THE THREAT OF MONEY LAUNDERING IN INTERMEDIATED SECURITIES SYSTEMS AND BITCOIN TRANSACTIONS

Ioannis Paraskevopoulos

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

Master of Science (MSc) in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law

Student name: **Ioannis Paraskevopoulos**

ID: **1104150034**

Supervisor: **Dr. Thomas Keijser**

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

February 2017

Thessaloniki Greece

Abstract

This dissertation was written as part of Master of Science (MSc) in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law at the International Hellenic University.

This dissertation notes the vulnerability of intermediated holding systems and bitcoin transactions to money laundering activities. It explains why the inherent features of the intermediated holding system are not in principle compatible with compliance procedures that would make investors' identities easily accessible at every tier of the holding chain for authorities engaged in fighting money laundering. It supports the proposition for a central register, within the existing framework of intermediated holding systems, where investors' identities will be recorded. Finally, accepts as necessary the Commissions' proposals for amendments to the 4th Money Laundering Directive, assessing that a totally unregulated trade in bitcoin would offer a vast field of action to criminals engaged in money laundering.

Foremost, I would like to express my sincere gratitude to Dr. Thomas Keijser for the academic guidance he provided me with for the purpose of writing this dissertation. His support has been invaluable in the true sense of the word. Moreover, his deep knowledge in the scientific field of intermediated securities combined with his patience, motivation and kindness, helped me conclude my work in the most optimal way. I could not have imagined having a better advisor and mentor for my thesis.

Ioannis Paraskevopoulos

15/2/2017

Contents

Introduction

The concealment of the origins of illegally obtained money is known as money laundering. While money laundering was originally associated typically with the proceeds from drug trafficking, it was subsequently connected with cash and any other financial asset acquired by any kind of illegal activity, including tax evasion. The methods of obscuring the trail that leads from the financial asset to the criminal and the source of the funds used to acquire the asset, vary depending on a number of factors. The rapid development of technology which enables dematerialized financial assets to be traded rapidly, especially when traded online, diminishes the ability of law enforcement authorities to detect the money laundering activity. Especially in the case of intangible assets, including dematerialized securities that are intermediated and bitcoin, the transactions take place in a highly complex and rapid manner that disassociates the asset from the investor or the user in the case of bitcoins. In this context, the degree of transparency regarding the identity of the investors or the bitcoin users becomes a critical factor for the authorities' ability to trace the criminals and the criminal activity that generated the illegal funds. The threat of money laundering activities in the framework of the two aforementioned areas will ultimately depend on the transparency requirements effective in relation to the personal information of investors in securities and bitcoin users alike.

CHAPTER 1: The EU anti-money laundering legislation

The ulterior motive of the vast majority of criminal actions lies without a doubt in acquiring illegal proceeds. The pillar stone both of past and more recent legislative initiatives in the fight against organized crime is the notion that, by limiting or eliminating the ability of criminals to circulate their proceeds of crime within the financial system and make a profit for themselves, the legislator would be successful in weakening the motives of potential criminals to engage in criminal actions. Furthermore, in line with the above reasoning, tracing financial assets of suspicious origins would contribute in tracing the crimes and the perpetrators. The current operative anti-crime model worldwide is based on the aforementioned strategy.

In particular, this strategy consists of setting-up law enforcement mechanisms by which seizures of property and of other financial assets are enabled, regardless of the nature of the financial assets and the time point at which these assets are discovered. Furthermore, part of the anti-money laundering strategy is the involvement of private entities and institutions, e.g. banks, upon which the legislator assigns the task to monitor and detect suspicious transactions that might be conducted for the purpose of money laundering. The legislator delegates law enforcement authorities not only to institutions holding key-positions in the financial market system, but also on natural persons who, due to their professional capacity, are likely to transact with criminals pursuing to legitimize their 'dirty' money, e.g. lawyers. Most importantly, the money laundering strategy is comprised by the creation of legal bases that render money laundering a distinct crime, i.e. a stand-alone crime punishable regardless of the punishment of the predicate offence, and the creation of legal bases that permit the confiscation of illicit proceeds by law enforcement authorities before the issuance of a court judgment[1].

In the context of EU Law, money laundering is seen as a threat to the soundness, integrity and stability of credit and financial institutions, and confidence in the financial system as a whole.[2] Between 1991 and 2005 three money laundering directives were adopted in 1991, 2001 and 2005 and it is notable that the initial focus of the 1st Directive was the laundering of the proceeds of certain drug offences, however the focus of the subsequent directives included a wider range of crimes and extended anti-money laundering obligations to a broader range of professions and activities.[3] On May 20 2015, the European Parliament and Council adopted a 4th Money Laundering Directive to be transposed into national law no later than June 2017. From June 26 2017 the 3rd directive currently in effect, and its implementation Directive (2006/70/EEC) will be revoked.

[1] T. Papakyriakou, (2017), 'The international regulatory framework for the prevention and suppression of money laundering: the rising and establishment of a new model of anti-crime policy' Lecture presented at the Seminar of Aristoteleion University of Thessaloniki Contemporary: 'Current legal issues of financial transactions' 2-4/2/2017

[2] 4th Money Laundering Directive, 2015/849/EU, preamble, para. (4)

[3] Rudi Fortson, 'Intensifying anti-money laundering laws-the last 30 years' [2016] Archbold Review, 4, 6-9

The 4th Money Laundering Directive applies to a range of business including banks, financial institutions, auditors and accountants. Its rules apply to other kind of businesses which make or receive cash payments for goods worth at least 10.000 euros regardless of the payment method. An important feature of the rules imposed by the Directive is, amongst others, the obligation of the Member States to set-up and maintain registers that record the ultimate beneficial owners of business. The registers will be accessible by national authorities and banks conducting due diligence into customers. On 5 July 2016, the European Commission proposed amendments to the 4th Money Laundering Directive, which have not entered into force until today. These changes provide for enhanced checks towards high risk third countries, enhancing the powers of Financial Intelligence Units and giving them swift access on bank and payment accounts, and, finally, they bring virtual currency exchange platforms under the scope of the Money Laundering Directive, as described below in the section of bitcoin regulation.[4]

CHAPTER 2: Vulnerabilities of the securities markets in relation to money laundering

Money laundering is usually described as consisting of three stages: Placement, layering and integration. However, not all money laundering transactions involve all three distinct phases and some may involve more (van Duyne 2003). The placement stage involves the physical movement of currency or funds produced by illegal activities to a place or form less suspicious to law enforcement authorities. Proceeds are introduced into financial institutions or into the retail economy. The second stage is characterized as layering and involves the separation of proceeds from their illegal source by using multiple complex financial transactions to obscure the audit trail and hide the funds. The third stage is called integration. Illegal proceeds are

[44] Barry Vitou, Michael Ruck and Elena Elia, 'Anti-money laundering: can money laundering really be prevented?' [2016] Compliance & Risk 2016, 5(5), 2-5

converted into apparently legitimate business profits through normal financial or commercial activities.[5]

Making proceeds appear as legitimate earnings from the financial markets would seem relatively easy within the borders of financial markets, given that frequent and numerous transactions involving securities take place, while at the same time these transactions are often international. Most financial participants do not accept cash transactions and consequently the securities sector will be exploited by criminals during the layering and integration stage. However, when the predicate offence takes place within the financial sector, as in the cases of insider trading or securities frauds, the non-cash funds are already present in the financial system and thus a placement stage is not necessary. During the layering phase, the criminal can simply acquire securities with 'dirty money' held in one or more accounts and then use the proceeds from this transaction as legitimate money.[6] In the case of bearer securities, i.e. securities that do not have a registered owner, the security's owner is simply the person who possesses it after the security having been handed over to that person, meaning that no paper trail exists that would allow authorities to easily detect the initial source of the funds used to acquire the security in question.

The so-called 'put' and 'call' transactions constitute another common laundering mechanism in the securities sector. A client pays with 'dirty money' for a financial transaction and the instructed broker places 'side bets' on a stock's gain or loss. The broker pays out the winning transaction with 'clean' money and destroys the losing transaction to avoid suspicion. The client may has merely broken even with this transaction in terms of losing or profiting, however profit is not the client's goal. The goal is to provide 'dirty money' as inflows in the financial market and get 'clean money' back at the end of the transaction. This type of transactions is commonly encountered in trading derivatives where the high volume of trading activity and a high degree of liquidity combined with the large number of brokers who trade the

[5] Peter Reuter and Edwin M. Truman, *Chasing Dirty Money – The Fight against Money laundering* (November 2004) chapter 3 p. 25

derivatives obscures the connection between each new participant and the original trade.[7]

Consequently, the securities market is a potentially attractive mechanism for money laundering. The attraction derives from the variety and complexity of the financial instruments traded, the ease and speed of transaction execution, e.g. online auctions, and the ability to execute international transactions. Securities can be used to 'break the chain' of documented transactions, to disguise the signs of illegal transactions and to justify high profits.[8] Suspicious transactions reporting in the sector remains relatively low because of the aforementioned inherent features of securities trading and possibly because of lack of awareness and insufficient securities-specific indicators.[9] The complexity of securities trading in the financial system seems much more acute in the case of intermediated securities where transparency issues arise as regards the identification of the beneficial owners.

CHAPTER 3: Money laundering in intermediated holding systems

In this chapter an analysis of the inherent characteristics of the intermediated holding system is attempted, in comparison to other holding systems, in order to establish why these very attributes of that particular holding system might potentially offer a more 'privileged' field of action for money launderers, given that its basic features do not promote the disclosure of the investors identity. Subsequently, the reasoning behind the proposal for a central register of investors within the intermediated holding system is analyzed.

3.1 Set-up of intermediated holding systems

Intermediated holding chains constitute a pillar stone of the global financial system. They contribute both in the development of economies of scale as regards the

[7] Stephen Schneider, 'Money Laundering through securities an analysis of Canadian Police cases' [2004] 4 Asper Rev. Int'l Bus. & Trade L. 169 2004

[8] Moneyval, *Typology research – Use of securities in money laundering schemes* (2008) Problem Overview Chapter 1 p. 9

[9] FATF, *Money Laundering and Terrorist Financing in the Securities Sector* (October 2009)

transactional costs, and in the increase of the securities mobility.[10] Indeed, the movement of huge amounts of capital between investors and governments and the financing of companies and financial organizations, both take place in an efficient, speedy and cost-effective manner thanks to the operation of a reliable intermediary holding system within a global financial market. The investors pursue future cash flows deriving from shares, bonds and other debt instruments. The rights issued to investors are negotiable and their value lies, to a great extent, on this very feature that enables investors to re-sell their rights to other investors in the capital markets.

The term "intermediated securities" refers to a holding system where banks and other financial institutions rely on central securities depositories (CSDs) for the safekeeping of their own securities and of their clients' securities. The physical delivery of securities, that used to take place in the past for the purpose of safekeeping or transfer, gave its way to a form of electronic book-keeping where securities are not delivered as moveable property but are rather credited or debited in securities accounts maintained by CSDs for their participating financial institutions. The participating financial institutions or "intermediaries" provide accounts for their client-investors and for their client-intermediaries and, in turn, those clients maintain accounts for other persons and so on, forming a securities holding chain that reaches down the ultimate account holder.[11] The transition from physical delivery of security to electronic means of transfer took place through the use of techniques that tackled the problem of too much paper, namely immobilization and dematerialization. Before an analysis of these techniques is attempted, certain terminology issues should be addressed.

In figure 1 below one can observe the illustration of the intermediated holding chain. Given that both in bibliography and in papers issued by international organizations, e.g. guidance, typology reports and other, some of the terms used to designate and

[10] Financial Crime Compliance Principles for Securities Custody and Settlement – Background and Overview, International Securities Services Association (ISSA), 6 October 2015, p.4 http://issanet.org/pdf/2015-10-05_ISSA_Background_Overview_Final.pdf

[11] Luc Thevenoz, 'The Geneva Securities Convention: objectives, history, and guiding principles' in Pierre – Henri Conac, Ulrich Segna and Luc Thevenoz (eds), *Intermediated Securities The Impact of the Geneva Securities Convention and the Future European Legislation* (Cambridge University Press 2013) p. 3-9

describe the participants of that chain might not be used under the same meaning or in the same context, the illustration below is useful in order to clarify the meaning of some of the terms employed in the present paper.

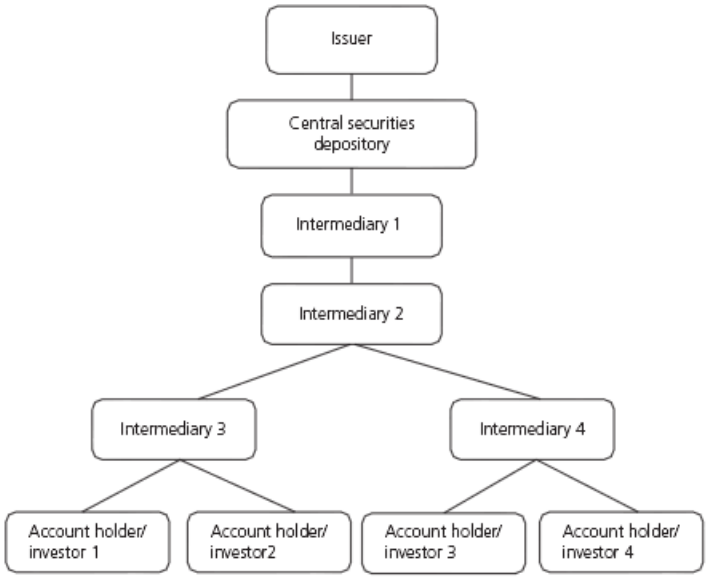

Figure 1: The intermediated holding chain

The above figure depicts the intermediated system in highly simplified form. Main actors who participate in the system is the issuer, the central securities depository (CSD), intermediaries and account holders or investors. Typical issuers of securities are governments, in the case of bonds, and commercial enterprises which issue shares or bonds. Depositories where paper securities are kept, may maintain or not electronic records and are responsible for safekeeping and/or proper administration. Intermediaries, such as banks or other financial institutions, stand between the issuer and the ultimate investor. They maintain accounts reflecting their own securities holdings and those of their account holders. The chain of intermediaries might be complex, including a large number of actors and multiple jurisdictions. The end of the chain includes the account holders or investors, which have the ultimate legal and/or economic interest. The ultimate account holder and the investor may be one and the same, but this is not necessarily so. Some investors do not form part of

the intermediated chain, preferring to remain anonymous and operate through nominees. An entity in the middle of the chain may at the same time qualify both as intermediary in relation to its lower tier account holder and as account holder in relation to its upper-tier intermediary.[12]

A different terminology is encountered in the Financial Crime Compliance Principles for Securities Custody and Settlement (ISSA, 27 August 2015). Under the IOSCO Principles on Client Identification and Beneficial Ownership for the Securities Industry of 2004, correspondent banks may undertake due diligence on their equivalently regulated financial institution customers in order to rely on the customers' programs to identify clients and ultimate beneficial owners. The Financial Crime Compliance Principles for Securities Custody and Settlement (ISSA, 27 August 2015) provides guidance to Custodians on the appropriate due diligence measures. The term 'Custodians' is used to designate the financial institutions that participate in the holding chain, which under the ISSA Principles (FCCP) is called a 'custody chain', and hold for clients that constitute institutional account holders named as 'Account Holders'. Account Holders are defined as the regulated financial institutions that act as Customers or Clients of the Custodians. In the context of these Principles, Custodians include but are not limited to banks acting as global custodians and sub-custodians, fund distributors, banks, brokers, International Central Securities Depositories and Central Securities Depositories, to the extent that cross-border operations are involved. Custodians are used by their Customers for the safekeeping of proprietary and third party interests in the securities, the settlement and clearing of securities trades and ancillary services including corporate action processing, securities lending and collateral management. These services might be provided for the Customer's own account and/or for the account of the Customer's clients (Clients of the Account Holder or Clients). The Clients of the Account Holder may be individuals, legal entities or even other financial institutions.[13]

---

[12] Roy Goode, Herbert Kronke and Ewan McKendrick, *Transnational Commercial Law - Text, Cases and Materials* (Second edition published in 2015 by Oxford University Press)

[13] The International Securities Services Association (ISSA), *Financial Crime Compliance Principles for Securities Custody and Settlement* (27 August 2015) p. 4-5

The transition from physical delivery of security to electronic means of payment took place through the use of techniques that tackled the problem of too much paper. The first technique that was adopted was the 'immobilization' of securities certificates to reduce the movement of physical securities in the marketplace and to facilitate book entry transfers. The certificates were held by a central depository who held for one or more intermediaries, who, in turn, held for investors or other intermediaries. The intermediaries participating in the relevant holding chain keep electronic records of the securities and this enables them to perform trading and settlement operations in a speedy and cost-effective manner. The end-investor down the holding chain, or the nominee of the investor, is the securities account holder and the second tier intermediary who acts as an account provider is the bank or other financial institution. A specific holding chain may be comprised of more than two intermediaries that each holds the securities for the intermediary immediately down the chain. The securities certificates, and in some cases a 'jumbo' certificate, are held by a Central Securities Depository which holds for the issuer. This means that the issuing company does not register each and every investor who holds part of the share capital and the transfer of the shares does not require, in order for the transfer of ownership to take effect, their physical delivery to the buyer and the registration of the transaction with the issuer company register. Bearer securities are usually held as global notes while registered securities, including equity securities, can also be immobilized.

Another technique to deal with too much paper, which led to expensive and slow trading of securities, was to dematerialize securities. The electronic entry on the books of a central operator suffices to produce a constitutive effect, i.e. the very existence of the right derives from the electronic entry *per se.* The fast electronic settlement of transactions which is achieved as a result of immobilization and dematerialization contributes a great deal in the efficient and fast completion of

millions of every day transactions which otherwise, in the event that physical delivery of papers was required, could not be concluded.[14]

Thanks to the development of the above techniques, traditional holding, where the investor received a certificate for his securities which was safely kept by a bank, was replaced by an intermediated holding system where all security certificates are "immobilized" and centrally kept in the Central Securities Depository or were dematerialized. As already described, the investor holds his securities with his own bank, the bank holds them through a second bank (second-tier intermediary) and finally an intermediary holds the securities with the CSD where the certificates are kept. The number of intermediaries that form part of that chain may differ every time. There are jurisdictions with so-called "transparent systems", i.e. investors hold their securities directly with the CSD and there is only one top-level intermediary. However, other institutions may share functions with the top-level intermediary and are also called intermediaries. The performance of functions of intermediaries by other persons is provided for in article 7 of the Unidroit Convention on Substantive Rules for Intermediated Securities. For example, in State A all governments bonds are held with the Central Bank. Investors in government bonds open a securities account with the Central Bank with the assistance of a commercial bank which acts for the account of the Central Bank in this context. All instructions are given to the commercial bank which, through a technical interface and under specific arrangements with the Central Bank causes government bonds to be credited and debited to the securities account.[15] In other jurisdictions, the holding chain could be comprised by only one or more intermediaries. In cross-border transactions holding chains may involve many intermediaries in different jurisdictions. Within an intermediated holding system, the transfer of securities is achieved by entries in the electronic records of the participating intermediaries, whereby entries are made in the form of credits and debits recorded in the relevant securities accounts of the

[14] Louise Gullifer, 'Ownership of Securities - The Problems Caused by Intermediation' in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010) p. 1-3

[15] Hideki Kanda, Charles Mooney, Luc Thevenoz, Stephane Beraud assisted by Thomas Keijser, *Official Commentary on the Unidroit Convention on Substantive Rules for Intermediated Securities* (Oxford University Press 2012) p. 45-46

investors involved in the transaction. Depending on the "distance" between sender and receiver of the relevant securities within the framework of the particular holding chain, one or more intermediaries would have to perform the credits and debits and therefore change the account balances.[16] The ease of transfer, especially through netting, is indisputable compared to the traditional holding system that required the physical delivery of securities.

3.2 Distinctions between different holding systems

The trust model is mainly effective in England and Wales, while similar models may be found in Ireland, Australia and other common law countries. Under the trust model, the issued securities are safe-kept by the CSD, which in England is called the CREST system and is operated by Euroclear UK & Ireland. The CSD has no legal interest in the securities and resembles to the company register as provided for in corporate law. The participants of the CREST systems (intermediaries) are treated as the legal owners of the securities which they hold for their clients or for their own account. The account holder of the above system, who holds its securities with a financial institution, is the actual beneficiary assuming the role of a trustor and has an equitable ownership right in the securities. When many tiers exist in the holding chain, the holder of an equitable interest is considered as a trustee for its own client, which is the case for all intermediaries down the chain until the end-investor who is the beneficial owner. The investor, in this case, has an equitable ownership in the securities that are held for him by the account provider (trustee). The beneficial owner enjoys in praxis approximately the same rights of a legal owner but legally its rights are not described as 'full ownership rights' but as 'equitable ownership in an equitable ownership in the securities'.[17]

---

[16] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.10-11

[17] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.14-15

The security entitlement model is similar to the trust model but, still, bears significant differences. The USA and Canada are the two countries where the particular model applies, the CSD being called, in the case of the USA, 'Depository and Trust Company'. The legal owner of the securities entitlements is a 100% subsidiary company of the NYSE. Each account holder has a right described as 'security entitlement' against his account provider. Moving up the holding chain, each intermediary, besides acting as an account provider, is also an account holder who possesses a security entitlement against its upper-tier account provider. As far as the legal nature of the right of 'security entitlement' is concerned, it is similar but not identical to legal ownership or equitable interest. For the final investor the 'securities entitlement right' encompasses substantial rights regarding the receipt of dividends, interests and participation in the general meetings of companies, according to the provisions of the account agreement. The investor lacks the right to claim the securities as its own assets as a whole and, on the contrary, is obliged to share them at its prorate values with other entitlement holders of that particular type of financial asset. Consequently, the investor may not assert a claim regarding its securities at the upper level of the holding chain given that he is not the holder of a right of exclusive ownership of certain specified financial assets but rather holds a pro rata interest[18]. Therefore, one could describe it as a type of co-ownership. The difference from the equitable interests under English law lies with the fact that security entitlements do not 'overlap'.[19] While trustors under English law enjoy equitable ownership in an equitable ownership and thus hold rights that concern the same underlying assets, *every security entitlement against an account provider is distinct from the security entitlements that the account provider itself holds.*[20]

[18] Louise Gullifer, 'Ownership of Securities - The Problems Caused by Intermediation' in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010) p. 23

[19] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.16

[20] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.16

However, both under US and English law, account holders may exercise their claims only against their immediate account providers and not against upper intermediaries or the CSD.

The undivided property model is adopted by French law. In this model only dematerialized securities are traded. The CSD acts as a mere register and neither the CSD or any intermediaries have legal interests or rights in the securities. Full proprietary rights belong to the investors and the securities are considered to be located directly in their securities accounts, while at the same time they can access their securities only through their account providers and not through upper tier intermediaries.[21]

The pooled property model entails the creation of a sui generis type of shared property. The investor is neither the legal owner of a number of individual financial assets nor the holder of separate rights but rather the holder of by nature proportionate rights (e.g. a tenth share in the share capital of a company). Another theoretical approach supports the idea that each account holder has a co-ownership interest in the securities that lie in the pooled account under a relative provision of the account agreement.[22] Consequently, the investor is not deemed as the possessor of the securities and has access to his securities only through his account provider while other upper tier account providers are unable to identify him given that he is not the holder of individual objects which can be distinguished in the pooled accounts.[23]

The transparent model is adopted by the Nordic countries, Greece, Poland, Brazil, China and others. The CSD holds directly for the investors while banks and other

[21] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.17

[22] Louise Gullifer, 'Ownership of Securities - The Problems Caused by Intermediation' in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010) p. 22-23

[23] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.18

financial institutions are not providers of securities accounts but only operate the account opened with the CSD according to the relevant national law rules, as described in article 7 of the Geneva Convention. Consequently, the beneficial owners enjoy a direct property interest in the securities that is separate and not shared with other investors. Obviously, the operation of the above mentioned accounts takes place according to the rules and within the legal and technical framework of the relevant jurisdiction[24].

The classification of the securities holding system which followed the criterion whether the investor had a proprietary in nature right linking him directly to his securities or merely a claim against his intermediary, lead to the distinction between direct and indirect holding systems. However, the above described distinctions have been concluded on the basis of more detailed and diverse criteria, which leaves considerable doubts whether the direct/indirect distinction has a practical significance. If one should take note, for example, of the pooled property model then one would assert, at a conceptual and theoretical level, that the particular holding systems are direct in the sense that a *sui generis in rem* right is enjoyed by the investor, yet the investor could exercise his claims only against his account provider as no upper intermediary would recognize and identify any such separate *in rem* rights. It is obvious that the notion of 'direct' here has merely an academic substance with no practical implications given that the financial assets held by upper intermediaries are somewhat cut-off from the end investor. Transparent holding systems seem like the only systems that fully comply with the definition of a direct holding system[25].

[24] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.19

[25] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011) p.19-20

3.3 The position of investors in the intermediated securities holding systems

A great number of intermediaries provide their services in the areas of the trade and the clearing and settlement of securities. The excessive number of transaction and settlement systems has been commented upon by scholars and participants of the financial services industry. According to the Lamfalussy report[26], this very situation may "*fragment liquidity and increase costs, especially for cross-border clearing and settlement".* The first Giovannini report[27] characterizes the EU market in clearing and settling trades as highly fragmented. But today as well, given that each of the involved intermediaries spends money on operating facilities and staff, and naturally pursues a profit and not only to cover the costs, it is obvious that the overall cost of holding intermediated securities rises dramatically.

However, the cost is not the only burden on the shoulders of the investor who invests in an intermediated holding system. There is an inherent legal risk of the investor's interests not accurately and adequately being protected due to the existence of many layers of intermediation between the end-investor and the issuer that create a significant gap.[28] Indeed, within the framework of an intermediated holding chain, each participant contracts with the intermediary of the immediately upper or lower tier. An agreement is reached, and the relevant documents are drafted and signed, between the CSD and the intermediary directly connected with it. This intermediary then has a contractual relationship with the second intermediary down the chain, until the lowest tier intermediary who is acting as the account provider of the end investor and has signed an account agreement with the investor client. All of these agreements are bilateral. When two intermediaries sign the agreement they actually agree on terms that are binding and create rights and obligations between them alone. As a result, a breach of contract on their behalf would be constituted if the specific terms included in that contract were not upheld, given that a legal link exists only between those two intermediaries, regardless

[26] Final Report of the Committee of Wisemen on the Regulation of European Securities Markets (Brussels, 15 February 2001)
[27] The Giovanini Group, *Cross-border Clearing and Settlement Arrangements in the European Union* (Brussels, November 2001)
[28] Eva Micheler, 'Transfer of Intermediated Securities and Legal Certainty' in Thomas Keijser (ed), *Transnational Securities Law* (Oxford University Press 2014) p. 119

whether specific acts or omissions of the two intermediaries are in line with the contractual terms of the agreement between the investor and its account provider or between two other intermediaries. Therefore, in determining the terms of the contract between them, the two intermediaries do not feel compelled to fully synchronize and adapt their terms with the contractual provisions of the other contracts but they rather prefer to focus on including terms that they consider less risky, in terms of how likely it is not to be able to comply with those terms by fulfilling an obligation towards their counterparty, as in that case they would be in breach of contract and liable against the counterparty intermediary (e.g. ensure that there is a reasonable amount of time to pass on instructions or payments to the level immediately below or above them).[29] But disregarding or not prioritizing or not aligning with the contractual provisions that are relevant to the end investor's rights practically entails the likelihood that the documentation created between intermediaries up the chain lacks the inclusion of those terms that safeguard the investor's interests or perhaps 'waters down' its interests. Indeed, if the contracts of the intermediaries up the chain provide for more time to pass on instructions or reject liability of the intermediary for certain mistakes, then obviously the above provisions are detrimental for the ultimate investor. Furthermore, processing corporate actions, voting actions, income, information flows, could be very problematic in an intermediated holding chain. Especially in cross-border holdings, investors with interests in different jurisdictions assign management of their assets to institutions that act as global custodians constituting an additional tier in the holding chain. This could deter the velocity of the information flows between ultimate investors and issuers. In regard to income collection, the investor's account might be credited with the income on a later date given that the due processing of corporate actions might cause delays.[30] Cross-border voting rights may also be difficult to exercise in cross-border holding chains.

---

[29] Eva Micheler, 'Transfer of Intermediated Securities and Legal Certainty' in Thomas Keijser (ed), *Transnational Securities Law* (Oxford University Press 2014) p. 122

[30] Nora Rachman and Maria Vermaas, 'Corporate Actions in the Intermediated System: Bridging the Gap Between Issuer and Investor' in Thomas Keijser (ed), *Transnational Securities Law* (Oxford University Press 2014) p. 161

If one had to extract a conclusive remark commenting on the investor's position in the intermediated holding chain, one would highlight the existing gap that seems to exist between the issuer and the ultimate investor. There are inherent legal risks deriving from this gap concerning the protection of the investor's interests, corporate and others. It seems that the greater the number of intermediaries, the greater the risk lies. National laws effective in each jurisdiction determine the degree of protection of the investors, e.g. in cases where an insolvent intermediary does not hold sufficient securities to cover the amount credited to account holders. Yet, the inherent legal risk of an intermediated holding chain due to the gap between the issuer and the investor always remains, notwithstanding all of its advantages for the investor and the integrity and efficiency of the financial markets.

3.4 Transparency and non-transparency of holding systems in relation to money-laundering threats

In a transparent holding system, the question of beneficial ownership seems relatively simple. The CSD knows the identity of all account holders and has a relationship with them while all transfers are entered on a central register. The record of transfers at the CSD level has constitutive effects and, apart from the existence of a top-level intermediary, there might be other banks or other financial institutions sharing functions. On the other hand, in non-transparent holding systems the CSD cannot identify their particular account holders. The relationships between the CSD and the intermediaries are independent from the relationships between the intermediaries and the account holders.[31] All the information flows concerning the holding and transfer of securities takes place only between the transacting participants. Each party only knows about the party immediately below or above them in chain, i.e. an intermediary knows its account holders but, in case that these account holders act as account providers as well, does not know their clients – account holders or any other account holders down the chain, and naturally does not know the end investor. Given the above lack of information, the rights of account holders are limited to the intermediary immediately above them, which

[31] Marek Dubovec, *The Law of Securities, Commodities and Bank Accounts – The Right of Account Holders* (Edward Elgar Publishing 2014) p. 42

constitutes the "no-look-through principle".[32] This principle does not allow an account holder to exercise a claim against any upper-tier intermediary other than its account provider immediately above him in chain. If that was not the case and upper-tier intermediaries could be sued by the account holder, the higher tier intermediary would have to gather information from participants down the chain to defend itself against the claims and this, inevitably, would lead to complex situations that would increase costs and eliminate many advantages of the intermediated holding system. This very lack of information is also the reason behind prohibiting upper-tier attachment. If, for example, a creditor attempts to enforce its debt against assets of an investor by attaching the investor's securities account with its account provider, that would be acceptable. But if the creditor attached a pooled account higher in the holding chain on the basis that the debtor holds his shares 'somewhere in the pooled account' together with shares of the same description that belong to other beneficiaries, then the upper-tier intermediary is in no position to identify which separate shares belong to the debtor because it would have no records that the particular investor has an interest in the specific type of securities. Then, complying with the attachment order would mean that the entire issue of the particular type of shares should be frozen and other investors would not be allowed to trade these securities to the detriment of the efficiency and integrity of the financial system.[33] This rule of prohibition of upper-tier attachment is included in article 22 of the Geneva Convention.

All of the above leads to the conclusion that information on the identity of the beneficial owner of securities, whether a legal entity or a natural person, its business activities and possibly the sources of its funds, all lie with the information recorded in the initial account agreement signed with the bank or the institution acting as an account provider. The flows of these information not only are incompatible with the legal structure of an intermediated holding system, where each intermediary relates

[32] Louise Gullifer, 'Ownership of Securities - The Problems Caused by Intermediation' in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010) p. 14-15

[33] Louise Gullifer, 'Ownership of Securities - The Problems Caused by Intermediation' in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010) p. 15-16

with the immediately below or above it in chain participant, but one could detect a tension with the desirable effects of the no-look-through principle that was analyzed in the above paragraph. Indeed, the existence of that principle has contributes in enhancing the legal certainty within the intermediated securities system in the sense that each intermediary and the CSD are only liable for fulfilling their obligations included in the contracts they signed as account holders or account providers and not for actions or omissions of other participants below or above them in chain, i.e. the rights conferred on an account holder by a credit may be exercised by the account holder only against the relevant intermediary. Additionally, the same principle is connected with the efficiency and the scale economies developed within such a holding chain. Intermediated securities are transferred by crediting these securities to that account holder's securities account. In the case of pooled accounts[34], the transfer of securities between two clients of the same intermediary is technically easy and simple and entails no delays, while netting is much easier as well, which means that transfers of securities between participants of the holding chain, depending on their position within the framework of the holding chain, may take place faster and in a cost-effective manner because each instruction that leads to crediting and debiting of the accounts is not executed separately and externally but is rather a part of an offsetting procedure between the values of multiple positions and payments due to be exchanged between participants and, thus, a final net position is recorded on the accounts of the relevant intermediaries adding to the speed and ease of transfer and settlement.[35] Consequently, one might argue that the legal structure of the intermediated securities holding system based on the no-look-through principle is characterized by an intrinsic feature: the lack of a direct link between the ultimate investor and the trading and settlement process of the financial assets that belong to him or, in other words, a form of limitation in the ability of the investor to exercise its rights against the issuer. Not only in the sense that the investor might be deprived of the ability to directly raise relevant claims

[34] The same advantage of the easy transfer is true for transparent holding systems as well.

[35] Louise Gullifer, 'Ownership of Securities - The Problems Caused by Intermediation' in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010) p. 12-14

against upper-tier intermediaries or the issuer but in the sense that the identity of the securities -as separate objects forming part of a pooled account- and the identity of that very investor as a natural or legal person, are not to be traced easily up the chain of intermediaries and relevant information is to be gathered by the lower tier account provider. Especially when netting via pooled accounts take place, it practically becomes extremely difficult to trace the transfer of securities from one account to another, or for a credit entry to be matched with a particular debit entry.[36]

3.5 Compliance principles for fighting money laundering in the intermediated securities system

The above designated difficulty to trace the transfer of securities and the identity or other information of the beneficial owner of the securities in an intermediated securities holding system, undoubtedly create a status of lack of transparency. Naturally, in the context of money laundering, the lack of transparency concerning the above issues reflects on the lack of transparency as regards the sources of the funds used to acquire the financial assets traded within the particular holding system. As a result, the concerns that huge illicit funds flow within the global financial system are even more acute when it comes to intermediated securities where beneficial owners of the traded financial assets are difficult to be traced.

Naturally, each jurisdiction has its own legal and regulatory framework that dictates compliance principles to the domestic participants of the financial market. However, mainly in cross-border holding situations things tend to be much more complicated. At an international level, the concerns regarding financial crime within the global finance system brought the adoption of guidance and principles by participants of the financial system. The International Organization of Securities Commissions (IOSCO) issued on May 2004 the “Principles On Client Identification and Beneficial Ownership for the Securities Industry”. These principles to guide securities regulators and serve as important parameters for authorized securities services

[36] Louise Gullifer, ‘Ownership of Securities - The Problems Caused by Intermediation’ in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010) p. 14

providers, i.e. regulated entities that perform securities transactions like mutual funds, broker dealers, securities firms and others. The above principles highlight the common features among the different regulatory approaches to client and beneficial owner identification among IOSCO members, despite the differences among the legal frameworks effective in different jurisdictions. They aim to contribute to the application of a client due diligence process (CDD) in the securities industry so as to prevent its exploitation through illegal activities such as money laundering and financing of terrorism.[37]

In particular, authorized securities service providers (ASSPs), when establishing a business relationship with a client should identify and verify the client's identity using reliable, independent source documents, data or other information. Cross-border omnibus accounts for certain investment vehicles, such as hedge funds, are considered as high-risk category of accounts. ASSPs should have specific client due diligence policies for omnibus accounts (principle 1a). The relevant recommended actions include gathering sufficient information regarding the financial institution that opens a segregated account with the ASSPs in order to deposit financial assets of its clients-investors contained in a pooled account, assessing the adequacy of that financial institution's CDD process, determining the physical presence of the financial institution in the jurisdiction where it is incorporated, assessing the regulatory regime of the country in which the financial institution is located, and documenting the respective responsibilities of each institution. Furthermore, ASSPs should obtain sufficient information in order to identify persons who beneficially own or control securities accounts (principle 2)[38]. Among the recommended actions is the certification on behalf of the client to the account provider of the identity of the persons who ultimately exercise effective control over a legal person. Know your client (KYC) practices, record keeping on the CDD process for at least five years, third party reliance and principles regarding the role of the regulator, form also a part of the principles of IOSCO.

---

[37] The International Organization of Securities Commissions, *Principles on Client Identification and Beneficial Ownership for the Securities Industry* (MAY 2004) p.1-2

[38] The International Organization of Securities Commissions, *Principles on Client Identification and Beneficial Ownership for the Securities Industry* (MAY 2004) p.4-12

The International Securities Services Association (ISSA) issued the 'Financial Crime Compliance Principles for Securities Custody and Settlement' on 27 August 2015, in order to provide global guidance on the establishment and maintenance of cross-border securities custody relationships. In particular, the principles aim to provide guidance to securities custodians, which are regulated financial institutions providing safekeeping accounts, securities settlement etc., on how to manage the risks that arise from the layers of intermediation between securities issuers and ultimate beneficial owners. These Principles, having taken into account the above described Principles of IOSCO on client identification and beneficial ownership for the securities industry, *provide market participants with practical guidance on the question of transparency of ownership and control in the intermediated securities custody arrangements.*[39]

According to the already discussed terminology used by the above ISSA Principles, the account provider used by its customers for the safekeeping of proprietary and third party interests in securities, and the settlement and clearing of securities trades, acts as a "custodian". The custodian financial institution shall be obliged to implement appropriate due diligence that will create a risk profile of the particular account holder which seeks to do business with the custodian. A strong indication that the account holder is not suspicious of conducting illegitimate business is the possible compliance of the account holder within a regulatory environment that applies and implements the principles of the Financial Action Task Force (FATF). However, other information regarding the account holder must be taken into account through the due diligence process and its risk profile should be monitored and updated periodically. The relevant risk considerations include the account holder's ownership and management structures, its geographic risk and the anti-money laundering policies that are implemented by the account holder. Additionally, the fact that not only the ownership interests of the account holder are intermediated but in many cases so are the interests of the account holder's clients should be documented. Consequently, the control must focus on asset holdings and

[39] The International Securities Services Association (ISSA), *Financial Crime Compliance Principles for Securities Custody and Settlement* (27 August 2015) p. 3

not just on the execution of transactions by asset owners. Therefore, the custodians, under the ISSA principles, should communicate to their account hoders their requirements regarding documentation relative to the business of the clients of their account holders and obtain representations and undertakings relating to them contractually, in order for them to control the business of third party clients.[40] Indeed, it should be the responsibility of the custodian to communicate to its account holders any relevant KYC standards and other compliance requirements that it expects them to follow. The account holder is then responsible for complying with these standards. The account holder will deposit securities with the custodian only when the assets' beneficial owners have been subjected to due diligence. In the case of omnibus client accounts held for several clients of the account holder, specific parameters of the business of the account holders are controlled by the custodians. Whether the account holders are regulated and authorized to accept client assets, the regulatory framework under which they perform their operations, whether they have applied and implemented any specific requirements of the custodian as regards their compliance policies, all of the above constitute relevant factors to be taken into account by the custodians in order to start or continue to do business with account holders that want to open or maintain with the custodian omnibus accounts commingling securities held for their clients. The custodian has the right to request that the assets' beneficial ownership of assets deposited on omnibus client accounts be disclosed to the custodian via an agreed operational procedure based on predetermined risk factors. Pursuant to Principle 17, the custodian should be entitled to require its account holder to disclose the identities of the ultimate buyers and sellers of securities within a reasonable period in response to a specific request predicated on risk factors.[41]

The above framework, including guidance and principles of IOSCO and ISSA, is extremely useful in recording a general idea that constitutes the pillar stone of the anti-money laundering policy of intermediaries that participate in the intermediated

[40] The International Securities Services Association (ISSA), *Financial Crime Compliance Principles for Securities Custody and Settlement* (27 August 2015) p. 9

[41] The International Securities Services Association (ISSA), *Financial Crime Compliance Principles for Securities Custody and Settlement* (27 August 2015) p. 13

holding system. The general idea governing the due diligence process in the intermediated securities is that the custodian bank which opens or maintains a securities account for another financial institution is obliged to screen and evaluate the compliance policies of that financial institution. If the regulatory framework under which it operates is adequate and offers the same level of protection against money laundering compared to the policy and standards of the custodian, then a strong positive indication that allows concluding transactions with the particular account holder does exist. An indirect control method to evaluate the legitimacy of the financial assets that are deposited by the beneficial owners and flow within the securities holding systems is thus being implemented. A series of factors are taken into account and evaluated by the custodian regarding the business of the account holder, even the ownership status and the management of the specific entity. However, that does not mean that the control on the ultimate investor is direct. However, the identity of the beneficial owner of the financial assets is usually required, within the framework of a risk-based approach, only according to the terms of an agreement between the institutions (the so-called red flags) or in cases of enquiries by regulatory or judicial authorities. As explained before, not all transfers and not all financial assets could actually be controlled in order to determine whether the ultimate investor circulates illegal money by way of investing in securities. It would be practically impossible and probably undesirable as regards the efficiency of the holding system. A risk-based approach is adopted instead, where the existence of certain risk factors, whether they constitute legislative provisions or agreed terms between institutions, leads to further control of specific securities accounts and transactions which might even lead to disclosing the identities of the ultimate buyers and sellers.

The question that now arises is whether this indirect control suffices to prevent money laundering and, if not, what would a realistic alternative be. It is almost self-evident that a transparent holding system, whereby the identities of the beneficial owners would emerge on the records of the CSD, would make things less complicated as no “drilling down to the beneficial owners” would be required. Nevertheless, a call for transforming intermediated to transparent holding systems

in all jurisdictions would obviously not meet the approval of governments and banking associations in jurisdictions where intermediated holding systems are operative since they would rather protect their respective business models. In any case one cannot overlook the advantages of such holding systems for investors and the economies worldwide alike. However, there is a strong argument that a mechanism could be created whereby the securities holding and transfer systems would record the name of ultimate investors on their books, irrespective of whether there are any intermediaries between the issuers and investors. A central register, possibly at the level of the Central Securities Depository, could be created and maintained in that context. The objective would be to create one central electronic system that held and transferred securities for all European jurisdictions. The holders of securities would enjoy the benefit of a direct access to that system.[42] According to those in favor of the idea, the European network of intermediaries was created before electronic communication became possible. Now that the technology allows the shape of a new computer program for settlement, there is no reason why this central electronic system could not be established, except maybe the obstacles that might be posed by current actors who represent banking and financial institutions participating in the intermediated holding chains as intermediaries and collecting fees by performing operations which might not be necessary if the operation of the aforementioned central electronic system was to be realized. Such an operation would bring about the reduction of costs created by too many intermediaries and would bridge the gap between the investors and the issuers. In the context of the money laundering issue, it would certainly offer a higher degree of transparency as regards the identity of the investors and would reduce the significant administrative costs that custodian institutions carry in order to e.g. assess the credibility of a foreign account holder that seeks to open a securities account or to comply with provisions dictated by national and international regulators.

[42] Eva Micheler, 'Transfer of Intermediated Securities and Legal Certainty' in Thomas Keijser (ed), *Transnational Securities Law* (Oxford University Press 2014) p. 142

3.6 Liquidity of financial markets and implementation of anti-money laundering policies. Are the two compatible?

Financial markets, including securities markets, are the basic source for financing business growth and government spending. Developing deep and liquid financial markets across borders constitutes a policy that contributes to the financing of business and governments.[43] The amounts of capital that are moved within the financial markets every day in one direction or the other are overwhelming. Today, the efficiency and the systemic stability of the financial markets is still the key for financing both the private and the public sector and thus contributing to world financial stability. In that context, the amount of capital flows within the financial markets is in principle desirable by all the participants of the financial markets.

The fact that the financial markets have been used in the past and are still being used mainly in the "layering" stage of money laundering is also indisputable. The mere fact that the implementation of strict money laundering policies, which would prevent the inflows of 'dirty' money in the system through methods of screening the identity of the investors and the sources of their financial assets, would result to fewer capital flows, might open a serious discussion on whether governments and market participants feel rather at ease with the lack of transparency in intermediated securities systems, to the extent that the particular financial market remains open and accessible to the inflows of financial assets regardless of the legitimacy of their source. Such an argument is recorded in *Wolfgang Hetzer's 'Money Laundering and Financial Markets'.*[44] The author seems to suggest that the interests of business, crime and politics coincide to a certain extent, leading to the tolerance of inadequate and *self-deceptive* legislation which is far from effective in the combat against 'dirty money'. Such an argument is naturally difficult to be justified by a legal, scientific method of analysis as it refers to the inner incentives of policy makers. However, one can assert that, notwithstanding the negative aspects of 'dirty' money circulating within a financial market for the credibility and the

[43] Pwc, 'Global financial markets liquidity study' (August 2015) https://www.pwc.com/gx/en/financial-services/publications/assets/global-financial-market-liquidity-study.pdf accessed 28-1-2017, p. 19

[44] Wolfgang Hetzer, 'Money Laundering and Financial Markets' (2003) 11 Eur. J. Crime Crim. L. & Crim. Just. 264 2003

attractiveness of that very market in regard to serious investors, strict compliance and anti-money laundering policies adopted by the financial institutions render the relevant market unwanted for the investment schemes that seek to keep the anonymity of their ultimate investors and subsequently will turn to investing in other less heavily regulated markets.

CHAPTER 4: Bitcoin transactions and money laundering

It is widely accepted that the nature of bitcoins, as regards mainly the anonymity of the participants of a transaction, renders them vulnerable to money laundering threats. The following description of the basic features of bitcoins aims at helping to assess the risks posed to the financial system, particularly in the areas of financial integrity that might be compromised by money laundering tactics, consumer protection, tax evasion and the regulation of capital movements.[45] Given that the bitcoin is a cryptocurrency, meaning that in principle the identity of the users is not publicly exposed, the risk of money launderers taking advantage of the anonymity offered to the transacting parties is to be seriously considered.

4.1 Overview of the basic features

The bitcoin currency is characterized as a decentralized virtual currency. It is decentralized because there is no single administrator of the system such as a state or banking authority which owns or controls the network or issues currency to the users.[46] As a result, bitcoins do not represent a claim on an issuer such as government or central bank. And they are indeed a virtual currency because they exist only on-line and they do not constitute legal tender in any particular country, as in the case of the so-called 'fiat currencies'. Furthermore, bitcoins fall under the

[45] International Monetary Fund (IMF), *Virtual Currencies and Beyond: Initial Considerations* (January 2016) p. 24

[46] Kavid Singh, 'The New Wild West: Preventing Money Laundering in the Bitcoin Network' (2015) 13 Nw. J. Tech. & Intell. Prop. Iii p. 40 <Hein Online> accessed 20 January 2017

definition of virtual currencies provided by the ECB in 2012, i.e. “a type of unregulated digital money which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” and by the European Banking Authority in 2014, i.e. “a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency but is accepted by natural or legal persons as means of payment and can be transferred, stored or traded electronically”. All of the above unique characteristics of virtual currencies that also fit the nature and operation of bitcoins, distinguish bitcoins from fiat currencies and other forms of investment or payment mechanisms.[47]

4.2 Payment system operation in the bitcoin network

Bitcoin operates through a peer-to-peer network created by multiple individuals running the designated software on their individual PCs and connect to each other without the involvement of a centralized website or server.[48] In peer-to-peer networks, every computer connected is an equal partner and can exchange data and services with every other member of the network[49]. The transactions are valid and legitimate without the authorization or the approve by a third-party such as bank. They are processed and validated based on the principles of cryptography.[50] In particular, the program is designed to solve a complicated math problem and, once the problem is resolved, individual bitcoins are created in a digital form and, in particular, in the form of long strings of numbers. The users of the network who solve the math problems acquire the newly created bitcoins as a reward for contributing their computing powers to resolving the problems. This process is called “mining” the bitcoins and the users are called ‘miners’. Mining occurs rather slowly, given that, even though more and more computer processing power is dedicated to

[47] Lucy Frew, Rich Folsom and Sophie van Wingerden, ‘Legal and regulatory issues relating to virtual currencies’ (July/August 2015) 7 JIBFL 438B

[48] Catherine Martin Christopher, ‘Whack-a-mole: Why prosecuting digital currency exchanges wont’ stop online money laundering’ (2014) 18 Lewis & Clark L. Rev. 1 p. 11 <Hein Online> accessed 20 January 2017

[49] David Steven Brown, ‘Cryptocurrency and criminality: the Bitcoin opportunity’ (2016) Pol. J. 327 p. 3

[50] Jeffrey E. Alberts & Bertrand Fry, ‘Is Bitcoin a Security?’ (2015) B. U. J. SCI. & TECH. L. Vol. 21:1 p. 2 <Hein Online> accessed 20 January 2017

the math problems solving every day, the program adjusts the difficulty level of the math problem over time so that, despite the fact that more computing powers is dedicated to the solving process, bitcoins are still released at a controlled and pre-established rate. Ultimately, there will be approximately 21 million bitcoins in circulation.[51]

Each transaction is subjected to a cryptographic equation and recorded in 'blocks'. Each new block is a continuation of the previous one and thus a chain is formed, called 'blockchain'. So each transaction on the bitcoin network is recorded on a decentralized public ledger, the "blockchain". The blockchain is visible to all computers in the network but does not reveal the identity of the parties involved in the transaction because each user's identity is encrypted. The public ledger, by using cryptography, verifies that a user transferring Bitcoin has in fact transferred the specified amount of Bitcoin to the user receiving that same amount. Thanks to the public ledger and through the use of cryptography the so-called 'double-spending' problem is confronted, meaning that a participant in a currency market is prevented from transferring at the same time a single unit of currency to two different recipients.[52]

Before a user can trade in bitcoin, the user must download a 'bitcoin wallet' application in order to obtain both a public and a private key. The public key is comprised of a series of characters that form the user's public address which serves as a mark of identification that the user can post on the internet in order to conclude a transaction. The private key is known only to the user and he may use it for signing his transactions. Buying a product for example would mean that the seller would first disclose his public address to the buyer and the latter would generate the transaction quantifying his bitcoin payment which is visible by all participants of the bitcoin network. The buyer would then sign the transaction with his unique private

[51] Catherine Martin Christopher, 'Whack-a-mole: Why prosecuting digital currency exchanges won't stop online money laundering' (2014) 18 Lewis & Clark L. Rev. 1 p. 12 <Hein Online> accessed 20 January 2017

[52] Jeffrey E. Alberts & Bertrand Fry, 'Is Bitcoin a Security?' (2015) B. U. J. SCI. & TECH. L. Vol. 21:1 p. 3 <Hein Online> accessed 20 January 2017

key. Finally, a miner would verify the transaction and confirm that 'double-spending' has not occurred.[53]

In the above context, the public ledger serves as a list of all past transactions in the network. The transactions are recorded in a chronological order and they are made publically available. As a result, one could trace back the transaction history of a single bitcoin until its very first use. This is possible merely by checking, in each trade of the bitcoin, the signature under the relevant respective transactions. These past signatures form a chain which involves the specific single bitcoin, due to the fact that no two bitcoins can share the same transaction history.

The above described function of the public ledger system lies in the very heart of the characterization of the bitcoin network as a decentralized network, as it renders third-party oversight unnecessary. Furthermore, it increases bitcoin liquidity and boosts consumer confidence as it excludes the possibility of 'double spending'. In addition, one could argue that there is a great deal of transparency present in the bitcoin network since, due to the function of the public ledger, all bitcoin transactions are traceable because the public addresses of those involved in each specific transaction are recorded. Indeed, a public address cannot reveal directly the identity of the user who transacted. However, it can be linked to an IP address assigned to devices accessing the Internet and thus the user's location and personal identity can be discovered easily. Because of that possibility, users employed software that hides the user's IP address in order to achieve total anonymity, mainly the 'Onion Router' (Tor).[54] Since Tor enables criminals to transact in bitcoins anonymously, money laundering activities might take place at a larger scale.

4.3 A set of common terms to describe the participants of the bitcoin network

In FATF's 'Virtual Currencies Guidance for a Risk-Based Approach' (June 2015) a non-exhaustive list of the basic participants of the virtual currency systems, including

[53] Kavid Singh, 'The New Wild West: Preventing Money Laundering in the Bitcoin Network' (2015) 13 Nw. J. Tech. & Intell. Prop. Iii p. 41 <Hein Online> accessed 20 January 2017
[54] Kavid Singh, 'The New Wild West: Preventing Money Laundering in the Bitcoin Network' (2015) 13 Nw. J. Tech. & Intell. Prop. Iii p. 42 <Hein Online> accessed 20 January 2017

bitcoin, are recorded and defined, thus providing a common set of terms. These terms, with the same meaning, are used in the present paper as well.

An exchanger (also called a virtual currency exchange) is a person or entity engaged as a business in the exchange of virtual currency (including bitcoin) for real currency, funds or other forms of virtual currency and also precious metals, for a fee (commission).

A user is a person or entity who obtains virtual currency (including bitcoin) and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person or who holds the virtual currency as a personal investment.

A miner is an individual or entity that participates in a decentralized virtual currency network (bitcoin network) by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system.

Virtual currency wallet is a means (software application or other mechanism) for holding, storing and transferring bitcoins or other virtual currency.

A wallet provider is an entity that provides a virtual currency wallet, including a bitcoin wallet. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provide storage and transaction security.

4.4. The risk of money laundering in bitcoin transactions

Bitcoin transactions are, to a significant extent and mainly because of the lack of user's personal identification, vulnerable to abuses by criminals who aim at legitimizing their 'dirty' money. Their vulnerability lies with the fact that they can be traded on the Internet and that anonymous transfers are easily conducted. They are usually employed in non-face-to-face customer relationships and may facilitate cash funding or third-party funding through exchange transactions where the source of the funding remains unknown.

In a bitcoin transaction on a peer-to-peer basis, there is no process involved that would require the personal identification of the users[55]. The addresses of 'bitcoin wallets' do not provide any indication of the user's names. Instead, they operate as accounts with no names or other customer identification attached. The historical record of transactions in a 'block-chain' does not entail identification and verification of the participants. Additionally, the possible suspicious transactions are not monitored by intermediaries, such as banks, and therefore the authorities lack a reliable and easily accessible source of relevant information. Law enforcement authorities also lack the possibility to target one central entity that operates as administrator and pursue investigation or asset seizure in a more effective manner.[56] Consequently, it is hard to trace a transaction due to the anonymity of the users and the anonymizing service providers that make the transaction chain unclear.[57]

Furthermore, the payment via bitcoins is globally widespread, given that the technological requirements that allow a user to transact using bitcoins are actually limited to an internet access. As a result, there are no jurisdictional borders. The wide spread of the infrastructure hinders the ability of the authorities to effectively intercept transactions. In that context, criminals might find it easier to deposit and transfer bitcoins globally, rapidly and irrevocably.

Additionally, the remittance money transfer market is constantly getting bigger. While traditionally the predominant players of this market were certain banks and companies like the Western Union and MoneyGram, the bitcoin network is more and more exploited by those who wish to transfer money across the world because payment transfers are conducted in a cheaper, faster and more efficient manner. Start-ups using block-chain technology, e.g. Bitspark, Abra, Align Commerce and many others, are competing with traditional players in the money transfer market[58].

---

[55] International Monetary Fund (IMF), *Virtual Currencies and Beyond: Initial Considerations* (January 2016) p. 27

[56] FATF, *Virtual Currencies – Guidance for a Risk-Based Approach* (June 2015) p. 32

[57] International Monetary Fund (IMF), *Virtual Currencies and Beyond: Initial Considerations* (January 2016) p. 27

[58] Prableen Bajpai, 'Bitcoin Remittances: How to send money home' (March 8, 2016) http://www.investopedia.com/articles/investing/030816/world-will-soon-use-bitcoin-send-money-home.asp accessed 10.2.2017

This new reality poses a risk that criminals or terrorists would use the bitcoin remittance systems and accounts for financing illegal activities.

All of the above mentioned money laundering risks are to be estimated together with the obvious intentions of criminals or terrorists to disguise the origins of criminal proceeds[59] and to undermine the ability of enforcement authorities to obtain evidence and recover criminal assets. The danger is more direct in the case where market participants are controlled by criminals, terrorists or related organizations.[60]

Another important risk factor is associated with the fact that bitcoins, as other virtual currencies as well, base their operation on complex infrastructures consisting of several entities which transfer funds or execute payments. These entities are globally spread and are to be found in many different jurisdictions which means that the regulatory status might be unclear, the relevant jurisdiction might not apply adequate AML controls and supervision or enforcement might become more complex. Indeed, a decentralized virtual currency like bitcoin, where anonymous person-to-person transactions take place, sometimes gives the impression of operating in a digital framework completely outside the reach of any particular jurisdiction.[61]

4.5 The use of bitcoin in online black markets

Hidden websites fostering the buying and selling of illegal products and services is not an uncommon phainomenon in the past years until today. Bitcoins were used as a means of payment and transaction within these markets.

'Silk Road' was a typical example of such a cyber global black-market where illegal drugs, weapons, stolen identity information and other illegal goods and services were traded. It was launched in January 2011 and was in operation until September 2013 when a criminal complaint was launched against its alleged owner and

[59] International Monetary Fund (IMF), *Virtual Currencies and Beyond: Initial Considerations* (January 2016) p. 27
[60] European Banking Authority (EBA), *EBA Opinion on 'virtual currencies'* (4 July 2014) EBA/Op/2014/8 p. 32-33
[61] FATF, *Virtual Currencies – Guidance for a Risk-Based Approach* (June 2015) p. 32

operator. By then, a total sales revenue of USD 1,2 billion (more than 9,5 million bitcoins) and USD 80 million in commissions for Silk Road was found to have been generated. Since transactions were conducted in bitcoins, the US Department of Justice seized approximately 173.991,00 bitcoins from seized computer hardware.

Bitcoins were the exclusive currency in Silk Road. Using bitcoins, in combination with operating on the hidden Tor network, offered the advantage of anonymity to participants, given that identification was based only on the anonymous bitcoin address, i.e. their account, and did not involve their identification as persons. In order to efficiently disguise the sources of their illicit proceeds, criminals who traded in Silk Road were using more than one bitcoin addresses, one for each transaction. Silk Road offered its users a cryptocurrency 'tumbler', or 'mixing service', i.e. a service aiming at mixing potentially identifiable or tainted cryptocurrency funds with others, so as to obscure the trail back to the fund's original source and thus achieve full anonymity bypassing the existence of a public ledger that records the history of all the transactions. Still, users of Silk Road were typically using additional 'anonymizers', beyond the above tumbler service, to diminish the possibility that the authorities could easily follow a trail leading to the initial transactions that they conducted.

In the above context, Silk Road's payment system functioned as a bitcoin bank where every user held an account in order to buy and sell on the site and also held one or many more bitcoin addresses linked with that user's account and stored on wallets maintained on servers that were administered by Silk Road. Buying and selling was realized with the implementation of a specific methodology. In particular, the user bought bitcoins through a bitcoin exchanger and sent them to a bitcoin address linked to his account. In this way, the account was provided with funds and was ready to be used for conducting a purchase. At the time of purchase, Silk Road transferred the user's bitcoins to an escrow account it held, while completion of the transaction was pending. Subsequently, the buyer's bitcoins were transferred from the escrow account to the bitcoin address of the seller. Furthermore, as discussed above, Silk Road was using a 'tumbler' in every purchase with the obvious intention,

as the site explained, '*to send all payments through a complex, semi-random series of dummy transactions making it nearly impossible to link your payment with any coins leaving the site'.*[62]

4.6 The transparency and non-transparency elements of the bitcoin network

The predominant characterization of the bitcoin network is 'pseudonymous' rather than 'anonymous' network. Indeed, the user's pseudonym, the bitcoin address that is, is recorded but the user's identity isn't. In particular, as described above, every transaction is recorded in the public ledger. The public addresses of the participants of specific transactions are visible and, consequently, all bitcoin transactions are traceable. Of course a public address cannot be linked directly to a person's identity and is only linked to an Internet Protocol Address (IP address), i.e. a unique numerical label assigned to each device participating in a computer network that uses the internet protocol for communication. This practically means that since public addresses in the bitcoin lead to IP addresses, then this would allow the discovery of the user's location and personal identity. However, users employed anonymizing software which hides a user's IP address and facilitates total anonymity.[63]

Given that there are no intermediaries who act as regulators or administrators, every transaction must be made public in order for all the participants to verify the validity of the transactions. Therefore, every single transaction is recorded in the online ledger. This very attribute of the bitcoin network constitutes the heart of the argument that bitcoin could actually be the most transparent payment method ever employed.[64] According to the reasoning of that argument, since every transaction is recorded and is publicly available in the block-chain, identities can be linked to

---

[62] FATF, *Virtual Currencies – Guidance for a Risk-Based Approach* (June 2015) p. 33-34

[63] Kavid Singh, 'The New Wild West: Preventing Money Laundering in the Bitcoin Network' (2015) 13 Nw. J. Tech. & Intell. Prop. Iii p. 42 <Hein Online> accessed 20 January 2017

[64] Dr. Tom Robinson, 'Bitcoin – through pseudonymity' (2015) http://www.moneylaunderingbulletin.com/risksandcontrols/technology/bitcoin--through-pseudonymity-111353.htm

bitcoin addresses, despite the fact that laundering tools like 'mixers' or 'tumblers' are employed by certain criminal users in their effort to break up the paper trail by exchanging one set of bitcoins for another with different addresses and transactions histories. These laundering tools might actually not perform their objective as far as large volumes are concerned and, additionally, the laundering process itself might be traced on the block-chain. In Silk Road, bitcoin transactions proved to be far from anonymous. The prosecution managed to furnish evidence, based on FBI's investigation results, that the accused person was indeed the operator of Silk Road as more than 700.000 bitcoins had been transferred from the Silk Road wallet directly to a wallet on the accused person's laptop. FBI's special agents managed to prove the aforementioned facts by investigating the transactions history recorded on the block-chain that formed a trail leading back to the criminal user whose identity was revealed.[65] The argument in favor of the existence of transparency in the bitcoin network estimates that, as in the case of Silk Road, identities can be linked to bitcoin addresses in many other cases as well. It should also be noted that the disclosure of both the user's bitcoin address and the user's identity to someone, perhaps in the case where the user transacts with an online retailer or with services that require information on the customer's identity, practically entails the leaking of the user's personal information which might, in turn, lead to the detection of all of the user's past and future transactions. In that context, law enforcement authorities always have a paper trail to follow when seeking the source of illicit funds and this renders bitcoin transactions traceable and, consequently, not particularly attractive to money launderers.[66]

On the other hand, one could hardly describe the bitcoin network as a fully transparent payment system, given that the identity of the users is not transparent. The lack of transparency and of easy access of the authorities to the personal information of the possible criminal user cannot be fully substituted by the possible

---

[65] Dr. Tom Robinson, 'Bitcoin – through pseudonymity' (2015) http://www.moneylaunderingbulletin.com/risksandcontrols/technology/bitcoin--through-pseudonymity-111353.htm

[66] Dr. Tom Robinson, 'Bitcoin – through pseudonymity' (2015) http://www.moneylaunderingbulletin.com/risksandcontrols/technology/bitcoin--through-pseudonymity-111353.htm

traceability based on the transactions' history recorded on the ledger, especially when complex software is widely used by criminals to obscure the trail of those transactions. Overall, notwithstanding that elements of transparency do exist in the bitcoin network, its inherent characteristics facilitate the conduct of transactions in an ultimately non-transparent manner. These main inherent features are relevant with the fact that there is no central administrative authority which could be subjected to regulation and, additionally, with the fact that the user's personal information remains hidden with only a mere possibility that this identity could be traced by law enforcement authorities. Consequently, due to the fact that criminal users could transact within the network while obscuring the trail that leads to the disclosure of their identity, one would be inclined to agree that the bitcoin network constitutes a 'friendly' environment for money laundering purposes.

4.7 EU regulation of bitcoin transactions

Payment transactions in a decentralized virtual currency, like bitcoin, are characterized by the absence of a third party intermediary. Instead, payments made in bitcoins are transmitted from buyer to seller through public and private keys functioning according to the principles of cryptography, while at the same the completed transactions are irreversible. In this context, the payment process in bitcoins falls outside the EU regulatory framework of electronic money and payment services.

In particular, virtual currencies like bitcoin do not incorporate a claim on an issuing state or banking authority, in contrast with electronic money which represent a claim on the electronic money issuer and are issued in exchange for funds. On the contrary, new bitcoins result from mining. Therefore, bitcoins do not constitute electronic money and do not fall under the scope of the EU Electronic Money Directive (2009/110/EC). Furthermore, bitcoins also fall outside the scope of the EU Payment Services Directive (2007/64/EC), regulating certain types of payment services by certain payment institutions. First of all, most of the provisions of the aforementioned Directive apply only to payment services made in euro or a currency of a Member State outside the euro area and, therefore, do not apply to

transactions in virtual currencies. Moreover, the payment service providers which fall under the Directive's scope and that might be considered relevant to virtual currencies, are e-money institutions and payment institutions. As noted above, bitcoins cannot be considered as electronic money. As far as payment institutions are concerned, they are defined by the Directive as entities authorized to provide and execute payment services, where payment services are defined as any business activity listed in the Annex to the Directive. If one examined how 'payment services' are defined in the Annex, one would find that in-scope payment services are the ones that funds are received from a payer without any payment accounts being created for the purpose of transferring a corresponding amount to another party. The definition of 'funds' is limited to banknotes, coins, scriptural and electronic money and, therefore, virtual currencies like bitcoins are excluded. Furthermore, under 'payment services' in the above Annex lies the description of services provided by technical service providers which support the provision of these services without entering into possession of the transferred funds at any time. Such technical service providers in the bitcoin network are generally the miners verifying the transactions and wallet developers. Therefore, such services do not fall under the scope of the Payment Services Directive.[67] Taking into account all of the above, a general conclusion regarding bitcoin transactions and their relationship with e-money and payment services would be that since bitcoin transactions do not involve any processing by third parties other than the verification process, they seem to resemble closer to cash transactions. However, cash transactions are specifically excluded from the PSD.

Directive (EU) 2015/849, or '4AMLD', did not include a reference to virtual currency exchanges. However, after the terrorist attacks in France in 2015, the Commission published an *Action Plan to strengthen the fight against the financing of terrorism* on 2 February 2016. In this Plan, the Commission proposes that certain aspects of the Directive should be re-examined towards the direction of building a more efficient defense against terrorist finance. One of these aspects was the issue of anonymity

[67] Lucy Frew, Rich Folsom and Sophie van Wingerden, 'Legal and regulatory issues relating to virtual currencies' (July/August 2015) 7 JIBFL 438B

associated with the purchase and use of virtual currencies. On 5 July 2016 the Commission published its proposals for amendments to the 4AML Directive in response to the EU Council's conclusions of February 2016 on the fight against the financing of terrorism and following the parallel resolution and report of the European Parliament in May 2016, in which the EP proposed that the Commission develop recommendations for any legislation required to regulate the virtual currencies sector.

The aforementioned proposals of the Commission included taking actions to bring custodian wallet providers and virtual currency exchange platforms within the scope of the Directive as obliged entities. As a result, these entities would be obliged to adopt policies that aim at detecting, preventing and reporting money laundering and terrorist financing. Moreover, the Commission proposes that the particular entities should be subject to licensing requirements and that those who own or manage these entities be subjected to 'fit and proper testing'.[68] The Council of the EU confirmed the plans of the Commission to regulate both exchanges and wallet providers, however the European Commission decided recently to delay new anti-money laundering legislation, i.e. to amend the 4AMLD, until June 2017 at the latest.

In particular, an analysis of the above Commission's proposals would lead to the conclusion that there is a call for alarm regarding the use of bitcoins as they are considered as *easy to use in facilitating anonymous funds transactions for criminal purposes.*[69] In case of implementation of these proposals, exchangers and wallet providers that administer transactions between fiat and virtual currencies would likely be required to turn over client lists to authorities. Moreover, the Commission seems to consider the possibility of establishing a mandatory database of digital currency users in order to prevent anonymity of digital money traders. National financial intelligence units will be issued more powers, including the ability to

---

[68] European Banking Authority (EBA), *'Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the Scope of Directive (EU) 2015/849 (4AMLd)'* (11 August 2016) EBA/Op/2016-07 p. 2

[69] Michael Scott, 'EU State-By-State Regulation of Bitcoin, Digital Currencies: What are the implications?' (2015) https://bitcoinmagazine.com/articles/eu-state-by-state-regulation-what-are-the-implications-1480975527/

demand information from banking and financial services firms, regardless of whether reports of suspicious activities have been issued. Finally, the beneficial owners of the aforementioned business entities will be more closely monitored for tax evasion purposes and will be subject to severe non-compliance penalties.[70]

4.8 Should bitcoins be regulated for anti-money laundering purposes?

Even though the expansion of the use of bitcoin as a currency remains relatively limited, retailers, consumers and investors would probably welcome the existence of clear rules regarding the treatment of bitcoin in terms of regulation and taxation. Such clear and sensible rules that would include reasonable taxes and non-excessive administrative procedures, would give rise to the confidence of a great number of users in bitcoins and limit investors' concerns[71]. On the other hand, opponents to bitcoin regulations feel that regulation will have a negative impact on the growth of digital assets. Furthermore, concerns are expressed that regulation in some developed countries will drive exchanges to countries with lower compliance standards and that transaction costs combined with administrative costs of regulation would outweigh the benefits since millions of users would be subjected to regulation.[72]

In the context of anti-money laundering strategies and on the question of whether bitcoin should be regulated or not, it seems obvious that the complete lack of a regulatory framework would encourage criminals to pursue disguising their proceeds of crime through a system that fosters anonymity. A balance should be pursued between fostering the positive impacts of the use of bitcoin on the economy on the one hand, such as the promotion of innovation and technology, benefits for consumers like payments with extremely small fees, zero maintaining balance and no credit checks requirements and even larger-scale effects like social and solidarity

[70] Michael Scott, 'EU State-By-State Regulation of Bitcoin, Digital Currencies: What are the implications?' (2015) https://bitcoinmagazine.com/articles/eu-state-by-state-regulation-what-are-the-implications-1480975527/

[71] David Descoteaux, 'How Should Bitcoin Be Regulated?' (June 2014) http://www.iedm.org/files/note0514_en.pdf

[72] Nicole D. Schwartz, 'Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as a Security or Commodity' (2014) 17 Tul. J. Tech. & Intell. Prop. 319 2014 p. 328

finance through block-chain technology in the under-developed countries, and avoiding fostering criminal activities through the bitcoin network on the other.

The ideal regulatory framework that would achieve such a balance would be the one that implemented increased levels of transparency in the bitcoin marketplace[73] and would render the bitcoin network a less attractive field of action for criminals. In this context, bitcoin miners should be required to register with an authority and follow predetermined guidelines, while bitcoin exchanges should be also subject to reporting requirements. The aforementioned Commissions' proposals to be included in the amendment of the AML Directive constitute a step to this very direction, given that they render participants of the bitcoin marketplace, such as bitcoin currency exchange and wallet providers, obliged entities. These changes in the EU anti-money laundering legislation would promote transparency, deter money launderers from using virtual currencies and protect bitcoin investors at the same time.

Conclusions

The 'money laundering' term describes the methods and strategies employed by criminals who wish to disguise their proceeds of crime and present them as having been acquired otherwise than by crime.[74] An international regulatory framework has been developed aiming at preventing and detecting the circulation of illegal funds in the financial system through the delegation of police powers to financial institutions and other legal entities or natural persons. In the context of EU legislation, the 4th money laundering Directive plays a predominant role in the fight against money laundering. The basic provisions of the Directive lead to the direction of implementing transparency principles as regards the identity and personal information of the ultimate beneficial owners of financial assets, e.g. the set-up and maintenance of a register of beneficial owners in each Member State. Amongst the proposed amendments to the 4th AML Directive, stands-out the designation of

[73] Nicole D. Schwartz, 'Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as a Security or Commodity' (2014) 17 Tul. J. Tech. & Intell. Prop. 319 2014 p. 335
[74] Peter Alldridge, 'Money Laundering and Globalization' (2008) 35 J.L. & Soc'y 437 2008 p. 441

certain entities, which perform business activities in the area of bitcoin trading, as ‘obliged entities’, i.e. they will be regulated and thus take on the obligation to monitor or report information on their client’s identities.

The vulnerability of the securities sector to money laundering activities is extremely high, given the complexity, the ease and the speed of the executed transactions which may very well be conducted in a cross-border framework. The degree of vulnerability is even higher in the case of intermediated holding systems which, by nature, are designed to foster the conduct of complex transactions in a fast and non-complicated manner, while the identity of the investors is not recorded in a central register and is not revealed by documentation concluded between upper-tier intermediaries due to the fact that their contractual obligations do not include the fulfillment of duties towards the investor. This so called ‘no-look-through’ principle in this particular holding system creates a gap between the investor and the issuer, including the upper-tier intermediaries as well, that creates legal, technical and practical difficulties in identifying easily the investor and subsequently the source of the funds used to acquire the traded securities. As a result, law enforcement authorities would have an extremely difficult task to perform in identifying the beneficial owners of securities that are held by an upper-tier intermediary, probably in an omnibus account. In that context, transparency requirements within the framework of anti-money laundering policies seem to clash with the inherent limitations of transparency in the intermediated holding system. The only logical solution, if considered as technologically feasible, is the creation of a central register within the intermediated holding system where the identities of investors would be kept and be easy to access upon legitimate inquiries by law enforcement and judicial authorities.

Not only in the intermediated securities area, but also in bitcoin trading, transparency problems seem to create a ‘friendly’ environment for potential money launderers. In particular, the fact that bitcoin constitutes a cryptocurrency where users operate under pseudonyms does not allow the identification of possible criminals who exploit the network for money laundering purposes. Indeed, while the

history of all transactions is recorded in the so-called 'block-chain' and is publically accessible, the users can hide their identities by employing anonymizing software. The Commissions' proposals for the amendment of the 4th Money Laundering Directive, in relation to regulating virtual currencies, constitute a step to the right direction as they impose transparency requirements to entities that are involved in bitcoin trading.

In general, as regards both the intermediated holding system and the bitcoin network, there is a common conclusion to be drawn: Any limitations posed on authorities acting under the requirements of the law in the fight against money laundering, whether these limitations are inherent or created by insufficient or ineffective legislation, regarding the fast and easy access to the personal information of investors in securities and bitcoin users, should be confronted with. In this context, the anonymity of both investors in securities and users of bitcoin is less than helpful in the fight against money laundering as it renders the connection between the proceeds of crime and the criminal difficult and unclear.

BIBLIOGRAPHY

Rudi Fortson, 'Intensifying anti-money laundering laws-the last 30 years' [2016] Archbold Review, 4, 6-9

Barry Vitou, Michael Ruck and Elena Elia, 'Anti-money laundering: can money laundering really be prevented?' [2016] Compliance & Risk 2016, 5(5), 2-5

Peter Reuter and Edwin M. Truman, *Chasing Dirty Money – The Fight against Money laundering* (November 2004) chapter 3

Stephen Schneider, 'Money Laundering through securities an analysis of Canadian Police cases' [2004] 4 Asper Rev. Int'l Bus. & Trade L. 169 2004

Luc Thevenoz, 'The Geneva Securities Convention: objectives, history, and guiding principles' in Pierre – Henri Conac, Ulrich Segna and Luc Thevenoz (eds), *Intermediated Securities The Impact of the Geneva Securities Convention and the Future European Legislation* (Cambridge University Press 2013)

Roy Goode, Herbert Kronke and Ewan McKendrick, *Transnational Commercial Law - Text, Cases and Materials* (Second edition published in 2015 by Oxford University Press)

Louise Gullifer, 'Ownership of Securities - The Problems Caused by Intermediation' in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities Legal Problems and Practical Issues* (Hart Publishing 2010)

Hideki Kanda, Charles Mooney, Luc Thevenoz, Stephane Beraud assisted by Thomas Keijser, *Official Commentary on the Unidroit Convention on Substantive Rules for Intermediated Securities* (Oxford University Press 2012)

Eva Micheler, 'Transfer of Intermediated Securities and Legal Certainty' in Thomas Keijser (ed), *Transnational Securities Law* (Oxford University Press 2014)

Nora Rachman and Maria Vermaas, 'Corporate Actions in the Intermediated System: Bridging the Gap Between Issuer and Investor' in Thomas Keijser (ed), *Transnational Securities Law* (Oxford University Press 2014)

Marek Dubovec, *The Law of Securities, Commodities and Bank Accounts – The Right of Account Holders* (Edward Elgar Publishing 2014)

Wolfgang Hetzer, 'Money Laundering and Financial Markets' (2003) 11 Eur. J. Crime Crim. L. & Crim. Just. 264 2003

Kavid Singh, 'The New Wild West: Preventing Money Laundering in the Bitcoin Network' (2015) 13 Nw. J. Tech. & Intell. Prop. Iii <Hein Online> accessed 20 January 2017

Lucy Frew, Rich Folsom and Sophie van Wingerden, 'Legal and regulatory issues relating to virtual currencies' (July/August 2015) 7 JIBFL 438B

Catherine Martin Christopher, 'Whack-a-mole: Why prosecuting digital currency exchanges wont' stop online money laundering' (2014) 18 Lewis & Clark L. Rev. 1 <Hein Online> accessed 20 January 2017

David Steven Brown, 'Cryptocurrency and criminality: the Bitcoin opportunity' (2016) Pol. J. 327

Jeffrey E. Alberts & Bertrand Fry, 'Is Bitcoin a Security?' (2015) B. U. J. SCI. & TECH. L. Vol. 21:1 <Hein Online> accessed 20 January 2017

Catherine Martin Christopher, 'Whack-a-mole: Why prosecuting digital currency exchanges won't stop online money laundering' (2014) 18 Lewis & Clark L. Rev. 1 <Hein Online> accessed 20 January 2017

Prableen Bajpai, 'Bitcoin Remittances: How to send money home' (March 8, 2016) http://www.investopedia.com/articles/investing/030816/world-will-soon-use-bitcoin-send-money-home.asp accessed 10.2.2017

Dr. Tom Robinson, 'Bitcoin – through pseudonymity' (2015) http://www.moneylaunderingbulletin.com/risksandcontrols/technology/bitcoin--through-pseudonymity-111353.htm

Michael Scott, 'EU State-By-State Regulation of Bitcoin, Digital Currencies: What are the implications?' (2015) https://bitcoinmagazine.com/articles/eu-state-by-state-regulation-what-are-the-implications-1480975527/

David Descoteaux, 'How Should Bitcoin Be Regulated?' (June 2014) http://www.iedm.org/files/note0514_en.pdf

Nicole D. Schwartz, 'Bursting the Bitcoin Bubble: The Case to Regulate Digital Currency as a Security or Commodity' (2014) 17 Tul. J. Tech. & Intell. Prop. 319 2014

Peter Alldridge, 'Money Laundering and Globalization' (2008) 35 J.L. & Soc'y 437 2008

T. Papakyriakou, (2017), 'The international regulatory framework for the prevention and suppression of money laundering: the rising and establishment of a new model of anti-crime policy' Lecture presented at the Seminar of Aristoteleion University of Thessaloniki Contemporary: 'Current legal issues of financial transactions' 2-4/2/2017

Moneyval, *Typology research – Use of securities in money laundering schemes* (2008) Problem Overview Chapter 1

FATF, *Money Laundering and Terrorist Financing in the Securities Sector* (October 2009)

Financial Crime Compliance Principles for Securities Custody and Settlement – Background and Overview, International Securities Services Association (ISSA), 6 October 2015 http://issanet.org/pdf/2015-10-05_ISSA_Background_Overview_Final.pdf

The International Securities Services Association (ISSA), *Financial Crime Compliance Principles for Securities Custody and Settlement* (27 August 2015

European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, *Cross-border issues of securities law: European efforts to support securities markets with a coherent legal framework* (IPA/ECON/NT/2011-09 MAY 2011)

Final Report of the Committee of Wisemen on the Regulation of European Securities Markets (Brussels, 15 February 2001)

The Giovanini Group, *Cross-border Clearing and Settlement Arrangements in the European Union* (Brussels, November 2001)

European Banking Authority (EBA), *EBA Opinion on 'virtual currencies'* (4 July 2014) EBA/Op/2014/8

The International Organization of Securities Commissions, *Principles on Client Identification and Beneficial Ownership for the Securities Industry* (MAY 2004)

Pwc, 'Global financial markets liquidity study' (August 2015) https://www.pwc.com/gx/en/financial-services/publications/assets/global-financial-market-liquidity-study.pdf accessed 28-1-2017

International Monetary Fund (IMF), *Virtual Currencies and Beyond: Initial Considerations* (January 2016)

FATF, *Virtual Currencies – Guidance for a Risk-Based Approach* (June 2015)

4th Money Laundering Directive, 2015/849/EU