

If yes, please provide your membership ID.

3. List of company shareholders.

Please provide information on the beneficial share ownership including the percentage of shares each beneficiary owns (Please note that we require documents that disclose the ownership structure up to the final beneficial owners).

Please identify all parties with beneficial voting rights for trusts.

4. Company business activity

Please provide a detailed description of your company's activity, who/ service you provide, your typical customer profile, what type of payments you accept and how your services are priced.

5. Is your business AML regulated?

If so, what is your specific policy? How do you perform KYC for your customers? Please provide us with a copy of your AML policy.

6. What is the purpose of you opening a Bitstamp account?

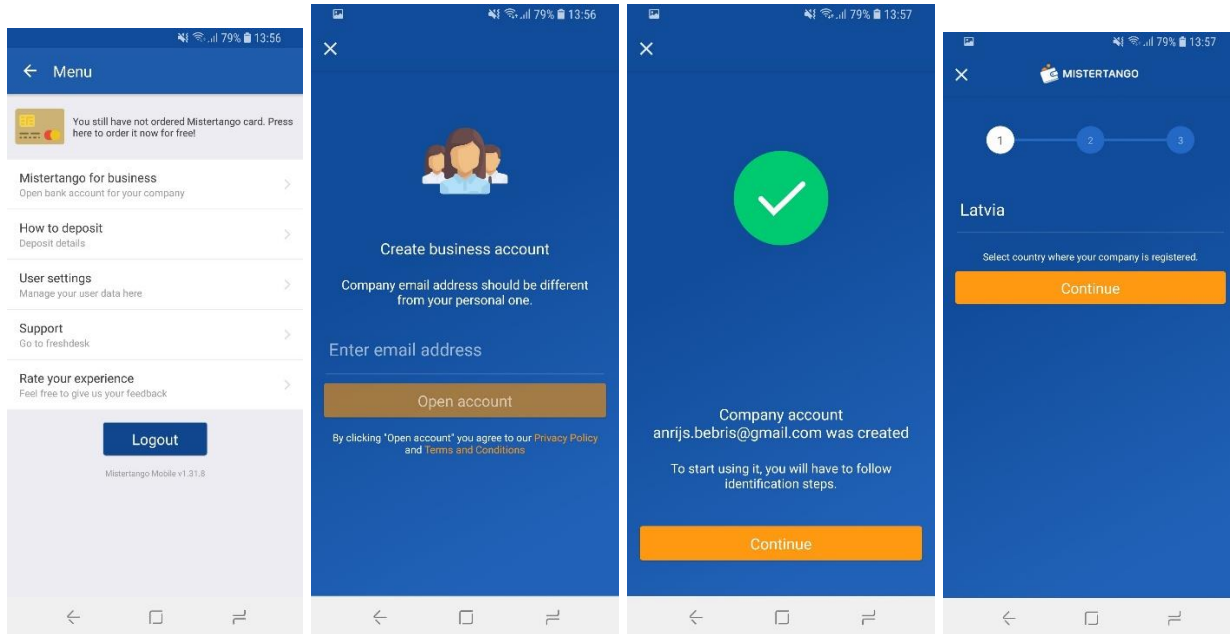
Please describe in as much detail as possible how you intend to use your trading account.

7. Source of funds.

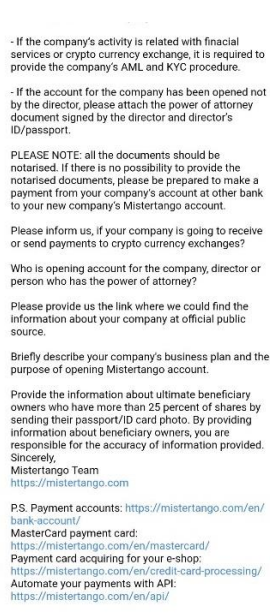
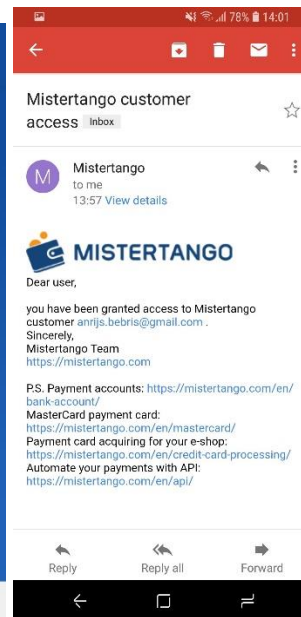
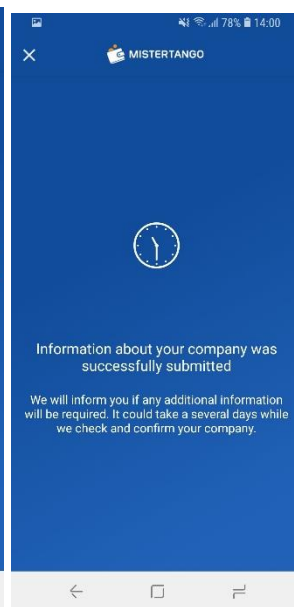
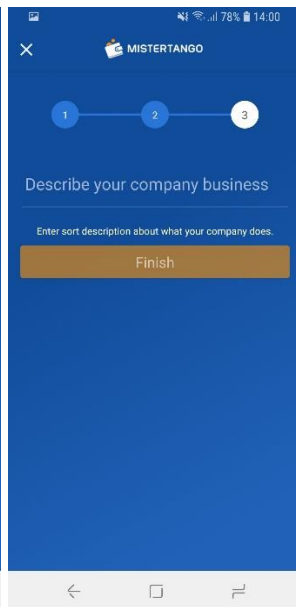
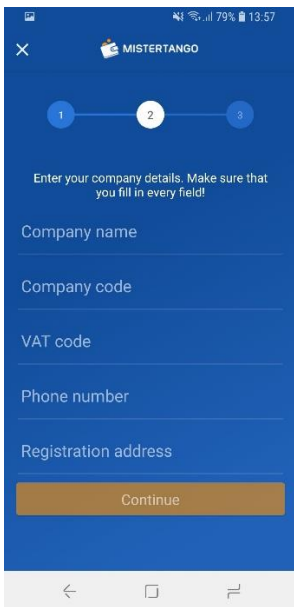
How were your funds acquired?

8. Name, address and SWIFT code of your bank.
9. Estimated monthly volumes, amounts (in USD and BTC) and frequency.
10. What type of trading will be conducted through your Bitstamp account?
11. Do you already have an account with any other bitcoin exchange?

## Mistertango







Globitex

**Globitex**  
Your Link to Institutional Grade Global Bitcoin Exchange

**Welcome!**  
0% Trading Fee

[Log in](#) [Become a Client](#)

Registration Form

[New Client](#) [E-mail Verification](#) [Phone Number Verification](#) [2-Factor Authenticator](#)

[New Client](#)

[Submit](#)

Registration Form

[New Client](#) ✓ [E-mail Verification](#) [Phone Number Verification](#) [2-Factor Authenticator](#)

[E-mail verification](#)

An email with a verification code has been sent to [\[redacted\]@gmail.com](#)  
please check and enter the code below

[Resend code](#) [Verify](#)

Registration Form

[New Client](#) ✓ [E-mail Verification](#) ✓ [Phone Number Verification](#) [2-Factor Authenticator](#)

[Phone number verification](#)

Country calling code

[Submit](#)

Registration Form

[New Client](#) ✓ [E-mail Verification](#) ✓ [Phone Number Verification](#) [2-Factor Authenticator](#)

[Phone number verification](#)

An SMS with a verification code has been sent to [+371 \[redacted\]](#)  
please check and enter the code below

[Resend code](#) [Submit](#)

Registration Form

[New Client](#) ✓ [E-mail Verification](#) ✓ [Phone Number Verification](#) ✓ [2-Step Verification](#)

[2-Step Verification](#)

Use Google Authenticator App

Scan the QR Code or enter the Secret Key manually

QR code

DNMEMQJRRXLHUHXX  
Secret Key

Enter one-time password

[Submit](#) [Need help?](#)

[Choose account type](#)

**Personal account**  
For private individual

**Corporate account**  
For representative of a legal entity

[Submit compliance data](#)

• Representative information ↑ Collapse

Given / Other name(s)

Surname

Representative role

• Corporate information ↑ Collapse

Name of legal entity

Name in original language

Legal form of entity

Registration date

Registration number

Tax residence country

Tax identification number

• Registered address ↓ Expand

• Business address ↓ Expand

• Financial data ↓ Expand

• Proof of funds ↓ Expand

• Account opening form ↓ Expand

• Account opening resolution ↓ Expand

• ID copies of representatives and shareholders ↓ Expand

• Incorporation documents ↓ Expand

Accept [General Terms](#)

• Registered address T Collapse

Country

Address

City / Place

State / Province

Postal code / ZIP

• Business address T Collapse

Country

Address

City / Place

State / Province

Postal code / ZIP

Business phone number

Business e-mail address

• Financial data T Collapse

Purpose of account:  Saving  
 Investment  
 Trading  
 Speculation  
 Hedging  
 Other

Other ...

Estimated annual deposit (EUR)

Origin of funds:  Share capital  
 Loan  
 Business income  
 Sale of assets  
 Client assets  
 Other

Other ...

Business activities:

Description of activities...

- Proof of funds T Collapse

Select proof of funds ▼

[Upload proof of funds document files](#)

Description of uploaded proof of funds document ...

- Account opening form T Collapse

**Account opening form**  
Press to download

[Upload account opening form](#)

- Account opening resolution T Collapse

**Account opening resolution**  
Press to download

[Upload resolution data](#)

- ID copies of representatives and shareholders T Collapse

[+ Add new identification document](#)

- Incorporation documents T Collapse

[+ Add new incorporation document](#)

Accept [General Terms](#)

Submit

## **Globitex** Directors Resolutions

The undersigned being the director(s) of Company name,  
 registered in Registration number a Company existing under the laws of the Country  
 do hereby certify that the following resolutions hereby are duly adopted in accordance with the procedures set forth in the Articles of Association of the Company and that said resolutions have not been amended or revoked, and are in no way in conflict with any of the provisions of the Company's Articles of Association.

- It was resolved:
- The following person is authorised on behalf of the Company.
- Name and surname, identity number and position
- to accept and sign any documents related to opening, maintaining and closing Company's account with Globitex;
  - to deposit and withdraw cryptocurrency and fiat currency funds to/from the account opened in the name of the Company with Globitex;
  - to buy and sell cryptocurrencies against fiat currencies and vice versa in the Company's account with Globitex;
  - to receive notices, confirmations, requests, reports and other communications of any kind in relation to Company's account or relations with Globitex;
  - to provide information and represent the Company in respect of any claims, requests or disputes;
  - to enter into legally binding arrangements, make decisions and act in relation to any of the foregoing matters.
- These listed powers shall not in any way limit or affect other authority, which the named representative might otherwise have.
- Any past transactions or dealings of any kind with Globitex on behalf of the Company are hereby approved and ratified.
  - Globitex is authorised to act upon the authority of these resolutions until receipt in writing of a revised or modified resolutions which is duly signed by the authorised representatives.

<small>Signature of authorized person</small>	<small>Signature of authorized person</small>
<small>Name, surname</small>	<small>Name, surname</small>
<small>Date</small>	<small>Date</small>

## **Globitex** Account Opening Form supplement for legal entities

In addition to the electronic account opening form, please complete this supplemental form, print and sign below, then scan and upload the form on Globitex website to complete the registration process.

### 1/6 Company information

Company name

Registration country

Registration number

Company's business activity requires a licence: Yes  No

If YES, provide details about activity of licence and regulator

Company's shares are publicly listed on a stock exchange: Yes  No

If YES, provide details about the listing exchange

### 2/6 Company representatives

Please, indicate all directors or other persons legally authorised to represent the company. If you have more than 4 representatives, add additional pages to cover all representatives. In addition you are required to upload personal identification document (passport or ID card) copies of each representative. If there are more than four company representatives, please copy this page to include all persons.

<small>1. Name, Surname</small>	Yes <input type="checkbox"/> No <input type="checkbox"/>
<small>Personal identification number</small>	<small>Position (office)</small>
<small>Residential address</small>	
<small>2. Name, Surname</small>	Yes <input type="checkbox"/> No <input type="checkbox"/>
<small>Personal identification number</small>	<small>Position (office)</small>
<small>Residential address</small>	
<small>3. Name, Surname</small>	Yes <input type="checkbox"/> No <input type="checkbox"/>
<small>Personal identification number</small>	<small>Position (office)</small>
<small>Residential address</small>	
<small>4. Name, Surname</small>	Yes <input type="checkbox"/> No <input type="checkbox"/>
<small>Personal identification number</small>	<small>Position (office)</small>
<small>Residential address</small>	

If any of representatives is a PEP, please provide details

PEP or publicly exposed person is a person entrusted with government public functions (either in domestic institutions or international organisations), or an immediate family member or close associate of such person.

### 3/6 Company shareholders

Please provide information about the Company's shareholders who hold 25% or more shares. If no shareholder holds 25% of the total issued shares, please, indicate 3 largest shareholders. In addition, please upload identification documents (passport or ID card copies for these individuals and registration documents for entities) of each shareholder below. If the Company is publicly listed on a stock exchange, you can skip this point.

1. Name, Surname / Company name	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number / Registration number	PEP status	US person*
Residential address / Registration address	Shareholding in %	
2. Name, Surname / Company name	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number / Registration number	PEP status	US person*
Residential address / Registration address	Shareholding in %	
3. Name, Surname / Company name	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number / Registration number	PEP status	US person*
Residential address / Registration address	Shareholding in %	
4. Name, Surname / Company name	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number / Registration number	PEP status	US person*
Residential address / Registration address	Shareholding in %	

If any of the shareholders is a PEP, please provide details

PEP or politically exposed person is a person entrusted with prominent public functions (either in domestic institutions or international organisations) or an immediate family member or close associate of such person.

If the company is a part of a group of companies or a holding, please provide a description/scheme of the structure of the group or the holding: names of the companies, countries of registration, registration number and % of share ownership. If more space is needed, please add a separate page.

Details

\* US person typically is a citizen or resident of the United States, as well as partnership or corporation organised in the US.

### 4/6 Beneficial owners (individuals)

Please provide information about Company's beneficial owners. This information may be the same as "shareholders" in point 3/6, or different according to your corporate structure. Beneficial owners are individuals who ultimately own or control the legal entity through direct or indirect ownership or control over more than 25% of the shares or voting rights in the legal entity. If no person has beneficial ownership of at least 25%, indicate 3 largest beneficial owners. If Company is publicly listed on a stock exchange, skip this point. In addition you are required to upload identification documents (passport or ID card copies) of each beneficial owner below.

1. Name, Surname	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number	PEP status	US person*
Residential address	Beneficial ownership in %	
2. Name, Surname	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number	PEP status	US person*
Residential address	Beneficial ownership in %	
3. Name, Surname	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number	PEP status	US person*
Residential address	Beneficial ownership in %	
4. Name, Surname	Yes <input type="checkbox"/> No <input type="checkbox"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Personal identification number	PEP status	US person*
Residential address	Beneficial ownership in %	

If any of beneficial owners is a PEP, please provide details

PEP or politically exposed person is a person entrusted with prominent public functions (either in domestic institutions or international organisations) or an immediate family member or close associate of such person.

#### 6/6 Declaration

The above Client hereby declares and certifies that the information provided on this form is, to the best of its knowledge, accurate and complete. The Client hereby agrees to provide Globitex upon request with any information or documentation which is required. The Client further undertakes to notify Globitex immediately of any change to the above information. Provided information may be used for reporting purposes according to the applicable law. Client hereby agrees to be bound by the General Terms and Conditions of Globitex (in the latest version published on the Globitex website).

#### 5/6 Tax status and self-certification

Please indicate all countries where the legal entity is registered as a tax resident or pays taxes

Country	Tax identification number (TIN)
Country	Tax identification number (TIN)
Country	Tax identification number (TIN)

Provide the entity status related to the business performed by ticking one of the appropriate boxes below

##### Financial Institution

- Company is a regulated professional financial institution (e.g. bank, insurance company, investment fund etc.)

##### Active Non-Financial Entity

More than 50% of gross income and assets derives from other than passive income, for instance sales of goods and/or services

- Corporation whose shares are regularly traded on one or more established securities markets or a related entity of such a publicly traded corporation
- A Governmental Entity or an International Organisation
- The entity is an Active NFE other than above

##### Passive Non-Financial Entity

More than 50% passive income deriving from e.g. interest, dividends, return on investments

- An entity that neither is a Financial Institution nor an Active Non-Financial Entity

Signature of authorised person

Name, surname

Date

Signature of authorised person

Name, surname

Date

## Appendix 12 – Examples of products and services inherent risk ratings

Examples of Increased Risk Products & Services	Rating
Alternative Investment/Structured Products	Moderate/High
Trade/Export Finance	Moderate/High
International Private Banking/WM	High
International Correspondent Banking	High
- International Wires	High
- Pouch Services	High
- Precious Metals (Physical Delivery)	High
- Banknotes	High
- Payable-through Accounts	High
- Downstream Clearing	High
Special Use Accounts	High
International Brokered Deposits	High
Safe Deposit Services	High
Precious Metals (Delivery) Services	High
Unlimited Cards	High
Benchmark and Other Setting of Indices	High

Examples of Increased Risk Transactions	Rating
Significant/Unusual Cash/Cash Like	High
Pass-through Transactions	High
Nested accounts	High
International Wires to High Risk Countries	High
Suspected Shell Company Transactions	High
Rapid In/Out (High Velocity Turnover)	High
Unusual Wire Transfers	High
Smurfing	High
Suddenly Active	High
Other Unusual/Suspicious	High