**Revista Jurídica** vol. 04, nº. 57, Curitiba, 2019. pp. 83 - 115

# LEGAL REMARKS ON THE OVERARCHING COMPLEXITIES OF CRYPTO ANTI-MONEY LAUNDERING REGULATION

# *COMENTÁRIOS JURÍDICOS A RESPEITO DAS COMPLEXIDADES SOBREJACENTES À REGULAMENTAÇÃO DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO COMETIDA ATRAVÉS DE CRIPTOATIVOS*

**GUSTAVO RABAY GUERRA**

Partner at Rabay, Palitot e Cunha Lima Law Firm and Founder of Legal Mind Academy (Legal Business EdTech), with a focus in compliance, corporate governance, cyberlaw and data privacy. Professor of Law at the Federal University of Paraíba (UFPB) and UNIPÊ. Ph.D. in Law, State and Constitution at the University of Brasília. Master in Public Law (M.Sc. LL.M.) at the Federal University of Pernambuco (UFPE). E-mail: *rabay@me.com*

**HENRIQUE JERÔNIMO BEZERRA MARCOS**

Researcher at the Center for Studies in International Courts (Núcleo de Estudos em Tribunais Internacionais – NETI-USP) of the University of São Paulo (USP). Ph.D. Candidate in International and Comparative Law at the University of São Paulo (USP). Master of Legal Sciences (M.Sc. LL.M.) at the Federal University of Paraíba. Professor of Scientific Methodology at "Mentoria da Pesquisa em Direito". ORCID: *https://orcid.org/0000-0003-0259-5530*. E-mail: *henriquemarcos5@gmail.com*

## ABSTRACT

**Objective:** The paper analyzes money laundering through crypto-assets and offers a legal perspective on how this new technology can be used to commit these felonies. The study intends to shed light on the matter, helping to visualize how future anti-


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

money laundering – AML regulation should focus on tackling crypto criminal activity effectively.

**Methodology:** The research adopts an inductive approach, bibliographic and documental research technique, with an exploratory and propositional methodological objective.

**Results:** The paper proposes the following framework of anti-money laundering principles for crypto-focused action: transnational approach for AML action; going beyond basic gatekeeper compliance approach, considering the lack of structural chokepoints in a blockchain protocol; private-sector cooperation and clear AML standards; usage of tracking and reverse-engineering anonymization techniques for the tracing of crypto transaction history; and adoption of a global blacklist for crypto-asset prefixes, preventing money laundering integration.

**Contributions:** The study addresses a topic that is still unfamiliar in the academic world due to its innovation and complexity, as well as elaborates a set of principles to combat money laundering with crypto-assets that could be of great value to companies and financial institutions.

**KEYWORDS:** Crypto-assets; crypto-currencies; bitcoin; blockchain; money laundering.

## RESUMO

**Objetivos:** O artigo analisa a lavagem de dinheiro através de ativos criptográficos e oferece uma perspectiva jurídica sobre como essa nova tecnologia pode ser usada para cometer tais crimes. O estudo busca esclarecer o assunto, ajudando a visualizar como a futura regulação contra a lavagem de dinheiro cometida através destes ativos deve ser estruturada para assegurar efetividade.

**Metodologia**: A pesquisa adota uma abordagem indutiva, a técnica de pesquisa é bibliográfica e documental, seu objetivo metodológico é exploratório e propositivo.

**Resultados:** O artigo propõe o seguinte conjunto de princípios para o combate à lavagem de dinheiro com criptoativos: a abordagem transacional para combate à lavagem de dinheiro; ir além de uma abordagem focada em intermediários, considerando a falta de pontos de estrangulamento em um protocolo block chain; a cooperação com o setor privado e padrões claros de compliance para prevenção à lavagem de dinheiro; uso de técnicas de rastreamento e de engenharia reversa para processos de ocultação de histórico de transações; e a adoção de listas sujas globais para evitar a fase de integração do processo de lavagem de dinheiro com criptoativos.


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

**Contribuições:** O estudo aborda um tema ainda muito pouco divulgado no meio acadêmico devido à sua inovação e complexidade, bem como elabora uma proposta de conjunto de princípios para o combate à lavagem de dinheiro com criptoativos que poderá ser de grande valia para empresas e instituições financeiras.

**PALAVRAS-CHAVE**: Criptoativos; criptomoedas; bitcoin; blockchain; lavagem de dinheiro.

## INTRODUCTION

Blockchain and crypto-assets (a comprehensive set that encompasses cryptocurrencies[1] and other blockchain-based tokens)[2] are new technologies that – even though not yet fully implemented – are already affecting the way the world understands money, value, and ownership. It is a computational and financial breakthrough with an array of potential benefits for individuals and societies from developed and developing States alike.[3]

[1] "[…] although most of the studies on blockchain are centered on the presence of a cryptocurrency such as Bitcoin; cryptocurrencies are mere applications of blockchain and they are only definitional. The essence of blockchain is related to a certain method of processing information and it does not have to be directly related to any monetary platform. Cryptocurrencies are powerful applications of the blockchain and their use has revealed much about the current and potential weaknesses and strengths of the technology. Bitcoin is in fact the first real applied example of a blockchain […] Blockchains can be designed without any application of their use as a cryptocurrency per se. That said, in financial applications, some sort of a "token" is still needed to record and transfer values of assets." [AKGIRAY, 2018, p. 6].

[2] A generally accepted taxonomic classification of crypto-assets divides them into three general categories. The first one is the cryptocurrencies, also known as payment tokens, which are designed as a means of payment, enabling users to acquire goods or services in a given system or achieving market value through trade. A second category is the utility tokens which provide digital access to an application or service. Finally, there are security or asset tokens, which represent assets such as shares in real values, companies, securities, and similar valuables (asset tokens are a species of crypto-assets and not a synonym). These categories are not mutually exclusive; it is possible for a token to be a hybrid between two or three categories [SWISS CONFEDERATION, 2018, p. 46].

[3] "Over the past two years, [World Food Programme] WFP has been using innovative technologies, notably blockchain, to enhance its ability to provide effective, efficient food assistance to the people it serves. WFP's efforts to use the latest technologies to better provide refugees with food are a good example of how tech can help accelerate progress on the [United Nations] UN's 17 Sustainable Development Goals (SDGs), notably – SDG 1: No Poverty and SDG 2: Zero Hunger.". [SMITH, 2018].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

Nevertheless, like any instrument, it is only as good as its user; some groups use the technology as a tool for felonies such as money laundering[4] and the financing of criminal and terrorist activities.[5 - 6] Differently from other criminal techniques, however, given their underlying technical characteristics, crypto-assets offer a unique set of complexities that must be considered by policymakers when enacting anti-money laundering – AML acts. In this sense, this paper aims to analyze and offer a legal perspective into some of the complexities that can be brought forward on regulation focused on fighting crypto-money laundering.

It is paramount that the transformations which criminal law and procedure undergo are subject to prior critical debate with a firm understanding of legal aspects and their underlying technical elements. The matter at hand should be studied in a systematic perspective capable of tackling the subject in its core technological facet and its legal consequences. Thus, this research intends to contribute to the debate concerning the criminal regulation of these new technologies, offering a critical judicial perspective into a highly technical discussion that is sometimes unfamiliar to the regulator and its legal subjects.

In order to do so, the paper will analyze crypto-assets from a technical perspective; presenting their critical technologic characteristics while correlating these aspects with the inherent risks of their usage for money laundering. Afterward, it will

[4] For the purposes herein, “money laundering”, pursuant to the United Nations Convention Against Transnational Organized Crime of 2000, is understood as the process by which “dirty money”, i.e., money obtained through crime, is cleaned in a way that is, or at least appears to be, legitimate money, with no signs of their criminal origin; the source of illegally obtained funds is obscured by one or more procedures so that the same funds may eventually be re-submitted as legitimate income. [BOOTH et al., 2011].

[5] For the purposes herein, “terrorism” and “terrorist activity” is understood in the definition given by Security Council Resolution 1.566 of 2004, as all criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism [MULLER; KÄLLIN; GOLDSWORTH, 2007].

[6] With the September 11, 2001 attack on the World Trade Center ("9/11"), national and international entities have established a link between the practice of money laundering and the financing of terrorism. Regulators hope that the methodology used to combat money laundering could be used to combat terrorism “[...] because of the pervasiveness and expansiveness of the financial foundation of foreign terrorists, financial sanctions may be appropriate for those foreign persons that support or otherwise associate with these foreign terrorists.” [UNITED STATES OF AMERICA, 2001].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

propose a specific framework of preliminary framework of principles for crypto-AML targeted towards policymakers and law enforcement agents. Concerning its methodology, the research adopts an inductive theoretical approach; the research technique is of a bibliographic and documental survey; its methodological objective is exploratory and propositional.

## 2 DISTRIBUTED PEER-TO-PEER ARCHITECTURE

In 2008, the world watched in awe as a series of traditional financial institutions in the United States – US and around the globe crumbled down into bankruptcy [LINDSEY, 2016].[7] The timeframe was also the stage for the individual (or group of individuals) identified as Satoshi Nakamoto to release the whitepaper[8] for a peer-to-peer electronic cash system known as Bitcoin [NAKAMOTO, 2008].[9]

According to Nakamoto, Bitcoin is a technology that presents an alternative to the contemporary financial model based around banks and similar financial institutions. The current paradigm is dependent on entities acting as intermediaries processing transactions between parties. This mediation by the trusted third party is necessary because there is widespread suspicion among contractual agents [GRUBER, 2013, p. 142]. Mistrust is maximized in relations through the internet where, usually, users are unknown to each other [NAKAMOTO, 2009]. Operations run through powerful intermediaries who are charged with overseeing the system, ensuring the safety of the financial transactions. This model, however, presents some fragilities if observed from

[7] The Financial Crisis of 2008 was an economic crisis caused, among other reasons, due to abuse of easily granted credit. Notably, in the United States, "subprime loans," i.e., mortgage loans granted to small-income families without considering their solvency for repaying these loans. The collapse of the real estate market caused widespread panic in the financial services, which, in turn, led to the bankruptcy of financial institutions such as "Lehman Brothers." Albeit originating in the United States, the crisis caused devastation in the globalized economy affecting European, Asian, and Latin American States alike [VAÏSSE, 2017].

[8] "Whitepaper" is a document published by a Government or an organization intended to serve as a report or guide. It is not unusual for a crypto asset to have a whitepaper released explaining its purposes, characteristics, and operational characteristics from a legal, commercial, technical and economic perspective.

[9] Bitcoin is also known by its ticker symbol "BTC" or "XBT".


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

a structural perspective.[10] It is even possible to argue that one of the causes of the 2008 crisis was the over-centralization of power in banking institutions and credit rating agencies [HODOROV, 2011, p. 42].

On the other hand, Bitcoin and crypto-assets are characterized as a distributed peer-to-peer system, i.e., devoid of centralized intermediaries [LEÃO; VIEGAS, 2017]. The technology presents a possible solution to the classic "Byzantine General's Problem"; a hypothetical consensus or agreement problem involving mutually-suspicious agents who have conflicting interests in a scenario lacking a centralized authority but must agree on a concerted strategy to avoid global catastrophe.[11] A possible solution to the enigma is presented through the root technology that makes the operation of crypto-assets possible: the blockchain protocol.[12]

Blockchain works by bridging two concepts: distributed ledger technology – DLT and block chaining. A distributed ledger is an open register that is managed by a network of users who have a similar hierarchy; there is no central authority responsible for recording operations in the ledger, the responsibility is shared (distributed) to all users of the Blockchain network.[13] In addition, the records are resistant to modification

[10] "The centralized network is obviously vulnerable as destruction of a single central node destroys communication between the end stations. In practice, a mixture of star and mesh components is used to form communications networks. […] Since destruction of a small number of nodes in a decentralized network can destroy communications, the properties, problems, and hopes of building "distributed" communications networks are of paramount interest.". [BARAN, 1963, p. 1-3].

[11] The "Byzantine General's Problem" also known as "Byzantine Fault" is a problem of epistemic modal logic. In the hypothetical scenario, a part of the Byzantine armies surrounds a city. Some of the generals wish to formulate a plan to attack the city, while others prefer to retreat. With these two possibilities (attack and retreat), a coordinated decision is paramount. It does not matter if the decision is to attack or retreat; the importance is that the decision is executed in an organized fashion by all parties. It is imperative for the survival of the army as a whole that the generals agree to a collective decision – a frail attack would be a cause to a defeat worse than a coordinated attack or retreat. The situation worsens when one considers that there are treacherous generals who can vote selectively, indicating that they intend to attack a part of the other generals and passing the vote of withdrawal to another part; this is called double-spending, i.e., double voting. [LAMPORT; SHOSTAK; PEASE, 1982, p. 382].

[12] "Bitcoin's invention is revolutionary because for the first time the double-spending problem can be solved without the need for a third party. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the bitcoin economy is registered in a public, distributed ledger, which is called the block chain. New transactions are checked against the block chain to ensure that the same bitcoins haven't been previously spent, thus eliminating the double-spending problem. The global peer-to-peer network, composed of thousands of users, takes the place of an intermediary; [...]" [BRITO; CASTILLO, 2013, p. 4].

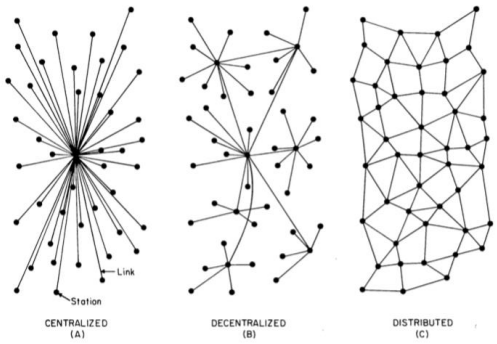
[13] This is the case in the Bitcoin Blockchain and some other Blockchains which can be considered public. There are, however, DLTs with limitations and restrictions in place, i.e., permissioned networks (private Blockchains). [XU et al., 2017].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

due to the cryptographic hash chaining of data blocks which create a growing list of ciphered information following a "Merkle Tree" [14] format; this is called the block chaining [WATTENHOFER, 2017, p. 62].

Operations with crypto-assets are authenticated through encryption and the work of a distributed network of "miners," i.e., users that allow the protocol to use the computational power of their machines to verify and register operations on the blockchain by solving complex mathematical problems (block creator) [WATTENHOFER, 2017, p. 112]. In exchange for their service, miners are rewarded with crypto-assets. It is the case in the Bitcoin protocol, but it is not absolute; some blockchain protocols do not adopt miners and others while adopting them have different rules for their operation (v.g., Iota and the Tangle protocol) [POPOV, 2018]. Mining is, under certain conditions, a productive activity; it is not unusual for companies to structure dedicated mining enterprises through an organized set of computers exclusively dedicated to the activity [LEWENBERG et al., 2015, p. 920].

**Figure 1 -** Centralized, Decentralized and Distributed Networks




**Source:** BARAN, 1963.

In this sense, as a general rule, the operation of blockchain protocols are distributed and independent, following only the mathematical rules imbued in its programming. For instance, there is no centralizing entity responsible for Bitcoin as a crypto-asset; it is not a company in the sense that a social media platform such as

[14] The expression "tree" is used in computer science to describe an upside-down branching data structure. The "Merkle Tree" is also known as a "Binary Hash Tree" and is a data structure which is generally used to summarize and verify the integrity of large data sets in an efficient manner. [ANTONOPOULOS, 2010, p. 170].

Facebook is.[15] Therefore, there is no individual or organization with the power to hold, prevent, censor, or return an operation [ANTONOUPOLOS, 2016, p. 2]. There is not even a command which can be operated to retrieve a lost access key.[16]

Its distributed nature, i.e., the absence of centralized intermediaries, is part of the very essence of crypto-assets, one of its most significant innovations, and the source of one of the leading legal complexities overlying the technology. Crypto-assets transactions operate peer-to-peer; this architecture offers an unprecedented potential for the empowerment of individuals and oppressed groups. It takes the decision-making powers which are traditionally in the hands of a small group of intermediaries such as Governments and multinational companies and places it on the hand of anyone who has access to the internet.

It is arguably the next step in the online revolution. Just as the internet enhanced the ability of individuals to exercise their freedom of expression by denouncing to the whole world the wrongdoings of a despotic dictatorship; crypto-assets make it possible to fund a revolution to overthrow that Government through donations from around the globe without any clear restrictions.[17] Along these lines, nothing is preventing the use of this technology with less than ideal intentions. The same characteristics that make crypto-assets attractive as an alternative financial system could also allow the evasion of taxes, illicit trade, money laundering, and the financing of criminal organizations and international terrorism [BRITO; CASTILLO, 2013, p. 1].

[15] "The architecture of bitcoin is peer-to-peer because every participant in the network speaks the bitcoin protocol on an equal level. There are no special bitcoin nodes; all nodes are the same. Peer-to-peer means that when you send a transaction to the network, every peer treats it the same. It has no context inside the peer's system other than what it gets from the network. An interesting issue in distributed systems is this issue of context and state. If you log in to Facebook and you have an account with Facebook, you're not using a protocol. All of the state is controlled by Facebook. You have a login session and all of the data is held by them. We call that architecture client-server. Bitcoin is different because it's peer-to-peer, just like email or TCP/IP.". [ANTONOPOULOS, 2016, p. 16].

[16] It is estimated that around four million Bitcoins are definitely lost because their holders lost the public or private keys that gave access to the digital assets. [RAPP; ROBERTS, 2017]

[17] "When an Egyptian blogger can not only blog about the revolution but also fund that revolution in bitcoin, and they can connect with people around the world who share their ideas for self-determination and freedom, they are expressing their own sovereignty as an individual, and they are expressing the sovereignty of their community through the use of that currency." [ANTONOPOULOS, 2016, p. 74].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

Concerning money laundering specifically, there is a clear correlation between the transnational potential of crypto-assets and the cross-border design of contemporary large-scale money laundering [FEDERAL BUREAU OF INVESTIGATION, 2012].[18-19] International and almost instantaneous electronic money transfers made possible through the internet and the globalized world are already a well-known challenge to AML law enforcement; which are forced to continuously develop and adopt specific techniques for cooperation between agencies, the private sector and even among criminals through witness immunity and leniency agreements [SILVA; SILVA; BRAGA, 2017, p. 31].

In electronic transfers executed through traditional means, there is – at some point in these operations – a need for an intermediary (a financial institution, *lato senso*); at these chokepoints, it is possible to adopt specific techniques for private-sector AML compliance [TURNER, 2011, p. 89]. The monitoring and collaboration with these intermediaries (gatekeepers) through a supervision and cooperation approach is considered a reasonably effective means to prevent and combat conventional financial system money laundering thus far [BANK POLICY INSTITUTE, 2018] [HUANG, 2015, p. 532]. Crypto-assets could be a turning point to these procedures, however.

As mentioned, crypto-based money transfers are peer-to-peer, i.e., operate without the necessary intervention of a third party. There are no clear gatekeepers in a distributed network – a cardinal characteristic of this architectural design [BARAN, 1963]. Hence, without gatekeeper intermediaries, it is not clear whether conventional private-sector compliance techniques could be sufficient for crypto-AML action.

[18] "Bitcoin will likely continue to attract cyber criminals who view it as a means to move or steal funds as well as a means of making donations to illicit groups. […] Since Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records - problems that might attract malicious actors to Bitcoin. Bitcoin might also logically attract money launderers and other criminals who avoid traditional financial systems by using the Internet to conduct global monetary transfers." [FEDERAL BUREAU OF INVESTIGATION, 2012].

[19] "The design of large-scale money laundering nearly always includes cross-border elements, since money laundering is a worldwide, global cooperation. […] As technology has increased, it has simplified both the mechanisms for moving money and the incentive to use the global financial network for both individuals and organizations involved in crimes that involve the crime of money laundering. Making use of jurisdictional differences as well as differences in laws and treaties around the globe, criminals moving money internationally present unique challenges to the investigation.". [TURNER, 2011, p. 12].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

Likewise, considering the difficulty of ensuring adequate supervision, it does not seem feasible to require every user to adopt an individually-based AML compliance program.

Notwithstanding, some business models act as intermediaries for crypto-transactions such as online crypto-exchanges, i.e., traditional businesses that provide a user-friendly online environment for intermediating the purchase and sale of crypto-assets and the barter of different kinds of crypto-assets and between users. These companies could be submitted to AML private-sector compliance requirements similar to the financial sector.

Nevertheless, on principle, these businesses are redundant and unnecessary; any educated user can circumvent the AML compliant exchanges and operate transactions in a peer-to-peer fashion. Even if all crypto-based businesses were to, hypothetically, adopt AML compliance standards and ensure their fulfillment by consumers and employees, any private individual interested in committing criminal offenses through crypto-assets would be able to use the internet to conduct their illegal activities. Be it through a darknet[20] agent such as Silk Road[21] or direct peer-to-peer operations [KETHINENI; CAO; DODGE, 2018].

## 3 CRYPTO-PSEUDONYMITY, PRIVACY COINS AND CRYPTO-MIXING

The question of owning a crypto-asset is a complex one; users do not guard these digital assets in the traditional sense of physical ownership. To “own” a crypto-

[20] “[…] Darknet, differs from the surface web and Deep Web in two ways. First, unlike websites found on the surface web, websites categorized as a part of the Darknet are unsearchable through conventional search engines. A visitor must know where to find the Darknet to access it. Distinguishing Darknet from the Deep Web is the requirement of specialty browsers (e.g., the Onion Router, also known as Tor, which was created by the U.S. Naval Research Laboratory for anonymous online communication; […]). It is open and free to everyone. It allows users to browse the Internet while protecting them from surveillance and traffic analysis by routing connections through third-party proxy servers, obscuring the IP address of the user. […] The Wired magazine estimates that the Darknet accounts for no more than 0.1% of the Internet. However, due to the anonymity and security that the Darknet provides, it is often used by cybercriminals for illegal activities. It has been reported that 57% of Darknet content is illegal, such as pornography, illicit finances, drug hubs, weapons, and terrorist communications […]”. [KETHINENI; CAO; DODGE, 2018].

[21] “The most infamous Darknet is probably the Silk Road, an online market- place known for facilitating sales of illegal products, especially drugs […] Ross William Ulbricht created the Silk Road in 2011. On the Silk Road, drugs, and other illegal products (e.g., stolen credit cards) and services (including murder for hire) are sold from dealer to doorstep […]. Bitcoin was the only accepted currency on the Silk Road. During its two years of successful operation, the Silk Road made over US$1.2 billion.”. [KETHINENI; CAO; DODGE, 2018].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

asset means only that one has access to both cryptographic keys – public and private – for the digital wallet where that asset is at that moment. The public key is the identifier that distinguishes an address by allowing anyone to verify if an operation came from the digital wallet where it claims it did. The private (secret) key, on the other hand, is used to digitally sign an operation; which, in turn, can be verified through the public key. Anyone who knows both the public and private key for the digital wallet effectively "owns" the crypto-asset [SWAN, 2015].

The keys are an alphanumeric code which represents the address of the digital wallet but holds no particular information indicating who is the person behind the operation.[22] These operations are pseudonymous;[23] there is a digital code for each wallet, but there is no direct indication of who that user is in the physical world [DRESCHER, 2017, p. 193].

It is feasible to create a cross-referenced spreadsheet database to correlate digital codes to known addresses (e.g., the first column for alphanumeric codes and the following columns for personal names, social security numbers, and other known personal information and, thus, be able to identify felons). However, nothing prevents an individual from having more than one wallet. More so, there would always be the possibility for a user to stop using a previous code and start using a new one, or even only use each code once. Hence, this database would only represent previous, potentially outdated information. Consequently, there is an apparent complication for identifying users, which, in turn, potentially affects law enforcement capabilities.

The matter grows in complexity when considering a different genus of crypto-assets called "privacy coins" such as Monero or ZCash. These assets share most of the structural characteristics of Bitcoin except for some specific technical characteristics that allow them to be theoretically anonymous (and not just

[22] Example of a Bitcoin public key: "12hQANsSHXxyPPgkhoBMSyHpXmzgVbdDGd"

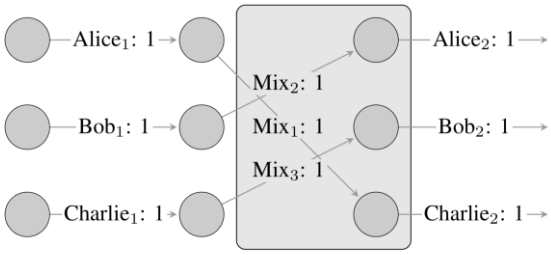
[23] "Pseudonyms are identifiers of subjects, in our setting of sender and recipient. (If we would like to, we could easily generalize pseudonyms to be identifiers of sets of subjects, but we do not need this in our setting.) The subject that may be identified by the pseudonym is the holder of the pseudonym. Pseudonymity is the use of pseudonyms as IDs. So sender pseudonymity is defined by the sender's use of a pseudonym, recipient pseudonymity is defined by the recipient's use of a pseudonym. A digital pseudonym is a bit string which is – unique as ID and – suitable to be used to authenticate the holder and his/her IOIs, e.g. messages.". [PFITZMANN; KÖHNTOPP, 2000, p. 4-5].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

pseudonymous) [CHRISTENSEN, 2018]. The Monero blockchain, for instance, incorporates a one-time random address design, i.e., a system which "[…] allows a sender (the signer) to anonymously sign the transaction (the message) on behalf of a 'ring' or group of other users" [KUMAR et al., 2017, p. 154-155]. Through this technique, the real output remains hidden among a group of outputs of the same amount belonging to other users. Hence, Monero transactions are theoretically unlinkable (it should be impossible to deduce that two transactions were sent from the same recipient) and untraceable (the output being redeemed in a transaction input should be anonymous among a set of other outputs) [KUMAR et al., 2017].

A similar intricacy is the crypto-mixing services (also known as "tumblers"). Given the block chaining element of the protocols, each crypto-asset has a unique data code which, in most cases, reflects the whole transaction history of that digital token (the chain of data); it is feasible to monitor Bitcoin transactions through this data trail [REYNOLDS; IRWIN, 2017]. Mixers are intermediary companies that offer services for users who are interested in mixing their transaction history (the block chaining of past transactions) with the history of the transactions operated by other users. It is done through a simulation of a large number of transactions by sending the assets from one public key to another repeatedly (shuffling), and, in the end, sending the final anonymized key to the intended party [MÖSER; BÖHME; BREUKER, 2013].[24]

**Figure 2 –** Block Diagram of a Hypothetical Crypto Mixing Service




[24] In a simplified example, consider that users "Alice 1", "Bob 1" and "Charlie 1" want to hide a future transaction in which each of them will send precisely one Bitcoin to, respectively, "Alice 2", "Bob 2" and "Charlie 2". The mixing service would shuffle transactions so that the operation which should be from "Alice 1" to "Alice 2" is sent to "Charlie 2" and, in turn, the transaction to "Charlie 2" is done by "Alice 1", "Charlie 1" sends the crypto-asset to "Bob 2" and so on. For an in-depth analysis, cf. Möser, Böhme and Breuker [2013].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

**Source:** MÖSER; BÖHME; BREUKER, 2013.

By keeping the order of the mixing hidden, and depending on the number of shuffles, it becomes continuously harder to track back the original intent of the transactions. It is easy to infer that the general purpose of these mixing services is to make the tracking of operations difficult in a manner not unlike that of privacy coins, be it to safeguard intimacy or to hinder criminal investigations. Mixing can be done on any genus of crypto-assets, even pseudonymous ones such as Bitcoin [MÖSER, BÖHME, BREUKER, 2013].

Each on a different level, pseudonymity, privacy coins and crypto-mixing carry roughly the same risks centered around enhanced identity flexibility,[25] allowing criminals to use simultaneously several fake online identities, replacing or disposing them at will. The latter two, however, have dissociative anonymity on top of flexible identities. This presents a different setting altogether and an even more complex challenge when this factor is used together with the specific routers necessary for accessing the darknet (i.e., the Onion Router or the Tor service) (which obscures user's IP address protecting them from traffic analysis) and the use of "Pretty Good

[25] "Identity flexibility is the first factor that brings criminal dealers online. First, all criminal dealers use fake identities online. Their fake IDs revealed some of their business to some extent. […] Identity flexibility provides cybercriminals many conveniences when communicating online. Although they contact each other often, all they know about each other is just a fake name. They have no idea about each other's gender, accent, or physical appearance. They are safely hidden behind the various IDs.". [KETHINENI; CAO; DODGE, 2018].

Privacy" – PGP asymmetric encryption software for communication between users [KETHINENI; CAO; DODGE, 2018].[26-27]

Flexible identity in crypto-pseudonymity is an issue which, at its core, is not entirely unfamiliar to cybercrime[28] law enforcement practice. Even if crypto-unrelated, crimes committed through the internet often carry the complexity of assumed anonymity. However, using both offline and online techniques, law enforcement have tools which help pinpoint and identify cybercriminals; be it through social engineering, Internet Protocol – IP address and Internet Service Providers – ISP triangulation, data

[26] "PGP stands for "pretty good privacy." The software uses various encryption algorithms to encrypt messages that are regularly updated to address cryptographic vulnerabilities. Conventional encryption, also known as symmetric encryption, utilizes a single secret key to both encrypt and decrypt electronic messages. This is problematic as users must somehow share the secret key so the message can be decrypted. Unless this information is passed in person, the key can be compromised, and the messages could be intercepted and read. PGP utilizes asymmetric, or public-key, cryptography. In asymmetric cryptography, a public key is used to encrypt the message, and a separate private key is used to decrypt it. This method is preferred as the private key is determined by the user receiving the message, so there is no need for additional information to be passed between users. This reduces the number of individuals capable of decrypting the messages and increases the security overall." [KETHINENI; CAO; DODGE, 2018].

[27] "Anonymity is perhaps the most important facilitative factor that brings traditional dealers to the Darknet. There are many techniques available to cybercriminals designed to protect their anonymity. […] Tor, Bitcoin, Silk Road Tumbler, and PGP are four key technologies that protect the anonymity of cybercriminals. With the availabilities of those techniques, it is tough for law enforcement to track cybercriminals online and reveal their identities." [KETHINENI; CAO; DODGE, 2018].

[28] For the purposes herein: "[…] cybercrime is understood as all criminal activity in which [Information and Communication Technology] ICT is used as a tool to commit a crime and/or in which ICT is a target of a crime. Such a broad understanding of cybercrime is also in line with international legal instruments in this field, and especially with the landmark Council of Europe Convention on Cybercrime […]". [BRODOWSKI, 2016, p. 334-335].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

mining[29] from multiple sources and even "external means" (contacting a partner which is less concerned with his or her privacy, v.g.).[30]

It was through these conventional techniques that the US' Federal Bureau of Investigation – FBI arrested Ross William Ulbricht (one of the individuals behind Silk Road). Inattentively, Ulbricht used his personal e-mail address in an online forum and, even though he noticed his mistake and deleted the message later, the FBI was able to trace his computer to the San Francisco area. Through the data extracted from Ulbricht's computer after his detention, law enforcement got the information needed and arrested other individuals allegedly involved in illicit trade and money laundering through Silk Road. Hence, it was through conventional techniques that the investigations and the subsequent arrests were made possible.[31]

[29] For the purposes herein: "Data mining is defined as the identification of interesting structure in data, where structure designates patterns, statistical or predictive models of the data, and relationships among parts of the data […]. Data mining in the context of crime and intelligence analysis for national security is still a young field. The following describes our applications of different techniques in crime data mining. Entity extraction has been used to automatically identify person, address, vehicle, narcotic drug, and personal properties from police narrative reports […]. Clustering techniques such as "concept space" have been used to automatically associate different objects (such as persons, organizations, vehicles) in crime records […]. Deviation detection has been applied in fraud detection, network intrusion detection, and other crime analyses that involve tracing abnormal activities. Classification has been used to detect email spamming and find authors who send out unsolicited emails […]. String comparator has been used to detect deceptive information in criminal records […]. Social network analysis has been used to analyze criminals' roles and associations among entities in a criminal network." [CHEN et al., 2003]

[30] "[…] [another] challenge is the assumed anonymity of the internet: the basic identification of each end point (an IP address) is, for most common customers, dynamically assigned and may easily be used by several if not thousands of users at the same time; not all Internet Service Providers (ISP) require a valid identification of their customers. From a purely technical perspective, therefore, the partners in an internet-based communication at first only know their (inconstant) IP address, but not their real identity. With the help of the ISPs that allocate the IP addresses it is (in many cases) possible to narrow down the possible participants in a communication. Users often identify themselves—sometimes also through reliable external means—and may thereby be identified by their communication partners. Finally, by using data mining techniques and by matching data from multiple sources, large internet sites may be able to profile persons and their behaviour—and thereby pinpoint an individual, even though they might not know the real name. Therefore, the anonymity of the internet is in many cases only assumed, but not asserted. Computers and ICT networks of today provide for an unbelievably quick speed of transactions; if data storage is overwritten just once, the previous data is lost—this volatility is seen as a third challenge, since incriminatory evidence may easily be lost. On the other hand, digital forensics excel in preserving and analysing data currently stored on computer systems. The vast amount of data stored permanently in com- puter systems - who deletes his or her e-mails any longer? - constitutes a 'data trail' and provides an incredible source for investigating people's lives and behaviour, and thereby also for investigating any criminal behaviour.". [BRODOWSKI, 2016, p. 336].

[31] "The Silk Road was shut down by the FBI in 2013. Ross Ulbricht carelessly used his personal email address in an online forum […]. Although he realized the mistake and removed the email address later,


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

It is not to say that these techniques are self-sufficient. A research on the recent trends of cybercriminals and terrorist reports that more than half of the contents of the darknet is illegal [WEIMANN, 2016], ranging from the selling of narcotics to counterfeit currency and weapons; Bitcoin is the most common currency for the purchasing of these services. [32] - [33] The maintenance of these highly active marketplaces is indicative that law enforcement is not entirely effective in combating and preventing cybercrime through the darknet [KETHINENI; CAO; DODGE, 2018].

Moreover, concerning privacy coins and crypto-mixing, their functionality and the degree of dissociative anonymity secured by these techniques offer an unheard risk and a considerably different challenge if tackled directly. However, it is admissible to hypothesize that indirect techniques – specifically the use of external means and social engineering – could be used similarly to traditional cybercrime law enforcement. It is warranted that, even if Ulbricht were using mixing services or privacy coins, his carelessness with personal data could still lead to his arrest.

## 4 PROPOSED PRINCIPLES FOR ADEQUATE CRYPTO-AML ACTION

the FBI was able to trace him, and he was finally caught in San Francisco […]. After the arrest of Ulbricht, eight Silk Road users were arrested all over the world, including in the UK, Sweden, and the United States. Other bitcoin exchange service providers were also arrested for exchanging BTCs for traditional currencies to the Silk Road users. After the Silk Road was shut down by the FBI, the Silk Road 2, the Evolution, and other online dark markets have emerged […]. The Silk Road 2 was shut down in November 2014. […] The key evidence that helped FBI linked Ross Ulbricht to DPR was an email address. When Ulbricht was seeking an IT assistant online, he left his personal email address "Rossulbricht at gmail dot com" by mistake. If were not for Ross Ulbricht's mistake, it would have been tough for police to trace and destroy Silk Road. In addition to Ulbricht, other cyber offenders were found through traditional means as well. Sadler, the drug vendor, was caught in a controlled delivery. Force's evidence was found in Ulbricht's laptop after Ulbricht was arrested. In general, the police relied on traditional techniques to investigate high-technology cybercrimes.". [KETHINENI; CAO; DODGE, 2018].

[32] "The financial category comprised primarily three prominent sub-categories: Bitcoin-based methods for money laundering, trade in illegally obtained credit cards and stolen accounts, and trade in counterfeit currency. As is often the case with unidentified vendors, the quality of the services offered was very difficult to ascertain. The sellers tried to sound professional, as in this fairly common boast about the quality of counterfeit notes […] Bitcoin is the most common currency employed in all Tor hidden-services trade, often via reliance on third-party escrow services to alleviate concerns stemming from anonymous, unverifiable transactions between two unscrupulous parties. As Bitcoin transactions can be monitored even if not easily de-anonymised, however, services to blur the trail of Bitcoins have proliferated as well, for a nominal transaction fee." [MOORE; RID, 2016, p. 22].

[33] "Using the TMM, we observed a dominance of commerce within Tor, largely around narcotics and illegal financial services. Victim based crimes such as child exploitation and illicit/illegal pornography, whilst less frequent, occur frequently enough to remain statistically material within the network, and presented motivations we hadn't anticipated.". [DALINS; WILSON; CARMAN, 2018].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

## 4.1 INTERNATIONAL COOPERATION

From the 80s onwards, there is a sensible move for the adoption of common international standards for AML law enforcement action. It starts with the United Nations' international treaties to fight money laundering in drug trafficking and organized crime, the establishing of the Financial Action Task Force – FATF, the Egmont Group for the cooperation of Financial Intelligence Units – FIUs, and the AML regional Directives in the European Union [STESSENS, 2003, p. 184]. One of the reasons for this progressive integration is the perception that, in a globalized world, money laundering is executed internationally;[34] criminals deliberately use State bureaucracy against law enforcement itself by including cross-border operations as part of their "layering"[35] process. [BOOTH et al., 2011, p. 5].[36-37]

[34] "Money laundering, like drug trafficking and fraud is International in character and uses cross-border movements of currency as part of the layering process. Money launderers may also indulge in their own version of "forum shopping" – carrying out financial and property transactions where they perceive anti-money laundering measures to be weak and the chances of detection lowest. Money laundering, therefore, needs an international response." [BOOTH et al., 2011, p. 5].

[35] As previously mentioned, money laundering is a criminal activity that involves a process focused on the concealment of assets to avoid the discovery of the illicit practice that caused those assets to arise in the first place. In order to achieve this, as a general rule, money laundering goes through three autonomous phases. (i) Placement: the agent performs the allocation of the assets in the economic system; in order to conceal their origin, the criminal seeks to move money in jurisdictions with more permissive rules and with a less regulated financial system. (ii) Layering: when the agent makes the tracking of the illicit resources more challenging by creating an intricate sequence of transactions (layers of transactions). (iii) Integration: when the assets are formally incorporated into the economic system through investments in lawful ventures, making them appear to be of legal origin. [HARRISON; RYDER, 2013, p. 9].

[36] "The effects of the new economy, most importantly the explosion of free trade and electronic commerce, increasingly connect the people in the Western Hemisphere to each other. Globalization has facilitated the growth of global capitalism, the information revolution, travel, and the blurring of national and subnational boundaries. Globalization has rendered meaningless the boundaries between domestic and foreign matters. Similarly, the distinctions of such boundaries among criminals, crime, an criminal justice are also increasingly broken or meaningless." [ZAGARIS, 2006].

[37] "The best illustration of the new sovereignty can be found in the operation of "government networks" - networks of national government officials of all kinds operating across borders to regulate individuals and corporations operating in a global economy, combat global crime, and address common problems on a global scale. As I have argued over the past decade, the state is not losing power so much as changing the way that it exercises its power. As corporations, nongovernmental organizations ("NGOs"), and criminals have all begun to operate increasingly through global networks rather than nation-based hierarchies, so too have government officials. The result is an ever denser web of government networks, allowing government officials to compensate for their decreasing territorial power by increasing their global reach." [SLAUGHTER, 2004, p. 288].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

Transnationality is felt even more intensely in cyber criminality. One of the core challenges for fighting against crimes committed through the internet is that the cyberspace allows free and rapid flow of data between endpoints regardless of geographic location (borderless) [BRODOWSKI, 2016, p. 336]. When crypto-assets are introduced in the formula, more than just information is now flowing through the web; any amount of money converted into Bitcoin, or another crypto-asset is, on principle, free to be sent and received around the world as fast as broadband internet allows. An apparent reason for money launderers to adopt the technology.[38] Hence, national regulation, no matter how well-structured it is, lacks the same potential for effectiveness in combating transnational criminality[39] as an international norm or internationally shared standards (binding or not) for cooperation and police assistance.

The principle that a globalized approach to law enforcement is more appropriate than a local one is already generally recognized [FLORES; CAMAPUM, 2019, p. 471] and, despite practical difficulties, it is a paragon established in the scientific literature [MADSEN, 2016, p. 17]. Global crime governance and the alignment of substantive criminal law is seen with even more enthusiasm in initiatives for action against cyber criminality [BRODOWKSI, 2016, p. 357]. This maxim should be equally pursued for law enforcement focused on crypto-money laundering. Hence, the first proposed principle is that crypto-AML legal action is a matter that should be preferably dealt within a transnational perspective through common standards, international norms, and legal cooperation between States. FATF shares this understanding in its guidance for a risk-based approach to crypto-assets ("virtual currencies") AML [FINANCIAL ACTION TASK FORCE , 2015].

[38] "When used anonymously, virtual currencies allow conducting transactions speedily and without having to disclose the identity of the "owner". By nature, given that they are provided through the internet, the cross-border element is the most prevailing one, increasing the risk to interact with high risk areas or high risk customers that cannot be identified. It is nevertheless important to mention that being currently a developing technology requiring IT skills and expertise, virtual currencies are not necessarily easy to use and the number of transactions is still quite low." [EUROPEAN COMMISSION, 2017]

[39] For the purposes herein, "[…] transnational crimes—also called 'crimes of international concern' or treaty crimes—involve more than one national jurisdiction and are subject to municipal, not international jurisdiction. Only limited extraterritoriality obtains in these treaty crimes that all originate in municipal legislation, which have been formulated 'in normative terms for the purpose of binding states'". [MADSEN, 2016, p. 17].

## 4.2 NON-EXCLUSIVE GATEKEEPER AML APPROACH

Applying the first principle, one of the first attempts at an international peremptory norm focused on crypto-money laundering is the European Anti-Money Laundering Directive 5 – AMLD5.[40] The Fifth Directive retains the fundamental AML axis of the previous norms, focusing on a risk-based approach through cooperation and supervision tactics with certain obliged entities (gatekeepers) [HAFFKE; FROMBERGE; ZIMMERMANN, 2019, p. 7]. Obliged entities are legally compelled to implement specific practices such as general due diligence, "know your customer" – KYC, and activity monitoring. These agents are also obliged to report suspicious practices to FIUs, which, in turn, maintain a unified register of beneficial owners [HOUBEN; SNYERS, 2018, p. 57-58].

AMLD-5 works with this framework, expanding the legal reach into crypto-assets by recognizing the overall risk of money laundering due to the lack of adequately focused regulation for these digital goods and their intrinsic technical characteristics.[41] Maintaining the conventional perspective, however, AMLD-5's focus remains on the regulation of gatekeepers as AML agents, specifically agents who broker legal tender money ("fiat currencies") and cryptocurrencies ("virtual currencies"),[42] i.e., crypto-exchanges. Attention was also given to custodian wallet providers, i.e., companies that provide a service for the safeguarding under their custody of private cryptographic keys.[43] Both of these businesses are now obliged

[40] European Union Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
[41] Cf. AMLD-5 Recital 8.
[42] AMLD-5 Article 1, (2), (d): "[…] 'virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically; […]"
[43] AMLD-5 Article 1, (2), (d): "[…] 'custodian wallet provider' means an entity that provides services to safe guard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.'; […]"


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

entities and, as intermediaries (gatekeepers), are obliged to adopt the necessary measures for private-sector AML cooperation.[44]

The European initiative is commendable. Nevertheless, it does not seem to be sufficient and neither entirely adequate to properly tackle the technical complexities of crypto-money laundering. A first critique is an unjustified restriction the Directive has, regulating only "virtual currencies" (cryptocurrencies) and, thus, opening margin to the usage of other categories of blockchain tokens for criminal activity (such as utility tokens, asset tokens or any other crypto-asset that does not fit the cryptocurrency definition in AMLD-5).[45]

Another flaw is the possible loophole left in the definition of crypto-exchanges given by AMLD-5 as "providers engaged in exchange services between virtual currencies and fiat currencies […]".[46] This definition makes it possible to interpret that only exchanges which operate with legal tender (crypto-to-fiat and fiat-to-crypto) are obliged entities. Thus, exclusively crypto-to-crypto exchanges (i.e., businesses that do not accept any form of fiat currencies) would be excluded from the regulation. It is not clear, however, why these businesses should be exempted from this rule, especially considering how crypto-exclusive exchanges could be purposefully used in the laundering process (specifically in the "layering" phase).

Moreover, AMLD-5 focuses on the intermediaries (be it crypto-exchanges or custodian wallet providers). As previously observed, this strategy is not optimal for crypto-AML, considering the inherently distributed structure and peer-to-peer capabilities. Even if AMLD-5 were entirely upheld, there would still be a significant loophole for private peers to conduct their illegal activities without going through the obliged entities.

[44] Cf. AMLD-5 Article 1, (1), (c).
[45] "All tokens can be used in a similar way for money laundering activities: Irrespective of its function, a token can be transferred, stored and traded electronically (even on the same platforms). This fact allows them to be used for money laundering in the same way. Therefore, it is the authors' view that all kinds of tokens should be treated equally in terms of anti-money laundering and counter-terrorist financing. The alternative would be a substantial regulatory gap—with consequences for the scope of intermediaries covered by AMLD5.". [HAFFKE; FROMBERGE; ZIMMERMANN, 2019, p. 9].
[46] AMLD-5 Article 1, (1), (c).

Thus, a second proposed principle for crypto-AML is that an effective regulatory approach cannot limit itself to creating regulations focused on intermediaries as gatekeepers. The fact that the architecture inherent to blockchain-based systems is devoid of structural chokepoints [AITZHAN; SVETINOVIC, 2018],[47] in hand with the peer-to-peer functionality of crypto-transactions, makes any attempt of focusing entirely on supposed chokepoints insufficient. In this sense, it does not seem that the level of effectiveness of conventional AML private-sector compliance is carried in its entirety to crypto-AML action. Hence, an adequate AML approach should not become exclusively dependent on gatekeepers.

However, the aforementioned cannot lead to the assumption that private-sector cooperation is without function. The conventional AML actions still retain their importance when fighting crypto-criminality (consider Ulbricht's arrest); cooperation and private-sector crypto-AML focused measures should still be valued as a useful tool. In this sense, conventional norms for financial-sector AML compliance could be adapted and enforced in crypto-based businesses, especially crypto-exchanges, considering their function as a redundant, but still relevant pseudo-gatekeeper to the conventional financial system (i.e., crypto-to-fiat converters). Other businesses such as wallet providers, crypto-investment funds, and crypto-miners should also be subject to AML compliance requirements individually suited to their activities.

In any case, AML private-sector compliance regulation should consider not only the scope of the business but the size of the operation and the total volume of money involved. Excessive or too burdensome requirements could force businesses to go into delinquency instead of ensuring ideal effectivity.[48] Moreover, pursuant to FAFT [2014] understanding, the general practice of de-risking, i.e., the "[…] phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage risk […]" is

[47] This conclusion is reachable through a simple observation of an illustrative representation of a distributed network; graphically there is no specific connection that, if severed, denies network transaction. The clearest possible means to prevent transactions, however, would be for one operator to control over fifty one percent of the whole network computational power.
[48] Coherence is considered a general principle for the effectiveness of AML-compliance for the banking sector. [MARTINEZ; LIMA, 2018, p. 60].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

reprehensible.[49] It seems that an adequate measure to help prevent this practice is to bring crypto-entrepreneurship to regulatory light by adopting appropriate AML standards and guidelines that should be met by these companies. Hence, the third proposed principle is that crypto-AML enforcement action should be done through close and adequate private-sector AML cooperation.

## 4.3 USAGE OF TRACKING TECHNOLOGIES AND CRYPTO-BLACKLISTS

Given the block chaining element of the protocols, crypto transactions are, as a rule, traceable through their data trail [REYNOLDS; IRWIN, 2017]. Some companies already use this functionality in close cooperation with national and international law enforcement agencies. Among others, it is the case of Elliptic, an analytics provider that uses a "[…] forensic analysis tool, which combines public blockchain data with a proprietary dataset of Bitcoin addresses associated with known entities, to provide visibility into who is transacting with whom in Bitcoin" [FANUSIE; ROBINSON, 2018]. Through these tools, it is possible to triangulate the origin of a given Bitcoin and, thus, tell whether that particular crypto-asset came from an address associated with suspected criminals. With preliminary evidence, it seems that these tracking (tracing) systems offer a new tool that attempts to counteract part of the characteristics that make crypto-assets attractive to criminals and, thus, should be used by law enforcement [KUZUNO; KARAM, 2017].[50]

[49] "Generally speaking, de-risking refers to the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach. De-risking can be the result of various drivers, such as concerns about profitability, prudential requirements, anxiety after the global financial crisis, and reputational risk. It is a misconception to characterise de-risking exclusively as an anti-money laundering issue. This issue is of crucial importance to the FATF for two main reasons: 1. De-risking can introduce risk and opacity into the global financial system, as the termination of account relationships has the potential to force entities, and persons into less regulated or unregulated channels. Moving funds through regulated, traceable channels facilitates the implementation of anti-money laundering / countering the financing of terrorism (AML/CFT) measures. 2. It is central to our mandate to ensure that the global AML/CFT standard is well understood and accurately implemented, and that countries and their financial institutions are provided with support in designing AML/CFT measures that meet the goal of financial inclusion." [FINANCIAL ACTION TASK FORCE, 2014].

[50] "Bitcoin technology is an innovative rebranding of e-payments but also has taken an important position in the criminal modus operandi, being used for trading or ransom payment. In order to prevent and


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

However, when one considers the different characteristics of privacy coins and the services offered by tumblers, different questions that must be considered. As mentioned, part of the appeal of these technologies is that, theoretically, they make transactions untraceable and unlinkable. On these grounds, the Japanese Financial Service Agency – JFSA's report considers the general restriction of activities with so-called "problematic virtual currencies", i.e., crypto-assets with characteristics that make them uniquely suited for money-laundering" [JAPANESE FINANCIAL SERVICE AGENCY, 2018, p. 9].[51]

The general prohibition of privacy coins and tumblers is a theoretical deterrent to money laundering through these means and, thus, could be a compelling AML tactic in a pragmatic perspective. On the other hand, in most legal systems, privacy is considered a civil right, (internationally, the Covenant on Civil and Political Rights of 1966 also establishes the right against unlawful interference or attacks against individual privacy)[52] this could lead to the argument that the usage of privacy coins or mixers is, in fact, the exercise of a legitimate right. The present research, however, does not intend to offer an answer to the ethical and legal aspects of this question. It is a dilemma with profound repercussions that go far beyond the more instrumental discussions at hand. Whatever the answer may be, proportionality is essential in order to reconcile these antipodal interests and find the right level of intervention.

detect these cases, we need to develop a practical methods, and suitable set of solutions at the local environment for the investigation process and training. We have proposed the Bitcoin analytical process and the practical system that can stand alone and provide effective Bitcoin analyzing result for the investigation field and training. In our evaluation, we could analyze the specific known addresses relate to suspicious activities in marketplace, ransomware and DDoS extortion case. We believe that the proposed analytical process and system can help throughout making investigation report at law enforcement. Additionally, we will be pushing for cooperation with other sites and researchers for better understanding and sharing of techniques, source code and data." [KUZUNO; KARAM, 2017].

[51] "Restricting Problematic Virtual Currencies. Each virtual currency has its own unique design and specification, and there are some virtual currencies that are difficult to trace and therefore likely to be used for money laundering due to non-disclosure of their transfer records, and others are vulnerable when maintaining and updating their transfer records. Therefore, it would be necessary for [virtual currency exchange service providers] SPs to take measures to prevent themselves from dealing in problematic virtual currencies in light of user protection, and proper and reliable business operation. On the other hand, the security of virtual currency may vary depending on the discussion of those who are involved in forming or changing technical specifications and the conditions of mining. Technological innovation may also lead to new problems that have not previously been anticipated. These changes may also occur rapidly." [JAPANESE FINANCIAL SERVICE AGENCY, 2018, p. 9].

[52] Cf. Covenant Article 17.

In any case, there is some evidence that suggests that privacy coins and tumblers are not entirely efficient. A study conducted by the National University of Singapore found it possible to trace the origin of Monero transactions through attack routines and temporal analysis [KUMAR et al., 2017].[53] Research by the University of Münster was able to reverse-engineer mixing services to a level that made it possible to link output and input transactions [MÖSER; BÖHME; BREUKER, 2013].[54] Hence, it seems feasible for law enforcement to work around tumblers and privacy coins, deanonymizing transactions. Further technical research in this area is relevant for the full understanding of the limits of the technology at hand, however. More so, it is crucial to observe that, at the same rate in which law enforcement works to develop technologies to deanonymize transactions, the companies behind mixers and privacy coins are in full effort to develop newer and more effective techniques to keep their operations untraceable and unlinkable. The Singaporean study, for instance, was shared with the team behind Monero and "fixes" are already undergoing implementation [KUMAR et al., 2017].[55]

[53] "This work performs a passive blockchain analysis of Monero and evaluates the efficacy of several attacks on its untraceability guarantees. These attacks are effective as around 88% of inputs are rendered traceable. We also found some traceability results on RingCTs and finally discuss a better strategy (than the one currently employed) to mitigate temporal analysis. Our results hereby reaffirm the weaknesses of anonymity-set size as a privacy metric when implemented in practice. As a future work, we aim to study traceability under active attacks on Monero, where the adversary can take part in the protocol to undermine users' privacy. We are further investigating the use of cryptographic primitives such as zero knowledge proofs and ORAM to strengthen the traceability guarantees beyond the current solutions." [KUMAR et al., 2017].

[54] "Several services offering increased transaction anonymization have emerged in the Bitcoin ecosystem – such as Bitcoin Fog, BitLaundry, and the Send Shared functionality of Blockchain.info. Some of these services routinely handle the equivalent of 6-digit dollar amounts. In a series of experiments, we use reverse-engineering methods to understand the mode of operation and try to trace anonymized transactions back to our probe accounts. While Bitcoin Fog and Blockchain.info successfully anonymize our test transactions, we can link the input and output transactions of BitLaundry." [MÖSER; BÖHME; BREUKER, 2013].

[55] "As a part of responsible disclosure, we shared our findings both with the Monero development team and the general community. We received varied feedback through diverse channels including but not limited to e-mail, Twitter and Reddit. Monero development team found our result on Attack II insightful: 'We hadn't had it [Attack II] accompanied by a model before, i.e., we've been approaching the problem more generally. It's NOT trivially solvable. Because most users will receive additional outputs and need to combine them; the combination betrays a small amount of correlation data.' […] Our results on Attack III has also catalyzed the ongoing work on developing better mitigation strategies. Several mitigation measures have been discussed: (1) Sampling mix-ins using our proposed approach of taking into account actual spending behavior, (2) Sampling mix-ins using Zipf distribution, (3) Developing a dynamic


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

In this sense, a fourth proposed principle is the investment of research and development on tracking and reverse-engineering techniques for the tracing of the transaction history of suspected criminal activity with crypto-assets. With further evidence confirming that these mechanics are efficient, law enforcement agencies should adopt them and use them in conjunction with the global user database. Together with the first and third principle, this approach should be executed internationally through cooperation between the States and the private sector.

Withal, another tactic is the usage of "blacklists" for crypto-assets in a similar manner to the already suggested database for addresses. Instead of blacklisting addresses or account holders, however, this database would register transaction histories, i.e., an individual crypto-asset. Every crypto-asset has a specific identity, which means that they are not entirely interchangeable. Adapting the analogy presented by Möser, Böhmer, and Breuker [2017], the address database is similar to a standard criminal register with names and social identity numbers as the primary reference; the crypto-blacklist would be similar to a register of serial numbers of bank notes used to pay ransoms to criminals.[56] The Mt. Gox crypto-exchange has already used the technique in 2012, where it blocked accounts that held particular Bitcoins that could be traced back to suspected criminal activity, only freeing the use of that account if the user would upload further identification [BUTERIN, 2012].

In this sense, it would be possible for the law to mandate that any entity that operates with crypto-assets observe these official blacklists, eliminating or reducing the usability of those specific assets. This could even affect tumblers, considering that, either they would be forced to reject tainted crypto-assets (and, thus, follow the legislation) or accept these tainted crypto-assets and loose part of their commercial appeal (given that their users could be sending non-blacklisted crypto-assets to be

sampling procedure, (4) Wallet-specific sampling procedure, etc. The ensuing limitations have also been discussed at length. For instance, a dynamic sampling procedure being costly; wallet-specific sampling leading to potential fingerprinting, etc." [KUMAR et al., 2017].

[56] "[…] KYC is only a first step that enables downstream activities such as blacklisting suspicious account holders. As Bitcoin accounts have weak identities at best, but all transaction records are public, for AML to be effective, it should blacklist transaction histories (i.e., bitcoins) rather than accounts or account holders. A good offline analogy is registering serial numbers of bank notes used to pay ransoms. There is some precedence in Bitcoin." [MÖSER; BÖHME; BREUKER, 2013].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

anonymized and receive tainted, i.e., less useful, crypto-assets in return; a bad deal). If this crypto-blacklist were to be globally enforced, a possible consequence would be that crypto-assets with tainted prefixes could even reduce in value; while crypto-exchanges that enforce effective AML compliance, filtering tainted crypto-assets, could even have their crypto-assets sold for a higher price (considering that would be offering a crypto-asset with an almost nil probability of being tainted, and, with lesser supply and higher demand, its prices could spike).[57]

Hence, a fifth proposed principle is the adoption of this global blacklist for tainted crypto-assets that should be ostracized from businesses. If adopted and enforced on an international basis, this blacklist may be able to reduce and help suffocate the usage of crypto-assets for money laundering purposes by preventing financial integration, i.e., stopping the assets of being formally incorporated into the economic system through investments in apparently lawful ventures.

## CONCLUSION

Through the understanding of crypto-assets and Blockchain, it gets continuously clearer that the regulation of this technology is a complicated matter and

[57] "Our observation calls into question the last function standing. Bitcoins are not alike. Every transaction has a different history. The fact that transaction anonymizers exchange the history for a fee implies that bitcoins with different histories have different value. Coinbase transactions, for example, should be valued highest because they are scarcest. They are an important resource required as input to make transactions provably untraceable. This effect is aggravated under the above-described policy of blacklisting transactions for AML, where "virgin" coinbase transactions have the lowest risk of being blacklisted at the time of conversion or spending. By contrast, bitcoins with known blacklisted transaction prefixes should have very little value, as they can only be used in the underground. One can complete this example by speculating that collectors might ascribe higher value to bitcoins with a famous transaction history. […] We believe that it is just a matter of time until price spreads between bitcoins of different provenance appear in the marketplace. The bottom line is that the uniqueness of every bitcoin thwarts the very idea of money as a homogeneous commodity to serve as unit of account. Inventors of future cryptographic currencies should take note." [MÖSER; BÖHME; BREUKER, 2013].


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

a challenge that must be faced wisely. Despite some isolated attempts [LAW LIBRARY OF CONGRESS, 2014], any State policy that limits itself to outlaw the technology is doomed to seeing its legislation fall short in effectivity [PINTO; RAMOS, 2018, p. 542]. Given the pervasiveness of the online world, banning crypto-assets – similarly to many other technologies and even physical goods – is trying to cover the sun with one finger [TEIXEIRA; SILVA, 2017, p. 117]. Any effective solution has to find a middle ground between free usage and necessary legal intervention.

Therefore, this research offered some perspective on how policymakers and law enforcement agents could organize their action program for crypto-AML. The general framework of proposed principles can be summarized in the following manner: (i) globalized, transnational AML action through common standards, international norms, and legal cooperation between States; (ii) going beyond traditional intermediary-gatekeeper AML compliance approaches, considering the lack of proper structural chokepoints in blockchain protocols; (iii) close private-sector cooperation and clear AML compliance standards for crypto-based businesses, bringing entrepreneurs into regulatory light; (iv) investment on research and development of tracking and reverse-engineering anonymization techniques for the tracing of the transaction history of criminal activity conducted through crypto-assets (privacy coins and tumblers included); (v) adoption of a global blacklist for crypto-assets prefixes that are believed to be connected to criminal activity.

These principles, in conjunction with conventional techniques, could lead to an AML law enforcement approach that, considering the specific complexities of crypto-assets, use them in its favor or, at least, find a backdoor for fighting criminality through this technology. Contemporary approaches to money laundering regulation have to consider not only the specific substantial economics of this kind of criminality [MASCIANDARO, 1999] but the material means by which the crime is committed. Money laundering through art is not the same as money laundering through blood diamonds, which is not the same as money laundering through Bitcoin.

In this sense, the regulator has a grave responsibility for measuring the line of proportionality for AML legislation. Crypto-assets and blockchain are no longer a niche phenomenon; mainstream companies such as Facebook's Libra are increasingly

interested in offering their own cryptocurrencies for the public [KOFFMAN, 2019]. In such a way, an irresponsible regulator that decides to create a far too demanding AML regulation for crypto-based business may as well be marginalizing the smaller startups innovators and lobbying in favor of big businesses that will be able to hire a battalion of lawyers to make sure that they are compliant with the law. This research believes that the framework of principles here presented is designed in a way that will not present too great a hindrance into innovation while offering a practical AML approach. It is necessary to observe, however, that these principles are, in essence, theoretical, i.e., have not been put to the test. It would be scientifically beneficial to see this framework, or evolution or adaptation of such a framework, put to the test through a regulatory sandbox approach.

## REFERENCES

AITZHAN, Nurzhan Zhumabekuly; SVETINOVIC, Davor. **Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams**. IEEE Transactions on Dependable and Secure Computing, vol. 15, issue 5, September-October, 2018.

AKGIRAY, Vedat. Blockchain Technology and Corporate Governance: Technology, Markets, Regulation and Corporate Governance. **OECD – Organization for Economic Co-operation and Development** – Directorate for Financial and Enterprise Affairs Corporate Governance Committee. 2018.

ANTONOPOULOS, Andreas M. **Mastering Bitcoin**. Sebastopol: O'Reilly, 2010.

_____. **The Internet of Money**. Maryland: Merkle Bloom LLC, 2016.

BANK POLICY INSTITUTE. **Getting to Effectiveness** – Report on US Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance. Washington DC: BPI, 2018.

BARAN, Paul. **On Distributed Communications Networks**. Rand Memorandum. Santa Monica, 1963.

BOOTH, Robin; FARRELL QC, Simon; BASTABLE, Guy; et al. **Money Laundering Law and Regulation**. Oxford: Oxford University Press, 2011.


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

BRITO, Jerry; CASTILLO, Andrea. **Bitcoin:** A Primer for Policymakers. Arlington: George Mason University, 2013.

BRODOWSKI, Dominik. Transnational Organised Crime and Cybercrime. In: HAUCK, Pierre; PETERKE, Sven (Ed.). **International Law and Transnational Organized Crime**. Oxford: Oxford University Press, 2016.

BUTERIN, Vitalik. MtGox: What the Largest Exchange is doing about the Linode Theft and the Implications. **Bitcoin Magazine**, 2012.

CHEN, Hsinchun; CHUNG, Wingyan; QIN, Yin; et al. **Crime Data Mining:** An Overview and Case Studies. Proceedings of the 2003 annual national conference on Digital Government Research. Digital Government Society of North America, 2003. Available at: <https://bit.ly/2W3qy9i>. Accessed on the 24th of June 2019.

CHRISTENSEN, Sofie. **A Comparative Study of Privacy-Preserving Cryptocurrencies: Monero and ZCash**. School of Computer Science, University of Birmingham, September 2018.

DALINS, Janis. WILSON, Campbell; CARMAN, Mark. **Criminal Motivation on the Dark Web:** A Categorisation Model for Law Enforcement. Digital Investigation, vol. 24, March, 2018.

DRESCHER, Daniel. **Blockchain Basics**. Frankfurt: Apress, 2017.

EUROPEAN COMMISSION. **Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities**. European Commission Staff Working Document, Brussels, 2017. Available at: <https://bit.ly/2WZZR1d>. Accessed on the 12th of June 2019.

FANUSIE, Yaya J.; ROBINSON, Tom. **Bitcoin Laundering:** An Analysis of Illicit Flows into Digital Currency Services. Elliptic, Center on Sanctions & Illicit Finance Foundation for Defense of Democracies, 2018.

FEDERAL BUREAU OF INVESTIGATION. **Bitcoin Virtual Currency:** Unique Features Present Distinct Challenges for Deterring Illicit Activity. Intelligence Assessment (Unclassified). Directorate of Intelligence of the Federal Bureau of Investigation, Washington DC, 2012.

FINANCIAL ACTION TASK FORCE. **FATF clarifies risk-based approach:** case-by-case, not wholesale de-risking. FATF, 2014. Available at: < http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html>. Accessed on the 12th of June 2019.


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

_____. **Guidance for a Risk-Based Approach to Virtual Currencies**. FATF/OECD. 2015. Available at: <http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html>. Accessed on the 12th of June 2019.

FLORES, Andréa; CAMAPUM, Rodrigo Alencar Machado. **O Combate ao Crime de Lavagem de Dinheiro no Direito Interno e Internacional**. Revista Jurídica, vol. 2, n. 55, Curitiba, 2019.

GRUBER, Sarah. **Trust Identity and Disclosure:** Are Bitcoin Exchanges the Next Vritual Havens for Money Laundering and Evasion?. Quinnipiac Law Review, vol. 32, issue 1, 2013.

HAFFKE, Lars; FROMBERGER, Mathias**;** ZIMMERMANN, Patrick. Cryptocurrencies and Anti-Money Laundering: The Shortcomings of the Fifth AML Directive (EU) and How to Address Them. **Journal of Banking Regulation**. Springer Nature Limited. 2019.

HARRISON, Karen; RYDER, Nicholas. **The Law Relating to Financial Crime in the United Kingdom**. Farnham: Ashgate, 2013.

HODOROV, S. Ye. Financial Crisis of 2008 – 2010 as a Phase of the Global Economic Cycle. **Bulletin of Saratov State Socio-Economic University**, n. 3, 37, 2011.

HOUBEN, Robby; SNYERS, Alexander. **Cryptocurrencies and Blockchain**: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion. European Parliament, European Union, 2018.

HUANG, Jimmy Yicheng. Effectiveness of US Anti-Money Laundering Regulations and HSBC Case Study. **Journal of Money Laundering Control**, vol. 18, issue 4, 2015.

JAPANESE FINANCIAL SERVICE AGENCY. **Report from Study Group on Virtual Currency Exchange Services**. Tokyo, September 2018

KETHINENI, Sesha; CAO, Ying; DODGE, Cassandra. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. **American Journal of Criminal Justice**, vol. 43, issue 2, June, 2018.

KOFFMAN, Tatiana. **Facebook's Libra White Paper is Now Live**. Forbes, June 18th, 2019. Available at: < https://www.forbes.com/sites/tatianakoffman/2019/06/18/facebooks-libra-white-paper-is-now-live/#6bc7d5f36e00>. Accessed on 20th of June 2019.

KUMAR, Amrit; FISCHER, Clément; TOPLE, Shruti; et al. **A Traceability Analysis of Monero's Blockchain.** Springer International Publishing: Lecture Notes in Computer Science Computer Security, 2017.


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

KUZUNO, Hiroki; KARAM, Christian. **Blockchain Explorer:** An Analytical Process and Investigation Environment for Bitcoin. 2017 APWG Symposium on Electronic Crime Research (eCrime), June, 2017.

LAMPORT, Leslie; SHOSTAK, Robert; PEASE, Marshall. **The Byzantine Generals Problem**. SRI International, ACM Transactions on Programming Languages and Systems, Vol. 4, N. 3, 1982.

LAW LIBRARY OF CONGRESS. **Regulation of Bitcoin in Selected Jurisdictions**. Washington D.C., 2014.

LEÃO, Luana da Costa; VIEGAS, Alessandra Depieri; SETTI, Bruna Migliaccio. *O Bitcoin à Luz do Comércio Internacional: Impacto das Moedas Virtuais na Economia Mundial. In: MENEZES, Wagner (Org.).* ***Direito Internacional em Expansão:*** *Volume XI. Belo Horizonte:* Arraes *Editores*, 2017.

LEWENBERG, Yoad; BACHRACH, Yoram; SOMPOLINSKY, Yonatan; et al. **Bitcoin Mining Pools:** A Cooperative Game Theoretic Analysis. Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems, 2015.

LINDSEY, David E. **A Century of Monetary Policy at the Fed:** Ben Bernanke, Janet Yellen, and the Financial Crisis of 2008. New York: Palgrave Macmillian, 2016.

MADSEN, Frank G. The Historical Evolution of the International Cooperation Against Transnational Organized Crime. In: HAUCK, Pierre; PETERKE, Sven (Ed.). **International Law and Transnational Organized Crime**. Oxford: Oxford University Press, 2016.

MARTINEZ, André Almeida Rodrigues; LIMA, Carlos Fernando dos Santos. **Compliance *Bancário***. Quartier Latin: São Paulo, 2018.

MASCIANDARO, Donato. **Money Laundering:** The Economics of Regulation. European Journal of Law and Economics, vol. 7, 1999.

MOORE, Daniel; RID, Thomas. **Cryptopolitik and the Darknet.** Survival: Global Politics and Strategy, vol. 58, 2016.

MÖSER, Malte; BÖHME, Rainer; BREUKER, Dominic. **An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem**. Conference eCRIME Researches Summit (eCRS) San Francisco, 2013.
MULLER, Wouter H.; KÄLLIN, Christian H.; GOLDSWORTH, John G. **Anti-Money Laundering:** International Law and Practice. Hoboken: John Wiley & Sons Inc, 2007.

NAKAMOTO, Satoshi. **Bitcoin:** A Peer-to-Peer Electronic Cash System. 2008. Available at: <https://bitcoin.org/bitcoin.pdf>. Accessed on the 12th of June 2019.


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

_____. **Bitcoin Open Source Implementation of P2P Currency**. 2009. Satoshi Nakamoto Institute. Available at: <https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/>. Accessed on the 12th of June 2019.

PFITZMANN, Andreas; KÖHNTOPP, Marit. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In: FEDERRATH, Hannes (Ed.). **Designing Privacy Enhancing Technologies:** Design Issues in Anonymity and Unobservability. Berlin: Springer, 2000.

PINTO, Felipe Chiarello de Souza; RAMOS, Tais. *Aspectos Controversos e Vantagens do Bitcoin: Análise da Visão das Instituições Financeiras Brasileiras.* ***Revista Jurídica****,* vol. 4, n. 53, Curitiba, 2018.

POPOV, Serguei. **The Tangle**. Descryptions, v. 1.4.3, 2018. Available at: <http://www.descryptions.com/Iota.pdf>. Accessed on the 12th of June 2019.

RAPP, Nicholas; ROBERTS, Jeff John. **Nearly 4 Million Bitcoins Lost Forever, New Study Says**. Fortune, 2017. Available at: <http://fortune.com/2017/11/25/lost-bitcoins/>. Accessed on the 12th of June 2019.

REYNOLDS, Perri; IRWIN, Angela S. M. **Tracking Digital Footprints:** Anonymity Within the Bitcoin System. Journal of Money Laundering Control, vol. 20, issue 2, 2017.

SILVA, Allan Jones Andreza; SILVA, Luciano Nasciomento; BRAGA, Rômulo Rhemo Palitot. *Delação Premiada e Lavagem de Dinheiro.* ***Revista Direito Público – RDU***, vol. 14, n. 78, nov-dez 2017, Porto Alegre, 2017.

SLAUGHTER, Anne-Marrie. Sovereignty and Power in a Networked World Order. **Stanford Journal of International Law**, v. 40, n. 2, 2004.

SMITH, Angela. **How the World Food Programme uses Blockchain to Better Serve Refugees**. International Telecommunication Union – ITU News, April, 2018. Available at: <https://news.itu.int/how-the-world-food-programme-uses-blockchain-to-better-serve-refugees/>. Accessed on the 12th of June 2019.

STESSENS, Guy. **Money Laundering:** A New International Law Enforcement Model. Cambridge: Cambridge University Press, 2003.

SWAN, Melanie. **Blockchain:** Blueprint for a New Economy. Sebastopol: O'Reilley, 2015.

SWISS CONFEDERATION. **Legal Framework for Distributed Ledger Technology and Blockchain in Switzerland**. Federal Council Report. Bern, 2018.


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]

TEIXEIRA, Rodrigo Valente Giublin; SILVA, Felipe Rangel da. *Bitcoin e a (Im)Possibilidade de sua Proibição: Uma Violação à Soberania do Estado.* ***Revista Brasileira de Políticas Públicas***, vol. 7, n. 3, dez. 2017.

TURNER, Jonathan E. **Money Laundering Prevention:** Deterring, Detecting, and Resolving Financial Fraud. Hoboken: John Wiley & Sons, Inc., 2011.

UNITED STATES OF AMERICA. **Executive Order 13.224 of September 23, 2001**. Federal Register, vol. 66, n. 186, 2001. Available at: <https://www.state.gov/j/ct/rls/other/des/122570.htm>. Accessed on the 12th of June 2019.

VAÏSSE, Maurice. ***As Relações Internacionais desde 1945***. Lisboa: Biblioteca 70. 2017.

WATTENHOFER, Roger. **Distributed Ledger Technology:** The Science of the Blockchain. Washington: Inverted Forest Publishing, 2017.

WEIMANN, Gabriel. **Terrorist Migration to the Dark Web**. Perspectives on Terrorism, vol. 10, n. 3, June, 2016.

XU, Xiwei; WEBER, Ingo; STAPLES, Mark; et al. **A Taxonomy of Blockchain-Based Systems for Architectural Design**. International Conference on Software Architecture, IEEE Computer Society, Sidney, 2017.

ZAGARIS, Bruce. Developments in the Institutional Architecture and Framework of International Criminal and Enforcement Cooperation in the Western Hemisphere. **The University of Miami Inter-American Law Review**, vol. 37, n. 3, Spring-Summer, 2006.


[Received/Recebido: Junho 17, 2018; Accepted/Aceito: Junho 30, 2019]