Cryptocurrencies and anti-money laundering regulation in the G20

INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY

Cryptocurrencies and anti-money laundering regulation in the G20

Authors
Gustavo Rodrigues
Lahis Kurtz

Graphic Project
André Oliveira, Felipe Duarte e Lucca Falbo

Cover
Freepik

Layout
Felipe Duarte

Editorial Production
Instituto de Referência em Internet e Sociedade

Revision
Lucas Costa dos Anjos

Finalization
Felipe Duarte

How to reference this paper

RODRIGUES, Gustavo; KURTZ, Lahis. **Cryptocurrencies and anti-money laundering regulation in the G20**. Institute for Research on Internet and Society: Belo Horizonte, 2019. Available at: http://bit.ly/32Fw4xD Access: DD mmm. YYYY

INSTITUTE
FOR RESEARCH
ON INTERNET
AND SOCIETY

DIRECTRESS

Luíza Couto Chaves Brandão

VICE-DIRECTOR

Odélio Porto Jr.

SCIENTIFIC ADVISORS

Fabrício Bertini Pasquot Polido
Lucas Costa dos Anjos

MEMBERS

Ana Bárbara Gomes / Researcher
Anna Célia Carvalho / Communication
Felipe Duarte / Communication
Gustavo Rodrigues / Researcher
Lahis Kurtz / Researcher
Paloma Rocillo Rolim do Carmo / Researcher
Pedro Vilela Resende Gonçalves / Co-founder and Researcher
Victor Barbieri Rodrigues Vieira / Researcher

SUMMARY

1. INTRODUCTION

Cryptocurrencies (CCs), crypto-assets, virtual currencies, virtual assets, digital currencies: the steep rise in the employment of these assets over the course of the 2010s has given rise to growing global interest in them. Commonly associated with the anonymous and decentralized features of their best-known representative, Bitcoin, these assets have raised mixed dispositions on the part of the stakeholders: on the one hand, curiosity and enthusiasm regarding their potential for innovation; on the other, concern and distrust regarding the risks and implications associated with their use.

While it is admitted that CCs do not currently pose a threat to international financial stability[1], especially as their combined global market value is still relatively low[2], this does not nullify the dilemmas faced by regulators. Some of the topics that national and international stakeholders have been addressing include the use of these assets for illicit purposes, taxation of gains from transactions involving them, protection of investors and consumers who use them, and even the environmental impacts of the industry. Therefore, while the debate over *whether* cryptographic assets should be regulated is not over[3], it is being gradually replaced in several countries by discussions over *how* and *when* regulations should take place.

In the midst of these issues, the risks related to the use of CCs for money laundering and terrorist financing (ML/TF) crimes stand out as one of the main focuses of national and international legal attention. This is partly due to the distributed accounting technology that lies at the heart of CCs, expressly designed to secure transactions that are not subject to state supervision[4]. Financial secrecy provided by cryptographic infrastructure has a facilitating effect on the conduct of the aforementioned practices. In addition, Bitcoin's initial insertion in the public debate was largely crossed by media associations with the financing and perpetration of criminal activities[5], which facilitated its approach to the ML/TF in the regulator's imagination.

In this scenario, both international and national policymakers seek to curb the possibilities of using CCs for ML/TF, either by means of more general prohibitive measures or by regulating the CC ecosystem. In particular, the Financial Action Task Force (FATF), the leading international authority in regulation, monitoring, and promotion of anti-money laundering policies, has been addressing the subject extensively[6]. Its Risk-Based Approach (ABR) encourages less the prohibition and more the regulation of private actors belonging to the CC ecosystem, especially *exchanges* - entities that perform exchange

1 This is the position that the G20 has taken in a statement released in march 2018. G20. **Communiqué:** Finance Ministers & Central Bank Governors 19-20 March 2018, Buenos Aires, Argentina. 2018. Available at: https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf. Accessed in 15 sep. 2018. p. 2.

2 Even as global market value peaked at USD 800 billion in january 2018, such an amount was still less than 1% of the global Gross Domestic Product at that time. CARNEY, Mark. FSB Chair's letter to G20 Finance Ministers and Central Bank Governors. **Financial Stability Board**, 18 mar. 2018. Available at: http://www.fsb.org/wp-content/uploads/P180318.pdf. Acess on 15 sep. 2018. p. 2.

3 UNITED NATIONS. Development Policy and Analysis Division. Department of Economic and Social Affairs. Global Issues: Challenges of cryptocurrencies for policymakers. **Monthly Briefing on the World Economic Situation and Prospects**, nº 108, pp. 1-2, 13 nov. 2017. p. 1.

4 SWARTZ, Lana. What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. **Cultural Studies**, v. 32, n. 4, jan. 2018.

5 PAGLIERY, Jose. **Bitcoin and the future of Money**. Chicago: Triumph Books, 2014. p. 57 e capítulo 9.

6 FINANCIAL ACTION TASK FORCE. **Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**. jun. 2019. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. Acess on 23 jun. 2019.

operations between different CCs and between CCs and legal tender currencies. The goal is to both address contact points between the regulated financial system and the universe of CCs and to inhibit regulatory arbitrage by the private sector.

In order to provide an empirical contribution to these debates, this research sought to map the state of the art of anti-money laundering regulations regarding CC service providers, particularly *exchanges*, in jurisdictions that comprise the Group of 20 (G20).

We have chosen to use the term cryptocurrency as an analytical category, even though there are many terms employed to refer to similar phenomena, such as "crypto-assets", "digital currencies", "virtual currencies", "virtual assets", "digital assets" etc. In fact, the universe of what is conventionally called cryptocurrencies is positively less broad than the universe that encompasses all applications of the blockchain[7] protocols, which lie at the center of these innovations. In addition, many international actors, such as the G20, employ the term crypto-assets, usually to highlight the fact that the representations of value operated on the platforms in question are not currencies neither from an economic[8] standpoint nor from a legal one[9].

This choice stems from a number of reasons. First, as internationalist Malcolm[10]Campbell-Verduyn notes, although the question of whether CCs are a currency has attracted much academic and regulatory interest, it is irrelevant from a global anti-money laundering governance standpoint. What matters is not the theoretical classification of these goods, but rather their use for participating in illicit transactions and financial flows. Second, our analysis emphasizes the contact points between the regulated financial system and the universe of CCs, in particular *exchanges* and their operations of exchanging legal currencies into CCs and vice-versa. We found it adequate to restrict analytical attention to technologies that lend themselves to operations similar to those of legal currencies. Since specific challenges posed by CCs to AML regulations relate directly to their anonymous and decentralized qualities, the scope analyzed is further restricted to designating assets that present such features[11]. Furthermore, the term cryptocurrency is widespread and well known, so its use favors the reach of this research to a wider audience.

Our methodology consisted of four steps. First, a bibliographic review on the topic of AML and cryptocurrency regulation was carried out, in order to identify and present the debate on cryptocurrency and AML, as well as the main challenges and initiatives arising from this relationship. The documents raised in this phase provided the basis

7 Set of protocols that enable the development of transaction networks in which records are distributed amongst network participants, which act as validating nodes. This allows for systems that are independent from centralizing entities, making it feasible to transact and trade directly between parties without intermediation of third parties.

8 In general, contemporary economic theory admits that a currency should perform efficiently three main functions: store of value, unit of account and means of exchange. With regards to CCs, several actors have argued that they do not successfully perform none of the three, meaning that they are not real money. A defense of this stance can be found in CLAEYS, Grégory; DEMERTZIS, Maria; EFSTATHIOU, Konstantinos. Cryptocurrencies and monetary policy. **Monetary Dialogue**, Bruxelas, jul. 2018. p. 12, entre outros.

9 Although there is some variation on the concept, the definition of legal currency usually requires two features: i) the currency has to be issued by the competent judicial monetary authority, usually a Central Bank; ii) legal tender, that is, it should be a legal means to fulfilling economic obligations that is accepted and/or mandatory in the reach of that prescriptive jurisdiction. For an in-depth discussion of the concept, see GOLDBERG, Dror. Legal Tender. **SSRN Electronic Journal**, [sl], p.1-17, 2008. Elsevier BV.

10 CAMPBELL-VERDUYN, Malcolm. Bitcoin, crypto-coins, and global anti-money laundering governance. **Crime, Law and Social Change**, v. 69, n. 2, 283–305, mar. 2018. p. 286.

11 There are applications of the blockchain protocols to the creation of assets issued by Central Banks, such as the Venezuelan Petro.

for the next step, which consisted in the elaboration of methodological instruments for data collection. This is a structured form (Appendix B) consisting of eight questions or checklists concerning AML regulation applicable to private actors in the cryptocurrency industry in the examined jurisdiction. The following aspects were addressed: the existence of prohibitive measures, nature of the applicable regulatory instruments, definitions offered in these instruments (of CCs, exchanges and service providers), existence of AML standards, the content of such standards and sanctions applicable in case of failure to comply with them.

Next, data was collected from the sample, which consisted of the jurisdictions that make up the G20. This selection stems from three factors: the economic importance of the jurisdictions that make up the international forum, their leading role in global economic governance, especially since 2008[12], and their joint engagement with the FATF on the specific topic of CC regulation[13]. For each jurisdiction analyzed, an entry was produced on the form. Finally, the results were organized into three frames of reference, covering the following aspects: cryptocurrency definitions, definitions of *exchange* and service provider, nature of instruments and AML rules and restrictions.

In addition to this introduction, this article is divided into 5 parts. In the first, we present the global AML regime, including a brief background, its main instruments and the general approach of the FATF. The second discusses the specific money laundering risks posed by CCs, as well as the self and external regulatory trends of these technologies for AML purposes over the past decade. Following, coordinated international efforts of external AML regulation of CCs are listed, including a review of the FATF's treatment of the topic. The fourth part details the methodology used for data collection and analysis. Finally, the results and the main findings coming from them are debated.

2. THE GLOBAL ANTI-MONEY LAUNDERING REGIME

This section contextualizes global anti-money laundering governance. Item 2.1. presents a brief history of the framing of the practice as a crime and as a social and economic problem, as well as the normative pillars that make up the global regime. Item 2.2. examines the emergence of the Financial Action Task Force, its approach to the subject and its main products.

2.1. The emergence of the international legal framework to combat money laundering

The development of an international regulatory approach to money laundering crimes is relatively recent, although the practice has been popular among organized criminal groups since at least the 1920s[14]. Its first nationwide protective measures date

12 RAMOS, Leonardo; VADELL, Javier; SAGGIORO, Ana; FERNANDES, Marcia. A Governança econômica global e os desafios do G-20 pós-crise financeira: análise das posições de Estados Unidos, China, Alemanha e Brasil. **Revista Brasileira de Política Internacional**, v. 55, n. 2, p. 10-27, 2012.

13 See G20, op. cit., and FINANCIAL ACTION TASK FORCE. **FATF Report to G20 Finance Ministers and Central Bank Governors Meeting**. abr. 2019. Available at: www.fatf-gafi.org/media/fatf/documents/G20-April-2019.pdf. Acess on 23 may 2019. p. 12-13.

14 It is not a coincidence that the origin of the "laundering" metaphor is allegedly related to the use of laundries for the

back to the Cold War period - as shown by the Bank Secrecy Act (BSA), passed in the US in 1970, and the code of conduct adopted by the Swiss Bankers Association in 1977[15]. The enforcement[16] of these instruments was lax, however, as they were strongly opposed by the banking sector, which framed the reduction of bank secrecy as a violation of its clients' financial privacy. As a consequence, the effectiveness of the standards in question was quite limited during the 1970s[17].

This regulatory environment was significantly transformed during the 1980s, largely due to the success of US state actors in modifying the public perception of the problem. Previously, illicit capital flows were primarily associated with tax evasion. In the context of the 1980s drug war, on the other hand, these flows became the subject of a scientific and media discourse[18] that emphasized the relationship of "dirty money" to organized crime and, above all, to drug trafficking. Resistance to AML measures was framed in public opinion as facilitating trafficking, which generated an incentive for compliance with AML laws. This was exemplified by the case of the Bank of Boston, which, after a conviction for failing to notify authorities of suspicious transactions in 1985, was the target of significant negative publicity.

In 1986, the approval of the Money Laundering Control Act made the United States a pioneer in criminalizing money laundering, a practice now closely associated with the drug war[19].

In the following years, the subject was addressed in several international acts[20], notably the Vienna[21], Palermo[22], and Merida[23]Conventions, the Inter-American Convention against Corruption,[24] and the OECD Anti-Bribery Convention[25]. This framework was complemented by non-binding rules such as the Model Regulations of the Organization

practice during that period. Two noteworthy cases that exemplify this point are the one of the drug trafficker Alphonse Capone, arrested for tax evasion during the 1920s, and of the gangster Meyer Lansky in the following decade. See ROMERO, Thiago Giovani. **Lavagem de capitais e cooperação jurídica internacional**: a contribuição do GAFI. 2017. 158f. Dissertação (Mestrado em Direito) - Universidade Estadual Paulista "Júlia de Mesquita Filho", Franca. p. 19

15 Amongst other things, the BSA aimed to reduce bank secrecy by imposing upon banks an obligation to notify cash transactions over a threshold of USD 10,000 . See LEVI, Michael; REUTER, Peter. Money Laundering. **Crime and Justice**, v. 34, p. 289-375, 2006. p. 296-305.

16 In legal parlance, the concept of enforcement refers to the executory dimension of jurisdiction, that is, to the aspects related to the implementation or execution of judicial commands.

17 AMICELLE, Anthony. When finance met security: Back to the War on Drugs and the problem of dirty money. **Finance and Society**, v. 3, n. 2, p. 106-123, 2017.

18 AMICELLE, op. cit., p. 113-118

19 HÜLSSE, Rainer. Creating Demand for Global Governance: The Making of a Global Money-laundering problem. **Global Society**, v. 21, n. 2, p. 155-178, abr. 2007. p. 166.

20 For a detailed review of each of these instruments, see CORRÊA, Luiz Maria Pio. **O Grupo de Ação Financeira Internacional (GAFI)**: organizações internacionais e crime transnacional. Brasília: FUNAG, 2013. p. 21-61.

21 ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção das Nações Unidas contra o Tráfico Ilícito de Entorpecentes e de Substâncias Psicotrópicas**. 1988. Available at: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0154.htm Accessed in 12 ago. 2019.

22 ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção das Nações Unidas contra o Crime Organizado Transnacional**. 2000. Available at: http://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_nu_criminalidade_organizada_transnacional.pdf. Accessed in 12 ago. 2019.

23 ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Convenção das Nações Unidas contra a Corrupção**. 2003. Available at: https://www.unodc.org/documents/lpo-brazil/Topics_corruption/Publicacoes/2007_UNCAC_Port.pdf Accessed in 12 ago. 2019.

24 ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Convenção Interamericana contra a Corrupção**. 1996. Available at: http://www.planalto.gov.br/ccivil_03/decreto/2002/D4410.htm. Accessed in 12 ago. 2019.

25 ORGANIZAÇÃO PARA A COOPERAÇÃO ECONÔMICA E O DESENVOLVIMENTO (OCDE). **Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais**. 1997. Available at: http://www.planalto.gov.br/ccivil_03/decreto/D3678.htm. Accessed in 12 aug. 2019.

of American States (OAS)[26] and the Basel Declaration of Principles[27]. These instruments and the organizations[28] responsible for their implementation, regulation, and supervision were gradually constituted as an increasingly cohesive global anti-money laundering regime[29].

The measures characterizing the global anti-money laundering regime can be divided analytically into two pillars: prevention and repression[30].

Prevention seeks to reduce incentives for money laundering, especially using regulatory interventions aimed at increasing institutional transparency. It has four axes: i) Customer Due Diligence (DDC), that is, ongoing verification and monitoring of customer and beneficial owner identities and information; ii) communication of relevant information to the competent authorities; iii) regulation and external supervision of compliance with the previous axes; iv) application of sanctions for failures in implementing the requirements of axes i and ii.

The repressive pillar, in turn, is related to the punishment of criminal subjects and their associates in the occurrence of the crime. It is also divisible into four axes: i) listing of crimes whose proceeds will be subject to AML measures; ii) investigation; iii) prosecution and punishment; iv) forfeiture of assets or capital of illicit origin.

2.2. The International Financial Action Task Force (FATF) and the Risk-Based Approach

Among the various international entities participating in the scheme, the Financial Action Task Force on Money Laundering and the Financing of Terrorism (FATF) have consolidated itself as the main global regulatory body. Created during the 15th G7 Summit in 1989, the FATF was set up as a task force to combat money laundering in the framework of the international war on narcotics trafficking. An informal entity, the task force was appointed and supervised by the G7 and had 11 Member States in its initial composition, with a specific mandate of annual duration. Its work would be on the proposition of measures AML, as well as the structuring of international mechanisms for coordinated implementation of these measures.

Since then, the task force has undergone considerable expansion. Currently composed of 39 members, 28 observer organizations - a category that includes key players in global financial governance, such as the Central Bank, the International Monetary Fund and the World Customs Organization - and 9 FATF-style regional bodies with the status of associate members. Originally focused on combating drug trafficking, its scope has been broadened to include a set of issues grouped under the heading of

26 ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Regulamento Modelo sobre Delitos de Lavagem Relacionados com o Tráfico Ilícito de Drogas e Outros Delitos Graves**. 1992. Available at: http://www.cicad.oas.org/lavado_activos/eng/Model_regula_eng12_02/REGLAMENTO%20LAVADO%20-%20ENG.pdf

27 COMITÊ DA BASILÉIA PARA SUPERVISÃO BANCÁRIA. **Princípios Fundamentais para uma Supervisão Bancária Efetiva**. 2006. https://www.bcb.gov.br/fis/supervisao/docs/core_principles_traducao2006.pdf

28 Examples include the Anti-Money Laundering Liaison Committee of the Franc Zone (CLAB), the Egmont Group of Financial Intelligence Units, the Group of International Finance Centre Supervisors (GIFCS), the International Association of Insurance Supervisors (IAIS), the OSCE, the OCDE and several UN committees. See ROMERO, op. cit., p. 66

29 HELLEINER, Eric. The Politics of Global Financial Reregulation: Lessons from the Fight against Money Laundering. **Center for Economic Policy Analysis**. Working Paper, n. 15, apr. 2000.

30 LEVI, Michael; REUTER, Peter, op. cit., p. 297-299

"threats to the international financial system's integrity": transnational financial crimes, proliferation of weapons of mass destruction, terrorist financing and even financial exclusion, even though the last topic is dealt with on a smaller scale[31].

The task force's growth has been associated with an increasing role in the context of AML/FT policies, in a way that the body is currently the main regulator and supervisor of the issue's governance. This has led to tension between the FATF's formally informal nature and its influence and concrete attributions - which, it is argued[32], are equivalent to those of a de facto international organization. Thus, it has been argued that the task force suffers from a "legitimacy deficit"[33] because it is not an international organization constituted by a charter and is not endowed with international legal personality.

At the regulatory level, the task force's main product is its 40 Recommendations, guidelines initially published in 1990 and formally updated in 1996, 2003/2004 and 2012. The Recommendations are the most well-known international legal instrument for legislative harmonization focused specifically on the theme of AML. In 2001, nine Special Recommendations for combating terrorist financing were also added. Created in a multistakeholder, multidisciplinary and multinational manner, the Recommendations have a deliberately flexible and comprehensive content, which aims to facilitate their implementation in different legal systems. With these characteristics, the FATF has adopted a risk-based approach - as opposed to a rule-based approach - since 2001, which assigns a central role to national regulators and the private sector.

The risk-based approach has been both criticized and praised, and its effectiveness has been the subject of intense debate. On the one hand, the focus on transactions and consumers deemed to be "high-risk" makes this model very dependent on the discretion of the private sector, as this assessment is delegated to private agents. This privatization of the risk identification process has been criticized[34], from a normative standpoint, for operating transferring responsibility from the state to private actors and from a technical standpoint on the assumption that such risks would be knowable by private actors. On the other hand, praise[35] has been made for its flexible, reticular, multistakeholder, dynamic content as well as for its focus on problem-solving, which would be in line with more experimental forms of contemporary governance and contribute to the successful implementation of the Recommendations and to the realization of the task force's broader goals.

Like its issuing body, the 40 Recommendations are informal and therefore non-binding instruments. Nonetheless, the FATF uses a range of enforcement mechanisms, including its mutual assessments - peer review procedures in which members investigate levels of compliance with the Recommendations and provide guidance on how evaluated States can meet their standards - and the practice of listing high-risk jurisdictions, whereby the FATF acquires objective economic sanctioning capacity by imposing restrictions on trade relations between its members and the less cooperative jurisdictions. In addition, FATF membership is conditional on the legislative implementation of the

31 NANCE, Mark T. The regime that FATF built: an introduction to the Financial Action Task Force. **Crime, Law and Social Change**, v. 69, n. 2, 109–129, mar. 2018.

32 HÜLSSE, op. cit., p. 166.

33 CORRÊA, op. cit., p. 118

34 For a summation of this criticism, ver HELGESSON, Karin Svedberg; MÖRTH, Ulrika. Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention. **Crime, Law and Social Change**, v. 69, n. 2, p. 227–248, mar. 2018. p. 230-231.

35 NANCE, op. cit., p. 119

Recommendations. For these reasons, it is argued that the Recommendations amount to practically a multilateral treaty with efficient means of enforcement[36].

The FATF approach emphasizes the expansion of the preventive and repressive capabilities of domestic states[37] rather than control over the cross-border movement of illicit goods and capital. This is accomplished by means of two main strategies: i) promoting legislative harmonization between domestic legal systems to reduce the possibility of capital flight to unregulated havens; ii) encouraging international legal cooperation and information sharing amongst states.

3. CRYPTOCURRENCIES AND MONEY LAUNDERING: REGULATORY RISKS AND TRENDS

The rationality behind the global AML regime is based on the premise that it is possible to intervene in institutional authorities that mediate transactions in order to maximize financial transparency. Item 3.1. of this section examines the ways cryptocurrencies destabilize these strategies from socio-technical innovations that produce new risks. Item 3.2, in turn, considers the two regulatory trends observed so far: private self-regulation and external regulation from nation-states, their merits, and limitations.

3.1. Risks associated with using cryptocurrencies for money laundering

Since 2013, the FATF has been extending its efforts to develop an anti-money laundering approach to cryptocurrencies. To understand the specific challenges faced by this endeavor, it is necessary to understand how money laundering is traditionally operationalized.

The practice of money laundering consists, in general terms, in the processing of proceeds of unlawful origin, existence and/or application in order to conceal and disguise such illegality. Although there is some variation in the literature regarding the topic[38], there is a relative academic[39] and regulatory[40] consensus regarding the possibility of dividing the operationalization of this process into three stages.

The first is the initial insertion of illicit values into the formal economy, a phase called **placement**. There are several ways this can occur, some of the most common of which include fractional bank deposits, or purchases of movable and immovable property and/or monetary instruments.

Then begins the **layering** step. It consists of performing a series of operations aimed at making it difficult to track the trajectory of illicit assets. This step usually involves the movement of values via a network of individuals and companies, which are often scattered

36 ROSE, Cecily. **International anti-corruption norms** - their creation and influence on domestic legal systems. 1 ed. Oxford: Oxford University Press, 2015.
37 HELLEINER, Eric. op. cit., p. 4-5.
38 See ROMERO, op. cit.. p. 19-31.
39 See ROMERO, op. cit., p. 23
40 FINANCIAL ACTION TASK FORCE. **Frequently Asked Questions**. Available at: http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223. Accessed in 15 jan. 2019.

across different jurisdictions. As in the previous stage, there are several mechanisms through which stratification can take place: electronic transfers to anonymous accounts located in secrecy jurisdictions[41], transfer mispricing for tax evasion and avoidance[42] etc.

The effect of this route is the production of a perception of legality in relation to control or ownership of assets, which prepares them for the final stage: **integration** when earnings are definitively reinserted into the formal economy.

When it comes to cryptocurrency and money laundering, there are two fundamental aspects of their infrastructure that underpin traditional AML mechanisms: decentralization and quasi-anonymity.

Decentralization refers to the independence of transactions performed by means of CCs with regards to centralized institutions. This makes it difficult to apply much of the AML regime, as, as previously explained, its framework is almost entirely directed towards regulation and supervision of entities that necessarily centralize most traditional transactions, such as banks and financial institutions.

The second aspect is related to the different levels of **quasi-anonymity** provided by the cryptographic mechanisms embedded in such systems. Customer due diligence requirements, one of the axes of the anti-money laundering preventive pillar, assumes the technical possibility of accessing customers and their related information for analyzing transactions, hence the importance of secrecy jurisdictions for criminals, especially during the layering phase. By decoupling the identities of the parties on the platform from any data that identifies them outside on the platform, cryptocurrencies automate financial secrecy so that it cannot be reversed using the regulatory pathway. This is aggravated by the existence of cryptocurrency tumblers or mixers[43] that further difficult identifying the parties.

41 Researchers associated with the Tax Justice Network, an international coalition of researchers and activists concerned with issues of tax evasion, avoidance and competition, have argued against the analytica use of the terms "tax haven" and offshore financial centers. According to them, the lack of clear and verifiable criteria for listing jurisdictions that fit this category could cause selection bias in the results of research that utilizes such groupings. Furthermore, this classifications' binary implications could damage the development of effective international policies designed to fight the practices related to them. As an alternative, they suggest a conceptual move away from tax aspects and towards legislative approaches to financial transparency among different jurisdictions. The result is a financial secrecy index in which countries are evaluated based on their legislations providing secrecy and their global economic impact. See COBHAM, Alex; JANSKÝ, Petr; MEINZER, Markus. The Financial Secrecy Index: Shedding New Light on the Geography of Secrecy. **Economic Geography**, v. 91, n. 3, p. 281-303, jul. 2015.

42 Tax evasion and avoidance are distinct manners by which individuals can avert paying taxes. Avoidance occurs when such a goal is accomplished by resorting to legally available mechanisms for preventing the tax generating fact from taking place. Evasion, on the other hand, happens when such a fact takes place and the individual employes illegal tools for sidestepping the obligation to pay.

43 This services mediate negotiations to prevent that transactions between specific wallets get traced. They work by receiving funds from several wallets, mixing them in a random fashion and redistributing them between wallets in a manner that it is not possible to identify senders and recipients of specific funds.

Table 1 - Money laundering risks posed by CCs

	Potential exploitation of vulnerabilities at each stage		
General risk factor	Placement	Layering	Integration
Quasi-anonymity	CCs can be used by criminals and associations	Suspicious names, particularly if money mules cannot be flagged	Allowing cashing out of proceeds of crime to be passed on anonymously to individuals that cannot be traced
Real-time transactions	Proceeds of crime can be transferred to another CC in another country	Transactions occur in real-time, allowing little time to stop them if suspected of money laundering	Proceeds of crime can be moved rapidly through the global financial system and withdrawn in another country

Source: Campbell-Verduyn[44]

3.2. Regulatory trends in the 2010s

According to Campbell-Verduyn[45], it can be said that there are three main regulatory trends in the decade of 2010 to combat money laundering with the aid of cryptocurrencies: industry self-regulation, national initiatives, and the FATF risk-based approach. The first two correspond less to regulation models that are planned and implemented in a coordinated fashion and more to scattered sets of initiatives that can be analytically grouped by certain common features.

3.2.1. Industry self-regulation

Industry self-regulation concerns a series of measures voluntarily adopted by players in the cryptocurrency ecosystem to comply with AML standards. Exchanges that exchange CCs for fiat money and vice-versa commonly impose certain requirements on their clients, such as proof of address and identification documents. Notwithstanding these efforts, the lack of sectoral consensus on which measures to take implies high variation in CDD levels between companies. In response, private sector initiatives have sought to establish common industry guidelines.

Examples of such initiatives include guidelines issued by the *Digital Asset Transfer Authority* (DATA), a self-regulatory organization based in Delaware, USA. Open for comment in 2015, its proposal[46] is expressly based on the FATF Recommendations and

44 CAMPBELL-VERDUYN, op. cit., p. 287.
45 CAMPBELL-VERDUYN, op. cit., p. 289-294.
46 DIGITAL ASSET TRANSFER AUTHORITY. **Anti-Money Laundering Guidelines**. 01 jul. 2015. Available at: https://www.slideshare.net/DataSecretariat/data-aml-guidelines-june-2015. Acess on 19 may 2019.

addresses several industry categories (*exchanges*, wallet[47] managers, mining companies[48] etc.). These guidelines include appointing a chief compliance officer, training employees to recognize the suspicious financial activity, implementing internal risk mitigation procedures (CDD, policies for responding to suspicious activity policies that include an obligation to notify authorities, recordkeeping) as well as risk assessments on consumers, transactions, and locations. This program should be demonstrably documented and subject to annual external reviews.

Several other industry organizations have been formed in recent years, most commonly nationally. In 2018, CryptoUK was created, an industry representative association with a code of conduct[49] aimed at self-regulation. In October of the same year, the Japan Virtual Currency Exchange Association, an institution founded by 16 exchanges operating in Japan, received broad regulatory powers from the country's financial authority[50], including those of overseeing, regulating, sanctioning, receiving complaints and offering advice to exchanges. Other examples are the Token Economy Association in Singapore and Croatia's Blockchain and Cryptocurrency Association.

3.2.2. External regulation at national level

Relations between national regulators and the industry have been marked by distrust and concern since the early 2010s. When these goods began to receive greater public attention, the initial reaction most commonly seen[51] by state actors from different jurisdictions was the issuance of an alert document (statement, public notice, etc.) about its potentially problematic aspects. These statements typically boasted that these assets are not, in fact, legal tender because they are not issued or supervised by the Central Bank of their jurisdiction. In addition, there were a number of associated risks: the absence of legal protections for investors and consumers, their high volatility, the possibilities of use for performing illicit acts such as money laundering and terrorist financing, and the lack of regulation on cryptocurrency service providers[52].

Two money laundering cases in 2013 reinforced the association between cryptographic currencies and financial crimes[53]. The first, from Liberty Reserve, was the largest online money-laundering scheme in history until then. Since 2006, the financial transmitter Liberty Reserve had conducted about 55 million transactions, most of them are criminal, using digital currencies called the Liberty Reserve Dollar or Liberty Reserve Euro (LR). Although transfers occurred in LR, the values at the recipients were stored in

47 Mechanisms for managing cryptocurrencies. Users can access these mechanisms in an individual and automated fashion or, as an alternative, they can hire them as services with specialized companies.

48 Entities that employ computer processing capabilities to produce new amounts of cryptocurrencies.

49 CRYPTOUK. **Code of conducts**. [SI]. Available at: http://www.cryptocurrenciesuk.info/code-of-conducts/. Acess on 19 mai. 2019.

50 JAPÃO. **Comunicado da Financial Services Authority**. 24 out. 2018. Available at: https://www.fsa.go.jp/news/30/virtual_currency/20181024-1.html. Acess on 19 mai. 2019.

51 ESTADOS UNIDOS DA AMÉRICA. The Law Library of Congress. Global Legal Research Directorate. **Regulation of Cryptocurrency Around the World**. Washington, jun. 2018. Available at: https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf. Acess on 21 mai 2019. p. 1.

52 As an example, see the notice from the Central Bank of Brazil. BRASIL. Banco Central do Brasil. **Comunicado nº 31.379, de 16 de novembro de 2017**. Available at: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379. Accessed in 23 ago. 2019.

53 For more detailed discussions of the cases in hand, see FINANCIAL ACTION TASK FORCE.. **Virtual Currencies** - Key Definitions and Potential AML/CFT Risks. Jun. 2014. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Accessed in 21 may 2019.

US dollars or euros. To transact in LR, users only needed to register on the transmitter's website, which could be done by reporting false data, since the information was not subject to any verification. Thus, while not involving cryptocurrencies in the strict sense of the term, the Liberty Reserve case was known for using digital representations of value to facilitate often criminal transactions carried out under false identities.

The second case, Silk Road, was based on the use of an Onion trading service in which illicit goods were customarily purchased[54]. The anonymity afforded by the service's infrastructure was complemented by the use of Bitcoin as the exclusive means of payment - each user registered on the platform should have at least one Bitcoin wallet associated with their account, although users could use different wallets for different transactions. At each transaction, the buyer's funds were transmitted to an escrow account maintained by the platform, which held them until the transaction was completed, and then transferred to the seller's wallet. In addition, a cryptocurrency mixer was used in all transactions to provide an additional layer of anonymity.

In this context, regulators are faced with a tension arising from opposing regulatory pressures, which are illustrated by a G20 statement[55] issued in July 2018. On the one hand, the document reaffirms the above-mentioned concerns regarding cryptocurrencies and financial illicit acts, as well as adding tax and financial integrity issues to them. On the other hand, the Group points to curiosity towards the technological innovations associated with these assets, pointing out that they may have "significant benefits for the financial system and the broader economy."

Thus, Campbell-Verduyn observes[56], two opposing regulatory races are engendered in parallel. There is a Race to The Top (RTT) stemming from the push for legal compliance with international AML standards, which is marked by the extension of national standards to the cryptocurrency ecosystem to generate a legitimizing reputational effect on cryptocurrency activities in such jurisdictions. In the midst of regulatory contexts already fraught with distrust and animosity, incentives to counteract the risks associated with cryptocurrency have led, in extreme cases, to prohibitive measures regarding the provision of cryptocurrency services. This is the case of China and India, for example.

By contrast, variation in adopted standards gives rise to opportunities for regulatory arbitrage by a regulated sector that remains encouraged to move to jurisdictions with less burdensome regulations. This last phenomenon, a race to the bottom, is illustrated by the exodus of Bitcoin-related startups in New York following the approval of a very onerous licensing policy in 2015[57]. Given that the race to the bottom undermines the effectiveness of national standards in meeting the broader goals of an ALD policy, Singh[58] argues that national initiatives not only do not succeed but also make legitimate uses of cryptocurrencies unfeasible.

54 Services that can be accessed through the Tor network - a software for navigating in a secure and anonymous manner which provides anonymity for the user and the service provider with regards to traditional means of online identification (via IP and server location, for instance).

55 G20. Communiqué. **G20 Finance Ministers & Central Banks Governors Meeting**. Buenos Aires, 23 jul. 2018. Available at: http://www.g20.utoronto.ca/2018/2018-07-22-finance-en.pdf. Acess on 21 may 2018.

56 CAMPBELL-VERDUYN, op. cit., p. 291-292

57 DEL CASTILLO, M. The 'great Bitcoin exodus' has totally changed New York's Bitcoin ecosystem. **New York Business Journal**, New York, 12 ago. 2015. Available at: https://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html. Acess on 21 may 2019.

58 SINGH, Kevin. New wild west: preventing money laundering in the Bitcoin network. **Northwestern Journal of Technology and Intellectual Property**, v. 13, n. 1, 38–64.

The tried alternatives - extraterritorial legal instruments produced mainly in the US - have done little to remedy the problem, as they rely on the unilateral submission of countries to US jurisdiction. In this scenario, Campbell-Verduyn[59] argues, a gap in global regulation emerges, which is quickly filled by coordinated approaches at the international level

4. INTERNATIONAL AML REGULATION OF CRYPTOCURRENCIES

In parallel with the two regulatory trends cited, some international coordinated regulation efforts have emerged over the last few years. Given the shortcomings of the industry self-regulation model regarding compliance and harmonization, and the regulatory arbitrage issues arising from individual national standards, it can be argued that such a strategy is especially suited to addressing the problem. Item 4.1. observes some initiatives of international regulation, albeit of a punctual and pulverized content. Item 4.2. briefly reviews FATF's treatment of the topic since 2010.

4.1. Directed international efforts

Both self-regulatory efforts by the industry and national initiatives have encountered obstacles to efficient implementation. In this context, several international organizations have sought to address cryptocurrency regulation in a coordinated manner.

In 2015[60], Interpol and Europol initiated a partnership to fight abuse of cryptocurrencies for ML/TF. The project's goal was to stimulate cooperation between organizations and to provide training in fighting criminal uses of cryptocurrencies to facilitate tracing and forfeiting these revenues. Similarly, in 2017[61], the United Nations Office on Drugs and Crime (UNODC) and the Organization for Security and Cooperation in Europe (OSCE), offered training for law enforcement agents and banking professionals to investigate money laundering and other Bitcoin-related financial crimes. The UNODC also issued a basic manual for detecting and investigating money laundering with CCs in 2014[62].

4.2. FATF's strategy: regulating service providers

In this international context, FATF has been noted for its efforts to update its risk-based approach to address the cryptocurrency industry ecosystem. The topic was first addressed by the Group as early as 2010, in a report[63] on new payment methods, which

59 CAMPBELL-VERDUYN, op. cit., p. 292.

60 EUROPEAN UNION. INTERPOL Cybercrime Conference makes the case for greater multi-sector cooperation. **Europol Newsroom**, [s. I.], 02. out. 2015. Available at: https://www.europol.europa.eu/newsroom/news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-for-greater-multisector-cooperation. Acess on 21 may 2019.

61 UN. UNODOC helps tackle bitcoin banking fraud and money laundering. **Escritório das Nações Unidas sobre Drogas e Crime**, Viena, 01 fev. 2017. Available at: https://www.unodc.org/unodc/en/frontpage/2017/February/unodc-helps-tackle-bitcoin-banking-fraud-and-money-laundering.html. Acess on 21 may 2019.

62 UN. **Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies**. jun. 2014. Available at: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Accessed in 21 may 2019.

63 FINANCIAL ACTION TASK FORCE. **Money Laundering Using New Payment Methods**. oct. 2010. Available at:

noted the risks arising from digital currencies and unregulated exchanges. Later, in 2013, the issue was taken up in a guide[64] on internet services, mobile payments, and prepaid cards. The document described the main functionalities of these technologies and pointed out that some of their variations could represent ML/TF risks, meaning that they fit the scope of the organization.

The following year, the organization produced its first specific and detailed study[65] on the matter, seeking to establish a common definitional vocabulary and identify the main risks of ML/TF. The study distinguished currencies convertible to fiat money from non-convertible currencies and centralized from decentralized ones. The organization also described key components of the cryptocurrency ecosystem (exchanges, administrators, users, miners, mixers, wallet providers, among others), as well as noted potential benefits and risks of virtual currencies, especially those arising from anonymity and global reach of its infrastructures. In addition, it considered the challenges for identifying the entities that should be the focus of AML investigation and prosecution activities.

In 2015, the Group produced a new guide[66] to clarify the implementation of its Recommendations for the convertible virtual currency ecosystem. The approach suggested that AML measures should emphasize "points of intersection that provide gateways to the regulated financial system — and not seek to regulate users who obtain VC to purchase goods or services."[67] The focus of the suggested approach was the exchanges, although national authorities were encouraged to consider regulating financial institutions and other agents who store and trade virtual currencies.

Noting the risks of regulatory arbitrage in the event of an operating ban and the negative impacts of this phenomenon globally, the guide suggests that authorities should regulate exchanges. Regulation should comply with the preventive pillar of the AML regime, that is, it should impose several requirements on exchanges: risk assessment and mitigation, CDD, recordkeeping, licensing or registration obligations and duty to report suspicious transactions to the authorities. It is also suggested that countries establish dissuasive and proportionate sanctions (administrative, civil or criminal) for dealing with infringements. In addition, national authorities should develop domestic coordination and cooperation mechanisms, such as interagency groups, to maximize enforcement effectiveness with different components of the ecosystem.

In October 2018, the FATF updated its Recommendations and Glossary to include the terms "virtual assets" and "virtual asset service providers" (VASPS), as well as the requirement that the latter be regulated, supervised and obliged to get licensed or registered[68]. This provision has been incorporated into the text of Recommendation 15 on new technologies, the implications of which have been examined in detail in a draft Interpretive Note to the Recommendation published on February 2019[69]. Amongst the

http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf. Acess on 21 mai. 2019.

64 FINANCIAL ACTION TASK FORCE. **Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services**. jun. 2013. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf. Acess on 21 may 2019.

65 FINANCIAL ACTION TASK FORCE, 2014, op. cit..

66 FINANCIAL ACTION TASK FORCE. Guidance for a Risk-Based Approach to Virtual Currencies - Convertible Virtual Currency Exchangers. jun. 2015. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Acess on 21 may 2019.

67 Tradução livre de: . GAFI, op. cit., 2015, p. 6th

68 FINANCIAL ACTION TASK FORCE, 2019, op. cit., p. 2.

69 FINANCIAL ACTION TASK FORCE. **Public Statement - Mitigating Risks from Virtual Assets**. GAFI, Paris, 22 fev.

project's guidelines: countries should consider CCs as "properties", "funds" or equivalents for or AML purposes, they should apply a risk-based approach to the CC ecosystem and appoint a competent authority to supervise service providers - that is, service providers cannot be subject to mere industry self-regulation. In addition, the Group explained that the guidelines apply to transactions and exchange operations between different "virtual assets" as well as between "virtual assets" and fiat currencies.

In June 2019, FATF updated its guide to a risk-based approach applied to "virtual assets"[70] to adapt it to some of the new developments in the field. Among the key innovations contained in the new version of the guide, is a change in the Group's treatment of the different categories of "virtual asset service providers" (VASPS). While the previous version emphasized exchanges and the conversion of "virtual assets" into fiat money, the 2019 guide highlights the increasing use of conversion schemes between different CCs to emulate the traditional money laundering layering step and produce higher levels of anonymity and obfuscation. In addition, it notes the growing role of mixing services and similar technology in ensuring anonymity.

In line with the broadening of concerns, the guide emphasizes that the concept of VASP encompasses any entity that conducts the operations of exchange (between different "virtual assets" and/or between any of them and sovereign currency), transfer, custody and/or administration of "Virtual assets" and/or instruments that facilitate control over their assets (such as wallets). In addition, entities that participate in the provision of services related to their offer, issue and/or sale are included - such as in Initial Coin Offering[71].

It is also specified that VASPS supervision and monitoring should not be assigned to a self-regulating entity. Its conduct should be carried out by competent authorities with the necessary powers to ensure compliance with applicable rules, including the conduct of inspections, the obligation to produce information and the imposition of disciplinary and financial sanctions - including powers relating to VASPS licenses. In addition, the provisions on the implementation of preventive measures (such as Know-Your-Customer and record-keeping obligations), CDD (applicable to occasional transactions over a threshold of USD/EUR 1000) and obligations regarding the processing of transfer information. Finally, the guide notes that countries should ensure harmonization between AML standards and privacy and personal data protection rules.

2019. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html Assunto em: 26 may 2019.

70 It is important to notice that due to the late launching of this document compared to the period in which this study took place, we did not implement its updates in data collection instrument nor were they considered during data analysis. As a consequence, this sections limits itself to briefly presenting some of the developments contained in the guidance, which can be accessed in FINANCIAL ACTION TASK FORCE. **Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**. jun. 2019. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. Acess on 23 jun. 2019.

71 Also known as tokensale, crowdsale ou coinsale, it is a mechanism for raising capital for new cryptocurrency-related projects. They usually involve selling digital tokens of a given coin through action and / or subscription before its launching. The tokens can be paid for in fiat money and / or other CCs. See CHOHAN, Usman W. Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. **SSRN Electronic Journal**, [sl], p.1-6, 2017.

5. METHODOLOGY FOR INFORMATION GATHERING

The regulatory concern regarding cryptocurrencies broadly focuses on two aspects: combating more sophisticated illicit capital flow practices while providing a favorable environment for the lawful development of new transactional possibilities brought about by the blockchain. A balance between these two regulatory objectives is sought in the internationally proposed harmonization of cryptocurrency laws.

In order to verify to what extent there is conformity between these objectives and the practices of the countries ahead of the proposed standardization, it was necessary to define an aspect to be studied in their regulation, an instrument to observe it and criteria for defining the sample that integrates the results. The following are the delimitation of each of these aspects and their relevance to the construction of the results, as well as the sources consulted.

5.1. Definition of a study subject: exchanges

The flow of cryptocurrencies is difficult to control or enforce, as there is usually no need for intermediaries or authorities to move large amounts internationally. Therefore, the FATF's normative proposal regarding this new technology is to encourage the standardization of the treatment of flows of value using international assessments, but also to promote the reception in state systems of an international anti-money laundering regulation standard applicable to institutions that handle transactions involving cryptocurrencies.

Thus, the enforcement proposed by the FATF standards would not fall on transactions made by individual users via blockchain, which are of low traceability. The regulation would focus on transactions involving the use of these assets in addition to transactions within the software. Regulated subjects would be the intermediaries that enable contact between the cryptocurrency ecosystem and that of assets and fiduciary currency, such as portfolio managers, exchanges, buying and selling establishments, and cryptocurrency issuers.

Even when moving large amounts of cryptocurrency from one country to another or from one person to another, users will eventually have to convert to local money if they wish to purchase goods and services. In addition, the illicit fiduciary money exchange may be used for the stratification procedure, i.e. opacity of the final beneficiary and the source of the traded amounts.

Exchanges would be services by means of which you can exchange different cryptocurrencies or exchange cryptocurrencies for fiduciary money and vice versa. Considering the role that exchanges play in this financial ecosystem, being a true point of contact between the fiat money and cryptocurrency systems, they were chosen as the research object. The aim was to evaluate the adequacy of anti-money laundering regulatory policies to the cryptocurrency scenario, taking into account the precautions taken with regard to effectively defining, regulating and supervising exchanges.

5.2. Creation of the observation instrument

In order to obtain information about the normative policies related to the research theme, benchmarks were initially selected to be observed in each country. Official documents from the International Financial Action Task Force (FATF) were listed with recommendations prepared by the Task Force regarding the adequacy of each member's internal regulations to anti-money laundering measures.

Referring to the document "Virtual Currencies, Guidance for a Risk-Based Approach"[72], which lists 18 recommended requirements focused on virtual assets, the relevant aspects to be observed were extracted. The full recommendations can be found in the document "International Standards on Combating Money Laundering and Financing Terrorism and Proliferation - The FATF Recommendations", which was consulted for further analysis.

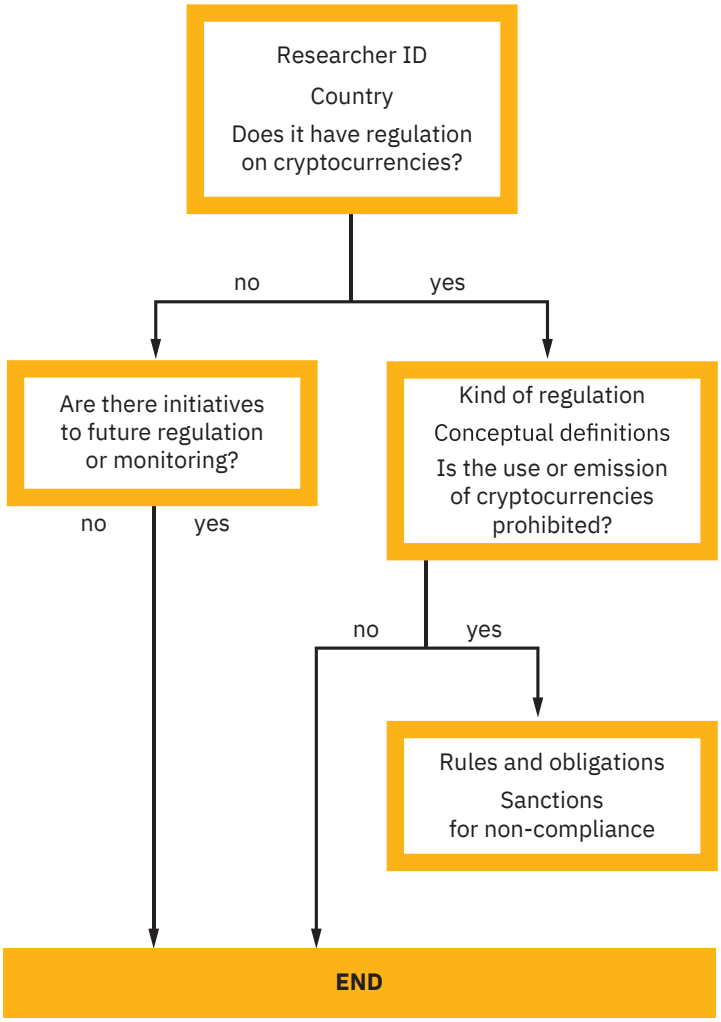
A summary table was prepared, drawing from each recommendation the aspect to be investigated in each country's normative system in order to conclude whether or not it is appropriate (at least in the legislative sphere) for anti-money laundering policies. This table can be found in Appendix A.

Transparency International's 2018 report[73] was also used as a reference for measures to assess the legal adequacy of G20 countries against money laundering. The questionnaire presented in this report was combined with the summary of FATF recommendations pertaining to virtual assets. Some questions have been removed from the G20 questionnaire applied by Transparency International because they are too focused on other institutions that do not deal with cryptocurrencies directly. Likewise, questions that were unverifiable by simply consulting a country's regulatory system or surveys previously published were ruled out, as they would require field research and/or interviews with experts.

Finally, the issues to be evaluated were summarized in 8 questions or checklists to assess cryptocurrency regulatory policy compliance to international ALD standards, focusing on fiat and cryptocurrency exchange services. The information-gathering instrument produced at the end of these steps was a structured evaluation form on the Google Forms platform, available at Appendix B at the end of this paper. The form has the following structure:

72 FAFT, Cited, 2015.

73 TRANSPARENCY INTERNATIONAL. **G20 leaders or laggards**? Reviewing G20 promises on ending anonymous companies. 2018. Available at: <https://www.transparency.org/_whatwedo/publication/g20_leaders_or_laggards>. Access on: 14 may 2019.



i) initial part, with identification of the researcher in charge, country evaluated and whether or not it has regulation on cryptocurrencies;

ii) if the regulatory response is negative, the form refers to a question about government initiatives for future regulation or monitoring of cryptocurrencies;

iii) If the answer on the regulation of item (i) is positive, the form refers to a block of questions regarding the type of regulatory instrument (whether binding or not, whether legislative or not), the conceptual definitions of cryptocurrencies, exchanges and related services present in it, as well as whether regulation is to prohibit such activities - in case of prohibitive legislation, the questionnaire ends in this block;

iv) In the case of regulatory and non-prohibitive rule in item (iii), the form refers to a last block, with two checklists: one on the restrictions and regulatory requirements of ALD applicable to cryptocurrency services (customer identification, transaction guard, minimum retention time, high risk threshold, notification of suspicious transactions, license to service before authority, cooperation with authorities, provision for external authority) and other sanctions applicable for non-compliance (warnings, acquiescence orders, fines, administrative restrictions on employees, suspension/withdrawal of leave, criminal sanctions).

5.3. Sample definition - G20 members

The sample selected for this survey was the G20 - Group of 20 countries, composed as a forum with the European Union as the leading organization plus 19 major or emerging countries: South Africa, Germany, Saudi Arabia, Argentina, Australia, Brazil, Canada, China, South Korea, United States, France, India, Indonesia, Italy, Japan, Mexico, United Kingdom, Russia and Turkey.

It is assumed that countries with higher economic potential are favorable environments for the settling of exchanges, due to the large volume of transactions and values of their economies, which would increase interest in foreign exchange operations. Moreover, as already portrayed in the introductory and theoretical-contextual sections of the research, the G20 has a direct connection with the FATF, which influences its financial policy.

The Group's relevance to the economic scenario is perceived since its foundation, at the time of the Asian financial crisis of 1999, when a meeting of finance ministers and central bankers was realized to address its consequences[74]. Consolidation of the G20 into its current format took place in 2008, during a global crisis following the collapse of Lehman Brothers bank, in which the G20 was brought to the level of a forum of leaders for international economic cooperation[75]. Its members are representative, as in 2011 they were about 90% of world gross national product and 80% of international trade, as well as 65% of the planet's population[76].

The focus of this research in the G20 is therefore due to the great flow of assets, people and capital in these states, which is expected to be an attractive factor for companies dealing with the exchange of financial values. The exchanges would have a market and customers in these places, as they are home to the largest open capital companies in the world[77], as well as the largest banks[78].

This survey aimed to investigate how the G20 countries politically and normatively approach this new financial service model - exchanges, or cryptocurrency/crypto assets, verifying the existence of incentives, requirements and/or prohibitions imposed on them.

5.4. Time scope

Data collection took place between March 15 and June 19, 2019, so that the regulations were analyzed according to the availability and modifications already implemented in this period.

Some draft legislation, notably that of France and Russia, are in the final proceedings at their respective congresses, therefore the available text and documents on these draft were considered in order to raise the concepts, rules, obligations, and sanctions

74 G20. **About G20.** Available at: <http://g20.org.tr/about-g20/>. Access on: 19 jun. 2019.

75 G20. **What is the G20 summit?** Available at: <https://g20.org/en/summit/about/>. Access on: 19 jun. 2019.

76 VIANA, André Rego; BARROS, Pedro Silva; CALIXTRE, André Bojikian. **Governança global e integração da América do Sul**. Brasília: Ipea, 2011.

77 FORBES. **The World's largest public companies**. 2019 ranking. Available at: <https://www.forbes.com/global2000/list/#tab:overall>. Access on: 09 aug. 2019.

78 FORBES. **The World's largest public companies**. 2019 ranking: Major banks. Available at: <https://www.forbes.com/global2000/list/#industry:Major%20Banks>. Access on: 09 aug. 2019.

envisaged. However, as pending projects may be vetoed and amended prior to final approval, these situations may change after the publication of this research. In the case of South Korea, the text considered was of regulation published to stay in force until January 2019, assuming its tacit renewal, due to the unavailability, among the documents available in English on the official website of translated Korean legislation, of another document about the topic. Regarding Canada, the provisions of the approved legislation were considered, although, on the Canadian Parliament website, where the norm can be consulted, it is noted that such law needs regulation in order to become effective.

Having made this delimitation and the corresponding caveats, the following are the sources consulted for each normative system.

5.5. Sources

The results of this research were obtained through the form constructed as described above, which was completed by consulting five source categories, in this order:

i) regulation of one's own country on money laundering, banks or fintechs[79];

ii) material produced by the Library of Congress on cryptocurrency regulation[80] [81];

iii) mutual evaluations of FATF member countries[82];

iv) indirect but official sources, such as institutional documents for instruction in financial services or surveys conducted by teams of lawyers from the respective countries (especially in Indonesia, Japan, and Russia, where there was a language barrier to accessing original regulatory material);

v) websites specialized in finance and cryptocurrency, as support for updating information and understanding the effects of each regulation.

79 Companies which work on the field of technologies for the financial market, mainly cryptocurrencies.

80 USA. THE LAW LIBRARY OF CONGRESS. Global Legal Research Directorate. **Regulation of Cryptocurrency in Selected Jurisdictions**: Argentina, Australia, Belarus, Brazil, Canada, China, France, Gibraltar, Iran, Israel, Japan, Jersey, Mexico, Switzerland. Washington, jun. 2018. Available at: <https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf>. Access on: 13 jun. 2019.

81 USA, Cited, 2018b.

82 FATF. **Mutual evaluations**. Available at: < http://www.fatf-gafi.org/publications/mutualevaluations/>. Access on: 13 jun. 2019.

5.6. Summary table of regulations and sources used

Table 01 - Jurisdictions, respective normative instruments, and sources consulted

Member	Instruments	Sources consulted
European Union	Directive 843/2018	https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L0843&from=EN
South Africa	Central bank position paper (2014); Financial authority position (2018)	https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf http://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx
Germany	Banking Act (updated in 2017)	https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_kwg_en.pdf?__blob=publicationFile&v=3
Saudi Arabia	Monetary authority announcement (2018)	http://www.sama.gov.sa/en-US/News/Pages/news12082018.aspx
Argentina	Income tax law (updated in 2017); Resolution 300/2014 of Financial Information Unity (2014)	http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/44911/texact.htm http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm
Australia	AML/CTF Act (updated in 2017);	https://www.legislation.gov.au/Details/C2019C00011
Brazil	Normative instruction RFB n 1888/2019; Letters n. 01/18 and n. 11/18 of the Securities Commission - CVM (2018)	http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592 http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-0118.pdf http://www.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sin/anexos/oc-sin-1118.pdf
Canada	Income Tax Act; Proceeds of Crime (Money Laundering) and Terrorist Act (2014)	https://laws-lois.justice.gc.ca/eng/acts/I-3.3/nifnev.html http://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/royal-assent/page-4 http://www.loc.gov/law/foreign-news/article/canada-canada-passes-law-regulating-virtual-currencies-as-money-service-businesses/
China	Joint declaration of 7 authorities banning cryptocurrency services (2017)	http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html https://www.coindesk.com/chinas-ico-ban-a-full-translation-of-regulator-remarks
South Korea	Directives anti-money laundering by Financial Intelligence Unity - KOFIU (2018)	http://meng.fsc.go.kr/common/pdfjs/web/viewer.html?file=/upload/press1/20180129185559_dd6b4ef5.pdf https://www.kofiu.go.kr/KOFIU/english/sub05/news_view.jsp?mm=5&sm=1&srl_no=26&table=tb_hp025&tbchar=offc_anc

United States	FinCen's Guide on applicability of regulations to Persons Administering, Exchanging or Using Virtual Currencies (2013)	https://br.cointelegraph.com/tags/usa https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
France	Action Plan for growth and transformation of companies (PACTE) (2019)	https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France http://www.assemblee-nationale.fr/15/ta/tap0258.pdf
India	Central Bank announcement banning cryptocurrency services (2018)	https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=11243&fn=2&Mode=0
Indonesia	Trade Ministry's announcement (2019)	http://bappebti.go.id/resources/docs/siaran_pers_2019_02_18_gpfdzt8b_id.pdf https://cointelegraph.com/news/indonesias-commodity-futures-regulator-releases-regulation-for-crypto-futures-market
Italy	Legislative Decree n. 90/2017	https://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg
Japan	Payment Services Act (2009 updated in 2017); Act on Prevention of Transfer of Criminal Proceeds (updated in 2017)	http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02
Mexico	Fintech Law (2018)	http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf
United Kingdom	Revenue and Customs Brief 9: Bitcoin and other cryptocurrencies (2014); Bank of England regulatory proposal	https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf
Rússia	Federal Law No. 115-FZ On Countering Money Laundering and the Financing of Terrorism (2001 as amended 2004), Central Bank Position (2017) and Bill on Digital Financial Assets (2019 - on deliberation)	https://www.legislationline.org/documents/id/4294 https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176664/russia https://gettingthedealthrough.com/area/92/jurisdiction/26/fintech-russia/ https://cointelegraph.com/news/russia-to-adopt-crypto-legislation-within-two-weeks-deputy-finance-minister
Turkey	Nonexistent	https://medium.com/@ogucluturk/current-regulatory-framework-of-cryptocurrencies-tokens-in-turkey-111bbc9dbab2 https://www.tspb.org.tr/wp-content/uploads/2017/12/Genel-Mektup-785-Sanal-Paralara-Dayal%C4%B1-%C4%B0%C5%9Flemler-hk..pdf

Source: the authors

6. RESULTS AND DISCUSSIONS

The data organization was as follows: compilation of the conceptual elements present in the regulation to characterize cryptocurrencies and exchanges; nature of the regulation on exchanges, including rules and obligations imposed on such services with regard to AML; and enforcement measures on compliance with these rules, with verification of sanctions applicable in case of violations and non-compliance. After their presentation, the results are discussed by topic at the end of this section.

6.1. Concepts adopted in the regulation

The innovative character of cryptocurrency-enabled transactions points to the need for proper recognition, conceptualization, and strategies to monitor the exchange of this type of asset for fiduciary money. For this to be possible, regulation should embrace conceptualization that can define its scope, especially when it comes to innovative technology and where there may be doubts about identification, such as cryptocurrencies. The first section of these results deals with the completeness assessment of the concepts presented in the regulation of countries regarding cryptocurrencies and exchanges.

6.1.1. Cryptocurrency

The concept of cryptocurrency may vary, containing or not all the potentially defining elements of this technology. Ideally, in normative instruments, we seek to specify the regulated object while maintaining the necessary scope so that the new transactional forms do not fall outside the norm. In general, the cryptocurrency conception is composed of 8 elements, which can be categorized according to their structural or functional character[83]:

83 The elements were identified from two documents:"Virtual Currencies: Key definitions and potential AML/CFT risks", of FATF, which works as a normative reference, indicating how it "ought to be" the concept; and "Global Cryptoasset Regulatory Landscape Study", of Alternative Finances Center, of Cambridge University, which indicates common aspects of the concept found in various regulations analyzed, besides proposing the categorization between structural and functional elements. See: FATF, 2014, Cited. AND BLANDIN, Apolline, et al. **Global Cryptoasset Regulatory Landscape Study**. Available at SSRN. University of Cambridge: Judge Business School, 2019, p. 36. Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf Access on: 18 jul. 2019.

Table 02 - Classification between functional and structural conceptual elements for cryptocurrencies

Functional elements	1) digital value representation
	2) tradable/transferable
	3) mean of payment
	4) value storage
	5) unity of account
Structural elements	6) no legal tender
	7) decentralized technology
	8) non-governmental or not ensured by jurisdiction before others

Source: the authors

The two broad categories are identified according to the characteristic concerning: i) uses or meanings that cryptocurrency gains as it is embedded in the economy (functions) and ii) ways of identifying and distinguishing cryptocurrency from physical currencies or digital representations of fiduciary currency or other types of virtual tokens (structure). Thus, the relevance given by the regulatory instruments to each aspect considered characteristic of cryptocurrencies was investigated, not only to have an idea of how the normative measures meet the reality of this type of asset but also to understand which elements are considered for creating standards and rules for cryptocurrencies.

The table below depicts the elements elected to delimit the regulated object in each jurisdiction:

Table 03 - Conceptual elements for cryptocurrencies

Country	Functional elements					Structural elements		
	digital value representation	tradable/ transferable	mean of payment	value storage	unity of account	no legal tender	decentralized technology	non-governmental
Japan	x	x	x	x				
Brazil	x	x	x	x	x	x	x	
Italy	x	x	x			x		x
Mexico	x		x					
European Union	x	x	x			x		x
United Kingdom	x	x	x	x			x	
France	x	x						
United States			x					
Australia	x	x	x	x	x			x
South Korea	x	x	x	x				
Germany	x		x	x				
Argentina	x	x	x	x	x	x		x
South Africa	x	x	x	x	x	x	x	
Russia	x							

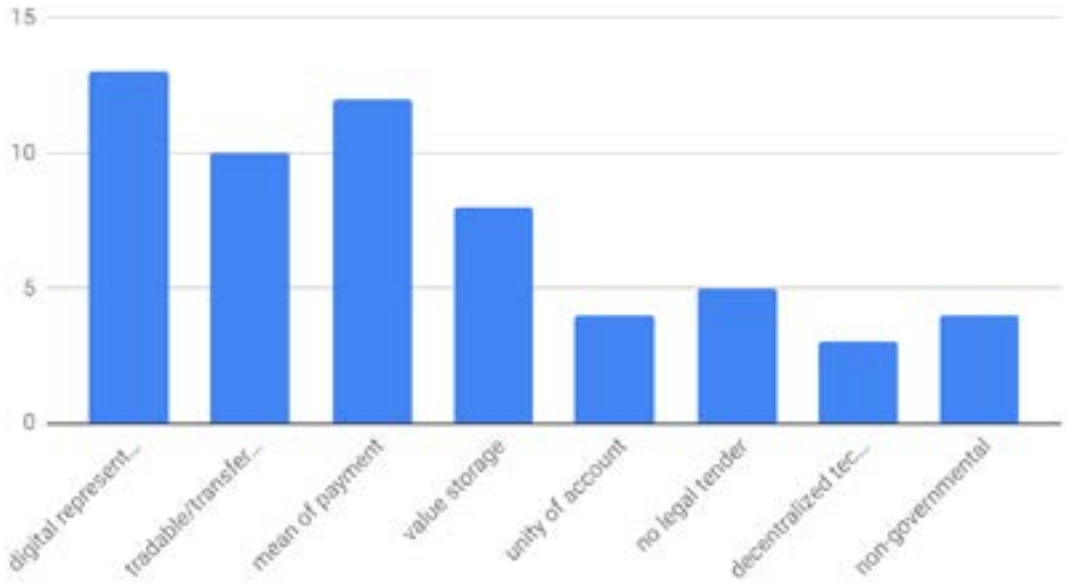
Source: the authors

It appears from the data obtained that none of the countries analyzed has a concept that explicitly covers all elements of the table. This may denote a lack of consensus as to which elements shape the concept of cryptocurrencies, or it may indicate a lack of knowledge of legislators about this technology.

Some regulations, such as the United States, Russia, Mexico, and the United Kingdom, use only two or even a single element to define cryptocurrencies. This may be a shortcoming in the normative instrument because, without limiting what is involved in the regulated situation, there is a risk that the rule will not be applicable. It may yet create uncertainty regarding the regulated subjects, allowing greater discretion in the supervision of these entities.

Combining the data, it can be seen that Australia, South Africa, Argentina, and Brazil present the most complete conceptualization, with 6 or 7 conceptual elements. In Brazil and South Africa, the only feature not presented in the regulation to identify cryptocurrencies is the absence of a link with State authority. In Argentina, although there is the non-governmental factor as a conceptual element, the use of technology without a central point is not directly mentioned in the regulation. In Australia, however, both the absence of a central point and the absence of legal value are not conceptual elements, and an asset that has a legal guarantee in some part of the globe can be considered as cryptocurrency, provided that it meets the other identification criteria.

Chart 01 - Frequency of elements present in the cryptocurrency concept



Source: the authors

The least frequent element was structural, about the absence of government bond or jurisdictional guarantee. This character would be linked to the conception of cryptocurrencies as an asset that is not dependent on or influenced by financial policies, that is, without the possibility of issuance by institutional demand and without being linked to any authority figure.

This would allow the autonomous functioning of the system, without a central control point, in accordance with the ideal propagated by several actors historically connected with the emergence of blockchain protocols[84]: a political-philosophical perspective marked by strong animosity towards centralized institutional authority and pro-use of cryptographic mechanisms to evade it.

Nevertheless, some cryptocurrencies have been dissociated from this original model and their functionality has been added to a centralized structure, or their value has been associated with that of a fiat currency. This is a possible reason why this element is not present in the cryptocurrency conceptualization of the analyzed regulations.

6.1.2. Exchange

The definition of exchange is relevant insofar as the absence of this concept in regulation can leave this type of enterprise on the sidelines of the normative scenario. Still, there is a risk of confusion between different types of services, and exchanges are of particular importance in the cryptocurrency services landscape, as they are one of the main bridges between the bureaucratic and regulated system of financial institutions and the global and liberal system proposed by cryptocurrencies.

According to a study commissioned by the European Parliament's Special Committee on Tax Evasion and Financial Crimes[85] there are 7 categories of agents involving cryptocurrencies: 1) users, who would be people who use cryptocurrencies as a store of value or means of payment in everyday transactions; 2) miners, who use computational power to perform mathematical operations that reveal new specific cryptocurrency units; 3) exchanges, which carry out exchange transactions between fiduciary currency and cryptocurrencies or between cryptocurrencies themselves; 4) trading platforms, where users exchange cryptocurrencies with each other; 5) wallet providers, which are categorized into three types: user wallet password managers, software that assists in encrypting the wallet of users, and hardware that assists in security of wallet encryption; 6) coin inventors, who developed the technical foundations of cryptocurrencies and defined their rules of use; 7) initial coin offerings, which offer cryptocurrencies when they are created, for payment or not.

A service that promotes wallet management, making transactions and investing with cryptocurrencies, for example, does not match exchanges. However, the European Parliament study points to regulatory blind spots, such as miners, wallet providers (as only wallet password managers are included in ALD regulations, which excludes management hardware and software), user-to-user cryptocurrency trading platforms, and coin offerors.

One hypothesis for this regulatory gap regarding cryptocurrency agents would be that there is no necessary contact with the fiduciary currency system and therefore neither with banks. This can cause difficulty in identifying the source and destination of managed values. Nevertheless, the same study[86] highlights the focus of AML policies

84 See SWARTZ, Cited, p. 3 - 6. See also PAGLIERY, Cited.

85 HOUBEN, Robby; SNYERS, Alexander. **Cryptocurrencies and blockchain** - legal context and implications for financial crime, money laundering and tax evasion. European Union: Policy Department for Economic, Scientific and Quality of Life Policies, jul. 2018. p. 76-79.

86 HOUBEN; SNYERS. Cited. p. 76-79.

on cryptocurrency wallet exchanges and password managers, which converges with the need to distinguish between these services and others in order to have appropriate regulations for each format.

The elements contained in the definition of exchange were obtained from reading and grouping common characteristics between regulations, reaching the following set:

Table 04 - Conceptual elements to characterize exchanges

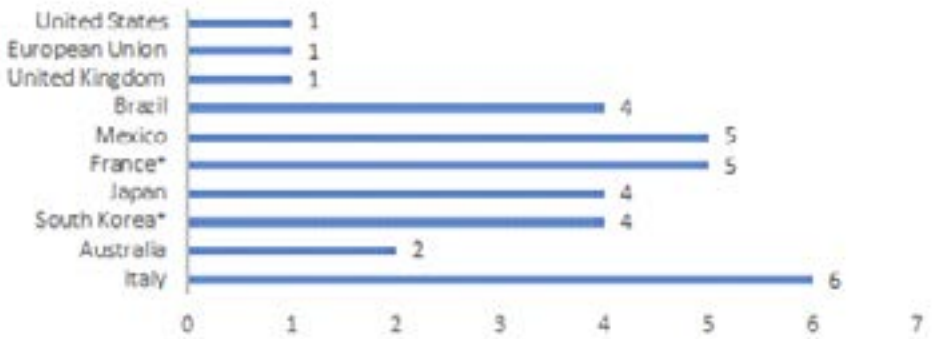
Elements used to characterize an exchange	Service character
1) The exchange between cryptocurrency and fiduciary currency	Contribute to framing exchanges as agents of the financial system
2) The exchange between different virtual currencies	
3) Issuance and control of virtual currency flow	
4) Buying and selling virtual assets	Contribute to framing exchanges as a generic service, that is, a category that does not necessarily approach the financial system
5) Third-party virtual asset management	
6) Virtual asset transaction enabler	
7) It is treated as a type of service provider	

Source: the authors

As with the concept of cryptocurrencies, not necessarily the absence of some elements characterizes incomplete or ineffective regulation. Cryptocurrency issuance, for example, is not an activity performed by all trading companies; some only transact, without the technology to issue or the logistics and purpose of purchasing or selling cryptocurrencies.

There are features that are confused with other services, such as transaction management and facilitation, which does not distinguish exchange from other companies that provide services involving cryptocurrency. Therefore, when the regulation has all the elements, it does not have specificity to the problems generated by cryptocurrency exchange operations. This makes it difficult to apply AML measures similar to those directed at financial institutions.

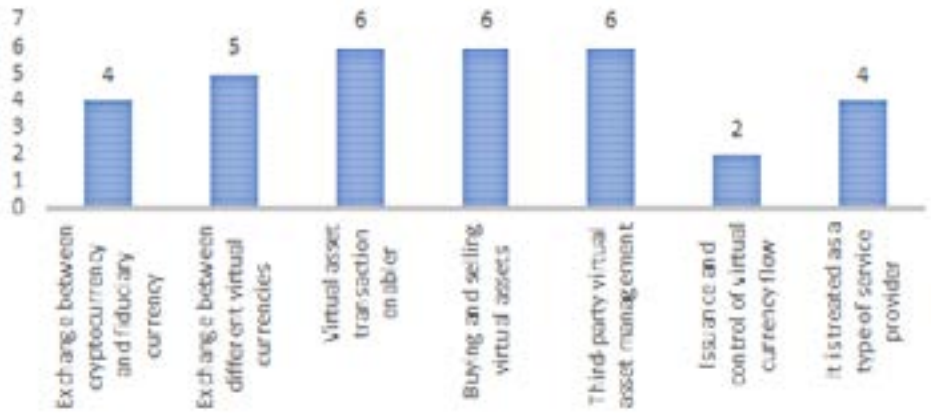
Chart 03 - Number of conceptual elements to define exchange, by jurisdiction



*France considered based on its Bill and South Korea considered assuming the revalidation of the document with an expiration date in January 2019.
Source: the authors

Only half of the G20 countries defines, though amid other types of activity, exchange services. The definition also has wide diversity between countries, with some countries including 6 conceptual elements and others using only one characteristic to define the regulated object. Some of the countries concerned with conceptualizing cryptocurrencies do not direct their regulatory policies toward ventures that exchange these assets.

Chart 04 - Frequency of conceptual elements for exchange



Source: the authors

Given the frequency of elements present in the conceptualization of exchange, it is noted that the regulatory concern does not focus on its distinction from other cryptocurrency service providers.

Only Japan, Italy, France, Australia, and South Korea, as countries, include exchange functions in the exchange concept, and only Australia distinguishes them from other services, not jointly dealing with Wallet management, buying and selling of assets and transaction facilitators.

The presence of conceptual elements for the *exchanges* in each regulation may be synthesized as the following table:

Table 05 - Conceptual elements for ALD regulation exchanges

	Elements present in the concept of exchanges						
	Contribute to framing exchanges as agents of the financial system			Contribute to framing exchanges as a generic service			
	The exchange between cryptocurrency and fiduciary currency	The exchange between different virtual currencies	Virtual asset transaction facilitator	Buying and selling virtual assets	Third-party virtual asset management	Issuance and control of virtual currency flow	It is treated as a type of service provider
Italy	x	x	x	x	x		x
Australia	x	x					
South Korea*	x	x		x	x		
Japan		x	x	x	x		
France*		x	x	x	x		x
Mexico			x	x	x	x	x
Brazil			x	x	x		x
United Kingdom			x				
European Union	x						
United States						x	

Source: the authors

In only 4 G20 member regulations, exchange is explicitly defined as an institution that “trades between virtual and fiduciary currency”, namely Italy, Australia, South Korea, and the European Union.

There is a tendency not to frame exchanges exclusively as financial agents in regulatory systems, and elements that configure them as generic services are present in 7 countries: Italy, South Korea, Japan, France, Mexico, Brazil, and the United States. The only two definitions that use the restrictive concept for exchange services, bringing them closer to financial agents without embracing other types of services together, are Australia and the European Union.

The restrictive definition may be more consistent with AML policy, since the framing of exchange as a category of service close to financial agents may lead to a more rigorous treatment of these ventures. Applying AML rules and obligations, if tailored to each service in an appropriate manner, can be more effective because it inserts specificities that would not be possible when dealing with a wide range of differentiated activities as if they were a single category.

The low granularity, represented by the lack of regulation directed to each type of cryptocurrency service in several countries, may indicate a lack of specific attention to exchanges as actors of contact with the financial system, as well as their centralizing potential for AML policy implementation with regard to cryptocurrencies.

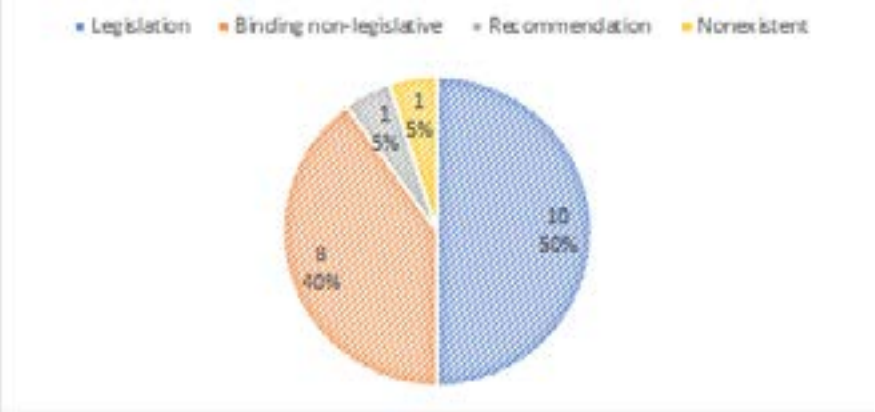
6.2. Regulation about exchanges

Having observed the way in which regulation conceptually approaches the regulated subjects studied here, it is now necessary to pay attention to the quality and content of the imposed norms. Specifically, for the reasons already outlined in the methodological section, attention is paid to the regulation of exchange services on AML scope. The nature of the regulatory instruments is addressed, as well as the degree of attention given to them according to the international parameters regarding the prediction of practices to be observed by these agents.

6.2.1. Nature of the regulatory instrument

Three categories of the regulatory instrument were identified, and the framework of the G20 members’ normative scenario regarding cryptocurrencies and ALD was distributed as follows:

Chart 05 - AML instruments for exchanges, by type



Source: the authors

In the universe of binding norms, the relevance of the distinction between legislative and non-legislative norms is justified by the differences between their processes of production, which have different implications from the point of view of democratic representation theory, as discussed by Pitkin[87].

The instruments of the first group are generally produced by majority and representative institutions such as parliaments. This implies a higher level of accountability, as parliamentarians are subject to electoral incentives to act in the interests of those represented[88]. However, the electoral mechanism also reduces the credibility of the commitments made by representatives in the medium term, as their priorities may change according to political pressures.

The second group is made up of rules generally issued by independent regulatory authorities such as Central Banks and Financial Intelligence Units. On the one hand, the bureaucratic isolation that characterizes these institutions implies greater resistance to electoral pressures, which increases the credibility of their regulatory commitments[89]. On the other hand, the same isolation implies a deficit of accountability if the country's institutional system is unable to guarantee it.

Thus, normative systems with non-legislative regulation instruments, designed in the medium term and with a greater commitment to concrete results, may tend to be more effective, in the sense that the guidelines are more directly implemented. Meanwhile, systems with legislative regulatory instruments, while intended to be more durable, face greater bureaucracy and decentralization in enforcing norms, so their effectiveness may be less significant.

In other words, non-legislative regulation is more granular and more efficient (faster and more massively enforced) but is of less normative force because it is more subject to institutional review (judicial, administrative and legislative). Thus, the premise of this research is that the systems that have legislation have greater normative force since laws are not so easily questioned using the institutional way, being subject only to legislative and constitutional revision. Furthermore, it is suggested that it would be interesting to combine both regulatory strategies in order to have a solid and effective regulatory environment.

87 PITKIN, Hannah. **The concept of representation**. Berkeley, University of California Press, 1967.
88 PITKIN, Hannah. Cited, 1967.
89 MELO, Marcus André. A política da ação regulatória: responsabilização, credibilidade e delegação. **Revista Brasileira de Ciências Sociais**, São Paulo, v. 16, n. 46, p. 55-68, jun. 2001.

6.2.1.1. Legislative

This category refers to norms issued by representative and legitimate institutions for legislative production. It is generally the result of a debate that aims at prescriptive regulation in a broad and lasting manner, focusing on long-term policies.

There are ten G20 members who adopt legislation (or consolidated bills pending enactment or further regulation) on cryptocurrencies and AML measures: Australia, Italy, Germany, Japan, Mexico, Argentina, France[90], Canada[91], Russia[92] and the European Union. The latter has issued guidelines on the subject, generating an obligation for its member countries to adapt their regulatory systems to include specific AML measures for cryptocurrencies[93].

6.2.1.2. Binding non-legislative

Documents issued by institutions responsible for practical situations involving the matter, which generally deal reactively and focused on present cases, and may be changed according to the conjuncture. In this category, some instruments were binding, establishing mandatory regime and supervision and fitting in as regulations, in fact. In all, eight G20 members regulate the cryptocurrency and ALD scenario in a non-legislative manner: the United States, South Korea[94], Indonesia, South Africa, Brazil, China, India, and the United Kingdom.

90 France has only one bill, approved in its final text, which has not yet passed all legislative procedures and is pending enactment, according to the website of the French assembly. In this research, we consider your predictions because it is the final text.See: FRANÇA. Assemblee Nationale. PACTE - Projet de loi relatif à la Croissance et la Transformation des Entreprises. Texte adopté n. 258. 11 abr. 2019. Available at: <http://www.assemblee-nationale.fr/15/ta/tap0258.pdf>. Access on: 13 jun. 2019. See also: AMF - Autorité des Marchés Financiers. Dossiers Thématiques. Fintech. Vers un nouveau régime pour les crypto-actifs en France. Available at: <https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France>. Access on:13 jun. 2019.

91 Canada's legislation, although already approved in its final wording, needs further regulation to enter into force. In this research, we consider its predictions because it is the final text. See: AHMAD, Tarig. Canada: Canada Passes Law Regulating Virtual Currencies as "Money Service Businesses". **The Law Library of Congress**. Global Legal Monitor. 9 jul. 2014. Available at: <http://www.loc.gov/law/foreign-news/article/canada-canada-passes-law-regulating-virtual-currencies-as-money-service-businesses/>. Access on: 13 jun. 2019.

92 Russia has only the Digital Financial Assets Bill, which is being deliberated in the Russian House of Representatives (Duma). There is no definition of exact scope or rules yet, but there are ALD measures currently applicable to exchanges and cryptocurrency service providers as they are broadly framed in ALD law. Operations involving crypto assets are automatically considered potentially suspect by Central Bank position and the Anti-Money Laundering and Terrorist Financing Act. See: PERVUNIN, Maxim; SANGADZHIEVA,Tatiana. The Virtual Currency Regulation Review - Russia. **The Law Reviews**. nov. 2018. Available at: <https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176664/russia>. Access on: 13 jun. 2019.

93 EUROPEAN UNION. **Official Journal of the European Union**. Directive (EU) 2018/843 of the european parliament and of the council of 30 may 2018. 19 jun. 2018. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN>. Access on: 13 jun. 2019.

94 The presence of South Korea in this category considers that there was a renewal of the regulatory instrument issued by the country's financial authority, whose latest English version available online had an expiration date until January 2019. See: SOUTH KOREA. KOFIU. **Virtual currency anti-money laundering guidelines**. Available at: <https://www.kofiu.go.kr/KOFIU/english/sub05/news_view.jsp?mm=5&sm=1&srl_no=26&table=tb_hp025&tbchar=offc_anc>. Access on: 13 jun. 2019.

6.2.1.3. Recommendation

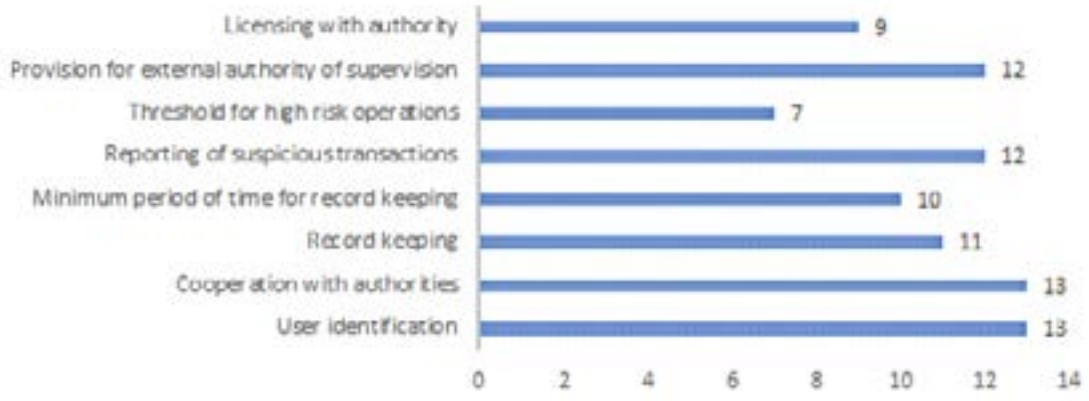
Normative systems in which there was no regulation specifically on cryptocurrencies. The documents found in these cases are purely consultative, stating intentions or advising the enterprises to adopt certain practices. In this category, it is uncertain whether or not their current money laundering laws apply to transactions involving them. Just Saudi Arabia does not have a binding instrument, relying only on a recommendation from the monetary authority[95], published in 2018, warning that cryptocurrencies are not guaranteed by any government and recommending that they were not to be used for trade operations.

Only Turkey has no regulatory or advisory provisions, whether legislative or from other institutions, regarding cryptocurrency services; This was noted in a statement from the Central Bank of Turkey about the use of these assets[96].

6.2.2. Rules and obligations

In the case of G20 members who presented regulatory instruments aimed at the AML and cryptocurrency scenario, the rules and obligations applicable in each normative system to the exchanges were observed. The presence or absence of eight regulatory requirements was verified, and their frequency is recorded in chart 06 below:

Chart 06 - Presence of AML rules in regulations



Source: the authors

The following results are the core of the present research, as they demonstrate the normative concerns effectively fulfilled by the authorities regarding these new services.

95 SAUDI ARABIAN MONETARY AUTHORITY. The standing committee for awareness on dealing in unauthorized securities activities in the foreign exchange market (forex) warns: "the virtual currencies are not regulated inside the kingdom of saudi arabia". Available at: <http://www.sama.gov.sa/en-US/News/Pages/news12082018.aspx>. Access on: 13 jun. 2019.

96 GÜÇLÜTÜRK, Osman Gazi. Current Regulatory Framework for Cryptocurrencies/Tokens in Turkey. 31 jul. 2018. Available at: <https://medium.com/@ogucluturk/current-regulatory-framework-of-cryptocurrencies-tokens-in-turkey-111bbc9dbab2>. Access on: 13 jun. 2019.

6.2.2.1. Overview of rules and obligations

Below is an overview of regulatory requirements:

Table 06 - Anti-money laundering and terrorist financing rules and obligations

	Anti-money laundering and terrorist financing rules and obligations							
G20 member	User identification	Cooperation with authorities	Record keeping	A minimum period of time for record-keeping	Reporting of suspicious transactions	The threshold for high-risk operations	Provision for the external authority of supervision	Licensing with authority
European Union	x	x	x	x	x	x	x	x
Italy	x	x	x	x	x	x	x	x
Germanu	x	x	x	x	x	x	x	x
Canada*	x	x	x	x	x	x	x	x
Japan	x	x	x	x	x	x	x	x
Australia	x	x	x	x	x		x	x
Mexico	x	x	x	x	x		x	x
France*	x	x	x	x	x		x	x
Argentina	x	x	x	x	x		x	
Russia*	x	x	x		x			
United States	x	x	x	x	x	x	x	
South Korea*	x	x			x	x	x	
Indonesia	x	x					x	x

* France, Canada, and Russia had results considering the legislation in final procedures on their respective legislative houses, and South Korea based on the assumption that the regulation with an expiration date on January 2019 was reissued and is still valid.
Source: the authors

Thirteen are the G20 members whose regulations set AML rules and obligations to exchanges: European Union, Australia, Italy, Germany, Canada, Japan, Mexico, France, Argentina, Russia, United States, South Korea, and Indonesia.

Seven G20 members are not present in this table because they have not specified in their regulations any of the AML rules and obligations according to internationally proposed standards. These are Brazil, India, South Africa, the United Kingdom, Saudi Arabia, Turkey (which has no regulation), and China, which only banned cryptocurrency services and transactions in its jurisdiction.

Most countries that do not have AML rules and obligations for exchanges can be identified as Global South countries. This may point to a tendency towards greater regulation in countries with greater economic consolidation, and further studies are needed to investigate the reasons for this regulatory gap.

The G20 members with the least regulatory compliance with AML parameters for exchanges are South Korea and Indonesia, from the list of thirteen jurisdictions with rules and obligations under review. They are the only two countries out of these thirteen that have non-legislative regulation.

When we look at the seven countries that do not have specific rules and obligations, it turns out that they also have no legislation, but less binding cryptocurrency regulations. This situation may indicate a correlation between the lower rigidity of AML rules and the restriction to normative instruments not built by a legislature elected for such a function and subject to public control and debate.

Indonesia, which regulates exchanges through a statement from the ministry of commerce, stipulates only four obligations for such services, for example. It is yet the only jurisdiction, among those that have some kind of regulation, that silences regarding the notification of suspicious transactions. On the other hand, the press release mentions the obligation to register such an undertaking before the authority, a rule which is present in only nine members of the G20.

In the case of Korea, the regulatory instrument enacted by the country's Financial Intelligence Unit does not focus directly on exchanges, but on financial corporations that engage in cryptocurrency-related financial transactions.

In addition, two of the BRICS are among the countries that do not have specific regulations for AML and exchanges: Brazil and South Africa. This may signal their engagement in the race to the bottom, potentially resorting to regulatory arbitrage, as they are investing in the acceleration of its economic growth. Meanwhile, the other three have a different approach: Russia has regulation, and China and India[97] have banned cryptocurrencies.

In general, some possibilities for the regulatory vacuum that may arise are: i) lower significance of cryptocurrency services in these jurisdictions, as they have a lower degree of industrialization; ii) view of regulation as a barrier to the establishment of these businesses, seeking to attract them by the absence of obligations; iii) lack of public knowledge about the economic possibilities presented by cryptocurrencies; iv) lack of public authority expertise to regulate the matter.

97 It should be noted, however, that there is an intense process of judicial dispute taking place as of now in India regarding the ban.

In addition, the five members that have all the standard rules and obligations in their AML exchange regulation are mostly from the Global North: European Union, Italy, Germany, Canada, Japan. Because they are jurisdictions dealing with consolidated financial institutions and industry, they may be race-to-the-top driven, that is, establishing a secure regulatory environment to control the cryptocurrency ecosystem and to appeal to businesses driven by reputation and legal certainty.

The following is a more detailed analysis of some points of the AML exchange regulatory framework, highlighting rules and obligations for their presence or absence in the G20 members' normative instruments.

6.2.2.2. User identification and cooperation with authorities

Among the members with rules and obligations, all thirteen require user identification as well as cooperation with authorities. They are the only two standards that are uniformly adopted in conjunction with other rules and obligations.

These two measures are concerned with making the flow of values involving cryptocurrencies traceable. They enable suspicious operations to be investigated and authorities to have information about them. Especially for exchanges, user identification procedures allow tracking the beneficiaries - at least immediate ones - of these transactions, as the exchange operation, involves only the customer and the service provider.

6.2.2.3. Record keeping obligation and minimum storage time

Eleven of the thirteen G20 members who have specific AML rules are required to keep records of exchanged transactions: Australia, the European Union, Italy, Germany, Canada, Japan, Mexico, France, and Argentina.

In only two countries, South Korea and Indonesia is there an obligation to keep transaction records.

The definition of minimum storage time for these records is present in 10 of the 11 countries that have a custody obligation, with Russia being the only one with a record-keeping obligation without stipulating minimum time.

The minimum record-keeping time in years ranges from five (European Union, Canada, France, Germany, and the United States), seven (Japan, Australia), and ten (Italy, Mexico). Argentina is subject to a specific regime that requires the monthly communication to the Financial Intelligence Unit (FIU) of all operations carried out with cryptocurrencies in the month.

6.2.2.4. Obligation to notify suspicious transactions and the threshold for suspicious transactions

Twelve of the thirteen G20 members with AML rules set out the obligation to report suspicious transactions. Only Indonesia does not mention this rule in the document about exchanges. This is a standard in which the risk analysis proposed by the FATF applies so that each jurisdiction assesses situations that are considered worthy of suspicion and which should be reported as such.

In this sense, one of the measures adopted is the setting of a threshold from which more care must be taken in verifying the beneficiary, his identity, and means of contact. Nine of the analyzed regulations have this value in their text, while five others - Mexico, France, Argentina, Russia, and Indonesia - do not set a threshold in their regulatory instruments to indicate suspicion of cryptocurrency transactions.

Of those with a minimum value for reporting suspicious transactions, amounts range from € 15,000 (Euro - European Union and Italy), C $ 10,000 within 24h (Canadian Dollar - Canada), ¥ 2,000,000 (Yen - Japan), U $ 2,000 (US Dollar) and ₩ 10,000,000 per day or ₩ 20,000,000 in seven days (Won - South Korea).

6.2.2.5. Provision of external supervisory authority and registration

Twelve members of the G20 point out in their AML exchange-oriented regulation that external authorities supervise the rules and risks of the cryptocurrency ecosystem. They are the European Union, Australia, Italy, Germany, Canada, Japan, Mexico, France, Argentina, United States, Indonesia, and South Korea.

In only one of the 13 jurisdictions analyzed, Russia, no provision for external supervisory authority regarding exchanges was identified. We reaffirm that the access to the rule of that country was by means of indirect documentation, in addition to being a bill pending voting and final reading, so there is still a chance that it may define the responsible authority.

Nine regulations analyzed define the obligation to register/license exchanges before an authority: the European Union, Australia, Italy, Germany, Japan, Mexico, France, Canada, and Indonesia. At this point, the correlation between the requirement of registration and framing as a financial agent is not sound, since three of them - Germany, Canada, and Indonesia - have no concept of exchange, and six of these jurisdictions - European Union, Australia, Italy, Japan, Mexico, France - present it on their regulations. Nevertheless, in the cases of Mexico and France, there is no focus on elements that would frame this service as a financial agent.

Meanwhile, four countries - Argentina, Russia, the United States, and South Korea - do not provide for registration of the exchange before the authority in their rules and obligations. This is consistent with the elements presented by these countries for conceptualizing exchanges in regulation, which move away from their framework as agents of the financial system, except for South Korea, which mentions cryptocurrency exchange activity in its financial authority's guidelines.

Members who frame exchanges as financial agents, containing some of the conceptual elements for this, however, are not unanimous in demanding the registration of this enterprise before a specific authority. Of these, only the European Union, Australia, Italy, Japan, Mexico, and France have this requirement in their regulations.

6.3. Regulatory compliance oversight

Considering the framework of rules and obligations imposed by the G20 normative instruments regarding cryptocurrency exchanges, the sanctions adopted by each normative system are presented.

In the scenario of economic and financial activities, sanctions can be considered as key elements in curbing irregularities. This is because in this context there are agents driven by efficiency and profit, so that every possible sanction is considered an opportunity cost in its operation, and may represent a disincentive to unwanted practices.

The focus of this research was the prediction of sanctions in the normative system, considering that this is a minimum requirement, although it is not ignored the relevance of a sanctioning and enforcement system for them to be effective.

Subsequent studies may examine how or in which cases these sanctions are applied, as well as their possible effect on the adoption rates of AML standards in cryptocurrency services. This research focuses on regulatory provisions that allow for oversight and action on money laundering practices. The following presents the scenario of coercive measures in relation to non-compliance with AML rules and obligations.

6.3.1. Sanctions

In order to assess which coercive measures are supported by the ALD regulation regarding cryptocurrency services, six categories of sanctions were listed: i) written warnings; ii) acquiescence orders to specific instructions; iii) fines; iv) administrative restrictions on employees; v) suspension or withdrawal of license; vi) restriction of freedom.

Sanctions can be categorized into two broad groups: the first includes those of standard enforcement, which rely on standardized enforcement and do not address a specific individual - fine and suspension or withdrawal of license; the second, consisting of sanctions whose supervision falls on specific individuals, for requiring that the conduct of someone in a particular situation be verified in order to execute and enforce them. Next is a summary table of the results found for the sanctions provided for in each regulation:

Table 07 - Types of sanction covered by each regulatory system

	Sanctions					
	Of standardized enforcement		Of supervision over specific individuals or conducts			
Jurisdiction	Fines	Suspension or withdrawal of a license	Acquiescence orders to specific instructions	Restriction of freedom	Written warnings	Administrative restrictions on employees
Australia	x	x	x	x	x	x
European Union	x	x	x		x	x
Mexico	x	x	x	x	x	
Argentina	x	x	x		x	
Germany	x	x		x		
United States	x	x	x	x	x	
France*	x	x		x		
Italy	x	x		x		
Canada*	x					x
South Korea*		x	x			
Japan			x			
Russia**	N/D	N/D	N/D	N/D	N/D	N/D
Indonesia**	N/D	N/D	N/D	N/D	N/D	N/D

* In regard to France and Canada, documents concerning bills on final procedures were considered; regarding South Korea, the text of the regulation available in English was considered, which is assumed to be still valid, even though its expiration date was January 2019, because no new document is available.
** Regarding Russia and Indonesia, the countries have, respectively, banking law and regulation, but we did not have access to the text or information about the sanctions.
Source: the authors

In the regulation of the 13 G20 members providing for AML rules and obligations for cryptocurrencies, sanctions associated with non-compliance with these rules were identified. The European Union, Australia, Mexico, and Argentina have a broader framework of sanctions, with provisions in their regulations for most enforcement measures against non-compliance with AML rules, with Australia being the only jurisdiction to provide for all modalities.

Another highlight is the Japanese regulation, which only provides for a specific supervisory sanction, which concerns orders to comply with instructions, being the only jurisdiction not to provide for standardized sanctions.

Following is a brief comment on the frequency of sanctions and their trends to be jointly foreseen.

6.3.1.1. Sanctions of standardized enforcement

With regard to how often sanctions appear in regulations, the two most common are fines and withdrawals, each being provided for in 9 jurisdictions - Australia, the European Union, Mexico, Argentina, Germany, the United States, France, and Italy provides for both, while Canada provides only for fines, South Korea only for prison and Japan provides for neither.

This is consistent with the type of subject matter that concerns economic and financial interests, as well as services that require a license to operate.

Therefore, there is a tendency to offer a sanctioning response of a pecuniary and restrictive nature of operations when the AML rules are not respected. These are also measures that do not require further specific supervision, and it is easy to check whether or not the fine was paid and whether activities for which the license would be proportionate sanctions were ceased.

6.3.1.2. Sanctions of specific supervision

Regarding the group of specific sanctions on individuals or those concerning the fulfillment of any order directed at the peculiarities of the irregular situation, the most frequently provided are acquiescence orders (provided for in 7 jurisdictions) and restriction of liberty (provided for in 6 jurisdictions), followed by written warning (provided for in 5 jurisdictions).

Interestingly, regulations that provide for one type do not necessarily provide for the other, and there is a concomitance between sanction of acquiescence order and restriction of liberty only in 3 jurisdictions - Australia, Mexico, and the United States. In the case of the acquiescence order and written warning, there is concurrency in 5 jurisdictions - Australia, European Union, Mexico, Argentina, United States.

The least frequent sanction is administrative restrictions on employees, present in only 3 jurisdictions (Australia, European Union, and Canada), not necessarily accompanied by other specific sanctions.

6.4. Discussion of results

The following are specific notes on the topics analyzed and the hypotheses they require.

6.4.1. On the conceptual approach of the regulated theme

The first aspect observed was the diversity of conceptual elements presented by the different regulations regarding the definition of cryptocurrency. The analysis was based on the identification of the scope of the regulations directed to this technology, as well as their suitability to the uses given to it.

The analysis of the results concluded that most jurisdictions whose regulation seeks to define cryptocurrencies are based on their functional characteristics, that is, what makes them similar to a currency.

On the other hand, details about the technology on which they rely, or structural elements, are less frequent in the regulatory definition of cryptocurrencies. This denotes more regulatory concerns, in fact, regarding the use of cryptocurrencies as money, especially with regard to their storage and value transfer functions. It also represents the recognition of their proximity to the dynamics of physical currencies, ie, that can be exchanged between users, without requiring an intermediary institution for operations.

Still, some jurisdictions used no more than two conceptual elements to characterize cryptocurrencies. This, coupled with the higher frequency of elements of approximation with fiat currency and their functionality, may indicate a lack of understanding of this technology. There may also be doubts by regulatory institutions in adopting too restrictive a concept, which would make regulation inapplicable to cases where it would be relevant.

6.4.2. On the character of regulation

By observing the type of regulation that is used in relation to cryptocurrencies, it was noticed diversity in the nature of regulatory instruments. Legislation has been observed in 10 or half of the jurisdictions. In the other half of the jurisdictions, existing instruments are more succinct and lack significant adherence to FATF recommendations.

It was also noted that countries with legislative instruments - and greater adherence to FATF recommendations - are mostly from the Global North.

The hypothesis that can be raised from this data is that there is a correlation between greater normative force (in the sense that there is a solid instrument, more difficult to change and with fewer instances of questioning) and greater regulatory harmonization with the standards defined by international mechanisms. control for this topic.

The existence of regulatory instruments issued by the institution that holds the legislative power, such as laws, maybe conditioning factors for a consistent and lasting protection system for transactions involving cryptocurrencies. But that does not mean that legislative instruments would be sufficient to this situation, as they may lack effective

implementation mechanisms in face of regulated services and they are dependent on efficient and equipped enforcement institutions to deal with the necessary controls.

The data collected here also allows us to consider the hypothesis that the existence of legislation makes jurisdictions more strict in the application of these rules to their recipients. In order to test this possibility, further research into local law enforcement can be conducted in each of these regulatory systems.

This research could also be complemented in the future with the comparison of compliance rates of cryptocurrency rules where there is legislation and where there is another type of regulation. Another pertinent question would be whether non-legislative regulation, when supported by legislation, is more effective than non-legislative regulation alone. This point emerges considering that technology-related issues may require some kind of expertise for effective control to be exercised, and regulatory instances based on technique rather than necessarily political representation may prove more effective in this scenario.

6.4.3. On rules and obligations

The framework of rules and obligations applicable to cryptocurrency services also has incompleteness. Some standards are more frequent, such as those concerning user identification, cooperation with authorities, record keeping and minimum time of data custody. Others are less frequent, such as the rules on reporting suspicious transactions, minimum thresholds for high-risk transactions, provision of external oversight authority, and service registration/licensing. This result points to a regulatory gap regarding cryptocurrency services, as important AML measures are outside the applicable regulatory system.

Mandatory registration is an important measure in identifying which services to monitor, and could also act as an incentive mechanism for mutual oversight. This is because regular services would be interested in maintaining competitiveness and, therefore, would have a regulatory incentive to point out irregularly/unlicensed established services.

The provision of an external authority is also key in the rules and obligations system proposed by international policies such as the FATF recommendations, as it empowers a disinterested party to verify industry compliance as such, preventing a situation of corruption or systematic wrongdoing in that environment. In this sense, the absence of this prediction in some regulations may discredit the entire control system sought with the standards.

Notification of suspicious transactions is not mandatory for exchange services in all regulated jurisdictions, nor do they all set a minimum value in the regulatory text. As a counterpoint, a potential contradiction can be argued with the FATF's own approach, which would be risk-based. In this sense, jurisdictions would be free to assess the potential risk of situations in order to set controls and checkpoints commensurate with the context presented. However, even in this understanding, it is indicated the setting of minimum values, although personalized for each jurisdiction, according to the standards identified in that context, to characterize suspicious operations and characteristics that, statistically, appear to be associated with illicit practices.

In this sense, one can refer to the hypothesis that has already ventured in the analysis of the conceptual approach to the theme. That is the possible lack of knowledge of regulators about this technology, which would underestimate the risks associated with AML. Another possibility is that this lack of expertise leads to not considering measures specifically directed to these services. Future studies could investigate whether this gap occurs because regulators are unaware of the specific risks or believe that regulation of the fiduciary value system is sufficient.

6.4.4. On sanctions

The regulations establish two types of sanctions, the most common being those whose supervision is independent of personalized measures to verify compliance, with standardized mechanisms for their measurement. Sanctions that rely on a personalized assessment of the action to be taken and also require targeted enforcement for each specific case are less frequent in regulatory systems.

Most jurisdictions that establish AML rules and obligations for exchanges also impose penalties for noncompliance. With few exceptions, sanctions include measures that are generally enforced. Thus, it can be considered that AML regulatory systems for cryptocurrencies, where they exist, generally have sufficient mechanisms to have regulatory force.

Future studies could test whether sanction prediction effectively means that it applies to cases of non-compliance by collecting information on how these punitive measures work, the institutional mechanisms for enforcing them, and how they are enforced.

7. CONCLUDING REMARKS

This research mapped the state of the art regulatory framework for cryptocurrency and money laundering services, focusing on the rules applicable to exchanges in G20 jurisdictions.

The subject of study was justified by the historical panorama supported by literature review. The origin of the Financial Action Task Force (FATF) was portrayed by the convergence of drug war and terrorism policies with anti-corruption and money laundering measures, as well as the growing governments are concerned about using cryptocurrency functionality to obscure illicit value streams.

In this sense, cryptocurrencies raise concerns associated with the topic of financial illicit since its inception, largely refractory to state monitoring of financial transactions.

It has been noted in official documents and literature on the subject that there are two common lines of concern when addressing cryptocurrencies and governance measures: i) the contribution (pseudo-anonymity and decentralization) they represent for the placement, stratification, and integration of illicit values and ii) the difficulty in regulating transactions made through its core technology, blockchain protocols. While concrete evidence of the frequency of using cryptocurrencies as a vehicle for money laundering practices is inconclusive, for regulatory purposes the risk and potential of cryptocurrencies cannot be ignored.

Mechanisms such as the FATF mutual assessments and recommendations have been producing material about the risk introduced by cryptocurrencies and recommending pertinent approaches to their control and regulation. Although there is uncertainty regarding danger, the regulatory gap increases the risks associated with such technologies.

The research started from the assumption that it is relevant and possible to establish regulation focused on the cryptocurrency environment. In order to present conclusive results, which point to good practice, and bearing in mind that the scope of influence of the main regulatory policy mechanism, the FATF, is limited to the G20 member jurisdictions, data collection has turned to this group of normative instruments, and was carried out using a structured form described in the methodological section.

For the analysis of the results, there was a focus on the rules applicable to exchanges, cryptocurrency and fiduciary currency exchange services, as they are the point of contact between the decentralized cryptocurrency system and the regulated fiat currency system, and have the potential to serve as a point of inspection for users of these assets, their origins and their flows.

The state of the art in relation to cryptocurrency and money laundering is still undefined and incomplete. It is undefined, regarding the understanding of the regulated object, since there is a diversity of concepts for both cryptocurrencies and exchange services; and it is incomplete because there is no harmonic incorporation by the G20 normative instruments of the FATF AML recommendations for cryptocurrencies.

We conclude that the regulation of the cryptocurrency environment still lacks, in the G20 jurisdictions, greater regulatory attention. Some possible obstacles pointed out are the lack of knowledge about the technology, which is difficult to conceptualize and delimit via normative text, as well as the lack of knowledge about the dimension of risks presented by it. The internationally expressed concern about the new transactional forms implemented by cryptocurrencies is very much related to their non-governmental and decentralized character, while at the same time it recognizes that it can be regulated by virtue of the growing role played by intermediaries who, to a certain extent, centralize these transactions.

Thus, there may be yet another factor that triggers greater or lesser regulatory concern, which is the actual presence of these intermediaries in the scope of regulatory action. That is, it can be considered as a hypothesis to be further explored if there is a correlation between the presence of exchanges - and even other enforceable services that deal with the transfer of values in cryptocurrencies - and the existence of ALD regulation aimed at these services. One can test whether there is a causal relationship between the two factors, and in which direction it occurs - that is, whether the absence of regulation attracts or drives away this type of enterprise, or whether the presence and market relevance of these services accelerates the process of regulation in the jurisdiction where they are established.

Considering that, although the amount of values that are processed in cryptocurrency before the financial system is under representative, some regulatory concern is recommended in order not to allow this representativeness to grow, studies should be undertaken to identify gaps and shortfalls, as well as good practices in terms of cryptocurrency regulation and money laundering.

APPENDIX A - FATF RECOMMENDATIONS AND CRITERIA FOR VERIFYING REGULATIONS

Recommendation number	Title	The regulatory topic that would indicate compliance with the recommendation
1	Assessing risks and applying a risk-based approach	1) Appointment of authority or mechanism to deal with the risks of money laundering; 2) Requiring cryptocurrency exchange and payment institutions to identify and take action to mitigate the risk of money laundering and terrorist financing
2	National coordination and cooperation	1) Having an anti-money-laundering policy; 2) identification of the responsible authority; 3) cooperation between relevant authorities to match anti-money laundering policy with data protection and privacy
6	Targeted financial sanctions related to terrorism and terrorist financing	Freezing of funds or assets as a sanction for terrorist financing under UN resolutions
8	Non-profit organizations	Legislation suitable for 1) identifying whether a terrorist organization pretends to be a legitimate entity; 2) verify that a legitimate entity is being used to prevent asset freezing measures; 3) protect against misappropriation of funds raised for purposes deemed to be legitimate for use in terrorist organizations
10	Customer due diligence	Financial Institutions should be: 1) prohibited from keeping anonymous or obviously fictitious accounts; 2) required to take DDC measures specified in the circumstances (document identification and verification regardless of customer identity, beneficiary identification and verification, understanding and obtaining business relationship information, ongoing business relationship DDC and conducted transactions ; 3) required to verify the identity of the client and the beneficiary in the circumstances of business relationships, transactions over 15,000 or wire transfers covered by the interpretative note of recommendation 16, suspicion of LD/FT, doubt about the truth or adequacy of data about the client); 4) Prohibited from opening accounts, starting business relationships, conducting transactions when unable to meet specified requirements
11	Record-keeping	Require financial (foreign exchange) institutions to store copies or records of due diligence documents, such as official identification documents, account files and business, including analysis of customers involved in unusually large transactions for at least five years after the business or after the occasional transaction date, for cooperation with competent authorities and evidence formation
14	Money or value transfer services	1) Require registration or licensing of money or money supply or transfer services; 2) mechanisms for identifying and sanctioning natural or legal persons who perform this service without a license or registration; 3) oblige these services to maintain a list of countries where they and their agents operate; 4) monitor these services

15	New technologies	Require service providers and virtual assets to be regulated and licensed or registered and subject to effective monitoring and enforcement systems
16	Wire transfers	Require financial institutions to 1) include information about senders and recipients of wire transfers and related messages and maintain it throughout the payment chain; 2) monitor wire transfers for missing information and take appropriate action 3) take freezing measures when processing wire transfers; 4) prohibit transactions with designated persons and entities in accordance with the obligations set forth in the relevant UN Security Council resolutions
20	Reporting of suspicious transactions	Require financial institutions to report directly whenever they suspect or have reasonable reason to suspect that the funds are the product of criminal activity or related to terrorist financing (regardless of the value of the transaction or just an attempt)
21	Tipping-off and confidentiality	Financial institutions, their directors, officers, and employees should be 1) protected from liability for violating information disclosure restrictions if they report in good faith their suspicions, even if they do not know exactly the criminal activity and regardless of whether it actually occurred. 2) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the Financial Intelligence Unit
22	DNFBPs: customer due diligence (CDD)	Apply the CDD and record-keeping requirements in recommendations 10, 11, 12, 15 and 17 to designated non-financial businesses and professions (DNFBPs) in the specified cases.
23	DNFBPs: Other measures	Apply the obligations set out in recommendations 18 and 21 to all designated non-financial businesses and professions (DNFBPs) specified
26	Regulation and supervision of financial institutions	It is the recommendation that recommends that mechanisms be created and that the other recommendations are being followed.
35	Sanctions	1) Are there effective sanctions against violations of recommendations 6, 8 and 23? 2) Sanctions should apply not only to financial institutions but also to their managers and senior executives.
36	International instruments	1) Countries have ratified or are in the process of ratifying the following international instruments: Vienna Convention 1988, Palermo Convention 2000, United Nations Convention Against Corruption 2003, Convention on the Financing of Terrorism, 1999. 2) If applicable, they should also be a party to regional conventions such as the Inter-American Counter-Terrorism.
37	Mutual legal assistance	Countries should not have restrictions or prohibitions on international cooperation mechanisms.
38	Mutual legal assistance: freezing and confiscation	Countries should ensure that they have mechanisms to freeze money laundering assets when required by other countries to do so, if consistent with their domestic law.

39	Extradition	Countries should execute extradition requests to prevent them from becoming havens for terrorists or money launderers. Should: 1) ensure that money laundering and terrorism are extraditable violations; 2) its extradition processes are fast and efficient; 3) not to introduce unreasonable or restrictive barriers to extradition; 4) have a suitable framework
40	Other forms of international cooperation	Countries should seek other effective forms of international cooperation in general.

APPENDIX B - FORM USED FOR GATHERING OF INFORMATION ON AML REGULATION FOR EXCHANGES

Cryptocurrency service providers

Cryptocurrency services provider: Natural or legal person engaged in provision, exchange, transfer, management and or custody of cryptocurrency, as well as in the participation and/or provision of financial services related to the emission and/or sale of cryptocurrency to or in behalf of another natural or legal person in the context of a business relation.

Specific regulatory instrument: Document that approaches explicitly the topic of cryptocurrencies, cryptoassets, virtual currencies and equivalents

1. Researcher

_____

2. Country

_____

3. Are there specific regulatory instruments concerning cryptocurrency service providers?
Check one option only

( ) Yes *After the last question in this section, go to question 8.*
( ) No *After the last question in this section, go to question 6.*
( ) Inconclusive

Observations concerning question 3:
1. Name of the instrument -> 2.Link to text -> 3. Short summary or commentary regarding the initiative. Repeat if there are more instruments.

_____
_____
_____

If there are no specific regulatory instruments

4A. Are there governmental initiatives directed towards future regulation and/or monitoring of the crypto-asset environment?
This question concerns working groups, public policies, draft legislation, amongst others

_____
_____
_____

Observations concerning question 4A:
1. Name of the initiative (If there is no specific name, describe shortly) -> 2.Links, if they exist -> 3. Short summary or commentary regarding the initiative

_____
_____
_____

If there are specific regulatory instruments

4b. Which is the highest degree of maturity of the existing specific regulatory instruments?
Legislation: highest degree of maturity, assuming that the debate that gave rise to the norm is most representative, having reached the public representatives of all society in the legislative power. Enforced, but non-legislative norm: A norm that did not emerge from a debate that included the same degree of public representation, but that nonetheless has legal mechanisms for ensuring compliance. Examples would include any regulation produced by independent regulatory institutions that effectively imposes restrictions on certain activities, subjecting violators to sanctions. Non-enforced guideline: An instrument that is neither produced by elected representatives nor legally enforced. This would include public notices, general guidelines,

position papers and other documents issued by authorities regarding cryptocurrency, such as public statements calling attention to risks of cryptocurrency.
Check one option only

( ) Legislation
( ) Enforced, non-legislative norm
( ) Non-enforced guideline

Observations concerning question 4b:
1. Name of the instrument -> 2. Link to the text -> 3. Short summary or commentary

_____
_____
_____

5. Do the existing specific regulatory instruments include which of the following definitions:
Check one option only

( ) Cryptocurrency, crypto-asset, virtual currency or equivalente
( ) Exchange service providers
( ) Cryptocurrency service providers

Observations concerning question 5
Include: 1. Definition of cryptocurrency, crypto-asset, virtual currency or equivalent given by the instrument-> 2. Definition of exchange service providers -> 3. Definition of cryptocurrency service providers -> 4. Short summary or commentary

_____
_____
_____

6. 6. Is there enforced regulation that prohibits the provision of cryptocurrency services?
Check one option only

( ) Yes
( ) Não
( ) Inconclusive

Observation concerning question 6:
1. Name of the instrument -> 2. Link to the text -> 3. Short summary or commentary

_____
_____
_____

If cryptocurrency service providers are regulated

7. Is there enforced regulation that establishes rules and restrictions to advance antimoney laundering/combating the financing of terrorism?
Check one option only

( ) Yes
( ) No
( ) Inconclusive

Observations regarding question 7:
1. Name of the instrument -> 2. Link to the text -> 3. Excerpt or mention to the legal device the establishes the restrictions -> 4. Short summary or commentary

_____
_____
_____

If the regulation establishes AML/CTF rules

8. Which of the following rules and restrictions are provided for in the regulation:
Check all that apply.

( ) Know Your Customer
( ) Recordkeeping of transactions

( ) Obligation to report suspicious transactions to authorities
( ) Obligation to be registered or licensed as service provider with authorities
( ) Minimum period of time for keeping records about transactions and/or customers
( ) Threshold value for reporting high risk transactions or operations
( ) Obligation to cooperate with authorities
( ) Provision for external authority responsible for supervising and regulating exchange service providers

Observations regarding question 8:
1. Name of the instrument -> 2. Link to the text -> 3. Excerpt or mention to the legal device the establishes the restrictions -> 4. Short summary or commentary

_____
_____
_____

9. Which of the following sanctions are provided for in case of violations:
Check all that apply.
( ) Written notices
( ) Orders to comply with specific instructions
( ) Fines
( ) Administrative restriction over employees
( ) Suspension or licence withdrawal
( ) Criminal sanctions that restrict freedom
( ) Other criminal sanctions

Observations concerning question 9:
1. Name of the instrument -> 2. Link to the text -> 3. Excerpt or mention to the legal device the establishes the restrictions -> 4. Short summary or commentary

_____
_____
_____

8. REFERENCE LIST AND BIBLIOGRAPHY

AHMAD, Tarig. Canada: Canada Passes Law Regulating Virtual Currencies as "Money Service Businesses". **The Law Library of Congress**. Global Legal Monitor. Washington, 9 jul. 2014. Available at: http://www.loc.gov/law/foreign-news/article/canada-canada-passes-law-regulating-virtual-currencies-as-money-service-businesses/. Access on: 13 jun. 2019.

AMF - Autorité des Marchés Financiers. Dossiers Thématiques. Fintech. Vers un nouveau régime pour les crypto-actifs en France. Available at: <https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France>. Access on: 13 jun. 2019.

AMICELLE, Anthony. When finance met security: Back to the War on Drugs and the problem of dirty money. **Finance and Society**, v. 3, n. 2, p. 106-123, 2017.

BLANDIN, Apolline, et al. **Global Cryptoasset Regulatory Landscape Study**. Available at SSRN. University of Cambridge: Judge Business School, 2019, p. 36. Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf. Access on: 18 jul. 2019.

BRASIL. Banco Central do Brasil. **Comunicado nº 31.379, de 16 de novembro de 2017**. Available at: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=31379. Access on: 23 aug. 2019.

CAMPBELL-VERDUYN, Malcolm. Bitcoin, crypto-coins, and global anti-money laundering governance. **Crime, Law and Social Change**, v. 69, n. 2, 283–305, mar. 2018. p. 286.

CARNEY, Mark. FSB Chair's letter to G20 Finance Ministers and Central Bank Governors. **Financial Stability Board**, 18 mar. 2018. Available at: http://www.fsb.org/wp-content/uploads/P180318.pdf. Acess on 15 set. 2018.

CHOHAN, Usman W. Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability. **SSRN Electronic Journal**, [s.l.], p.1-6, 2017.

CLAEYS, Grégory; DEMERTZIS, Maria; EFSTATHIOU, Konstantinos. Cryptocurrencies and monetary policy. **Monetary Dialogue**, Bruxelas, jul. 2018.

COBHAM, Alex; JANSKÝ, Petr; MEINZER, Markus. The Financial Secrecy Index: Shedding New Light on the Geography of Secrecy. **Economic Geography**, v. 91, n. 3, p. 281-303, jul. 2015.

CORÉIA DO SUL. KOFIU. **Virtual currency anti-money laundering guidelines**. Available at: <https://www.kofiu.go.kr/KOFIU/english/sub05/news_view.jsp?mm=5&sm=1&srl_no=26&table=tb_hp025&tbchar=offc_anc>. Access on: 13 jun. 2019.

CORRÊA, Luiz Maria Pio. **O Grupo de Ação Financeira Internacional (GAFI)**: organizações internacionais e crime transnacional. Brasília: FUNAG, 2013.

CRYPTOUK. **Code of conducts**. [S. I.]. Available at: http://www.cryptocurrenciesuk.info/code-of-conducts/. Acess on 19 may 2019.

DEL CASTILLO, M. The 'great Bitcoin exodus' has totally changed New York's Bitcoin ecosystem. **New York Business Journal**, New York, 12 ago. 2015. Available at: https://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html. Acess on 21 may 2019.

DIGITAL ASSET TRANSFER AUTHORITY. **Anti-Money Laundering Guidelines**. 01 jul. 2015. Available at: https://www.slideshare.net/DataSecretariat/data-aml-guidelines-june-2015. Acess on 19 may 2019.

ESTADOS UNIDOS DA AMÉRICA (EUA). THE LAW LIBRARY OF CONGRESS. Global Legal Research Directorate. **Regulation of Cryptocurrency Around the World**. Washington, jun. 2018a. Available at: https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf. Acess on 21 may 2019.

ESTADOS UNIDOS DA AMÉRICA (EUA). THE LAW LIBRARY OF CONGRESS. Global Legal Research Directorate. **Regulation of Cryptocurrency in Selected Jurisdictions**: Argentina, Australia, Belarus, Brazil, Canada, China, France, Gibraltar, Iran, Israel, Japan, Jersey, Mexico, Switzerland. Washington, jun. 2018b. Available at: https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf. Access on: 13 jun. 2019.

FORBES. **The World's largest public companies**. 2019 ranking. Available at: https://www.forbes.com/global2000/list/#tab:overall. Access on: 09 aug. 2019

FORBES. **The World's largest public companies**. 2019 ranking: Major banks. Available at: https://www.forbes.com/global2000/list/#industry:Major%20Banks. Access on: 09 aug. 2019

FRANÇA. Assemblee Nationale. PACTE - Projet de loi relatif à la Croissance et la Transformation des Entreprises. Texte adopté n. 258. 11 abr. 2019. Available at: http://www.assemblee-nationale.fr/15/ta/tap0258.pdf. Access on: 13 jun. 2019

G20. **About G20.** Available at: http://g20.org.tr/about-g20/. Access on: 19 jun. 2019.

G20. **Communiqué**. Finance Ministers & Central Bank Governors 19-20 March 2018, Buenos Aires, Argentina. 2018. Available at: https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf. Access on: 15 sep. 2018.

G20. **G20 Finance Ministers & Central Banks Governors Meeting**. Buenos Aires, 23 jul. 2018. Available at: http://www.g20.utoronto.ca/2018/2018-07-22-finance-en.pdf. Acess on 21 may 2018.

G20. **What is the G20 summit?** Available at: https://g20.org/en/summit/about/. Access on: 19 jun. 2019.

GOLDBERG, Dror. Legal Tender. **SSRN Electronic Journal**, [s.l.], p.1-17, 2008.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **FATF Report to G20 Finance**

Ministers and Central Bank Governors Meeting. Abr. 2019. Available at: www.fatf-gafi.org/media/fatf/documents/G20-April-2019.pdf. Acess on 23 mai. 2019

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Frequently Asked Questions**. Available at: http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223. Access on: 15/01/2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services**. Jun. 2013. Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf. Acess on 21 may 2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Guidance for a Risk-Based Approach to Virtual Currencies -** Convertible Virtual Currency Exchangers. Jun. 2015. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Acess on 21 may 2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**. Jun. 2019. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. Acess on 23 jun. 2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). International standards on combating money laundering and the financing of terrorism & proliferation. **The FATF Recommendations**, Paris. Available at: <http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf>, 2012. Access on: 14 may 2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Money Laundering Using New Payment Methods**. Out. 2010. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf. Acess on 21 may 2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Mutual evaluations**. Available at: http://www.fatf-gafi.org/publications/mutualevaluations/. Access on: 13 jun. 2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Public Statement - Mitigating Risks from Virtual Assets**. GAFI, Paris, 22 fev. 2019. Available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html Assunto em: 26 may 2019.

GRUPO DE AÇÃO FINANCEIRA INTERNACIONAL (GAFI). **Virtual Currencies** - Key Definitions and Potential AML/CFT Risks. Jun. 2014. Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. Access on: 21 may 2019.

GÜÇLÜTÜRK, Osman Gazi. Current Regulatory Framework for Cryptocurrencies/ Tokens in Turkey. 31 jul. 2018. Available at: https://medium.com/@ogucluturk/current-regulatory-framework-of-cryptocurrencies-tokens-in-turkey-111bbc9dbab2. Access on: 13 jun. 2019.

HELGESSON, Karin Svedberg; MÖRTH, Ulrika. Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention. **Crime, Law and Social Change**, v. 69, n. 2, p. 227–248, may 2018.

HELLEINER, Eric. The Politics of Global Financial Reregulation: Lessons from the Fight against Money Laundering. **Center for Economic Policy Analysis**. Working Paper, n. 15, apr. 2000.

HOUBEN, Robby; SNYERS, Alexander. **Cryptocurrencies and blockchain** - legal context and implications for financial crime, money laundering and tax evasion. European Union: Policy Department for Economic, Scientific and Quality of Life Policies, July 2018. p. 76-79.

HÜLSSE, Rainer. Creating Demand for Global Governance: The Making of a Global Money-laundering problem. **Global Society**, v. 21, n. 2, p. 155-178, apr. 2007.

JAPÃO. **Comunicado da Financial Services Authority**. 24 out. 2018. Available at: https://www.fsa.go.jp/news/30/virtual_currency/20181024-1.html. Acess on 19 may 2019

LEVI, Michael; REUTER, Peter. Money Laundering. **Crime and Justice**, v. 34, p. 289-375, 2006. p. 296-305.

MELO, Marcus André. A política da ação regulatória: responsabilização, credibilidade e delegação. **Revista Brasileira de Ciências Sociais**, São Paulo, v. 16, n. 46, p. 55-68, jun. 2001.

NAÇÕES UNIDAS. Escritório das Nações Unidas sobre Drogas e Crime. **Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies**. jun. 2014. Available at: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Access on: 21 may 2019.

NAÇÕES UNIDAS. UNODOC helps tackle bitcoin banking fraud and money laundering. **Escritório das Nações Unidas sobre Drogas e Crime**, Viena, 01 fev. 2017. Available at: https://www.unodc.org/unodc/en/frontpage/2017/February/unodc-helps-tackle-bitcoin-banking-fraud-and-money-laundering.html. Acess on 21 may 2019.

NANCE, Mark T. The regime that FATF built: an introduction to the Financial Action Task Force. **Crime, Law and Social Change**, v. 69, n. 2, 109–129, mar. 2018.

PAGLIERY, Jose. **Bitcoin and the future of Money**. Chicago: Triumph Books, 2014.

PERVUNIN, Maxim; SANGADZHIEVA,Tatiana. The Virtual Currency Regulation Review - Russia. **The Law Reviews**. noV. 2018. Available at: https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176664/russia. Access on: 13 jun. 2019.

PITKIN, Hannah. **The concept of representation**. Berkeley, University of California Press, 1967.

RAMOS, Leonardo; VADELL, Javier; SAGGIORO, Ana; FERNANDES, Marcia. A Governança econômica global e os desafios do G-20 pós-crise financeira: análise das posições de

Estados Unidos, China, Alemanha e Brasil. **Revista Brasileira de Política Internacional**, v. 55, n. 2, p. 10-27, 2012.

ROMERO, Thiago Giovani. **Lavagem de capitais e cooperação jurídica internacional**: a contribuição do GAFI. 2017. 158f. Dissertação (Mestrado em Direito) - Universidade Estadual Paulista "Júlia de Mesquita Filho", Franca.

ROSE, Cecily. **International anti-corruption norms** - their creation and influence on domestic legal systems. 1 ed. Oxford: Oxford University Press, 2015.

SAUDI ARABIAN MONETARY AUTHORITY. The standing committee for awareness on dealing in unauthorized securities activities in the foreign exchange market (forex) warns: "the virtual currencies are not regulated inside the kingdom of saudi arabia". Available at: http://www.sama.gov.sa/en-US/News/Pages/news12082018.aspx. Access on: 13 jun. 2019.

SINGH, Kevin. New wild west: preventing money laundering in the Bitcoin network. **Northwestern Journal of Technology and Intellectual Property**, v. 13, n. 1, 38–64.

SWARTZ, Lana. What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. **Cultural Studies**, v. 32, n. 4, jan. 2018.

TRANSPARENCY INTERNATIONAL. **G20 leaders or laggards**? Reviewing G20 promises on ending anonymous companies. 2018. Available at: https://www.transparency.org/whatwedo/publication/g20_leaders_or_laggards

UNIÃO EUROPEIA. **Official Journal of the European Union**. Directive (EU) 2018/843 of the european parliament and of the council of 30 may 2018. 19 jun. 2018. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN. Access on: 13 jun. 2019.

UNIÃO EUROPEIA. Serviço Europeu de Polícia. Europol – INTERPOL Cybercrime Conference makes the case for greater multisector cooperation. **Europol Newsroom**, [s. l.], 02. out. 2015. Available at: https://www.europol.europa.eu/newsroom/news/europol-%E2%80%93-interpol-cybercrime-conference-makes-case-for-greater-multisector-cooperation. Acess on 21 may 2019.

UNITED NATIONS. Development Policy and Analysis Division. Department of Economic and Social Affairs. Global Issues: Challenges of cryptocurrencies for policymakers. **Monthly Briefing on the World Economic Situation and Prospects**, nº 108, pp. 1-2, 13 nov. 2017.

UNITED NATIONS. Escritório das Nações Unidas sobre Drogas e Crime. **Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies**. jun. 2014. Available at: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Access on: 21 may 2019.

UNITED NATIONS. UNODOC helps tackle bitcoin banking fraud and money laundering. **Escritório das Nações Unidas sobre Drogas e Crime**, Viena, 01 fev. 2017. Available at: https://www.unodc.org/unodc/en/frontpage/2017/February/unodc-helps-tackle-

bitcoin-banking-fraud-and-money-laundering.html. Acess on 21 may 2019.

VIANA, André Rego; BARROS, Pedro Silva; CALIXTRE, André Bojikian. **Governança global e integração da América do Sul**. Brasília: Ipea, 2011.

WIKIPEDIA. **Token**. Available at: https://en.wikipedia.org/wiki/Token. Access on: 09 aug. 2019.