UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS CONTÁBEIS

JAIME WAGNER RODRIGUES BARBOSA

PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: uma abordagem baseada em risco para a profissão contábil

RIO DE JANEIRO
2023

JAIME WAGNER RODRIGUES BARBOSA

PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: uma abordagem baseada em risco para a profissão contábil

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciências Contábeis, Faculdade de Administração e Ciências Contábeis, Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Ciências Contábeis.

Orientador: Prof. Dr. Pierre Ohayon

Rio de Janeiro

2023

FICHA CATALOGRÁFICA

B238p Barbosa, Jaime Wagner Rodrigues

Prevenção e combate ao crime de utilização de criptoativos na lavagem de dinheiro: uma abordagem baseada em risco para a profissão contábil / Jaime Wagner Rodrigues Barbosa. - 2023.

220 f.; 31 cm.

Orientador: Pierre Ohayon.

Dissertação (mestrado) – Universidade Federal do Rio de Janeiro, Faculdade de Administração e Ciências Contábeis, Programa de Pós-Graduação em Ciências Contábeis, 2023.

Bibliografia: f. 153-176.

1. Lavagem de dinheiro. 2. Criptomoeda. 3. Crime. I. Ohayon, Pierre, orient. II. Universidade Federal do Rio de Janeiro. Faculdade de Administração e Ciências Contábeis. III. Título.

CDD 341.559

Ficha catalográfica elaborada pelo bibliotecário: Priscila Gonçalves Soares CRB 7 – 7061

Biblioteca Eugênio Gudin/CCJE/UFRJ

JAIME WAGNER RODRIGUES BARBOSA

PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: uma abordagem baseada em risco para a profissão contábil

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciências Contábeis, Faculdade de Administração e Ciências Contábeis, Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Ciências Contábeis.

Aprovado em 28 de março de 2023.

_____

Pierre Ohayon, Dr. (PPGCC/FACC/UFRJ)

_____

José Augusto Veiga da Costa Marques, Dr. (PPGCC/FACC/UFRJ)

_____

Francisco José dos Santos Alves, Dr. (PPGCC/FAF/UERJ)

Dedico este trabalho ao Prof. Dr. Claudio Ulysses Ferreira Coelho (*in memoriam*).

Aos meus pais João (*in memoriam*) e Areli, e à minha irmã Queila.

AGRADECIMENTOS

Agradeço a Deus, meu refúgio e fortaleza.

À minha mãe Areli, que depois de Deus, foi onde encontrei maior apoio e encorajamento para manter-me firme no propósito de concluir minha pesquisa de dissertação.

À minha irmã Queila e aos meus amigos Vania e Lennin, pelo incentivo para continuar a caminhada rumo a conclusão deste trabalho.

Deixo meus agradecimentos a dois grandes amigos que tive a felicidade de conhecer durante a graduação do curso de Ciências Contábeis na FAF/UERJ, Diego e Michael, e à professora da FAF/UERJ, Profa. Viviane Miranda Silva do Nascimento. Pessoas que influenciaram diretamente na minha decisão em participar do processo seletivo deste mestrado. Dois amigos, com que compartilhei minhas angústias diante dos desafios apresentados no mestrado, e as alegrias quando da superação desses desafios.

Ao meu prezado orientador Prof. Dr. Pierre Ohayon pela confiança ao acolher o tema da minha dissertação, conduzindo a orientação deste trabalho com muita seriedade e generosidade. Pelos ensinamentos e contribuições durante o processo de desenvolvimento desta pesquisa.

Agradeço ao Prof. Dr. Claudio Ulysses Ferreira Coelho (*in memoriam*), pelas contribuições realizadas na banca de qualificação deste trabalho.

Aos professores componentes da banca de defesa deste trabalho, Prof. Dr. José Augusto Veiga da Costa Marques e Prof. Dr. Francisco José dos Santos Alves.

Aos demais Professores Drs. do PPGCC-UFRJ, por todo conhecimento compartilhado durante o curso. E, também, a todos os funcionários da secretaria do PPGCC-UFRJ.

Aos meus colegas de turma, cujas conversas e trocas de experiências me ajudaram nessa trajetória, em especial aos colegas mais chegados Sheila, Eduardo e Vagner.

Agradeço aos profissionais que dedicaram seu tempo e conhecimento para que este trabalho se tornasse possível, em particular Lucas Carrara e Telmo Navarro Junior, pelas reuniões trazendo importantes contribuições para a versão final do questionário e seleção de possíveis participantes da pesquisa. Aos participantes da pesquisa, que concederam as informações necessárias para a realização deste trabalho, tanto os que participaram da realização do pré-teste do questionário, como os que responderam aos questionários.

Por fim, agradeço a todos que de alguma forma contribuíram para a realização deste trabalho. Muito obrigado!

RESUMO

BARBOSA, Jaime Wagner Rodrigues. **Prevenção e Combate ao Crime de Utilização de Criptoativos na Lavagem de Dinheiro**: uma abordagem baseada em risco para a profissão contábil. Rio de Janeiro, 2023. Dissertação (Mestrado em Ciências Contábeis) – Faculdade de Administração e Ciências Contábeis, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2023.

Os serviços desenvolvidos para o mercado de criptoativos, cuja operação traz maior liquidez com diferentes pontos de interseção entre o ambiente virtual e o ambiente físico, estão introduzindo uma nova realidade com muitos desafios e ameaças, como a inovação na prática de lavagem de dinheiro (LD), por meio da utilização de criptoativos. Considerando a necessidade de prevenção e combate à lavagem de dinheiro (PCLD), este estudo tem como objetivo identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na LD. O presente estudo é classificado como documental, com uma abordagem de natureza qualitativa e de caráter exploratório e descritivo, a partir de uma análise de conteúdo e documental. Foram analisados diferentes documentos de domínio público, referentes às políticas, estratégias e ações dos agentes nacionais e internacionais acerca das questões decorrentes do uso dos criptoativos, em particular as criptomoedas, no crime de LD. Essa análise permitiu: (i) Elaborar um questionário, que foi aplicado junto a 62 profissionais com experiência na prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT) e experiência com criptoativos; e (ii) Verificar as orientações sobre a contabilização de transações envolvendo criptomoedas. Ao analisar as percepções dos respondentes sobre as assertivas apresentadas no questionário, conclui-se que, de forma geral, os respondentes entendem que todas as assertivas relacionadas aos riscos e desafios de crime de LD enfrentados ao lidar com criptoativos apresentam: (i) significante nível de ocorrência; e (ii) significante nível de relevância. Conclusão semelhante obteve-se em relação às assertivas relacionadas às possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos, que apresentam: (i) significante nível de relevância; e (ii) significante nível de eficácia. Quanto ao tratamento contábil aplicado aos criptoativos, evidenciou-se que a natureza das criptomoedas atende à definição de um ativo intangível conforme CPC 04 (R1) – Ativo Intangível, sendo o CPC 16 (R1) – Estoques aplicados às criptomoedas quando mantidas para venda no curso normal dos negócios. Além das assertivas presentes no questionário, que estão diretamente relacionadas

aos elementos de uma abordagem baseada em risco (ABR), por meio da análise dos comentários deixados pelos respondentes, emergiram temas que reforçam a implementação de uma ABR para *anti-money laundering* e combate ao financiamento do terrorismo (AML/CFT) por parte dos profissionais que venham se envolver em atividades relacionadas com as criptomoedas. Esses achados justificam a possibilidade de seguir uma ABR para a profissão contábil no tocante ao uso das criptomoedas no crime de LD, uma vez que se faz necessário que os profissionais da contabilidade identifiquem, avaliem e entendam os riscos de LD com criptoativos a que estão expostos, para a aplicação de medidas necessárias de PLD-FT. Sendo possível concluir que o profissional da contabilidade pode desempenhar um papel de agente na prevenção e combate aos crimes relacionados à utilização dos criptoativos na LD, ao aplicar uma ABR para AML/CFT quando se envolver em atividades de criptomoedas ou fornecer produtos e serviços relacionados às criptomoedas.

Palavras-chave: Lavagem de dinheiro; Criptoativos; Responsabilidade do contador; ABR; PLD-FT.

ABSTRACT

BARBOSA, Jaime Wagner Rodrigues. **Prevenção e Combate ao Crime de Utilização de Criptoativos na Lavagem de Dinheiro**: uma abordagem baseada em risco para a profissão contábil. Rio de Janeiro, 2023. Dissertação (Mestrado em Ciências Contábeis) – Faculdade de Administração e Ciências Contábeis, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2023.

The services developed for the crypto market, whose operation brings greater liquidity with different points of intersection between the virtual environment and the physical environment, are introducing a new reality with many challenges and threats, such as innovation in the practice of money laundering (ML), through the use of cryptoassets. Considering the need to prevent and combat money laundering (PCML), this study aims to identify possible approaches that help the accounting professional in preventing and combating crimes related to the use of crypto assets in ML. The present study is classified as documentary, with a qualitative approach and exploratory and descriptive character, based on a content and documentary analysis. Different documents in the public domain were analyzed, referring to the policies, strategies, and actions of national and international agents regarding issues arising from the use of cryptoassets, in particular cryptocurrencies, in the crime of ML. This analysis allowed: (i) Preparing a questionnaire, which was applied to 62 professionals with experience in preventing money laundering and terrorist financing (PML-FT) and experience with crypto assets; and (ii) Review guidance on accounting for transactions involving cryptocurrencies. By analyzing the respondents' perceptions about the assertions presented in the questionnaire, it is concluded that, in general, the respondents understand that all the assertions related to the risks and challenges of ML crime faced when dealing with crypto-assets present: (i) significant level occurrence; and (ii) significant level of relevance. A similar conclusion was obtained in relation to the assertions related to possible approaches that would help to minimize the risks and challenges faced when dealing with crypto assets, which present: (i) significant level of relevance; and (ii) significance level of efficacy. As for the accounting treatment applied to cryptoassets, it was shown that the nature of cryptocurrencies meets the definition of an intangible asset according to CPC 04 (R1) – Intangible Assets, with CPC 16 (R1) – Inventories applied to cryptocurrencies when held for sale in the ordinary course of business. In addition to the assertions present in the questionnaire, which are directly related to the elements of a risk-based approach (RBA), through the analysis of the comments left by the respondents, themes

emerged that reinforce the implementation of an RBA for *anti-money laundering and combating financing of terrorism* (AML/CFT) by professionals who become involved in activities related to cryptocurrencies. These findings justify the possibility of following an RBA for the accounting profession regarding the use of cryptocurrencies in the crime of ML, since it is necessary for accounting professionals to identify, assess and understand the risks of ML with cryptoassets to which they are exposed, for the application of necessary PML-FT measures. It is possible to conclude that the accounting professional can play an agent role in preventing and combating crimes related to the use of crypto assets in the ML, by applying an RBA for AML/CFT when engaging in cryptocurrency activities or providing products and services related to cryptocurrencies. cryptocurrencies.

Keywords: Money laundering; Cryptoassets; Accountant's responsibility; RBA; PML-FT.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AASB	*Australian Accounting Standards Board*
ABCripto	Associação Brasileira de Criptoeconomia
ABR	Abordagem Baseada em Risco
ACFE	*Association of Certified Fraud Examiners*
AML	*Anti-Money Laundering*
ANBIMA	Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais
ANR	Avaliação Nacional de Riscos
APJERJ	Associação dos Peritos Judiciais do Estado do Rio de Janeiro
APNFDs	Atividades e Profissões não Financeiras Designadas
ATM	*Automated Teller Machine*
ASBJ	*Accounting Standards Board of Japan*
AV	Ativo Virtual
BCB	Banco Central do Brasil
BI	*Business Intelligence*
BTC	*Bitcoin*
CCS	Cadastro de Clientes do Sistema Financeiro Nacional
CDD	*Customer Due Diligence*
CEP	Comitê de Ética em Pesquisa
CEPC	Código de Ética Profissional do Contador
CFC	Conselho Federal de Contabilidade
CFT	*Combating Financing of Terrorism*
CGAI	Coordenação-Geral de Articulação Institucional
CGCCO	Coordenação Geral de Combate ao Crime Organizado
CGR	Comitê de Gestão de Riscos
CGRP	Central de Gerenciamento de Riscos e Prioridades
CNAE	Classificação Nacional de Atividades Econômicas
COAF	Conselho de Controle de Atividades Financeiras
CONCLA	Comissão Nacional de Classificação
CPA	*Certified Public Accountant*
CPC	Comitê de Pronunciamento Contábil
CRC	Conselho Regional de Contabilidade

CRC-RJ	Conselho Regional de Contabilidade do Estado do Rio de Janeiro
CTIF-CFI	*Belgian Financial Intelligence Processing Unit*
CVM	Comissão de Valores Mobiliários
DASH	*Dash*
DLT	*Distributed Ledger Technology*
DRCI	Departamento de Recuperação de Ativos e Cooperação Internacional
EAR	Entidade Autorreguladora
E-Digital	Estratégia Brasileira para a Transformação Digital
ENCCLA	Estratégia Nacional de Combate à Corrupção e Lavagem de Dinheiro
ETH	*Ethereum*
EY	*Ernst & Young*
FAC	*Financial Conduct Authority*
FAQ	*Frequently Asked Questions*
FATF	*Financial Action Task Force*
FEBRABAN	Federação Brasileira de Bancos
FENACON	Federação Nacional das Empresas de Serviços Contábeis e das Empresas de Assessoramento, Perícias, Informações e Pesquisas
FINCEN	*Financial Crimes Enforcement Network*
FINTRAC	*Financial Transactions and Reports Analysis Centre of Canada*
FSB	*Financial Stability Board*
FT	Financiamento do Terrorismo
FTP	Financiamento do Terrorismo e da Proliferação
GAFI	Grupo de Ação Financeira Internacional
GGI	Gabinete de Gestão Integrada
GIABA	Grupo InterGovernamental de Acção contra o Branqueamento de Capitais na África Ocidental
IAASB	*International Auditing and Assurance Standards Board*
IASB	*International Accounting Standards Board*
IBGE	Instituto Brasileiro de Geografia e Estatística
IBRACON	Instituto dos Auditores Independentes do Brasil
ICAEW	*Institute of Chartered Accountants in England and Wales*
ICCE	Instituto de Criminalista Carlos Éboni
ICO	*Initial Coin Offering*

IESBA	*International Ethics Standards Board for Accountants*
IF	Instituição Financeira
IFAC	*International Federation of Accountants*
IFRIC	IFRS *Interpretations Committee*
IFRS	*International Financial Reporting Standard*
IOSCO	*International Organization of Securities Commissions*
IoT	*Internet of Things*
IP	*Internet Protocol*
IPC	Índice de Percepção da Corrupção
IPO	*Initial Public Offering*
ISA	*International Standard of Auditing*
KYC	*Know Your Customer*
LD	Lavagem de Dinheiro
LTC	*Litecoin*
MCTI	Ministério da Ciência, Tecnologia e Inovações
MJSP	Ministério da Justiça e Segurança Pública
MPF	Ministério Público Federal
MP-RJ	Ministério Público do Estado do Rio de Janeiro
NBC	Norma Brasileira de Contabilidade
NIC	Normas Internacionais de Contabilidade
NIR	Nota Interpretativa da Recomendação
NYSDFS	*New York State Department of Financial Services*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PAS	Processo Administrativo Sancionador
PCLD	Prevenção e Combate à Lavagem de Dinheiro
PEP	Pessoa Exposta Politicamente
PF	Polícia Federal
PIB	Produto Interno Bruto
PLD	Prevenção à Lavagem de Dinheiro
PLD-FT	Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo
PME	Pequena e Média Empresa
PNLD	Programa Nacional de Capacitação e Treinamento no Combate à Corrupção e à Lavagem de Dinheiro

PNUD	Programa das Nações Unidas para o Desenvolvimento
PPGCC	Programa de Pós-Graduação em Ciências Contábeis
PSAV	Provedor de Serviços de Ativos Virtuais
P2P	*Peer-to-Peer*
RCLE	Registro de Consentimento Livre e Esclarecido
Rede-LAB	Rede Nacional de Laboratórios contra Lavagem de Dinheiro
RFB	Receita Federal do Brasil
RIF	Relatórios de Inteligência Financeira
RTS	Relatório de Transação Suspeita
SAR	*Suspicious Activity Report*
SENAJUS	Secretaria Nacional de Justiça
SEOPI	Secretaria de Operações Integradas
SESCON	Sindicato das Empresas de Serviços Contábeis, Assessoramento, Perícias, Informações e Pesquisa do Estado do Rio de Janeiro
SIMBA	Sistema de Movimentação Bancária
SIN	Superintendência de Supervisão de Investidores Institucionais
SNBA	Sistema Nacional de Bens Apreendidos
Sox	*Sarbanes Oxley Act*
TI	Tecnologia da Informação
UFRJ	Universidade Federal do Rio de Janeiro
UNCTAD	*United Nations Conference on Trade and Development*
UIF	Unidade de Inteligência Financeira
UNIPEC-RJ	União dos Profissionais e Escritórios de Contabilidade do Estado do Rio de Janeiro
UNODC	*United Nations Office on Drugs and Crime*
VACG	*Virtual Asset Contact Group*
XMR	*Monero*
XRP	*Ripple*
ZEC	*Zcash*

SUMÁRIO

1 INTRODUÇÃO

O surgimento da Internet trouxe um aumento na circulação e na velocidade do acesso às informações de diversas naturezas. A comunicação entre indivíduos tomou dimensões globais sem precedentes, possibilitando maior facilidade nas relações pessoais, profissionais e comerciais, o que provocou muitas mudanças nos hábitos e práticas nas culturas envolvidas. Para Castells (2003, Abertura) "a Internet passou a ser a base tecnológica para a forma organizacional da Era da Informação: a rede". Tal fato é confirmado por Chadwick citado por Lucero (2011, p. 35) em sua definição da Internet:

> *A Internet é uma rede de redes de tecnologias de informação e comunicação nos níveis global, nacional, local, um-a-um, um-a-muitos, muitos-a-muitos, com padrões e protocolos relativamente abertos e barreiras de entrada comparativamente baixas* (CHADWICK, 2006, *apud* LUCERO, 2011, p. 35, grifo do autor).

A Internet não é uma entidade única, mas uma reunião de redes que operam de maneira relativamente descentralizada, mas conectadas entre si, permitindo a comunicação de muitos com muitos, em escala global, com aumento de transações comerciais, movimentações financeiras e prestações de serviços públicos em meio virtual, tornando as barreiras de entrada cada vez mais tênues (CASTELLS, 2003; LUCERO, 2011; MCTI, 2018).

Nesse ambiente global criado pela Internet, novos modelos de negócios tornam-se viáveis, com capacidade de se desenvolverem organicamente com inovação, sistemas de produção de produtos e prestação de serviços e demanda de mercado (CASTELLS, 2003; LUCERO, 2011). Nele, se modela uma nova revolução industrial baseada em dados, computação e automação, onde atividades humanas e processos industriais passaram a ser aprimorados, criados e recriados com base em volume de dados em escala antes inexistentes (MCTI, 2018). Essa afirmação é ratificada pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, em inglês):

> Com mais dispositivos acessando a Internet, um número cada vez maior de pessoas usando serviços digitais e mais cadeias de valor conectadas digitalmente, o papel dos dados e tecnologias digitais está definido para expandir ainda mais (UNCTAD, 2019, p. 3, tradução nossa).[1]

Por meio dessas transformações surgiu a economia digital, com as tecnologias digitais, como plataformas digitais, aplicativos móveis e serviços de pagamento, que sustentando suas transações, a torna cada vez mais inseparável do funcionamento da economia como um todo.

[1] "With more devices accessing the Internet, an ever-increasing number of people using digital services and more value chains being digitally connected, the role of digital data and technologies is set to expand further".

Sua evolução está associada ao progresso em várias tecnologias de fronteira, como a tecnologia *blockchain*, impressão tridimensional (3D), internet das coisas (IoT), banda larga móvel 5G, computação em nuvem e análise de dados (UNCTAD, 2019).

Os novos modelos de negócios desenvolvidos na economia digital podem trazer contribuições significativas para um sistema financeiro mais eficiente e melhorar a inclusão financeira, mas também podem contribuir para o surgimento de novos riscos. Weeks-Brown (2018) explica que as transações financeiras na economia digital, apesar de terem usos legítimos e produtivos, também podem ser usadas para ocultar ou facilitar atividades criminosas.

Essas questões representam desafios para estruturas regulatórias e de supervisão financeira. António Guterres, Secretário-Geral das Nações Unidas, explica que a cooperação entre Governos, sociedade civil, academia, comunidade científica e indústria de tecnologia é essencial para o desenvolvimento de novas soluções (UNCTAD, 2019, p. iv). Mukhisa Kituyi, Secretário-Geral da UNCTAD, esclarece que há mais perguntas do que respostas sobre como tratar esses novos desafios, dado ao ritmo acelerado das mudanças tecnológicas, e que os tomadores de decisão enfrentam um "alvo em movimento" ao tentarem adotar políticas sólidas a respeito da economia digital (UNCTAD, 2019, p. v).

1.1 CONTEXTO

Os crimes financeiros envolvendo fraudes, corrupção e lavagem de dinheiro (LD), trazem prejuízos econômicos e sociais, que denigrem a reputação de um país e expõe seu povo aos mais variados crimes. Impedem o crescimento sustentável e inclusivo. Provocam graves efeitos negativos na economia, diminuindo os recursos disponíveis para fins produtivos como a construção de estradas, escolas e hospitais. Além de provocarem o aumento nas taxas de emigração de mão de obra qualificada, especialmente nos países em desenvolvimento (WEEKS-BROWN, 2018; SCHANEIDER, 2018).

As Nações Unidas estimaram recentemente que o produto do crime da prática de LD atinge aproximadamente 2% a 5% do Produto Interno Bruto (PIB) global, ou US$ 800 bilhões a US$ 4 trilhões por ano (UNODC, 2018). O estudo realizado pela Associação de Examinadores Certificados de Fraudes (ACFE, em inglês), evidenciou que 2.504 casos de fraude em 125 países causaram perdas totais de aproximadamente US$ 3,6 bilhões anuais, representando cerca de 5% das receitas das organizações, sendo a corrupção o esquema mais comum em todas as regiões (ACFE, 2020). Segundo a Transparência Internacional, a corrupção ainda é um dos maiores obstáculos ao desenvolvimento econômico e social no Brasil, que mantém 35 pontos

no Índice de Percepção da Corrupção (IPC), seguindo estagnado em sua menor pontuação desde 2012 (TRANSPARÊNCIA INTERNACIONAL, 2020). Esse índice que é elaborado desde 1995 pela Transparência Internacional avalia 180 países e territórios em uma escala de 0 a 100 (quanto mais próximo de zero, mais corrupto é o país).

Para Kratcoski e Maximilian (2018) o conceito de fraude é amplamente definido como sendo qualquer ato deliberado cometido com o objetivo de obter um ganho ilegal, sendo a corrupção definida como o uso indevido de poder para obter uma vantagem ilegal, podendo ser encontrada em organização ou grupo que tenha alguma forma de estrutura de poder.

Segundo Jung (2007), o termo "lavagem de dinheiro" é utilizado genericamente, tanto no Brasil quanto no exterior, para designar uma operação cujo objetivo é introduzir ou reintroduzir na cadeia econômica valores que se originaram de atividades ilícitas. Conforme Chaikin (2008), as práticas de corrupção e de LD ocorrem simultaneamente, pois as receitas geradas pela corrupção precisam ser ocultadas por meio do processo de LD. A prática de corrupção se tornou um elemento chave na obtenção de vantagens oportunistas em determinadas situações, sendo o crime mais comum em todas as regiões do mundo, tendo fortes impactos no desenvolvimento econômico e social (ARAÚJO, 2014; MARAGNO; KNUPP; BORBA, 2019).

Vás e Sales (2015) explicam que a existência da prática de LD dá-se pela tentativa de justificar os lucros obtidos por meio de atos ilícitos, como tráfico de drogas, crimes contra a ordem tributária, crimes contra o sistema financeiro, crimes contra a Administração Pública e outros que resultam em expressivos retornos financeiros. Jung (2007) expõe que grande parte dessas práticas ilícitas envolvem, em alguma das suas etapas, de forma ativa ou passiva, organizações empresariais, organizações da sociedade civil sem fins lucrativos ou organizações do poder público, individualmente ou em consórcio.

No Brasil há uma legislação específica para o assunto, a Lei nº 9.613 de 1998, conhecida como a "Lei de Lavagem de Dinheiro", primeiro dispositivo legal que tipifica o crime de LD no Brasil. Seu artigo 9º define como um dos sujeitos submetidos às medidas de prevenção à lavagem de dinheiro (PLD), as pessoas físicas ou jurídicas que prestem, mesmo que eventualmente, serviços de assessoria, consultoria, contadoria, auditoria, aconselhamento ou assistência, de qualquer natureza, em operações que possam resultar em práticas de LD (BRASIL, 1998). Dessa forma, foram atribuídas responsabilidades aos profissionais da contabilidade para uma participação mais efetiva na prevenção e acompanhamento de qualquer atividade que possa estar relacionada a esse crime.

Em 2017, o Conselho Federal de Contabilidade (CFC) editou a Resolução CFC nº 1.530, que "Dispõe sobre os procedimentos a serem observados pelos profissionais e organizações contábeis para cumprimento das obrigações previstas na Lei nº 9.613 de 1998 e alterações posteriores", reforçando ainda mais a responsabilidade do profissional da contabilidade sobre a prevenção e combate ao crime de LD (CFC, 2017).

Dentro desse contexto, o profissional da contabilidade deve estar sempre atualizado sobre o surgimento de novas práticas de crimes contra a sociedade, como os crimes de corrupção, LD, financiamento do terrorismo e armas de destruição em massa, tráfico de crianças, dentre outros crimes. O Conselho Internacional de Padrões Éticos para Contadores (IESBA, em inglês) orienta o profissional da contabilidade de qualquer área de atuação a informar as autoridades competentes quaisquer suspeitas ou descobertas de irregularidades, descumprimento de leis ou regulamentos envolvendo casos de fraude, corrupção, LD, entre outras, demonstrando mais um avanço efetivo na direção do *compliance* e da transparência no universo corporativo e no setor público, tudo em favor do interesse público (IFAC, 2016).

1.2 PROBLEMA DE PESQUISA

Para as Nações Unidas, o rápido desenvolvimento em informações financeiras, tecnológicas e comunicação tornou a tarefa de combate à prática de LD mais urgente, uma vez que o dinheiro pode ser movimentado para qualquer lugar do mundo com maior rapidez e facilidade (UNODC, 2018). Sallaberry *et al*. (2020), explicam que esse desenvolvimento tem dificultado a detecção e monitoramento de atividades ilícitas, tanto para órgãos de controle, como para as empresas que optam em realizar suas atividades negociais de forma lícita e transparente.

Nesse sentido, têm-se os serviços desenvolvidos para o mercado de criptoativos. Esses serviços, segundo a Estratégia Nacional de Combate à Corrupção e Lavagem de Dinheiro (ENCCLA), são qualquer solução técnica, como aplicativo, sistema ou rede, desenvolvida para circulação e liquidez desse ativo virtual (ENCCLA, 2017a). A operação desses serviços pode ocorrer por meios de *exchanges*, instituições financeiras (IFs); cartões de crédito e pagamento; provedores de remessas de dinheiro; caixas eletrônicos (ATMs, em inglês), como os ATMs *Bitcoin*, que suportam tanto moedas fiduciárias como criptoativos; comércio, tanto nas lojas físicas, como no *e-commerce*, nos *sites* de transações *peer-to-peer* (P2P), de transferências, entre outros, que juntos, ajudam configurar novas formas de transferência de riqueza (FATF, 2015; KEATINGE; CARLISLE; KEEN, 2018).

A estrutura do mercado de criptoativos, em especial das criptomoedas, está firmada na política de descentralização, com a eliminação ou redução do papel de um ou mais intermediários ou processos centralizados tradicionalmente presentes nas prestações de serviços financeiros. A ausência de regulamentação específica e controle do Estado ou qualquer outra instituição particular, onde o livre comércio é a premissa de sua existência, traz grande preocupação para os Governos. O uso criminoso desse mercado tem trazido grandes problemas para a sociedade de forma geral, como a integridade do investidor e do mercado, LD e instabilidade financeira. Havendo também, o uso lícito desse mercado, trazendo grandes benefícios para essa mesma sociedade, como a universalização de serviços financeiros e a redução de custos em transações financeiras (BOFF; FERREIRA, 2016; FSB, 2018, 2019a, 2020; POSKRIAKOV; CHIRIAEVA; CAVIN, 2019).

O mercado de criptoativos está introduzindo uma nova realidade repleta de desafios, e com muitas ameaças, como a inovação na prática de LD, por meio da utilização de criptoativos.

Considerando a necessidade de prevenção e combate ao crime de lavagem de dinheiro, este estudo busca elucidar a seguinte questão: **Como o profissional da contabilidade pode desempenhar um papel de agente na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro**?

Para Silva (2007, p. 28), os diferentes crimes financeiros revelam a importância do sistema de controle da qual a contabilidade faz parte, "*seja pela análise e registro dos fatos administrativos primários ou pela relevância das informações produzidas e relatadas por intermédio das Demonstrações Contábeis e dos relatórios específicos*".

Vincent e Wilkins (2020) explicam que os criminosos muitas vezes procuram os serviços de consultores profissionais inconscientes, como os profissionais da contabilidade, para ocultar a atividade criminosa das autoridades policiais e adicionar uma fachada de legitimidade ao produto do crime.

A esse respeito o Grupo de Ação Financeira Internacional (GAFI) explica que os esquemas montados para a ocultação de bens ocorrem de alguma forma com a participação de especialistas e profissionais intermediários, seja de modo intencional, seja por negligência, resultado do pouco, ou nenhum conhecimento do negócio em que está prestando assessoria. Aponta também que o profissional da contabilidade, devido à sua perspicácia financeira e facilidade de identificar atividades financeiras suspeitas, não está vulnerável à exploração involuntária para facilitar esses esquemas. Contudo, os profissionais da contabilidade devem identificar e entender os riscos de LD a que estão expostos e tomar as medidas necessárias de

prevenção e combate à lavagem de dinheiro (PCLD), mitigando e gerenciando os riscos, para evitar o auxílio a criminosos ou facilitar atividades criminosas (FATF, 2018a, 2019a).

1.3 OBJETIVO GERAL

O objetivo geral do presente estudo é identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro.

1.4 OBJETIVOS ESPECÍFICOS

a) Identificar possíveis aplicações dos criptoativos nos crimes de lavagem de dinheiro;

b) Verificar como as partes interessadas (instituições e atores) na prevenção e combate à lavagem de dinheiro estão tentando coibir a utilização dos criptoativos na prática desse crime; e

c) Verificar o tratamento contábil aplicado aos criptoativos.

1.5 JUSTIFICATIVA

Tendo em vista que se passou mais de uma década desde o lançamento em 2008 da criptomoeda *bitcoin* no mundo e da sua tecnologia subjacente, a tecnologia *blockchain*, indústrias, negócios, empresários e Governos em todo o mundo estão trabalhando para entender seus impactos e desenvolverem aplicativos que aproveitem ao máximo os benefícios desta tecnologia. Muitas organizações estão desenvolvendo práticas em tecnologia *blockchain* e criptoativos, tornando-se líderes de pensamento sobre seus funcionamentos e estão trabalhando em direção a soluções que afetarão todos os aspectos da vida moderna, desde a "tokenização", por meio da digitalização, à custódia de criptoativos, o uso da tecnologia *blockchain* na prática legal, a regulamentação governamental.

Mas surgiram outros interessados em entender como essa tecnologia poderia ser usada para o desenvolvimento de atividades ilícitas, como a LD. Esse risco tem gerado preocupação por parte de Governos e organismos internacionais, que na tentativa de coibir esse crime, estão tentando criar medidas regulatórias sobre o mercado de criptoativos. Relatórios e orientações para as organizações e profissionais que podem ser afetados por esse crime também estão sendo elaborados.

Os criptoativos estão em contínua evolução, e as expectativas e experiências de partes interessadas podem mudar de acordo. Portanto, perguntas, exemplos, desafios, riscos, considerações e procedimentos potenciais devem ser considerados. Profissionais da contabilidade, auditores e responsáveis pela governança precisam ficar a par dos desenvolvimentos dos criptoativos e considerar as implicações desses desenvolvimentos.

Nesse sentido, a inovação na prática de LD, por meio da utilização de criptoativos, deve ser considerada por profissionais da contabilidade, auditores e responsáveis pela governança, justificando, assim, a realização da presente pesquisa.

A relevância do estudo encontra-se na atualidade, ambiguidade e falta de orientação oficial em torno das transações de criptoativos, e na possibilidade de trazer às teorias, práticas e políticas existentes um debate mais aprofundado sobre os dilemas na prevenção e combate ao crime de LD.

Pesquisas anteriores abordaram as questões decorrentes dos criptoativos como instrumento no crime de LD sob as lentes do Direito. Silveira (2020) analisou as possíveis respostas penais a respeito da questão envolvendo a dimensão criminal do uso das criptomoedas nos crimes de evasão de divisas, sonegação fiscal e LD. Assim como Estellita (2020), que estudou a hipótese do uso dos criptoativos no incremento do risco de LD. Grupenmacher (2019) tratou das plataformas de criptoativos pelo viés da proteção do investidor e de políticas voltadas para a prevenção à lavagem de dinheiro (PLD), enquanto Telles (2018) estudou o Sistema *Bitcoin* e a sua utilização na prática do crime de LD.

Possíveis abordagens regulatórias foram tratadas por Rodrigues e Kurtz (2019), que buscaram mapear a regulamentação de combate à LD em relação as *exchanges* de criptomoedas, nas jurisdições que compõem o G20. Sendo tratadas, também, por Dupuis e Gleason (2020), que descreveram as oportunidades e limitações das criptomoedas como ferramenta de LD por meio de seis “portas abertas” (mecanismos de câmbio) disponíveis, vinculando o paradigma dialético regulatório para conhecer o seu cliente e as técnicas de evasão à LD.

Tendo como objeto de estudo as instituições financeiras (IFs), Sharma (2020), em sua pesquisa, procurou compreender os desafios que os bancos enfrentam ao lidar com transações de LD relacionadas às criptomoedas.

Em pesquisas sobre tratamentos contábeis e auditoria dos criptoativos, Marques (2019) estudou os possíveis modelos de tratamento contábil para o reconhecimento e mensuração das criptomoedas, enquanto Vincent e Wilkins (2020) desenvolveram um modelo para auxiliar os auditores nas decisões de aceitação e continuidade do cliente e identificar os riscos de

criptomoeda que devem ser considerados durante o planejamento de auditoria e a coleta de evidências de auditoria. Smith (2018) também desenvolveu um guia e itens a serem considerados pelos *Certified Public Accountants* (CPAs) no auxílio na prevenção de fraudes relacionadas a criptomoedas.

O presente estudo avança na pesquisa sobre a prevenção e combate ao crime de utilização de criptoativos na lavagem de dinheiro (LD) sob as lentes da Contabilidade, ao examinar as abordagens regulatórias e de supervisão para os criptoativos e aplicar questionários junto aos profissionais com experiência na prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT) e experiência com criptoativos, com a finalidade de seguir uma abordagem baseada em risco (ABR) para a profissão contábil.

2 REFERENCIAL TEÓRICO

Neste capítulo é realizada uma revisão de literatura e são abordadas as bases teóricas que sustentam o estudo proposto. Aqui se procura conhecer o "estado da arte" referente às moedas virtuais, *tokens* digitais, criptoativos, ao crime de LD, à responsabilidade do contador, à abordagem baseada em risco (ABR) e às criptomoedas e a LD.

2.1 MOEDAS VIRTUAIS

Para uma melhor compreensão dos criptoativos, a definição de moedas virtuais torna-se necessária, pois o domínio dos termos mais básico facilita a realização do estudo.

As moedas virtuais estão diretamente relacionadas com as moedas digitais, que para Bible *et al*. (2017) podem ser definidas como uma forma de moeda baseada na Internet ou meio de troca com propriedades semelhantes às moedas físicas, permitindo a realização de transações instantâneas e transferências de propriedades sem fronteiras.

A moeda virtual é um exemplo de moeda digital, conforme explica o GAFI:

> **Moeda digital** pode significar uma representação digital de qualquer moeda virtual (não-fiduciária) ou moeda eletrônica (fiduciária) e, portanto, é muitas vezes usada de forma intercambiável com o termo 'moeda virtual' (FATF, 2014, p. 4, grifo do autor, tradução nossa).[2]

Comumente o termo moeda digital é muitas vezes confundido com o de moeda virtual, trazendo certa confusão para quem deseja entender o que realmente vem a ser uma moeda virtual. Assim, como o equívoco de ter como sinônimos a moeda virtual e a moeda eletrônica, uma vez que ambas são consideradas uma espécie moeda digital (gênero), mas guardam características que as diferenciam entre si:

> Ela [moeda virtual] é distinta da **moeda eletrônica**, que é uma representação digital da moeda fiduciária utilizada para transferir eletronicamente o valor denominado em moeda fiduciária. A moeda eletrônica é um mecanismo de transferência digital para moeda fiduciária – ou seja, ela transfere eletronicamente o valor com status de curso legal (FATF, 2014, p. 4, grifo do autor, tradução nossa).[3]

---

[2] "**Digital currency** can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency". In this paper to avoid confusion, only the terms "virtual currency" or "e-money" are used."

[3] "It is distinct from **e-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency - i.e., it electronically transfers value that has legal tender status."

A representação digital de uma moeda fiduciária com *status* de curso legal é uma característica da moeda eletrônica que a diferencia da moeda virtual, que é definida pelo GAFI:

> **Moeda virtual** é uma representação digital de valor que pode ser negociada digitalmente e funciona como (1) um meio de troca; e/ou (2) uma unidade de conta; e/ou (3) uma reserva de valor, mas não tem curso legal (ou seja, quando ofertada a um credor, é uma oferta válida e legal de pagamento) em qualquer jurisdição. Não é emitida nem garantida por qualquer jurisdição, e cumpre as funções acima apenas por acordo dentro da comunidade de usuários da moeda virtual. A moeda virtual se distingue da moeda fiduciária (também conhecida como **"moeda real"**, **"dinheiro real"** ou **"moeda nacional"**), que é a moeda e o papel-moeda de um país que é designado como sua moeda legal; circular; e é habitualmente utilizada e aceita como um meio de troca no país emissor. (FATF, 2014, p. 4, grifo do autor, tradução nossa).[4]

Uma "representação digital" é uma representação de algo na forma de dados digitais, que só terá funcionalidade quando vinculado digitalmente, via Internet, a um sistema monetário virtual. No caso das moedas virtuais, os dados digitais são as próprias moedas virtuais, não o meio no qual os dados virtuais são armazenados.

As diferenças entre moedas eletrônicas e moedas virtuais podem ser observadas no **Quadro 1**, que apresenta a moeda virtual como uma espécie de moeda digital e a sua distinção em relação à moeda eletrônica.

As moedas virtuais podem ser classificadas conforme a **conversibilidade** ou a **forma de emissão**. Conforme a conversibilidade, uma moeda virtual pode ser: **conversível**, quando existe uma garantia de sua conversão em alguma moeda soberana ou qualquer ativo com valor de revenda e liquidez razoavelmente previsível; ou **não conversível**, quando não existe um mecanismo específico e regular que ofereça liquidez para a sua troca (ENCCLA, 2017a).

Quanto à forma de emissão, uma moeda virtual pode ser: **centralizada**, quando possui um único controlador para todo o seu sistema, estabelecendo a governança da moeda, emitindo-a ou retirando-a de circulação, além de manter o registro de transações de pagamentos; ou **não centralizada** (descentralizada), quando não possuem autoridade administradora central (ENCCLA, 2017a). Böhme *et al.* (2015) sinalizam, como uma das vantagens da descentralização, a possibilidade de se evitar um ponto central de falha em um sistema de computador.

---

[4] "**Virtual currency** is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. **"real currency," "real money,"** or **"national currency"**), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country."

Quadro 1 – Comparação entre Moedas Eletrônicas e Moedas Virtuais

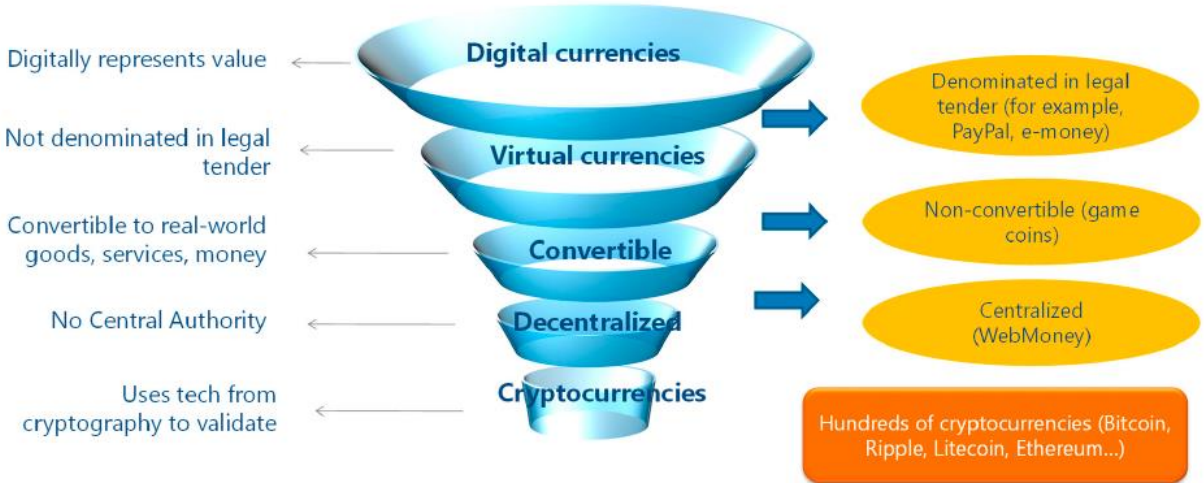
Quadro comparativo entre moedas eletrônicas e moedas virtuais	**Moedas eletrônicas**	**Moedas Virtuais**	
		Centralizadas	**Distribuídas (criptomoedas)**
Formato do dinheiro	Digital.	Digital.	Digital.
Unidade de conta	Moeda soberana.	Determinada por entes privados.	Definida por algoritmo e preço de mercado.
Aceitação	De acordo com os padrões de aceitação das moedas soberanas que representam.	Associadas a utilização para descontos e gratuidades na aquisição de produtos ou serviços específicos, tais como bilhetes aéreos e jogos de computador.	Puramente fiduciária. Depende exclusivamente da confiança dos usuários da sua aceitação futura como meio de pagamento.
Status legal	Regulada.	Não-regulada.	Não-regulada.
Emissor	Instituições de moedas eletrônicas instituídas em conformidade com os padrões do sistema financeiro local.	Agentes privados não regulados.	Agentes privados não regulados e não personificados.
Fornecimento do dinheiro	Regras dependem das decisões do governo emissor ou com jurisdição sobre o espaço legal da moeda. Sua oferta está geralmente associada à existência de um lastro em moeda de banco central no caso de instituições não-financeiras e a lastro em moedas de bancos comerciais por instituições financeiras.	Decisões dependem do emissor privado.	Definido por algoritmos preestabelecidos no sistema de seu livro distribuído.
Possibilidade de resgate de fundos	Geralmente os governos garantem a sua convertibilidade pelo valor nominal em moeda física ou depósitos bancários no mesmo padrão monetário.	Não há nenhuma garantia de conversibilidade para nenhuma moeda.	Geralmente não há nenhuma garantia de conversibilidade para nenhuma moeda, embora a liquidez entre criptomoedas e moedas soberanas tenha apresentado aumento crescente.

Fonte: ENCCLA (2017a, p. 8).

O GAFI afirma que todas as moedas virtuais não conversíveis são centralizadas, pois são emitidas por uma autoridade central que estabelece regras tornando-as não conversível, e que as moedas virtuais conversíveis podem ser centralizadas ou descentralizadas (FAFT, 2014).

Na **Figura 1**, encontra-se um esquema de classificação das moedas virtuais onde moedas digitais, como *PayPal* e *e-money*, que são moedas eletrônicas, são reconhecidas como uma representação digital de valor, e as moedas virtuais não são reconhecidas como representante legal de uma moeda soberana.

Figura 1 – Taxonomia de moedas virtuais



Fonte: He *et al*. (2016, p. 8).

A **Figura 1** demonstra, também, os aspectos de conversibilidade e descentralização da moeda virtual, que pode ser conversível para bens, serviços e dinheiro do mundo real sem o domínio de uma autoridade central, caso contrário das *game coins* que não são conversíveis e da *WebMoney* que é controlada por uma autoridade central.

Aponta, ainda, para as criptomoedas que se utilizam da tecnologia de criptografia para validar suas transações, como *Bitcoin* (BTC), *Ripple* (XRP), *Litecoin* (LTC), *Ethereum* (ETH), etc.

Assim, os aspectos de uma criptomoeda são: ser uma moeda digital, virtual, conversível, descentralizada e criptograficamente validada em suas transações.

2.2 *TOKENS* DIGITAIS

Blandin *et al.* (2019) definem *token* digital como uma sequência de caracteres que constitui uma representação protegida por criptografia de um conjunto de direitos que podem ser usados em um contexto específico. Uma representação digital de um interesse, que pode ser de valor, um direito de receber um benefício ou executar funções específicas ou pode não ter um propósito ou uso especificado (FSB, 2018).

Segundo Nascimento *et al*. (2019), a possibilidade do uso dos *tokens* digitais para representar não somente um meio de pagamento, mas também, para serem associados a uma promessa genérica de pagamento ou entrega de qualquer outra mercadoria ou serviço, levou ao surgimento de "*tokens* digitais", geralmente referidos como "*tokens*", como uma nova classe de produtos financeiros e um novo modelo de intermediação financeira. A tecnologia *blockchain* e a tecnologia de registro distribuído (DLT, em inglês)[5] permitem o desenvolvimento de ativos nativamente digitais (ativos que só existem em formato digital dentro dos limites do sistema de emissão), assim como a tokenização de ativos existentes (representação digital de ativos, incluindo direitos, mantidos em outro lugar), que podem ser transferidos através das fronteiras organizacionais, por meio dessas mesmas tecnologias (BLANDIN *et al*., 2019).

Nesse contexto, Klayman, Cohen e Sosnow (2017) explicam o que são *tokens* digitais:

> [...] os *tokens* digitais não são mais nem menos do que entradas numeradas em um livro razão eletrônico baseado em *blockchain.* Esses lançamentos contábeis podem, de fato, ser estruturados para se parecerem com "títulos" tradicionais - representando promessas de pagamento de valores no futuro, propriedade ou outros interesses em uma entidade etc. No entanto, os *tokens* digitais também podem representar unidades de valor, o que pode torná-los mais parecidos com *commodities*; podem funcionar como registros de propriedade ou recibos de depósito; eles podem conferir aos proprietários o direito de usar um sistema de *software*, o que os torna mais parecidos com licenças. Alguns *tokens* digitais simplesmente podem representar pontos de dados em uma estrutura de dados maior. Isso é o que muitos advogados e outros querem dizer quando alertam que não existe um tipo único, nem um conjunto de categorias claras, de *tokens* digitais. Há uma enorme flexibilidade em como estruturar os *tokens* digitais e o que esses *tokens* digitais podem representar (Tradução nossa).[6]

---

[5] *Distributed Ledger Technology* (DLT) ou "Tecnologia de Registro Distribuído" (tradução livre) é uma tecnologia que possibilita salvar informações por meio de um razão distribuído, ou seja, uma cópia digital repetida de dados disponíveis em vários locais (FSB, 2018).

[6] "[...] digital tokens are no more or less than numbered entries on a blockchain-based electronic ledger. These ledger entries may indeed be structured to look very much like traditional "securities" – representing promises to pay amounts in the future, ownership, or other interests in an entity, etc. However, digital tokens can also represent units of value, which may make them look more like commodities; they can function as property records or warehouse receipts; they can entitle owners to the right to use a software system, which makes them look more like licenses. Some digital tokens simply may represent data points in a larger data structure. This is what many lawyers and others mean when they caution that there is no single type, nor set of clear categories, of digital tokens. There is tremendous flexibility in how to structure digital tokens and what those digital tokens may represent."

Os *tokens* digitais possuem diversos significados e funções. Um *token* digital pode, em vários momentos e às vezes ao mesmo tempo, representar uma propriedade, uma *commodity*, dinheiro ou um título. No acesso prévio a um serviço ou na compra de um *software* de computador, após a instalação, pode ser solicitado do cliente a digitação de uma chave de licença, geralmente uma sequência de letras ou números. Na identificação de propriedade pessoal, como uma joia preciosa ou autenticação de um documento legal, é especificado uma sequência de números que corresponde aos mesmos. Em um modelo próximo às ações, uma pessoa que possui uma série de números emitidos por uma empresa ou projeto pode ter o direito de receber um valor monetário ou uma participação percentual especificada nos retornos econômicos da empresa ou do projeto, ou o direito de votar em determinadas atividades ou desenvolvimentos da empresa ou projeto.

Nesse sentido, o Instituto de Contadores Públicos da Inglaterra e do País de Gales (ICAEW, em inglês), apresenta duas subcategorias principais de *token* digitais: (i) s*ecurity token* ou "tokens de segurança" na tradução livre, concebidos como investimento, com características associadas aos instrumentos financeiros tradicionais; (ii) *utility/access token* ou "tokens de utilidade/acesso" na tradução livre, concebidos como direito de acesso a um produto ou serviço fornecido por uma organização ou negócio específico. Apontando, ainda, uma terceira categoria de *token* digital, conhecida como *token* de pagamento ou de troca, geralmente associado às criptomoedas (ICAEW, 2019).

2.3 CRIPTOATIVOS

Não há uma definição única para os criptoativos, variando significativamente em cada país e contexto, pois ainda se encontram em fase inicial de desenvolvimento e num acelerado processo de mudanças.

Os criptoativos podem ser definidos como uma representação digital de valor ou direito contratual, protegida por criptografia e mantida em sistema de registro distribuído, suscetível de custódia, transferência e negociação eletrônica (FCA, 2019).

A Comissão de Valores Mobiliários (CVM) conceitua os criptoativos como "ativos virtuais, protegidos por criptografia, presentes exclusivamente em registros digitais, cujas operações são executadas e armazenadas em uma rede de computadores" (CVM, 2018a).

A Instrução Normativa de Nº 1.888 de 2019, da Receita Federal do Brasil, define criptoativos como:

> [...] a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal (RFB, 2019, Art. 5º, inciso I).

Essa definição é semelhante à proposta por Dinenzon *et al*. (2018), quando da representação digital de valor, possibilitada pelos avanços na criptografia e na DLT, denominadas em sua própria unidade de conta, podendo ser transferida ponto a ponto (P2P) sem intermediários. Sendo definidos, ainda, como um tipo de ativo privado que depende principalmente de criptografia e contabilidade distribuída ou tecnologia similar como parte de seu valor percebido ou inerente (FSB, 2018).

A maior parte dos projetos relacionados aos criptoativos é lançada no mercado por meio da *Initial Coin Offering* (ICO) ou "Oferta Inicial de Moedas" na tradução livre. Comparadas às Ofertas Públicas Iniciais (IPOs, em inglês), nas ICOs, os *tokens* emitidos representam interesses econômicos no negócio de emissão, como ações ordinárias. As ICOs permitem que as empresas financiem seus empreendimentos por meio de pré-vendas, ou vendas em massa, desses criptoativos para o público. O público tem acesso as informações a respeito do projeto de desenvolvimento do criptoativo por meio de um "*white paper*"[7] publicado pelo responsável do projeto (DANIEL; GREEN, 2018; ZHANG *et al*., 2019). De acordo com o ICAEW (2019), os criptoativos abrangem todos os ativos desenvolvidos em um registro distribuídos, incluindo todas as criptomoedas, e os ativos não monetários, como os s*ecurity token* e *utility/access token*. No presente estudo, será tratado somente das criptomoedas. Essa escolha justifica-se pelo fato de as criptomoedas apresentarem maior risco de LD.

2.3.1 **Criptomoedas**

Criptomoedas, como *bitcoin* (BTC) e *éter* (ETH), unidades de moeda utilizadas pelos Protocolos *Bitcoin* e *Ethereum*, estão entre os primeiros e mais conhecidos exemplos de criptoativos, mas o espaço continua a crescer e evoluir, com novos tipos de ativos comumente chamados de *tokens* (DANIEL; GREEN, 2018). Para Giudici, Milne e Vinogradov (2020), as criptomoedas podem ser vistas como um criptoativo com transferências de valor digital *peer-to-peer* (P2P), sem envolver instituições terceirizadas para fins de certificação de transações.

---

[7] É no "*white paper*" que geralmente são apresentados os detalhes técnicos da funcionalidade dos *tokens* e onde são explicadas as propostas de valor do sistema que eles sustentam (DANIEL; GREEN, 2018, p. 5).

A criptomoeda BTC surgiu no ano de 2008, por meio da publicação do *white paper* "*Bitcoin: A Peer-to-Peer Electronic Cash System*", cujo autor mantém o pseudônimo de Satoshi Nakamoto (NAKAMOTO, 2008). Sua criação deu início a revolução dos criptoativos, levando ao surgimento de muitas outras criptomoedas conhecidas como "*altcoins"*[8], cujos exemplo são: *Monero* (XMR), *Dash* (DASH), *Zcash* (ZEC), *Litecoin* (LTC), dentre muitas outras.

Conforme visto anteriormente, uma criptomoeda guarda os seguintes aspectos: é uma moeda digital, virtual, conversível, descentralizada e criptograficamente validada em suas transações, sendo classificada como um *token* de pagamento ou de troca.

Sua tecnologia subjacente é a tecnologia *blockchain*. Uma forma de DLT, que permite o envolvimento de várias partes em transações seguras e confiáveis sem qualquer intermediário (UNCTAD, 2019). Uma tecnologia que permite registrar informações através de um registro distribuído, possibilitando que os nós[9] de uma rede proponham, validem e registrem alterações de estado (ou atualizações) de forma consistente entre os nós da rede (FSB, 2019a). É um livro digital descentralizado que armazena, conecta e verifica informações usando blocos gerados por muitos computadores. Zhang *et al*. (2019), explicam que enquanto um livro razão típico é mantido de forma centralizada em um local físico ou banco de dados, acessível por profissionais da contabilidade em uma organização, existe um livro razão digital descentralizado, com cópias das transações realizadas mantidas por todos os participantes de uma rede *blockchain*. A tecnologia *blockchain* é uma forma de livro razão distribuído em que os detalhes das transações são mantidos no livro razão na forma de blocos de informações. Um bloco de novas informações é anexado à cadeia de blocos pré-existentes por meio de um processo computadorizado pelo qual as transações são validadas (FSB, 2018).

As transações com as criptomoedas ocorrem nas plataformas de negociação, que são mercados bilaterais/multifacetados com uma infraestrutura *online* que suporta trocas entre várias partes diferentes (UNCTAD, 2019). Esse ambiente de negociação pode se desenvolver por meio de *exchanges*[10], instituições financeiras (IFs); cartões de crédito e pagamento; provedores de remessas de dinheiro; caixas eletrônicos (ATMs *Bitcoin*) que suportam tanto moedas fiduciárias como criptoativos; comércio, tanto nas lojas físicas, como no *e-commerce*, nos *sites* de transações *peer-to-peer* (P2P), de transferências, entre outros.

---

[8] *Altcoin* é o termo utilizado para descrever as criptomoedas alternativas ao *Bitcoin*.
[9] Qualquer participante de uma rede que possua as características necessárias para acessar a rede e enviar ou validar transações nela, conforme sua capacidade (definida no protocolo da rede) (ENCCLA, 2017a, p. 6).
[10] São prestadores de serviços de câmbio entre criptoativos, *tokens* e moedas fiduciárias (ICAEW, 2019).

Para que essas transações ocorram, os usuários devem possuir uma carteira eletrônica de criptomoeda (*e-wallet*), um instrumento ou um meio de aplicação de *software* para armazenar e transferir criptomoedas. Uma *e-wallet* é definida pela ENCCLA (2017a, p. 6) como "um serviço de administração de dados de terceiros que, em geral, inclui a guarda de chaves privadas do usuário de moedas virtuais e faz a publicação de transações desse usuário nos registros distribuídos da moeda". Conforme Keatinge, Carlisle e Keen (2018, p. 12), uma *e-wallet* representa as "chaves privadas" dos usuários, que são, em essência, senhas usadas para assinar transações correspondentes aos endereços públicos de criptomoedas de um usuário que aparecem na *blockchain*. No mercado de criptoativos, há uma variedade de serviços de *e-wallet* disponíveis para criptomoedas, cujas mais comuns estão presentes no **Quadro 2**.

Quadro 2 – *E-wallets* disponíveis para criptomoedas

Carteira de criptomoedas (*e-wallet*)	**Serviços oferecidos**
Carteiras de hardware (hardware wallet)	Permitem que os usuários armazenem chaves *offline* em dispositivos físicos, como *pen drives*.
Carteiras de software (software wallet)	Aplicativos que podem ser instalados em um *desktop* ou dispositivo móvel, permitindo o armazenamento seguro de chaves privadas no dispositivo.
Carteiras hospedadas/custodiadas (hosted/custodial wallets)	São mantidas na *Web* e oferecidas por meio de *sites* de provedores de serviços terceirizados, como *exchanges* de criptomoedas. Esses serviços são "custodiados", onde o provedor da carteira retém o acesso às chaves privadas dos usuários.
Carteiras híbridas (hybrid wallets)	Semelhante as carteiras hospedadas/custodiadas, mas os provedores dessas carteiras não têm acesso às chaves privadas dos usuários.
Carteiras com várias assinaturas (multi-signature wallets)	Fornecem segurança apropriada, exigindo que várias chaves sejam usadas para autorizar uma transação, reduzindo o risco de roubo quando uma única chave privada for comprometida.

Fonte: Keatinge, Carlisle e Keen (2018, p. 14).

Uma carteira de criptomoeda, ainda pode ser *cold storage*, que se refere a *e-wallet offline*, ou seja, uma carteira que não está conectada à Internet, ou *hot storage*, que se refere a uma *e-wallet online*, ou seja, uma carteira que está conectada à Internet.

As entidades que fornecem carteiras de criptomoedas, os provedores de carteira (*wallet providers*), ajudam no aumento da liquidez dos criptoativos, permitindo os usuários, *exchanges* e comerciantes realizarem mais facilmente suas operações em criptomoedas (FATF, 2014).

2.4 CRIME DE LAVAGEM DE DINHEIRO

Apesar de não haver consenso na literatura a respeito da origem da lavagem de dinheiro (LD), a expressão “lavagem de dinheiro” já se encontra consagrada no glossário das atividades econômico-financeiras e no vocabulário popular, resultado da expressão “*money laundering*” empregada em âmbito internacional. Para Nance (2018), sua definição está em qualquer tentativa de ocultar as fontes ilegais de lucro, cuja origem de sua expressão é disposta por diferentes autores como derivada do uso de lavanderias pelos criminosos do início do século XX na tentativa esconder seu dinheiro. O mesmo, explica que, ainda que essa história possa parecer apócrifa, como metáfora ela permite ilustrar as dificuldades no combate a prática de LD, pois uma lavanderia *self-service* não fornece nenhum registro documental de quantas pessoas utilizaram os serviços da lavanderia.

O Conselho de Controle de Atividades Financeiras (COAF) define LD como sendo um conjunto de operações comerciais ou financeiras que buscam a incorporação na economia de cada país, de modo transitório ou permanente, de recursos, bens e valores de origem ilícita. Sendo o disfarce dos lucros ilícitos realizados por meio de um processo dinâmico envolvendo três fases independentes que, com frequência, ocorrem simultaneamente (COAF, 1999):

i) **Colocação**: Nessa fase, países com regras mais permissíveis ou um sistema financeiro liberal, são procurados para a movimentação do dinheiro através de depósitos, compra de instrumentos negociáveis ou bens. São utilizadas técnicas para dificultar a identificação da procedência do dinheiro, como o fracionamento dos valores movimentados no sistema financeiro e a utilização de estabelecimentos comerciais que usualmente negociam com dinheiro em espécie;

ii) **Ocultação**: Passada a fase de colocação, agora, para dificultar o rastreamento contábil do dinheiro, procura-se quebrar a cadeia de evidências sobre a origem do dinheiro. Busca-se movimentar os ativos de forma eletrônica entre contas anônimas ou com depósitos em contas abertas em nome de “laranjas” ou empresas fictícias ou de fachada; e

iii) **Integração**: Completando o processo, os ativos são incorporados formalmente ao sistema econômico através de investimentos em empreendimentos que viabilizem as atividades das organizações criminosas. Esses empreendimentos podem ocorrer entre as próprias organizações. Formada a cadeia, a legitimidade do dinheiro ilegal torna-se mais fácil.

Por meio desse processo, um criminoso tem a possibilidade de tentar fazer com que o produto monetário com origem nas suas atividades ilícitas pareça ter origem legal (McDOWELL, 2001).

Estudos tratando do processo de LD por meio de diamantes brutos e ouro, em países europeus de língua alemã, foram realizados por Teichmann e Falker (2020, 2023). Teichmann e Falker (2020) constataram que os diamantes brutos são extremamente convenientes para LD, podendo ser usados nas três fases do processo de LD. Igualmente, Teichmann e Falker (2023), evidenciaram que o comércio de ouro continua adequado para LD, podendo ser usado tanto na fase de colocação, como na fase de ocultação.

Lamentavelmente a LD afeta a economia global há muitos anos, abrangendo atividades ilegais usadas para fazer com que fundos adquiridos ilegalmente pareçam legais e legítimos (CHEN *et al.*, 2018). McDowell (2001) explica que a LD tem consequências econômicas, de segurança e sociais potencialmente devastadoras. Segundo estudo realizado por Hendriyetty e Grewal (2017), a LD acomete a economia de um país, aumentando a economia paralela e atividades criminosas, fluxos ilícitos e impedindo a cobrança de impostos.

Nesse contexto, a definição de economia paralela está nas atividades econômicas que não são registradas nas contas oficiais de um país, mas que podem contribuir para o Produto Interno Bruto (PIB) oficialmente calculado (SCHNEIDER, 2005; GOEL; NELSON, 2016). Essa economia tornou-se um dos principais problemas enfrentados em todo o mundo, devido sua natureza de retardar o desenvolvimento do mercado financeiro (GOEL; NELSON, 2016; HAJILEE; STRINGER; METGHALCHI, 2017). Seu fomento foi discutido por Ardizzi, De Franceschis e Giammatteo (2018) e Giammatteo, Iezzi e Zizza (2022), quando analisaram o papel do uso do dinheiro em espécie na Itália, em nível de municípios. Ardizzi, De Franceschis e Giammatteo (2018), verificaram que os depósitos em dinheiro demonstraram estar positivamente correlacionados com a relevância da atividade local de LD, enquanto Giammatteo, Iezzi e Zizza (2022), concluíram que o aumento da utilização do dinheiro consiste num maior nível de subnotificação por parte das empresas italianas junto à Unidade de Inteligência Financeira (UIF) na Itália.

A relação entre a LD e a corrupção de funcionários públicos e evasão fiscal realizada por líderes políticos tem sido de interesse para os estudiosos. O estudo de Ramos (2010), que abordou a corrupção na Administração Pública e crimes de LD no Brasil, concluiu que a Administração Pública se encontra em uma situação longe da ideal quando da adoção de medidas contra a corrupção e a LD, tendo em vista que os órgãos de controle interno no país, ao atuarem de maneira conjunta e integradamente, ainda não alcançaram um nível satisfatório nas diversas esferas de Governo. O autor aponta ainda para o pouco conhecimento, por parte dos agentes dos órgãos de controle interno no país, sobre os mecanismos e às tipologias da LD.

O trabalho de Stack (2015), quando examinou o papel das organizações de LD na evasão fiscal e corrupção na Ucrânia, verificou que as redes de empresas e bancos fraudulentos da Ucrânia geram fluxos internacionais significativos de dinheiro sujo e desfrutam de proteção política de alto nível na Ucrânia. Da mesma forma, Markovska e Adams (2015) analisaram a relação entre a corrupção política e a LD na Nigéria, verificando que a corrupção endêmica da elite política nigeriana resulta em abuso da cláusula constitucional de imunidade e impedimentos às atividades das agências de combate à LD. Ainda, o estudo de Shah e Aish (2022), ao investigarem a relação entre LD, corrupção e inflação em cinco países do Sul da Ásia (Paquistão, Índia, Bangladesh, Sri Lanka e Nepal), descobriram que a corrupção e o LD têm uma ligação significativa e positiva com a inflação nos cinco países.

Com foco na relação da LD com a corrupção no setor privado, o estudo de Chaikin (2008), aponta a corrupção comercial como uma ameaça à integridade do sistema *anti-money laundering* (AML), em particular na fase de colocação no processo de LD. O pesquisador entende que entidades obrigadas a relatar do setor privado podem ser sujeitadas a participarem ativamente em esquemas de LD, não apresentando relatórios de transações suspeitas (RTSs) ou comunicando seus clientes sobre as possibilidades de serem alvos de uma investigação do Governo. Nessa direção, Barone, Masciandaro e Schneider (2019) explicam que, no setor privado, as oportunidades de corrupção mais evidentes parecem surgir na fase de colocação no processo de LD, justamente a fase que geralmente envolve a participação de instituições financeira (IFs). Os autores, em caráter de exemplo, discorrem sobre a possibilidade de suborno dos funcionários de uma IF para que sejam ignorados os requisitos de RTSs impostos por lei.

Retornando à história sobre a origem do termo “lavagem de dinheiro”, narrada anteriormente, Nance (2018) solicita uma reflexão sobre a existência de uma série de lavanderias, todas com nomes diferentes e em jurisdições legais diferentes, tornando a supervisão muito cara. Em um sistema financeiro liberal ou ineficiente, onde bancos e outras instituições aceitam depósitos sem conseguirem verificar as verdadeiras identidades dos proprietários das contas, os criminosos podem fazer o mesmo, tornando a fonte do dinheiro quase impossível de ser encontrada. Com um sistema financeiro cada dia mais rápido e global, a tarefa de rastrear a origem dos recursos torna-se mais difícil, porque o dinheiro se move mais rápido do que aqueles que o rastreiam. Devido a essa natureza transnacional, onde os recursos com origem ilícita transitam por diferentes jurisdições, torna-se imprescindível a existência de uma cooperação internacional para prevenção e combate à lavagem de dinheiro (PCLD).

Assim sendo, a relação entre os paraísos fiscais e a LD, quando dos países com baixos padrões regulatórios de combate à LD, Schwarz (2011) investigou se os paraísos fiscais têm um incentivo para manter baixos padrões regulatórios a fim de atrair atividades de dinheiro ilícito. Os resultados mostram que paraísos fiscais e serviços de LD coincidem no mesmo país.

Ao discutirem os efeitos das políticas de pressão, como listas negras e sanções em centros financeiros *offshore*, bem como sua capacidade de garantir a conformidade desses centros com os regulamentos de combate à LD, Picard e Pieretti (2011) descobriram que os bancos *offshore* atenderiam às políticas de pressão, como o monitoramento das identidades dos investidores e da origem de seus fundos, quando essas políticas tivessem o potencial de criar danos suficientes à reputação dos investidores. Igualmente, Balakina, D'Andrea e Masciandaro (2017), ao avaliarem empiricamente se há um estigma na lista negra do GAFI sobre o sigilo dos bancos *offshore*, constataram que os efeitos das políticas de pressão, como listas negras, provavelmente será uma solução política fraca para um problema estrutural cujas bases estão nos arranjos de incentivos de países *offshore*.

A respeito do fluxo transfronteiriço de dinheiro ilícito, Ferwerda *et al*. (2020) estimam que os fundos de origem ilícita são transferidos através de bancos localizados em 4 a 6 países diferentes antes de serem incorporados formalmente ao sistema econômico como dinheiro limpo. Ao explorarem a ligação entre os fluxos transfronteiriços de dinheiro ilícito e os regimes do sistema regulatório e judicial de combate à LD, D'Avino (2023) concluiu que um aumento nas taxas de investigações, processos e condenações está associado a fluxos de LD mais baixos entre países e a uma menor centralidade de um país na rede internacional de LD, ou seja, a eficiência dos regimes contra a LD é o impedimento crucial para as transações e fluxos de LD.

2.4.1 Grupo de Ação Financeira Internacional (GAFI)

Em julho de 1989, durante a reunião da Cúpula de Paris, os sete países mais ricos do mundo (G-7), em linha com a Convenção de Viena, e no âmbito da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), decidiram criar uma "força-tarefa", o Grupo de Ação Financeira Internacional (GAFI), com a incumbência de examinar, desenvolver e promover políticas de PCLD. O objetivo dessas políticas é impedir que os produtos de tráfico de drogas e outros delitos sejam utilizados em futuras atividades de crimes transnacionais, financiamento do terrorismo (FT), proliferação de armas de destruição em massa, e outras ameaças relacionadas à integridade do sistema financeiro internacional (COAF, 1999; CORRÊA, 2013; NANCE, 2018).

Na introdução ao seu primeiro relatório anual, o GAFI deixa clara a preocupação com a expansão do tráfico de drogas e a prática de LD:

> Os Chefes de Estado ou de Governo de sete grandes nações industrializadas e o Presidente da Comissão das Comunidades Europeias reuniram-se em Paris, em julho de 1989, para a 15ª Cúpula Econômica anual. Afirmaram que o problema das drogas atingiu proporções devastadoras e ressaltaram a necessidade urgente de ações decisivas, tanto em âmbito nacional como internacional. Entre outras resoluções sobre questões relacionadas às drogas, eles convocaram uma Força-Tarefa de Ação Financeira (FATF) dos Participantes da Cúpula e outros países interessados nestes problemas, para avaliar os resultados da cooperação já realizada para evitar a utilização do sistema bancário e das instituições financeiras para o propósito de lavagem de dinheiro, e considerar esforços preventivos adicionais neste campo, incluindo a adaptação dos sistemas estatutários e regulatórios para melhorar a assistência jurídica multilateral. Decidiram que a primeira reunião desta Força-Tarefa seria convocada pela França e que seu relatório seria concluído em abril de 1990. (FATF, 1990, p. 3, tradução nossa).[11]

O GAFI é um órgão intergovernamental independente que desenvolve e promove políticas para proteger o sistema financeiro global dos riscos de LD e FT. É um "órgão formulador de políticas" que trabalha para gerar a vontade política necessária para promover reformas legislativas e regulatórias nacionais nessas áreas. Sendo o principal resultado de suas atividades a existência de leis e instituições similares em diferentes países, que configuram sistemas nacionais direcionados à PCLD e ao *combating financing of terrorism* (CFT), "combate ao financiamento do terrorismo" na tradução livre, trazendo reforços e modernização ao arsenal do Estado no combate ao crime, de modo geral (CORRÊA, 2013; SUXBERGER; CASELATO JR, 2019).

Em 1990, o GAFI publicou as "40 Recomendações" com a intenção de estabelecer ações a serem seguidas pelos países comprometidos em prevenir e combater o crime de LD. Essas Recomendações são revisadas periodicamente a fim de que possam refletir as tendências atuais dos crimes de LD e FT e potenciais ameaças futuras. São reconhecidas como o padrão global, constituindo o primeiro instrumento jurídico internacional direcionado exclusivamente a medidas que devem ser adotadas pelos países para a configuração de um sistema de PLD. Nesse

---

[11] "The Heads of State or Government of seven major industrial nations and the President of the Commission of the European Communities met in Paris in July 1989 for the fifteenth annual Economic Summit. They stated that the drug problem has reached devastating proportions, and stressed the urgent need for decisive actions, both on a national and international basis. Among other resolutions on drug issues, they convened a Financial Action Task Force (FATF) from Summit Participants and other countries interested in these problems, to assess the results of the cooperation already undertaken to prevent the utilization of the banking system and financial institutions for the purpose of money laundering, and to consider additional preventive efforts in this field, including the adaptation of the statutory and regulatory systems to enhance multilateral legal assistance. They decided that the first meeting of this Task Force would be called by France, and that its report would be completed by April 1990."

sentido, avaliações mútuas são periodicamente realizadas pelo GAFI junto aos países membros acerca da adoção de tais medidas. A persistência na inobservância a essas Recomendações por parte dos Governos é possível de resultar em sanções, como a inclusão dos não cooperadores em uma "lista negra" com a "pecha" imposta de "países e territórios não cooperantes", resultando na exclusão do sistema internacional, com privação dos acessos aos benefícios concedidos aos países que cooperam (COAF, 1999; CORRÊA, 2013; SUXBERGER; CASELATO JR, 2019).

O Brasil tornou-se membro observador a partir da XI Reunião Plenária do GAFI, realizada em 1999, passando a membro efetivo do GAFI em 2000, após aprovação da primeira avaliação mútua a que foi submetido. Como membro do GAFI, o Brasil está comprometido em atender as Recomendações e submeter-se a avaliações mútuas realizadas pelo GAFI. Sua última visita para avaliação foi realizada em junho do ano de 2010, estando agendada a próxima em período possível de março de 2023 (COAF, 1999; CORRÊA, 2013; FATF, 2023).

Sendo as 40 Recomendações do GAFI padrões internacionais, com mais de 170 jurisdições que as endossam e estão em processo de implementação dessas Recomendações por meio de mudanças nas leis, regulamentos e instituições nacionais, torna-se imperativo avaliar o quadro legal e regulamentar existente sobre *anti-money laundering* (AML) para apresentar soluções no sentido de tratar as questões de LD de forma mais eficaz (CHAIKIN, 2009; BEEBEEJAUN; DULLOO, 2023).

Como tal, a eficácia do regime global AML e seus efeitos sobre outros campos e na economia têm despertado o interesse dos pesquisadores. Ao avaliar o papel das políticas AML na dissuasão de criminosos de atividades ilegais, Ferwerda (2009) concluiu que melhores políticas AML estão associadas a taxas de criminalidade mais baixas. Chong e Lopez de Silanes (2015), ao investigarem empiricamente os determinantes da LD e sua regulamentação em cerca de 100 países, obtiveram resultados comprovando que regulamentações mais rígidas sobre LD tem impacto na redução da LD e na extensão de suas atividades alimentadoras. Barone e Masciandaro (2011), quando procuraram estimar o benefício público para a Europa frente a redução no valor de retorno nas atividades de LD, descobriram que os benefícios públicos superam os custos das medidas AML. No entanto, Barone, Delle Side e Masciandaro (2018) sinalizam que, apesar da melhora nas políticas AML trazer um aumento nos custos para o crime organizado, ao mesmo tempo, pode impactar negativamente nos custos de PCLD na economia em geral. Assim também, o estudo de Pol (2020) concluiu que a intervenção da política AML

tem menos de 0,1% de impacto nas finanças criminosas, sendo que, os custos de conformidade excedem os fundos criminais recuperados em mais de cem vezes.

Por conseguinte, considerando o contexto no qual os regulamentos AML oneram as IFs, e, portanto, regulamentos AML excessivos podem não promover o desenvolvimento do setor financeiro, Ofoeda *et al.* (2022), ao estudarem o efeito das regulamentações AML no desenvolvimento do setor financeiro de 165 países entre 2012 a 2018, encontraram evidências de que os regulamentos AML geralmente promovem o desenvolvimento do setor financeiro, sendo que, esse efeito positivo está concentrado nos países em desenvolvimento. Conforme os autores, os regulamentos AML promovem o desenvolvimento do setor financeiro até o valor limiar além do qual não impactam o desenvolvimento do setor financeiro. Mediante ao fato de que regulamentos AML excessivos podem não ter os resultados necessários, os autores apontam para a necessidade de que as economias desenvolvidas revisem sua estrutura regulatória AML para torná-la econômica para as IFs. Os estudos de Issah *et al*. (2022) e Durguti *et al*. (2023) contribuem para esse resultado. Issah *et al*. (2022) ao analisarem a relação entre os regulamentos AML e a estabilidade do setor bancário em 51 países africanos durante o período de 2012 a 2019, assim como Durguti *et al*. (2023), que estudaram a eficácia dos regulamentos AML na estabilidade do setor bancário nos países dos Balcãs Ocidentais entre 2012 e 2021, compreenderam que os regulamentos AML provocam um impacto positivo e estatisticamente significativo na estabilidade do setor bancário desses países. Huang (2015), ao analisar o processo judicial do banco HSBC de 2012, concluiu que seguir os regulamentos de AML dos EUA resulta em uma melhor detecção e PLD, contudo, o estudo de Balani (2019) sugere que a regulamentação AML recente é um ônus de conformidade de custos para o setor bancário dos EUA, onde os custos das operações superam os benefícios dos processos aprimorados.

Sobre os determinantes da conformidade em AML, Mekpor, Aboagye e Welbeck (2018), ao analisarem o nível de conformidade em AML para 155 países membros do GAFI entre 2004 e 2016, constataram que a adesão aos padrões AML melhorou ligeiramente ao longo dos anos, e que tecnologia, qualidade regulatória, concentração bancária, abertura comercial e centro de inteligência financeira determinaram e melhoraram significativamente a conformidade em AML. Corroborando para esse achado, Hamin (2017), ao examinar algumas alterações na antiga lei AML da Malásia, considerou-as como oportunas e positivas em relação a intensão do Governo em aderir aos padrões AML do GAFI. No entanto, o autor sinaliza como imperativa, uma abordagem sobre as deficiências instrumentais e normativas remanescentes na lei AML, como forma de garantia de que a revisão seja suficientemente abrangente para

prevenir e regular a LD na Malásia. Ainda sobre a Malásia, Zolkaflil, Omar e Syed Mustapha Nazri (2019), visando compreender os desafios enfrentados pelas agências de aplicação da lei na investigação de atividades de LD na Malásia, concluíram que, embora essas agências tenham o poder de investigar a LD sob a lei, a Malásia carece de um sistema de apoio investigativo preparado para auxiliar essas agências durante o processo de investigação.

Firas (2022), que analisou a evolução dos procedimentos de AML na Palestina desde 2004, constatou que a Palestina estabeleceu a base jurídica AML necessária para combater a LD, onde Unidade de Acompanhamento Financeiro dotou-se de todas as competências exigidas pelas UIFs, assim como emissão de políticas e planos para responder aos resultados do processo de Avaliação de Risco Nacional (ARN). Em contraste, o autor entende haver vários desafios, em particular no que diz respeito aos fatores políticos e suas consequências esperadas durante a preparação e condução do processo de avaliação mútua para a Palestina. Contudo, Jayasekara (2021), ao estudar o impacto dos padrões globais de AML nos esforços de combate à LD, constatou que a implementação efetiva do quadro jurídico AML é importante, mas não o suficiente para combater a LD, importando que o GAFI fortaleça o mecanismo de monitoramento de países deficientes em políticas AML com mais sanções para combater as atividades globais de LD.

Por conseguinte, Manning, Wong e Jevtovic (2021), ao examinarem a relação entre o nível de LD e o nível de conformidade em AML, concluíram que a irregularidade nas diretrizes usadas pelos países para desenvolver uma política AML pode impactar negativamente em sua segurança AML, sendo que, os países altamente adaptáveis aos padrões do GAFI são os que tendem a desfrutar de menor risco de LD.

2.4.2 Lei de Lavagem de Dinheiro

Em março de 1998, o Brasil aprovou a Lei nº 9.613, conhecida como “Lei de Lavagem de Dinheiro”, primeiro dispositivo legal que tipifica o crime de LD no Brasil, sendo considerada o principal marco na organização do sistema de prevenção e combate à lavagem de dinheiro (PCLD) no País. Essa Lei foi constituída por meio da execução nacional de compromissos internacionais assumidos pelo Brasil, cujo primeiro compromisso foi com a Convenção das Nações Unidas sobre o Tráfico Ilícito de Entorpecentes e de Substâncias Psicotrópicas, conhecida como “Convenção de Viena”, aprovada em Viena, Áustria, em 1988, e ratificada pelo Brasil em junho de 1991, por meio do Decreto nº 154 (BRASIL, 1991, 1996, 1998).

Segundo Corrêa (2013) a Convenção de Viena reforçou e ampliou a abrangência de dispositivos em outras Convenções das Nações Unidas, incorporando as dimensões do crime organizado e da LD. Seu objetivo estava em promover a cooperação internacional no tratamento das questões relacionadas ao tráfico de drogas e crimes correlatos, dentre eles a LD. É reconhecida como o primeiro instrumento jurídico internacional a tipificar como crime a operação de LD (BRASIL, 1991, 1996).

A Convenção de Viena institui em seu "ARTIGO 3" a obrigação de os países criminalizarem a prática de LD:

> 1 - Cada uma das Partes adotará as medidas necessárias para caracterizar como delitos penais em seu direito interno, quando cometidos internacionalmente:
> [...]
> i) a conversão ou a transferência de bens, com conhecimento de que tais bens são procedentes de algum ou alguns dos delitos estabelecidos no inciso a) deste parágrafo, ou da prática do delito ou delitos em questão, com o objetivo de ocultar ou encobrir a origem ilícita dos bens, ou de ajudar a qualquer pessoa que participe na prática do delito ou delitos em questão, para fugir das consequências jurídicas de seus atos;
> ii) a ocultação ou o encobrimento, da natureza, origem, localização, destino, movimentação ou propriedade verdadeira dos bens, sabendo que procedem de algum ou alguns dos delitos mencionados no inciso a) deste parágrafo ou de participação no delito ou delitos em questão;
> [...] (BRASIL, 1991).

A LD está associada aos delitos penais quando cometidos a conversão ou transferência e a ocultação ou encobrimento de bens de origem ilícita.

O Art. 1º da Lei de Lavagem de Dinheiro, com a nova redação conferida pela Lei nº 12.683 de 2012, tipifica o crime de LD como a prática de "ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal", com pena de reclusão de três a dez anos, e multa. Assim, como:

> § 1º incorre na mesma pena quem, para ocultar ou dissimular a utilização de bens, direitos ou valores provenientes de infração penal:
> I – os converte em ativos lícitos;
> II – os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, tem em depósito, movimento ou transfere;
> III – importa ou exporta bens com valores não correspondentes aos verdadeiros.
> § 2º Incorre, ainda, na mesma pena quem:
> I – utiliza, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal;
> II – participa de grupo, associação ou escritório tendo conhecimento de que sua atividade principal ou secundária é dirigida à prática de crimes previstos nesta Lei (BRASIL, 1998).

Essa definição encontra-se amparada pelo artigo 180 do Código Penal, que define o crime de receptação, cuja ação de "adquirir, receber, transportar, conduzir ou ocultar, em proveito próprio ou alheio, coisa que sabe ser produto de crime, ou influir para que terceiro, de boa-fé, a adquira, receba ou oculte" (BRASIL, 1940).

Conforme Jung (2007), certas atividades financeiras guardam maior risco de exposição aos efeitos dos crimes relacionados à prática de LD, seja pela sua natureza, ativo que operam ou pela impessoalidade dos agentes, entre outras características. No artigo 9º da Lei de Lavagem de Dinheiro encontra-se uma série de atividades, cujos operadores estão sujeitos às obrigações a respeito da identificação e manutenção de informações sobre o cliente, e da comunicação de operações financeiras. Conforme seu inciso XIV, as pessoas tanto físicas como jurídicas que prestarem, mesmo que eventualmente, serviços de assessoria, consultoria, contadoria, auditoria, aconselhamento ou assistência, de qualquer natureza, estão sujeitas a essas obrigações quando realizarem as seguintes operações:

> a) de compra e venda de imóveis, estabelecimentos comerciais ou industriais ou participações societárias de qualquer natureza;
> b) de gestão de fundos, valores mobiliários ou outros ativos;
> c) de abertura ou gestão de contas bancárias, de poupança, investimento ou de valores mobiliários;
> d) de criação, exploração ou gestão de sociedade de qualquer natureza, fundações, fundos fiduciários ou estruturas análogas;
> e) financeiras, societárias ou imobiliárias; e
> f) de alienação ou aquisição de direitos sobre contratos relacionados a atividades desportivas ou artísticas profissionais; (BRASIL, 1998).

Esses serviços normalmente se enquadram nas atividades desenvolvidas pelos profissionais da contabilidade, que ficam sujeitos às obrigações de identificar seus clientes, manter os cadastros de seus clientes atualizados e comunicar a existência de operações financeiras que possam constituir-se em indícios de crimes, ou com eles se relacionarem. O inciso III, do artigo 11, afirma que a comunicação deverá ser feita ao órgão regulador ou fiscalizador da profissão regulamentada ou, na sua falta, ao COAF (BRASIL, 1998).

De fato, diferentes normativos foram emitidos pelos órgãos reguladores dos setores mais propícios para a prática de LD, com objetivo de implementar essas obrigações.

Esses setores devem adotar políticas, procedimentos e controles internos, que sejam compatíveis com seu porte e volume de operações, para atenderem os normativos a eles aplicados.

Sobre a necessidade de instituir esses mecanismos de controle em atendimento a legislação de PLD, Nakamura, Nakamura e Jones (2019), confirmam que, para fortalecer sua

posição no mercado, as organizações precisam entender a importância e abrangência da área de *Compliance*, e as consequências de sua não implementação.

Nessa direção, Coelho Junior e Da Silva Abbad (2010), ao analisarem a percepção dos alunos de curso aplicado a agentes do setor bancário para análise e aplicação de medidas de PLD, entenderam como válido o treinamento "Prevenção à Lavagem de Dinheiro" oferecido por uma universidade corporativa de certa organização bancária de âmbito nacional. Assim como, Da Silva, Marques e Teixeira (2011), ao avaliarem a percepção dos funcionários de IFs quanto aos procedimentos de controles internos para PLD, concluíram que eles demonstram ter conhecimento dos normativos e atenção às medidas de PLD.

No entanto, Calastro Junior e Mendonça Neto (2018), ao analisarem processos administrativos cujos envolvidos foram os intermediários do mercado de valores mobiliários brasileiro, identificaram deficiências como a ausência ou falha nos controles internos, ausência de diligência pelos intermediários e ausência de procedimentos e de treinamento.

Do mesmo modo, Façanha *et al*. (2020) ao investigarem as informações sobre gerenciamento de risco e gestão de controles internos divulgadas no Formulário de Referência por companhias de capital aberto envolvidas em crimes de corrupção e LD, observaram a ausência ou implementação tardia de uma política de gerenciamento de risco formal, assim como uma gestão de controles internos ineficaz.

Como resultado, ao estudarem o impacto da implementação desses mecanismos de controle, os trabalhos de Amorim, Cardozo e Vicente (2012) e Ferreira, Onzi e Ramalho (2019), evidenciaram uma alta na quantidade de comunicados que resultaram no aumento do número de Relatórios de Inteligência Financeira (RIF) elaborados no Brasil, o que demonstra um impacto positivo na implementação dos mecanismos de controle inerentes à PLD.

2.4.3 Conselho de Controle de Atividades Financeiras (COAF)

Por meio da Lei de Lavagem de Dinheiro, foi criado, no âmbito do Ministério da Economia, o Conselho de Controle de Atividades Financeiras (COAF), com a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas em lei. Sua principal tarefa está em promover o empenho conjunto dos vários órgãos governamentais do Brasil responsáveis pela implementação de políticas nacionais direcionadas à prevenção e combate da prática de LD, impedindo a utilização dos setores da economia nessas operações ilícitas (BRASIL, 1998; COAF, 1999).

Em 1999, o COAF passou a integrar o Grupo de *Egmont*, um organismo internacional informacional, criado pelas Unidades de Inteligência Financeira (UIFs) belga, *Belgian Financial Intelligence Processing Unit* (CTIF-CFI), e norte-americana, *Financial Crimes Enforcement Network* (FINCEN). O Grupo de *Egmont* congrega UIFs de todo o mundo, com o objetivo de realizar trocas de informações, recebimento e tratamento de comunicados suspeitos sobre a prática de LD. Assim, o COAF mantém uma cooperação bilateral com outras UIFs, tendo acesso a informações sobre novas tendências de combate à prática de LD, ferramentas de análise financeira, desenvolvimento tecnológico, assim como treinamento e capacitação.

O COAF realiza a análise financeira das comunicações de suspeitas de práticas de LD com base na abordagem baseada em risco (ABR). Os sinais de alerta identificados nas bases de dados são analisados e processados por meio da Central de Gerenciamento de Riscos e Prioridades (CGRP). Os fatores ligados aos crimes antecedentes à LD e ao crime de corrupção, por exemplo, são classificados de forma qualificada, dentre diferentes atributos de risco (COAF, 2016).

O Sistema do COAF é formado por uma base de dados que reúne mais de 19 milhões de comunicações de operações financeiras, com aproximadamente 2,7 milhões recebidas em 2019. No período de janeiro a setembro de 2019, foram elaborados 5.273 Relatórios de Inteligência Financeira (RIF), os quais relacionaram 255.638 pessoas físicas ou jurídicas, e consolidaram 244.551 comunicações de operações financeiras. Nos setores regulados e fiscalizados, foram realizadas 130 ações de fiscalização sobre a conformidade das obrigações direcionadas à PLD, onde 12 resultaram em Processo Administrativo Sancionador (PAS). Durante o ano de 2020, até setembro, foram julgados 59 PAS de empresas e dirigentes, com aplicação de R$ 3,5 milhões em multas (COAF, 2020).

2.4.4 Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA)

A Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA), assim como COAF, proporciona a oportunidade de articulação de arranjos institucionais para a formulação de políticas públicas e soluções voltadas ao combate coordenado desses crimes. Proporcionando, ainda, a oportunidade de compartilhar experiências de prevenção, repressão, capacitação e difusão, criando uma verdadeira estratégia nacional sobre essa temática. Criada em 2003 pelo Ministério da Justiça e Segurança Pública, a ENCCLA tem a seguinte estrutura:

> 1. **Plenária**: realizada, em geral, na última semana do mês de novembro de cada ano, no sistema de imersão total, os membros participantes da Estratégia aprovam as Ações do ano em curso e as do ano seguinte, além das recomendações e das declarações.
> 2. **Gabinete de Gestão Integrada (GGI)**: consiste em um grupo de órgãos e entidades específicos que se reúnem a cada três meses para realizar o acompanhamento da execução das Ações. No âmbito do GGI, há dois grupos (corrupção e lavagem de dinheiro) com o objetivo de propor ações que serão debatidas na Plenária.
> 3. **Grupos de Trabalho Anual**: sob a coordenação de órgãos específicos, segundo a definição temática e de assuntos institucionais correlacionados, dão vida às atividades para concluir os objetivos determinados na Plenária. Cada ano tem um número de Ações específicas que são definidas na Plenária.
> 4. **Grupos de Trabalho de Combate à Corrupção e de Combate à Lavagem de dinheiro**: formados para discutir e dar forma às propostas das Ações vindouras e que serão referendadas na Plenária, reúnem-se a partir do segundo semestre e, em média, resolvem as propostas em duas reuniões.
> 5. **Secretaria Executiva**: as funções administrativas da ENCCLA são exercidas pelo Departamento de Recuperação de Ativos e Cooperação Internacional (DRCI), da Secretaria Nacional de Justiça e Cidadania, ficando internamente sob a responsabilidade da Coordenação-Geral de Articulação Institucional (CGAI/DRCI/SENAJUS/MJSP) (ENCCLA, 2020).

A ENCCLA tem como colaboradores o Banco Central do Brasil (BCB), Comissão de Valores Mobiliários (CVM), Receita Federal do Brasil (RFB), Conselho de Controle de Atividades Financeiras (COAF), Federação Brasileira de Bancos (FEBRABAN), Ministério Público Federal (MPF), Polícia Federal (PF), dentre outros. Esses trabalhos são realizados nas chamadas “Ações”, que são elaboradas e pactuadas anualmente pelos membros da ENCCLA. Para cada Ação é criada um grupo de trabalho composto por vários órgãos e instituições, que procuram alcançar uma ou mais metas predefinidas.

A respeito dos aspectos da formatação e da articulação existente na ENCCLA, Rocha (2008) entende que a interação em rede por parte dos órgãos e/ou entidades favorece o alcance de resultados mais concretos, uma vez que espaços interativos de articulação interorganizacional podem ser criados pela diversidade de atores e a atuação em rede, o que permitiria uma sinergia em busca dos objetivos da ENCCLA. No entanto, Florêncio Filho e Zanon (2018) entendem que apesar da ENCCLA ter alcançado importantes resultados como uma iniciativa relevante no combate ao crime organizado, sendo considerada pelo GAFI um modelo de articulação governamental, existem alguns pontos críticos no seu desenho jurídico-institucional que podem afetar negativamente a efetividade e a institucionalização das políticas elaboradas no âmbito da ENCCLA. Como um dos pontos mais críticos observados pelos autores, está o “arranjo institucional relacionado”, que tem como objetivo a interação e articulação dos órgãos e/ou entidades participantes da ENCCLA. Esse objetivo parece

ameaçado, segundo os autores, quando os meios de comunicação, gestão de informações e os mecanismos jurídicos nos quais os participantes norteiam-se, parecem não serem suficientes.

Outro ponto crítico evidenciado por Florêncio Filho e Zanon (2018), está na "ausência de um suporte legal", ou seja, a ausência de uma norma legal que proteja a Estratégia de indesejáveis efeitos de uma insegurança jurídica. Para Queiroz (2019), essa falta de regulação referente a Estratégia torna frágil e vulnerável a participação de membros da sociedade civil, uma vez que o responsável por essa decisão é o Gabinete de Gestão Integrada (GGI), que não conta com parâmetros claros e objetivos para a deliberação. Queiroz (2019) entende que mesmo diante de algumas oportunidades de participação da sociedade civil serem permitidas durante o trabalho da ENCCLA, essa participação continua sendo realizada de maneira muito tímida.

Florêncio Filho e Zanon (2018) e Queiroz (2019) entendem que, apesar dos obstáculos que a ENCCLA tem que superar, ela tem alcançado importantes resultados por meio de suas Ações, destacando como principais os seguintes resultados: (i) Programa Nacional de Capacitação e Treinamento no Combate à Corrupção e à Lavagem de Dinheiro (PNLD); (ii) Rede Nacional de Laboratórios contra Lavagem de Dinheiro (Rede-LAB); (iii) Sistema de Movimentação Bancária (SIMBA); (iv) Cadastro de Clientes do Sistema Financeiro Nacional (CCS); (v) Sistema Nacional de Bens Apreendidos (SNBA); e (vi) Proposição legislativa que resultou na promulgação da Lei nº 12.683/12, que modernizou a Lei nº 9.613/98.

2.5 A RESPONSABILIDADE DO CONTADOR

Segundo o Código de Ética Profissional do Contador (CEPC), cujo um dos objetivos é fixar a conduta do contador, quando no exercício da sua atividade e nos assuntos relacionados à profissão e à classe, o profissional da contabilidade deve exercer a profissão com zelo, diligência, honestidade e capacidade técnica, observando as Normas Brasileiras de Contabilidade e a legislação vigente, resguardando o interesse público, dos seus clientes ou seus empregadores, sem prejuízo da dignidade e independência profissional (CFC, 2019).

Portanto, quando o CEPC é observado pelo profissional da contabilidade, torna-se possível o cumprimento das responsabilidades administrativa, civil, tributária e penal, por parte desse profissional, contribuindo para que não ocorram erros e omissões voluntárias ou involuntárias que acarretarão julgamentos. O profissional da contabilidade está sujeito às fiscalizações e sanções dos órgãos de classe quando cometer infrações ético-disciplinares no exercício legal de suas atividades.

Conforme o artigo 10 do Decreto-Lei nº 9.295 de 1946, os Conselhos Regionais de Contabilidade (CRCs) têm como umas das atribuições, fiscalizar o exercício das atividades do contador, com objetivo de impedir e punir as infrações, assim como enviar às autoridades competentes relatórios sobre fatos apurados cuja solução ou repressão não seja de sua competência. Sendo as sanções aplicadas: multa, advertência, censura, suspensão e cassação do registro, de acordo com a gravidade da infração (BRASIL, 1946).

A respeito da responsabilidade civil do profissional de contabilidade, o parágrafo único do artigo 1.177 da Lei nº 10.406 de 2002, que instituiu o novo Código Civil brasileiro, expõe que "no exercício de suas funções, os prepostos são pessoalmente responsáveis, perante os preponentes, pelos atos culposos; e, perante terceiros, solidariamente com o preponente, pelos atos dolosos". Seu artigo 186 estabelece que "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" (BRASIL, 2002).

Desta forma o contabilista responderá tanto individualmente perante seu cliente, como solidariamente perante terceiros, pelos atos ilícitos praticados com dolo. O novo Código Civil também trata da profissão contábil quando da escrituração em seus artigos 1.179 a 1.195 (BRASIL, 2002).

A Lei de Falências, que regula a recuperação judicial, a extrajudicial e a falência do empresário e da sociedade empresária, também deve ser observada pelo profissional da contabilidade. Em seu artigo 168, determina-se pena de reclusão de três a seis anos, e multa para quem "praticar, […] ato fraudulento de que resulte ou possa resultar prejuízo aos credores, com o fim de obter ou assegurar vantagem indevida para si ou para outrem" (BRASIL, 2005). As penas ainda podem ser aumentadas, conforme o § 1º do mesmo artigo, em 1/6 (um sexto) a 1/3 (um terço), se o agente (BRASIL, 2005):

> I – elabora escrituração contábil ou balanço com dados inexatos;
> II – omite, na escrituração contábil ou no balanço, lançamento que deles deveria constar, ou altera escrituração ou balanço verdadeiro;
> III – destrói, apaga ou corrompe dados contábeis ou negociais armazenados em computador ou sistema informatizado;
> IV – simula a composição do capital social;
> V – destrói, oculta ou inutiliza, total ou parcialmente, os documentos de escrituração contábil obrigatórios.

Os profissionais da contabilidade estão sujeitos às sanções penais presentes no artigo 168 se concorrerem para condutas criminosas, na medida de sua culpabilidade, inclusive quanto à manutenção de contabilidade paralela à exigida pela legislação.

A Lei nº 8.137 de 1990, que traz ao profissional de contabilidade uma responsabilidade tributária, expõe em seu artigo 1º que suprimir ou reduzir tributo constitui crime contra a ordem tributária, com pena de reclusão de dois a cinco anos, mais multa, podendo, conforme seu artigo 11, incidir, na medida de sua culpabilidade, sobre quem, que de qualquer forma, inclusive por meio de pessoa jurídica, concorra para esse crime. Ao contribuir para inserção de dados inexatos, ou omissão de operação de qualquer natureza em documento ou livro exigido pela lei fiscal, omissão de informação, ou prestação de declaração falsa às autoridades fazendárias, o profissional da contabilidade está sujeito a essa penalidade, assim como, dentre outras práticas, elaborar, fornecer, emitir ou utilizar documentos que tenha ou deva ter ciência sobre falsidade ou inexatidão (BRASIL, 1990).

Sobre a responsabilidade penal dos profissionais de contabilidade, o Código Penal brasileiro, em seu artigo 297, prevê além de multa, pena de reclusão de dois a seis anos para quem falsificar ou alterar documento público. Prevendo em seu § 2º que "para os efeitos penais, equiparam-se a documento público o emanado de paraestatal, o título ao portador ou transmissível por endosso, as ações de sociedade comercial, os livros mercantis e o testamento particular". O § 3º, inciso III do mesmo artigo, expõe que nas mesmas penas incorrem quem insere ou faz inserir "em documento contábil ou em qualquer documento relacionado com as obrigações da empresa perante a previdência social, declaração falsa ou diversa da que deveria ter constado" (BRASIL, 1940).

O profissional da contabilidade também responde penalmente nos crimes de LD, com pena de reclusão de três a dez anos. Como visto na seção 2.4.2 – Lei de Lavagem de Dinheiro, do presente estudo, que a definição de crime de LD encontra-se amparada pelo artigo 180 do Código Penal, e que o inciso XIV do artigo 9º da Lei de Lavagem de Dinheiro define o profissional da contabilidade como um dos sujeitos obrigados às medidas de prevenção e combate à lavagem de dinheiro (PCLD), o Conselho Federal de Contabilidade (CFC) emitiu a Resolução CFC nº 1.530 de 2017, em substituição a Resolução CFC nº 1.445 de 2013.

Essa resolução trata sobre os procedimentos que devem ser observados pelos profissionais e organizações contábeis no cumprimento das obrigações elencadas na Lei de Lavagem de Dinheiro alterada pela Lei nº 12.683 de 2012. O § 4º do artigo 4º da Instrução CVM nº 617 de 2019 esclarece que a política de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT), elaborada e implementada pelos auditores independentes, deve abranger, no mínimo, o conteúdo definido em regulamentação específica emitida pelo CFC, ou seja, a Resolução CFC nº 1.530 de 2017.

A Resolução CFC nº 1.530 de 2017 regulamenta procedimentos e normas gerais decorrentes da Lei de Lavagem de Dinheiro. Quanto ao seu alcance, essa resolução impõe ao seu cumprimento os profissionais e organizações contábeis sujeitos as obrigações elencadas no artigo 9º da Lei de Lavagem de Dinheiro. Sobre a política de prevenção, de acordo com artigo 2º dessa resolução, devem ser adotados políticas, procedimentos e controles internos compatíveis com porte e volume de operações. No que se refere ao cadastro dos clientes e registro das operações, os seus artigos 3º e 4º, estabelecem o dever de se manter atualizados cadastro de clientes e registro dos serviços prestados, sendo, conforme seu artigo 12, conservados, por no mínimo, cinco anos, contados da data de entrega do serviço contratado. Essa resolução, ao procurar orientar o profissional da contabilidade e as organizações contábeis em relação à análise de riscos, prevê em seu artigo 5º quais são operações e propostas de operações que devem ser analisadas com especial atenção, conforme **Quadro 3**.

Quadro 3 – Operações e propostas de operações a serem analisadas com especial atenção

Inciso	Operações e propostas de operações
I	Operação que aparente não ser resultante das atividades usuais do cliente ou do seu ramo de negócio;
II	Operação cuja origem ou fundamentação econômica ou legal não seja claramente aferível;
III	Operação incompatível com o patrimônio, com a capacidade econômica-financeira, com a atividade ou ramo de negócio do cliente;
IV	Operação com cliente cujo beneficiário final não é possível identificar;
V	Operação ou proposta envolvendo pessoa jurídica domiciliada em jurisdições consideradas pelo GAFI de alto risco ou com deficiências de PCLD e ao CFT, ou países ou dependências consideradas pela RFB de tributação favorecida e/ou regime fiscal privilegiado;
VI	Operação ou proposta envolvendo pessoa jurídica cujos beneficiários finais, sócios, acionistas, procuradores ou representantes legas mantenham domicílio em jurisdições consideradas pelo GAFI de alto risco ou com deficiências estratégicas de PCLD e ao CFT, ou países ou dependências consideradas pela RFB de tributação favorecida e/ou regime fiscal privilegiado;
VII	Operação, injustificadamente, complexa ou com custos mais elevados que visem dificultar o rastreamento dos recursos ou a identificação do real objetivo da operação;
VIII	Operação que vise adulterar ou manipular características das operações financeiras ou a identificação do real objetivo da operação;
IX	Operação aparentemente fictícia ou com indícios de superfaturamento ou subfaturamento;
X	Operação com cláusulas que estabeleçam condições incompatíveis com as práticas no mercado;
XI	Qualquer tentativa de fracionamento de valores com o fim de evitar a comunicação em espécie a que se refere o Art. 6º; e
XII	Quaisquer outras operações que, considerando as partes e demais envolvidos, os valores, modo de realização e meio de pagamento, ou a falta de fundamento econômico ou legal, possam configurar sérios indícios da ocorrência dos crimes previstos na Lei n.º 9.613/1998 ou com eles relacionar-se.

Fonte: Resolução CFC nº 1.530 de 2017.

Sendo observado, após a análise de risco, que determinada operação ou proposta de operação configura indício de ocorrência de ilícitos, o COAF deve ser comunicado da ocorrência. Contudo, independentemente de análise, o parágrafo único do artigo 6º da Resolução CFC nº 1.530 de 2017, estabelece a obrigatoriedade de comunicação ao COAF das operações, mesmo que fracionadas, relacionadas com:

> (a) aquisição de ativos e pagamentos a terceiros, em espécie, acima de R$ 50.000,00 (cinquenta mil reais), por operação; e/ou (b) constituição de empresa e/ou aumento de capital social com integralização, em espécie, acima de R$ 100.000,00 (cem mil reais), em único mês calendário.

Na ausência de ocorrência das operações ou propostas de operações descritas no **Quadro 3**, durante o ano civil, o artigo 10 dessa resolução, estabelece que o profissional da contabilidade e as organizações contábeis devem apresentar comunicação negativa até o dia 31 de janeiro do ano seguinte.

O não cumprimento das obrigações dessa resolução resulta em responsabilidade administrativa, com aplicação de sanções previstas no artigo 27 do Decreto-Lei nº 9.295 de 1946, independentemente da aplicação do artigo 12 da Lei de Lavagem de Dinheiro.

Nesse contexto, observa-se que o profissional de contabilidade, além do seu código de ética e fiscalização de seus órgãos de classe, se sujeita à legislação cível e penal.

Diante da obrigatoriedade de identificar e comunicar operações suspeitas de LD para o COAF por parte dos setores obrigados, ou seja, o profissional da contabilidade e as organizações contábeis, Gomes *et al*. (2018) e Ferreira, Onzi e Ramalho (2019) lançam luz sobre um grande desafio para a classe contábil, como a criação de uma consciência sobre a relevância das informações ao Governo, que segundo os autores, mantém prerrogativas fiscalizadora e punitiva cada vez mais abrangentes. Sallaberry *et al*. (2020) explicam que apesar da convocação dos profissionais da contabilidade para auxiliar o Governo nos esforços para minimizar os riscos de crimes financeiros, esses profissionais geralmente não recebem formação para tal atividade. Essa demanda de cursos de graduação e pós-graduação, bem como cursos de atualização e aperfeiçoamento, com objetivo de capacitar os profissionais da contabilidade a respeito da PCLD, está entre os achados dos estudos de Ribeiro *et al.* (2016), Gomes *et al*. (2018), Da Rocha Alves *et al*. (2019) e Lubas *et al*. (2021).

2.6 ABORDAGEM BASEADA EM RISCO (ABR)

Dentre as 40 Recomendações do GAFI, a Recomendação Nº 1 – Avaliação de riscos e aplicação de uma abordagem baseada em risco, orienta que os países devem identificar, avaliar e compreender os riscos de lavagem de dinheiro (LD) e com base nessa avaliação, deve-se aplicar uma abordagem baseada em risco (ABR) para garantir que as medidas para prevenir ou mitigar a LD sejam proporcionais aos riscos identificados (FATF, 2020a, p. 10).

Conforme o GAFI, a ABR para prevenção à lavagem de dinheiro (PLD) significa que os países, autoridades competentes, instituições financeiras (IFs) e atividades e profissões não financeiras designadas (APNFDs), devem identificar, avaliar e compreender os riscos de LD a que estão expostos e tomar as medidas de PLD necessárias para mitigar e gerir os riscos de forma eficaz e eficiente (FATF, 2019a, p. 14).

O princípio geral de uma ABR está na implantação de medidas proporcionais aos riscos identificados, isto é, onde houver riscos mais elevados, os países devem exigir que as IFs e as APNFDs tomem medidas aprimoradas para gerenciar e mitigar esses riscos; e medidas menos aprimoradas onde os riscos são menores (FATF, 2020a, p. 31).

Sathye e Islam (2011) entendem que a liberdade para desenvolver procedimentos e processos de conformidade que abordem os riscos específicos enfrentados pelas entidades que relatam, e alocar recursos de forma adequada no combate desses riscos, caracteriza a ABR como uma abordagem baseada em princípios e não em regras. Com seu conteúdo flexível, reticular, multissetorial e dinâmico, com foco na resolução de problemas, a ABR é o eixo central das normas de PLD, cuja adoção caracteriza-se pela transição de uma condição prescritiva para uma visão mais de princípio dessas normas, atribuindo, assim, um papel central aos reguladores nacionais e ao setor privado (RODRIGUES; KURTZ, 2019; ANBIMA, 2020).

Para Jakobi (2018), a ABR consiste em avaliações baseadas na experiência e no conhecimento de atores do setor privado, que segundo Nance (2018) atribui maior responsabilidade a esses atores, pressupondo que os riscos de LD são conhecidos por eles e que eles podem e irão agir em linha com as intenções dos reguladores nacionais. Irão monitorar as transações em busca de atividades suspeitas e avaliarão se essas transações podem representar uma prática de LD ou outras transações ilícitas (JAKOBI, 2018). Nesse sentido, Tsingou (2010) observa que, os atores que se encontram na vanguarda das atividades de *anti-money laundering* (AML) são, na prática, em sua maioria atores do setor privado.

Dentro desse contexto, os atores do setor privado regulados são incentivados a prevenir o crime de LD de forma proativa, em vez de obedecer passivamente às regras determinadas pelos reguladores nacionais.

2.6.1 Abordagem Baseada em Risco (ABR) e o Contador

Embora, o GAFI tenha, inicialmente, se concentrado na implementação de medidas para evitar a utilização do sistema bancário e das instituições financeiras (IFs) no crime de LD (FATF, 1990, p. 3), tal fato, segundo Suxberger e Pasiani (2018), além de não excluir a possibilidade de que outros setores econômicos tenham sido utilizados por criminosos, pode ter induzido o deslocamento das atividades criminosas para setores mais vulneráveis. Jeans (2019) afirma que o uso dos setores das APNFDs por criminosos e sindicatos de LD há muito foi compreendido e evidenciado por processos criminais reais, e que as vulnerabilidades das APNFDs representam uma ameaça real à estabilidade econômica dos países e das empresas.

Conforme Helgesson e Mörth (2018), ainda que o sistema bancário e outras IFs continuem sendo os principais grupos-alvo do GAFI, o aumento da pressão sobre as APNFDs para se envolverem no combate à LD e ao FT tem ampliado o público-alvo do GAFI. Cabello (2011) explica que o surgimento de diferentes técnicas de LD permitiu que as atividades não financeiras fossem utilizadas de forma mais eficiente no crime de LD, resultando na inclusão das APNFDs no rol de atividades também sujeitas aos deveres de PLD e CFT. Tal fato ocorreu em outubro de 2003, quando o GAFI revisou suas 40 Recomendações, para incluir requisitos específicos para as APNFDs, colocando-as sob sua estrutura de conformidade global de PLD e CFT, classificando-as como entidades relatoras com obrigações de PLD e CFT definidas e listando-as como: (i) Cassinos; (ii) Corretores de imóveis; (iii) Comerciantes de metais preciosos e pedras preciosas; (iv) Advogados, notários, outras profissões jurídicas independentes e contadores; e (v) Prestadores de serviços a empresas e *trusts* (JEANS, 2019; FATF, 2020a; NDUKA; SECHAP, 2021). Em fevereiro de 2012, o GAFI revisou suas 40 Recomendações, que mantiveram as Recomendações para as APNFDs, mas renumerou-as e substituiu a Recomendação 12 por 22 e a Recomendação 16 por 23. O GAFI recomenda que as APNFDs cumpram os requisitos específicos cobertos, especialmente na Recomendação Nº 22 – APNFDs: Devida diligência acerca do cliente – (antiga Recomendação 12), e na Recomendação Nº 23 – APNFDs: Outras medidas – (antiga Recomendação 16), os quais são definidos em outras Recomendações relacionadas no **Quadro 4**.

Quadro 4 – Recomendações que definem os requisitos das Recomendações Nº 22 e 23

Recomendações Nº 22 e 23	**Recomendações Nº 10, 11, 12, 15, 17, 18, 19, 20 e 21**
Recomendação Nº 22 – APNFDs: Devida diligência acerca do cliente	Recomendação Nº 10 – Devida diligência acerca do cliente
	Recomendação Nº 11 – Manutenção de registros
	Recomendação Nº 12 – Pessoas expostas politicamente
	Recomendação Nº 15 – Novas tecnologias
	Recomendação Nº 17 – Recursos a terceiros
Recomendação Nº 23 – APNFDs: Outras medidas	Recomendação Nº 18 – Controles internos e filiais e subsidiárias estrangeiras
	Recomendação Nº 19 – Países de alto risco
	Recomendação Nº 20 – Comunicação de operações suspeitas
	Recomendação Nº 21 – Revelação (*tipping-off*) e confidencialidade

Fonte: GAFI (FATF, 2020a).

Na condição de entidades que relatam, deseja-se que as APNFDs tenham sistemas internos de combate à LD e ao FT, e que monitorem e comuniquem atividades suspeitas de LD e FT, por meio do cumprimento dos requisitos para: (i) realizar avaliação de risco; (ii) mitigar riscos; (iii) conduzir a devida diligência acerca do cliente (*customer due diligence*), que abrange a verificação da identidade do cliente, *know your customer* (KYC), "conheça seu cliente" na tradução livre, e identificação de proprietários beneficiários; (iv) manter registros adequados; e (v) registrar relatórios de transação suspeita para a Unidade de Inteligência Financeira (UIF). Traduzindo, assim, as obrigações de PLD e CTF em ações práticas e significativas que alcancem a conformidade com PLD e CFT e abordem sistematicamente as obrigações de *compliance* (GIKONYO, 2018; JEANS, 2019; GICHUKI, 2021; NDUKA; SECHAP, 2021).

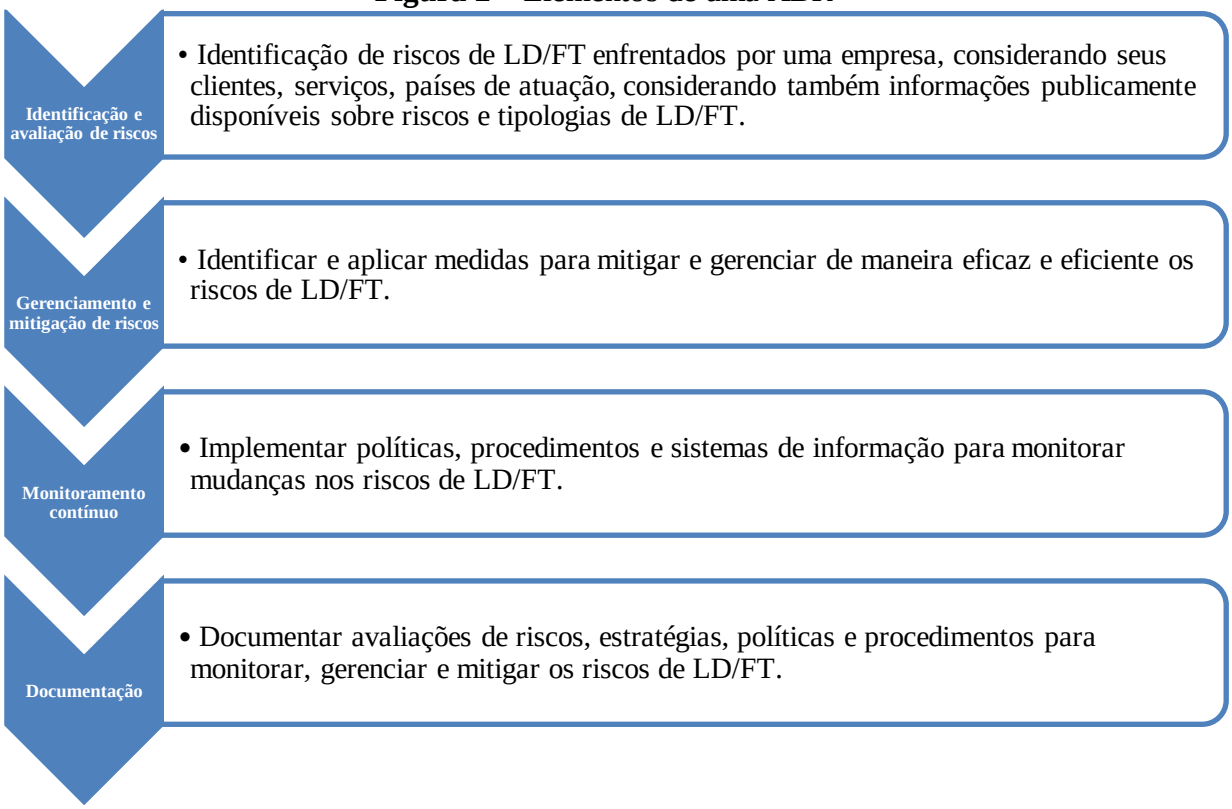
Nesse contexto, a ABR torna-se fundamental para a implementação eficaz dos Padrões Internacionais de Combate à LD e ao FT e da Proliferação definidos pelo GAFI, delegando, segundo Jakobi (2018), para as profissões, a avaliação para determinar se existe ou não motivos razoáveis que sustentem a suspeita de determinada transação, enquanto os regulamentos apenas descrevem os riscos potenciais.

No entanto, para Omar e Johari (2015), a baixa conformidade das APNFDs com as Recomendações do GAFI, está diretamente relacionada à falta de conhecimento ou a não aplicação da lei por parte dos reguladores.

Essa baixa conformidade pode ser comprovada no estudo de Molla Imeny *et al*. (2021) sobre as expectativas dos auditores na detecção e denúncia de LD no Irã, cujos resultados apontaram para uma ausência de alinhamento entre a percepção dos auditores em relação aos deveres investigativos e as expectativas do GAFI.

Como APNFDs, os profissionais da contabilidade devem seguir uma ABR para mitigar os riscos de LD. Significa que os profissionais da contabilidade devem tomar as medidas apropriadas para identificar e avaliar seus riscos de LD e implementar políticas, controles e procedimentos que lhes permitam gerenciar e mitigar efetivamente os riscos que foram identificados, levando em consideração as estruturas legais, regulamentares e de supervisão nacionais aplicáveis (FATF, 2019a). Na **Figura 2** é apresentado um resumo dos principais elementos de uma ABR.

Figura 2 – Elementos de uma ABR



Fonte: GAFI (FATF, 2019a, p. 14).

Para tomar as medidas adequadas para identificar e avaliar os principais riscos de LD que sua empresa enfrenta, os profissionais da contabilidade devem considerar as áreas do seu negócio que são mais vulneráveis de serem utilizadas por criminosos na condução de atividades de LD.

Segundo o GAFI, os riscos de LD podem ser organizados em três categorias: (i) Risco país/geográfico; (ii) Risco de cliente; e (iii) Risco de transação/serviços e canal de entrega associado (FATF, 2019a, p. 22).

(i) **Risco país/geográfico**: Clientes, transações, produtos e serviços entregues ou disponíveis em certas jurisdições podem representar um nível maior de risco de LD do que outras. Ao procurar identificar até que ponto uma jurisdição pode representar um alto risco de LD, os profissionais da contabilidade precisam considerar questões como ambiente político, ambiente jurídico, estrutura econômica, cultura, padrões de governança, dentre outras, fazendo uso de informações publicamente disponíveis sobre o risco de LD de uma determinada jurisdição, como informações publicadas por organizações da sociedade civil ou análises de avaliação mútua do GAFI (SATHYE; ISLAM, 2011; FATF, 2019a; IFAC, 2020a).

(ii) **Risco de cliente**: Certos tipos de clientes podem representar maior risco do que outros. Os profissionais da contabilidade devem aplicar as medidas de *customer due diligence* (CDD) para identificar e qualificar adequadamente os clientes e a identificação dos verdadeiros beneficiários da transação, bem como obter o entendimento da fonte de recursos e da riqueza desses clientes, seus proprietários e o objetivo da transação. O conhecimento sobre os clientes e seus negócios se desenvolverá ao longo de um relacionamento profissional interativo e de longo prazo, o que permitirá determinar o nível de risco de LD desses clientes. No entanto, os relacionamentos com clientes de curto prazo precisam ser considerados, uma vez que os riscos apresentados podem ser de alto risco de LD, apesar da sua natureza de baixo risco de LD (FATF, 2019a; IFAC, 2020a).

(iii) **Risco de transação/serviços e canal de entrega associado**: Algumas transações, produtos e serviços oferecidos podem apresentar maiores oportunidades de serem usados para LD em comparação com outros. Os profissionais da contabilidade precisam conhecer a natureza exata de seu negócio e entender como esse negócio pode facilitar a circulação ou a ocultação do produto do crime de LD. Devem realizar um balanço das atividades do seu negócio, seus recursos e o potencial de exploração por criminosos na LD. Entende-se que as transações, produtos e serviços que são fornecidos pessoalmente apresentem um risco menor em comparação com os fornecidos *online* (SATHYE; ISLAM, 2011; FATF, 2019a).

Essas categorias de risco de LD devem servir de base para os profissionais da contabilidade realizarem a avaliação do risco de LD, que deverá ser documentada, uma vez que, os procedimentos para monitoramento e revisão contínuos do perfil de risco do cliente serão realizados por meio da devida diligência em andamento no relacionamento comercial, conhecida como diligência contínua acerca do cliente, que possibilitará que os documentos, dados ou informações coletadas no processo de CDD sejam mantidos atualizados e relevantes, facilitando, também, o arquivamento preciso de relatórios de transações suspeitas (RTSs) para

a UIF, ou para responder a solicitações de informações de uma UIF e das agências policiais (FATF, 2019a).

A conformidade do regime AML de um país com as Recomendações do GAFI para as APNFDS tem sido tema de estudo de diferentes pesquisadores. Choo (2014) revisou os Relatórios de Avaliação Mútua do GAFI para 15 jurisdições, incluindo o Brasil, cujo Relatório de Avaliação Mútua foi publicado em junho de 2010. O autor constatou um expressivo número de jurisdições avaliadas com conformidade ausente ou parcial em relação às Recomendações para as APNFDs. No entanto, no Brasil, as obrigações AML/CFT se aplicavam a dois tipos de APNFDS: (i) Corretoras imobiliárias; e (ii) Comerciantes de metais e pedras preciosas (FATF, 2010, p. 195). Omar *et al*. (2015) ao examinarem o cumprimento das Recomendações do GAFI na legislação nacional de dez países do Sudeste Asiático em relação às APNFDs, verificaram que muitos países ainda não tinham implementado uma legislação relevante para as APNFDs. O estudo de Newbury (2017) ao procurar identificar as vulnerabilidades no regime AML da Austrália por meio da não conformidade da Austrália com as Recomendações do GAFI sobre a regulamentação das APNFDs, destaca que a não inclusão de muitos setores das APNFDs da regulamentação AML mantem as vulnerabilidades dentro do regime AML da Austrália. Mediante os Relatórios de Avaliação Mútua dos países da região da África Ocidental apontarem uma fraca implementação das medidas AML pelas APNFDs em comparação com as IFs, Nduka e Sechap (2021) examinaram como os países da Comunidade Econômica dos Estados da África Ocidental poderiam melhorar seu desempenho durante a avaliação mútua. Os autores constataram que o risco de LD associado às APNFDs é geralmente identificado como alto nesses países e que o foco da assistência técnica AML tem sido mais em IFs do que em APNFDs.

A percepção das APNFDs sobre os requisitos AML, também têm sido objeto de estudo dos pesquisadores. Vás e Sales (2015) analisaram a percepção dos profissionais da contabilidade sobre os requisitos AML no Brasil presentes na Lei nº 9.613 de 1998, atualizada pela Lei nº 12.683 de 2012, e na Resolução CFC nº 1.445 de 2013, substituída pela Resolução CFC nº 1.530 de 2017. Os autores verificaram uma ampla desinformação sobre o assunto, sendo que alguns participantes não sabiam da existência dessas normas. Contudo, no estudo de Da Rocha Alves *et al*. (2019), cerca de 89% dos participantes entendem como importante o conhecimento a respeito do que é determinado na Resolução CFC nº 1.530 de 2017. Nesse contexto, Telles (2021) entende que o profissional da contabilidade, como parte do mecanismo de PCLD, deve compreender seus riscos e reponsabilidades.

Corroborando para esse entendimento, no estudo realizado por Da Rocha Alves *et al*. (2019), a maioria dos participantes (70%) têm expressiva percepção acerca da importância da Contabilidade como instrumento de PCLD, bem como nos estudos de Neves Júnior e Moreira (2011) e Ribeiro *et al*. (2016), onde foi comprovada a importância da Perícia Contábil e da Contabilidade Forense na PCLD. Neves Júnior e Moreira (2011), ao estudarem sobre a possiblidade da Perícia Contábil, materializada em Laudos Periciais, surgir como importante ferramenta de Inteligência na PCLD, verificaram que, na percepção dos investigadores da área de Inteligência Policial, a Perícia Contábil, no limite de suas atribuições, é um relevante meio de prova para a solução de controvérsias relativas ao crime organizado. Também, o estudo de Ribeiro *et al*. (2016) permitiu concluir que a Contabilidade Forense é percebida pelos profissionais ligados ao combate à LD como um componente relevante no combate à LD e na produção de provas no processo investigatório das organizações criminosas. No entanto, Carneiro *et al*. (2016) e Ribeiro *et al*. (2016) concluíram que a Contabilidade Forense pode ser considera como um ramo de conhecimento novo dentro do arcabouço contábil, fazendo-se necessário um aprofundamento.

2.7 CRIPTOMOEDAS E A LAVAGEM DE DINHEIRO

O processo de LD é complexo e complicado, uma vez que envolve uma série de transações para disfarçar a origem criminosa dos ativos financeiros, permitindo o uso desses ativos sem comprometer os criminosos. Com o advento da Internet, os sistemas financeiros tonaram-se mais eficientes, facilitando o comércio legítimo, mas, também, permitiu que criminosos operassem transferências de milhões de dólares instantaneamente usando computadores pessoais, fazendo com que o processo de LD migrasse para o mundo digital (McDOWELL, 2001; ALBRECHT *et al*., 2019).

Apesar das diferentes atitudes em relação às criptomoedas, como desde o completo desinteresse de seu potencial e benefícios, seu uso com finalidades legítimas, como investimento ou pagamento de bens e serviços, até a adoração total como uma oportunidade para a libertação do controle financeiro do Governo, as agências de aplicação da lei em todo o mundo identificaram o uso de criptomoedas nos crimes de LD (DYNTU; DYKYI, 2018; KEATINGE; CARLISLE; KEEN, 2018; DUPUIS; GLEASON, 2020). Segundo Grauer *et al*. (2023), o valor total de criptomoedas utilizadas no crime de LD em 2022 foi de aproximadamente US$ 23,8 bilhões, com origem em endereços ilícitos, representando um aumento de 68% em relação a 2021.

Com objetivo de estudar os fatores socioeconômicos e institucionais relacionados a potenciais motivadores de interesse no desenvolvimento de criptomoedas, Saiedi, Broström e Ruiz (2021) conseguiram evidenciar que a adoção da criptomoeda *bitcoin* é maior onde o risco de LD relacionado ao comércio de drogas ilegais é maior, assim como onde as percepções do estado de direito são mais fortes. Os autores explicam que o desejo dos usuários de se envolver em atividades ilícitas em países onde as percepções sobre a capacidade e qualidade dos órgãos governamentais são positivas, faz com que esses usuários recorram ao comércio *on-line* como meio mais seguro de adquirir drogas ilegais.

Procurando quantificar e caracterizar o comércio ilegal facilitado pelas criptomoedas, o estudo realizado por Foley, Karlsen e Putniņš (2019), traçou o perfil dos usuários de *bitcoin* legais e ilegais em conformidade com um conjunto de características. Os dados foram coletados por meio da extração do registro completo das transações com *bitcoin* de sua *blockchain* pública, desde o primeiro bloco em 2009 até abril de 2017. Os pesquisadores descobriam que aproximadamente 26% de todos os usuários e 46% das transações com *bitcoin* estão associadas a atividades ilegais, evidenciando que as criptomoedas estão tendo um impacto material na forma como o mercado negro de bens e serviços ilegais opera.

Na medida em que certas características das criptomoedas, como seu forte potencial para transações anônimas ou pseudoanônimas e os serviços especializados no anonimato são usados na LD com criptomoedas na *darknet*, os estudos de van Wegberg, Oerlemans e van Deventer (2018) e Albrecht *et al*. (2019) discutem a eficiência dessa característica e serviços, e como esses serviços estão se tornando disponível para um público mais amplo. O estudo de van Wegberg, Oerlemans e van Deventer (2018) concluiu que a LD usando *bitcoin* é um conceito praticamente concebível e guarda muita semelhança para ser integrado em esquemas de LD atuais e futuros. Da mesma forma, Albrecht *et al*. (2019) concluíram que o uso das criptomoedas na LD pode trazer implicações generalizadas nas economias de todo o mundo, uma vez que elas, ao eliminar a necessidade de IFs intermediárias, permitem transações financeiras ponto a ponto. Os autores entendem que a possibilidade de anonimato fez com que as criptomoedas fossem aceitas pela *darknet* e outras redes criminosas.

Por conseguinte, o trabalho de Möser, Böhme e Breuker (2013) realizou uma análise sistemática em alguns anonimizadores de transações com base no gráfico de transações extraído da cadeia de blocos no ecossistema *Bitcoin*. Os pesquisadores perceberam como improvável que o princípio *Know Your Customer* (KYC) possa ser aplicado no sistema *Bitcoin*.

No entanto, Turner, McCombie e Uhlmann (2020), ao discutirem as abordagens técnicas de *machine learning* (aprendizado de máquina, na tradução livre) quanto as considerações não técnicas, legais e de governança, enfatizam que as medidas de KYC e CDD associadas ao surgimento do *machine learning* e sua aplicação a gráficos formados pelas transações e endereços na rede *Bitcoin*, são fundamentais no combate ao crime de LD. Mas, os autores entendem que as diferentes aplicações de medidas de AML nas jurisdições podem atrapalhar o combate a anonimização e a atribuição ao mundo real de identidades virtuais no ecossistema das criptomoedas. Igualmente, os trabalhos de Irwin e Turner (2018) e Turner e Irwin (2018), evidenciaram que além de uma arquitetura de *machine learning* e inteligência artificial, o ideal seria a aplicação de medidas que permitissem uma abordagem preventiva por parte de todos os atores envolvidos na PCLD, e o compartilhamento de informações entre várias partes interessadas na aplicação da lei, Unidades de Inteligência Financeira (UIFs), organizações de segurança cibernética e indústria *fintech*. Kethineni e Cao (2019) destacam a necessidade de desenvolver avaliações monetárias, legais, regulatórias e de risco tanto no ambiente doméstico quanto internacional, entendendo que a ausência de uma regulação uniforme, nacional e internacional, representa um risco significativo para o setor financeiro e incentiva, dentre outras atividades ilegais, a LD com criptomoedas.

3 METODOLOGIA

Considerando o objetivo do presente estudo de identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro, são utilizadas as orientações para uma abordagem baseada em risco (ABR) relativamente à profissão contábil elaboradas pelo GAFI (FAFT, 2019a), e aplicação de questionário junto aos profissionais com experiência na prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT) e experiência com criptoativos. O resultado encontrado serve de auxílio na prevenção e combate à lavagem de dinheiro (PCLD).

Na presente etapa da pesquisa, torna-se necessário apresentar os detalhes da metodologia adotada, pois segundo Kothari (2004, p. 8, grifo do autor, tradução nossa):

> *Assim, quando falamos de metodologia de pesquisa, não falamos apenas dos métodos de pesquisa, mas também consideramos a lógica por trás dos métodos que usamos no contexto de nosso estudo de pesquisa e explicamos porque estamos usando um método ou técnica particular e porque não estamos usando outros para que os resultados da pesquisa possam ser avaliados pelo próprio pesquisador ou por terceiros*.[12]

A definição adequada da metodologia adotada é fundamental para a compreensão dos procedimentos e técnicas que o pesquisador entendeu como apropriados para alcançar todos os objetivos propostos de acordo com o tema abordado. Gil (2008, p. 8) explica o método científico como sendo o conjunto de procedimentos cognitivos e técnicos adotados no processo para se alcançar o conhecimento, que só será considerado científico quando viável a identificação dos procedimentos que possibilitam a sua verificação. Portanto, a seguir será apresentado o tipo de pesquisa, os procedimentos adotados para seleção dos participantes da pesquisa, assim como a descrição do instrumento de coleta de dados, os procedimentos de coleta e as etapas da análise dos dados, e por fim as limitações da pesquisa.

3.1 TIPO DE PESQUISA

Em relação aos objetivos este estudo pode ser definido como de caráter exploratório e descritivo, pois o tema escolhido, a utilização dos criptoativos nos crimes de lavagem de dinheiro (LD), é um tema bastante complexo.

---

[12] "*Thus, when we talk of research methodology we not only talk of the research methods but also consider the logic behind the methods we use in the context of our research study and explain why we are using a particular method or technique and why we are not using others so that research results are capable of being evaluated either by the researcher himself or by others*."

Segundo Raupp e Beuren (2013), a caracterização do estudo como exploratório geralmente ocorre quando há pouco conhecimento sobre a temática a ser abordada. Conforme Gil (2008), a pesquisa exploratória é desenvolvida no sentido de proporcionar uma visão geral acerca de determinado fato, quando o tema escolhido é pouco explorado. Para Leavy (2017), quando se tem um tópico novo ou relativamente pouco pesquisado, a pesquisa exploratória é uma forma de preencher uma lacuna no conhecimento sobre esse tópico, ou de abordar o tópico de uma perspectiva diferente para gerar percepções novas e emergentes.

O caráter descritivo do estudo, segundo Gil (2008), está no objetivo de descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre as variáveis. Conforme Kothari (2004), os estudos descritivos têm como objetivo retratar com precisão as características de uma determinada situação ou grupo. Para Leavy (2017), quando se deseja descrever grupos, atividades, eventos ou situações, a pesquisa descritiva é apropriada.

O estudo segue abordagem qualitativa que, segundo Godoy (1995a), parece ser mais adequada quando a pesquisa é de cunho exploratório, onde os temas são pouco conhecidos, ou de caráter descritivo, cujo objetivo é a busca do entendimento do fenômeno como um todo, na sua complexidade. Godoy (1995b) caracteriza os estudos com abordagens qualitativas como estudos cujo objetivo é o entendimento do fenômeno como um todo, no contexto em que ocorre e do qual é parte, com sua "captura" a partir da perspectiva das pessoas nele envolvidas, onde vários dados são coletados e analisados para que se entenda a sua dinâmica.

Por conseguinte, Sutton e Austin (2015) explicam que a pesquisa qualitativa pode ajudar no acesso aos pensamentos e sentimentos dos participantes da pesquisa, permitindo o desenvolvimento de uma compreensão do significado que as pessoas atribuem às suas experiências. Seu objetivo, de acordo com Moser e Korstjens (2017), está em fornecer percepções aprofundadas e compreensão de problemas do mundo real, envolvendo, segundo Hammarberg, Kirkman e De Lacey (2016), a coleta sistemática, organização, descrição e interpretação de dados textuais, verbais ou visuais.

Quanto aos procedimentos adotados, esta pesquisa é caracterizada como uma pesquisa bibliográfica e documental.

A pesquisa bibliográfica é um estudo sistematizado desenvolvido a partir de material já publicado, constituído principalmente de livros e artigos científicos (VERGARA, 1998; GIL, 2008). Devido sua natureza teórica, que permite o conhecimento sobre a produção científica existente, a pesquisa bibliográfica é parte obrigatória em praticamente todos os outros tipos de estudos (RAUPP; BEUREN, 2013).

A pesquisa documental é constituída pelo exame de materiais de natureza diversa, que ainda não foram analisados, ou que possibilitem um reexame, na busca de informações novas e/ou complementares (GODOY, 1995b). Seu objetivo está em selecionar, tratar e interpretar a informação bruta, de onde se pretende extrair algum sentido e introduzir algum valor, trazendo, assim, uma possível contribuição para a comunidade científica com o intuito de permitir que outros possam realizar o mesmo procedimento no futuro (RAUPP; BEUREN, 2013). A principal diferença entre a pesquisa bibliográfica e a pesquisa documental está na natureza das fontes. A pesquisa bibliográfica utiliza-se basicamente das contribuições de diferentes autores a respeito de determinado tema, atentando para as fontes secundárias, enquanto a pesquisa documental recorre a materiais que ainda não receberam tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetivos da pesquisa, ou seja, as fontes primárias (GIL, 2008; SÁ-SILVA; ALMEIDA; GUINDANI, 2009; RAUPP; BEUREN, 2013).

Para fins de pesquisa científica, são aceitos como documento qualquer material que forneça informações sobre um determinado fato ou fenômeno social e que exista independentemente das ações do pesquisador, podendo incluir materiais escritos (diários, autobiografias, obras literárias, científicas e técnicas, atos do Parlamento, sentenças judiciais, balanços patrimoniais da empresa, entre outros), as estatísticas (que produzem um registro ordenado e regular de vários aspectos da vida de determinada sociedade) e elementos iconográficos (sinais, grafismo, imagens, fotografias, filmes, entre outros). Sua produção procura atender outros fins que não a pesquisa social, onde são considerados como “primários” aqueles que não receberam quaisquer tratamentos analíticos (cartas, revistas, documentos oficiais, artigos de jornal, contratos, gravações, entre outros), ou “secundários” aqueles que de alguma forma já foram analisados (relatórios de pesquisa, relatórios de empresas, tabelas estatísticas, entre outros), mas que podem ser utilizados pelo pesquisador para fins cognitivos (GODOY, 1995b; CORBETTA, 2003; GIL, 2008).

Foi utilizada a análise de conteúdo, que segundo Franco (2008), é um procedimento de pesquisa que tem a mensagem como ponto de partida, podendo esta ser verbal (oral ou escrita), gestual, silenciosa, figurativa, documental ou diretamente provocada, cuja expressão de significado e sentido se faz necessária. O termo “análise de conteúdo” designa:

> *Um conjunto de técnicas de análise das comunicações visando obter, por procedimentos, sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens* (BARDIN, 1977, p. 42, grifo do autor).

Nesse sentido, Colauto e Beuren (2013) explicam que a análise de conteúdo é um método de análise de dados cujo objetivo está em estudar as comunicações entre os homens, com maior ênfase no conteúdo das mensagens, privilegiando os dados qualitativos, ainda que aplicado na abordagem quantitativa.

Diante da possibilidade de aplicação da análise de conteúdo tanto para estudos qualitativos como para estudos quantitativos, torna-se importante a contribuição de Bauer e Gaskell (2002, p. 24), que entendem como incorreto o fato de se assumir que a pesquisa qualitativa possui o monopólio da interpretação, assim como assumir que a pesquisa quantitativa chega a suas conclusões quase que automaticamente, sem a necessidade de interpretação, sinalizando, assim, a necessidade de complementação entre os estudos.

3.2 PARTICIPANTES DA PESQUISA

A presente seção tem como objetivo expor os procedimentos adotados para a seleção de possíveis participantes da pesquisa. São discutidas as três etapas de contatos dessa seleção.

3.2.1 Primeira etapa de contatos para seleção de possíveis participantes da pesquisa

Para Gaskell (2002), a finalidade real da pesquisa qualitativa não é contar opiniões ou pessoas, mas explorar o espectro de opiniões, as diferentes representações sobre o assunto em questão. Dessa forma, a seleção de possíveis participantes considera a amostragem intencional, onde os participantes são selecionados devido a algumas características predeterminadas pelo pesquisador antes do estudo (STOCKEMER, 2019, p. 63).

Neste sentido, em primeiro momento, os participantes da pesquisa deveriam ser profissionais com formação acadêmica em Ciências Contábeis, com experiência na prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT) e experiência com criptoativos.

Levando em consideração as características predeterminadas dos possíveis participantes da pesquisa, em 02/2021, com o objetivo de iniciar o processo de levantamento dos participantes da pesquisa, foram realizados os primeiros contatos com as entidades profissionais de contabilidade e organizações com ações de pesquisa e desenvolvimento e/ou prestações de serviços voltados à prevenção e combate do crime de LD.

Nos **Quadro 5** e **Quadro 6** são apresentadas, respectivamente, a relação das entidades profissionais de contabilidade e as organizações, onde foram realizados os primeiros contatos para levantamento dos possíveis participantes da pesquisa.

Quadro 5 – Relação das entidades profissionais de contabilidade

Entidade profissional de contabilidade	Meio de contato
Associação dos Peritos Judiciais do Estado do Rio de Janeiro (APJERJ)	Telefone
Conselho Regional de Contabilidade do Estado do Rio de Janeiro (CRC-RJ)	Telefone e *e-mail*
Federação Nacional das Empresas de Serviços Contábeis e das Empresas de Assessoramento, Perícias, Informações e Pesquisas (FENACON)	Telefone e *e-mail*
Instituto dos Auditores Independentes do Brasil (IBRACON)	Telefone
Sindicato das Empresas de Serviços Contábeis, Assessoramento, Perícias, Informações e Pesquisa do Estado do Rio de Janeiro (SESCON)	Telefone e *e-mail*
União dos Profissionais e Escritórios de Contabilidade do Estado do Rio de Janeiro (UNIPEC-RJ)	Telefone e *e-mail*

Fonte: Elaborado pelo autor.

Quadro 6 – Relação das organizações com ações de pesquisa e desenvolvimento e/ou prestações de serviços voltados à prevenção e combate do crime de lavagem de dinheiro

Organização	Meio de contato
Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA)	Telefone e *e-mail*
Conselho de Controle de Atividades Financeiras (COAF)	Telefone e *e-mail*
Deloitte Brasil	Canal institucional
Ernst & Young Brasil	Canal institucional
Instituto de Criminalista Carlos Éboli (ICCE) – Centro de Estudos	Telefone e *e-mail*
KPMG Brasil	Canal institucional
Ministério Público do Estado do Rio de Janeiro (MP-RJ) – Divisão de Laboratório de CLD e Corrupção	Telefone
PWC Brasil	Canal institucional

Fonte: Elaborado pelo autor.

Dentre as entidades profissionais da contabilidade e organizações presentes nos **Quadro 5** e **Quadro 6**, somente no Centro de Estudos do Instituto de Criminalista Carlos Éboli (ICCE) foi possível prosseguir no processo de contato com profissional que atendesse as características predeterminadas para o possível participante da pesquisa.

Na data de 23/02/2021 foi enviado um *e-mail* para o Centro de Estudos do ICCE com informações sobre a pesquisa e arquivos anexos com a Declaração de situação acadêmica do pesquisador e cópia do projeto apresentado no Exame de Qualificação.

Em 02/03/2021 o *e-mail* com a confirmação do recebimento dos documentos foi enviado. No dia seguinte, 03/03/2021, outro *e-mail* da parte do Centro de Estudos do ICCE informava que o projeto havia sido encaminhado ao Perito Chefe do Serviço de Perícia Contábil, informando, ainda, o seu contato telefônico para maiores detalhes e entendimento.

3.2.2 Segunda etapa de contatos para seleção de possíveis participantes da pesquisa

Como a presente pesquisa é de caráter exploratório, ocorreram mudanças que refletiram no andamento da seleção de possíveis participantes da pesquisa. O público-alvo, que era somente os profissionais com formação acadêmica em Ciências Contábeis, passou a abranger, também, profissionais com diferentes áreas de formação acadêmica. Assim, os participantes da pesquisa deveriam ter experiência na prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT) e experiência com criptoativos, sendo desejável, mas não obrigatório, que o participante tenha formação acadêmica em Ciências Contábeis.

Tal mudança deu-se em decorrência do Brasil, como membro do GAFI, estar comprometido em atender as 40 Recomendações e submeter-se a avaliações mútuas realizadas pelo GAFI. As 40 Recomendações do GAFI definem as medidas essenciais que os países devem adotar para o combate da LD e do FT, entre outras medidas (FAFT, 2020b).

Nessa direção, todas as organizações participantes do mercado de valores mobiliários no Brasil estão reguladas pela Instrução CVM nº 617, de 5 de dezembro de 2019, que dispõe sobre a PLD-FT no âmbito do mercado de valores mobiliários (CVM, 2019).

No âmbito do sistema financeiro, a Circular nº 3.978 de 2020 emitida pelo BCB dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo BCB visando à prevenção da utilização do sistema financeiro para a prática dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998 (BCB, 2020).

Em linha com anteriormente exposto, a Resolução CFC nº 1.530 de 2017, emitida pelo CFC, dispõe sobre os procedimentos a serem observados pelos profissionais e organizações contábeis para cumprimento das obrigações previstas na Lei nº 9.613/1998 e alterações posteriores (CFC, 2017).

A Resolução COAF nº 36 de março 2021, emitida pelo COAF, disciplina a forma de adoção de políticas, procedimentos e controles internos de PLD-FT que permitam o atendimento ao disposto nos artigos 10 e 11 da Lei nº 9.613 de 1998, por aqueles que se sujeitam, nos termos do seu artigo 14, § 1º, à supervisão do COAF (COAF, 2021a).

Dentro desse contexto, os profissionais com experiência na PLD-FT e experiência com criptoativos, sejam profissionais da contabilidade ou com outra formação acadêmica, tornam-se potenciais possíveis participantes da pesquisa.

Entendeu-se, ainda, que as organizações para contato dos seus respectivos profissionais deveriam ser instituições que forneçam ao menos uma das seguintes prestações de serviços

voltados aos fundos de investimentos em criptoativos autorizados pela CVM: i) administração; ii) gestão; iii) distribuição; iv) custódia; ou v) controle de ativos e passivos.

Esse entendimento justifica-se pelo fato de a CVM publicar, em setembro de 2018, o Ofício Circular nº 11/2018/CVM/SIN[13] dirigido aos administradores e gestores de fundos de investimentos regulados pela Instrução CVM nº 555, cujo assunto refere-se ao investimento indireto em criptoativos pelos fundos de investimentos, com o objetivo de complementar o Ofício Circular nº 1/2018/CVM/SIN, trazendo o seguinte esclarecimento:

> A Instrução CVM nº 555, em seu artigo 98 e seguintes, ao tratar do investimento no exterior, autoriza o investimento indireto em criptoativos por meio, por exemplo, da aquisição de cotas de fundos e derivativos, entre outros ativos negociados em terceiras jurisdições, desde que admitidos e regulamentados naqueles mercados. No entanto, no cumprimento dos deveres que lhe são impostos pela regulamentação, cabe aos administradores, gestores e auditores independentes observar determinadas diligências na aquisição desses ativos (CVM, 2018b).

Essa manifestação por parte da CVM trouxe a possibilidade de investimentos, de forma indireta, em criptoativos pelos fundos de investimentos no Brasil.

Assim sendo, no **Quadro 7** está a relação dos fundos de investimentos em criptoativos existentes no Brasil que foram autorizados pela CVM.

Quadro 7 – Relação dos fundos de investimentos em criptoativos no Brasil

Fundos
BLP CRIPTOATIVOS FIM
BLP CRYPTO ASSETS FIM IE
BOHR ARBITRAGE CRIPTO FIM IE
HASHDEX 20 NASDAQ CRYPTO INDEX FIC FIM
HASHDEX 40 NASDAQ CRYPTO INDEX FIC FIM
HASHDEX 100 NASDAQ CRYPTO INDEX FIM IE
HASHDEX BITCOIN FULL 100 FIC FIM IE
HASHDEX BITCOIN I FIM IE
HASHDEX CRIPTOATIVOS I FIM
HASHDEX CRIPTOATIVOS II FIM
HASHDEX OURO BITCOIN RISK PARITY FIC FIM
QR BLOCKCHAIN ASSETS FIM IE
QR BTC MAX FIM IE
VITREO CRIPTO DEFI FIC FIM IE
VITREO CRIPTO METALS BLEND FIC FIM
VITREO CRIPTOMOEDAS FIC FIM IE
VTR QR CRIPTO FIM IE

Fonte: Gusson (2021).

[13] Superintendência de Supervisão de Investidores Institucionais (SIN).

Por meio de consultas realizadas no *site* da Associação Brasileira das Entidades do Mercado Financeiro (ANBIMA) foi possível identificar as instituições que atuam como administradores, gestores, distribuidores, custodiantes, controladores de ativos e passivos dos fundos presentes no **Quadro 7**.

Posteriormente, nos *sites* dos gestores dos fundos, foi possível ampliar a lista de distribuidores dos fundos, resultando em 30 instituições atuantes junto aos fundos de investimentos com exposição em criptoativos.

Na data de 04/2021 iniciou-se uma nova etapa de contatos, dessa vez, com as instituições atuantes junto aos fundos de investimentos em criptoativos no Brasil.

O **Quadro 8** apresenta a relação das 21 instituições contactadas por meio de *e-mail* ou canal institucional.

Quadro 8 – Relação das instituições dos fundos de investimentos em criptoativos no Brasil

Instituição	Meio de contato
A5 Gestão de Investimentos LTDA	*E-mail*
Ativa Investimentos	Canal institucional
Azimut Brasil Wealth Management LTDA	*E-mail*
Banco BS2	Canal institucional
Banco BTG Pactual S/A	Canal institucional
BLP Gestora de Recursos LTDA	Canal institucional
Brasil Plural S.A. Banco Múltiplo	*E-mail*
Consulenza Investimentos	Canal institucional
Easynvest - Título Corretora de Valores S/A	Canal institucional
Guide Investimentos S/A Corretora de Valores	*E-mail*
Hashdex Gestora de Recursos Ltda	*E-mail*
Modal Distribuidora de Títulos e Valores Mobiliários Ltda	Canal institucional
MyCAP Investimentos	*E-mail*
Necton Investimentos S.A. Corretora de Valores Mobiliários e Commodities	Canal institucional
Nova Futura Investimentos	Canal institucional
Órama Distribuidora de Títulos e Valores Mobiliários S.A.	Canal institucional
Planner Corretora de Valores S/A	*E-mail*
QR Capital Gestora de Recursos Ltda	Canal institucional
RB Capital Distribuidor de Títulos e Valores Mobiliários Ltda	Canal institucional
Vitreo Gestão de Recursos Ltda	*E-mail*
Warren Corretora de Valores Mobiliários e Cambio Ltda	Canal institucional

Fonte: Elaborado pelo autor.

Dentre as instituições presentes no **Quadro 8**, em nenhuma delas foi possível contato com profissional que atendesse as características predeterminadas para possível participante da pesquisa.

3.2.3 Terceira etapa de contatos para seleção de possíveis participantes da pesquisa

Por fim, uma terceira etapa de contatos para seleção de possíveis participantes da pesquisa foi iniciada, ainda na data de 04/2021. Nessa etapa foram realizados contatos com profissionais via plataforma *LinkedIn*, com base na avaliação do perfil do profissional por parte do pesquisador.

A justificativa para a utilização da rede social de negócios *LinkedIn* está na possibilidade de *networking* profissional e desenvolvimento de carreira, onde as pessoas podem fazer conexões de negócios, compartilhar suas experiências e currículos e encontrar empregos. Para López-Carril, Anagnostopoulos e Parganas (2020) uma ferramenta de mídia social como o *LinkedIn* parece ser a opção ideal para *networking* e busca de informações relacionadas ao emprego. Segundo Caers e Castelyns (2011), o *site* de rede social *LinkedIn* se tornou uma ferramenta extra para recrutar candidatos, para encontrar informações adicionais sobre eles e para decidir quem será convidado para uma entrevista. Bradbury (2011) explica que por meio do recurso de pesquisa do *LinkedIn* é possível encontrar pessoas com base em diversos critérios, como pesquisar pessoas que trabalham (ou que já trabalharam) em uma organização específica e/ou setores específicos.

Por consequência, o presente estudo utilizou o *LinkedIn* como ferramenta para encontrar possíveis participantes da pesquisa, verificando, por meio do recurso de pesquisa do *LinkedIn*, profissionais que trabalham (ou que já trabalharam) nas organizações presentes nos **Quadro 5**, **Quadro 6** e **Quadro 8**, assim como nos diferentes segmentos do setor de serviços ou órgão da Administração Pública, como escritórios de advocacia, escritórios de contabilidade, *exchange* de criptoativos, instituições financeiras (IFs), instituições de pesquisa, BCB, CVM, RFB, MPF, PF, entres outras organizações cuja atividade esteja de alguma forma relacionada aos criptoativos, conforme Rodrigues e Kurtz (2019, APÊNDICE B), ou seja: i) envolvimento no fornecimento, troca, transferência, gestão e/ou custódia de criptoativos; ii) participação e/ou prestação de serviços financeiros relacionados com a emissão e/ou venda de criptoativos para ou em nome de outra pessoa física ou jurídica no contexto de uma relação comercial; iii) elaboração de instrumentos regulatórios específicos relativos aos provedores de serviços de criptoativos; e iv) iniciativas governamentais voltadas para a futura regulamentação e/ou monitoramento do ambiente de criptoativos, como grupos de trabalho, políticas públicas, projetos de lei, entre outros.

Para López-Carril, Anagnostopoulos e Parganas (2020), o perfil é provavelmente a seção mais importante para qualquer usuário do *LinkedIn*, pois é a imagem que o usuário projeta

para a comunidade mais ampla do *LinkedIn*. Bradbury (2011) explica que o perfil do *LinkedIn* é o ponto central para obter informações sobre uma pessoa, mesmo que ela não faça parte da rede de quem está realizando a pesquisa, uma vez que o perfil devidamente preenchido revela o cargo que ocupa, onde trabalha e onde estudou. Desse modo, o perfil do profissional selecionado está no profissional ter experiência em criptoativos e na PLD-FT, e trabalhar (ou ter trabalhado) em pelo menos uma das seguintes áreas: i) área de PLD-FT; ii) área de gerenciamento de riscos; iii) área de *compliance*; iv) área de controles internos; e/ou vi) área de auditoria.

Dentre as diferentes combinações de palavras-chave utilizadas durante toda a terceira etapa de contatos para seleção de possíveis participantes da pesquisa, as combinações "contador; *bitcoin*", "contador; BTC", "contador; criptomoedas", "contabilidade; *bitcoin*", "contabilidade; criptomoedas", "contabilidade; *cryptocurrency*", "contabilidade; criptomoedas; PLD" e "contabilidade; *blockchain*" foram as primeiras a serem aplicadas.

O contato foi realizado de forma individual, ou seja, um a um, via mensagem privada na plataforma *LinkedIn* na rede de contatos do pesquisador. A mensagem introdutória para o novo contato em potencial forneceu o contexto sobre o motivo pelo qual o pesquisador estava pedindo para se conectar com aquele profissional em particular. Após aceita a solicitação, era encaminhada uma nova mensagem onde era feito o pedido de cooperação. Ambas as mensagens se encontram no APÊNDICE C.

Após a realização de 3.131 convites para a rede de contatos do pesquisador na plataforma *LinkedIn*, 1.649 convites foram aceitos para a rede de contatos do pesquisador. Desses 1.649 novos contatos, 160 contatos aceitaram participar da pesquisa.

Em um segundo momento (2ª etapa), após evidenciar que entre os 1.649 novos contatos havia os que não se posicionaram a respeito de participar ou não da pesquisa, optou-se por incluir 1.136 contatos como possíveis participantes da pesquisa.

A **Tabela 1** apresenta a formação acadêmica dos possíveis participantes da pesquisa.

Tabela 1 – Formação acadêmica dos possíveis participantes

Formação acadêmica	Quantidade (1ª etapa)	Quantidade (2ª etapa)	Quantidade (Total)
Administração	23	256	279
Ciências Contábeis	51	346	397
Ciências Econômicas	15	90	105
Direito	48	212	260
Outra	23	232	255
Total	**160**	**1.136**	**1.296**

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio da **Tabela 1** é possível perceber a prevalência de possíveis participantes com formação acadêmica em Ciências Contábeis, sendo aproximadamente 31% (397/1.296) dos possíveis participantes da pesquisa.

Em vista da dificuldade em encontrar profissionais que tenham conhecimento de PLD-FT e criptoativos, a pesquisa manteve-se indefinida a respeito de aplicação de questionário e/ou entrevista. Mas tal indefinição foi superada após confirmação de um número superior a 30 possíveis participantes da pesquisa e a decisão do pesquisador em realizar somente a aplicação de questionário devido ao fato de poucos profissionais estarem à vontade em participar da pesquisa por meio de entrevista.

3.3 INSTRUMENTOS DE COLETA DE DADOS

Os instrumentos de coleta dos dados são a análise documental e questionário. Na análise documental, os dados analisados dizem respeito aos documentos de domínio público referentes às abordagens regulatórias e de supervisão emitidos por organizações nacionais e internacionais, a respeito das questões decorrentes dos criptoativos. Segundo Spink (2013) os documentos de domínio público são produtos sociais públicos, abertos eticamente para análise, podendo refletir as transformações lentas em posições e posturas institucionais assumidas pelos aparelhos simbólicos que permeiam o dia a dia, assim como no âmbito das redes sociais, pelos agrupamentos e coletivos que dão forma ao informal, refletindo o ir e vir de versões circulantes assumidas ou advogadas.

No questionário, o objetivo de sua aplicação é verificar a percepção dos profissionais que atuam na área PLD-FT acerca da utilização dos criptoativos no crime de lavagem de dinheiro, os riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos e as possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos.

Corbetta (2003, p. 117, tradução nossa) explica que:

> Embora a observação seja a maneira mais direta e imediata de estudar comportamentos manifestados abertamente, a única maneira de explorar a motivação, as atitudes, as crenças, os sentimentos, as percepções e as expectativas é perguntando.[14]

[14] "While observation is the most direct and immediate way of studying openly manifested behaviors, the only way we can explore motivation, attitudes, beliefs, feelings, perceptions and expectations is by asking."

De acordo com Stockemer (2019), em princípio, em uma pesquisa, um pesquisador pode fazer perguntas sobre o que as pessoas pensam, o que fazem, quais são os atributos que possuem e quanto conhecimento têm sobre um determinado assunto. Gil (2008) define questionário como uma técnica de investigação composta por um conjunto de questões que são submetidas às pessoas com o propósito de obter informações sobre conhecimentos, crenças, sentimentos, valores, expectativas, situações vivenciadas.

Segundo Colauto e Beuren (2013) as questões que compõe o questionário podem ser questões abertas e/ou questões fechadas, onde as questões abertas permitem à pessoa responder livremente, com suas próprias palavras, emitindo opiniões quando necessário, e as questões fechadas apresentam à pessoa um conjunto de alternativas de respostas para que seja selecionada a que melhor evidencia a situação ou ponto de vista da pessoa.

Conforme Stockemer (2019) os questionários podem ser abertos e fechados ou podem incluir uma mistura de perguntas abertas e fechadas.

3.3.1 Questionário

O questionário utilizado na pesquisa (APÊNDICE A) foi elaborado a partir de fontes distintas cuja análise está baseada nos Padrões Internacionais de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo e Proliferação – As Recomendações do GAFI (FATF, 2020a), conforme **Quadro 9**.

Quadro 9 – Referências relacionadas às perguntas 9 a 18 do questionário da pesquisa

Objetivo Geral	Objetivos Específicos	Perguntas	Referências	Análise	Autores
Identificar possíveis abordagens que auxiliem o profissional de contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro.				Análise baseada nos Padrões Internacionais de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo e Proliferação – As Recomendações do GAFI.	FATF (2020a)
	Identificar possíveis aplicações dos criptoativos nos crimes de lavagem de dinheiro.	9	CFC (2017, p.2); FATF (2018b, p.58); FATF (2019a, p.11); FINTRAC (2018)	**Recomendação 1: Avaliação de riscos e aplicação de uma abordagem baseada em risco**. A abordagem baseada em risco (ABR) é central para a implementação eficaz das Recomendações do GAFI. Significa que supervisores, instituições financeiras (IFs) e profissionais da contabilidade devem identificar, avaliar e compreender os riscos de lavagem de dinheiro (LD) aos	FATF (2020a); FATF (2019b)

				quais estão expostos e implementar as medidas de mitigação mais apropriadas (FATF, 2019a, p. 5, item 1).	
		10	FATF (2019a, p. 25)	**Recomendação 1: Avaliação de riscos e aplicação de uma abordagem baseada em risco**. Os riscos de LD podem ser organizados em três categorias: (a) risco país/geográfico, (b) risco de cliente e (c) transação/serviço e risco associado ao canal de entrega (FATF, 2019a, p. 22, item 61).	
		11	FATF (2020b, p. 5, 13, 15 e 17)	**Recomendação 1: Avaliação de riscos e aplicação de uma abordagem baseada em risco**. Os riscos e as bandeiras vermelhas listadas em cada categoria de risco não são exaustivos, mas fornecem um ponto de partida para os profissionais da contabilidade usarem ao projetar sua ABR (FATF, 2019a, p. 22, item 61).	
		12	FATF (2020b, p. 9)		
		13	FATF (2019a, p. 13)	**Recomendação 22: Atividades e Profissões Não-Financeiras Designadas (APNFDs): devida diligência acerca do cliente.** A intenção básica por trás das Recomendações do GAFI, no que se refere aos profissionais da contabilidade, é consistente com suas obrigações éticas como profissionais, ou seja, para evitar auxiliar criminosos ou facilitar atividades criminosas. Os requisitos da R.22 em relação à devida diligência acerca do cliente (CDD em inglês), manutenção de registros, Pessoas Expostas Politicamente (PEPs), novas tecnologias e dependência de terceiros estabelecidos nas R. 10, 11, 12, 15 e 17 se aplicam aos profissionais da contabilidade em determinadas circunstâncias (FATF, 2019a, p. 13, item 31).	
		14	FATF (2019a, p. 19)	**Recomendação 22: Atividades e Profissões Não-Financeiras Designadas (APNFDs): devida diligência acerca do cliente.** Quando os riscos de LD são maiores, os profissionais da contabilidade devem sempre aplicar CDD aprimorado, embora a lei ou regulamentação nacional possa não prescrever exatamente	

				como esses riscos mais altos devem ser mitigados (FATF, 2019a, p. 19, item 49).	
	Verificar como as partes interessadas (instituições e atores) na prevenção e combate à lavagem de dinheiro estão tentando coibir a utilização dos criptoativos na prática desse crime.	15	FATF (2019a, p. 22)	**Recomendação 1: Avaliação de riscos e aplicação de uma abordagem baseada em risco**. Ao avaliar o risco, os profissionais da contabilidade devem considerar todos os fatores de risco relevantes antes de determinar o nível de risco geral e o nível apropriado de mitigação a ser aplicado. Essa avaliação de risco pode ser informada por diferentes fontes (FATF, 2019a, p. 22, item 62).	
		16	FATF (2019a, p. 32 e p. 33)	**Recomendação 1: Avaliação de riscos e aplicação de uma abordagem baseada em risco.** Os profissionais da contabilidade devem ter políticas, controles e procedimentos que lhes permitam gerenciar e mitigar efetivamente os riscos que identificarem (ou que foram identificados pelo País) (FATF, 2019a, p. 33, item 86).	
		17	FATF (2019a, p. 36)	**Recomendação 22: Atividades e Profissões Não-Financeiras Designadas (APNFDs): devida diligência acerca do cliente.** Os profissionais da contabilidade devem elaborar procedimentos de CDD para permitir estabelecer com razoável segurança a verdadeira identidade de cada cliente e, com um grau adequado de confiança, conhecer os tipos de negócios e transações que o cliente provavelmente realizará (FATF, 2019a, p. 34, item 84).	
		18	FATF (2019a, p. 40)	**Recomendação 23: Atividades e Profissões Não-Financeiras Designadas (APNFDs): outras medidas.** A natureza e extensão dos controles AML, bem como o atendimento aos requisitos legais nacionais, precisam ser proporcionais ao risco envolvido nos serviços oferecidos. Além de outros controles internos de conformidade, a natureza e extensão dos controles AML abrangerão vários aspectos (FATF, 2019a, p. 40, item 111).	

Fonte: Elaborado pelo autor.

O questionário foi organizado em três partes: Parte 1 – Perfil dos respondentes; Parte 2 – Riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos; e Parte 3 – Possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos. A Parte 1, que compreende o perfil dos respondentes, tem como objetivo a identificação qualitativa dos respondentes através das perguntas presentes no **Quadro 10**.

Quadro 10 – Perguntas relacionadas ao perfil dos respondentes

Perguntas
1. Formação acadêmica:
2. Familiaridade com as regras e regulamentos domésticos de *anti-money laundering* (AML):
3. Familiaridade com as recomendações do Grupo de Ação Financeira Internacional (GAFI):
4. Experiência na prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT):
5. Familiaridade com criptoativos:
6. Experiência com criptoativos:
7. Em qual segmento do setor de serviços ou órgão da Administração Pública se concentra sua experiência de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT) e criptoativos?
8. Qual a área de atividade conforme a resposta da pergunta anterior se concentra sua experiência de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT) e criptoativos?

Fonte: Elaborado pelo autor.

Esta parte do questionário foi formulada com perguntas fechadas de múltipla escolha de resposta única, ou seja, o respondente pode escolher apenas uma opção.

A Parte 2, que aborda os riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos, procura obter a percepção dos respondentes por meio das perguntas apresentadas no **Quadro 11**.

Quadro 11 – Perguntas relacionadas aos riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos

Perguntas	**Quantidade de assertivas**
9. Em que medida as seguintes vulnerabilidades associadas às práticas e serviços oferecidos são exploradas nos crimes de lavagem de dinheiro com criptomoedas?	10
10. Qual a relevância dos seguintes fatores de risco de lavagem de dinheiro ao lidar com criptomoedas?	9
11. Em que medida os seguintes *red flag indicators* sobre lavagem de dinheiro com criptomoedas ocorrem?	9
12. Em que medida os seguintes *red flag indicators* associados ao anonimato são mais explorados ao lidar com criptomoedas?	10
13. Em que medida as seguintes atividades apresentam um desafio para a aplicação das medidas de *customer due diligence* ao lidar com criptomoedas?	5
14. Caso considere que a regulamentação seja um dos desafios ao lidar com as criptomoedas, qual das opções lhe parece mais apropriada?	Múltipla escolha

Fonte: Elaborado pelo autor.

Esta parte do questionário foi formulada com uma pergunta fechada de múltipla escolha de resposta única (pergunta 14) e demais perguntas fechadas em nível de matriz, perguntas do tipo matriz, que segundo Stockemer (2019), consistem em várias perguntas com as mesmas opções de resposta que frequentemente seguem uma escala.

Gil (2008) define escalas sociais como instrumentos construídos com o objetivo de medir a intensidade das opiniões e atitudes da maneira mais objetiva possível. Corbetta (2003, p. 165) explica que o processo de avaliação de atitudes envolve apresentar aos respondentes uma série de afirmações e pedir-lhes que expressem suas opiniões sobre elas e que ao combinar adequadamente as respostas, obtém-se uma pontuação individual que estima a posição de cada respondente em relação à atitude em questão.

Para a avaliação dos respondentes, nas perguntas 9, 11, 12 e 13 os respondentes têm opções de respostas com as seguintes escalas de frequência: nunca; raramente; ocasionalmente; frequentemente; muito frequente; e não saberia optar. Na pergunta 10, utilizaram-se opções de respostas com as seguintes escalas de importância: sem importância; pouco importante; razoavelmente importante; importante; muito importante; e não saberia optar.

Além da escolha por utilizar uma escala intervalar de cinco pontos, decidiu-se, ainda, por adicionar a opção "não saberia optar", no sentido de evitar trazer ao respondente, com falta de conhecimento sobre determinado assunto, desconforto ao responder o questionário, não o induzindo a responder de forma arbitrária, o que poderia afetar a validade e a confiabilidade da pesquisa.

A Parte 3, que trata das possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos, procura obter a percepção dos respondentes por meio das perguntas presentes no **Quadro 12**.

Quadro 12 – Perguntas relacionadas às possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos

Perguntas	Quantidade de assertivas
15. Qual a relevância das seguintes fontes de informação sobre avaliação de risco de lavagem de dinheiro ao lidar com criptomoedas?	5
16. Qual a relevância dos seguintes fatores e medidas para gerenciar e mitigar efetivamente os riscos de lavagem de dinheiro ao lidar criptomoedas?	10
17. Em que medida os seguintes procedimentos de *customer due diligence* apresentam eficácia ao lidar com criptomoedas?	10
18. Em que medida as políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de lavagem de dinheiro, apresentam eficácia ao lidar com criptomoedas?	10

Fonte: Elaborado pelo autor.

Esta parte do questionário foi formulada com perguntas do tipo matriz. Nas perguntas 15 e 16 foram utilizadas opções de respostas com as seguintes escalas de importância: sem importância; pouco importante; razoavelmente importante; importante; muito importante; e não saberia optar. Nas perguntas 17 e 18 foram utilizadas opções de respostas com as seguintes escalas de eficácia: sem eficácia; pouco eficaz; razoavelmente eficaz; eficaz; muito eficaz; e não saberia optar.

Todas as perguntas presentes tanto na Parte 2, como na Parte 3, contam com abertura para comentários.

3.3.2 Pré-teste

A versão final do questionário foi precedida de reuniões com profissionais formados em Ciências Contábeis, com experiência em PLD-FT e criptoativos e a realização pré-testes.

Foram realizadas três reuniões, uma reunião por telefone com perito criminal contábil do Centro de Estudos do Instituto de Criminalista Carlos Éboli (ICCE) e duas reuniões *online* via *Google Meet* com profissional com experiência em *exchange* de criptoativos. Ambos os profissionais participaram do pré-teste.

Em 04/03/2021 foi realizado contato telefônico com o perito criminal contábil do ICCE, onde foram discutidos maiores detalhes da pesquisa e entendimentos a respeito de sua participação e orientação para o andamento do processo de seleção de possíveis participantes da pesquisa. Um dos entendimentos está no fato de que sua atuação se concentra na repressão ao crime de LD com criptoativos e que seria interessante procurar possíveis participantes que atuassem na área de PLD-FT em organizações privadas. Outro entendimento está no fato que ele é o único perito criminalista do ICCE com as características predeterminadas para os possíveis participantes da pesquisa, não tendo ninguém que pudesse indicar para contato. Entendeu-se, ainda, que aceitava em participar da pesquisa somente por meio de aplicação de questionário e que ficaria a disposição para ajudar na elaboração do mesmo e sobre qualquer dúvida envolvendo sua área de atuação.

Nas datas de 28/04/2021 e 11/05/2021 foram realizadas reuniões com profissional contábil que atuou na área de PLD-FT em uma *exchange* de criptoativos, onde foram discutidos maiores detalhes da pesquisa, informações sobre o processo de PLD-FT e sua participação e indicação de possíveis participantes na pesquisa. Igualmente ao profissional perito criminal contábil do ICCE, foi oferecida ajuda na elaboração do questionário e sobre qualquer dúvida sobre sua área de atuação.

A experiência do profissional na PLD-FT em uma *exchange* de criptoativos traz outras informações além do profissional envolvido diretamente no processo de combate ao crime de LD, complementando, assim, a contribuição do profissional perito criminal contábil do ICCE. Conforme Moser e Korstjens (2018) participantes que compartilham uma experiência, mas variam em características e em suas experiências individuais, podem ajudar o pesquisador a obter informações valiosas para compreender os fenômenos estudados.

Nesse sentido, o pré-teste ocorreu junto à seis profissionais (já incluídos os dois profissionais anteriormente citados), cinco com formação acadêmica em Ciências Contábeis e uma com formação acadêmica em Direito.

A profissional com formação em Direito não relatou dificuldades em responder o questionário, mas ao escolher mais de uma opção de resposta nas perguntas de nº 7 e 8, apresentou em sua observação uma única opção de resposta entre as duas já escolhidas para cada pergunta, caso fosse possível somente resposta única às perguntas. Tal fato se repetiu com um profissional com formação em Ciências Contábeis, quando escolheu duas opções na pergunta de nº 1.

Com vista em evitar novas ocorrências de escolha de mais de uma opção de resposta nas perguntas de resposta única, foi incluída a observação sobre a possibilidade de escolha de somente uma opção de resposta para as perguntas.

Outro ponto observado foi o fato de a profissional com formação em Direito ter deixado o item 17.9 da pergunta 17 em branco.

Na esperança de se evitar que alguma opção de resposta fosse deixada em branco, foi incluída, no final do questionário, solicitação de verificação das respostas às perguntas do questionário.

A profissional com formação em Ciências Contábeis sugeriu a inclusão na pergunta de nº 6 da confirmação do tempo de existência dos criptoativos para entendimento de que a pergunta não foi formulada de forma equivocada.

Desta forma, foi inserida uma Nota de Rodapé informando que a pergunta leva em consideração que já se passaram mais de 10 anos desde o surgimento do *Bitcoin* em 2008.

Um profissional com formação em Ciências Contábeis sugeriu a inclusão de Notas de Rodapé com esclarecimento a respeito de alguns itens do questionário. Logo, foram inseridas Notas de Rodapé para esclarecimento de termos que poderiam trazer certa dificuldade no entendimento do questionário.

Esse profissional sugeriu, também, maior detalhamento nos itens 9.6, 9.7 e 9.10 da pergunta de nº 9, para melhor entendimento sobre a que se referem. Por isso foram realizadas as mudanças para um melhor entendimento desses itens.

3.4 COLETA DE DADOS

A presente seção tem como objetivo expor os procedimentos adotados para a coleta de dados. São apresentadas as duas fases de coleta de dados. Na primeira fase são descritos os procedimentos adotados para a análise documental. Na segunda são explicados os procedimentos adotados na aplicação do questionário.

3.4.1 Primeira fase da coleta de dados

Para Chaumier citado por Bardin (1977, p. 45), a análise documental pode ser definida como "uma operação ou conjunto de operações visando representar o conteúdo de um documento sob uma forma diferente do original, a fim de facilitar num estado ulterior, a sua consulta e referenciação". Acerca dos procedimentos metodológicos da análise documental, Lüdke e André (1986, p. 40) explicam que o primeiro passo a ser dado é a caracterização dos documentos que serão usados ou selecionados, uma vez que a escolha dos documentos não é aleatória, ocorrendo de modo geral alguns propósitos, ideias ou hipóteses direcionando a sua escolha.

Deste modo, a seleção dos documentos seguiu os seguintes objetivos de pesquisa estabelecidos: (i) identificar possíveis aplicações dos criptoativos nos crimes de LD; (ii) verificar como as partes interessadas (instituições e atores) na PCLD estão tentando coibir a utilização dos criptoativos na prática desse crime; e (iii) verificar o tratamento contábil aplicado aos criptoativos. As políticas, estratégias e ações dos agentes nacionais e internacionais acerca das questões decorrentes do uso dos criptoativos no crime de LD, formaram a temática que deveria ser observada nos documentos pesquisados.

Na escolha dos documentos, manteve-se o foco no conteúdo, levando-se em consideração o contexto, a utilização e a função dos documentos. Conforme Cellard (2008, p. 299), efetuou-se um estudo: (i) do contexto; (ii) do autor ou dos autores; (iii) da autenticidade e da confiabilidade do texto; (iv) da natureza do texto; e (v) dos conceitos-chave e da lógica interna do texto.

O acesso as fontes dos documentos primários e secundários foi realizado pela Internet. Através de mecanismos de busca como o *Google*, foram acessados *sites* de instituições não governamentais, governamentais e intergovernamentais, nacionais e internacionais. Conforme orientação de De Almeida (2011, p. 18), foram adotados critérios cuidadosos para a seleção de fontes da Internet, como: (i) observar se o conteúdo de um determinado *site* corresponde a uma fonte integral, ou se foi retirado parcialmente de outra fonte; (ii) evidenciar a precisão das informações contidas nos *sites*, testando-as por meio de comparações com outras fontes; e (iii) observar qual instituição está respaldando o *site* em questão.

3.4.2 Segunda fase da coleta de dados

Nesta seção são explicadas as duas etapas dos procedimentos adotados na realização da aplicação do questionário.

3.4.2.1 Primeira etapa da aplicação dos questionários

A coleta de dados por meio da aplicação de questionário teve início logo após o presente estudo ser aprovado pelo Comitê de Ética em Pesquisa (CEP) da Universidade Federal do Rio de Janeiro (UFRJ), conforme Parecer de nº 5.157.673 de 9/12/2021 (ANEXO B). O envio da Carta Convite juntamente com o questionário, e o documento "Registro de Consentimento Livre e Esclarecido (RCLE)" (APÊNDICE B) para os *e-mails* dos 160 profissionais que aceitaram participar da pesquisa, foi realizado a partir do dia 15/12/2021. Simultaneamente ao envio dos questionários por *e-mail* foram encaminhadas mensagens aos possíveis participantes na plataforma *LinkedIn*.

O andamento do processo de aplicação dos questionários na presente etapa está demonstrado na **Tabela 2**.

Tabela 2 – Processo de aplicação dos questionários (Primeira etapa)

Data de envio dos questionários	Quantidade de questionários aplicados	Quantidade de questionários respondidos
A partir de 15/12/2021	160	28
A partir de 18/01/2022	132	17
A partir de 15/02/2022	115	12
A partir de 18/03/2022	103	2
Total		**59**

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

As mensagens enviadas nos *e-mails* e encaminhadas aos possíveis participantes na plataforma *LinkedIn*, durante as diferentes datas apresentadas na Tabela 2, constam no APÊNDICE C.

3.4.2.2 Segunda etapa da aplicação dos questionários

Nesta etapa, a partir do dia 25/03/2022, foram encaminhados a Carta Convite juntamente com o questionário, e o documento "Registro de Consentimento Livre e Esclarecido (RCLE)" para os *e-mails* dos 1.136 profissionais que não se posicionaram a respeito de participarem ou não da pesquisa.

O andamento do processo de aplicação dos questionários na presente etapa, está demonstrado na **Tabela 3**.

Tabela 3 – Processo de aplicação dos questionários (Segunda etapa)

Data de envio dos questionários	Quantidade de questionários aplicados	Quantidade de questionários respondidos
A partir de 25/03/2022	1.136	3
Total		**3**

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

O término da fase de coleta de dados por meio da aplicação de questionário foi na data de 20 de abril de 2022, com aproximadamente 5% dos questionários envidados respondidos, conforme demonstrado na **Tabela 4**.

Tabela 4 – Processo de aplicação dos questionários

Data de envio dos questionários	Quantidade de questionários aplicados	Quantidade de questionários respondidos
A partir de 15/12/2021	160	28
A partir de 18/01/2022	132	17
A partir de 15/02/2022	115	12
A partir de 18/03/2022	103	2
A partir de 25/03/2022	1.136	3
Total		**62**

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Procurando manter o sigilo da identidade dos 62 participantes em relação aos questionários respondidos, durante a exposição dos resultados, os respondentes foram nomeados ficticiamente e de forma aleatória, sendo representados pelos nomes R1, ..., R62.

3.5 ANÁLISE DOS DADOS

Na presente pesquisa, a análise dos dados ocorreu por meio de três etapas. Durante a primeira etapa foi realizada a análise documental nos seguintes documentos: (i) Documento I – "*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*" (FATF, 2019b); (ii) Documento II – "*Risk-Based Approach for the Accounting Profession*" (FATF, 2019a); e (iii) Documento III – "*IFRIC Update June 2019: Holdings of Cryptocurrencies*" (IASB, 2019). Na segunda etapa são descritos os procedimentos adotados na análise dos dados coletados pelos questionários, com exceção dos comentários deixados pelos participantes no "Espaço aberto para comentários referentes à pergunta" do questionário, que foram analisados na terceira etapa.

3.5.1 Primeira etapa da análise dos dados

Na fase de a análise dos dados, inicialmente foi realizada a análise documental, no Documento I, fazendo relação com o Documento II, no qual foram verificadas as orientações para uma abordagem baseada em risco (ABR) no contexto dos criptoativos que se pretendem desenvolver em uma ABR para a profissão contábil.

É importante notar que a publicação tardia do documento "*Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*" (FATF, 2021a), em relação ao período de desenvolvimento do presente estudo, comprometeu sua utilização na pesquisa.

O Documento I – "Orientação para uma Abordagem Baseada em Risco para Ativos Virtuais e Provedores de Serviços de Ativos Virtuais" (Tradução livre) atualizou a Orientação do GAFI de 2015 para uma ABR para moedas virtuais. Essa atualização tornou-se necessária devido a evolução do espaço dos ativos virtuais[15] (AVs), que permitiu a inclusão de uma gama de novos produtos e serviços, modelos de negócios e atividades e interações, incluindo as transações entre AVs (FATF, 2019b).

[15] **Ativo virtual** é uma representação digital de valor que pode ser negociado digitalmente ou transferido e pode ser usado para fins de pagamento ou investimento. Os ativos virtuais não incluem representações digitais de moedas fiduciárias, valores mobiliários e outros ativos financeiros que já estão incluídos em outras partes das Recomendações do GAFI (FATF, 2019b, Glossário FATF).

Esse novo documento apresenta novas definições de AVs e Provedores de Serviços de Ativos Virtuais[16] (PSAVs), a Recomendação revisada Nº 15 – Novas Tecnologias e sua Nota Interpretativa, a Nota Interpretativa da Recomendação 15 (NIR – 15).

Na análise documental realizada no Documento III, foram verificadas as orientações sobre a contabilização de transações envolvendo criptomoedas, uma vez que, o GAFI orienta o profissional da contabilidade, mesmo quando não está realizando uma auditoria, a considerar o documento *International Standard of Auditing* 315 (ISA 315) – *Identifying and assessing the risks of material misstatement* (revisado pelo *International Auditing and Assurance Standards Board* (IAASB) em 2019), que, no Brasil, mantém correlação com a Norma Brasileira de Contabilidade, NBC TA 315 (R2) – Identificação e avaliação dos riscos de distorção relevante (FATF, 2019a, p. 31).

O item 19, da NBC TA 315 (R2), menciona a obrigação do auditor de realizar procedimentos de avaliação de riscos para obter entendimento da estrutura de relatório financeiro aplicável, e as políticas contábeis da entidade, de acordo com o item A82, transcrito, em parte, a seguir (CFC, 2021):

> A82. Assuntos que o auditor pode considerar ao obter entendimento da estrutura de relatório financeiro aplicável da entidade e de como ela se aplica no contexto da natureza e das circunstâncias da entidade e de seu ambiente incluem:
> - as práticas de relatório financeiro da entidade em termos da estrutura de relatório financeiro aplicável, tais como:
>
> [...]
>
> - a contabilização de transações não usuais ou complexas, inclusive aquelas em áreas controversas ou emergentes (por exemplo, contabilização para criptomoedas);
>
> [...].

Devido aos desafios decorrentes da natureza global e da constante evolução das criptomoedas, em relação às regras contábeis, órgãos reguladores contábeis, como o *Accounting Standards Board of Japan* (ASBJ), o Australian *Accounting Standards Board* (AASB) e o *International Accounting Standards Board* (IASB), iniciaram discussões a respeito das avaliações das criptomoedas para definir a sua classificação adequada (KATARZYNA, 2019; MARQUES, 2019).

---

[16] **Provedor de serviços de ativos virtuais** significa qualquer pessoa física ou jurídica que não esteja coberta pelas Recomendações e, como empresa, realiza uma ou mais das seguintes atividades ou operações para ou em nome de outra pessoa física ou jurídica: i) troca entre ativos virtuais e moedas fiduciárias; ii) troca entre uma ou mais formas de ativos virtuais; iii) transferência de ativos virtuais; iv) guarda e/ou administração de ativos virtuais ou instrumentos que permitem o controle sobre ativos virtuais; e v) participação e prestação de serviços financeiros relacionados à oferta e/ou venda de um ativo virtual de um emissor (FATF, 2019b, Glossário FATF).

Em junho de 2019, o Comitê de Interpretações, IFRS *Interpretations Committee* (IFRIC), comitê de interpretações das *International Financial Reporting Standard* (IFRS), por meio do IFRIC *Update June* 2019, publicou na *Committee's agenda decisions*, o documento *Holdings of Cryptocurrencies – Agenda Paper* 12 (Documento III), decisão de agenda sobre como os Padrões IFRS se aplicam às *holdings* de criptomoedas.

Mediante a decisão do Brasil, em buscar promover o alinhamento das normas brasileiras às Normas Internacionais de Contabilidade (NIC) emitidas pelo *International Accounting Standars Board* (IASB), que são denominadas IFRS, a decisão do IFRIC pode ser interpretada como aplicável às normas emitidas pelo Comitê de Pronunciamento Contábil (CPC), uma vez que o contexto do documento não apresenta divergências entre elas.

Considerando que a decisão da agenda não trata dos criptoativos além das criptomoedas, e que o desenvolvimento de criptoativos ainda está em um estágio inicial, os detentores de criptomoedas devem continuar monitorando as atividades de normatização, bem como as orientações emitidas pelos reguladores para garantir que uma contabilização adequada das *holdings* de criptomoedas conforme Padrões IFRS (EY, 2019).

3.5.2 Segunda etapa da análise dos dados

Os dados coletados por meio de questionários, com exceção dos comentários deixados pelos participantes no "Espaço aberto para comentários referentes à pergunta" do questionário, foram tabulados com o auxílio do *software Microsoft Excel* e organizados de forma sistematizada para análise no *software* IBM SPSS.

Nas Partes 2 e 3 do questionário, nas perguntas 9, 11, 12 e 13, onde foi utilizada a escala de frequência de 5 pontos, mais a opção "não saberia optar", para a análise dos dados, aplicou-se a seguinte codificação, conforme **Quadro 13**:

Quadro 13 – Codificação da escala de frequência

Escala de frequência	Valor atribuído
Nunca	1
Raramente	2
Ocasionalmente	3
Frequentemente	4
Muito frequente	5
Não saberia optar	Nulo

Fonte: Elaborado pelo autor.

Nas perguntas 10, 15 e 16, onde foi utilizada escala de importância de 5 pontos, mais a opção “não saberia optar”, para a análise dos dados, aplicou-se a seguinte codificação, conforme o **Quadro 14**:

Quadro 14 – Codificação da escala de importância

Escala de importância	Valor atribuído
Sem importância	1
Pouco importante	2
Razoavelmente importante	3
Importante	4
Muito importante	5
Não saberia optar	Nulo

Fonte: Elaborado pelo autor.

Nas perguntas 17 e 18, onde foi utilizada escala de eficácia de 5 pontos, mais a opção “não saberia optar”, para a análise dos dados, aplicou-se, conforme **Quadro 15**, a seguinte codificação:

Quadro 15 – Codificação da escala de eficácia

Escala de eficácia	Valor atribuído
Sem eficácia	1
Pouco eficaz	2
Razoavelmente eficaz	3
Eficaz	4
Muito eficaz	5
Não saberia optar	Nulo

Fonte: Elaborado pelo autor.

Nesta etapa foi utilizada a análise descritiva dos dados coletado, com objetivo de se obter a frequência relativa percentual das percepções dos respondentes em relação a cada assertiva a eles indicadas.

3.5.3 Terceira etapa da análise dos dados

Uma análise qualitativa também foi realizada nos comentários deixados pelos participantes no “Espaço aberto para comentários referentes à pergunta” do questionário. Sua importância está em auxiliar no entendimento dos resultados e para elucidar pontos da literatura.

A análise dos comentários deixados pelos participantes foi realizada, dentre as técnicas da análise de conteúdo apresentadas por Bardin (1977, p. 153), por meio da análise categorial, seguindo as seguintes etapas: (i) transcrição dos comentários de maneira agrupada em cada

pergunta e uma leitura flutuante; (ii) leitura dos textos de forma mais criteriosa, onde foram identificados argumentos e ideias que versem em uma mesma direção; (iii) agrupamento dos argumentos e ideias em uma mesma linha; e (iv) realização, junto à literatura, uma busca de relatos ou confirmação do que foi escrito pelos participantes.

A análise de conteúdo efetuada sobre os comentários dos participantes buscou não a acumulação de dados, mas buscou explorar as relações psicológicas – percepções aprofundadas e compreensão de problemas do mundo real – dos participantes acerca do tema da pesquisa. Essas relações psicológicas foram classificadas em diferentes temas que, posteriormente foram classificados em categorias temáticas (categorias de análise).

Para a condução da análise dos comentários foram utilizadas as categorias de análise presentes no **Quadro 16**:

Quadro 16 – Categorias de análise dos comentários dos respondentes

Categoria de análise	Descrição resumida
1 Vulnerabilidades associadas às práticas e serviços oferecidos	Identificação dos riscos principais apresentados pela LD aos profissionais da contabilidade ao lidar com criptomoedas.
2 Fatores de risco de LD	Identificação das categorias de risco como ponto de partida para aplicação da ABR pelo profissional da contabilidade ao lidar com criptomoedas.
3 *Red flag indicators*	Identificação da relação dos *red flag indicators* associados as etapas de LD ao lidar com criptomoedas.
4 *Red flag indicators* associados ao anonimato	Identificação das estratégias de anonimato ao lidar com criptomoedas.
5 Desafios para a aplicação das medidas de CDD	Identificação dos desafios para a aplicação das medidas de CDD ao lidar com criptomoedas.
6 Abordagem regulatória	Identificação da resposta regulatória AML/CFT mais apropriada ao lidar com as criptomoedas.
7 Orientações	Identificação de questões referentes as fontes de informação sobre avaliação de risco de LD ao lidar com criptomoedas.
8 Mitigação de riscos	Identificação de fatores e medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar criptomoedas.
9 Medidas preventivas	Identificação das medidas de CDD aprimoradas ao lidar com criptomoedas.
10 Controles internos e governança	Identificação das políticas, procedimentos e controles da organização projetados para limitar e controlar os riscos de LD ao lidar com criptomoedas.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Para cada uma das categorias de análise presente no **Quadro 16**, serão apresentadas no APÊNDICE D descrições detalhadas com informações adicionais para seu melhor entendimento.

3.6 LIMITAÇÕES DA PESQUISA

As limitações da pesquisa estão na ausência de taxonomia dos criptoativos padronizada, o que dificulta determinar a aplicabilidade de possíveis padrões. Ainda, devido à diversidade e ao ritmo de inovação associados aos criptoativos, os fatos e as circunstâncias de cada caso individual serão diferentes, tornando difícil abordar completamente tudo o que um profissional de contabilidade deve saber sobre as possíveis abordagens contábil na prevenção e combate ao crime de LD por meio dos criptoativos.

Na dificuldade em encontrar profissionais com conhecimento tanto na prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT), como em criptoativos. Essa limitação torna-se mais significativa quando relacionada a profissionais com formação em Ciências Contábeis.

No processo de pesquisa junto a rede social de negócios *LinkedIn*, quando desrespeitado o limite de convites para conexão semanal, acarretando a aplicação de sanções como o bloqueio temporário da conta. Tal limitação não foi superada nem mediante a assinatura de uma conta *Premium* realizada pelo pesquisador.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

A apresentação e análise dos resultados obtidos a partir dos dados coletados por meio dos questionários e da análise documental, estão estruturados em três seções.

Na primeira seção é evidenciada a análise dos dados coletados por meio dos questionários aplicados junto aos profissionais que atuam na área PLD-FT com experiência em criptoativos.

A análise documental realizada no Documento III – "*IFRIC Update June 2019*: *Holdings of Cryptocurrencies*" é apresentada na segunda seção, e na terceira é discutido os resultados da pesquisa.

4.1 PERCEPÇÃO DOS PROFISSIONAIS QUE ATUAM NA ÁREA PLD-FT

A partir da aplicação do questionário junto aos profissionais que atuam na área PLD-FT, buscou-se verificar a percepção desses profissionais acerca da utilização dos criptoativos no crime de LD, os riscos e desafios de crime de LD enfrentados ao lidar com criptoativos e as possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos.

Seguindo a organização aplicada ao questionário, a presente seção está dividida em três partes: primeira parte – Perfil dos respondentes; segunda parte – Riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos; e terceira parte – Possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos.

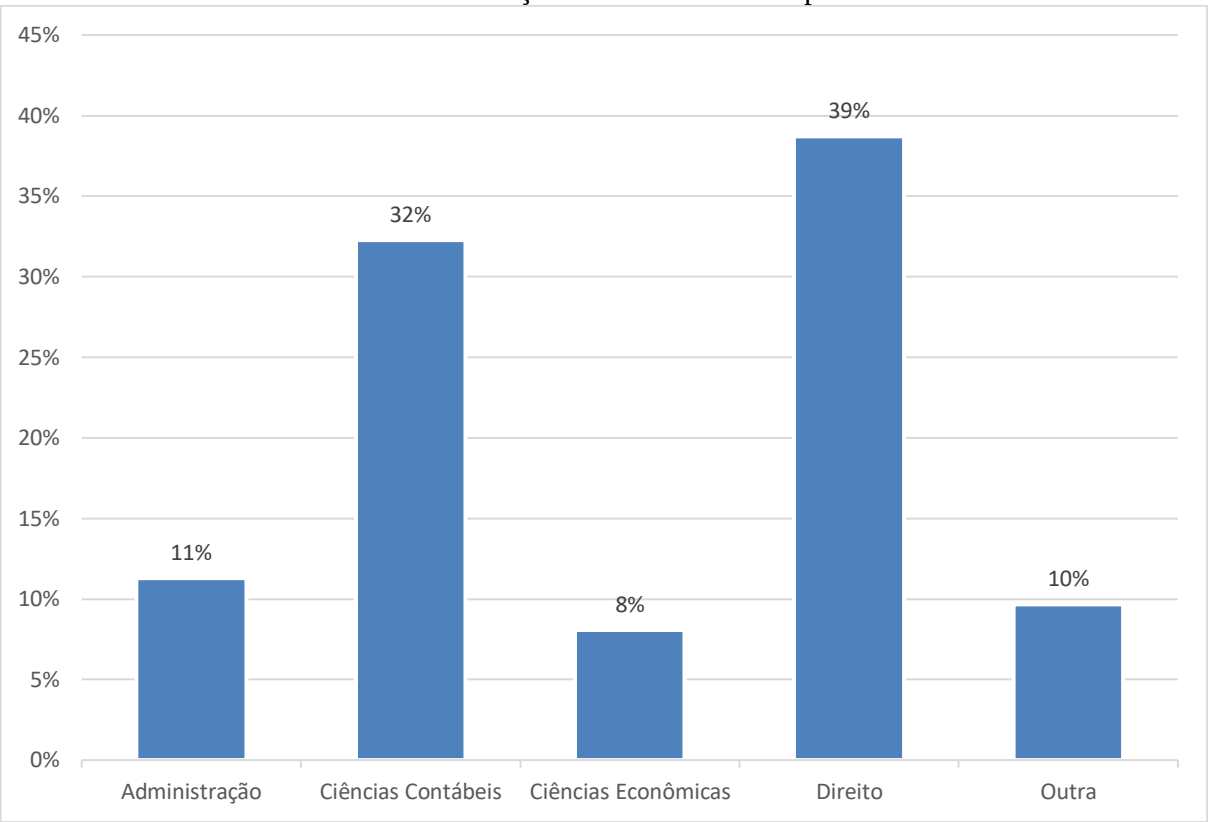
4.1.1 Perfil dos respondentes

Nesta seção serão expostas informações a respeito dos participantes da pesquisa.

4.1.1.1 Formação Acadêmica

No que tange à formação acadêmica dos respondentes, conforme **Gráfico 1**, observa-se que dentre os 62 respondentes, aproximadamente 39% (24/62), tem formação acadêmica em Direito, cerca de 32% (20/62) dos respondentes tem formação acadêmica em Ciências Contábeis, seguido de aproximadamente 11% (7/62) dos respondentes com formação acadêmica em Administração e 8% (5/62) dos respondentes tem formação acadêmica em Ciências Econômicas.

Gráfico 1 – Formação acadêmica dos respondentes



Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Em relação aos 10% (6/62), de "Outra", estes correspondem aos respondentes com as seguintes diferentes áreas de formação acadêmica, apresentadas na **Tabela 5**.

Tabela 5 – Áreas de formação acadêmica que compõem a opção "Outra"

Formação acadêmica	Quantidade
Biblioteconomia	1
Ciências da Computação	1
Comércio Exterior	1
Engenharia Civil	1
Engenharia Mecânica	1
Sistema de Informação	1
Total	**6**

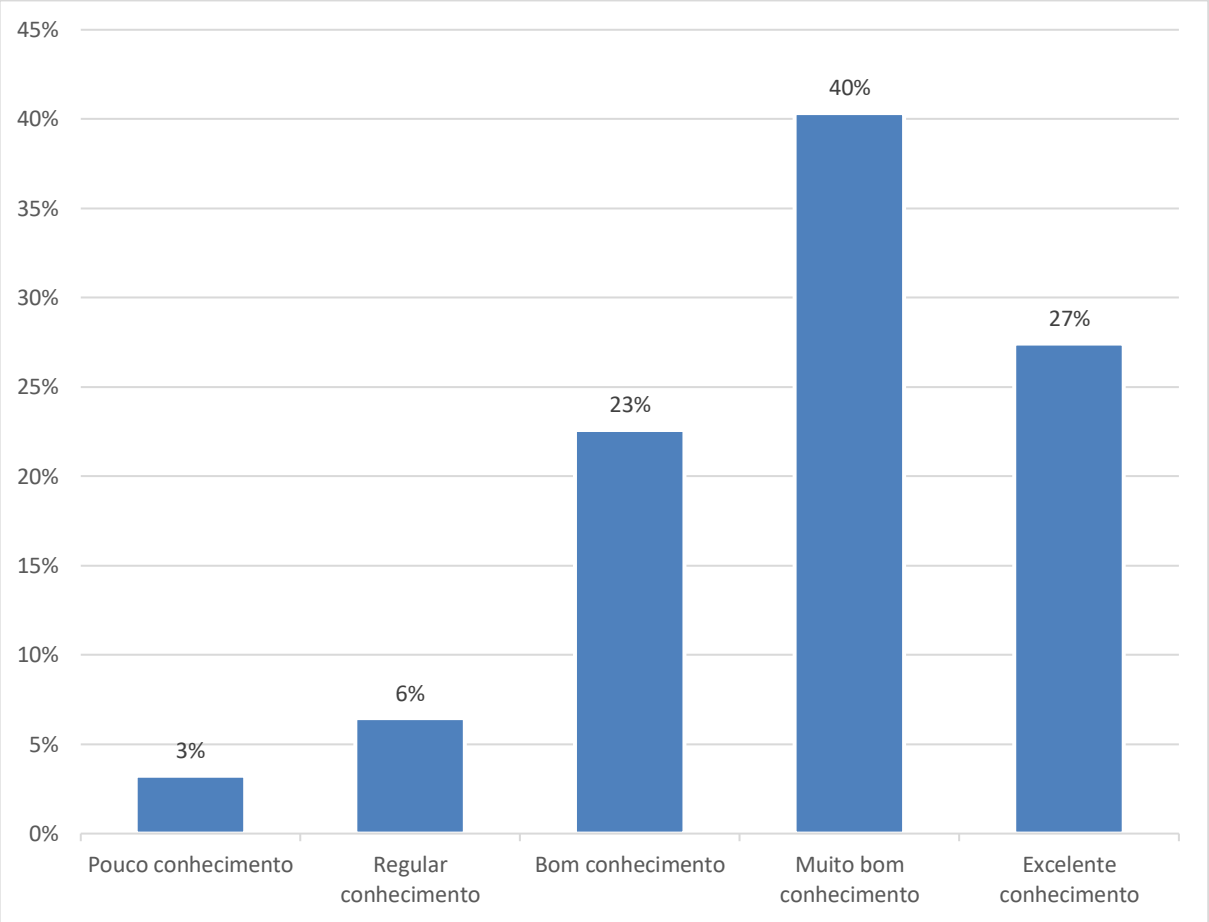
Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Ao longo do processo de seleção de possíveis participantes da pesquisa foi possível evidenciar que a área de PLD-FT é bastante multidisciplinar, o que responde a presença de profissionais com diferentes áreas de formação acadêmica.

4.1.1.2 Familiaridade com as Regras e Regulamentos Domésticos de AML

Acerca do nível de familiaridade dos respondentes com as regras e regulamentos domésticos de AML, conforme o **Gráfico 2**, é possível evidenciar que 40% dos respondentes entendem que possuem muito bom conhecimento, enquanto 27% avaliam ter excelente conhecimento. Portanto é possível aceitar que aproximadamente 67% (40% + 27%) dos respondentes provavelmente guardam elevado nível de conhecimento a respeito das regras e regulamentos domésticos de AML.

Gráfico 2 – Familiaridade com as regras e regulamentos domésticos de AML



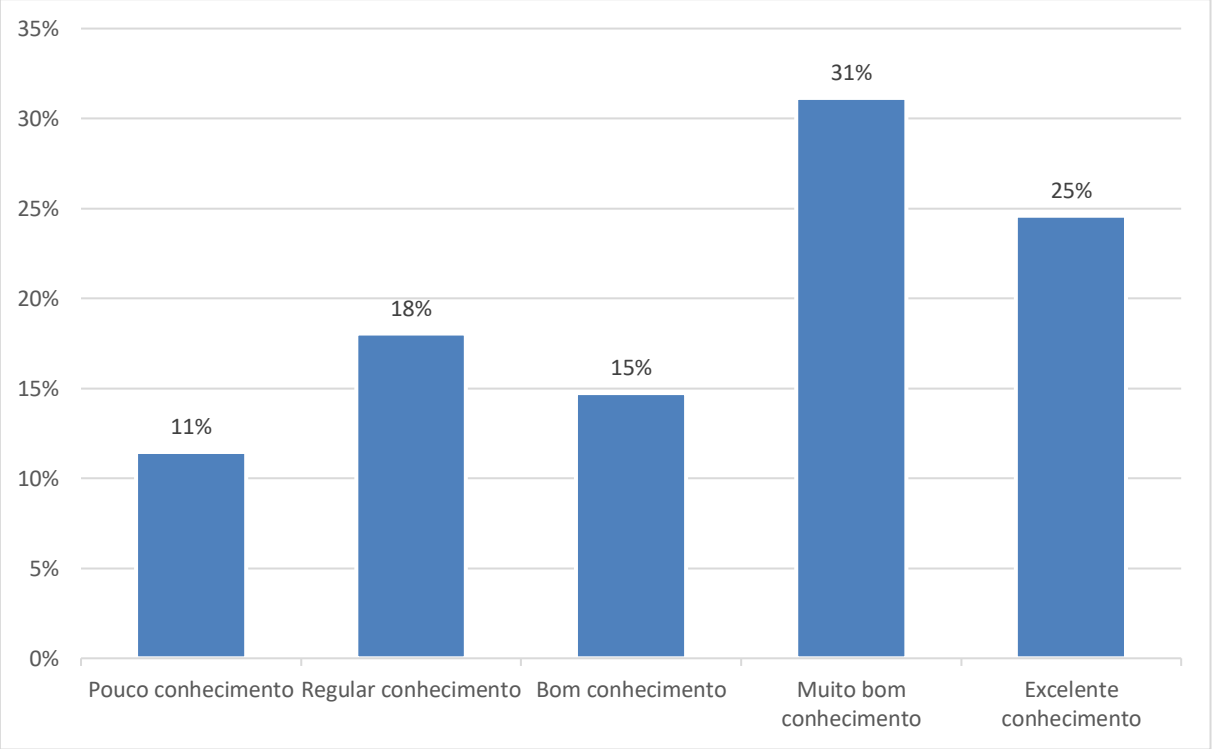
Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Gráfico 2** é possível perceber, também, que possivelmente cerca de 9% (3% + 6%) dos respondentes têm pouco (3%) ou regular (6%) conhecimento a respeito das regras e regulamentos domésticos de AML.

4.1.1.3 Familiaridade com as Recomendações do GAFI

Sobre o nível de familiaridade dos respondentes com as recomendações do GAFI, por meio do **Gráfico 3**, observa-se que 31% dos respondentes entendem dispor de muito bom conhecimento, ao mesmo tempo que 25% julgam possuir excelente conhecimento. Assim, torna-se aceitável o entendimento de que cerca de 56% (31% + 25%) dos respondentes percebem-se com elevado nível de conhecimento a respeito das recomendações do GAFI.

Gráfico 3 – Familiaridade com as recomendações do GAFI



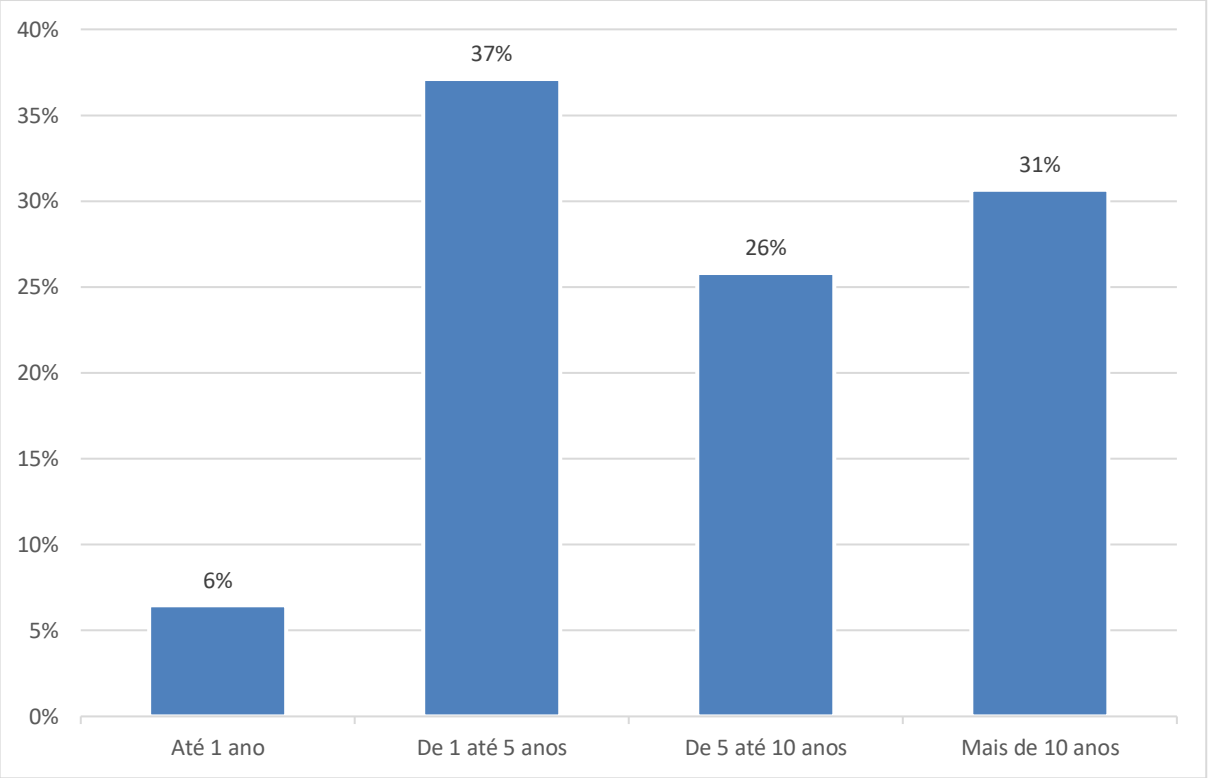
Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Gráfico 3**, percebe-se que provavelmente 29% (11% + 18%) dos respondentes compreendem ter nível incipiente de conhecimento sobre as recomendações do GAFI, pois 11% dos respondentes entendem possuir pouco conhecimento, quando 18% avaliam ter regular conhecimento.

4.1.1.4 Experiência na Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD-FT)

A respeito do tempo de experiência dos respondentes na PLD-FT, conforme o **Gráfico 4**, a maioria dos respondentes, cerca de 37%, possuem de 1 até 5 anos de experiência e aproximadamente 31% dos respondentes contam com mais de 10 anos de experiência.

Gráfico 4 – Experiência na PLD-FT



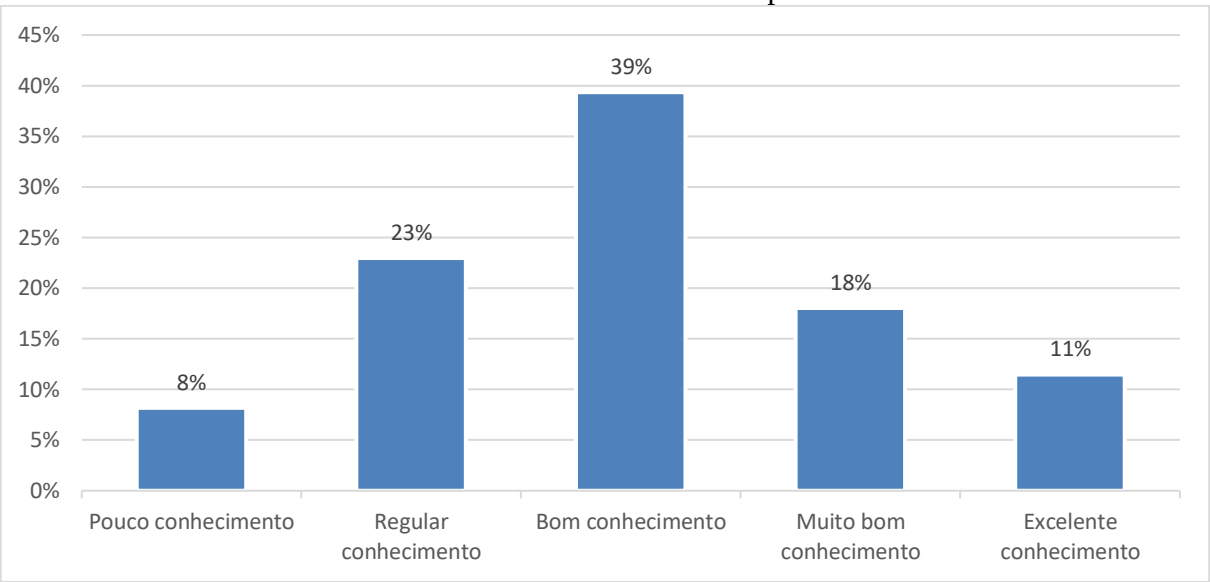
Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Com relação aos respondentes que possuem tempo de experiência na PLD-FT de até 1 ano, conforme o **Gráfico 4**, observa-se a percentagem é de aproximadamente 6% dos respondentes.

4.1.1.5 Familiaridade com criptoativos

Sobre a familiaridade dos respondentes com os criptoativos, no **Gráfico 5**, é possível evidenciar que aproximadamente 39% dos respondentes julgam ter bom conhecimento a respeito dos criptoativos. Possivelmente cerca de 29% (18% + 11%) dos respondentes possuem elevado nível de conhecimento, quando 18% entendem possuir muito bom e 11% avaliam ter excelente conhecimento a respeito dos criptoativos.

Gráfico 5 – Familiaridade com criptoativos



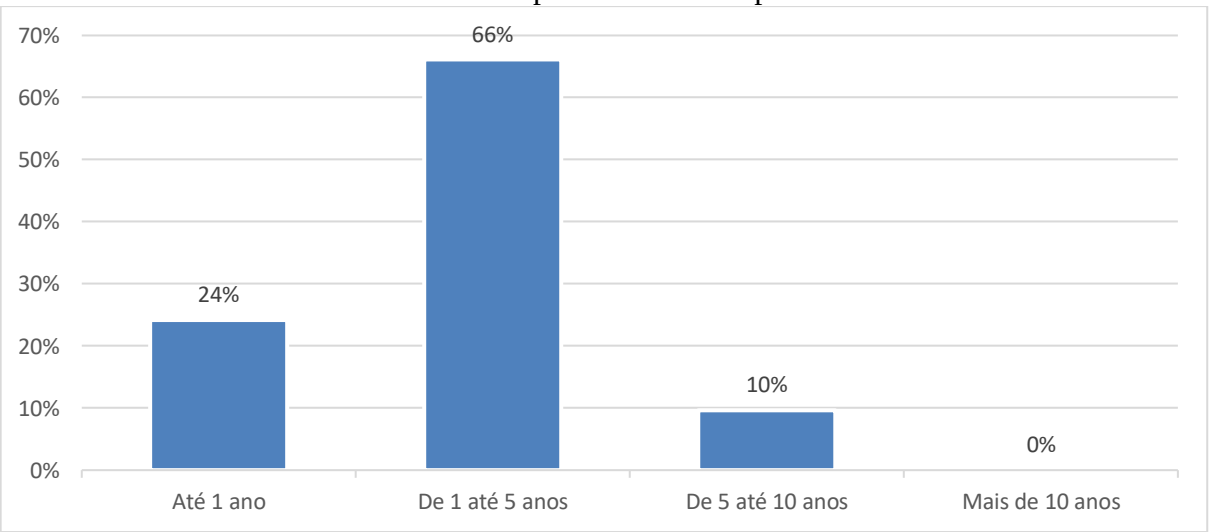
Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Aproximadamente 31% (8% + 23%) dos respondentes possuem nível incipiente de conhecimento sobre criptoativos, sendo 8% com pouco e 23% com regular conhecimento.

4.1.1.6 Experiência com criptoativos

Em relação a experiência dos respondentes com criptoativos, conforme o **Gráfico 6**, a maioria dos respondentes, aproximadamente 66%, possuem de 1 a 5 anos de experiência com criptoativos e 24% dos respondentes têm até 1 ano de experiência.

Gráfico 6 – Experiência com criptoativos



Fonte: Elaborado pelo autor com base nos dados da pesquisa.

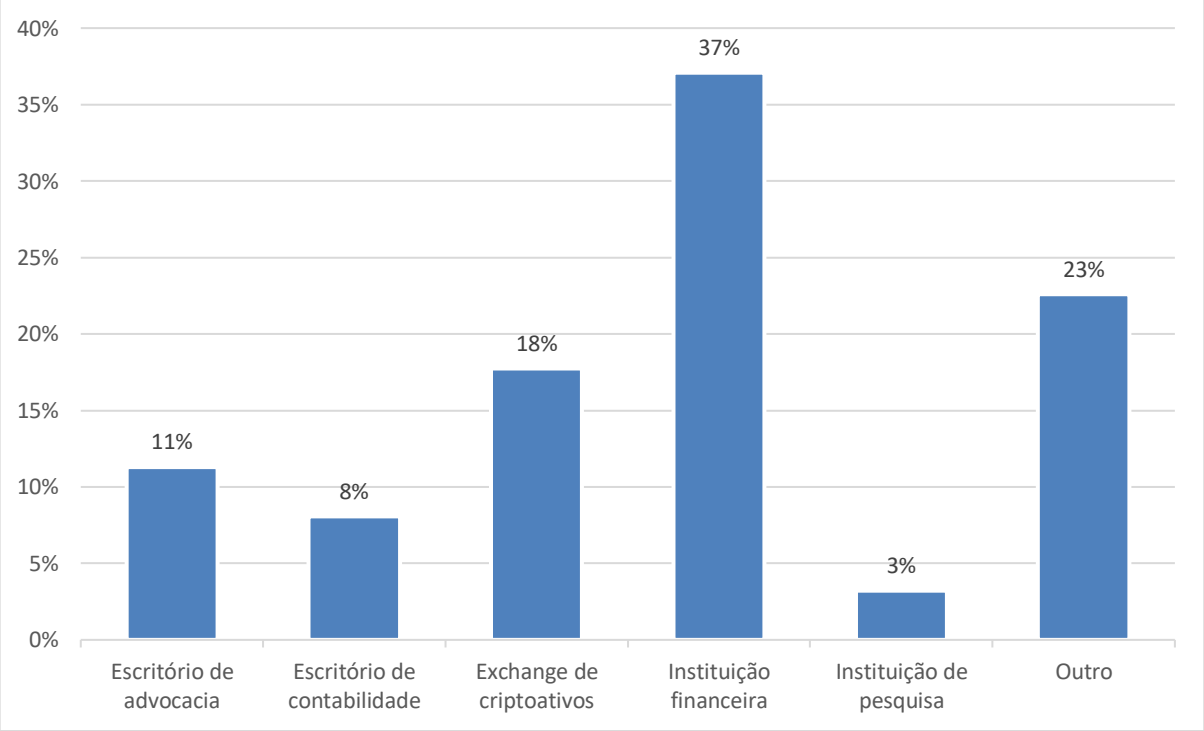
A porcentagem de respondentes com 5 até 10 anos de experiência é de 10%, conforme o **Gráfico 6**, onde observa-se a ausência de respondentes com mais de 10 anos de experiência em criptoativos. A ausência de respondentes com mais de 10 anos de experiência pode estar diretamente relacionada com a data de surgimento do *Bitcoin* em 2008, pouco mais de 10 anos.

4.1.1.7 Segmento do Setor de Serviços ou Órgão da Administração Pública em que se Concentra a Experiência em PLD-FT e Criptoativos

No tocante ao segmento do setor de serviços ou órgão da Administração Pública que se concentra a experiência dos respondentes com PLD-FT e criptoativos, conforme o **Gráfico 7**, a maioria dos respondentes, aproximadamente 37%, têm nas instituições financeiras (IFs) concentrada sua experiência com PLD-FT e criptoativos.

Para cerca de 18% dos respondentes as *exchanges* de criptoativos são onde se concentra sua experiência, para 11%, os escritórios de advocacia, para 8%, os escritórios de contabilidade e para 3%, as instituições de pesquisa.

Gráfico 7 – Segmento do setor de serviços ou órgão da Administração Pública que se concentra a experiência dos respondentes com PLD-FT e criptoativos



Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Conforme o **Gráfico 7**, para aproximadamente 23% dos respondentes a opção "Outro" é onde se concentra sua experiência com PLD-FT e criptoativos.

A opção "Outro" representa diferentes segmentos do setor de serviços ou órgão da Administração Pública onde se concentra a experiência dos respondentes com PLD-FT e criptoativos, conforme exposto no **Quadro 17**.

Quadro 17 – Diferentes segmentos que compõem a opção "Outro"

Segmentos
• Administração Pública.
• Auditoria.
• Auditoria interna no corporativo de empresas privadas e de consultoria, como "*big four*".
• Contabilidade Forense.
• Consultoria.
• Empresa americana que paga salários em criptomoedas.
• Instituto de auditoria independentes.
• Investigação e processamento de empresas privadas envolvidas em casos de corrupção na Administração Pública.
• Laboratório de Tecnologia contra LD – Polícia Civil do Estado de Goiás/Núcleo de Operações com Criptoativos/Coordenação Geral de Combate ao Crime Organizado (CGCCO)/ Secretaria de Operações Integradas (SEOPI)/Ministério da Justiça e Segurança Pública.
• Polícia Federal – Setor de perícia criminal.
• Polícia Judiciária, Representação em Delegação Brasileira perante o GAFI e Avaliador do GAFI, com formação no Grupo InterGovernamental de Acção contra o Branqueamento de Capitais na África Ocidental (GIABA) e Programa das Nações Unidas para o Desenvolvimento (PNUD) no Ocidente Africano.
• Unidade de Inteligência Financeira (UIF) e órgão regulador.

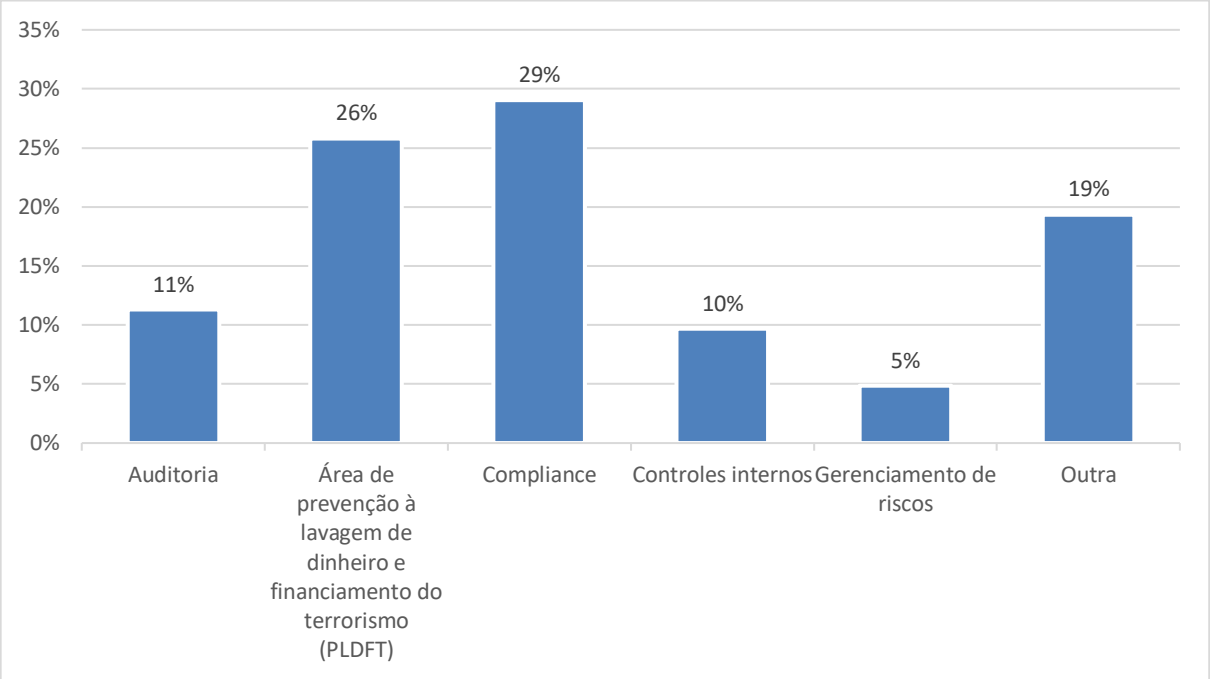
Fonte: Elaborado pelo autor com base nos dados da pesquisa.

4.1.1.8 Área de Atividade em que se Concentra a Experiência de PLD-FT e Criptoativos

Em relação à área de atividade que se concentra a experiência dos respondentes com PLD-FT e criptoativos, de acordo com o **Gráfico 8**, a maioria dos respondentes, aproximadamente 29%, tem na área de *compliance* sua concentração de experiência com PLD-FT e criptoativos.

Para cerca de 26% dos respondentes, a área de PLD-FT é onde se concentra sua experiência, para 11%, a área de auditoria, para 10%, a área de controle interno e para 5%, a área de gerenciamento de risco.

Gráfico 8 – Área de atividade que se concentra a experiência dos respondentes com PLD-FT e criptoativos



Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Conforme o **Gráfico 8**, para aproximadamente 19% dos respondentes a opção "Outra" é onde se concentra sua experiência com PLD-FT e criptoativos.

A opção "Outra" representa diferentes áreas de atividades em que se concentra a experiência dos respondentes com PLD-FT e criptoativos, conforme **Quadro 18**.

Quadro 18 – Diferentes áreas de atividades que compõem a opção "Outra"

Áreas
• Advocacia Criminal Contenciosa.
• Corregedoria (aplicação da Lei Anticorrupção).
• Desenvolvimento de sistemas e projetos.
• Investigação.
• Investigação criminal.
• Investigação forense.
• Órgão de persecução penal.
• Polícia Judiciária – Laboratório de Tecnologia contra LD – Polícia Civil do Estado de Goiás/Núcleo de Operações com Criptoativos/CGCCO/SEOPI/Ministério da Justiça e Segurança Pública.
• Prevenção e combate (Uma vez que atividade pericial pode desempenhar tanto funções de prevenção, quanto de combate à LD).
• Tecnologia da Informação (TI).

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

4.1.2 Riscos e Desafios de Crime de Lavagem de Dinheiro Enfrentados ao Lidar com Criptoativos

Nesta seção serão abordados os riscos e desafios de crime de LD enfrentados ao lidar com criptoativos, apresentando as percepções obtidas dos respondentes por meio das perguntas que se seguem.

4.1.2.1 Vulnerabilidades associadas às práticas e serviços oferecidos

Na **Tabela 6** são descritos os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito das vulnerabilidades associadas às práticas e serviços oferecidos que são comumente explorados por criminosos na condução de atividades de LD por meio do uso de criptoativos.

Tabela 6 – Frequência com que as vulnerabilidades associadas às práticas e serviços oferecidos são exploradas nos crimes de LD com criptomoedas

Assertiva	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
9.1 Assessoria/consultoria financeira e tributária.	3%	16%	26%	23%	21%	11%
9.2 Formação de empresas e *trustes*.	5%	11%	19%	21%	27%	16%
9.3 Compra/venda de imóveis e estabelecimentos comerciais/industriais.	3%	18%	20%	30%	20%	10%
9.4 Gestão de fundos, valores mobiliários e outros ativos.	0%	23%	16%	23%	31%	7%
9.5 Prestação de serviços não presenciais (internet, correio, telefone).	5%	16%	20%	26%	20%	13%
9.6 Transferência eletrônica de fundos e valores mobiliários.	5%	11%	13%	40%	26%	5%
9.7 Realização de apresentações para instituições financeiras, com profissionais específicos como intermediários.	11%	13%	11%	15%	19%	31%
9.8 Prestação de serviços a clientes residentes no exterior.	6%	8%	23%	21%	23%	19%
9.9 Privilégio profissional legal e confidencialidade do cliente.	8%	13%	19%	23%	18%	19%
9.10 Obrigações *anti-money laundering* (AML) limitadas para Atividades e Profissões Não-Financeiras Designadas (APNFDs).	3%	8%	20%	28%	18%	23%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

As vulnerabilidades observadas, ora associadas às práticas e serviços oferecidos foram consideradas com significante nível de ocorrência, onde as assertivas 9.6 “Transferência eletrônica de fundos e valores mobiliários” e 9.4 “Gestão de fundos, valores mobiliários e outros ativos” são as que apresentam maiores oportunidades de serem exploradas nos crimes de LD por meio do uso de criptomoedas.

No **Quadro 19** são expostos os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com os temas classificados.

Quadro 19 – Quadro matricial da categoria das vulnerabilidades associadas às práticas e serviços oferecidos que são exploradas nos crimes de LD com criptomoedas

Categoria: Vulnerabilidades associadas às práticas e serviços oferecidos	
Temas	**Comentários**
Risco de ser usado para LD	**R20**: As vulnerabilidades relacionadas às práticas de lavagem de dinheiro com o uso de criptoativos são frequentemente exploradas nos segmentos de transferências eletrônicas de ativos financeiros, tendo em vista que os criptoativos são todos manipulados eletronicamente, favorecendo a transformação de ativos sujos para os ativos limpos no processo de lavagem de capitais com o uso de criptomoedas. **R26**: Atribuir a lavagem de dinheiro ao pagamento de serviços de assessoria/consultoria financeira e tributária associa-se a formação de empresas e *trustes*, digo isso porque a constituição da empresa teria origem maliciosa, pois do contrário, caso o criminoso desejasse utilizar esse serviço e a empresa prestadora de serviços executasse um processo de diligência, o criminoso teria grandes chances de ser denunciado. Desta forma, considero a opção 9.1 com frequência ocasional. Para a compra/venda de imóveis e estabelecimentos comerciais/indústrias, no Brasil, utilizando criptomoedas exigiria uma rede criminosa que estivesse presente em todos os personagens da transação, pois é necessário: (i) partes interessadas de compra e venda, (ii) cartório de registro de imóveis, (iii) cartório de notas, (iv) corretor de imóveis, e (v) instituição financeira. Caso o criminoso tenha a criptomoeda e desejar efetivar uma compra, ele deverá converter em moeda nacional corrente, que somente é possível por meio de uma instituição financeira, que identificaria imediatamente uma movimentação atípica. Se o criminoso, ainda quiser reduzir a rastreabilidade, ele deveria transferir a criptomoeda, entre carteiras de laranjas, que transfeririam o dinheiro para contas bancárias, sem gerar suspeitas, e fariam saque de moeda em espécie, para juntar o montante financeiro e pagar em dinheiro. Considero esse caso, raramente, pois é necessária uma rede criminosa complexa, falha de controles da instituição financeira, cartórios colaborando com o criminoso e o corretor de imóveis como parte no esquema. **R37**: O que já presenciei no uso de criptoativos não se limita apenas a lavagem de dinheiro, mas principalmente a recebimentos de valores por venda ou prestação de serviço por meio de caixa dois, devido ao sigilo e a irrastreabilidade das transações. **R54**: A transferência eletrônica de fundos (normalmente valores mobiliários) traz uma grande preocupação (vulnerabilidade) em razão do caráter anônimo das transferências que envolvem criptoativos.

Risco de ser usado para facilitar a LD por outra pessoa	**R17**: Na minha prática profissional, entendo que a maior vulnerabilidade seja a criação de empresas de fachada, com negociações forjadas, para fluxo de recursos ilícitos. **R31**: Durante os últimos 15 anos tive a oportunidade de trabalhar com questões ligadas ao setor financeiro, onde os casos mais clássicos para Lavagem de Dinheiro foram as empresas de consultoria de faixada e formação de empresas fantasmas ou em paraísos fiscais.
Risco de sofrer danos legais, regulatórios ou de reputação por não ter identificado os sinais de alerta de LD e relatado	**R1**: Penso que qualquer negócio pode ser objeto de lavagem com criptomoedas, na mesma medida que negócios lícitos, o que muda é a origem desse recurso, se ilícito denota LD. **R11**: A utilização de criptoativos para fins de lavagem de dinheiro, em sua grande maioria, está associada a pagamentos ocultos, de difícil identificação. **R21**: Importante ressaltar que o ecossistema de criptoativos permite que o usuário consiga agir sem a necessidade de serviços especializados já que o controle das chaves privadas permite total controle dos ativos, sem a necessidade de intermediações. No entanto, certamente os serviços oferecidos para o sistema financeiro encontrarão correspondência no mercado cripto, que permite até mesmo a criação de cardápio de serviços não existente no cenário das práticas de AML tradicionais. **R27**: Considero que as maiores vulnerabilidades estão nos setores de assessorias, consultorias e ambientes não regulados, isto porque os ambientes regulados contam com robustos (mas, não por isso, absolutamente suficientes) controles de conhecimento normativo e de tendências, prevenção, monitoramento e resposta. **R32**: A maioria das práticas mencionadas possui margem para a lavagem de dinheiro, especialmente por criptomoeda ser um ativo de difícil rastreamento e pela tempestividade nas transações, o que leva a um maior volume de transações em um curto espaço de tempo, inclusive para exchanges ou wallets estrangeiras que não necessariamente são conhecidas e/ou seguem as exigências mínimas globais de PLD/FT conforme orientação de reguladores, como o GAFI. **R52**: Importante reforçar que, muito embora o comum da Lavagem de Dinheiro desassociada à tecnologia fosse criar novas empresas, contratar pessoas laranjas ou locar/adquirir novos lugares, a lavagem com operações de criptoativos dão maior importância ao: a. sistemas de cryptocurrency de rastreabilidade e com registro em países de baixo aspecto regulatório, bem como a ter profissionais com vasto conhecimento tecnológico atuando em diversas 'pessoas', como nas próprias exchanges, em bancos, em sistemas provedores e até para a própria Associação Criminosa. **R58**: Por tratar-se de uma moeda com alta volatilidade, é comumente usada por "assessores de investimentos falsos", tendo como estratégia alto retorno e investimento garantido. Além de escritórios de alto padrão, propagandas ostensivas nas mídias e contratos sigilosos (eles operam muito como uma seita criminosa, tentam o máximo mascarar seu "modus operandis"). Apesar de usarem muito o lado ostensivo a favor deles, como forma de mostrar maior credibilidade e confiança para sua carteira de clientes, eles tentam o máximo mascarar seu modo estratégico e operacional. Classificamos este tipo de operadores como "piramedeiros" [*sic*], por utilizar-se da estratégia de marketing multinível como forma de escalar suas operações.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Quadro 19**, é possível entender que, segundo R1, a origem dos recursos é relevante para determinar o crime de LD com criptomoedas, uma vez que na mesma medida que negócios lícitos, qualquer negócio pode ser objeto de LD com criptomoedas, devido a origem de recursos ilícita. R17 e R31 consideram a formação de empresas de fachada, com negociações forjadas para a liquidez de recursos ilícitos, como sendo a prestação de serviço com significante nível de ser explorada nos crimes de LD por meio do uso de criptomoedas.

Para R26, a LD por meio de pagamentos de serviços de assessoria/consultoria financeira e tributária (Assertiva 9.1 na **Tabela 6**) pode ser associada a formação de empresas e *trustes* (Assertiva 9.2 na **Tabela 6**), quando há cumplicidade dos atores envolvidos na prestação de serviços da assertiva 9.1 com as operações ilícitas, caso contrário, na execução dos processos de diligência, o criminoso poderia ser denunciado. Assim sendo, a assertiva 9.1 é considerada por R26, com frequência ocasional à exploração por parte de clientes que procuram fazer uso indevido de serviços legítimos para fins de LD com criptomoedas.

Contudo, para R27, os setores de assessorias, consultorias e ambientes não regulados guardam as maiores vulnerabilidades relacionadas às práticas de LD com criptomoedas, devido ao fato dos robustos controles de conhecimento normativo, prevenção, monitoramento e resposta, presentes em um ambiente regulado, não serem suficientes quando do envolvimento de criptomoedas. Países com baixos aspectos regulatórios, a utilização de sistemas de *cryptocurrency* de irrastreabilidade de transações e profissionais com amplo conhecimento tecnológico atuando junto à diferentes participantes do mercado de criptomoedas, mantêm, segundo R52, significante nível de importância para usuários que praticam crimes de LD através de operações com criptomoedas. A associação dos serviços oferecidos ao sistema financeiro tradicional com o mercado de criptomoedas, de acordo com R21, criará diferentes opções de serviços antes inexistentes no cenário das práticas de AML tradicionais.

Quanto à assertiva 9.3 na **Tabela 6**, R26 entende que sua ocorrência seja rara, devido a necessidade de uma rede criminosa complexa, falha de controles das IFs envolvidas e a cumplicidade dos cartórios e corretores de imóveis. R26 explica que a compra/venda de imóveis e estabelecimentos comerciais/industriais, no Brasil, com criptomoedas, exigiria a cumplicidade de todos os envolvidos na transação. Como etapa de integração no crime de LD, onde a conversão de criptomoedas em moedas fiduciária é realizada para aquisição de imóveis, R26 discorre sobre os caminhos possíveis para a execução dessa etapa, conforme o **Quadro 19**.

De acordo com os relatos de R20 e R54, a possibilidade de manipulação eletrônica das criptomoedas e o caráter anônimo das transferências envolvendo criptomoedas, viabilizam a

execução do processo de LD com uso de criptomoedas, uma vez que a conversão de ativos com origem criminosa em ativos lícitos é favorecida, trazendo grande atenção em torno da transferência eletrônica de ativos financeiros, como valores mobiliários envolvendo criptomoedas.

Para R11, as transações com difícil identificação dos participantes, geralmente estão associadas aos crimes de LD com criptomoedas. R21 ressalta que o usuário do ecossistema de criptomoedas, ao manter a posse das chaves privadas, tem total controle das criptomoedas para realizar operações sem o auxílio de serviços especializados, ou seja, sem a necessidade de intermediações. R32 entende que a maioria das práticas mencionadas na **Tabela 6** possui margem para LD com criptomoedas, devido às características de difícil rastreabilidade e tempestividade das transações envolvendo criptomoedas, que permitem maior volume de operações em um curto espaço de tempo, preferencialmente por meio de *exchanges* ou *wallets* estrangeiras que nem sempre são conhecidas e/ou seguem as obrigações mínimas globais de PLD-FT, de acordo com as orientações de reguladores, como o GAFI.

Outros crimes financeiros, que na maioria das vezes estão associados ao crime de LD, são mencionados por R37 e R58. Segundo R37, devido a possibilidade de sigilo e irrastreabilidade nas transações, as criptomoedas são utilizadas para a prática de “caixa dois”. Graças a característica de ser um ativo de alta volatilidade (ativo cujo preço varia muito e de maneira muito rápida), as criptomoedas, conforme R58, são frequentemente usadas por “assessores de investimentos falsos”, que apresentam como estratégia para atrair investidores, a garantia de alto retorno dos investimentos, caracterizando assim, a prática fraudulenta de captação de dinheiro conhecida como “esquema de pirâmide financeira”. No **Quadro 19**, R58 discorre sobre as principais características dessa operação.

4.1.2.2 Fatores de risco de lavagem de dinheiro

Na **Tabela 7** estão presentes os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa acerca dos fatores de risco de LD ao lidar com criptomoedas.

Todos os fatores de risco de LD ao lidar com criptomoedas observados foram considerados com significante nível de relevância, tendo as assertivas 10.2 “Clientes que conduzem seu relacionamento comercial em circunstâncias incomuns/não convencionais” e 10.5 “Clientes em que o relacionamento dificulta a identificação oportuna do verdadeiro beneficiário final” representando maior grau de importância.

Tabela 7 – Relevância dos fatores de risco de LD ao lidar com criptomoedas

Assertiva	Sem importância	Pouco importante	Razoavelmente importante	Importante	Muito importante	Não saberia optar
10.1 Clientes cuja origem/localização atual da fonte de suas riquezas/fundos está associada a um país de maior risco.	2%	0%	13%	24%	56%	5%
10.2 Clientes que conduzem seu relacionamento comercial em circunstâncias incomuns/não convencionais.	0%	0%	5%	29%	61%	5%
10.3 Transferências de bens que são inerentemente difíceis de avaliar, como ativos virtuais, onde isso não é comum para o tipo de clientes.	0%	0%	8%	24%	61%	6%
10.4 Clientes residentes em um país/região geográfica de alto risco.	2%	3%	10%	32%	48%	5%
10.5 Clientes em que o relacionamento dificulta a identificação oportuna do verdadeiro beneficiário final.	2%	0%	3%	18%	71%	6%
10.6 Serviços em relação a ofertas iniciais de moedas (*Initial Coin Offering* – ICO).	2%	6%	21%	24%	34%	13%
10.7 Cliente com beneficiário final residente em um país/região geográfica de alto risco.	2%	3%	6%	23%	61%	5%
10.8 Clientes com negócios intensivos em dinheiro/equivalente, como corretores e outros prestadores de serviços em ativos virtuais.	0%	10%	19%	23%	44%	5%
10.9 Uso de ativos virtuais em transações sem aparente motivo legal, tributário, comercial e econômico.	2%	2%	8%	23%	58%	8%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Conforme o **Quadro 20**, onde estão expostos os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com os temas classificados, R21 e R56 relatam que a natureza transfronteiriça das criptomoedas aumenta o nível de risco de serem utilizadas na LD. Contudo, para R24, a origem/localização atual da fonte de riquezas/fundos é determinante no uso das criptomoedas na LD, e não as características das criptomoedas em si.

De acordo com R58, a utilização maliciosa das criptomoedas geralmente ocorre por meio de *exchanges* e *hashes* com IPs de paraísos fiscais, como Suíça e Ilhas Cayman. No entendimento de R32, a geolocalização é um fator importante na PLD, na medida em que alguns países não seguem diretrizes e boas práticas de transparências nas transações envolvendo, tanto moeda fiduciária como criptomoedas. Nesse sentido, R55 aponta como resultados das assertivas 10.1 e 10.4 na **Tabela 7**, a ausência de realização de operações, por parte de IFs, com clientes que possuem fundos em jurisdição com deficiência de controles para AML, e o impedimento,

por meio do processo de checagem de listas restritivas no momento de abertura e manutenção de conta, dos clientes residentes em países identificados como de alto risco de LD. Esses clientes, conforme R52, ao solicitarem informações sobre aquisição de imóveis com criptomoedas, são classificados como de alto risco. No entanto, R28 entende que há uma preocupação exacerbada em relação aos países identificados como de alto risco, visto que a participação desses países é irrisória, gerando trâmites quase inexistentes.

Quadro 20 – Quadro matricial da categoria dos fatores de risco de LD ao lidar com criptomoedas

Categoria: Fatores de risco de LD	
Temas	**Comentários**
Risco país/geográfico	**R20**: Esta é uma questão extremamente sensível. Os pontos 10.7, 10.8 e 10.4 podem ser tidos, à primeira vista, apenas como *red flags* indicativas de uma prática de *laudering*. Entretanto, o fato de serem *red flags* apresenta um ponto de sensibilidade em relação à implementação de programas de governança e *compliance* destinados a "perseguir" tais pontos de atenção, tendo em vista que pode gerar uma limitação da liberdade de operacionalização financeira do usuário, ao passo que o ponto 10.2 demanda o incremento de uma política de *know your client* eficaz, sob pena de incorrer nos mesmos riscos anteriormente expostos. Numa análise sob uma ótica expandida, todos os pontos levantados nesta pergunta conduzem ao mesmo problema: não podem ser analisados por si só numa política de prevenção à lavagem de dinheiro com o uso de criptoativos. **R21**: A neutralidade do *blockchain*, assim como a possibilidade de transações ponto a ponto entre pessoas localizadas em diversos países por certo serão fatores agregadores de risco para as práticas de combate à lavagem de dinheiro. **R24**: Entendo que a questão geográfica sobre a fonte e origem do dinheiro ou destino é determinante para o uso de Lavagem de Dinheiro em cripto ativos, e não o mecanismo "cripto" ou virtual em si. **R28**: Eu acho que existe uma preocupação exacerbada com países percebidos em alto risco, eles quase nunca aparecem, a participação é irrisória e gera trâmites quase inexistentes. [...]. **R32**: A geolocalização é um fator importante e relevante na prevenção à lavagem de dinheiro [...]. [...] nem todos os países seguem diretrizes e boas práticas de transparência, seja em moeda fiduciária ou em criptoativos [...]. **R52**: [...] clientes de países de alto risco que solicitam informações sobre procedimentos de compra de imóveis [...] utilizando criptomoedas. [...]. **R55**: Clientes cuja origem/localização atual da fonte de suas riquezas/fundos está associada a um país de maior risco – Em grande maioria as instituições não realizam operações com clientes que possuem fundos em jurisdição com deficiência de controles para AML. O mesmo se repete para cliente residente em pais de alto risco para Lavagem de Dinheiro, eles são barrados no processo de checagem de listas restritivas na abertura e manutenção da conta. **R56**: A natureza transfronteiriça dos ativos virtuais apresenta risco adicional pois aumenta o potencial de transferências de ativos de/para contrapartes e/ou jurisdições sancionadas.

	R58: Frequentemente os usuários maliciosos de criptomoedas utilizam exchanges e hash's [*sic*] com IP's [*sic*] de paraíso fiscal (suíça, ilhas Cayman e etc...). [...].
Risco de cliente	**R22**: [...] A rigor, a existência de negócios em si não é problema, e o viés investigativo parte de uma premissa equivocada de que há algo errado. No direito brasileiro prevalece o princípio da presunção de inocência. [...]. **R27**: Em PLD-FTP, há de se tomar o cuidado de distinguir entre suspeitas, indícios e crimes. É importante ter a sensibilidade, sobretudo no cotidiano da prática, de não criminalizar antecipadamente determinadas condutas que, sim, representam um risco potencial, mas devem ser averiguadas. O papel das áreas de Governança/*Compliance*/Auditoria/PLD-FTP é de análise e não de julgamento. **R44**: O fator mais importante acredito que esteja relacionado à dificuldade de identificação do beneficiário final, especialmente quando se trata de privilégio profissional. **R52**: [...]. Ainda, colocávamos como de alto risco clientes familiares entre si, clientes PEP [...].
Risco de transação/serviços e canal de entrega associado	**R26**: Um dos principais cenários que devem ser observados no uso de criptomoedas relacionado a lavagem de dinheiro são aqueles onde a transação financeira ocorre exclusivamente por redes de computadores ("Internet"), seja na *surface web* ou na *deep web*, restando para conclusão a prestação/entrega do serviço/produto. Podemos considerar como caso de rastreabilidade muito difícil, quando movimentações ilícitas têm sua origem e enriquecimento pela Internet, e a criptomoeda nunca é convertida em moeda corrente do país onde o criminoso está atuando. Como exemplo, o criminoso recebe o pagamento de uma fonte lícita de receita, proveniente do comprador ou contratante, que converteu a moeda corrente do seu país em criptomoeda para realizar o pagamento. O criminoso, por sua vez, controla seu caixa exclusivamente em criptomoedas e financia sua rede de fornecedores e distribuidores. Há um grande alerta de risco, que pode aumentar o poder transacional de criminosos, se bens, bens de consumo e serviços começarem a aceitar criptomoedas como mecanismo final de pagamento. **R31**: As conhecidas moedas virtuais ganharam o mercado por conta de sua vantagem competitiva em relação a outros ativos de investimentos. Porém, ainda é prematuro afirmar que se trata de uma operação [...], rastreável [...]. **R37**: Transações de alto valor realizadas num único pagamento ou recorrentes em valores pequenos e que possam caracterizar fracionamento. O spread das transações realizadas em criptoativos também é difícil de ser controlado. É válido avaliar os ganhos de capital e crescimento de patrimônio a partir da carteira digital. **R54**: A localização geográfica já não oferece tanta importância porque as carteiras virtuais (cold e hot wallets) podem ser acessadas pelos seus titulares em qualquer lugar do mundo. **R58**: [...]. Toda moeda virtual nova é passível de utilização para o crime de lavagem de dinheiro, pois além da operação de lavagem virtual, os usuários ganham na valorização do ativo virtual novo, por tratar-se de uma novidade/oportunidade para o mercado cripto.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

De acordo com o **Quadro 20**, R52 relata que clientes familiares entre si e pessoas expostas politicamente (PEPs) são classificados como de alto risco, sendo a dificuldade de

obtenção de informações sobre o beneficiário final, no entendimento de R44, um importante fator de risco de LD ao lidar com criptomoedas, que pode aumentar quando do privilégio profissional legal.

R26 aponta a dificuldade de rastrear transações financeiras envolvendo criptomoedas que ocorrem exclusivamente na Internet (*surface web* ou *deep web*), como um significativo fator de risco de LD ao lidar com criptomoedas. Explica que um caso de difícil rastreabilidade pode surgir em um cenário de movimentações ilícitas que têm sua origem e enriquecimento na Internet e com a ausência de um ponto de intercessão entre o ecossistema virtual e o sistema financeiro do país alvo do criminoso, quando da não conversão das criptomoedas em moedas fiduciária. R26 exemplifica, conforme o **Quadro 20**, o alerta a respeito da liquidez do mercado de criptomoedas, que facilita a integração de riquezas/fundos dos criminosos, poder ser potencializada pelo aumento da lista de bens e serviços para os quais o pagamento em criptomoedas é aceito. Ainda sobre a dificuldade de rastrear transações financeiras envolvendo criptomoedas, R31 expõe que, apesar das criptomoedas terem aumentado sua participação no mercado de capitais, devido vantagens competitivas sobre outros ativos de investimentos, é prematuro afirmar que as operações envolvendo criptomoedas podem ser rastreadas. Igualmente, R37 relata que o *spread* das transações com criptomoedas também apresenta dificuldades de ser rastreado, sendo válida uma análise nas carteiras digitais utilizada nas transações. R58 relata a possibilidade de novas criptomoedas serem utilizadas na LD, devido as oportunidades de ganhos na valorização dessas novas criptomoedas no mercado cripto.

R37 sinaliza, também, como fator de risco de LD ao lidar com criptomoedas, a realização de transações de alto valor em um único pagamento, ou transferências em pequenas quantias. Essas transferências, quando realizadas entre carteiras virtuais, permitem que a origem de riquezas/fundos dos criminosos seja ofuscada, podendo, conforme R54, atenuar a importância da geolocalização devido seu acesso em qualquer lugar do mundo.

Para R20, a questão a respeito dos fatores de risco de LD ao lidar com criptomoedas é extremamente sensível, e que numa análise ampliada, é possível concluir como inadequada, a análise isolada de cada assertiva na **Tabela 7** durante o cumprimento de uma política de PLD envolvendo criptomoedas. R20 entende que a implementação de programas de governança e *compliance* destinados a atenuar os riscos de LD ao lidar com criptomoedas, quando somente da presença das *red flags* indicativas de uma prática de *laudering*, podem gerar uma limitação da liberdade de operacionalização financeira do cliente. Nesse sentido, R27 sinaliza que o papel das áreas de governança/compliance/auditoria/PLD-FT é de análise e não de julgamento, onde

a cautela na distinção entre suspeitas, indícios e crimes deve se fazer presente. R27 menciona a importância da sensibilidade de não criminalizar antecipadamente determinadas condutas que, na medida em que representam um risco potencial, devem ser averiguadas. Para R22, a mera existência do negócio em si não sinaliza um problema, mas a premissa equivocada de que há algo de errado conduz a um viés investigativo, uma vez que, no direito brasileiro, prevalece o princípio da presunção de inocência.

4.1.2.3 *Red flag indicators* para AML/CFT

Na **Tabela 8** estão presentes os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito dos *red flag indicators* sobre LD com criptomoedas.

Tabela 8 – Frequência dos *red flag indicators* sobre LD com criptomoedas

Assertiva	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
11.1 Os fundos do cliente são originados/enviados para uma *exchanger* que não está registrada na mesma jurisdição do cliente.	0%	10%	21%	24%	32%	13%
11.2 Cliente fornece identificação/conta (um endereço *Internet Protocol* – IP não padrão) compartilhadas por outra conta.	2%	8%	23%	16%	27%	24%
11.3 Transferência em quantias abaixo dos limites de manutenção de registros/relatórios.	3%	6%	21%	29%	32%	8%
11.4 O cliente utiliza *exchanger* localizada em jurisdição de alto risco com regulamentos *anti-money laundering* (AML) inadequados.	2%	5%	13%	13%	55%	13%
11.5 Cliente com endereço IP associado a seu perfil diferente do endereço IP pelo qual as transações estão sendo iniciadas.	2%	8%	24%	24%	24%	18%
11.6 Realização de várias transações de alto valor com padrão escalonado e regular.	3%	7%	23%	26%	31%	10%
11.7 O cliente utiliza provedor de serviços de ativos virtuais (PSAV) que opera em jurisdição sem regulamentação para ativos virtuais.	2%	10%	16%	23%	29%	21%
11.8 Clientes que utilizam vários cartões de crédito/débito vinculados a uma carteira de criptomoedas.	3%	10%	19%	16%	29%	23%
11.9 Transação anormal (nível e volume) de criptomoedas em *exchangers* de carteiras associadas à plataforma *peer-to-peer* (P2P).	2%	6%	19%	16%	40%	16%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Os *red flag indicators* sobre LD com criptomoedas vistos foram considerados com significante nível de ocorrência, onde as assertivas 11.4 “O cliente utiliza *exchanger* localizada em jurisdição de alto risco com regulamentos *anti-money laundering* (AML) inadequados” e 11.3 “Transferência em quantias abaixo dos limites de manutenção de registros/relatórios” apresentam as maiores ocorrências.

Segundo o **Quadro 21**, em que estão os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com os temas classificados, R56 explica que as transações envolvendo PSAVs domiciliados ou operados em jurisdições sem regulamentação AML sobre AVs e PSAVs, não são devidamente monitoradas.

A esse respeito, R18 relata que, mesmo com a ausência de uma regulamentação específica para operações envolvendo criptomoedas no Brasil, a CVM permitiu que alguns fundos no Brasil investissem em criptomoedas. Contudo, R21 sinaliza que as transações realizadas com PSAV não domiciliados no Brasil, facilitada pela ausência de fronteiras na Internet, não caracteriza, por si só, a existência de um risco em potencial.

R31 afirma que por meio dos *red flag indicators*, a *exchange* deve classificar o *score* de risco de determinado cliente, elaborando políticas de monitoramento, que devem ser revisadas tempestivamente, com objetivo de mitigar os riscos associados a carteira de criptomoedas. Para R54, um dos *red flag indicators* mais comum, está no cliente solicitar um aumento de seu limite para operações com criptomoedas sem comprovar sua capacidade financeira para tais operações. Da mesma forma, R32 sinaliza a respeito da importância de se entender o perfil do cliente, seus aportes, a origem dos recursos e como este cliente gerencia sua carteira. R32 exemplifica, conforme o **Quadro 21**, o alerta a respeito de uma transação realizada fora do padrão de perfil do cliente. A análise do perfil do cliente, como a identificação do cliente, de acordo com R20, é um dos fatores que desencorajam os criminosos de usarem cartões de crédito e débitos para a LD com criptoativos.

Conforme R58, dentre os *red flag indicators* sobre LD no ecossistema das criptomoedas, os associados aos endereços e IPs, localização da operação e controles extraídos da Lei nº 12.683 de 2012, são os mais importantes e mais complexos quando se tratando de transações P2P, devido à ausência de um intermediário para a aplicação do processo de KYC. As operações P2P, segundo R20, são mais utilizadas pelos usuários que desejam realizar atividades criminosas, na intenção de evitar o processo de KYC aplicado pelas *exchanges*. Em linha com R58, R21 expõe que a análise dos endereços de IP do cliente é um importante indicador de risco

de LD ao lidar com criptomoedas, mas que, devido a especificações técnicas observadas no **Quadro 21**, deve ser feita em conjunto com os demais *red flag indicators*.

Quadro 21 – Quadro matricial da categoria dos *red flag indicators* sobre LD com criptomoedas

Categoria: *Red flag indicators*	
Temas	**Comentários**
Etapa de colocação	**R18**: Com relação a questão 11.7, nem mesmo no Brasil temos regulamentação para operações com criptoativos. A CVM permitiu alguns fundos terem um % de Criptomoedas na carteira, mas não temos uma regulamentação que protege o cliente. **R32**: Cada cliente possui um perfil de operação e um comportamento que usualmente é padrão, sendo possível monitorar semanalmente/mensalmente. Um cliente que realiza depósitos de 4 mil mensais por exemplo levantaria suspeitas ao depositar 10 mil mensalmente. De onde veio a origem dos recursos? Por que ocorreu uma mudança tão significativa no volume de transações? É extremamente importante entender o perfil do cliente, seus aportes, origem dos recursos e como ele gerencia sua carteira. **R54**: Um dos red flags mais comuns, entretanto, está associado ao pedido de aumento de limite operacional sem que o cliente consiga (adequadamente) comprovar capacidade financeira para transacionar volumes financeiros mais altos.
Etapa de ocultação	**R21**: Importante frisar que a análise dos endereços de IP do cliente, em que pese ser um indicador de risco importante, deve ocorrer em conjunto com os demais indicadores em razão de especificidades técnicas como o dinamismo dos números de IP atribuídos pelos provedores de conexão, utilização de mais de um provedor de conexão, utilização de VPN por questões de segurança. Ainda, a não existência de fronteiras na internet é propícia à utilização de VASP não domiciliadas no Brasil, o que não quer dizer, por si só, que o cliente é um risco em potencial. **R31**: As Red Flags devem observar o comportamento do investidor e passar a classificar o seu Score de Risco. Cada Exchange tem a sua política de monitoramento, entretanto, o indivíduo fraudador também conhece como são essas políticas e portanto as mesmas devem passar por revisões tempestivas para mitigar desvios de comportamento da carteira de ativos eletrônicos.
Etapa de integração	**R20**: O problema de uso de cartões de crédito e débito para operar criptoativos – sobretudo com finalidades ilícitas – é que gera, quase que necessariamente, a identificação e individualização do usuário, o que não é agradável para quem utiliza criptomoedas para as práticas criminosas. Inclusive, o mais comum é que o usuário que objetiva uma operação de lavagem de dinheiro com criptoativos utilize de operações p2p, ao invés de *exchanges*, sobretudo recentemente, que a muitas *exchanges* exigem alguns dados de identificação do usuário. **R56**: O fato de não haver uma regulamentação estabelecida em diversas jurisdições associado ao fato de não haver uma equalização entre as regulamentações já em vigor em outras jurisdições, possibilita transações com VASPs em qualquer localidade, bem como a realização de transações sem que haja o devido monitoramento. **R58**: Uns dos meios mais importantes de identificar transações ilícitas no ambiente cripto é por meio dos endereços e ip's [*sic*], localização da operação (fazendo um confronto com a operação de origem versus a operação que o dinheiro foi destinado), controle que é extraído da lei de PLD 12.683. Uma das etapas mais complexas são as transações p2p, pois não temos um intermediário para realizar o processo de KYC.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

4.1.2.4 *Red flag indicators* associados ao anonimato

Na **Tabela 9** constam os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito dos *red flag indicators* associados ao anonimato ao lidar com criptomoedas. Todas as assertivas foram consideradas com significante nível de ocorrência, onde as assertivas 12.1 e 12.10 apresentam as maiores ocorrências.

Tabela 9 – Frequência com que os *red flag indicators* associados ao anonimato são explorados ao lidar com criptomoedas

Assertiva	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
12.1 Transações envolvendo mais de um tipo de criptomoeda, incluindo as que fornecem maior anonimato.	0%	3%	18%	21%	47%	11%
12.2 Mover criptomoeda de *blockchain* pública e transparente para uma *exchanger* centralizada e logo trocá-la para criptomoeda de anonimato.	2%	8%	16%	23%	39%	13%
12.3 Operações realizadas em *sites* de troca *peer-to-peer* (P2P).	0%	3%	21%	23%	38%	15%
12.4 Transações com serviços de *mixing cryptocurrency*, sugerindo a intenção de ocultar o fluxo de fundos ilícitos entre mercados *darknet*.	2%	2%	10%	23%	39%	26%
12.5 Fundos movimentados em carteira com *links* de exposição direta e indireta para fontes suspeitas conhecidas, incluindo mercados *darknet*.	0%	8%	6%	23%	34%	29%
12.6 O uso de carteiras de *hardware* descentralizadas/não hospedadas para transportar ativos virtuais além das fronteiras.	2%	8%	19%	11%	32%	27%
12.7 Usuários de provedores de serviços de ativos virtuais (PSAV) registrando seus nomes de domínio da Internet por meio de *proxies*.	2%	5%	21%	24%	13%	35%
12.8 Usuários de PSAV usando um endereço *Internet Protocol* (IP) associado a *darknet.*	0%	6%	13%	23%	19%	39%
12.9 Grande número de carteiras de ativos virtuais aparentemente não relacionadas, controladas a partir do mesmo endereço IP.	0%	3%	18%	32%	26%	21%
12.10 Transações utilizando meios de comunicação criptografados anônimos, como fóruns, *chats*, aplicativos móveis e jogos *online*.	0%	5%	15%	23%	44%	15%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

No **Quadro 22** são expostos os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com o tema classificado.

Quadro 22 – Quadro matricial da categoria dos *red flag indicators* associados ao anonimato com criptomoedas

Categoria: *Red flag indicators* associados ao anonimato	
Tema	**Comentários**
Estratégias de anonimato	**R20**: Basicamente, as operações de lavagem com criptoativos objetivam esconder a fonte da receita ilícita e o rastro que esta receita faz até o processo final de reintegração do capital na economia formal. Para isto, os serviços de mixing são muito úteis, além das operações p2p e canais de comunicação anônimos. **R21**: É comum a utilização de *hardware wallets*, assim como seu transporte. A segurança ofertada por tais dispositivos acaba trazendo mais usuários com maior volume de ativos. Também é comum que um mesmo usuário controle dezenas ou centenas de endereços diferentes em razão da forma como seu *client* de *wallet* gerencia a criação de novos endereços de troca, por exemplo. **R32**: [...] não vejo este tipo de comportamento tão recorrente na América Latina que é o foco da minha CIA. Já recebi relatos de amigos que trabalham em exchanges maiores e globais que enfrentam esses problemas mais elaborados, especialmente no que tange alteração de IPs, proxys [*sic*], anonimato e criptos não tão conhecidas. **R54**: A grande maioria das exchanges de criptoativos que estão registradas em mercados já regulados possuem procedimentos de KYC, CDD/EDD satisfatórios e que não permitem o completo anonimato dos clientes. O anonimato ocorre quando os criptoativos saem das exchanges e vão para carteiras privadas ou cold wallets. **R56**: As principais características dos ativos digitais que são velocidade, descentralização e anonimato potencializam os riscos de lavagem de dinheiro e financiamento ao terrorismo, especialmente onde ainda não há regulamentação estabelecida. **R58**: Uma das estratégias dos operadores maliciosos de cripto comumente usada é a técnica de mixer, que consiste em granular uma criptomoeda em várias (por ex: 1 bitcoin após passar no processo de mixer pode transformar-se em (0,25 eth), (0,25 xrp), (0,25 btcash) e (0,25 bnb), dificultando saber a origem do recurso e aumentando o leque de pulverização do beneficiário final. Uma vez que ela não será enviada apenas de uma hash para a outra, mas de 4 hashs [*sic*] desta vez. Chats e fóruns on-line são as formas de comunicação destes usuários, pelas características intrínsecas destes meios (mensagens criptografadas e histórico facilmente manipulado).

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Quadro 22**, é possível entender que R20 relata sobre o objetivo do uso das criptomoedas na LD, por meio de serviços de mixagem de criptomoedas (*mixing cryptocurrency*), operações *peer-to-peer* (P2P) e canais de comunicação anônimos, para tentar ofuscar a origem e o caminho até a integração na economia formal das riquezas/fundos dos criminosos. Nesse sentido, R58 explica que a técnica de *mixer* consiste em granular uma criptomoeda em várias outras diferentes, dificultando o reconhecimento das partes envolvidas na transação, que geralmente utilizam como meio de comunicação, *chats* e *fóruns on-line*, com possibilidade de enviar mensagens criptografadas e manipular o histórico das mensagens.

R32 relata que não percebe a recorrência de *red flag indicators* associados ao anonimato com criptomoedas na América Latina, foco de sua companhia, no entanto, segundo relatos de seus amigos, operações com alteração de IPs, *proxies*, anonimato e criptomoedas desconhecidas, são problemas enfrentados por *exchanges* maiores e globais. Segundo R54, grande parte das *exchanges* registradas em mercados regulados contam com processos de *due diligence* de AML adequados para evitar o completo anonimato dos clientes, e que o anonimato passa a ser possível, quando as criptomoedas são enviadas para carteiras privadas. Contudo, R56 sinaliza que o anonimato, juntamente com a velocidade e descentralização, são características das criptomoedas que podem potencializar o risco de LD, em particular, nos mercados ainda não regulados. Sobre as carteiras privadas, R21 explica que a *hardware wallets*, devido a segurança, mobilidade e possibilidade de gerenciamento de dezenas/centenas de endereços de troca, está, cada vez mais, sendo utilizada para armazenamento de significativo volume de criptomoedas.

4.1.2.5 Desafio para a aplicação das medidas de *customer due diligence*

Na **Tabela 10** encontram-se os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito das atividades que apresentam um desafio para a aplicação das medidas de *customer due diligence* ao lidar com criptomoedas.

Tabela 10 – Frequência com que as atividades apresentam um desafio para a aplicação das medidas de *customer due diligence* ao lidar com criptomoedas

Assertiva	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
13.1 Compra/venda de imóvel e estabelecimento comercial/industrial.	2%	19%	29%	24%	16%	10%
13.2 Gestão de fundos, valores mobiliários e outros ativos do cliente.	2%	15%	26%	23%	29%	6%
13.3 Gestão de contas bancárias, de poupança e investimentos.	2%	13%	26%	31%	23%	6%
13.4 Organização de contribuições para a criação/operação de empresas.	0%	15%	26%	31%	18%	11%
13.5 Gestão de entidades empresariais.	0%	15%	27%	31%	15%	13%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

As atividades que apresentam um desafio para a aplicação das medidas de *customer due diligence* ao lidar com criptomoedas expostas foram consideradas com significante nível de ocorrência, onde as assertivas 13.3 “Gestão de contas bancárias, de poupança e investimentos” e 13.2 “Gestão de fundos, valores mobiliários e outros ativos do cliente” apresentam maiores ocorrências.

No **Quadro 23** estão os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com o tema classificado.

Quadro 23 – Quadro matricial da categoria dos desafios para a aplicação das medidas de CDD ao lidar com criptomoedas

Categoria: Desafios para a aplicação das medidas de CDD	
Tema	**Comentários**
Desafios	**R18**: [...] as operações citadas acima necessitam da identificação do beneficiário final, conforme previsto na legislação atual. **R20**: [...] dentre as opções ofertadas, todo o desafio está na política de know your client, que se mostra com um instrumento eficaz para identificar red flags nas operações de determinados clientes. **R21**: A reprodução de medidas de *customer due diligence* tradicionais ao ecossistema dos criptoativos deve ocorrer de forma ajustada às novas possibilidades surgidas com essa tecnologia. **R22**: As maiores dificuldades estão nas medidas que possam envolver atividades relacionadas ao sigilo bancário e fiscal, que dependem de autorização judicial, restringindo a atuação proativa. **R26**: A resposta *raramente* para todos os casos, considera o Brasil como país observado. Isso porque há regulação das atividades apresentadas, onde os mecanismos de *due diligence* podem ser aprimorados para mitigar riscos provenientes de transações com criptomoedas. **R32**: Cada companhia possui seu próprio Customer Due Diligence baseado no risco do cliente. Não chega a ser tão desafiador, porém o entendimento do uso/origem dos recursos nem sempre é claro ou simples. **R52**: Realizar a validação documental do cliente de uma Exchange que seja de fora do país, bem como fazer a conferência de bens para clientes de carteiras altas que solicitam operações atípicas. **R54**: As medidas de CDD normalmente são aplicadas no momento de abertura de conta em uma exchange e são atualizadas periodicamente. **R56**: Os novos normativos de PLD incorporaram medidas adicionais para o processo de CDD e caso haja dificuldade na obtenção das informações, isso pode ser refletido na classificação de risco do cliente e consequentemente impor controles mais rígidos de monitoramento. Adicionalmente, é possível contar com bureaus e empresas de dados que fornecem informações adicionais dos clientes, tornando mais robusto os processos de CDD e EDD. **R58**: Em um processo de due-diligence a rastreabilidade do ativo virtual sempre será questionada, pois antes de ser um ativo virtual para a compra de um determinado bem, esse ativo virtual precisa ter rastros de sua aquisição, seja por alguma operação p2p ou por meio de uma exchange/banco e etc.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Quadro 23**, entende-se que R26 considera que as atividades expostas na **Tabela 10**, raramente se apresentam como um desafio para a aplicação das medidas de *customer due diligence* (CDD) ao lidar com criptomoedas, devido ao fato dessas atividades serem reguladas, possibilitando o aprimoramento das medidas de CDD para transações envolvendo criptomoedas.

As medidas aprimoradas de CDD, conforme R56, envolvem medidas adicionais no processo de CDD, que são incorporadas por novos normativos de PLD, e a consulta de fontes de informações como *bureaus* e empresas de dados de clientes. Dessa forma, R54 relata que as *exchanges*, além de aplicarem as medidas de CDD durante a abertura de conta, atualizam periodicamente essas medidas. No entanto, R22 aponta as medidas que envolvam atividades relacionadas ao sigilo bancário e fiscal, como as que apresentam maiores dificuldades, pois dependem de autorização judicial, o que restringe uma atuação proativa.

Ainda, R20 sinaliza a aplicação do processo de *know your customer* (KYC), considerado uma ferramenta eficaz na identificação de *red flags*, como um desafio presente nas atividades observadas na **Tabela 10**. Nesse sentido, R21 relata que as medidas de CDD tradicionais, quando aplicadas ao ecossistema das criptomoedas, devem levar em consideração as possibilidades associadas à essa nova tecnologia.

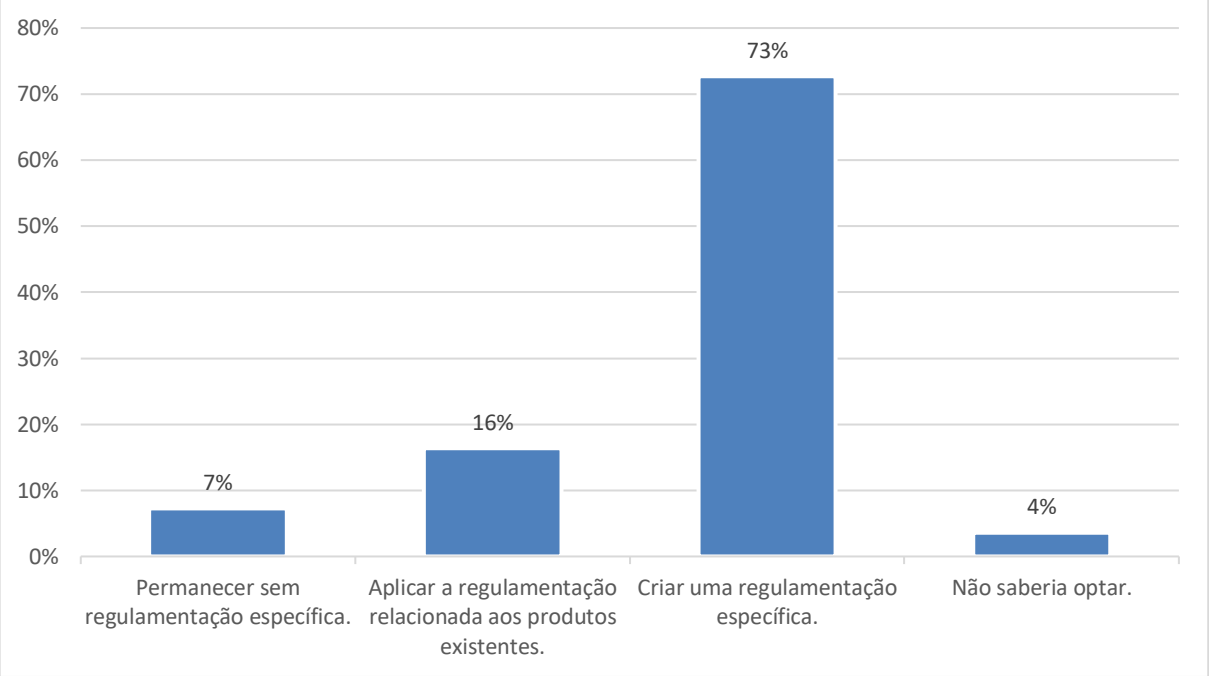
R18 explica que, em cumprimento da legislação atual, o beneficiário final envolvido em cada uma das atividades presentes na **Tabela 10** deve ser identificado. Entretanto, R52 sinaliza a realização de avaliação documental do cliente de uma *exchange* estrangeira, e a conferência de bens de clientes com carteiras altas quando solicitam operações atípicas, como desafios para a aplicação das medidas de CDD ao lidar com criptomoedas.

Segundo R32, apesar de cada companhia possuir seu próprio processo de CDD baseado no risco do cliente, o entendimento do uso/origem dos recursos poucas vezes é claro ou simples. A esse respeito, R58 explica que, no processo de CDD, a rastreabilidade das criptomoedas sempre será a etapa mais sensível, sendo preciso sempre considerar que cada transação envolvendo criptomoedas oferece uma trilha a ser examinada.

4.1.2.6 Abordagem regulatória

Acerca de se considerar a regulamentação um dos desafios ao lidar com as criptomoedas, conforme o **Gráfico 9**, a maioria dos respondentes, aproximadamente 73%, entendem que criar uma regulamentação específica para o mercado de criptomoedas seja a decisão mais apropriada.

Gráfico 9 – Abordagem regulatória mais apropriada ao lidar com as criptomoedas



Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Para 16% dos respondentes, o apropriado para o mercado seria aplicar a regulamentação relacionada aos produtos existentes, enquanto cerca de 7% dos respondentes, entendem que o mercado deve permanecer sem regulamentação específica.

No **Quadro 24** são expostos os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com os temas classificados.

Quadro 24 – Quadro matricial da categoria da abordagem regulatória mais apropriada ao lidar com as criptomoedas

Categoria: Abordagem regulatória	
Temas	**Comentários**
Regulação existente	**R34**: É essencial regulamentar o tema, face suas especificidades. Na ausência de legislação específica, então a decisão judicial deve ser pautada por analogia na legislação dos produtos existentes. **R39**: Entretanto até que a regulamentação específica não seja criada, recomendamos utilizar uma legislação relacionado com produtos existentes nesse tempo. **R48**: Não basta criar uma regulamentação específica. É necessário criar equipe que conheça e possa entender o produto e aplicá-lo conforme regulação e controles já existentes. Copiar e colar uma legislação não geraria efeito prático positivo que não uma confusão generalizada.
Regulação adaptada	**R43**: A regulamentação existente não cobre todas as particularidades do mercado, deveria ser atualizada, mas já deveria ser aplicada seguindo o modelo de autorregularão da ABcryto que vai em linha com a regulamentação do Bacen.

Regulação específica	**R4**: Exchanges formais deveriam ser ente obrigado e devem ser criados mecanismos indutivos, dissuasórios para que elas sejam usadas, já que não é compulsório. **R8**: O problema da ideia da criação de regulamentação específica é o controle/fiscalização. Como não é possível de se controlar quem detém esses ativos, torna-se difícil de fiscalizar. **R16**: Fundamenta a regulamentação específica em face das peculiaridades, assim como da atividade supervisora, na linha da Recomendação nº 15 do FATF-GAFI e dos guias sobre a matéria. **R17**: Entendo que seja adequada a criação de uma regulação específica seja o melhor caminho. Já existe iniciativa de uma autorregularão em cripto, baseada nas regras do Mercado Financeiro e Mobiliário, mas ainda são incipientes e não consideram especificidades do negócio. **R18**: Este é o maior desafio, pois por se tratar de negociações totalmente eletrônicas, com servidores e sites em diversos locais do mundo, isso pode ser um grande problema para as autoridades. **R32**: Entendo que a regulamentação se faz necessária e urgente, especialmente para que todas as companhias e exchanges estejam alinhadas no que tange PLD/FT, e que os processos sejam horizontais e semelhantes. Isso traria controle para as empresas lidarem com casos suspeitos e traria maior segurança para os órgãos reguladores na aceitação deste novo meio de transação financeira. **R35**: Uma regulação específica e principalmente sem restrições herdadas de conhecimentos não relacionados pode ser super eficiente [*sic*]. O importante é entender que a origem da lavagem de dinheiro vem de players maliciosos e entender a motivação dos players. Se as barreiras forem maiores que as notificações, temos um sistema anti-fragil [*sic*]. Porém não podemos punir a utilização de bom caráter dos criptoativos. **R37**: O mercado de criptoativos e muito dinâmico e se altera com velocidade, seja nas regras, na tecnologia e até mesmo no surgimento diário de novos ativos. Vejo que o principal desafio e conseguir abarcar num regulamento todas as nuances, flexibilidade e volatilidade do mercado. Outro desafio e o fato de que este mercado e supranacional, ou seja, não está atrelado necessariamente a nenhum sistema financeiro nacional, sendo “cross-border”. **R52**: No Brasil seria criar uma regulamentação específica e realizar a criação de tipos penais adequados e atuais para estas transações, além dos já existentes (como a de Lavagem e a Antiterror). Mas, ainda, uma dificuldade é operar com clientes que sejam de países de restrição/proibição de criptomoedas. **R56**: Deve ser elaborada uma regulamentação especifica considerando as características dos diferentes ativos digitais e o papel de cada um dos agentes que participam de todo ecossistema sejam eles emissores, prestadores de serviços ou intermediários. No entanto, é importante sempre analisar as regulamentações existentes para os “ativos tradicionais” e buscar aproveitá-las para os ativos digitais que tiverem natureza semelhante. **R57**: Tem que ter uma regulamentação específica, tomando como base algumas já existentes, por exemplo, movimentações em conta. **R58**: A lei de PLD 12.683 é bem completa e dar para ser usada como modelo de criação para a norma específica de pld para criptomoedas. Por questões intrínsecas a tecnologia (moeda descentralizada e anônima) faz se necessária a criação de regras e parâmetros específicos. Tendo como estudo de casos os corretores nacionais e internacionais. Bem como também as recomendações da GAFI e da certificação Bitlicense (NYSDFS), que servem como base para tal. No que tange a esfera pública, é necessário também ter um estudo de caso com o COAF/UIF e MP, uma vez que todos os reportes de transações ilícitas são encaminhas para estas entidades.

Arcabouço regulatório específico	**R21**: O ecossistema dos criptoativos representa desafios ao legislador uma vez que a definição de sua natureza jurídica vai depender do fim a que o ativo se e a tecnologia se propõem. Regulação para os efeitos dos contratos inteligentes no direto privado por óbvio deve ser diferente do cenário regulatório de criptoativos como meio de troca ou reserva de valor. Assim, é importante, num primeiro momento, definir a natureza jurídica daquilo que se pretende regular, para posteriormente tecer o regamento jurídico. **R27**: Acredito que, no Brasil, onde se tenta abarcar todas as possibilidades atitudinais e fenomenológicas em uma regulamentação, o maior desafio seja lidar com a dinamicidade das criptomoedas em um instrumento que tende ao engessamento (norma regulamentadora). Em minha opinião, caminhos interessantes para o solucionamento da questão são: em um primeiro momento, debates/consultas públicas com a comunidade especializada (na teoria e na prática), com autorregulações reguladas e *sandboxes*; e regulações gerais, provenientes dos órgãos reguladores, com foco em Abordagem Baseada em Risco (ABR) dos regulados.
Sem regulação específica	**R2**: A ausência de regulamentação específica faz prosperar o submundo e fortalece mercados como *darknet*. **R14**: É impossível regular a tecnologia. O caminho mais apropriado é o de mínima regulação, principalmente no sentido de identificação de VASP (Virtual Asset Service Providers) e obtenção de informações de transações. **R20**: A ausência de regulamentação é um marco na dificuldade de persecução e de punição da lavagem de ativos com criptos. Inclusive, entendo que nem seria lavagem de capitais caso as operações sejam realizadas no Brasil e com o uso de criptos pois não há regulamentação satisfatória que aponte a natureza de "moeda de troca" para os criptoativos. Entretanto, ante o acelerado crescimento da utilização de criptomoedas para operações legais, a escassa regulamentação gera prejuízos para quem as utiliza como investimento e moeda de troca, sendo a auto-regulamentação [*sic*] uma ideia bastante coerente [...]. **R28**: Parece-me que se as empresas estão tendo dificuldade em criar seus protocolos, entidades que não lidam com isso no dia a dia teriam enorme dificuldade em criar algum tipo de regulação não-nociva ao mercado. Há pontos que devem ser considerados, mas me parece que agora estamos muito longe, embora alguns elementos como SAR são cabíveis. **R54**: O mercado de criptoativos no Brasil ainda permanece completamente desregulado. A única normativa aplicável diretamente às exchanges é a IN RFB nº 1888, de 3 de maio de 2019, que institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). **R60**: Para lavagem de dinheiro não é necessário a criação de nova legislação, pois a criptomoeda é apenas um meio, não o fim.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Quadro 24**, é possível verificar que R34 e R39 defendem a utilização da legislação relacionada com produtos existentes, quando da ausência de uma regulação específica para as atividades envolvendo criptomoedas. Conforme R34, diante dessa ausência, a decisão judicial deve estar pautada, por analogia, na legislação direcionada aos produtos existentes. Para R48, é necessária a formação de um grupo de trabalho que conheça e possa entender o produto e aplicá-lo de acordo com a regulação e controles já existentes.

Contudo, R20 e R43 entende que a regulação existente não abrange todas as particularidades do mercado de criptomoedas, gerando prejuízos para quem utiliza as criptomoedas como investimento ou meio de troca.

R20 menciona a autorregulação como uma ideia bastante coerente, mediante ao acelerado crescimento de operações legais envolvendo as criptomoedas. Segundo R43, mesmo diante da necessidade de uma atualização, a regulação deveria ser aplicada seguindo o modelo de autorregulação elaborado pela Associação Brasileira de Criptoeconomia (ABCripto), que está em linha com a regulamentação do Bacen. Iniciativas de autorregulação para o mercado de criptomoedas, baseadas nas regras do mercado financeiro e mobiliário, segundo R17, são incipientes e não consideram especificidades do negócio, o que torna a criação de uma regulação específica o melhor caminho.

R52, R56, R57 e R58 manifestam a necessidade de uma regulação específica, com as regulamentações existentes sendo analisadas, para servirem de modelo no que for possível. Para R52, a norma deve trazer tipos penais adequados e atuais para transações envolvendo criptomoedas, que, conforme R60, é apenas um meio e não o fim, justificando a não necessidade de uma nova legislação para LD. Uma regulação específica fundamentada em conhecimentos relacionados a matéria pode ser muito eficiente, segundo R35, que menciona a importância do entendimento de que a origem da LD está nos *players* maliciosos, e da importância do entendimento sobre a motivação desses *players*, para que não ocorra a punição da utilização com boa fé das criptomoedas. Conforme R16, R56 e R58, as características das criptomoedas, como descentralização e anonimato, e o papel de cada agente participante do ecossistema das criptomoedas, como emissores, prestadores de serviços ou intermediários, precisam ser considerados na elaboração dessa resposta regulatória. Para R16 e R58, a regulação específica deve estar alinhada com: (i) As Recomendações do GAFI, em especial a Recomendação Nº 15 – Novas tecnologias; (ii) A Certificação *BitLicense* (*New York State Department of Financial Services* – NYSDFS); (iii) Os estudos de caso com o COAF e MP; (iv) Os estudos de casos com os corretores nacionais e internacionais; e (v) Os guias e orientações sobre a matéria.

Para que sejam cumpridas, por parte das companhias e *exchanges*, as obrigações de PLD-FT, R32 entende como necessária e urgente, a regulamentação, que permitirá maior controle para as organizações administrarem a ocorrência de casos suspeitos e maior segurança para que os órgãos reguladores se posicionem de forma favorável a respeito deste novo meio de transação financeira. Da mesma forma, para R4, as *exchanges* deveriam ser entes obrigados, com mecanismos indutivos e dissuasórios para que sejam cumpridos os requisitos de PLD-FT,

já que não é compulsório. R54 explica que a única norma aplicável diretamente as *exchanges*, no Brasil, é a IN RFB nº 1.888, de 2019, que institui e disciplina a obrigatoriedade de prestação de informações relativas às operações envolvendo criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB).

Para R18, uma resposta regulatória ao mercado de criptomoedas é um desafio, pelo fato desse mercado contar com negociações totalmente eletrônicas, envolvendo servidores e *sites* distribuídos pelo mundo. Nessa direção, R8 sinaliza, como problema para uma regulação específica, o controle/fiscalização a respeito dos detentores de criptomoedas. R52 aponta a dificuldade de operar com clientes que sejam de países com restrição/proibição de criptomoedas. Devido ao dinamismo nas regras, tecnologia e surgimento de novos ativos no mercado de criptomoedas, R37 aponta, como principais desafios, a capacidade de abarcar num regulamento todas as nuances, flexibilidade e volatilidade do mercado, assim como, o fato desse mercado não estar atrelado necessariamente a nenhum sistema financeiro nacional.

R21 apresenta como desafio do ecossistema dos criptoativos ao legislador, a definição de sua natureza jurídica, que dependerá do fim a que o ativo e sua tecnologia subjacente se propõem, uma vez que, uma regulação direcionada aos efeitos dos contratos inteligentes no direito privado será diferente de uma abordagem regulatória sobre os criptoativos utilizados como meio de troca ou reserva de valor. A definição da natureza jurídica do que se pretende regular, segundo R21, deve ser o primeiro passo útil para orientar uma resposta regulatória aos criptoativos. R27 acredita que, no Brasil, o maior desafio seja lidar com a dinamicidade das criptomoedas em um instrumento que tende ao engessamento, como a norma regulamentadora. Na opinião de R27, essa questão pode ser solucionada pelos seguintes caminhos: (i) Debates/consultas públicas com a comunidade especializada, tanto na teoria como na prática; (ii) Autorregulações reguladas e *sandboxes*; e (iii) Regulações gerais, provenientes dos órgãos reguladores, com foco em abordagem baseada em risco (ABR) dos regulados.

R14 menciona a impossibilidade de se regular a tecnologia, sendo o caminho mais apropriado o da mínima regulação, em particular, para a identificação de PSAVs e prestação de informações a respeito das transações. Na percepção de R28, se as organizações envolvidas nas atividades relacionadas às criptomoedas estão enfrentando dificuldades em criar seus protocolos, dificuldades ainda maiores seriam enfrentadas por entidades que não lidam com o mercado de criptoativos, ao tentarem elaborar alguma regulação que não seja nociva ao mercado. Desta forma, R28 entende que, a momento, diante da impossibilidade de elaborar uma regulação específica, alguns elementos como *Suspicious Activity Report* (SAR), “Relatório de

Atividades Suspeitas" na tradução livre, podem ser considerados como cabíveis. Contudo, R2 e R20 encontram problemas relacionados a ausência de uma regulação específica. Para R2, essa ausência amplia mercados como *darknet*, enquanto R20 a define como um marco na dificuldade de persecução e de punição do crime de LD com criptomoedas.

4.1.3 Possíveis Abordagens que Ajudariam a Minimizar os Riscos e Desafios Enfrentados ao Lidar com Criptoativos

Nesta seção serão tratadas as possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos, apresentando as percepções obtidas dos respondentes por meio das perguntas que se seguem.

4.1.3.1 Fontes de informação sobre avaliação de risco de lavagem de dinheiro

Na **Tabela 11** constam os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito das fontes de informação sobre avaliação de risco de LD ao lidar com criptomoedas. Todas as assertivas foram consideradas com significante nível de relevância, onde as assertivas 15.3 e 15.2 apresentam maior grau de importância.

Tabela 11 – Relevância das fontes de informação sobre avaliação de risco de LD ao lidar com criptomoedas

Assertiva	Sem importância	Pouco importante	Razoavelmente importante	Importante	Muito importante	Não saberia optar
15.1 Avaliação nacional de riscos (ANR).	2%	5%	8%	29%	45%	11%
15.2 Avaliações de risco supranacionais.	2%	2%	2%	38%	48%	10%
15.3 Relatórios setoriais das autoridades competentes sobre os riscos de lavagem de dinheiro inerentes ao serviço/setor do profissional.	0%	3%	6%	32%	55%	3%
15.4 Relatórios de risco de outras jurisdições onde o profissional está localizado.	0%	3%	10%	34%	50%	3%
15.5 Informações públicas amplamente disponíveis que destaquem questões que podem ter surgido em jurisdições específicas.	0%	2%	13%	32%	47%	6%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

No **Quadro 25** são demonstrados os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com o tema classificado.

Quadro 25 – Quadro matricial da categoria das orientações sobre avaliação de risco de LD ao lidar com as criptomoedas

Categoria: Orientações	
Tema	**Comentários**
Questões referentes as fontes de informação	**R20**: Por ser um espaço ainda cinzento quanto aos riscos operacionais do uso de criptoativos em relação às práticas criminosas, é difícil mensurar as fontes de indicadores de risco. Entendo que todas são importantes, desde que analisadas dentro de um contexto e com lógica, sem termos absolutos de uma fonte em detrimento de outra. **R21**: Aqui se verifica a importância da determinação legal de autoridades responsáveis pela supervisão do mercado de criptoativos. **R22**: É preciso cuidar com as fontes de informação, garantindo a integridade e oficialidade dos dados, bem como os meios para que seja garantida a cadeia de custódia. **R27**: Também são muito importantes os conhecimentos de tipologias e tendências, para que tanto a regulação quanto os controles sejam adaptados à dinamicidade da realidade. **R52**: Listas Restritivas Globais e análise de julgamentos e processos cujo cliente possa estar envolvido (também podem ser informações públicas). **R54**: As autoridades brasileiras ainda não têm o conhecimento técnico e nem os recursos (humanos, administrativos, financeiros, etc.) para lidar corretamente com o problema da lavagem de dinheiro no Brasil, envolvendo criptoativos. Por isso, não se pode confiar em avaliações oriundas do poder público brasileiro. **R56**: As fontes citadas acima são, sem dúvida, importantes, mas outra fonte de extrema relevância que não foi citada é o compartilhamento de informações entre as jurisdições, sejam entre reguladores, organismos atuantes no tema de PLD e até mesmo entre IFs. **R58**: O crime de lavagem de dinheiro dá para ser feito de diversos modos no universo de cripto, então uma associação/órgão que forneça estas informações, estudos e cartilhas de boas práticas seria de suma importância para a sustentação e manutenção dos programas de prevenção a lavagem de dinheiro. Além de questões de obrigatoriedade de certificação específica para trabalhar na área.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Quadro 25**, é possível verificar que R20 entende que todas as fontes de indicadores de risco de LD com criptomoedas são importantes, quando analisadas dentro de um contexto e lógica, não havendo termos absolutos de uma fonte em detrimento de outra. R20 discorre sobre a dificuldade para que as fontes de indicadores de risco sejam mensuradas, devido às incertezas quanto aos riscos operacionais da utilização dos criptoativos nas práticas criminosas.

Diante das diferentes possibilidades de se efetuar o crime de LD envolvendo criptomoedas, R58 entende como de suma importância, uma associação/órgão, que: (i) Ofereça informação, estudos e material de boas práticas para a os programas de PLD, e (ii) Trate de questões envolvendo a obrigatoriedade de certificação específica para os profissionais da área.

Por consequência, R27 sinaliza a importância dos conhecimentos de tipologias e tendencias, para que à dinamicidade da realidade do ecossistema das criptomoedas seja considerada na regulação e nos controles, enquanto R21 aponta a importância de uma autoridade competente designada na supervisão desse mercado. Contudo, para R54, as autoridades brasileiras ainda necessitam de conhecimento técnico e recursos, tanto humanos quanto administrativos e financeiros para enfrentarem, de forma eficiente e eficaz, o problema de LD com criptomoedas no Brasil. R54 entende que as avaliações oriundas do poder público brasileiro não são confiáveis. Característica, que segundo R22, deve ser observada, quando alerta para a garantia da integridade e oficialidade dos dados cedidos pelas fontes de informação.

R56 entende que as fontes que estão na **Tabela 11** são importantes, assim como o compartilhamento de informações entre as jurisdições, quer entre reguladores, organismos envolvidos no tema de PLD e ainda, entre IFs.

Nesse entendimento, R52 cita, como possibilidade de serem fontes de informações públicas, as Listas Restritivas Globais e análise de julgamentos e processos, cujo potencial cliente esteja envolvido.

4.1.3.2 Fatores e medidas para gerenciar e mitigar efetivamente os riscos de lavagem de dinheiro

Na **Tabela 12** são demonstrados os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito dos fatores e medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar criptomoedas.

Os fatores e medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar com criptomoedas expostos foram considerados com significante nível de relevância, com as assertivas 16.8 “Treinamento específico para conscientização dos profissionais que fornecem atividades especificas para clientes de maior risco” e 16.9 “Revisão periódica dos serviços oferecidos e avaliação periódica da estrutura *anti-money laundering* (AML) aplicável ao profissional” apresentando maior grau de importância.

Tabela 12 – Relevância dos fatores e medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar criptomoedas

Assertiva	Sem importância	Pouco importante	Razoavelmente importante	Importante	Muito importante	Não saberia optar
16.1 Participação de instituições financeiras devidamente reguladas.	0%	6%	13%	18%	61%	2%
16.2 Localização de profissionais e clientes em países semelhantes.	3%	16%	16%	29%	29%	6%
16.3 Supervisão de um regulador.	2%	5%	6%	18%	65%	5%
16.4 Regularidade/duração do relacionamento com o cliente.	0%	3%	19%	44%	31%	3%
16.5 Envolvimento de organizações privadas, transparentes e conhecidas no domínio público.	0%	0%	11%	39%	47%	3%
16.6 Familiaridade do profissional com um país específico, incluindo conhecimento e conformidade com as leis e regulamentos locais.	0%	2%	13%	40%	39%	6%
16.7 Treinamento geral sobre métodos de lavagem de dinheiro e riscos para os profissionais.	0%	0%	5%	19%	73%	3%
16.8 Treinamento específico para conscientização dos profissionais que fornecem atividades especificas para clientes de maior risco.	0%	0%	5%	19%	73%	3%
16.9 Revisão periódica dos serviços oferecidos e avaliação periódica da estrutura *anti-money laundering* (AML) aplicável ao profissional.	0%	0%	3%	16%	76%	5%
16.10 Revisão periódica dos relacionamentos com os clientes para determinar se o risco de lavagem de dinheiro aumentou.	0%	2%	10%	19%	65%	5%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Através do **Quadro 26**, onde são expostos os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com o tema classificado, pode-se verificar que no entendimento de R43, independentemente do tipo de ativo que está sendo transacionado, o processo de *know your customer* (KYC) é um fator de extrema importância na mitigação do risco de LD. Igualmente, R56 menciona as revisões periódicas dos serviços e o processo de KYC, como importantes para que a avaliação de riscos seja ajustada.

Para R43, a regulação do mercado de criptoativos, o envolvimento de instituições privadas que auxiliem na padronização e a certificação dos profissionais de atuam nesse mercado, possibilizariam maior segurança nas operações envolvendo criptomoedas.

Por essa razão, R56 acredita que, mediante a ausência de uma resposta regulatória específica para os agentes envolvidos nas atividades de criptomoedas, a participação de IFs regulamentadas pode ser importante.

De acordo com R21, a adaptação das regras aplicadas no mercado financeiro tradicional ao mercado das criptomoedas, deve considerar as diferentes características presentes na tecnologia subjacente as criptomoedas. R58 entende que o estudo contínuo é a única forma de prevenir o crime de LD com criptomoedas, devido à tecnologia das criptomoedas possibilitarem "n" formas de transacionar e o constante aprimoramento dos usuários maliciosos.

No **Quadro 26**, R58 discorre sobre os fatores e medidas que entende como apropriados para gerenciar e mitigar efetivamente os riscos de LD ao lidar com criptomoedas.

Quadro 26 – Quadro matricial da categoria de mitigação de riscos de LD ao lidar com as criptomoedas

Categoria: Mitigação de riscos	
Tema	**Comentários**
Fatores e medidas	**R21**: [...] a adaptação de regras para o mercado financeiro ao ecossistema de criptoativos deve ocorrer de forma adaptada às diversas facetas que a tecnologia embutida permite. **R43**: KYC é um fator extremamente importante na mitigação do risco de LD independente do tipo de ativo que está transacionando. A regulação do mercado e envolvimento de instituições privadas que auxiliem na padronização, tokens etc. traz mais segurança para as transações. A certificação de profissionais também pode ser um meio de garantir a expertise de profissionais que atuam no tema, assim como criaram no ano passado o Selo de Câmbio para AML, poderia ser criado algo similar para instituições e profissionais que atuam no setor. **R56**: A participação de IFs regulamentadas talvez seja importante enquanto não houver regulamentações específicas para todos os agentes. Mas sem dúvida as revisões periódicas dos serviços e KYC são importantes para que a avaliação de riscos seja ajustada – este processo deve ser contínuo e usar ferramentas, tecnologia e dados. **R58**: As palavras chaves e processos para um bom processo de PLD são: estudo contínuo das parametrizações de regras criadas a partir do histórico de transações ilícitas, estudo de projeções de movimentações atípicas, indicadores de efetividade do programa, conscientizações em toda a estrutura organizacional, principalmente a alta liderança, compliance, onboarding operacional PLD, comercial, T.I. e estrutura de PLD como um todo. A única forma de prevenir o crime de PLD é o estudo contínuo, pois além da tecnologia das criptomoedas terem "n" formas de transacionar, o usuário malicioso está em constante aprimoramento também.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

4.1.3.3 Procedimentos de *customer due diligence*

Na **Tabela 13** estão os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito da eficácia dos procedimentos de *customer due diligence* ao lidar com criptomoedas.

Tabela 13 – Eficácia dos procedimentos de *customer due diligence* ao lidar com criptomoedas

Assertiva	Sem eficácia	Pouco eficaz	Razoavelmente eficaz	Eficaz	Muito eficaz	Não saberia optar
17.1 Identificar o cliente e verificar a identidade desse cliente usando documentos, dados e informações confiáveis.	0%	0%	18%	19%	60%	3%
17.2 Identificar o beneficiário final e tomar medidas razoáveis com base em riscos para verificar sua identidade.	0%	5%	10%	23%	60%	3%
17.3 Compreender e obter informações sobre o objetivo e a natureza pretendida do relacionamento comercial.	2%	2%	11%	39%	44%	3%
17.4 Conduzir a *due diligence* contínua sobre o relacionamento comercial.	2%	0%	8%	32%	55%	3%
17.5 Obter informações sobre a fonte de recursos/riqueza do cliente e evidenciá-las claramente através da documentação apropriada obtida.	0%	2%	8%	24%	63%	3%
17.6 Atualizar regularmente os dados de identificação do cliente e do beneficiário final.	0%	2%	11%	32%	52%	3%
17.7 Realizar pesquisas adicionais para melhor informar o perfil de risco do cliente.	0%	5%	16%	31%	45%	3%
17.8 Obter a aprovação da alta administração para iniciar/continuar o relacionamento comercial.	5%	13%	26%	32%	19%	5%
17.9 Aumento do número e tempo dos controles, com seleção de padrões de transações que precisam de exame mais aprofundado.	0%	8%	15%	39%	32%	6%
17.10 Maior conscientização sobre clientes e transações de maior risco, em todos os departamentos envolvidos no relacionamento comercial.	0%	2%	8%	29%	56%	5%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Os procedimentos de *customer due diligence* (CDD) ao lidar com criptomoedas vistos foram considerados com significante nível de eficácia, sendo as assertivas 17.4 “Conduzir a *due diligence* contínua sobre o relacionamento comercial” e 17.5 “Obter informações sobre a fonte de recursos/riqueza do cliente e evidenciá-las claramente através da documentação apropriada obtida”, consideradas as mais eficazes.

No **Quadro 27** são exibidos os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com o tema classificado.

Quadro 27 – Quadro matricial da categoria de medidas preventivas ao lidar com as criptomoedas

Categoria: Medidas preventivas	
Tema	**Comentários**
Medidas de CDD aprimoradas	**R16**: Importante a autonomia da área de pld-cft para orientar e definir o início ou continuidade do relacionamento comercial. **R20**: O problema de algumas políticas de due diligence é a invasão de privacidade que o cliente sofre, como a opção 17.5, por exemplo. **R21**: Segundo recomendações do FATF (GAFI) as exchanges (*Virtual Asset Servisse Providers*) devem manter políticas de Know Your Client e Know Your Transaction da mesma maneira (ou até mais profundamente) que as instituições financeiras, assim procedimentos *de customer due diligence* revelam-se imprescindíveis para políticas de AML/TF. **R25**: O segredo de um bom acompanhamento de AML, não se dá apenas no início do relacionamento, mas conhecendo as transações do cliente e suas movimentações diárias, que nos leva ao verdadeiro conhecimento de quem é o cliente. **R43**: A aprovação da alta administração para iniciar ou continuar um relacionamento comercial deve ser usada como alçada superior para os casos de maior risco. **R54**: Geralmente, a alta administração não tem o poder de aprovar, sozinha, o início ou a continuidade de uma relação comercial se houve qualquer problema detectado ou risco inerente apontado pela área de compliance. Essa decisão é soberana da área de compliance, que deve agir com independência e transparência. **R56**: Todos os procedimentos acima são elementos de um processo de KYC robusto e devem ser performados para todos os clientes que operam tanto com criptomoedas quanto com ativos tradicionais. O número e tempo de controles devem ser determinados de acordo com a classificação do risco dos clientes e dos produtos/serviços. **R58**: A alta administração tem um papel ímpar no processo de PLD, pois ela que juntamente com a equipe de PLD, consegue definir e parametrizar qual é o apetite de risco financeiro, operacional e regulatório que a entidade assume e aceita. Tanto para a perpetuidade do negócio, quanto para se proteger dos riscos de imagem que acaba sendo inerente ao negócio de criptomoedas.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Por meio do **Quadro 27**, é possível verificar que, ao mencionar a obrigação imposta às *exchanges*, por parte do GAFI, para manter políticas de *due diligence* de AML/CFT, que geralmente são impostas às IFs, quando não, mais aprimoradas, R21 conclui pela importância dos procedimentos de CDD para as políticas de AML/CFT ao lidar com criptomoedas.

Para R56, todos os procedimentos presentes na **Tabela 13** são elementos presentes no processo de KYC robusto, que deve ser projetado para clientes que operam tanto com criptomoedas quanto com outros ativos tradicionais, fazendo parte do controle AML/CFT, cuja natureza e extensão serão determinadas conforme a classificação dos riscos do cliente e produtos/serviços. No entanto, R20 alerta para o fato de algumas políticas de *due diligence* apresentarem problemas relacionados à invasão de privacidade do cliente, apontando ainda, como exemplo, a assertiva 17.5 na **Tabela 13**.

R25 defende que, apesar dos procedimentos de CDD aplicados no início do relacionamento comercial, a conformidade plena com os requisitos de AML/CFT será alcançada somente com a realização do monitoramento contínuo do relacionamento comercial, que permite conhecer melhor o cliente. Sobre o relacionamento comercial, R16 e R54 sinalizam como necessária, a autonomia das áreas de PLD e *compliance*, quando da aprovação de seu início ou continuidade. R54 alega que a alta administração, geralmente, não detém o direito exclusivo de decidir sobre o início ou continuidade de um relacionamento comercial onde foram detectados problemas ou apontados riscos inerentes pela área de *compliance*. Contudo, para R43, a alta administração deve ser quem aprova o início ou continuidade do relacionamento comercial, quando se tratar de casos de maior risco. Para R58, nos negócios envolvendo criptomoedas, a alta administração desempenha um papel ímpar dentro do processo de PLD, uma vez que, juntamente com a área de PLD, define e parametriza o apetite de risco financeiro, operacional e regulatório, que a organização está disposta a assumir e aceitar.

4.1.3.4 Políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de lavagem de dinheiro

Na **Tabela 14** estão os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa a respeito da eficácia das políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de LD ao lidar com criptomoedas.

As políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de LD ao lidar com criptomoedas apresentaram significante nível de eficácia, sendo as assertivas 18.8 “Maior atenção nas operações da organização que são mais vulneráveis ao abuso por lavagem de dinheiro” e 18.6 “Ter sistema de gerenciamento de risco capaz de determinar se um cliente/beneficiário final é uma pessoa exposta politicamente” consideradas as mais eficazes.

Tabela 14 – Eficácia das políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de LD ao lidar com criptomoedas

Assertiva	Sem eficácia	Pouco eficaz	Razoavelmente eficaz	Eficaz	Muito eficaz	Não saberia optar
18.1 Realizar revisão regular das políticas e procedimentos da organização para garantir sua permanente adequação ao objetivo.	0%	2%	11%	31%	52%	5%
18.2 Realizar revisão regular de conformidade a fim de verificar a implementação correta das políticas e procedimentos da organização.	0%	0%	8%	27%	60%	5%
18.3 Fornecer à alta administração relatório regular de iniciativas de conformidade e relatório de transação suspeita, arquivados.	2%	5%	21%	35%	31%	6%
18.4 Atender os requisitos de manutenção de registros/relatórios e as recomendações para conformidade de *anti-money laundering* (AML).	0%	5%	5%	18%	68%	5%
18.5 Possibilitar a identificação oportuna de transações reportáveis, com a garantia do preenchimento preciso dos relatórios necessários.	0%	3%	2%	24%	66%	5%
18.6 Ter sistema de gerenciamento de risco capaz de determinar se um cliente/beneficiário final é uma pessoa exposta politicamente.	0%	0%	6%	27%	65%	2%
18.7 Providenciar controles adequados para clientes e serviços de maior risco, conforme necessário.	0%	0%	11%	26%	61%	2%
18.8 Maior atenção nas operações da organização que são mais vulneráveis ao abuso por lavagem de dinheiro.	0%	0%	2%	29%	66%	3%
18.9 Revisão periódica dos processos de avaliação e gerenciamento de riscos, considerando o ambiente/serviço de operação da organização.	0%	3%	5%	31%	60%	2%
18.10 Prever a função de conformidade AML e programa de revisão conforme a escala da organização e a natureza da prática profissional.	0%	3%	5%	39%	45%	8%

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

A respeito das melhores práticas para prevenir os crimes de LD, por meio do **Quadro 28**, em que são divulgados os resultados obtidos a partir da associação dos comentários dos respondentes da pesquisa com o tema classificado, é possível verificar no relato de R31, a necessidade de que a cultura de PLD esteja presente em toda a cadeia de negócio da organização, para que os valores e propósitos da organização sejam observados. Para que a eficiência e eficácia do programa de PLD sejam alcançadas, R56 menciona a política como um instrumento de governança, que não deve sofrer alterações constantes, diferentemente dos

procedimentos e controles, que definidos com base no perfil da organização e no resultado da avaliação interna de risco, devem ser revisados e avaliados periodicamente. A política, para R32, é a principal base para o entendimento dos casos de PLD em cada serviço de operação da organização, que traz orientações a respeito da execução do trabalho, da frequência dos *reports* aos reguladores e dos critérios para avaliação de risco. Os controles, segundo R43, devem ser implantados pela organização proporcionalmente aos riscos do cliente e produto classificados.

A eficácia das medidas de PLD, conforme R16, está assegurada através de certa independência e autonomia em relação a alta administração, que deve reconhecer a relevância do trabalho de PLD, assim como a responsabilidade e transparência sobre suas ações. A respeito do controle das informações fornecidas pelos clientes, quando das ferramentas e treinamento, R15 sinaliza a *Sarbanes Oxley Act* (SOx), "Lei *Sarbanes-Oxley*" na tradução livre, como referência para regras de avaliação da responsabilidade da alta administração. Sobre a ética aplicada pela alta administração, R31 expõe a necessidade de uma *due diligence* interna, com o objetivo de garantir a imparcialidade e lisura das deliberações do conselho de administração a respeito da manutenção dos negócios da organização.

O conhecimento da saúde das operações efetuadas na organização, por parte da alta administração, de acordo com R25, se dará por meio da apresentação da avalição regular do cliente e de suas movimentações. Por conseguinte, R43 argumenta que o relatório fornecido à alta administração deve conter os indicadores de ocorrência de falso positivo, para que decisões e ajustes de metodologias sejam aprovados, em particular, a utilização de soluções tecnológicas para a redução de eventos de falso positivo, permitindo o aumento da assertividade no monitoramento dos riscos.

Quadro 28 – Quadro matricial da categoria de controles internos e governança ao lidar com as criptomoedas

Categoria: Controles internos e governança	
Tema	**Comentários**
Políticas, procedimentos e controles	**R15**: Similar a Lei Sarbanes-Oxley, os profissionais da alta administração deveriam ser responsabilizados em algum grau pelas informações prestadas pelos clientes, junto a treinamentos e ferramentas para controle de tais informações. **R16**: Importante sensibilizar a alta administração sempre, acerca da relevância do trabalho de pldcft, dentre outros, e da responsabilidade, na linha do famoso brocardo de que o exemplo vem de cima, e nessa perspectiva também dar transparência das ações, contudo, fundamental certa independência e autonomia dos trabalhos de prevenção e decisão em relação a alta administração para se ter maior eficácia das medidas.

	R21: As Exchanges de criptoativos precisam encontrar seu espaço na legislação nacional uma vez que não são consideradas instituições financeiras (e não o são) e tampouco constam como entidades obrigadas no artigo 9º da Lei 9613/1998. **R25**: A apresentação de uma avaliação do cliente regular (mensal) e de suas movimentações é importante para dar conhecimento a Alta Administração da saúde das operações cursadas na instituição. **R31**: A cultura de Prevenção a Lavagem de Dinheiro precisa permear toda cadeia de Negócio da Organização. Observando os valores e propósitos daquele negócio, tornando-o transparente de forma a garantir a preservação do capital investido pelos investidores. A ética aplicada pela alta administração é outro ponto a ser monitorado e observado nas decisões tomadas e registradas em atas de reuniões do conselho de administração, cabendo, sempre uma Due Diligence interna para assegurar a imparcialidade e lisura das decisões tomadas para perpetuidade dos negócios da Organização. **R32**: As políticas são as principais bases para entendermos como lidamos com casos de PLD/FT dentro de cada serviço em específico. Elas servem especialmente para guiar como o trabalho será feito, a frequência dos reports aos reguladores e os critérios de riscos mínimos para cada análise. **R43**: Importante que a instituição inclua a classificação de risco do cliente e também do produto que está operando e estes fatores se reflitam nos controles a serem implementados de acordo com o risco que a transação representa para a instituição. Quanto à comunicação de transações suspeitas deve ser feita de maneira tempestiva e o relatório para administração deve também incluir indicadores de volume de falsos positivos para que a administração também possa tomar decisões e ajustes de metodologias e ser assertivo no monitoramento dos riscos, incluindo tecnologias que auxiliem nesta efetividade. **R54**: Em geral, o procedimento de KYC já indica, no momento de abertura da conta, se um cliente é PEP. Em sendo, ele automaticamente é classificado como cliente de alto risco. **R56**: A política é o instrumento de governança que dará a diretriz e não deve ter alterações constantes, já os procedimentos e controles devem ser definidos com base no perfil da instituição e no resultado da avaliação interna de riscos, e devem ainda ser revisados e avaliados periodicamente – isso é essencial para que o programa de PLD seja realmente eficiente e eficaz. **R58**: [...] Todo o processo de PLD é massivamente desgastante, são muitas bases legais, listas restritivas, parâmetros e regras regulatórias a serem seguidas (independente se atualmente não temos uma regulamentação específica para criptomoedas), esse conjunto de normas e recomendações, são os que apelidamos de “boas práticas”, e são exatamente elas que usamos como diretrizes dos processos de PLD. Para que o processo de PLD seja efetivo, é necessário ganhar velocidade e alta escalabilidade de processamento de dados, uma vez que uma transação de btc em uma corretora pode percorrer em apenas 5 minutos (ou menos dependendo da agilidade e complexidade da operação). Para que isso seja possível, é necessária a ponte entre o departamento responsável de PLD e B.I. Para que os processos sejam cada vez mais rápidos e efetivos, com parametrizações de alertas, tempo de resposta hábil e processo e controle que cobre possíveis riscos e/ou falhas operacionais. Protegendo assim a empresa e o ecossistema cripto dos usuários maliciosos.

Fonte: Elaborado pelo autor com base nos dados da pesquisa.

Através do **Quadro 28**, é possível compreender que, para que a regulação aplicável seja cumprida pela organização, os procedimentos para comunicação de transações suspeitas às autoridades competentes, de acordo com R43, devem ser tempestivos, assim como a adoção de procedimentos de KYC, que segundo R54, geralmente identifica, já na realização de abertura de conta, um cliente como PEP, classificando-o, automaticamente, como cliente de alto risco. No entanto, para as *exchanges* possam administrar efetivamente sua exposição ao risco regulatório associado ao crime de LD, segundo R21, elas devem ser alcançadas pela legislação nacional, já que não se enquadram como IFs e não constam como entidades obrigadas no artigo 9º da Lei nº 9.613 de 1998, conhecida como "Lei de Lavagem de Dinheiro".

R58 explica que, independentemente da ausência de uma regulação específica para as criptomoedas, o processo de PLD é massivamente desgastante para a organização, devido muitas bases legais, listas restritivas, parâmetros e regras regulatórias que devem ser seguidos. Conforme R58, esse conjunto de normas e recomendações, reconhecido como "boas práticas", é utilizado como diretrizes dos processos de PLD. Entretanto, para que o processo de PLD seja efetivo, R58 aponta a necessidade de velocidade e escalabilidade de processamento de dados, devido a velocidade com que uma transação envolvendo BTC em uma *exchange* pode alcançar. Logo, R58 argumenta que a cooperação entre as áreas de PLD e *Business Intelligence* (BI) pode tornar os processos mais tempestivos e efetivos.

4.2 ANÁLISE DO TRATAMENTO CONTÁBIL APLICADO AOS CRIPTOATIVOS

Em junho de 2019, o IFRIC publicou sua decisão de agenda sobre como os Padrões IFRS se aplicam às *holdings* de criptomoedas, evidenciando a existência de uma gama de criptoativos, considerando, para a discussão, um subconjunto de criptoativos que a decisão se refere como uma "criptomoeda", devido a presença de todas as características apresentadas a seguir:

i) uma moeda digital ou virtual registrada em um livro-razão distribuído que usa criptografia para segurança;

ii) não emitido por uma autoridade jurisdicional ou outra parte; e

iii) não dá origem a um contrato entre o titular e outra parte.

Somete os criptoativos que guardam essas características foram objeto da discussão a respeito dos possíveis tratamentos contábeis nas negociações realizadas nesse mercado.

Na discussão sobre a natureza de uma criptomoeda, o IFRIC observou que seu *holding* atende à definição de um ativo intangível segundo a *International Accounting Standards* (IAS)

38 – *Intangible Assets*, que, no Brasil, mantém correlação com o Pronunciamento Técnico CPC 04 (R1) – Ativo Intangível.

Assim, uma criptomoeda pode ser separada do detentor e vendida ou transferida individualmente, não dando ao titular o direito de receber um número fixo ou determinável de unidades monetárias.

A respeito de qual Padrão IFRS se aplica a contabilização das *holdings* de criptomoedas, o IFRIC concluiu que a IAS 2 – *Inventories*, que mantém correlação com o CPC 16 (R1) – Estoques, se aplica as criptomoedas quando são mantidas para venda no curso normal dos negócios. Se a IAS 2 / CPC 16 (R1) não for aplicável, a entidade deve aplicar a IAS 38 / CPC 04 (R1) às *holdings* de criptomoedas.

Por conseguinte, ao considerar a definição de um ativo financeiro de acordo com a IAS 32 / CPC 39, o IFRIC concluiu que uma *holding* de criptomoeda não é um ativo financeiro, pelo fato de uma criptomoeda não ter, atualmente, as características de caixa. Não sendo, também, um instrumento patrimonial de outra entidade. Concluindo, ainda, que uma *holding* de criptomoeda não dá origem a um direito contratual para o titular e não é um contrato que será ou poderá ser liquidado com os próprios instrumentos de patrimônio do titular.

Examinando a definição de moeda (caixa) no item AG3 da IAS 32 / CPC 39, o IFRIC entende que, apesar de algumas criptomoedas poderem ser usadas na troca de bens ou serviços específicos, não há conhecimento de qualquer criptomoeda que seja usada como meio de troca e como unidade monetária na precificação de bens ou serviços a tal ponto que seria a base sobre a qual todas as transações são mensuradas e reconhecidas nas demonstrações financeiras. Assim, o IFRIC conclui que a posse de criptomoeda não é caixa, devido à ausência das características inerentes à moeda (caixa).

Nesse contexto, o IFRIC observou que numa situação em que uma entidade mantém criptomoedas para venda no curso normal dos negócios, a *holding* de criptomoeda é um estoque da entidade, que será contabilizada conforme a IAS 2 / CPC 16 (R1). Mas, em uma situação em que uma entidade atue como corretora de criptomoedas, deve ser considera os requisitos do item 3 (b) da IAS 2 / CPC 16 (R1), para corretores-negociantes de *commodities* que mensuram seus estoques pelo valor justo menos os custos de venda.

No **Quadro 29** estão as definições consideradas pelo IFRIC para chegar a sua conclusão:

Quadro 29 – IAS's consideradas pelo IFRIC na decisão

IAS 2 / CPC 16 (R1) – Estoques
Item 3: Esta Norma não se aplica também à mensuração dos estoques mantidos por: [...] (b) comerciantes de *commodities* que mensurem seus estoques pelo valor justo deduzido dos custos de venda. Nesse caso, as alterações desse valor devem ser reconhecidas no resultado do período em que tenha sido verificada a alteração.
Item 5: Os operadores (*broker-traders*) de *commodities* são que aqueles que compram ou vendem *commodities* para outros ou por sua própria conta. Os estoques referidos no item 3 (b) são essencialmente adquiridos com a finalidade de venda no futuro próximo e de gerar lucro com base nas variações dos preços ou na margem dos operadores. Quando esses estoques são mensurados pelo valor justo menos os custos de venda, eles são excluídos apenas dos requisitos de mensuração desta Norma.
Item 6: Estoques são ativos: (a) mantidos para venda no curso normal dos negócios; (b) em processo de produção para venda; ou; (c) na forma de materiais ou suprimentos a serem consumidos ou transformados no processo de produção ou na prestação de serviços.
IAS 21 / CPC 02 (R2) – Efeitos das Mudanças nas Taxas de Câmbio e Conversão de Demonstrações Contábeis
Item 16: [...] a característica essencial de item não monetário é a ausência do direito a receber (ou da obrigação de entregar) um número fixo ou determinado de unidade de moeda. [...].
IAS 32 / CPC 39 – Instrumentos Financeiros: Apresentação
Item 11: [...] *Ativo financeiro* é qualquer ativo que seja: (a) caixa; (b) instrumento patrimonial de outra entidade; (c) direito contratual: (i) de receber caixa ou outro ativo financeiro de outra entidade; ou (ii) de troca de ativos financeiros ou passivos financeiros com outra entidade sob condições potencialmente favorável a entidade; (d) um contrato que seja ou possa vir a ser liquidado por instrumentos patrimoniais da própria entidade [...].
Item AG3: Moeda (caixa) é um ativo financeiro porque representa um meio de troca e, portanto, constitui a base sobre a qual todas as transações são mensuradas e reconhecidas nas demonstrações contábeis. Um depósito de caixa em banco ou instituição financeira similar é um ativo financeiro porque representa o direito contratual do depositante de obter caixa da instituição ou de descontar cheque, ou instrumento similar, reduzindo o saldo em favor de credor, em pagamento de passivo financeiro.
IAS 38 / CPC 04 (R1) – Ativo Intangível
Item 2: A presente Norma aplica-se à contabilização de ativos intangíveis, exceto: (a) ativos intangíveis dentro do alcance de outro Pronunciamento Técnico; (b) ativos financeiros, conforme definidos na IAS 32 / CPC 39 – Instrumentos Financeiros: Apresentação; [...].
Item 8: *Ativo intangível* é um ativo não monetário identificável sem substância física.
Item 12: Um ativo satisfaz o critério de identificação, em termos de definição de um ativo intangível quando: (a) for separável, ou seja, puder ser separado da entidade e vendido, transferido, licenciado, alugado ou trocado, individualmente ou junto com um contrato, ativo ou passivo relacionado, independente da intenção de uso pela entidade; ou; (b) resultar de direitos contratuais ou outros direitos legais, independentemente de tais direitos serem transferíveis ou separáveis da entidade ou de outros direitos e obrigações.

Fonte: Elaborado pelo autor.

Sobre a divulgação no contexto das *holdings* de criptomoedas, o IFRIC considerou os seguintes requisitos de divulgação dentro dos Padrões IFRS atuais:

- Uma entidade deve fornecer as divulgações exigidas pelos itens 36-39 da IAS 2 / CPC 16 (R1) para criptomoedas mantidas para venda no curso normal dos negócios; e pelos itens 118-128 da IAS 38 / CPC 04 (R1) para *holdings* de criptomoedas dentro do seu alcance;
- Se uma entidade mensura a posse de criptomoedas pelo valor justo, os itens 91-99 da IFRS 13 – *Fair Value Measurement*, que mantém correlação com o CPC 46 – Mensuração do Valor Justo, especificam os requisitos de divulgação aplicáveis;
- Aplicando o item 122 da IAS 1 – *Presentation of Financial Statements*, que mantém correlação com o CPC 26 (R1) – Apresentação das Demonstrações Contábeis, uma entidade deve divulgar, juntamente com suas políticas contábeis significativas ou em outras notas explicativas, os julgamentos que sua administração fez em relação à contabilização de *holdings* de criptomoedas, se eles fizerem parte dos julgamentos que tiveram o efeito mais significativo sobre os montantes reconhecidos nas demonstrações financeiras; e
- O item 21 da IAS 10 – *Events after the Reporting Period*, que mantém correlação com o CPC 24 – Evento Subsequente, exige que uma entidade divulgue detalhes de quaisquer eventos relevantes subsequentes ao período contábil a que se referem as demonstrações contábeis, mas que não originam ajustes, incluindo informações sobre a natureza do evento e uma estimativa de seu efeito financeiro ou uma declaração de que tal estimativa não pode ser feita. Por exemplo, uma entidade detentora de criptomoedas consideraria se as mudanças no valor justo dessas participações após o período de relato são de tal importância que a não divulgação poderia influenciar as decisões econômicas que os usuários das demonstrações financeiras tomam com base nas demonstrações financeiras.

4.3 DISCUSSÃO DOS RESULTADOS

Os profissionais da contabilidade e organizações contábeis, como APNFDs, devem seguir uma ABR para mitigar os riscos de LD, ou seja, devem adotar medidas apropriadas para identificar e avaliar seus riscos de LD e implementar políticas, controles e procedimentos que lhes possibilitem gerenciar e mitigar efetivamente os riscos que foram identificados. Assim sendo, os resultados deste estudo permitem concluir que os riscos e desafios de crime de LD enfrentados ao lidar com criptoativos e as possíveis abordagens que ajudariam a minimizar esses riscos e desafios trazem as seguintes questões que precisam ser observadas:

Questões relacionadas às vulnerabilidades associadas às práticas e serviços oferecidos ao lidar com criptomoedas.

Os profissionais da contabilidade devem identificar os seguintes riscos que lhes são apresentados pela LD: (i) risco de ser usado para LD; (ii) risco de ser usado para facilitar a LD por outra pessoa; e (iii) risco de sofrer danos legais, regulatórios ou de reputação por não ter identificado os sinais de alerta de LD e relatado.

Por conseguinte, questões envolvendo a assertiva 9.3 "Compra/venda de imóveis e estabelecimentos comerciais/industriais" da **Tabela 6** podem estar associadas ao risco de o profissional da contabilidade ser usado para LD com criptomoedas. No entanto, esse achado diverge parcialmente dos resultados do estudo realizado por Zavoli (2020). Conforme o estudo, devido à baixa adesão do mercado imobiliário do Reino Unido no uso de criptomoedas, pode-se considerar um possível desinteresse dos criminosos nesse mercado para LD com criptomoedas. Nessa direção, ainda que a assertiva 9.3, assim como as demais assertivas, guarde significante nível de ocorrência, os respondentes da presente pesquisa entendem a ocorrência da assertiva 9.3 como rara, devido a necessidade de uma rede criminosa complexa, falha de controles das IFs envolvidas e a cumplicidade dos cartórios e corretores de imóveis.

No tocante às questões sobre o profissional da contabilidade ser usado para facilitar a LD por outra pessoa, têm-se os comentários a respeito da criação de empresas de fachada com negociações forjadas para fluxo de recursos ilícitos com criptomoedas.

Tal associação pode ser constatada nos resultados da "Operação Colossus", deflagrada em setembro de 2022 pela Polícia Federal (PF) com o apoio da Receita Federal do Brasil (RFB). Nessa operação foi comprovada a participação de um profissional da contabilidade como responsável por 1.300 empresas em São Paulo, sendo a maioria empresas de fachada, que movimentaram aproximadamente R$ 1 bilhão em criptomoedas no período de 2017 a 2021 (MJSP, 2023).

O comentário dos respondentes de que o controle da chave privada, no ecossistema das criptomoedas, possibilita ao usuário o controle total dos ativos, traz à baila um importante tema de discursão sobre as vulnerabilidades associadas às práticas e serviços oferecidos pelos profissionais da contabilidade. Questões envolvendo a posse da chave privada, ou seja, a possibilidade de controle de uma criptomoeda, estão na sua geração, uso, autorização, armazenamento, identificação do verdadeiro proprietário, entre outras questões. Essas questões foram consideradas pelos definidores de padrão de auditoria e organizações profissionais *Chartered Professional Accountants of Canada* (CPAC), *Public Company Accounting*

Oversight Board (PCAOB), e *American Institute of Certified Public Accounting* (AICPA), quando da identificação e avaliação de riscos de distorção relevante em transações com criptomoedas (CPAC, 2018, 2020; PCAOB, 2020; AICPA, 2022). Na pesquisa de Harrast, McGilsky e Sun (2022), conforme avaliação dos participantes sobre a probabilidade e o impacto dos riscos de criptomoeda, essas questões foram classificadas em ordem de risco inerente (soma de probabilidade e impacto). Nos estudos de Vincent e Wilkins (2020) e Hsieh e Brennan (2022), elas foram tratadas quando da elaboração, respectivamente, dos "*Cryptocurrency Risk Framework*" e "*Framework for auditing crypto asset transactions*". Tais questões, quando observadas pelos profissionais da contabilidade, pode evitar que eles sofram danos legais, regulatórios ou de reputação por não ter identificado os sinais de alerta de LD e relatado.

Questões relacionadas aos fatores de riscos de LD ao lidar com criptomoedas.

A avaliação de risco de LD, como ponto de partida para aplicação da ABR, deve ser realizada pelo profissional da contabilidade proporcionalmente ao seu modelo de negócio, examinando os fatores de risco de LD, que podem ser organizados nas categorias de risco país/geográfico, risco de cliente e risco de transação/serviços e canal de entrega associado.

Como tal, é possível afirmar que os comentários sobre a regulamentação ou supervisão inadequadas das atividades e provedores financeiros de criptomoedas em diferentes jurisdições levantam questões relativas aos riscos país/geográfico.

Esse achado pode confirmar os resultados da pesquisa de Teichmann (2021), onde, cerca de 84% dos participantes afirmaram que setores ou jurisdições com pouca ou nenhuma regulamentação correm maior risco de LD com criptomoedas. Igualmente, o entendimento dos respondentes do presente estudo, de que a natureza transfronteiriça das criptomoedas apresenta um risco adicional de LD, pode respaldar os 37% dos participantes do estudo de Teichmann (2021), que entendem que os setores que envolvem transferências internacionais correm risco de LD, assim como, os relatos dos participantes do estudo de Limba, Stankevičius e Andrulevičius (2019).

Em relação às questões pertinentes ao risco de cliente, tem-se a assertiva 10.8 "Clientes com negócios intensivos em dinheiro/equivalente, como corretores e outros prestadores de serviços em ativos virtuais" da **Tabela 7**. Esse achado, também pode atestar o estudo de Teichmann (2021), uma vez que aproximadamente 86% dos entrevistados entendem que os setores de uso intensivo de dinheiro correm risco de LD.

Os comentários acerca da identificação do cliente/beneficiário, entendimento da fonte de fundos/riquezas do cliente e objetivo da transação, igualmente enfatizam questões pertinentes ao risco de cliente. Esse risco deve ser observado por organizações contábeis que desejam aceitar clientes que negociam com criptomoedas ou clientes cripto-nativos, ou seja, empresas cripto-nativas, que são companhias criadas e que operam no ecossistema das criptomoedas e da tecnologia *blockchain*. Deste modo, os participantes do estudo de Dyball e Seethamraju (2022), com foco no cliente, apontaram considerações acerca dos sistemas de controles internos, protocolos de gerenciamento de riscos, dentre outras preocupações. Jones, Jeffery e Fields (2020), sinalizam, dentre outras questões, a necessidade de saber do cliente, como ele garante a conformidade com as leis e regulamentos relevantes. A pesquisa de Pimentel *et al*. (2021) revelou que muitos clientes-cripto são rejeitados pelos profissionais da contabilidade, por não implementarem sistemas com um ambiente de controle interno adequado para uma possível auditoria. Conforme o estudo, esses clientes são geradores de ideias tecnológicas disruptivas, mas não têm conhecimento dos controles internos necessários para se protegerem de atividades fraudulentas.

Ainda, os comentários no tocante aos produtos ou serviços envolvendo criptomoedas que, ao facilitarem transações com pseudônimo ou com anonimato, podem dificultar a capacidade de rastrear os fundos associados e identificar as contrapartes da transação, apontam questões pertinentes ao risco de transação/serviços e canal de entrega associado. Serviços referentes às ofertas iniciais de moedas (*Initial Coin Offering* – ICO) podem gerar implicações para os profissionais da contabilidade, devido a possibilidade de participação de partes antiética no projeto. Essas questões foram tratadas nos estudos de Smith (2018) e Boulianne e Fortin (2020), ao elaborarem, respectivamente, um guia para os profissionais da contabilidade que buscam evitar fraudes ou atividades antiéticas relacionadas com criptomoedas e um "*Framework of risks and benefits for unregulated and regulated ICOs*". Essas questões também foram consideradas pelos participantes do estudo de Angeline *et al*. (2021), assim como, o reconhecimento sobre a importância da regulamentação AML/CFT ao lidar com criptomoedas.

A prestação de serviços virtuais, como a gestão de carteiras de criptomoedas, com transações e investimentos envolvendo criptomoedas, e a capacidade de movimentar valores virtualmente na ausência de contato direto e pessoal com provedor de serviços profissionais ou IFs, provavelmente acarretará numa dificuldade de identificar a fonte e o destino dos valores sob a gestão das organizações contábeis, podendo aumentar o risco dessas organizações facilitarem atividades ilícitas.

Questões relacionadas aos red flag indicators sobre LD ao lidar com criptomoedas.

O estado de atenção acerca dos *red flag indicators* sobre LD, por parte dos profissionais da contabilidade, é fundamental para o cumprimento de parte de suas obrigações regulatórias gerais. A identificação dos *red flag indicators* associados as etapas de LD com criptomoedas, em muitos casos pode exigir o conhecimento das estratégias de anonimato ao lidar com criptomoedas.

Vários respondentes entendem que as características inerentes as criptomoedas, como possibilidade de anonimato, negociações além-fronteiras e velocidade, facilitam seu uso nos crimes de LD. Diferentes métodos concretos que os usuários ilegais utilizam na LD com criptomoedas foram expostos pelos respondentes. As percepções dos respondentes em relação aos *red flag indicators* ao lidar com criptomoedas precisam ser consideradas pelos profissionais da contabilidade, pois a falta do conhecimento a respeito pode ter influenciado nos achados de Salawu e Moloi (2018), que apontam para uma descrença, por parte dos profissionais da contabilidade nigerianos, a respeito de possível anonimato nas transações envolvendo criptomoedas. Essa possibilidade de anonimato foi considerada pela CPAC quando exemplificou questões a serem consideradas na identificação e avaliação de riscos de distorção relevante em transações com criptomoedas (CPAC, 2018). A questão "A entidade celebra e registra uma transação de criptomoeda com uma parte relacionada que não pode ser identificada devido ao anonimato das partes nas transações de blockchain", exemplificada pela CPAC, foi considerada no estudo de Vincent e Wilkins (2020), Harrast, McGilsky e Sun (2022) e Hsieh e Brennan (2022).

Os comentários dos respondentes sobre os *red flag indicators,* fizeram emergir questões relacionadas ao uso de serviço de anonimização ou serviço de mixagem de criptomoedas (*mixing cryptocurrency*) e o acesso a *sites* de jogos *online,* durante o processo de LD. Tais questões encontram-se de acordo com os achados de Fanusie e Robinson (2018). Os autores identificaram os serviços de mixagem de criptomoedas e jogos de azar *online*, dentre os demais serviços, como os que receberam, no período de 2013 a 2016, os maiores volumes de *bitcoins* de atividades ilícitas. De acordo com o relatório emitido pela Chainalysis, de todo o volume enviado para os serviços de mixagem de criptomoedas em 2022, aproximadamente 24% eram de endereços ilícitos, e os totais enviados em 2021, cerca de 10% eram de endereços ilícitos, apontando um significante aumento do provável uso desse serviço no crime de LD com criptomoedas (GRAUER *et al*., 2023).

Quanto ao acesso a *sites* de jogos de azar *online* com protocolos ineficientes de KYC, o estudo de Andrade *et al*. (2023), que analisaram 40 operadoras de jogos de azar *online* baseados em criptomoedas, frequentemente acessados no Reino Unido, constatou que menos da metade das operadoras analisadas possuía licença válida (47,5%) e nenhuma das operadoras com página de depósito disponível exigia verificação de identidade antes de habilitar os depósitos. Haq *et al*. (2022), sinalizam sobre a não concordância com as classificações que Bangladesh recebeu por seu nível de conformidade com as Recomendações do GAFI sobre APNFDs e Novas Tecnologias, devido as descobertas de uma série de incidentes recentes relacionados a cassinos e criptomoedas. Conforme os autores, apesar dos cassinos serem proibidos e o banco central de Bangladesh ter emitido um aviso de advertência sobre transações com criptomoedas, vários cassinos foram descobertos ao mesmo tempo que a polícia reprimiu e fez várias prisões relacionadas a transações ilegais envolvendo criptomoedas em Bangladesh. Tal questão precisa ser observada no Brasil, onde os cassinos físicos são proibidos, mas apostas *online* são permitidas ao mesmo tempo em que várias operações policiais resultaram em prisões devido ao uso de criptomoedas no crime de LD.

A conscientização e educação, por parte dos profissionais da contabilidade, acerca da identificação dos *red flag indicators* associados as etapas de LD e das estratégias de anonimato ao lidar com criptomoedas, pode aumentar o estado de atenção acerca dos *red flag indicators* para AML/CFT quando do envolvimento com criptomoedas.

Questões relacionadas às fontes de informação sobre avaliação de risco de LD ao lidar com criptomoedas.

Tendo como pré-requisito para aplicar uma ABR eficaz, durante o processo de avaliação de risco, o profissional da contabilidade necessita ter acesso às informações precisas, oportunas e objetivas sobre os riscos de LD/FT com criptomoedas. Nesse contexto, questões relacionadas às fontes de informação sobre avaliação de risco de LD ao lidar com criptomoedas, devem ser acompanhadas pelas autoridades competentes designadas, entidades autorreguladoras (EARs) ou outras fontes confiáveis.

Os respondentes, de forma geral, consideraram com significante nível de relevância todas assertivas relacionadas as fontes de informação, sendo que a assertiva 15.1 “Avaliação nacional de riscos” da **Tabela 11** apresentou menor grau de importância. Esse menor grau de importância da assertiva 15.1 deve estar relacionado ao fato de sua primeira edição ocorrer em 2021.

Na 1ª Avaliação Nacional de Riscos de LD/FTP (ANR) do Brasil, os "contadores", ou seja, o profissional da contabilidade e as organizações contábeis, como segmento dos setores obrigados, foram classificados com vulnerabilidade ponderada "média" e os PSAVs com vulnerabilidade ponderada "alta" (COAF, 2021b, p.64). Devido ao alcance global, liquidez, capacidade de permitir transações ponto a ponto, potencial de maior anonimato e ofuscação de fluxos de transações de AVs e desafios associados à realização de identificação e verificação eficazes do cliente, os AVs e PSAVs, em geral, podem ser considerados como de alto risco de LD/TF, podendo exigir a aplicação de medidas de CDD aprimoradas.

Nesse sentido, torna-se imperativa uma abordagem mais abrangente, considerando que o profissional da contabilidade e as organizações contábeis, quando se envolverem em atividades ou operações financeiras com criptomoedas ou PSAVs, devem ser classificados com vulnerabilidade ponderada "alta".

Diante das considerações dos respondentes de que as autoridades brasileiras ainda necessitam de conhecimento técnico e recursos, tanto humanos quanto administrativos e financeiros para enfrentarem, de forma eficiente e eficaz, o problema de LD com criptomoedas no Brasil, pode-se afirmar que tais considerações apoiam os resultados do estudo de Coelho, Fishman e Ocampo (2021), que observaram como a supervisão dos PSAVs com suas obrigações AML/CFT está em seu estágio inicial na maioria das jurisdições. Os autores sinalizam que as ações de fiscalização são elementos fundamentais de dissuasão e educação. Tais observações, também foram colocadas pelos respondentes da presente pesquisa, quando apontam a importância de uma associação/órgão, que ofereça informação, estudos e material de boas práticas para os programas de PLD.

Também emergiram resultados que confirmam os achados de Kethineni e Cao (2019), Coelho, Fishman e Ocampo (2021), Ilbiz e Kaunert (2022) e Trozze *et al.* (2022), sobre a importância de cooperação e a coordenação em nível nacional e internacional, apontando para a concordância entre a necessidade de uma melhor colaboração entre o setor privado, das agências da lei e as UIFs, uma vez que nenhum desses setores, isoladamente, podem resolver as questões relacionadas ao amadurecimento dos mercados de criptomoedas e sua aplicação nos crimes de LD/FT. Os relatos dos respondentes da atual pesquisa expõem a relevância do compartilhamento de informações entre as jurisdições, quer entre reguladores, organismos envolvidos no tema de PLD e ainda, entre IFs, assim como a relevância das Listas Restritivas Globais e análise de julgamentos e processos, cujo potencial cliente esteja envolvido nesses crimes.

As questões expostas trazem para discussão a importância de um estudo a respeito de um modelo de plataforma para uma solução em uma parceria público-privada eficiente no contexto da LD com criptomoedas, onde atores públicos e privados poderão compartilhar de forma ideal recursos, como conhecimento sobre o tema e a oferta de uma oportunidade de *networking*, principalmente para os profissionais da contabilidade e as organizações contábeis.

Questões relacionadas às medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar com criptomoedas.

Após a identificação e avaliação dos riscos de LD, a organização contábil deve aplicar as medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar com criptomoedas.

Implicações para as organizações contábeis com presença internacional podem surgir devido à arbitragem regulatória, consequência das diferentes abordagens regulatórias das jurisdições, cujo objetivo está em preencher lacunas em suas estruturas regulatórias e de supervisão e combater os riscos de LD com criptomoedas. Talvez, por esse motivo, os respondentes consideraram as assertivas 16.2 "Localização de profissionais e clientes em países semelhantes" e 16.6 "Familiaridade do profissional com um país específico, incluindo conhecimento e conformidade com as leis e regulamentos locais" da **Tabela 12**, assim como as demais assertivas, com significante nível de relevância.

As percepções dos respondentes sobre a necessidade de treinamento e estudo contínuo, para conscientização, conhecimento e compreensão do mercado de criptomoedas junto as partes interessadas, corroboram para as recomendações da *European Union Agency for Law Enforcement Cooperation* (EUROPOL). A EUROPOL sinaliza que as entidades com obrigações AML/CFT – no caso da presente pesquisa trata-se dos profissionais da contabilidade e organizações contábeis, na condição de APNFDs – devem considerar a introdução de treinamento em criptomoedas para funcionários relevantes, considerando sua posição na linha de frente da detecção e denúncia de transações suspeitas (EUROPOL, 2022). A lacuna de conhecimento sobre o mercado foi comprovada em 52% dos profissionais da contabilidade participantes no estudo de Minhat *et al*. (2022), de modo que, mais da metade dos mesmos participantes, não tinham certeza sobre a relevância da chave privada, cujas implicações foram anteriormente expostas na presente discussão. Segundo Johari *et al*. (2020), o treinamento contínuo a respeito dos requisitos mais recentes, regras e regulamentos que regem as transações com criptomoedas permitirá a aplicação de medidas de *customer due diligence* (CDD) aprimoradas a fim de proteger a organização de ser explorada por criminosos sofisticados.

Tais achados são suportados pelos comentários da presente pesquisa acerca a aplicação de medidas CDD aprimoradas nas políticas de AML/CFT ao lidar com criptoativos, mediante a necessidade de aplicação dos processos de KYC e *Know Your Transaction* (KYT) da mesma maneira (ou até mais profundamente) que as IFs. Esses comentários, também seguem em concordância com a análise de Wronka (2022), que entende como possível a aplicação do processo KYT para o monitoramento e identificação de transações envolvendo criptomoedas. A necessidade de aplicação de medidas CDD aprimoradas está nos relatos dos participantes da pesquisa de Chou, Agrawal e Birt (2022), que enfatizaram sobre a necessidade de tais medidas relacionadas ao risco de LD, assim como risco de armazenamento de criptomoeda, serem incluídas nas demonstrações financeiras. Conforme os relatos dos participantes do estudo de Pimentel *et al*. (2021), muitos clientes cripto-nativos têm sofrido resistência em serem auditados, devido à ausência de conhecimento necessário, por parte dos profissionais da contabilidade, para lidarem efetivamente com os riscos pertinentes a esses clientes.

O treinamento e estudo contínuo, devem permitir que os profissionais da contabilidade formulem sólidos julgamentos sobre a qualidade das avaliações dos riscos associados às atividades envolvendo criptomoedas e ao fornecimento de produtos ou serviços por PSAVs, que podem ser potencialmente mais elevados, e que os profissionais da contabilidade sejam capazes de considerar a adequação e proporcionalidade dos controles de AML/CFT. Essas implicações se revelam uma oportunidade para os órgãos profissionais e universidades ajudarem a preencher essa lacuna.

Questões relacionadas às políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de LD ao lidar com criptomoedas.

As organizações contábeis devem criar uma cultura de conformidade em AML/CFT, assegurando que seus funcionários cumpram as políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de LD/FT. Quando as organizações contábeis atuarem como PSAVs, ou se envolverem com AVs e PSAVs, terão o desafio de atender as exigências de CDD, monitoramento de transações, relatórios e manutenção de registros com o objetivo de responder as demandas de um mercado que está amadurecendo e cada vez mais difícil de se ignorar.

Conforme entendimento dos respondentes, os serviços oferecidos para o sistema financeiro encontrarão correspondência no mercado das criptomoedas, permitindo a criação de diferentes serviços não existente no cenário das práticas de AML tradicionais. Esse

entendimento pode ser encontrado no estudo de Poskriakov, Chiriaeva e Cavin (2019), quando os autores sinalizam que as criptomoedas podem facilitar a LD através de mecanismos básicos usados com moedas fiduciárias. Os autores explicam que na etapa de integração no processo de LD, a aquisição de bens e serviços, com pares criptomoeda/criptomoeda ou criptomoeda/moeda fiduciária, é facilitada pelo aumento de bens e serviços cujo pagamento em criptomoedas é aceito, bem como a participação de atores institucionais, trazendo maior liquidez ao mercado. Leuprecht, Jenkins e Hamilton (2023), ao analisarem como as criptomoedas são alavancadas para fins ilícitos em todo o sistema financeiro global, concluíram que o uso ilícito de criptomoedas é predominante nas etapas de colocação e ocultação no processo de LD e que as criptomoedas são usadas com mais frequência em conjunto com outras moedas fiduciárias.

Os respondentes da atual pesquisa, também observaram que qualquer negócio pode ser objeto de LD com criptomoedas, na mesma medida que negócios lícitos, mudando somente a origem desse recurso, que sendo ilícito denota LD. A esse respeito, a EUROPOL (2022) expõe que os profissionais no crime de LD estão aproveitando a crescente lista de opções oferecidas pelas criptomoedas para limpar os lucros de crimes tanto *online* como *offline*, e que os serviços de LD fornecidos por redes criminosas tradicionais estão cada vez mais sendo utilizados.

A necessidade, na percepção dos respondentes da presente pesquisa, de uma cooperação entre as áreas de PLD e *Business Intelligence* (BI) para tornar os processos mais tempestivos e efetivos, poderá sanar a demanda de novas competências, que segundo o estudo de Limba, Stankevičius e Andrulevičius (2019), é resultado do obstáculo para implementar os regulamentos de KYC e AML apropriados para o contexto das criptomoedas, pelo fato delas serem um produto digital. O estudo de Pettersson Ruiz e Angelis (2022), ao investigar a aplicabilidade das técnicas de *machine learning* para combater atividades de LD usando criptomoeda, constataram que as técnicas de *machine learning* implementadas atualmente em *exchanges* de criptomoedas são lentas e precisam ser otimizadas. Esse estudo confirma a reflexão dos respondentes da corrente pesquisa, ao relatarem sobre a efetividade do processo de PLD, que para ser alcançada, é necessário ganhar velocidade e escalabilidade de processamento de dados, uma vez que uma transação com BTC em uma *exchange* pode ocorrer em apenas 5 minutos, ou menos dependendo da agilidade e complexidade da operação.

Diante das implicações apresentadas para uma conformidade em ALM no contexto das criptomoedas, se faz imperativa a observação, por parte dos profissionais da contabilidade e organizações contábeis, de todas as assertivas presentes na **Tabela 14**, uma vez que todas foram percebidas pelos respondentes como que apresentando significante nível de eficácia.

Questões relacionadas ao tratamento contábil aplicado aos criptoativos.

A análise das possíveis abordagens contábeis aplicadas aos criptoativos realizada na presente pesquisa seguiu as orientações existentes informadas pela decisão da agenda do IFRIC sobre como os Padrões IFRS se aplicam às *holdings* de criptomoedas.

Ao esclarecer a contabilização das criptomoedas, o IFRIC considerou os requisitos contábeis para ativos intangíveis, ativos financeiros, caixa e estoque, explicando que as criptomoedas têm as características de ativo intangível ou estoque, dependendo da finalidade de manter a criptomoeda. O IFRIC considerou os requisitos de divulgação, incluindo os requisitos aplicáveis ao CPC 46 se uma entidade mensurar suas participações em criptomoedas pelo valor justo e quaisquer outros requisitos de divulgação aplicáveis.

Conforme observado anteriormente a decisão da agenda do IFRIC abordou apenas as criptomoedas onde não há reivindicação da parte emissora. Mediante ao fato de que apenas as criptomoedas estão no escopo da presente pesquisa, torna-se necessário estudos futuros, com vista na continuidade das pesquisas envolvendo as características econômicas e implicações contábeis para criptoativos como os s*ecurity token*, *utility/access token* e *stablecoins*.

5 CONSIDERAÇÕES FINAIS

Retomando a questão de pesquisa de como o profissional da contabilidade pode desempenhar um papel de agente na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro, o objetivo geral do presente estudo foi o de identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro.

Para alcance dos objetivos da pesquisa, tanto o geral como os específicos, recorreu-se ao arcabouço teórico sobre as políticas, estratégias e ações dos agentes nacionais e internacionais acerca das questões decorrentes do uso dos criptoativos, em particular as criptomoedas, no crime de LD.

Foram levantados conceitos norteadores que permitiram: (i) Elaborar um questionário, que foi aplicado junto aos profissionais com experiência na prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT) e experiência com criptoativos; e (ii) Verificar as orientações sobre a contabilização de transações envolvendo criptomoedas.

Os objetivos específicos (a) Identificar possíveis aplicações dos criptoativos nos crimes de lavagem de dinheiro, e (b) Verificar como as partes interessadas (instituições e atores) na prevenção e combate à lavagem de dinheiro estão tentando coibir a utilização dos criptoativos na prática desse crime, foram alcançados por meio da análise das percepções dos participantes da pesquisa acerca da utilização dos criptoativos no crime de LD, os riscos e desafios de crime de LD enfrentados ao lidar com criptoativos e as possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos. Quanto ao objetivo específico (c) Verificar o tratamento contábil aplicado aos criptoativos, seu alcance ocorreu por meio da análise do documento "*IFRIC Update June 2019: Holdings of Cryptocurrencies*".

Quanto a amostra constituída de 62 participantes, pode-se concluir que a prevalência observada de possíveis participantes com formação acadêmica em Ciências Contábeis, aproximadamente 31% (397/1.296) dos possíveis participantes da pesquisa, não se repetiu, dada a predominância de respondentes com formação acadêmica em Direito, aproximadamente 39% (24/62), contra cerca de 32% (20/62) dos respondentes com formação acadêmica em Ciências Contábeis.

Ao analisar o perfil dos 62 participantes, evidenciou-se que: (i) Aproximadamente 67% dos respondentes possuem elevado nível de conhecimento a respeito das regras e regulamentos domésticos de AML; (ii) Cerca de 56% dos respondentes mantem elevado nível de conhecimento a respeito das Recomendações do GAFI; e (iii) Em torno de 57% dos

respondentes possuem mais de 5 anos de experiência em PLD-FT, sendo que, aproximadamente 37%, têm nas IFs a maior concentração de sua experiência, assim como, aproximadamente 29% dos respondentes, tem na área de *compliance* sua concentração de experiência com PLD-FT.

Com relação a familiaridade dos respondentes com os criptoativos, foi possível evidenciar que aproximadamente 39% dos respondentes possuem bom conhecimento a respeito dos criptoativos, sendo que a maioria dos respondentes, cerca de 66%, têm de 1 a 5 anos de experiência com criptoativos.

Em relação ao objetivo específico de identificar possíveis aplicações dos criptoativos nos crimes de LD, conclui-se que de forma geral, os respondentes entendem que todas as assertivas relacionadas aos riscos e desafios de crime de LD enfrentados ao lidar com criptoativos, presentes na seção 4.1.2, apresentam: (i) significante nível de ocorrência; e (ii) significante nível de relevância. E que, também de forma geral, os respondentes entendem que a regulamentação específica para o mercado de criptomoedas seja a decisão mais apropriada.

Conclusão semelhante obteve-se, quando do objetivo específico de verificar como as partes interessadas (instituições e atores) na prevenção e combate à lavagem de dinheiro estão tentando coibir a utilização dos criptoativos na prática desse crime, uma vez que, os respondentes, de forma geral, entendem que todas as assertivas relacionadas ás possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos, presentes na seção 4.1.3, apresentam: (i) significante nível de relevância; e (ii) significante nível de eficácia.

Quanto ao objetivo específico de verificar o tratamento contábil aplicado aos criptoativos, conforme demonstrado na seção 4.2, a natureza das criptomoedas atende a definição de um ativo intangível conforme o Pronunciamento Técnico CPC 04 (R1) – Ativo Intangível. O CPC 16 (R1) – Estoques se aplica às criptomoedas quando são mantidas para venda no curso normal dos negócios. Se o CPC 16 (R1) não for aplicável, a entidade deve aplicar o CPC 04 (R1) às *holdings* de criptomoedas.

Servindo os objetivos específicos de subsídio para alcançar o objetivo geral, torna-se possível seguir uma abordagem baseada em risco (ABR) para a profissão contábil no tocante ao uso das criptomoedas no crime de LD, uma vez que se faz necessário que os profissionais da contabilidade identifiquem, avaliem e entendam os riscos de LD com criptoativos a que estão expostos, para a aplicação de medidas necessárias de PLD-FT.

Além das assertivas presentes nas seções 4.1.2 e 4.1.3, que estão diretamente relacionadas aos elementos de uma ABR, presentes na seção 2.6.1, por meio da análise dos

comentários deixados pelos respondentes, emergiram temas que reforçam a implementação de uma ABR para AML/CFT por parte dos profissionais que venham se envolver em atividades relacionadas com as criptomoedas.

Nesse sentido é possível concluir que o profissional da contabilidade pode desempenhar um papel de agente na prevenção e combate aos crimes relacionados à utilização dos criptoativos na LD, ao aplicar uma ABR para AML/CFT quando se envolver em atividades de criptomoedas ou fornecer produtos e serviços relacionados às criptomoedas.

Considerando as orientações para os profissionais da contabilidade sobre a implementação de uma ABR para AML/CFT no contexto das criptomoedas, os achados da pesquisa corroboram com os construtos teóricos que embasaram a pesquisa. As evidências a partir da integração das teorias foram averiguadas considerando as percepções dos respondentes com relação à identificação, avaliação e determinação da melhor forma de mitigar os riscos de LD associados às atividades de criptomoedas e ao fornecimento de produtos ou serviços envolvendo criptomoedas.

Os resultados da pesquisa levam ao conhecimento dos riscos e desafios de crime de LD ao lidar com criptomoedas, e das possíveis abordagens que ajudariam a minimizar esses riscos e desafios.

Temas como principais riscos apresentados pela LD aos profissionais da contabilidade ao lidar com criptomoedas, e os associados às categorias de risco como ponto de partida para aplicação da ABR pelo profissional da contabilidade ao lidar com criptomoedas, puderam ser identificados a partir dos comentários dos respondentes. Assim como os temas associados aos *red flag indicators* relacionados com as etapas de LD com criptomoedas, e às estratégias de anonimato ao lidar com criptomoedas.

Reconhecendo que as Recomendações do GAFI se aplicam igualmente aos profissionais da contabilidade quando eles estão envolvidos em atividades ligadas às criptomoedas, incluindo obrigações relacionadas à CDD, os temas associados aos desafios ao lidar com criptomoedas, e às respostas regulatórias AML/CFT mais apropriadas ao lidar com as criptomoedas, emergiram após análise dos comentários dos respondentes.

Estando no acesso a informações precisas, oportunas e objetivas sobre os riscos de LD/FT, o pré-requisito para que o profissional da contabilidade possa aplicar uma ABR para AML/CFT eficaz, durante o processo de avaliação de risco, o tema correspondente as questões referentes as fontes de informação sobre avaliação de risco de LD ao lidar com criptomoedas,

foi identificado como mais um importante tema entre os que reforçam a implementação de uma ABR para AML/CFT no contexto das criptomoedas.

Outros importantes temas foram identificados junto aos comentários deixados pelos respondentes, como o tema correspondente aos fatores e medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar com criptomoedas, o tema associado às medidas de *customer due diligence* aprimoradas ao lidar com criptomoedas, e o tema relacionado às políticas, procedimentos e controles da organização projetados para limitar e controlar os riscos de LD ao lidar com criptomoedas.

O conhecimento dos riscos e desafios de crime de LD ao lidar com criptomoedas, e das possíveis abordagens que ajudariam a minimizar esses riscos e desafios, levantam questões para uma conformidade em ALM no contexto das criptomoedas, que foram discutidas na seção 4.3.

Mediante discussão dessas questões presentes nos elementos de uma ABR no contexto das criptomoedas, foi possível concluir que essas implicações podem promover impactos materiais significativos e devem ser observadas pelos profissionais da contabilidade.

Portanto, quando as organizações contábeis atuarem como PSAVs, ou se envolverem com AVs e PSAVs, terão que compreender as implicações apresentadas na presente pesquisa, para poderem desempenhar um papel de agente na prevenção e combate aos crimes relacionados à utilização dos criptoativos na LD.

A contribuição esperada por meio da presenta pesquisa está na possibilidade de trazer às teorias, práticas e políticas existentes um debate mais aprofundado sobre os dilemas na PLD no contexto dos criptoativos. Trazer aos profissionais da contabilidade uma oportunidade de contato com as medidas de prevenção que precisarão saber para cumprir e proteger a si mesmos, seus clientes e suas organizações, quando do envolvimento com as criptomoedas.

Como sugestão de pesquisas futuras, com vista na continuidade das pesquisas envolvendo o uso dos criptoativos nos crimes de LD, recomenda-se uma abordagem junto aos profissionais da contabilidade, que atuem em três diferentes grupos bem definidos, sob diferentes óticas, como sob a ótica da perícia criminal, da inteligência e da investigação.

REFERÊNCIAS

AHERN, D. M. Regulators Nurturing FinTech Innovation: Global Evolution of the Regulatory Sandbox as Opportunity Based Regulation. **European Banking Institute Working Paper Series**, Frankfurt, n. 60, mar. 2020.

ALBRECHT, C.; DUFFIN, K. M.; HAWKINS, S.; MORALES ROCHA, V. M. The use of cryptocurrencies in the money laundering process. **Journal of Money Laundering Control**, Leeds, v. 22, n. 2, p. 210-216, 2019.

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTING (AICPA). **Accounting for and auditing of digital assets**. Durham: AICPA, 2022.

AMORIM, E. C.; CARDOZO, M. A.; VICENTE, E. F. R. Os impactos da implementação de controles internos, auditoria e compliance no combate e prevenção à lavagem de dinheiro no Brasil. **Enfoque Reflexão Contábil**, Paraná, v. 31, n. 3, p. 23-35, set./dez. 2012.

ANDRADE, M.; SHARMAN, S.; XIAO, L. Y.; NEWALL, P. W. S. Safer gambling and consumer protection failings among 40 frequently visited cryptocurrency-based online gambling operators. **Psychology of Addictive Behaviors**, Washington, DC, v. 37, issue 3, p. 545-557, May 2023.

ANGELINE, Y. K. H.; CHIN, W. S.; MELISSA, T. T. T.; SALEH, Z. Accounting Treatments for Cryptocurrencies in Malaysia: The Hierarchical Component Model Approach. **Asian Journal of Business and Accounting**, Kuala Lumpur, v. 14, n. 2, p. 137-171, Dec. 2021.

ARAÚJO, R. F. de. **A percepção de diferentes tipos de corrupção na ótica dos profissionais da contabilidade**. 2014. 78 f. Dissertação (Mestrado em Ciências Contábeis) – Programa Multiinstitucional e Inter-regional de Pós-graduação em Ciências Contábeis, Universidade de Brasília, Universidade Federal da Paraíba, Universidade Federal do Rio Grande do Norte, Natal, 2014.

ARDIZZI, G.; DE FRANCESCHIS, P.; GIAMMATTEO, M. Cash payment anomalies and money laundering: An econometric analysis of Italian municipalities. **International Review of Law and Economics**, Amsterdam, v. 56, p. 105-121, Dec. 2018.

ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIROS E DE CAPITAIS (ANBIMA). Guia ANBIMA de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo. **ANBIMA – Informação pública**, [RJ], 3ª versão do Guia ANBIMA de PLD-FT, 2020.

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS (ACFE). **REPORT TO THE NATIONS**: 2020 GLOBAL STUDY ON OCCUPATIONAL FRAUD AND ABUSE. Austin: Association of Certified Fraud Examiners, Inc., 2020.

BALAKINA, O.; D'ANDREA, A.; MASCIANDARO, D. Bank secrecy in offshore centres and capital flows: Does blacklisting matter? **Review of Financial Economics**, Amsterdam, v. 32, issue 1, p. 30-57, Jan. 2017.

BALANI, H. Assessing the introduction of anti-money laundering regulations on bank stock valuation: An empirical analysis. **Journal of Money Laundering Control**, Leeds, v. 22, n. 1, p. 76-88, 2019.

BANCO CENTRAL DO BRASIL (BCB). Ministério da Economia. **Circular nº 3.978, de 23 de janeiro de 2020**. Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016. Brasília, DF, 2020. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3978. Acesso em: 3 fev. 2021.

BANCO CENTRAL DO BRASIL (BCB). Ministério da Economia. **Comunicado nº 25.306, de 19 de fevereiro de 2014**. Esclarece sobre os riscos decorrentes da aquisição das chamadas "moedas virtuais" ou "moedas criptográficas" e da realização de transações com elas. Brasília, DF, 2014. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=25306. Acesso em: 15 ago. 2020.

BANCO CENTRAL DO BRASIL (BCB). Ministério da Economia. **Comunicado nº 31.379, de 16 de novembro de 2017**. Alerta sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais. Brasília, DF, 2017. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadVoto.asp?arquivo=/Votos/BCB/2017246/Voto_2462017_BCB.pdf. Acesso em: 15 ago. 2020.

BARDIN, L. **Análise de conteúdo.** Lisboa: Edições 70, 1977.

BARONE, R.; DELLE SIDE, D.; MASCIANDARO, D. Drug trafficking, money laundering and the business cycle: Does secular stagnation include crime? **Metroeconomica**, Hoboken, v. 69, issue 2, p. 409-426, May 2018.

BARONE, R.; MASCIANDARO, D. Organized crime, money laundering and legal economy: theory and simulations. **European Journal of Law and Economics**, Berlin, v. 32, issue 1, p. 115-142, Aug. 2011.

BARONE, R.; MASCIANDARO, D.; SCHNEIDER, F. Money laundering and corruption: birds of a feather flock together. **CESifo Working Paper**, n. 7687. Munich: Center for Economic Studies and ifo Institute (CESifo), 2019.

BAUER, M. W.; GASKELL, G. **Pesquisa qualitativa com texto, imagem e som**. 2. ed. Petrópolis: Editora Vozes, 2002.

BEEBEEJAUN, A.; DULLOO, L. A critical analysis of the anti-money laundering legal and regulatory framework of Mauritius: a comparative study with South Africa. **Journal of Money Laundering Control**, Leeds, v. 26, n. 2, p. 401-417, 2023.

BIBLE, W.; RAPHAEL, J.; TAYLOR, P.; ORIS VALIENTE, I. **Blockchain technology and its potential impact on the audit and assurance profession**. Toronto: Deloitte Development LLC, 2017.

BLANDIN, A.; CLOOTS, A. S.; HUSSAIN, H.; RAUCHS, M.; SALEUDDIN, R.; ALLEN, J. G.; ZHANG, B.; CLOUD, K. **The Global Cryptoasset Regulatory Landxcape Study**. United Kingdom: Cambridge Centre for Alternative Finance, 2019.

BOFF, S. O.; FERREIRA, N. A. Análise dos benefícios sociais da bitcoin como moeda. **Anuario Mexicano de Derecho Internacional**, Ciudad de México, v. 16, p. 499-523, jan. 2016.

BÖHME, R.; CHRISTIN, N.; EDELMAN, B.; MOORE, T. Bitcoin: economics, technology, and governance. **Journal of Economic Perspectives**, Pittsburgh, v. 29, n. 2, p. 213-238, Spring 2015.

BORG, J. F.; SCHEMBRI, T. The regulation of blockchain technology. In: DEWEY, J. (Contributing Editor). **GLI, Global Legal Insights** – Blockchain & Cryptocurrency Regulation 2019, First Edition. London: Global Legal Group, 2019. p. 188-192.

BOULIANNE, E.; FORTIN, M. Risks and Benefits of Initial Coin Offerings: Evidence from impak Finance, a Regulated ICO. **Account Perspectives**, Toronto, v. 19, n. 4, p. 413-437, Dec. 2020.

BRADBURY, D. Data mining with LinkedIn. **Computer Fraud & Security**, Amsterdam, v. 2011, issue 10, p. 5-8, Oct. 2011.

BRASIL. **Decreto nº 154, de 26 de junho de 1991.** Promulga a Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas. Brasília, DF, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0154.htm. Acesso em: 23 set. 2020.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 14 out. 2020.

BRASIL. **Decreto-Lei nº 9.295, de 27 de maio de 1946**. Cria o Conselho Federal de contabilidade, define as atribuições do Contador e dos Guarda-livros, e dá outras providências. Brasília, DF, 1946. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del9295.htm. Acesso em: 13 out. 2020.

BRASIL. **Lei nº 8.137, de 27 de dezembro de 1990**. Dispõe sobre os crimes contra a ordem tributária, econômica e contra as relações de consumo e dá outras providências. Brasília, DF, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8137.htm. Acesso em: 14 out. 2020.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF, e

dá outras providências. Brasília, DF, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9613compilado.htm. Acesso em: 4 ago. 2020.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em: 14 out. 2020.

BRASIL. **Lei nº 11.101, de 9 de fevereiro de 2005**. Regula a recuperação judicial, a extrajudicial e a falência do empresário e da sociedade empresária. Brasília, DF, 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11101.htm. Acesso em: 14 out. 2020.

BRASIL. **Lei nº 12.683, de 9 de julho de 2012.** Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Brasília, DF, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12683.htm. Acesso em: 17 out. 2020.

BRASIL. Ministério da Justiça. **EM nº 692, de 18 de dezembro de 1996**. Exposição de motivos da Lei nº 9.613 de março de 1998. Brasília, DF, 1996. Disponível em: http://www.fazenda.gov.br/orgaos/coaf/legislacao-e-normas/legislacao/exposicao-de-motivos-lei-9613.pdf. Acesso em: 10 set. 2020.

CABELLO, M. E. A política criminal de prevenção e repressão à lavagem de dinheiro perpetrada através do futebol. **Revista Brasileira de Políticas Públicas**, Brasília, v. 1, n. 3 – número especial, p. 179-205, dez. 2011.

CAERS, R.; CASTELYNS, V. LinkedIn and Facebook in Belgium: The Influences and Biases of Social Network Sites in Recruitment and Selection Procedures. **Social Science Computer Review**, Thousand Oaks, v. 29, n. 4, p. 437-448, Nov. 2011.

CALASTRO JUNIOR, J. A.; MENDONÇA NETO, O. R. Prevenção à lavagem de dinheiro no mercado de valores mobiliários brasileiro. Revista Gestão & Tecnologia, Pedro Leopoldo, v. 18, n. 3, p. 228-251, Ed. extraordinária 2018.

CARNEIRO, Y. F. F.; SZUSTER, N. S., SIQUEIRA, J. R. M.; FONSECA, A. C. P. D. D. Contabilidade forense: A aplicação da atividade contábil investigativa e sua perspectiva futura no Brasil. **Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ**, Rio de Janeiro, v. 21, n. 3, p. 56-73, set./dez. 2016.

CASTELLS, M. **A Galáxia da Internet:** reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CELLARD, A. A Análise Documental. In: POUPART, J.; DESLAURIERS, J. P.; GROULX, L. H.; LAPERRIÈRE, A.; MAYER, R.; PIRES, A. (Orgs.). **A pesquisa qualitativa**: enfoques epistemológicos e metodológicos. Petrópolis, RJ: Vozes, 2008. p. 295-316.

CHADWICK, A. Internet Politics: States, Citizens, and New Communication Technologies. In: LUCERO, E. **Governança da Internet:** Aspectos da Formação de um Regime Global e

Oportunidades para a Ação Diplomática. Ministério das Relações Exteriores. Brasília: Fundação Alexandre de Gusmão (FUNAG), 2011.

CHAIKIN, D. Commercial corruption and money laundering: a preliminary analysis. **Journal of Financial Crime**, Leeds, v. 15, issue 3, p. 269-281, 2008.

CHAIKIN, D. How effective are suspicious transaction reporting systems? **Journal of Money Laundering Control**, Leeds, v. 12, n. 3, p. 238-253, 2009.

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA (CPAC). **Audit Considerations Related to Cryptocurrency Assets and Transactions**. Toronto: CPAC, 2018.

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA (CPAC). **Viewpoints: Applying Canadian Auditing Standards (CASs) in the crypto-asset sector**. Toronto: CPAC, 2020.

CHAUMIER, J. Les Techniques documentaires. In: BARDIN, L. **Análise de conteúdo.** Lisboa: Edições 70, 1977.

CHEN, Z.; VAN KHOA, L. D.; TEOH, E. N.; NAZIR, A.; KARUPPIAH, E. K.; LAM, K. S. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. **Knowledge and Information Systems**, Berlin, v. 57, issue 2, p. 245-285, Nov. 2018.

CHONG, A. E.; LOPEZ DE SILANES, F. Money laundering and its regulation. **Economics & Politics**, Hoboken, v. 27, n. 1, p. 78-123, Mar. 2015.

CHOO, K. K. R. Designated non-financial businesses and professionals: A review and analysis of recent financial action task force on money laundering mutual evaluation reports. **Security Journal**, Stuttgart, v. 27, n. 1, p. 1-26, Feb. 2014.

CHOU, J. H.; AGRAWAL, P.; BIRT, J. Accounting for crypto-assets: stakeholder's perceptions. **Studies in Economics and Finance**, Leeds, v. 39, n. 3, p. 471-489, 2022.

COELHO JUNIOR, F. A.; DA SILVA ABBAD, G. Construção e validação de uma escala de avaliação de impacto em profundidade de um treinamento a distância em uma organização do setor bancário brasileiro. **REAd** – Revista Eletrônica de Administração, Porto Alegre, v.16, n. 1, p. 91-119, jan./abr. 2010.

COELHO, R.; FISHMAN, J.; OCAMPO, D. G. Supervising cryptoassets for anti-money laundering. **FSI Insights on Policy Implementation No 31**, Basel, 2021.

COLAUTO, R. D.; BEUREN, I. M. Coleta, Análise e Interpretação dos Dados. In: BEUREN, I. M. (Org.). **Como Elaborar Trabalhos Monográficos em Contabilidade**: Teoria e Prática. 3 ed. São Paulo: Atlas, 2013. p. 117-144.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **Criptoativos** – Série Alertas. Rio de Janeiro, 2018a. Disponível em:

https://www.investidor.gov.br/portaldoinvestidor/export/sites/portaldoinvestidor/publicacao/Alertas/alerta_CVM_CRIPTOATIVOS_10052018.pdf. Acesso em: 6 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **FAQ** – Perguntas Frequentes. Initial Coin Offering (ICO). Rio de Janeiro, 2017b. Disponível em: http://www.cvm.gov.br/noticias/arquivos/2017/20171116-1.html. Acesso em: 10 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **Instrução CVM nº 555, de 17 de dezembro de 2014**. Dispõe sobre a constituição, a administração, o funcionamento e a divulgação de informações dos fundos de investimento. Rio de Janeiro, [2014]. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst555.html. Acesso em: 10 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **Instrução CVM nº 617, de 5 de dezembro de 2019**. Dispõe sobre a prevenção à lavagem de dinheiro e ao financiamento do terrorismo – PLDFT no âmbito do mercado de valores mobiliários. Rio de Janeiro, 2019. Disponível em: http://www.cvm.gov.br/legislacao/instrucoes/inst617.html. Acesso em: 9 set. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **Instrução CVM nº 626, de 15 de maio de 2020**. Dispõe sobre as regras para constituição e funcionamento de ambiente regulatório experimental (sandbox regulatório). Rio de Janeiro, 2020. Disponível em: http://www.cvm.gov.br/audiencias_publicas/ap_sdm/2019/sdm0519.html. Acesso em: 18 jun. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **Nota de esclarecimento**. Initial Coin Offering (ICO). Rio de Janeiro, 2017a. Disponível em: https://www.gov.br/cvm/pt-br/assuntos/noticias/initial-coin-offering--ico--a0e4b1d10e5a47aa907191d5b6ce5714. Acesso em: 15 ago. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **Ofício Circular nº 1/2018/CVM/SIN, de 12 de janeiro de 2018**. Rio de Janeiro 2018c. Disponível em: http://www.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-0118.html. Acesso em: 10 out. 2020.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Ministério da Fazenda. **Ofício Circular nº 11/2018/CVM/SIN, de 19 de setembro de 2018**. Rio de Janeiro, 2018b. Disponível em: http://www.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-1118.html. Acesso em: 10 out. 2020.

COMITÊ DE PRONUNCIAMENTO CONTÁBEIS (CPC). **Pronunciamento Técnico CPC 02 (R2)** – Efeitos das Mudanças nas Taxas de Câmbio e Conversão de Demonstrações Contábeis. Brasília, DF, 2010. Disponível em: http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=9. Acesso em: 11 out. 2020.

COMITÊ DE PRONUNCIAMENTO CONTÁBEIS (CPC). **Pronunciamento Técnico CPC 04 (R1)** – Ativo Intangível. Brasília, DF, 2010. Disponível em:

http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=35. Acesso em: 7 out. 2020.

COMITÊ DE PRONUNCIAMENTO CONTÁBEIS (CPC). **Pronunciamento Técnico CPC 16 (R1)** – Estoques. Brasília, DF, 2009. Disponível em: http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=47. Acesso em: 7 out. 2020.

COMITÊ DE PRONUNCIAMENTO CONTÁBEIS (CPC). **Pronunciamento Técnico CPC 24** – Evento Subsequente. Brasília, DF, 2009. Disponível em: http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=55. Acesso em: 9 out. 2020.

COMITÊ DE PRONUNCIAMENTO CONTÁBEIS (CPC). **Pronunciamento Técnico CPC 26 (R1)** – Apresentação das Demonstrações Contábeis. Brasília, DF, 2011. Disponível em: http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=57. Acesso em: 9 out. 2020.

COMITÊ DE PRONUNCIAMENTO CONTÁBEIS (CPC). **Pronunciamento Técnico CPC 39** – Instrumentos Financeiros: Apresentação. Brasília, DF, 2009. Disponível em: http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=70. Acesso em: 11 out. 2020.

COMITÊ DE PRONUNCIAMENTO CONTÁBEIS (CPC). **Pronunciamento Técnico CPC 46** – Mensuração do Valor Justo. Brasília, DF, 2012. Disponível em: http://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos/Pronunciamento?Id=78. Acesso em: 9 out. 2020.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF). **Avaliação Nacional de Riscos** – Brasil 2021: Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa. Brasília, DF, 2021b.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF). **Casos & Casos**: Coletânea de casos brasileiros de lavagem de dinheiro. Consolidação das Coletâneas I, II e III, ampliada e atualizada em julho de 2016. Brasília, DF, 2016.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF). **Coaf em números**. 2020. Disponível em: http://fazenda.gov.br/orgaos/coaf. Acesso em: 24 out. 2020.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF). **Lavagem de dinheiro: um problema mundial**. Brasília, DF, [1999]. Disponível em: https://www.gov.br/fazenda/pt-br/centrais-de-conteudos/publicacoes/cartilhas/arquivos/cartilha-lavagem-de-dinheiro-um-problema-mundial.pdf/view. Acesso em: 17 out. 2020.

CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF). **Resolução COAF nº 36, de 10 de março de 2021**. Disciplina a forma de adoção de políticas, procedimentos e controles internos de prevenção à lavagem de dinheiro, ao financiamento do

terrorismo e ao financiamento da proliferação de armas de destruição em massa que permitam o atendimento ao disposto nos arts. 10 e 11 da Lei nº 9.613, de 3 de março de 1998, por aqueles que se sujeitam, nos termos do seu art. 14, § 1º, à supervisão do Conselho de Controle de Atividades Financeiras – Coaf. Brasília, DF, 2021a. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-coaf-n-36-de-10-de-marco-de-2021-307765911. Acesso em: 13 abr. 2021.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). **Norma Brasileira de Contabilidade, NBC PG 01, de 7 de fevereiro de 2019**. Aprova a NBC PG 01 – Código de Ética Profissional do Contador. Brasília, DF, 2019. Disponível em: https://www2.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2019/NBCPG01&arquivo=NBCPG01.doc. Acesso em: 13 out. 2020.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). **Norma Brasileira de Contabilidade, NBC TA 315 (R2), de 2 de setembro de 2021**. Dá nova redação à NBC TA 315 (R1). Que dispõe sobre a identificação e a avaliação dos riscos de distorção relevante por meio do entendimento da entidade e do seu ambiente. Brasília, DF, 2021. Disponível em: https://www2.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2021/NBCTA315(R2)&arquivo=NBCTA315(R2).doc. Acesso em: 21 set. 2022.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). **Resolução CFC nº 1.445, de 26 de julho de 2013.** Dispõe sobre os procedimentos a serem observados pelos profissionais e organizações contábeis, quando no exercício de suas funções, para cumprimento das obrigações previstas na Lei nº 9.613/1998 e alterações posteriores. Brasília, DF, 2013. Disponível em: https://www2.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2013/001445&Codigo=2013/001445. Acesso em: 13 set. 2020.

CONSELHO FEDERAL DE CONTABILIDADE (CFC). **Resolução CFC nº 1.530, de 22 de setembro de 2017**. Dispõe sobre os procedimentos a serem observados pelos profissionais e organizações contábeis para cumprimento das obrigações previstas na Lei nº 9.613/1998 e alterações posteriores. Brasília, DF, 2017. Disponível em: https://www2.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2017/001530&arquivo=Res_1530.doc. Acesso em: 13 set. 2020.

CORBETTA, P. **Social research:** Theory, methods and techniques. London: Sage, 2003.

CORRÊA, L. M. P. **O Grupo de Ação Financeira Internacional (GAFI): organizações internacionais e crime transnacional.** Brasília, DF: Fundação Alexandre de Gusmão - FUNAG, 2013.

DANIEL, J.; GREEN, A. **IFRS (#) Accounting for crypto-assets**. London: EYGM Limited, 2018.

DA ROCHA ALVES, I. J. B.; DE SOUZA, M. I.; DA COSTA ALVES, P. G.; DA ROCHA SILVA, N. Percepção dos contabilistas de Campina Grande – PB acerca da Contabilidade e da responsabilidade do profissional contábil como instrumento de prevenção e combate à corrupção. **Polêm!ca**, Rio de Janeiro, v. 19, n. 3, p. 60-85, set./dez. 2019.

DA SILVA, J. L. R.; MARQUES, L. F. B.; TEIXEIRA, R. Prevenção à lavagem de dinheiro em instituições financeiras: Avaliação do grau de aderência aos controles internos. **Base Revista de Administração e Contabilidade da UNISINOS**, São Leopoldo, v. 8, n. 4, p. 300-310, out./dez. 2011.

D'AVINO, C. Money laundering and AML regulatory and judicial system regimes: investigation of FinCEN files. **European Journal of Law and Economics**, Berlin, v. 55, issue 2, p. 195-223, Apr. 2023.

DE ALMEIDA, F. C. O historiador e as fontes digitais: uma visão acerca da internet como fonte para pesquisas históricas. **Revista Aedos**, Porto Alegre, v. 3, n. 8, p. 9-30, jan./jun. 2011.

DEWEY, J. N. Foreword. In: DEWEY, J. N. (Contributing Editor). **GLI, Global Legal Insights** – Blockchain & Cryptocurrency Regulation 2019, Fourth Edition. London: Global Legal Group, 2022. Disponível em: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations#:~:text=GLI%20%2D%20Blockchain%20%26%20Cryptocurrency%20Regulation%202022,%2C%20mining%20%E2%80%93%20in%2030%20jurisdictions. Acesso em: jun. 2022.

DINENZON, M.; JOSYULA, V.; MORENO-RAMIREZ, J. C.; DIPPELSMAN, R.; RAZIN, T. **Treatment of Crypto Assets in Macroeconomic Statistics**. Washington: International Monetary Fund – IMF; Statistics Department, [2018]. Disponível em: https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf. Acesso em: 2 fev. 2020.

DUPUIS, D.; GLEASON, K. Money laundering with cryptocurrency: open doors and the regulatory dialectic. **Journal of Financial Crime**, Leeds, v. 28, n. 1, p. 60-74, 2020.

DURGUTI, E.; ARIFI, E.; GASHI, E.; SPAHIU, M. Anti-money laundering regulations' effectiveness in ensuring banking sector stability: Evidence of Western Balkan. **Cogent Economics & Finance**, Abingdon, v. 11, issue 1, p. 1-16, 2023.

DYBALL, M. C.; SEETHAMRAJU, R. Client use of blockchain technology: exploring its (potential) impact on financial statement audits of Australian accounting firms. **Accounting, Auditing & Accountability Journal**, Leeds, v. 35, n. 7, p. 1656-1684, 2022.

DYNTU, V.; DYKYI, O. Cryptocurrency in the system of money laundering. **Baltic Journal of Economics Studies**, Riga, v. 4, n. 5, p. 75-81, 2018.

ERNST & YOUNG (EY). **Holdings of cryptocurrencies**. London: EYGM Limited, 2019.

ESTELLITA, H. Criptomoedas e lavagem de dinheiro. **Revista Direito GV**. São Paulo, v.16, n. 1, p. 1-13, 2020.

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E LAVAGEM DE DINHEIRO (ENCCLA). **Ação 8**: Aprofundar os estudos sobre a utilização de ativos virtuais para fins de lavagem de dinheiro e financiamento do terrorismo, apresentando (i)

levantamento de boas práticas relacionadas com a investigação do delito em diversas esferas; (ii) eventual proposta de adequação normativa em matéria investigativa e de persecução penal. Brasília, DF, 2019. Disponível em: http://enccla.camara.leg.br/acoes/acoes-de-2019. Acesso em: 25 jun. 2020.

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E LAVAGEM DE DINHEIRO (ENCCLA). **Ação 8**: Aprofundar os estudos sobre a utilização de moedas virtuais para fins de lavagem de dinheiro e eventualmente apresentar propostas para regulamentação e/ou adequação legislativa. Brasília, DF, 2018. Disponível em: http://enccla.camara.leg.br/acoes/acoes-de-2018-1. Acesso em: 25 jun. 2020.

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E LAVAGEM DE DINHEIRO (ENCCLA). **Ação 8**: Elaborar diagnóstico sobre a atual conjuntura da utilização de moedas virtuais e meios de pagamento eletrônico. Brasília, DF, 2017b. Disponível em: http://enccla.camara.leg.br/acoes/acoes-de-2017. Acesso em: 25 jun. 2020.

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E LAVAGEM DE DINHEIRO (ENCCLA). **Estrutura**. Brasília, DF, 2020. Disponível em: http://enccla.camara.leg.br/quem-somos/gestao. Acesso em: 24 out. 2020.

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E LAVAGEM DE DINHEIRO (ENCCLA). **Glossário**. São Paulo: ENCCLA, 2017a.

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E LAVAGEM DE DINHEIRO (ENCCLA). **Moedas Virtuais e Meios Eletrônicos de Pagamento**: Tipologias. São Paulo: ENCCLA, 2017c.

EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL). Seizing the opportunity: 5 recommendations for crypto assets – related crime and money laundering. 2022 Recommendations of the Joint Working Group on Criminal Finances and Cryptocurrencies. In: 6th Global Conference on Criminal Finances and Cryptocurrencies. 1-2 September 2022, The Hague, Netherlands. **Proceedings** […]. The Hague: EUROPOL, 2022. Disponível em: https://www.europol.europa.eu/publications-events/publications/seizing-opportunity-five-recommendations-for-crypto-assets-related-crime-and-money-laundering. Acesso em: 6 maio 2023.

FAÇANHA, M. C.; DE LIMA, F. D. A. P.; DE LUCA, M. M. M.; DE VASCONELOS, A. C. Gerenciamento de riscos e gestão de controles internos em empresas brasileiras envolvidas em crimes de corrupção e lavagem de dinheiro. **Revista Contemporânea de Contabilidade**, Florianópolis, v. 17, n. 43, p. 34-50, abr./jun. 2020.

FANUSIE, Y. J.; ROBINSON, T. Bitcoin laundering: an analysis of illicit flows into digital currency services. **Center on Sanctions & Illicit Finance Memorandum**. Washington, DC: Foundation for Defense of Democracies (FDD), 2018.

FERREIRA, L. F.; ONZI, S. M. D.; RAMALHO, F. Eficácia das normas de compliance no Brasil a partir da perspectiva do modelo adotado pelo COAF. **Revista Eletrônica de Estratégia e Negócios**, Florianópolis, v. 12, n. 3, p. 130-153, set./dez. 2019.

FERWERDA, J. The economics of crime and money laundering: Does ant-money laundering policy reduce crime? **Review if Law & Economics**, Berlin, v. 5, issue 2, p. 903-929, Dec. 2009.

FERWERDA, J.; VAN SAASE, A.; UNGER, B.; GETZNER, M. Estimating money laundering flows with a gravity model-based simulation. **Scientific Reports**, Berlin, v. 10, n. 1, p. 1-11, 2020.

FINANCIAL ACTION TASK FORCE (FATF). **12-month Review Virtual Assets and VASPS**. Paris: FATF, 2020c.

FINANCIAL ACTION TASK FORCE (FATF). **Concealment of Beneficial Ownership**. Paris: FATF, 2018b.

FINANCIAL ACTION TASK FORCE (FATF). **FATF Report to the G20 Finance Ministers and Central Bank Governors**. Paris: FATF, 2018a.

FINANCIAL ACTION TASK FORCE (FATF). **Financial Acton Task Force on Money Laundering** – Report. Paris: FATF, 1990.

FINANCIAL ACTION TASK FORCE (FATF). **Global Assessment Calendar**. Year 2023. Disponível em: https://www.fatf-gafi.org/en/calendars/assessments.html. Acesso em: 24 mar. 2023.

FINANCIAL ACTION TASK FORCE (FATF). **Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**. Paris: FATF, 2019b.

FINANCIAL ACTION TASK FORCE (FATF). **Guidance for a Risk-Based Approach**: Virtual Currencies. Paris: FATF, 2015.

FINANCIAL ACTION TASK FORCE (FATF). **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**. Paris: FATF, 2020a.

FINANCIAL ACTION TASK FORCE (FATF). **Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets**. Paris: FATF, 2020b.

FINANCIAL ACTION TASK FORCE (FATF). **Mutual Evaluation Report. Anti-Money Laundering and Combating the Financing of Terrorism. Federative Republic of Brazil.** Paris: FATF, 2010.

FINANCIAL ACTION TASK FORCE (FATF). **Risk-Based Approach for the Accounting Profession**. Paris: FATF, 2019a.

FINANCIAL ACTION TASK FORCE (FATF). **Second 12-month Review Virtual Assets and VASPS**. Paris: FATF, 2021b.

FINANCIAL ACTION TASK FORCE (FATF). **Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**. Paris: FATF, 2021a.

FINANCIAL ACTION TASK FORCE (FATF). **Virtual Currencies**: Key Definitions and Potential *AML*/CFT Risk. Paris: FATF, 2014.

FINANCIAL CONDUCT AUTHORITY (FCA). **Guidance on Cryptoassets**. Consultation Paper 19/3. London: FCA, 2019.

FINANCIAL STABILITY BOARD (FSB). **Crypto-asset markets**: Potential channels for future financial stability implications. Basel: FSB, 2018.

FINANCIAL STABILITY BOARD (FSB). **Crypto-assets**: Work underway, regulatory approaches and potential gaps. Basel: FSB, 2019b.

FINANCIAL STABILITY BOARD (FSB). **Decentralised financial technologies**: Report on financial stability, regulatory and governance implications. Basel: FSB, 2019a.

FINANCIAL STABILITY BOARD (FSB). **Global Monitoring Report on Non-Bank Financial Intermediation 2019**. Basel: FSB, 2020.

FINANCIAL TRANSACTIONS AND REPORTS ANALYSIS CENTRE OF CANADA (FINTRAC). **Risk-based approach workbook Accountants**. Ottawa, December 2018. Disponível em: https://www.fintrac-canafe.gc.ca/guidance-directives/compliance-conformite/rba/rba-acc-eng. Acesso em: 22 jan. 2021.

FIRAS, M. Measures to combat money laundering and terrorist financing in Palestine. **Journal of Money Laundering Control**, Leeds, v. 25, n. 2, p. 268-279, 2022.

FLORÊNCIO FILHO, M. A.; ZANON, P. B. ARRANJO INSTITUCIONAL NO ÂMBITO DA ENCCLA – ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E LAVAGEM DE DINHEIRO: ENCCLA'S INSTITUTIONAL ARRANGEMENT – NATIONAL STRATEGY TO COMBAT CORRUPTION AND MONEY LAUNDERING. ***Delictae*: Revista de Estudos Interdisciplinares sobre o Delito**, Belo Horizonte, v. 3, n. 5, p. 201-235, jul./dez. 2018.

FOLEY, S.; KARLSEN, J. R.; PUTNIŅŠ, T. J. Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? **The Review of Financial Studies**, Oxford, v. 32, issue 5, p. 1798-1853, May 2019.

FRANCO, M. L. P. B. **Análise de Conteúdo**. 3 ed. Brasília: Liber Livro Editora, 2008.

GASKELL, G. Entrevistas individuais e grupais. In: Bauer, M. W.; GASKELL, G. (ed.). **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis: Vozes, 2002. p. 64-89.

GIAMMATTEO, M.; IEZZI, S.; ZIZZA, R. Pecunia olet. Cash usage and the underground economy. **Journal of Economic Behavior and Organization**, Amsterdam, v. 204, p. 107-127, Dec. 2022.

GICHUKI, N. E. The conflict between anti-money laundering reporting obligations and the doctrine of confidentiality for legal practitioners in Kenya. **Journal of Money Laundering Control**, Leeds, v. 24, n. 3, p. 607-620, 2021.

GIKONYO, C. Detection mechanisms under Kenya's anti-money laundering regime: omissions and loopholes. **Journal of Money Laundering Control**, Leeds, v. 21, n. 1, p. 59-70, 2018.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6 ed. São Paulo: Atlas, 2008.

GIUDICI, G.; MILNE, A.; VINOGRADOV, D. Cryptocurrencies: market analysis and perspectives. **Journal of Industrial and Business Economics**, Berlin, v. 47, issue 1, p. 1-18, Mar. 2020.

GODOY, A. S. Introdução à pesquisa qualitativa e suas possibilidades. **Revesta Administração de Empresas**, São Paulo, v. 35, n. 2, p. 57-63, abr. 1995a.

GODOY, A. S. Pesquisa Qualitativa: tipos fundamentais. **Revista Administração de Empresas**, São Paulo, v. 35, n. 3, p. 20-29, jun. 1995b.

GOEL, R. K.; NELSON, M. A. Shining a light on the shadows: identifying robust determinants of the shadow economy. **Economic Modelling**, Amsterdam, v. 58, p. 351-364, Nov. 2016.

GOMES, H. O.; RAMOS, M. O.; SILVA, M. V. D. D. C.; SANTOS, L. M. V. D. A Contabilidade do Crime no Brasil: Avanços e Desafios. **Revista Evidenciação Contábil & Finanças**, João Pessoa, v. 6, n. 2, p. 81-94, mai./ago. 2018.

GRAUER, K.; JARDINE, E.; LEOSZ, E.; UPDEGRAVE, H. **The 2023 Crypto Crime Report**: Everything you need to know about cryptocurrency-based crime. New York: Chainalysis, 2023.

GRUPENMACHER, G. T. **As plataformas de negociação de criptoativos**: uma análise comparativa com as atividades das corretoras e da Bolsa sob a perspectiva da proteção do investidor e da prevenção à lavagem de dinheiro. 2019. 218 f. Dissertação (Mestrado em Direito e Desenvolvimento) – Escola de Direito de São Paulo da Fundação Getúlio Vargas, São Paulo, 2019.

GULLKVIST, B.; JOKIPII, A. Perceived importance of red flag across fraud types. **Critical Perspective on Accounting**, Amsterdam, v. 24, issue1, p. 44-61, Feb. 2013.

GUSSON, C. **Brasil ganha o primeiro fundo de investimento em DeFi aprovado pela CVM**. Cointelegraph. [S. l.]. APR 8, 2021. Disponível em: https://cointelegraph.com.br/news/brazil-wins-the-first-defi-investment-fund-approved-by-the-cvm. Acesso em: 8 abr. 2021.

HAJILEE, M.; STRINGER, D. Y.; METGHALCHI, M. Financial market inclusion, shadow economy and economic growth: New evidence from emerging economies. **The Quarterly Review of Economics and Finance**, Amsterdam, v. 66, p. 149-158, Nov. 2017.

HAMIN, Z. Recent changes to the AML/CFT law in Malaysia. **Journal of Money Laundering Control**, Leeds, v. 20, n. 1, p. 5-14, 2017.

HAMMARBERG, K.; KIRKMAN, M.; DE LACEY, S. Qualitative research methods: When to use them and how to judge them. **Human Reproduction**, Oxford, v. 31, issue 3, p. 489-501, Mar. 2016.

HAQ, M. Z.; AYUB, Z. A.; YUSOFF, Z. M.; KHAN, M. A. A. Factors influencing anti-money laundering regulatory approaches towards casinos and cryptocurrencies in Bangladesh. **Journal of Money Laundering Control**, Leeds, v. 25, n. 2, p. 445-454, 2022.

HARRAST, S. A.; McGILSKY, D.; SUN, Y. T. Determining the Inherent Risks of Cryptocurrency: A Survey Analysis. **Current Issues in Auditing**, [S. l.], v. 16, n. 2, p. A10-A17, Fall, 2022.

HE, D.; HABERMEIER, K; LECKOW, R.; HAKSAR, V.; ALMEIDA, Y.; KASHIMA, M.; KYRIAKOS-SAAD, N.; OURA, H.; SEDIK, T. S.; STETSENKO, N.; VERDUGO-YEPES, C. **Virtual Currencies and Beyond**: Initial Considerations. Washington: IFM Staff Discussion Notes, 2016.

HELGESSON, K. S.; MÖRTH, U. Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention. **Crime, Law and Social Changer**, Berlin, v. 69, n. 2, p. 227-248, Mar. 2018.

HENDRIYETTY, N.; GREWAL, B. S. Macroeconomics of money laundering: effects and measurements. **Journal of Financial Crime**, Leeds, v. 24, n. 1, p. 65-81, 2017.

HSIEH, S. F.; BRENNAN, G. Issues, risks, and challenges for auditing crypto asset transactions. **International Journal of Accounting Information Systems**, Amsterdam, v. 46, p. 1-15, Sep. 2022.

HUANG, J. Y. Effectiveness of US ant-money laundering regulations and HSBC case study. **Journal of Money Laundering Control**, Leeds, v. 18, n. 4, p. 525-532, 2015.

ILBIZ, E.; KAUNERT, C. Sharing Economy for Tackling Crypto-Laundering: The Europol Associated 'Global Conference on Criminal Finances and Cryptocurrencies'. **Sustainability**, Basel, v. 14, issue 11, p. 1-15, June 2022.

INSTITUTE OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES (ICAEW). CRYPTO-ASSETS: ANTI-MONEY LAUNDERING GUIDANCE FOR ACCOUNTANTS. GUIDE. **ICAEW KNOW-HOW INTEGRITY AND MARKETS**. London: ICAEW, 2019.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **IFRIC Update June 2019** – Holdings of Cryptocurrencies. IFRS Interpretations Committee (IFRIC). Agenda Paper 12. London, 2019. Disponível em: Disponível em: https://www.ifrs.org/projects/2019/holdings-of-cryptocurrencies/#published-documents. Acesso em: 29 set. 2020.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **International Accounting Standards (IAS) 1** – Presentation of Financial Statements. London, 2014. Disponível em: https://www.ifrs.org/issued-standards/list-of-standards/ias-1-presentation-of-financial-statements/#translations. Acesso em: 9 out. 2020.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **International Accounting Standards (IAS) 2** – Inventories. London, 2003. Disponível em: https://www.ifrs.org/issued-standards/list-of-standards/ias-2-inventories/#translations. Acesso em: 9 out. 2020.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **International Accounting Standards (IAS) 10** – Events after the Reporting Period. London, 2003. Disponível em: https://www.ifrs.org/issued-standards/list-of-standards/ias-10-events-after-the-reporting-period/#translations. Acesso em: 9 out. 2020.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **International Accounting Standards (IAS) 21** – The Effects of Changes in Foreign Exchange Rates. London, 2005. Disponível em: https://www.ifrs.org/issued-standards/list-of-standards/ias-21-the-effects-of-changes-in-foreign-exchange-rates/#translations. Acesso em: 11 out. 2020.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **International Accounting Standards (IAS) 32** – Financial Instruments: Presentation. London, 2017. Disponível em: https://www.ifrs.org/issued-standards/list-of-standards/ias-32-financial-instruments-presentation/#translations. Acesso em: 11 out. 2020.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **International Accounting Standards (IAS) 38** – Intangible Assets. London, 2014. Disponível em: https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/#translations. Acesso em: 9 out. 2020.

INTERNATIONAL ACCOUNTING STANDARDS BOARD (IASB). **International Financial Reporting Standard (IFRS) 13** – Fair Value Measurement. London, 2011. Disponível em: https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/#translations. Acesso em: 9 out. 2020.

INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD (IAASB). **International Standard of Auditing 315 (Revised 2019)** – ISA 315 (Revised 2019) and Conforming and Consequential Amendments to Other International Standards Arising from ISA 315 (Revised 2019). New York: INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC), 2019. Disponível em: https://www.iaasb.org/publications/isa-315-revised-2019-identifying-and-assessing-risks-material-misstatement. Acesso em: 21 set. 2022.

INTERNATIONAL ETHICS STANDARDS BOARD FOR ACCOUNTANTS (IESBA). **Responding to Non-Compliance with Laws and Regulations**. Final Pronouncement. New York: International Federation of Accountants – IFAC, 2016.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). **Anti-Money Laundering, The Basics**: Installment 1 – Introduction to Anti-Money Laundering for Professional Accountants. New York: IFAC, 2020b.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). **Anti-Money Laundering, The Basics**: Installment 2 – A Risk-Based Approach. New York: IFAC, 2020a.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). **Anti-Money Laundering, The Basics**: Installment 7 – Virtual Assets. New York: IFAC, 2020c.

IRWIN, A. S. M.; TURNER, A. B. Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. **Journal of Money Laundering control**, Leeds, v. 21, n. 3, p. 297-313, 2018.

ISSAH, M.; ANTWI, S.; ANTWI, S. K.; AMARH, P. Anti-money laundering regulations and banking sector stability Africa. **Cogent Economics & Finance**, Abingdon, v. 10, issue 1, p. 1-16, 2022.

JAKOBI, A. P. Governing illicit finance in transnational security spaces: the FATF and anti-money laundering. **Crime, Law and Social Change**, Berlin, v. 69, n. 2, p. 173-190, Mar. 2018.

JAYASEKARA, S. D. How effective are the current global standards in combating money laundering and terrorist financing? **Journal of Money Laundering Control**, Leeds, v. 24, n. 2, p. 257-267, 2021.

JEANS, N. **A Tranche Too Hard? The AML/CFT Regulation of Australian Designated Non-Financial Businesses and Professions**. Melbourne: Initialism AML Compliance Solutions, 2019.

JOHARI, R. J.; ZUL, N. B.; TALIB, N.; HUSSIN, S. A. H. S. Money laundering: Customer due diligence in the era of cryptocurrencies. In 1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019). **Proceedings** […]. Atlantis Press, 2020. DOI: 10.2991/aebmr.k.200305.033. Disponível em: https://www.atlantis-press.com/proceedings/icamer-19/125936204. Acesso em: 5 jan. 2023.

JONES, J.; JEFFERY, S.; FIELDS, B. Accounting and financial reporting: Key challenges facing institutionalization of crypto. In: GHOSH, A.; HUNTER, C.; CAPLAIN, J. **Institutionalization of cryptoassets**: Cryptoassets have arrived. Are you ready for institutionalization? KPMG, 2020. p. 24-27.

JUNG, L. W. Lavagem de dinheiro e a responsabilidade do contador. **Revista Catarinense da Ciência Contábil**, Florianópolis, v. 6, n. 17, p. 39-54, abr./jul. 2007.

KATARZYNA, C. Cryptocurrencies: Opportunities, risks and challenges for anti-corruption compliance systems. **2019 OECD Global Anti-corruption & Integrity Forum**. Paris, 2019.

KEATINGE, T.; CARLISLE, D.; KEEN, F. **Virtual currencies and terrorist financing**: assessing the risks and evaluating responses. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs, 2018.

KETHINENI, S.; CAO, Y. The rise in popularity of cryptocurrency and associated criminal activity. **International Criminal Justice Review**, Thousand Oaks, v. 30, issue 3, p. 1-20, Sep. 2019.

KLAYMAN, J. A.; COHEN, L. R.; SOSNOW, R. **Perspective**: There are Two Sides to the Initial Coin Offering Debate. CROWDFUND INSIDER. October 30, 2017. Disponível em: https://www.crowdfundinsider.com/2017/10/123863-perspective-two-sides-initial-coin-offering-debate/. Acesso em: 5 mar. 2020.

KOTHARI, C. R. **Research Methodology**: methods & techniques. 2 ed. New Delhi: New Age International, 2004.

KRATCOSKI, P. C.; MAXIMILIAN, E. Part I – Introduction: Fraud and Corruption. In: KRATCOSKI, P. C.; MAXIMILIAN, E. (Editors). **Fraud and Corruption**: Major Types, Prevention, and Control. Cham: Springer Nature Switzerland AG, 2018. p. 1-2.

KRIMMINGER, M. H.; LLOYD, C.; ROCKS S. Custody and transfer of digital assets: Key U.S. legal considerations. In: DEWEY, J. (Contributing Editor). **GLI, Global Legal Insights** – Blockchain & Cryptocurrency Regulation 2019. First Edition. London: Global Legal Group, 2019. p. 121-131.

LEAVY, P. **Research Design** – Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches. New York: The Guilford Press, 2017.

LEUPRECHT, C.; JENKINS, C.; HAMILTON, R. Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. **Journal of Financial Crime**, Leeds, v. 30, n. 4, p. 1036-1054, 2023.

LIMBA, T.; STANKEVIČIUS, A.; ANDRULEVIČIUS, A. Towards sustainable cryptocurrency: risk mitigations from a perspective of national security. **Journal of Security and Sustainability Issues**, [Vilnius], v. 9, n. 2, p. 375-389, Dec. 2019.

LÓPEZ-CARRIL, S.; ANAGNOSTOPOULOS, C.; PARGANAS, P. Social media in sport management education: Introducing LinkedIn. **Journal of Hospitality, Leisure, Sport & Tourism Education**, Amsterdam, v. 27, p. 1-6, Nov. 2020.

LUBAS, K. M.; MARQUES, D. A. R.; SALLABERRY, J. D.; SANTOS, E. A. Discussões Conceituais e Éticas sobre Lavagem de Dinheiro nos Cursos de Ciências Contábeis. In: 18º Congresso USP de Iniciação Científica em Contabilidade, São Paulo, 18., 2021, São Paulo. **Anais eletrônicos** […]. São Paulo: USP, 2021. Disponível em: https://congressousp.fipecafi.org/anais/21UspInternational/congressinho-consultar-trabalho-por-titulo.html. Acesso em: 18 abr. 2023.

LUCERO, E. **Governança da Internet**: Aspectos da Formação de um Regime Global e Oportunidades para a Ação Diplomática. Ministério das Relações Exteriores. Brasília: Fundação Alexandre de Gusmão – FUNAG, 2011.

LÜDKE, M.; ANDRÉ, M. E. D. A. Pesquisa em educação: abordagens qualitativas. São Paulo: EPU, 1986.

MANNING, M.; WONG, G. T.; JEVTOVIC, N. Investigating the relationships between FATF recommendation compliance, regulatory affiliations and the Basel Anti-Money Laundering Index. **Security Journal**, Berlin, v. 34, issue 3, p. 566-588, Sep. 2021.

MARAGNO, L. M. D.; KNUPP, P. S.; BORBA, J. A. Corrupção, Lavagem de Dinheiro e Conluio no Brasil: Evidências Empíricas dos Vínculos entre Fraudadores e Cofraudadores no Caso Lava Jato. **Revista de Contabilidade e Organizações**, Butantã, v. 13, n. 1, p. 5-18, 2019.

MARKOVSKA, A.; ADAMS, N. Political corruption and money laundering: lessons from Nigeria. **Journal of Money Laundering Control**, Leeds, v. 18, n. 2, p. 169-181, 2015.

MARQUES, M. L. T**ratamento Contábil das Criptomoedas**. 2019. 86 f. Dissertação (Mestrado em Ciências Contábeis) – Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2019.

McDOWELL, J. Consequences of money laundering and financial crime. **Economic Perspectives**, Washington, v.6, n. 2, p. 6-8, May 2001.

MEKPOR, E. S.; ABOAGYE, A.; WELBECK, J. The determinants of anti-money laundering compliance among the Financial Action Task force (FATF) member states. **Journal of Financial Regulation and Compliance**, Leeds, v. 26, n. 3, p. 442-459, 2018.

MENDES, A. C. C. Moeda eletrônica bitcoin: análise do uso na cidade de Brasília – DF. **Revista científica multidisciplinar núcleo do conhecimento**. 3 ed. [São Paulo], ano 2, vol. 3, p. 37-73, jun. 2017.

MINHAT, M.; ABDULLAH, M.; DZOLKANAINI, N.; SHAROJA, N. **Cryptocurrency and Uncertainty**. Malaysian Institute of Accountants. [S. l.], 26 January 2022. Disponível em: https://www.at-mia.my/2022/01/26/cryptocurrency-and-uncertainty/. Acesso em: 17 jul. 2023.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES (MCTI). **Estratégia Brasileira para a Transformação Digital**. E-Digital. Brasília: MCTI, 2018.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA (MJSP). **PE e Receita reprimem crimes de evasão de divisas, lavagem de dinheiro e associação criminosa**. COMUNICAÇÃO SOCIAL DA PF EM SÃO PAULO. Brasília, DF, 27 de janeiro de 2023. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2022/09/copy_of_pf-e-receita-reprimem-crimes-de-evasao-de-divisas-lavagem-de-dinheiro-e-associacao-criminosa. Acesso em: 17 jul. 2023.

MOLLA IMENY, V.; NORTON, S. D.; MORADI, M.; SALEHI, M. The anti-money laundering expectations gap in Iran: auditor and judiciary perspectives. **Journal of Money Laundering Control**, Leeds, v. 24, n. 4, p. 681-692, 2021.

MOSER, A.; KORSTJENS, I. Series: Practial guidance to qualitative research. Part 1: Introduction. **European journal of General Practice**, Abingdon, v. 23, issue 1, p. 271-273, 2017.

MOSER, A.; KORSTJENS, I. Series: Practial guidance to qualitative research. Part 3: Sampling, data collection and analysis. **European journal of General Practice**, Abingdon, v. 24, issue 1, p. 9-18, 2018.

MÖSER, M.; BÖHME, R.; BREUKER, D. An inquiry into money laundering tools in the Bitcoin ecosystem. In: 2013 APEG eCrime Researchers Summit, 2013, San Francisco, CA, USA. **Proceedings** […]. San Francisco: IEEE, 2013. DOI: 10.1109/eCRS.2013.6805780. Disponível em: https://ieeexplore.ieee.org/document/6805780. Acesso em: 13 jan. 2023.

NAKAMOTO, S. **Bitcoin**: A Peer-to-Peer Electronic Cash System. [S. l.], 2008. Artigo tem 9 páginas. Disponível em: https://bitcoin.org. Acesso em: 15 ago. 2020.

NAKAMURA, E. A. M. V.; NAKAMURA, W. T.; JONES, G. D. C. Necessidade de estrutura de compliance nas instituições financeiras. **Revista Gestão & Tecnologia**, Pedro Leopoldo, v. 19, n. 5, p. 257-275, out./dez. 2019.

NANCE, M. T. The regime that FATF built: an introduction to the Financial Action Task Force. **Law and Social Change**, Berlin, v. 69, n. 2, p. 190-129, 2018.

NASCIMENTO, S. (ed); PÓLVORA, A. (ed), ANDERBERG, A.; ANDONOVA, E.; BELLIA, M.; CALÈS, L.; SANTOS, A. I.; KOUNELIS, I.; FOVINO, I. N., GIUDICI, M. P.; PAPANAGIOTOU, E.; SOBOLEWSKI, M.; ROSSETTI, F.; SPIRITO, L. **Blockchain Now And Tomorrow**: Assessing Multidimensional Impacts of Distributed Ledger Technologies. Luxembourg: Publications Office of the European Union, 2019.

PETTERSSON RUIZ, E.; ANGELIS, J. Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. **Journal of Money Laundering Control**, Leeds, v. 25, n. 4, p. 766-778, 2022.

PIMENTEL, E.; BOULIANNE, E.; ESKANDARI, S.; CLARK, J. Systemizing the Challenges of Auditing Blockchain-Based Assets. **Journal of Information Systems**, [S. l.], v. 35, n. 2, p. 61-75, Summer, 2021.

NDUKA, B. (O). E.; SECHAP, G. Refocusing designated nonfinancial businesses and professions on the path of anti-money laundering and combating the financing of terrorism compliance. **Journal of Money Laundering Control**, Leeds, v. 24, n. 4, p. 693-711, 2021.

NEVES JÚNIOR, I. J. das; MOREIRA, E. M. de S. Perícia contábil: uma ferramenta de combate ao crime organizado. **REPeC** – Revista de Educação e Pesquisa em Contabilidade, Brasília, DF, v. 5, Edição Especial, p. 126-156, set./dez. 2011.

NEWBURY, M. Designated non-financial businesses and professions: The weak link in Australia's AML/CTF regime. **Journal of Money Laundering Control**, Leeds, v. 20, n. 3, p. 247-261, 2017.

OFOEDA, I.; AGBLOYOR, E. K.; ABOR, J. Y.; OSEI, K. A. Anti-money laundering regulations and financial sector development. **International Journal of Finance & Economics**, Hoboken, v. 27, issue 4, p. 4085-4104, Oct. 2022.

OMAR, N.; JOHARI, R. J.; AZAM, M. A. M.; HAKIM, N. O. Mitigating money laundering: The role of designated non-financial businesses and professions in Southeast Asian Countries. In: DJAJADIKERTA, H.; ZHANG, Z. (Editors) A New Paradigm for International Business: Proceedings of the Conference on Free Trade Agreements and Regional Integration in East Asia. **Springer Proceedings in Business and Economics**. Singapore: Springer, 2015. p. 285-294.

OMAR, N.; JOHARI, Z. A. An international analysis of FATF recommendations and compliance by DNFBPS. **Procedia Economics and Finance**, Amsterdam, v. 28, p. 14-23, 2015.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors**. Paris: OECD, 2019.

PICARD, P. M.; PIERETTI, P. Bank secrecy, illicit money and offshore financial centers. **Journal of Public Economics**, Amsterdam, v. 95, issue 7-8, p. 942-955, Aug. 2011.

POL, R. F. Anti-money laundering: The word's least effective policy experiment? Together, we can fix it. **Policy Design and Practice**, Abingdon, v. 3, issue 1, p. 73-94, 2020.

POSKRIAKOV, F.; CHIRIAEVA, M.; CAVIN, C. Cryptocurrency compliance and risks: A European KYC/AML perspective. In: DEWEY, Josias (Editor). **GLI, Global Legal Insights** – Blockchain & Cryptocurrency Regulation 2019, First Edition. London: Global Legal Group, 2019. p. 163-174.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). **Audits Involving Cryptoassets Information for Auditors and Audit Committees**. Washington, DC.: PCAOB, 2020.

QUEIROZ, F. V. **Enfrentamento à Corrupção**: Participação Social na Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA). 2019. 80 f. Dissertação (Mestrado em Administração Pública) – Instituto Brasiliense de Direito Público, Escola de Administração Pública, Brasília, DF, 2019.

RAMOS, P. R. A. Corrupção na Administração Pública e crimes de "lavagem" ou ocultação de bens, direitos e valores. **Revista da CGU**, Brasília, DF, v. 5, n. 8, p. 71-87, out. 2010.

RAUPP, F. M.; BEUREN, I. M. Metodologia da Pesquisa Aplicável às Ciências Sociais. In: BEUREN, I. M. (Org.). **Como Elaborar Trabalhos Monográficos em Contabilidade**: Teoria e Prática. 3 ed. São Paulo: Atlas, 2013. p. 76-97.

RECEITA FEDERAL DO BRASIL (RFB). Ministério da Fazenda. **Imposto Sobre a Renda – Pessoa Física**: Perguntas e Respostas. Brasília: RFB, 2017.

RECEITA FEDERAL DO BRASIL (RFB). **Instrução Normativa de Nº 1.888, de 03 de maio de 2019**. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil. Brasília, DF, 2019. Disponível em:

http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592. Acesso em: 30 jun. 2020.

RIBEIRO, A. A. D.; RODRIGUES, R. N.; PRAZERES, R. V. dos; DE ARAÚJO, J. G. Um estudo sobre a relevância da contabilidade forense como instrumento de investigação: A percepção de profissionais ligados ao combate à lavagem de capitais. **Revista de Gestão, Finanças e Contabilidade**, Salvador, v. 6, n. 1, p. 45-75, jan./abr. 2016.

ROCHA, L. G. O combate à corrupção em redes interorganizacionais: um estudo da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro. **Revista da CGU**, Brasília, DF, v. 3, n. 5, p. 70-82, dez. 2008.

RODRIGUES, G.; KURTZ, L. **Cryptocurrencies and anti-money laundering regulation in the G20**. Belo Horizonte: Institute for Research on Internet and Society – IRIS, 2019.

ROWLAND, G. S.; KIVIAT, T. I. Cryptocurrency and other digital assets for asset managers. In: DEWEY, J. (Contributing Editor). **GLI, Global Legal Insights** – Blockchain & Cryptocurrency Regulation 2019. First Edition. London: Global Legal Group, 2019. p. 90-100.

SAIEDI, E.; BROSTRÖM, A.; RUIZ, F. Global drives of cryptocurrency infrastructure adoption. **Small Business Economics**, Berlin, v. 57, issue 1, p. 353-406, June 2021.

SALAWU, M. K.; MOLOI, T. Benefits of legislating cryptocurrencies: Perception of Nigerian professional accountants. **Academy of Accounting and Financial Studies Journal**, [S. l.], v. 22, issue 6, p. 1-17, 2018.

SALLABERRY, J. D.; SILVA, R. O. da; PRATES, A.; FLACH, L. CONTABILIDADE E A LAVAGEM DE DINHEIRO: REVISÃO DA LITERATURA CIENTÍFICA BRASILEIRA. **RAGC** – Revista de Auditoria, Governança e Contabilidade, Monte Carmelo, v. 8, n. 33, p. 64-76, 2020.

SÁ-SILVA, J. R.; ALMEIDA, C. D.; GUINDANI, J. F. Pesquisa documental: pistas teóricas e metodológicas. **Revista Brasileira de História & Ciências Sociais**, Rio Grande, v. 1, n. 1, p. 1-15, jan./jun. 2009.

SATHYE, M.; ISLAM, J. Adopting a risk-based approach to AMLCTF compliance: the Australian case. **Journal of Financial Crime**, Leeds, v. 18, n. 2, p. 169-182, 2011.

SCHANEIDER, F. Foreword. In: KRATCOSKI, P. C.; MAXIMILIAN, E. (Editors). **Fraud and Corruption**: Major Types, Prevention, and Control. Cham: Springer Nature Switzerland AG, 2018.

SCHNEIDER, F. Shadow economies around the word: what we really know? **European Journal of Political Economy**, Amsterdam, v. 21, issue 3, p. 598-642, Sep. 2005.

SCHWARZ, P. Money launderers and tax havens: two sides of the same coin? **International Review of Law and Economics**, Amsterdam, v. 31, issue 1, p. 37-47, Mar. 2011.

SHAH, I. H.; AISH, K. A nexus between corruption, money laundering (ML) and inflation: evidence from South Asian countries. **Journal of Money Laundering Control**, Leeds, v. 25, n. 4, p. 730-741, 2022.

SHARMA, A. M. **Cryptocurrency and Financial Risks**. 2020. 191 f. Tese (Doutorado em Administração de Empresas) – Liberty University. Lynchburg, 2020.

SILVA, L. G. D. **A regulamentação do uso de criptomoedas no Brasil**. 2017. 124 f. Dissertação (Mestrado em Direto Político e Econômico) – Universidade Presbiteriana Mackenzie. São Paulo, 2017.

SILVA, L. M. da. A NORMATIZAÇÃO DA CONTABILIDADE GOVERNAMENTAL: FATORES CRÍTICOS QUE IMPACTAM AS INFORMAÇÕES DADAS AOS USUÁRIOS DAS INFORMAÇÕES CONTÁBEIS. **REPeC** – Revista de Educação e Pesquisa em Contabilidade, Brasília, DF, v. 1, n. 1, p. 25-38, jan./abr. 2007.

SILVEIRA, R. M. J. "Criptocrime": considerações penais econômicas sobre criptomoedas e criptoativos. **Revista de Direito Penal Econômico e Compliance**, São Paulo, v. 1, p. 1-21, jan./mar. 2020.

SMITH, S. S. How Cryptocurrencies Are Changing What CPAs Need to Know about Fraud Prevention. **Theoretical Economics Letters**, [S. l.], v. 8, n. 14, p. 3252-3266, Oct. 2018.

SPINK, P. Análise de documentos de domínio público. In: SPINK, M. J. (Org.). **Práticas discursivas e produção de sentidos no cotidiano**: aproximações teóricas e metodológicas. Edição virtual. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais, 2013.

STACK, G. Money laundering in Ukraine: Tax evasion, embezzlement, illicit international flows and state capture. **Journal of Money Laundering Control**, Leeds, v. 18, n. 3, p. 382-394, 2015.

STOCKEMER, D. **Quantitative Methods for the Social Sciences**: A Practical Introduction with Examples in SPSS and Stata. Cham: Springer Nature Switzerland AG, 2019.

SUTTON, J.; AUSTIN, Z. Qualitative research: data collection, analysis, and management. **The Canadian Journal of Hospital Pharmacy**, Ottawa, v. 68, n. 3, p. 226-231, May-June 2015.

SUXBERGER, A. H. G.; CASELATO JR, D. O papel do GAFI/FATF: natureza jurídica de suas recomendações e formas de coerção aos países membros pela sua inobservância. **Revista Cadernos de Direito Actual**. [S. l.], n. 11, p. 173-185, 2019.

SUXBERGER, A. H. G.; PASIANI, R. P. R. O papel da inteligência financeira na persecução dos crimes de lavagem de dinheiro e ilícitos relacionados. **Revista Brasileira de Políticas Públicas**, Brasília, v. 8, n. 1, p. 290-319, abr. 2018.

TEICHMANN, F. M. J.; FALKER, M. C. Money laundering – the gold method. **Journal of Money Laundering Control**, Leeds, v. 26, n. 3, p. 509-522, 2023.

TEICHMANN, F. M. J.; FALKER, M. C. Money laundering through raw diamonds. **Journal of Money Laundering Control**, Leeds, v. ahead-of-print, n. ahead-of-print, 2020.

TEICHMANN, F. M. J. How effective are financial sanctions against individuals? **Journal of Money Laundering Control**, Leeds, v. 24, n. 2, p. 440-445, 2021.

TELLES, C. M. S. **Sistema bitcoin, lavagem de dinheiro e regulação**. 2018. 145 f. Dissertação (Mestrado em Governança Regulatória, Instituições e Justiça) – Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, Rio de Janeiro, 2018.

TELLES, C. V. D. Lavagem de dinheiro e o papel do profissional da Contabilidade. **Boletim Economia Empírica**, Brasília, DF, v. 2, n. 10, p. 4-15, 2021.

TRANSPARÊNCIA INTERNACIONAL. Índice de Percepção da Corrupção 2019. **Transparência Internacional Brasil**. 2020. Disponível em: https://transparenciainternacional.org.br/ipc/?gclid=CjwKCAiAyeTxBRBvEiwAuM8dnT8nf6Pfdv1x0kRD8AFZPOIuni-INrmyxL9FMCqPBMH-2kaQDKcodxoCkfoQAvD_BwE. Acesso em: 12 set. 2020.

TROZZE, A.; KAMPS, J.; AKARTUNA, E. A.; HETZEL, F. J.; KLEINBERG, B.; DAVIES, T.; JOHNSON, S. D. Cryptocurrencies and future financial crime. **Crime Science**, Berlin, v. 11, n. 1, p. 1-35, 2022.

TSINGOU, E. Global financial governance and the developing anti-money laundering regime: What lessons for international political economy? **International Politics**, Berlin, v. 47, n. 6, p. 617-637, Nov. 2010.

TURNER, A. B.; McCOMBIE, S.; UHLMANN, A. J. Analysis Techniques for Illicit Bitcoin Transactions. **Frontiers in Computer Science**, [Lausanne], v. 2, p. 1-12, Nov. 2020.

TURNER, A.; IRWIN, A. S. M. Bitcoin transactions: a digital discovery of illicit activity on the blockchain. **Journal of Financial Crime**, Leeds, v. 25, n. 1, p. 109-130, 2018.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). Digital Economy Report 2019. **Value Creation and Capture**: implications for developing countries. Geneva: United Nations, 2019.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). **Money-Laundering and Globalization**. Vienna, [2018]. Disponível em: https://www.unodc.org/unodc/en/money-laundering/globalization.html. Acesso em: 19 set. 2020.

VAN DER LAAN, C. R. **É crível uma Economia Monetária Baseada em *Bitcoins***? Limites à disseminação de moedas virtuais privadas. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, dezembro 2014 (Texto para Discussão nº 163).

VAN WEGBERG, R.; OERLEMANS, J. J.; VAN DEVENTER, O. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. **Journal of Financial Crime**, Leeds, v. 25, n. 2, p. 419-435, 2018.

VÁS, D. A. D.; SALES, E. N. O crime de lavagem de dinheiro e as responsabilidades do contador. **Revista Liceu On-line**, São Paulo, v. 5, n. 1, p. 29-44, jan./jun. 2015.

VERGARA, S. C. **Projetos e Relatórios de Pesquisa em Administração**. São Paulo: Atlas, 1998.

VINCENT, N. E.; WILKINS, A. M. Challenges when Auditing Cryptocurrencies. **Current Issues in Auditing**, [S. l.], v. 14, issue 1, p. 46-58, Spring, 2020.

WEEKS-BROWN, R. Countries are advancing efforts to stop criminals from laundering their trillions. **FINANCE & DEVELOPMENT**: A Quarterly Publication of International Monetary Fund. Washington, v. 55, n. 4, p. 44-45, Dec. 2018.

WEINSTEIN, J.; COHN, A.; PARKER, C. Promoting innovation through education: The blockchain industry, law enforcement and regulators work towards a common goal. In: DEWEY, J. (Contributing Editor). **GLI, Global Legal Insights** – Blockchain & Cryptocurrency Regulation 2019, First Edition. London: Global Legal Group, 2019. p. 1-4.

WRONKA, C. Money laundering through cryptocurrencies – analysis of the phenomenon and appropriate prevention measures. **Journal of Money Laundering Control**, Leeds, v. 25, n.1, p. 79-94, 2022.

ZAVOLI, I. The use of cryptocurrencies in the UK real estate market: an assessment of money laundering risks. In: BENSON, K.; KING, C.; WALKER, C. (Editors). **Assets, Crimes and the State**: Innovation in 21st Century Legal Responses. Routledge, 2020.

ZHANG, A. R.; RAVEENTHIRAN, A.; MUKAI, J.; NAEEM, R.; DHUNA, A.; PARVEEN, Z.; KIM, H. The Regulation Paradox of Initial Coin Offerings: A Case Study Approach. **Frontiers in Blockchain**, [Lausanne], v. 2, n. 2, p. 1-10, Apr. 2019.

ZOLKAFLIL, S.; OMAR, N.; SYED MUSTAPHA NAZRI, S. N. F. Implementation evaluation: a future direction in money laundering investigation. **Journal of Money Laundering Control**, Leeds, v. 22, n. 2, p. 318-326, 2019.

APÊNDICE A – QUESTIONÁRIO

Prezado (a)

Como aluno mestrando junto ao Programa de Pós-Graduação em Ciências Contábeis – PPGCC da Universidade Federal do Rio de Janeiro – UFRJ estou conduzindo uma pesquisa como parte dos requisitos necessários para obtenção do título de Mestre em Ciências Contábeis. O objetivo da pesquisa é identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro, e você está sendo convidado (a) a participar desse estudo por meio de aplicação desse questionário.

É necessário que o participante tenha experiência na Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo (PLD-FT) e experiência com criptoativos. É desejável, mas não obrigatório, que o participante tenha formação acadêmica em Ciências Contábeis.

Esse questionário não é um teste de conhecimento, mas o objetivo de sua aplicação é verificar a percepção dos profissionais que atuam na área de PLD-FT acerca da utilização dos criptoativos no crime de lavagem de dinheiro, os riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos e as possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos. Assim, não há respostas certas ou erradas, mas somente respostas com base na percepção individual do participante.

Os registros deste estudo serão mantidos em sigilo. Os relatórios publicados não incluirão nenhuma informação que permita identificar o participante. Os registros da pesquisa serão armazenados de forma segura, e apenas o pesquisador terá acesso aos registros. As respostas dos participantes serão mantidas em sigilo por meio do uso de pseudônimos/códigos.

A participação é voluntária, porém muito importante para o andamento da pesquisa. Um documento de consentimento “Registro de Consentimento Livre e Esclarecido”, que contém informações adicionais sobre a pesquisa, está anexado. Se você decidir participar da pesquisa, deverá, após a leitura completa do Registro de Consentimento Livre e Esclarecido, assinar e datar o Registro de Consentimento Livre e Esclarecido e devolvê-lo por e-mail.

Atenciosamente,

Jaime Wagner Rodrigues Barbosa
Mestrando PPGCC-UFRJ
Matrícula nº 119084606

QUESTIONÁRIO – A PERCEPÇÃO DOS PROFISSIONAIS ACERCA DA UTILIZAÇÃO DOS CRIPTOATIVOS NO CRIME DE LAVAGEM DE DINHEIRO

O objetivo desse questionário é verificar a percepção dos profissionais que atuam na área de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT) acerca da utilização dos criptoativos no crime de lavagem de dinheiro.

PARTE 1 – PERFIL DOS RESPONDENTES

A seguir estão listadas perguntas fechadas de múltipla escolha de resposta única. Assinale a melhor opção, de acordo com a sua experiência acadêmica/profissional.

1. Formação acadêmica:

( ) Administração.
( ) Ciências Contábeis.
( ) Ciências Econômicas.
( ) Direito.
( ) Outra (especifique):
_____

2. Familiaridade com as regras e regulamentos domésticos de *anti-money laundering* (AML)[1]:

( ) Pouco conhecimento.
( ) Regular conhecimento.
( ) Bom conhecimento.
( ) Muito bom conhecimento.
( ) Excelente conhecimento.

3. Familiaridade com as recomendações do Grupo de Ação Financeira Internacional (GAFI):

( ) Pouco conhecimento.
( ) Regular conhecimento.
( ) Bom conhecimento.
( ) Muito bom conhecimento.
( ) Excelente conhecimento.

4. Experiência na prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT):

( ) Até 1 ano.
( ) De 1 até 5 anos.
( ) De 5 até 10 anos.
( ) Mais de 10 anos.

5. Familiaridade com criptoativos:

( ) Pouco conhecimento.
( ) Regular conhecimento.
( ) Bom conhecimento.
( ) Muito bom conhecimento.

[1] Na tradução livre, *anti-money laundering* (AML) corresponde a antilavagem de dinheiro (ALD) em português.

( ) Excelente conhecimento.

6. Experiência com criptoativos:[2]

( ) Até 1 ano.
( ) De 1 até 5 anos.
( ) De 5 até 10 anos.
( ) Mais de 10 anos.

7. Em qual segmento do setor de serviços ou órgão da Administração Pública se concentra sua experiência de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT) e criptoativos?

( ) Escritório de advocacia.
( ) Escritório de contabilidade.
( ) *Exchanger* de criptoativos.
( ) Instituição financeira.
( ) Instituição de pesquisa.
( ) Outro (especifique):

_____

8. Qual a área de atividade conforme a resposta da pergunta anterior se concentra sua experiência de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD-FT) e criptoativos?

( ) Auditoria.
( ) Área de prevenção à lavagem de dinheiro e financiamento do terrorismo (PLD-FT).
( ) *Compliance*.
( ) Controles internos.
( ) Gerenciamento de riscos.
( ) Outra (especifique):

_____

PARTE 2 - RISCOS E DESAFIOS DE CRIME DE LAVAGEM DE DINHEIRO ENFRENTADOS AO LIDAR COM CRIPTOATIVOS

A seguir estão listadas perguntas fechadas em nível de matriz com resposta única para cada item e perguntas fechadas de múltipla escolha de resposta única. Assinale a melhor opção, de acordo com a sua experiência acadêmica/profissional. Todas as perguntas contam com abertura para comentários.

9. Em que medida as seguintes vulnerabilidades associadas às práticas e serviços oferecidos são exploradas nos crimes de lavagem de dinheiro com criptomoedas?

[2] Esta pergunta leva em consideração que já se passaram mais de 10 anos desde o surgimento do *Bitcoin* em 2008.

	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
9.1 Assessoria/consultoria financeira e tributária.						
9.2 Formação de empresas e *trustes*.						
9.3 Compra/venda de imóveis e estabelecimentos comerciais/industriais.						
9.4 Gestão de fundos, valores mobiliários e outros ativos.						
9.5 Prestação de serviços não presenciais (internet, correio, telefone).						
9.6 Transferência eletrônica de fundos e valores mobiliários.						
9.7 Realização de apresentações para instituições financeiras, com profissionais específicos como intermediários.						
9.8 Prestação de serviços a clientes residentes no exterior.						
9.9 Privilégio profissional legal e confidencialidade do cliente.						
9.10 Obrigações *anti-money laundering* (AML) limitadas para Atividades e Profissões Não-Financeiras Designadas (APNFDs).						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

10. Qual a relevância dos seguintes fatores de risco de lavagem de dinheiro ao lidar com criptomoedas?

	Sem importância	Pouco Importante	Razoavelmente importante	Importante	Muito importante	Não saberia optar
10.1 Clientes cuja origem/localização atual da fonte de suas riquezas/fundos está associada a um país de maior risco.						
10.2 Clientes que conduzem seu relacionamento comercial em circunstâncias incomuns/não convencionais.						

10.3 Transferências de bens que são inerentemente difíceis de avaliar, como ativos virtuais, onde isso não é comum para o tipo de clientes.						
10.4 Clientes residentes em um país/região geográfica de alto risco.						
10.5 Clientes em que o relacionamento dificulta a identificação oportuna do verdadeiro beneficiário final.						
10.6 Serviços em relação a ofertas iniciais de moedas (*Initial Coin Offering* – ICO).						
10.7 Cliente com beneficiário final residente em um país/região geográfica de alto risco.						
10.8 Clientes com negócios intensivos em dinheiro/equivalente, como corretores e outros prestadores de serviços em ativos virtuais.						
10.9 Uso de ativos virtuais em transações sem aparente motivo legal, tributário, comercial e econômico.						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

11. Em que medida os seguintes *red flag indicators*[3] sobre lavagem de dinheiro com criptomoedas ocorrem?

	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
11.1 Os fundos do cliente são originados/enviados para uma *exchanger* que não está registrada na mesma jurisdição do cliente.						
11.2 Cliente fornece identificação/conta (um endereço *Internet Protocol* – IP não padrão) compartilhadas por outra conta.						
11.3 Transferência em quantias abaixo dos limites de manutenção de registros/relatórios.						
11.4 O cliente utiliza *exchanger* localizada em jurisdição de alto risco com regulamentos *anti-money laundering* (AML) inadequados.						
11.5 Cliente com endereço IP associado a seu perfil diferente do endereço IP pelo qual as transações estão sendo iniciadas.						

[3] Na tradução livre, *red flag indicators* corresponde a indicadores de bandeira vermelha em português.

11.6 Realização de várias transações de alto valor com padrão escalonado e regular.						
11.7 O cliente utiliza provedor de serviços de ativos virtuais (PSAV) que opera em jurisdição sem regulamentação para ativos virtuais.						
11.8 Clientes que utilizam vários cartões de crédito/débito vinculados a uma carteira de criptomoedas.						
11.9 Transação anormal (nível e volume) de criptomoedas em *exchangers* de carteiras associadas à plataforma *peer-to-peer* (P2P)[4].						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

12. Em que medida os seguintes *red flag indicators* associados ao anonimato são mais explorados ao lidar com criptomoedas?

	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
12.1 Transações envolvendo mais de um tipo de criptomoeda, incluindo as que fornecem maior anonimato.						
12.2 Mover criptomoeda de *blockchain* pública e transparente para uma *exchanger* centralizada e logo trocá-la para criptomoeda de anonimato.						
12.3 Operações realizadas em *sites* de troca *peer-to-peer* (P2P).						
12.4 Transações com serviços de *mixing cryptocurrency*, sugerindo a intenção de ocultar o fluxo de fundos ilícitos entre mercados *darknet*.						
12.5 Fundos movimentados em carteira com *links* de exposição direta e indireta para fontes suspeitas conhecidas, incluindo mercados *darknet*.						
12.6 O uso de carteiras de *hardware* descentralizadas/não hospedadas para transportar ativos virtuais além das fronteiras.						
12.7 Usuários de provedores de serviços de ativos virtuais (PSAV) registrando seus nomes de domínio da Internet por meio de *proxies*.						
12.8 Usuários de PSAV usando um endereço *Internet Protocol* (IP) associado a *darknet.*						

[4] Na tradução livre, *peer-to-peer* corresponde a ponto-a-ponto em português.

12.9 Grande número de carteiras de ativos virtuais aparentemente não relacionadas, controladas a partir do mesmo endereço IP.						
12.10 Transações utilizando meios de comunicação criptografados anônimos, como fóruns, *chats*, aplicativos móveis e jogos *online*.						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

13. Em que medida as seguintes atividades apresentam um desafio para a aplicação das medidas de *customer due diligence*[5] ao lidar com criptomoedas?

	Nunca	Raramente	Ocasionalmente	Frequentemente	Muito frequente	Não saberia optar
13.1 Compra/venda de imóvel e estabelecimento comercial/industrial.						
13.2 Gestão de fundos, valores mobiliários e outros ativos do cliente.						
13.3 Gestão de contas bancárias, de poupança e investimentos.						
13.4 Organização de contribuições para a criação/operação de empresas.						
13.5 Gestão de entidades empresariais.						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

14. Caso considere que a regulamentação seja um dos desafios ao lidar com as criptomoedas, qual das opções lhe parece mais apropriada?

( ) Permanecer sem regulamentação específica.
( ) Aplicar a regulamentação relacionada aos produtos existentes.
( ) Criar uma regulamentação específica.

[5] Na tradução livre, *customer due diligence* corresponde a devida diligência acerca do cliente em português.

( ) Não saberia optar.

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

PARTE 3 – POSSÍVEIS ABORDAGENS QUE AJUDARIAM A MINIMIZAR OS RISCOS E DESAFIOS ENFRENTADOS AO LIDAR COM CRIPTOATIVOS

A seguir estão listadas perguntas fechadas em nível de matriz com resposta única para cada item. Assinale a melhor opção, de acordo com a sua experiência acadêmica/profissional. Todas as perguntas contam com abertura para comentários.

15. Qual a relevância das seguintes fontes de informação sobre avaliação de risco de lavagem de dinheiro ao lidar com criptomoedas?

	Sem importância	Pouco Importante	Razoavelmente importante	Importante	Muito importante	Não saberia optar
15.1 Avaliação nacional de riscos (ANR).						
15.2 Avaliações de risco supranacionais.						
15.3 Relatórios setoriais das autoridades competentes sobre os riscos de lavagem de dinheiro inerentes ao serviço/setor do profissional.						
15.4 Relatórios de risco de outras jurisdições onde o profissional está localizado.						
15.5 Informações públicas amplamente disponíveis que destaquem questões que podem ter surgido em jurisdições específicas.						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

16. Qual a relevância dos seguintes fatores e medidas para gerenciar e mitigar efetivamente os riscos de lavagem de dinheiro ao lidar criptomoedas?

	Sem importância	Pouco Importante	Razoavelmente importante	Importante	Muito importante	Não saberia optar
16.1 Participação de instituições financeiras devidamente reguladas.						
16.2 Localização de profissionais e clientes em países semelhantes.						
16.3 Supervisão de um regulador.						
16.4 Regularidade/duração do relacionamento com o cliente.						
16.5 Envolvimento de organizações privadas, transparentes e conhecidas no domínio público.						
16.6 Familiaridade do profissional com um país específico, incluindo conhecimento e conformidade com as leis e regulamentos locais.						
16.7 Treinamento geral sobre métodos de lavagem de dinheiro e riscos para os profissionais.						
16.8 Treinamento específico para conscientização dos profissionais que fornecem atividades especificas para clientes de maior risco.						
16.9 Revisão periódica dos serviços oferecidos e avaliação periódica da estrutura *anti-money laundering* (AML) aplicável ao profissional.						
16.10 Revisão periódica dos relacionamentos com os clientes para determinar se o risco de lavagem de dinheiro aumentou.						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

17. Em que medida os seguintes procedimentos de *customer due diligence* apresentam eficácia ao lidar com criptomoedas?

	Sem eficácia	Pouco eficaz	Razoavelmente eficaz	Eficaz	Muito eficaz	Não saberia optar
17.1 Identificar o cliente e verificar a identidade desse cliente usando documentos, dados e informações confiáveis.						
17.2 Identificar o beneficiário final e tomar medidas razoáveis com base em riscos para verificar sua identidade.						

17.3 Compreender e obter informações sobre o objetivo e a natureza pretendida do relacionamento comercial.						
17.4 Conduzir a *due diligence* contínua sobre o relacionamento comercial.						
17.5 Obter informações sobre a fonte de recursos/riqueza do cliente e evidenciá-las claramente através da documentação apropriada obtida.						
17.6 Atualizar regularmente os dados de identificação do cliente e do beneficiário final.						
17.7 Realizar pesquisas adicionais para melhor informar o perfil de risco do cliente.						
17.8 Obter a aprovação da alta administração para iniciar/continuar o relacionamento comercial.						
17.9 Aumento do número e tempo dos controles, com seleção de padrões de transações que precisam de exame mais aprofundado.						
17.10 Maior conscientização sobre clientes e transações de maior risco, em todos os departamentos envolvidos no relacionamento comercial.						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

18. Em que medida as políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de lavagem de dinheiro, apresentam eficácia ao lidar com criptomoedas?

	Sem eficácia	Pouco eficaz	Razoavelmente eficaz	Eficaz	Muito eficaz	Não saberia optar
18.1 Realizar revisão regular das políticas e procedimentos da organização para garantir sua permanente adequação ao objetivo.						
18.2 Realizar revisão regular de conformidade a fim de verificar a implementação correta das políticas e procedimentos da organização.						
18.3 Fornecer à alta administração relatório regular de iniciativas de conformidade e relatório de transação suspeita arquivados.						
18.4 Atender os requisitos de manutenção de registros/relatórios e as recomendações para conformidade de *anti-money laundering* (AML).						
18.5 Possibilitar a identificação oportuna de transações reportáveis, com a garantia do preenchimento preciso dos relatórios necessários.						

18.6 Ter sistema de gerenciamento de risco capaz de determinar se um cliente/beneficiário final é uma pessoa exposta politicamente.						
18.7 Providenciar controles adequados para clientes e serviços de maior risco, conforme necessário.						
18.8 Maior atenção nas operações da organização que são mais vulneráveis ao abuso por lavagem de dinheiro.						
18.9 Revisão periódica dos processos de avaliação e gerenciamento de riscos, considerando o ambiente/serviço de operação da organização.						
18.10 Prever a função de conformidade AML e programa de revisão conforme a escala da organização e a natureza da prática profissional.						

Espaço aberto para comentários referentes à pergunta:

_____

_____

_____

IMPORTANTE

Por favor, verifique todas as respostas às perguntas do questionário, para confirmação de que não há opções em branco.

APÊNDICE B – REGISTRO DE CONSENTIMENTO LIVRE E ESCLARECIDO (RCLE)

REGISTRO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Informações aos participantes

1) Título do protocolo do estudo:

PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: UMA ABORDAGEM BASEADA EM RISCO PARA A PROFISSÃO CONTÁBIL

2) Convite

Você está sendo convidado(a) a participar da pesquisa PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: UMA ABORDAGEM BASEADA EM RISCO PARA A PROFISSÃO CONTÁBIL. Antes de decidir se participará, é importante que você entenda por que o estudo está sendo feito e o que ele envolverá. Reserve um tempo para ler cuidadosamente as informações a seguir e faça perguntas se algo não estiver claro ou se quiser mais informações. Não tenha pressa de decidir se deseja ou não participar desta pesquisa.

3) O que é o projeto?

O projeto consiste em uma pesquisa de dissertação para a obtenção do título de mestre.

4) Qual é o objetivo do estudo?

O projeto visa identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro.

5) Por que eu fui escolhido(a)?

Os participantes da pesquisa serão profissionais que atuam no setor de serviços ou órgão da Administração Pública, sendo desejável, mas não obrigatório, que possuam formação acadêmica em Ciências Contábeis. É necessário que os participantes tenham experiência na Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo (PLD-FT) e experiência com criptoativos.

Ressaltamos que a participação é voluntária, conforme seu desejo e autorização.

6) Eu tenho que participar?

Você é quem decide se gostaria de participar ou não desta pesquisa. Se decidir participar da pesquisa PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: UMA ABORDAGEM BASEADA EM RISCO PARA A PROFISSÃO CONTÁBIL você deverá assinar este Registro e receberá uma via assinada pelo pesquisador, a qual deverá guardar. Mesmo se você decidir participar, você ainda tem a

liberdade de se retirar das atividades a qualquer momento, sem qualquer justificativa. Isso não afetará em nada sua participação em demais atividades e não causará nenhum prejuízo.

7) O que acontecerá comigo se eu participar? O que eu tenho que fazer?

Os voluntários responderão um questionário sobre o tema em estudo, ou seja, a utilização dos criptoativos no crime de lavagem de dinheiro.

8) O que é exigido de mim nesse estudo além da prática de rotina?

Apenas relatar sobre sua percepção em relação às questões acerca da utilização dos criptoativos no crime de lavagem de dinheiro, dos riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos e das possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos.

As percepções serão divulgadas, porém o nome dos participantes será mantido em sigilo.

9) Eu terei alguma despesa ao participar da pesquisa?

Não.

10) Quais são os eventuais riscos ao participar do estudo?

De acordo com as Resoluções 466 e 510 do Conselho Nacional de Saúde, todas as pesquisas envolvem riscos, ainda que mínimos. O voluntário durante a pesquisa poderá se sentir desconfortável, intimidado ou receoso de que o sigilo seja quebrado. Também poderá sentir desconforto ou algum tipo de constrangimento em relação às questões. Dessa forma, os registros deste estudo serão mantidos em sigilo. Os relatórios publicados não incluirão nenhuma informação que permita identificar o participante. Os registros da pesquisa serão armazenados de forma segura, e apenas o pesquisador terá acesso aos registros. As respostas dos participantes serão mantidas em sigilo por meio do uso de pseudônimos/códigos. O voluntário poderá parar de responder ao questionário a qualquer momento, bem como desistir de participar.

11) Quais são os possíveis benefícios de participar?

Ao participar da pesquisa você contribuirá para o alcance do objetivo desse projeto que é identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro. Sua participação na pesquisa é essencial para alcançar esse objetivo e contribuir para a academia de Ciências Contábeis e a sociedade em geral.

12) O que acontece quando o estudo termina?

Ao fim da pesquisa, após defesa e aprovação pela banca examinadora, o material será disponibilizado para a Biblioteca da Faculdade de Administração e Ciências Contábeis da Universidade Federal do Rio de Janeiro e estará disponível no sítio do Programa de Pós-Graduação em Ciências Contábeis – PPGCC da Universidade Federal do Rio de Janeiro – UFRJ - http://ppgcc.ufrj.br/ para futuras consultas e pesquisas. Se for de seu interesse também poderá ser enviado por e-mail assim que concluída e defendida a pesquisa.

13) E se algo der errado?

Ao decidir participar, você ainda tem a liberdade de retirar seu consentimento em qualquer fase da pesquisa ou mesmo se retirar dela quando desejar, sem qualquer prejuízo ou justificativa.

14) Minha participação neste estudo será mantida em sigilo?

Sim, sua participação será mantida em sigilo.

15) Contato para informações adicionais

Dados do pesquisador responsável: Jaime Wagner Rodrigues Barbosa – Mestrando PPGCC/UFRJ – Matrícula nº 119084606, Av. Pasteur, nº 250 – sala 250 – Urca, Rio de Janeiro – Telefone (21) 97696-0358 – E-mail: jaimewrodrigues@yahoo.com.br

Dados da Instituição Proponente: Faculdade de Administração e Ciências Contábeis – FACC da Universidade Federal do Rio de Janeiro – UFRJ, Av. Pasteur, nº 250 – Urca, Rio de Janeiro – Telefone (21) 3938-5106

Dados do CEP: Comitê de Ética em Pesquisa do CFCH – Campus da UFRJ da Praia Vermelha – Prédio da Decania do CFCH, 3º andar, Sala 30 – Telefone: (21) 3938-5167 – E-mail: cep.cfch@gmail.com

O Comitê de Ética em Pesquisa é um colegiado responsável pelo acompanhamento das ações deste projeto em relação a sua participação, a fim de proteger os direitos dos participantes desta pesquisa e prevenir eventuais riscos.

16) Remunerações financeiras

Nenhum incentivo ou recompensa financeira está previsto pela sua participação nesta pesquisa.

Obrigado por ler estas informações. Se deseja participar deste estudo, assine este Registro de Consentimento Livre e Esclarecido e devolva-o ao pesquisador. Você deve guardar uma via deste documento para sua própria garantia.

1 – Confirmo que li e entendi as informações sobre o estudo acima e que tive a oportunidade de fazer perguntas.

2 – Entendo que minha participação é voluntária e que sou livre para retirar meu consentimento a qualquer momento, sem precisar dar explicações, e sem sofrer prejuízo ou ter meus direitos afetados.

3 – Concordo em participar da pesquisa acima.

Nome do participante: _____

Assinatura do participante: _____

Data: _____/_____/_____

OBS: Duas vias devem ser feitas, uma para o usuário e outra para o pesquisador.

APÊNDICE C – MENSAGNES ENVIADAS AOS POSSÍVEIS PARTICIPANTES DA PESQUISA

- Mensagens enviadas na terceira etapa de contatos para seleção de possíveis participantes da pesquisa:

A seguinte mensagem de apresentação foi incluída na solicitação de conexão:

> Como aluno mestrando do Programa de Pós-Graduação em Ciências Contábeis – PPGCC da UFRJ, estou conduzindo uma pesquisa de dissertação cujo objetivo é identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção de crimes relacionados ao uso dos criptoativos na LDFT.

Quando aceita a solicitação, era encaminhada uma nova mensagem onde era feito o pedido de cooperação:

> Prezado (a),
> Obrigado por aceitar meu convite.
> Conforme anteriormente informado, como aluno mestrando junto ao Programa de Pós-Graduação em Ciências Contábeis – PPGCC da Universidade Federal do Rio de Janeiro – UFRJ, estou conduzindo uma pesquisa como parte dos requisitos necessários para obtenção do título de Mestre em Ciências Contábeis. O objetivo da pesquisa é identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro, e estou escrevendo para solicitar cooperação na participação ou indicação de possíveis participantes qualificados para o estudo por meio de aplicação de questionário ou entrevista.
> É necessário que o participante tenha experiência na Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo (PLD-FT) e experiência com criptoativos. É desejável, mas não obrigatório, que o participante tenha formação acadêmica em Ciências Contábeis.
> O objetivo da aplicação de questionário ou entrevista é verificar a percepção dos profissionais que atuam na área de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLDFT) acerca da utilização dos criptoativos no crime de lavagem de dinheiro. Os riscos e desafios de crime de lavagem de dinheiro enfrentados ao lidar com criptoativos. As possíveis abordagens que ajudariam a minimizar os riscos e desafios enfrentados ao lidar com criptoativos.
> Atenciosamente,
> Jaime Wagner Rodrigues Barbosa
> Mestrando PPGCC/FACC-UFRJ
> Matrícula nº 119084606

- Mensagens enviadas na primeira da aplicação dos questionários.

Nos *e-mails* enviados a partir do dia 15/12/2021 constava a seguinte mensagem:

> Bom dia (Boa tarde ou noite) ...
> Conforme solicitação de *e-mail* para encaminharmos, quando aprovados pelo Comitê de Ética em Pesquisa (CEP) da UFRJ, a Carta Convite juntamente com o Questionário e o REGISTRO DE CONSENTIMENTO LIVRE E ESCLARECIDO (RCLE), informamos que o Projeto de Pesquisa com Certificado de Apresentação para

> Apreciação Ética (CAAE) sob o nº 52267921.3.0000.5582, foi aprovado através do Parecer de nº 5.157.673 de 9/12/2021.
> Nesse sentido, informamos que a Carta Convite juntamente com o Questionário e o REGISTRO DE CONSENTIMENTO LIVRE E ESCLARECIDO (RCLE), aprovados pelo CEP, seguem anexos.
> Sua participação é muito importante para nós!
> Desde já, o nosso agradecimento!
> Atenciosamente,
> Jaime Wagner Rodrigues Barbosa
> Mestrando PPGCC/FACC-UFRJ
> Matrícula nº 119084606

Simultaneamente ao envio dos questionários por *e-mail* foram encaminhadas mensagens aos possíveis participantes na plataforma *LinkedIn*, com o seguinte comunicado:

> Bom dia (Boa tarde ou noite) ...
> O Projeto de Pesquisa foi aprovado pelo Comitê de Ética em Pesquisa (CEP) da UFRJ.
> Nesse sentido, informo que a Carta Convite juntamente com o Questionário e o REGISTRO DE CONSENTIMENTO LIVRE E ESCLARECIDO (RCLE), aprovados pelo CEP, foram encaminhados para o e-mail ...
> Atenciosamente,
> Jaime Wagner Rodrigues Barbosa
> Mestrando PPGCC/FACC-UFRJ
> Matrícula nº 119084606

A partir do dia 18/01/2022 foram encaminhados 132 *e-mails* que já haviam sidos enviados aos possíveis participantes da pesquisa, juntamente com a seguinte mensagem na plataforma *LinkedIn*:

> Bom dia (Boa tarde ou noite) ...
> Estamos realizando uma nova rodada de contato com nossos possíveis participantes na pesquisa.
> Nesse sentido, informamos que a Carta Convite juntamente com o Questionário e o REGISTRO DE CONSENTIMENTO LIVRE E ESCLARECIDO (RCLE), aprovados pelo Comitê de Ética em Pesquisa (CEP) da UFRJ, foram encaminhados para o e-mail ...
> Sua participação é muito importante para o desenvolvimento do estudo sobre o uso dos criptoativos no crime de lavagem de dinheiro.
> Precisamos da sua cooperação para concluirmos essa etapa da pesquisa.
> Desde já, o nosso agradecimento!
> Atenciosamente,
> Jaime Wagner Rodrigues Barbosa
> Mestrando PPGCC/FACC-UFRJ
> Matrícula nº 119084606

A partir do dia 15/02/2022 foram encaminhados 115 *e-mails* que já haviam sidos enviados e encaminhados aos possíveis participantes da pesquisa, juntamente com a seguinte mensagem na plataforma *LinkedIn*:

> Bom dia (Boa tarde ou noite) ...
> Estamos realizando a última rodada de contato com nossos possíveis participantes na pesquisa.
> Nesse sentido, informamos que a Carta Convite juntamente com o Questionário e o REGISTRO DE CONSENTIMENTO LIVRE E ESCLARECIDO (RCLE), aprovados pelo Comitê de Ética em Pesquisa (CEP) da UFRJ, foram encaminhados para o e-mail ...
> Sua participação é muito importante para o desenvolvimento do estudo sobre o uso dos criptoativos no crime de lavagem de dinheiro.
> Desde já, o nosso agradecimento!
> Atenciosamente,
> Jaime Wagner Rodrigues Barbosa
> Mestrando PPGCC/FACC-UFRJ
> Matrícula nº 119084606

A partir do dia 18/03/2022 foram encaminhados 103 *e-mails* que já haviam sidos enviados e encaminhados aos possíveis participantes da pesquisa, juntamente com a seguinte mensagem na plataforma *LinkedIn*:

> Bom dia (Boa tarde ou noite) ...
> Entendendo a oportunidade que a pesquisa está tendo mediante contato com profissionais que podem contribuir de forma significativa para o desenvolvimento do estudo sobre o uso dos criptoativos no crime de lavagem de dinheiro, estamos realizando uma nova rodada de contato com nossos possíveis participantes na pesquisa.
> Nesse sentido, informamos que a Carta Convite juntamente com o Questionário e o Registro de Consentimento Livre e Esclarecido (RCLE), aprovados pelo Comitê de Ética em Pesquisa (CEP) da UFRJ, foram encaminhados para o e-mail ...
> Desde já, o nosso agradecimento!
> Atenciosamente,
> Jaime Wagner Rodrigues Barbosa
> Mestrando PPGCC/FACC-UFRJ
> Matrícula nº 119084606

APÊNDICE D – DESCRIÇÃO DAS CATEGORIAS DE ANÁLISE

1. Vulnerabilidades associadas às práticas e serviços oferecidos

O setor contábil é uma grande indústria que oferece serviços e assessoria a uma variedade de clientes, onde, dentre uma gama de serviços oferecidos, os serviços de auditoria, tributação e consultoria representam a grande maioria dos negócios (FATF, 2018b, p. 52).

Os profissionais da contabilidade, como atividades e profissões não financeiras designadas (APNFDs), são atores-chave no desenvolvimento financeiro e econômico, sendo, por consequência, altamente vulneráveis aos riscos de LD/FT (NDUKA; SECHAP, 2021).

As vulnerabilidades associadas às práticas e serviços oferecidos podem sujeitar os profissionais da contabilidade à exploração por parte de clientes que procuram fazer uso indevido de serviços legítimos para fins de LD, que apresenta aos profissionais da contabilidade três riscos principais (IFAC, 2020b): (i) **Risco de ser usado para LD**: Quando o profissional da contabilidade, que tem conhecimento real da criminalidade em que está envolvido, mantém os produtos do crime em uma conta bancária ou participa de um acordo que disfarce a propriedade efetiva dos produtos do crime; (ii) **Risco de ser usado para facilitar a LD por outra pessoa**: Quando o profissional da contabilidade, que tem conhecimento real da criminalidade em que está envolvido, cria um veículo corporativo a ser usado para LD ou apresenta um lavador de dinheiro a outro consultor profissional; e (iii) **Risco de sofrer danos legais, regulatórios ou de reputação por não ter identificado os sinais de alerta de LD e relatado**: Quando o profissional da contabilidade é inconsciente ou negligente sobre um cliente (ou um ou seus associados) estar envolvido em esquemas de LD.

As organizações contábeis podem manter e operar contas fiduciária para facilitar transações financeiras em nome de clientes, como transferência eletrônica de fundos e valores mobiliários, ou manter fundos em custódia, para gestão de fundos, valores mobiliários e outros ativos (FATF, 2018b, p. 63). Como provedor de serviços de ativos virtuais (PSAV), a organização contábil pode manter a custódia ou controle sobre ativos virtuais (AVs), carteiras e/ou chaves privadas de outra pessoa física ou jurídica, tornando-se significativamente envolvida nas transações realizadas com criptomoedas sob sua custódia ou controle. As criptomoedas permitem que os usuários, indivíduos e organizações, negociem diretamente entre si, transferindo valores diretamente uns aos outros, sem a presença de um terceiro como intermediário, contudo, no contexto de uma organização contábil com modelo de negócio que a caracterize como um PSAVs, transferência de AVs significa realizar uma transação em nome de outra pessoa física ou jurídica que mova uma criptomoeda de um endereço ou conta de

criptomoeda para outro endereço ou conta de criptomoeda (FATF, 2019b; OECD, 2019). Transferência envolvendo criptomoedas em quantias abaixo dos limites de manutenção de registros/relatórios pode ocorrer em uma das etapas de LD, por meio da "microlavagem", onde grandes quantias de criptomoedas podem ser divididas em quantias menores e menos visíveis armazenadas em muitas carteiras de custódia, ou trocadas por moedas fiduciárias e posteriormente depositadas em contas bancárias regulares (ICAEW, 2019; KATARZYNA, 2019). Segundo o GAFI, custódia e/ou administração de AVs ou instrumentos que permitem o controle sobre AVs, devem ser considerados como:

> ...serviços ou modelos de negócios que combinem a função de salvaguardar o valor dos AVs de um cliente com o poder de gerir ou transmitir os AVs independentemente do titular, no pressuposto de que tal gestão e transmissão apenas serão feitos de acordo com as instruções do titular/cliente. Os serviços de custódia e administração incluem pessoas que têm controle exclusivo ou independente da chave privada associada a AVs pertencentes a outra pessoa ou controle exclusivo e independente de contratos inteligentes dos quais não são parte que envolvam AVs pertencentes a outra pessoa (FATF, 2019b, p. 16, tradução nossa).[1]

Uma vez que não é possível mover fisicamente as unidades de criptomoedas de sua *blockchain* relevante e armazená-las em outro lugar, devido à ausência de manifestação física das criptomoedas, elas existem exclusivamente como entradas na *blockchain*, onde a propriedade e transferência geralmente são registradas. Uma *blockchain* normalmente opera por meio do uso de chaves públicas e chaves privadas[2], que, estando em posse de um indivíduo ou organização, essas chaves criptográficas permitem o controle sobre as criptomoedas. Nesse sentido, o controle da chave privada pode permitir a custódia de uma criptomoeda por parte de um indivíduo ou organização, que desejando realizar a transferência dessa criptomoeda, precisará inserir a chave privada correspondente a chave pública que a *blockchain* mostra como proprietária da criptomoeda (BLANDIN *et al.*, 2019; KRIMMINGER; LLOYD; ROCKS, 2019; ROWLAND; KIVIAT, 2019).

---

[1] "…services or business models that combine the function of safeguarding the value of a customer's VAs with the power to manage or transmit the VAs independently from the owner, under the assumption that such management and transmission will only be done according to the owner's/customer's instructions. Safekeeping and administration services include persons that have exclusive or independent control of the private key associated with VAs belonging to another person or exclusive and independent control of smart contracts to which they are not a party that involve VAs belonging to another person."

[2] A criptografia de chave pública é um sistema de autenticação e criptografia assimétrica que usa um par de chaves matematicamente relacionadas (pública e privada). A chave pública, que pode ser amplamente compartilhada, é usada para criptografar uma mensagem antes de enviá-la, e somente a chave privada correspondente, que deve ser mantida em segredo, pode posteriormente descriptografar a mensagem criptografada com a chave pública. A chave privada pode ser comparada a uma senha que desbloqueia a conta de usuário, enquanto a chave pública associada se assemelha a um número de conta de usuário.

A prestação de serviços virtuais, como a gestão de carteiras de criptomoedas, com transações e investimentos envolvendo criptomoedas, e a capacidade de movimentar valores virtualmente na ausência de contato direto e pessoal com provedor de serviços profissionais ou IFs, provavelmente acarretará numa dificuldade de identificar a fonte e o destino dos valores sob a gestão das organizações contábeis, podendo aumentar o risco dessas organizações contábeis de facilitarem atividades ilícitas, tornando assim, as práticas e serviços envolvendo criptomoedas comumente vulneráveis de serem exploradas por criminosos para LD/FT.

Nesse contexto, os comentários dos respondentes foram associados a temas correspondentes aos principais riscos apresentados pela LD aos profissionais da contabilidade ao lidar com criptomoedas, como: (i) Risco de ser usado para LD; (ii) Risco de ser usado para facilitar a LD por outra pessoa; e (iii) Risco de sofrer danos legais, regulatórios ou de reputação por não ter identificado os sinais de alerta de LD e relatado.

2. Fatores de risco de LD

A avaliação de risco de LD/FT, como ponto de partida para aplicação da ABR, deve ser realizada pelo profissional da contabilidade proporcionalmente ao seu modelo de negócio, examinando os fatores de risco nas seguintes categorias de risco: (i) Risco país/geográfico; (ii) Risco de cliente; e (iii) Risco de transação/serviços e canal de entrega associado (FATF, 2019a, p. 5). Os esclarecimentos a respeito de cada categoria de risco foram divulgados na seção 2.6.1 – Abordagem Baseada em risco (ABR) e o Contador, da presente pesquisa.

No ecossistema das criptomoedas essas categorias de risco podem ser examinadas partindo dos seguintes fatores de risco: (i) **Risco país/geográfico**: Risco associado às jurisdições de origem, destino e trânsito de uma transação, enfatizando o alcance global e a velocidade de transação que as criptomoedas fornecem, assim como a regulamentação ou supervisão inadequadas das atividades e provedores financeiros de criptomoedas em diferentes jurisdições, que possibilitam as criptomoedas de serem usadas para transferir fundos globalmente ou em uma ampla área geográfica com um grande número de contrapartes, tornando-as mais atraentes para criminosos para fins de LD/FT (FATF, 2019b, p. 12); (ii) **Risco de cliente**: Risco associado à identificação do cliente/beneficiário, ao entendimento da fonte de fundos/riquezas do cliente e ao objetivo da transação, enfatizando a necessidade de um monitoramento e exames adicionais, com o objetivo de alcançar uma justificativa para o negócio ou fins econômicos da transação envolvendo criptomoedas, uma vez que esses fatores de risco podem apresentar riscos mais elevados de LD/FT (FATF, 2019a, p. 28); e (iii) **Risco**

de transação/serviços e canal de entrega associado: Risco associado aos produtos ou serviços envolvendo criptomoedas que, ao facilitarem transações com pseudônimo ou com anonimato, podem dificultar a capacidade de rastrear os fundos associados e identificar as contrapartes da transação, apresentando assim, riscos de LD mais altos (FATF, 2019b, p. 11).

Sobre o entendimento da fonte de recursos/riqueza do cliente, o GAFI esclarece:

> A fonte de fundos e a fonte de riqueza são relevantes para determinar o perfil de risco de um cliente. A fonte de fundos é a atividade que gera os fundos para um cliente (por exemplo, salário, receitas comerciais ou pagamentos de um fundo), enquanto a fonte de riqueza descreve as atividades que geraram o patrimônio líquido total de um cliente (por exemplo, propriedade de um negócio, herança ou investimentos). Embora possam ser iguais para alguns clientes, podem ser parciais ou totalmente diferentes para outros clientes. Por exemplo, uma PEP que recebe um salário oficial modesto, mas que possui fundos substanciais, sem quaisquer interesses comerciais aparentes ou herança, pode levantar suspeitas de suborno, corrupção ou uso indevido de cargo. De acordo com a ABR, os contadores devem certificar-se de que as informações adequadas estão disponíveis para avaliar a fonte de fundos e a fonte de riqueza de um cliente como legítimas com um grau de certeza proporcional ao perfil de risco do cliente (FATF, 2019a, p. 24, tradução nossa).[3]

O GAFI traz a seguinte definição para Pessoas Expostas Politicamente (PEPs):

> *PEPs estrangeiras* são indivíduos que são ou foram encarregados de funções públicas proeminentes por um país estrangeiro, por exemplo, Chefes de Estado ou de governo, políticos de alto escalão, altos funcionários do governo, autoridades judiciais ou militares, altos executivos de empresas estatais, importantes autoridades de partidos políticos. *PEPs domésticas* são indivíduos que são ou foram encarregados internamente de funções públicas proeminentes, por exemplo, Chefes de Estado ou de governo, políticos de alto escalão, altos funcionários do governo, autoridades judiciais ou militares, altos executivos de empresas estatais, importantes autoridades do partido político. As pessoas que são ou foram encarregadas de uma função de destaque por uma organização internacional referem-se a membros da alta administração, ou seja, diretores, vice-diretores e membros do conselho ou funções equivalentes. A definição de PEPs não se destina a abranger indivíduos de classificação média ou mais juniores nas categorias anteriores (FATF, 2019a, Glossário de terminologia, grifo do autor, tradução nossa).[4]

---

[3] "The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funds for a client (e.g. salary, trading revenues, or payments out of a trust), while the source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). While these may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client."

[4] "*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a

Conforme o GAFI, o uso indevido das criptomoedas está relacionado a atividades criminosas, como tráfico de drogas, fraude, roubo e extorsão, cujos sinais de alerta mais comuns relacionados à fonte de fundos ou riqueza ligada a tais atividades criminosas são apresentadas no **Quadro 30**.

Quadro 30 – *Red flag indicators* de fontes de fundos/riqueza ligadas a atividades criminosas

Red flags indicators
• Transações com endereços de AVs ou cartões bancários ligados a esquemas conhecidos de fraude, extorsão ou *ransomware*, endereços sancionados, mercados *darknet* ou outros sites ilícitos.
• Transações de AVs originadas ou destinadas a serviços de jogos de azar *online*.
• O uso de um ou vários cartões de crédito e/ou débito vinculados a uma carteira AVs para sacar grandes quantidades de moeda fiduciária ou fundos para comprar AVs são provenientes de depósitos em dinheiro em cartões de crédito.
• Os depósitos em uma conta ou endereço de AVs são significativamente maiores do que o normal com uma fonte de fundos desconhecida, seguidos de conversão para moeda fiduciária, o que pode indicar roubo de fundos.
• Falta de transparência ou informações insuficientes sobre a origem e os proprietários dos fundos, como os que envolvem o uso de empresas de fachada ou os fundos colocados em uma ICO onde os dados pessoais dos investidores podem não estar disponíveis ou transações recebidas de sistemas *online* de pagamentos através de cartões de crédito/pré-pagos seguido de saque instantâneo.
• Os fundos de um cliente que são obtidos diretamente de *mixing services* de terceiros ou *wallet tumblers*.
• A maior parte da fonte de riqueza de um cliente é derivada de investimentos em AVs, ICOs ou ICOs fraudulentas etc.
• A fonte de riqueza de um cliente é desproporcionalmente retirada de AVs originados de outros PSAVs que não possuem controles AML/CFT.

Fonte: GAFI (FATF, 2020b, p. 15).

Profissionais e organizações contábeis que se envolvam em atividades ou operações financeiras com criptomoedas ou PSAVs, devem identificar, avaliar e tomarem medidas eficazes para mitigar seus riscos de LD/FT por meio das criptomoedas (FATF, 2019b, p. 11).

Nesse contexto, os comentários dos respondentes foram associados a temas correspondentes as categorias de risco como ponto de partida para aplicação da ABR pelo profissional da contabilidade ao lidar com criptomoedas, como: (i) Risco país/geográfico; (ii) Risco de cliente; e (iii) Risco de transação/serviços e canal de entrega associado.

---

prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories."

3. ***Red flag indicators***

Em seu Glossário de terminologia, o GAFI define *red flags* como qualquer fato ou conjunto de fatos ou circunstâncias que, vistos isoladamente ou em combinação com outros fatos e circunstâncias, indiquem a presença de maior risco de atividades ilícitas (FATF, 2019a). As *red flags* são geralmente prescritas pelos reguladores para detecção e previsão de riscos de fraude (GULLKVIST; JOKIPII, 2013).

O estado de atenção sobre os *red flag indicators* para AML/CFT, por parte dos profissionais da contabilidade, é fundamental para o cumprimento de parte de suas obrigações regulatórias gerais (FATF, 2019a, p. 23). Como consequência da ausência de conscientização e educação acerca dos riscos de LD/FT entre os profissionais da contabilidade, o estado de atenção acerca dos *red flag indicators* para AML/CFT é inibido, aumentando a vulnerabilidade dos profissionais da contabilidade de serem explorados por clientes que procuram fazer uso indevido de serviços legítimos para fins de LD/FT (FATF, 2018b, p. 8).

A prática criminosa de LD, que é antiga e conhecida por envolver diversos instrumentos financeiros, conta, desde 2008, com outro instrumento, as criptomoedas, que vêm se tornando um mecanismo muito promissor para execução desse crime (KATARZYNA, 2019). As criptomoedas podem estar envolvidas em qualquer uma das etapas de LD (ICAEW, 2019; KATARZYNA, 2019; OECD, 2019; FATF, 2020b; IFAC, 2020c): (i) **Etapa de colocação**: Os recursos angariados por meio de atividades ou serviços ilegais são convertidos em criptomoedas, uma vez que as criptomoedas podem ser negociadas anonimamente em qualquer lugar do mundo através da Internet; (ii) **Etapa de ocultação**: Utilizada para romper o vínculo inicial das criptomoedas com suas origens criminosas, pode ocorrer de várias formas, envolvendo: (a) Uso de serviço de anonimização; (b) *Sites* de jogos de azar e cripto-cassinos recém-criados que não são obrigados a seguir quaisquer regras e regulamentos; e (c) Muitos processos de troca repetitivos com "moedas de privacidade" até que não haja sinal de conexões ilegais; e (iii) **Etapa de integração**: As criptomoedas podem ser incorporadas formalmente ao sistema financeiro regular quando enviadas para PSAVs domiciliados ou operados em jurisdições com regulamentações AML/CFT mínimas ou inexistentes sobre AVs e PSAVs, onde os criminosos exploram as lacunas na AML/CFT sobre AVs e PSAVs ao executarem: (a) A conversão de criptomoedas em moedas fiduciária; (b) A formação de uma empresa *online* que aceite pagamentos envolvendo criptomoedas para legitimar a renda; e (c) Investimentos em imóveis, ativos de luxo ou empreendimentos comerciais, entre outros investimentos.

Nesse contexto, os comentários dos respondentes foram associados a temas correspondentes aos *red flag indicators* relacionados com as etapas de LD com criptomoedas, como: (i) Etapa de colocação; (ii) Etapa de ocultação; e (iii) Etapa de integração.

4. ***Red flag indicators*** **associados ao anonimato**

As criptomoedas, em algumas circunstâncias, podem oferecer maior anonimato do que as moedas fiduciárias tradicionais, tornando mais difícil rastrear o produto de atividades criminosas (ICAEW, 2019). Conforme visto anteriormente, entre as etapas de LD, o uso de serviço de anonimização ou serviço de mixagem de criptomoedas (*mixing cryptocurrency*), o acesso a *sites* de jogos *online* e a realização de repetidas trocas usando moedas de privacidade, caracterizam o processo de execução das etapas de LD. *Anonymiser*, segundo o GAFI, refere-se a ferramentas e serviços projetados para ocultar a origem de uma transação envolvendo criptomoedas e facilitar o anonimato (FATF, 2014, p. 6). *Mixer* ou *tumbler*, é um tipo de *anonymiser* que obscurece a cadeia de transações na *blockchain* ao agregar transações de vários usuários, quebrando o vínculo entre as partes de origem e destino de cada transação. No momento que as criptomoedas são processadas por meio da aplicação de *mixer*, embora a trilha exata das transações individuais possa ser obscurecida, a ocorrência de mixagem é detectável na *blockchain* relevante, mostrando que uma transação teve origem em um dos muitos possíveis pagadores, com destino em um dos muitos possíveis beneficiários (FATF, 2014; ICAEW, 2019; POSKRIAKOV; CHIRIAEVA; CAVIN, 2019).

O acesso a *sites* de jogos de *online*, como cassinos *online* com protocolos ineficientes de KYC, permite o depósito de criptomoedas diretamente no saldo do jogador, que posteriormente poderão ser retiradas instantaneamente para uma conta bancária, ou outro serviço de pagamento, como cartões de crédito pré-pagos, sem que a identidade do cliente e a origem das criptomoedas sejam conhecidas (OECD, 2019, p. 56).

Comumente chamadas de “moedas de privacidade”, criptomoedas como *Dash* (DASH), *Monero* (XMR) e *Zcash* (ZEC), são projetadas para serem altamente privadas, com objetivo de fornecer completo anonimato, impedindo a identificação do proprietário legal e do beneficiário das criptomoedas. A capacidade de rastrear transações na cadeia (*onchain*) envolvendo criptomoedas está na utilização de metadados armazenados na *blockchain* relevante e na aplicação de análise de padrões. Esse procedimento de rastreamento pode ser dificultado devido a especificação de *design* do *software* subjacente das moedas de privacidade, onde os endereços de carteira, transações e informações sobre transações podem não ser registradas publicamente

na *blockchain* relevante (BLANDIN *et al*., 2019; POSKRIAKOV; CHIRIAEVA; CAVIN, 2019).

Os profissionais da contabilidade devem estar cientes de que a presença de indicadores que se baseiam nas características e vulnerabilidades inerentes associadas à tecnologia subjacente das criptomoedas, como a possibilidade de anonimato, não sugerem automaticamente uma transação ilícita, uma vez que, tal presença deve ser considerada no contexto de outras características sobre o cliente e o relacionamento, ou uma explicação lógica do negócio (FATF, 2020b, p. 9). Assim, os comentários dos respondentes foram associados ao tema correspondente as estratégias de anonimato ao lidar com criptomoedas.

5. Desafios para a aplicação das medidas de CDD

Conforme o GAFI, a natureza dos serviços prestados pelo profissional da contabilidade determinará o escopo e a profundidade da *due diligence* e avaliação de riscos (FATF, 2019a, p. 9). Os profissionais da contabilidade podem ser procurados por clientes envolvidos no mercado de criptoativos para consultoria contábil acerca de negócios típicos desse mercado, como plataformas de câmbio de criptomoedas, provedores de carteiras de custódia, entre outros negócios (ICAEW, 2019).

É fato que os criminosos estejam sempre entre os primeiros a adotar qualquer nova tecnologia que funcione, tecnologia da "nova escola", para cometer crimes da "velha escola", e que a aplicação da lei sempre teve que evoluir à medida que novas tecnologias projetadas para fins legítimos, como as criptomoedas, são usadas em atividades criminosas (WEINSTEIN; COHN; PARKER, 2019). Certas características das criptomoedas, como, (i) sua natureza distribuída e transfronteiriça; (ii) sua fácil transferência; (iii) seu forte potencial para transações anônimas ou pseudoanônimas; e (iv) possibilidade de ser negociada por meio de entidades que operam sem ou com supervisão regulatória limitada, podem tornar as criptomoedas atraentes para a realização de atividades ilícitas, como LD/FT (FSB, 2018). As criptomoedas e seus produtos e serviços de pagamentos relacionados globalmente, devido ao rápido desenvolvimento, aumento da funcionalidade e crescente adoção, têm representado significativos desafios para reguladores e instituições do setor privado na prevenção de seu uso na LD/FT (POSKRIAKOV; CHIRIAEVA; CAVIN, 2019). Portanto, os comentários dos respondentes foram associados ao tema correspondente aos desafios ao lidar com criptomoedas.

6. Abordagem regulatória

Segundo Dewey (2022), apesar da clareza regulatória no espaço dos AVs manter-se indescritível, o interesse em regular as criptomoedas nunca foi tão grande entre formuladores de políticas e reguladores. Autoridades governamentais de todo o mundo têm debatido sobre formas de regulamentar as criptomoedas e atividades relacionadas. O conhecimento sobre este mercado tem sido um desafio para os órgãos reguladores e legisladores locais. Eles estão acompanhando o comportamento dessas estruturas e redes descentralizadas. Alguns países já se posicionaram de forma bem definida, tanto a favor como contra a existência desse mercado em suas economias locais (FATF, 2018a).

Para Van Der Laan (2014), é natural que o Estado, como elemento-chave da organização das economias modernas, apresente resposta às demandas sociais. Segundo Mendes (2017) a regulamentação das criptomoedas divide opiniões entre quem é a favor da autonomia de suas transações sem nenhum controle do Estado, e os que entendem que uma legislação para esse mercado atenuaria o suposto anonimato em crimes de tráficos, LD, entre outros crimes. Boff e Ferreira (2016) explicam que a busca de entendimento sobre as criptomoedas por parte dos governantes e legisladores está relacionada à aplicação ou criação de normas que garantam seu uso de maneira que não coloquem em risco seus usuários nem o *status quo* do modelo de sistema financeiro atual. Segundo Silva (2017), a regulamentação desse tipo de mercado deve sempre buscar a criação de um sistema que possibilite a concorrência entre seus participantes, evitando qualquer normatização que asfixie essa nova tecnologia. Para Borg e Schembri (2019), o objetivo da regulação nunca deve ser desacelerar ou delimitar a tecnologia, mas seu foco deve sempre estar na criação de padrões, bem como em princípios éticos e de boa governança, uma vez que essas são basicamente as ferramentas necessárias para que um novo setor amadureça, cresça e floresça.

Dessa forma, Blandin *et al*. (2019, p. 41) retratam quatro categorias de resposta regulatória: (i) **Regulação existente**: Aplicação das leis ou regulações existentes para atividades com criptoativos, cujo esclarecimento a respeito da aplicação de determinado instrumento legal existente geralmente vem de orientações regulatórias; (ii) **Regulação adaptada**: Revisão das leis ou regulações existentes para incluir uma ou mais atividades com criptoativos, expandindo o escopo de alguma lei ou regulação para cobrir explicitamente determinadas atividades com criptoativos; (iii) **Regulação específica**: Nova lei ou regulação editada especificamente para regular as atividades com criptoativos; e (iv) **Arcabouço**

regulatório específico: Uma estrutura regulatória distinta aplicada a um conjunto de atividades, das quais aquelas envolvendo criptoativos são apenas um aspecto.

Portanto, os comentários dos respondentes foram associados aos temas correspondentes às respostas regulatórias AML/CFT mais apropriadas ao lidar com as criptomoedas.

7. Orientações

Conforme o GAFI, o pré-requisito para que o profissional da contabilidade possa aplicar uma ABR eficaz, durante o processo de avaliação de risco, está no acesso a informações precisas, oportunas e objetivas sobre os riscos de LD/FT. A avaliação de risco de LD/FT pode ser realizada com base nas informações recebidas de uma autoridade competente designada, entidades autorreguladoras (EARs) ou outras fontes confiáveis (FATF, 2019a). Quanto a obrigação dos supervisores[5] e EARs de comunicar suas orientações aos profissionais da contabilidade, o GAFI enuncia o seguinte:

> Supervisores e EARs devem comunicar suas expectativas regulatórias. Isso pode ser feito por meio de um processo consultivo após um envolvimento significativo com as partes interessadas relevantes, incluindo contadores. Essa orientação pode estar na forma de requisitos de alto nível com base nos resultados desejados, regras baseadas em risco e informações sobre como os supervisores interpretam a legislação ou regulamentação relevante, ou orientações mais detalhadas sobre como determinados controles AML/CFT são melhor aplicados. As orientações emitidas para os contadores também devem discutir o risco de LD/FT em seu setor e delinear indicadores de LD/FT para ajudá-los a identificar transações e atividades suspeitas. Todas essas orientações devem ser preferencialmente consultadas, quando apropriado, e redigidas de maneira apropriada ao contexto do papel dos supervisores e EARs na jurisdição relevante (FATF, 2019a, p. 52, tradução nossa).[6]

No contexto dos criptoativos, os supervisores, após terem identificado e avaliado os riscos de LD/FT associados a produtos, serviços e atividades de AVs, bem como aos PSAVs,

---

[5] Supervisores refere-se às autoridades competentes designadas ou entidades não públicas com responsabilidades destinadas a assegurar o cumprimento por parte das instituições financeiras ("supervisores financeiros") e/ou APNFDs dos requisitos para combater a lavagem de dinheiro e o financiamento do terrorismo. Entidades não públicas (que podem incluir certos tipos de EARs) devem ter o poder de supervisionar e sancionar instituições financeiras ou APNFDs em relação aos requisitos de AML/CFT. Essas entidades não públicas também devem ser habilitadas por lei para exercer as funções que desempenham e serem supervisionadas por uma autoridade competente em relação a essas funções. (FATF, 2019a, Glossário de terminologia).

[6] "Supervisors and SRBs should communicate their regulatory expectations. This could be done through a consultative process after meaningful engagement with relevant stakeholders, including accountants. This guidance may be in the form of high-level requirements based on desired outcomes, risk-based rules, and information about how supervisors interpret relevant legislation or regulation, or more detailed guidance about how particular AML/CFT controls are best applied. Guidance issued to accountants should also discuss ML/TF risk within their sector and outline ML/TF indicators to help them identify suspicious transactions and activity. All such guidance should preferably be consulted on, where appropriate, and drafted in ways that are appropriate to the context of the role of supervisors and SRBs in the relevant jurisdiction."

devem comunicar suas expectativas de *compliance* dos PSAVs com suas obrigações legais e regulamentares (FATF, 2019b). De acordo com Blandin *et al*. (2019, p. 12), os bancos centrais geralmente têm sido a primeira autoridade reguladora a emitir declarações oficiais, incluindo avisos sobre criptoativos, seguidos por departamentos governamentais e órgãos de fiscalização financeira. Em maio de 2019, o Conselho de Estabilidade Financeira (FSBF em inglês), por meio de seu relatório "Criptoativos: Trabalhos em andamento, abordagens regulatórias e possíveis lacunas" na tradução livre, procurou atualizar os Ministros das Finanças e os Governadores do Banco Central do G20, a respeito dos trabalhos em andamento sobre abordagens regulatórias e de supervisão para criptoativos e possíveis lacunas (FSB, 2019b). No **Quadro 31** são apresentadas as organizações internacionais apontadas nesse relatório, e seus trabalhos a respeito dos criptoativos.

Quadro 31 – Trabalhos internacionais relacionados aos criptoativos

Organizações Internacionais	**Trabalhos relacionadas aos criptoativos**
Comitê de Supervisão Bancária de Basiléia	• Desenvolvimento de expectativas de supervisão de alto nível para os bancos envolvidos em atividades de criptoativos; • Monitoramento de desenvolvimentos relacionados a criptoativos, quantificando as exposições diretas e indiretas dos bancos a esses ativos; e • Esclarecimento ao tratamento prudencial das exposições dos bancos aos criptoativos.
Comitê de Pagamentos e Infraestrutura de Mercado	• Monitoramento das implicações das inovações digitais, incluindo moedas digitais, tokenização e registros distribuídos; • Desenvolvimento de relatórios e estruturas analíticas para auxiliar os bancos centrais em suas avaliações sobre moedas digitais e tecnologia de registros distribuídos, em compensação e liquidação de pagamentos; • Desenvolvimento de estrutura analítica sobre moedas digitais do banco central; e • Fornecimento de informações sobre os fluxos de trabalho de monitoramento de criptoativos.
Conselho de Estabilidade Financeira	• Monitoramento dos riscos para a estabilidade financeira; • Elaboração de diretório de reguladores sobre criptoativos; e; • Estudo da estabilidade financeira, das implicações regulatórias e de governança de tecnologias financeiras descentralizadas, como DLT e plataformas ponto a ponto (P2P).
Organização Internacional de Comissões de Valores Mobiliários	• Levantamento das preocupações sobre criptoativos em áreas que vão desde negociação, custódia, compensação e liquidação, contabilidade, avaliação e intermediação, até a exposição de fundos de investimento aos criptoativos; • Emissão de declaração a seus membros sobre os riscos das ofertas iniciais de moedas (ICO em inglês); • Implantação de uma Rede de Consulta da ICO, para os membros discutirem suas experiências e trazerem suas preocupações, incluindo questões transfronteiriças, à atenção dos reguladores;

	• Criação de portal para seus membros poderem acessar e compartilhar informações sobre fiscalização e outras questões relevantes para criptoativos e outras ameaças digitais; • Desenvolvimento de Estrutura de Suporte da ICO como um recurso educacional para ajudar seus membros a considerar os problemas domésticos e transfronteiriços para as ICOs; • Desenvolvimento de Relatório de Consulta analisando os problemas e riscos associados à negociação de criptoativos em plataformas de negociação de criptoativos; e; • Colaboração, por meio de seu comitê de políticas em contabilidade, junto ao Comitê Internacional de Interpretações de Relatórios Financeiros e ao *International Accounting Standards Board (IASB)*, para o desenvolvimento de um padrão contábil apropriado para criptoativos.
Grupo de Ação Financeira Internacional	• Adoção de alterações em suas Recomendações e Glossário, esclarecendo explicitamente que as Recomendações se aplicam as atividades financeiras que envolvam ativos virtuais (AVs), como criptoativos; e; • Alteração na Recomendação 15 exigindo que os provedores de serviços de ativos virtuais (PSAVs) sejam regulamentados para fins de combate à LD e CFT, licenciados ou registrados, e sujeitos a sistemas eficazes de monitoramento ou supervisão.
Organização de Cooperação e Desenvolvimento Econômico	• Realização de trabalhos sobre criptoativos e aplicações de DLT nos mercados financeiros; • Exame das ICOs como uma das aplicações mais proeminentes da *blockchain* para financiamento; • Análise dos benefícios potenciais do uso de ICOs regulamentadas para pequenas empresas, formação de capital de negócios, emissão e negociação de *tokens*, *tokenomics*, limitações na estruturação de ICOs, bem como riscos aos quais os investidores que subscrevem ofertas da ICO e *tokens* de emissão de pequenas e médias empresas (PMEs) estão expostos; • Análise sobre o potencial das ICOs como instrumentos de financiamento "convencionais" para as PMEs, independentemente do tipo de projeto ou modelo de negócios empregado pela empresa; • Exame das implicações políticas das ICOs relacionadas à regulamentação e supervisão de emissão de *tokens* em âmbito nacional e transfronteiriço, proteção financeira ao consumidor e educação financeira, pedido de clareza e proporcionalidade na estrutura regulatória e de supervisão aplicada às ICOs; e; • Realização de trabalho analítico sobre tokenização de ativos e o impacto que uma possível proliferação de tal mecanismo teria nos mercados financeiros, bem como em torno dos benefícios e riscos das *stablecoins*.

Fonte: Adaptado pelo autor (FSB, 2019b).

Essas organizações internacionais estão abordando questões relacionadas a proteção do investidor, integridade do mercado, combate à LD, exposições bancárias e monitoramento da estabilidade financeira, cobrindo aspectos importantes dos riscos relacionados aos criptoativos dentro de suas respectivas áreas de monitoramento. No tocante à PLD têm-se as diretrizes dos principais organismos internacionais que lidam com essa temática, em especial o GAFI. Entender e responder aos riscos identificados de LD está no cerne do que o GAFI faz.

Assim, foram selecionados, por meio do acesso ao *site* oficial do GAFI, os trabalhos desenvolvidos pelo GAFI acerca das questões decorrentes dos criptoativos, que estão no **Quadro 32**.

Quadro 32 – Trabalhos relacionados aos criptoativos desenvolvidos pelo GAFI

Orientações relacionadas aos criptoativos	Objetivos
Moedas Virtuais: Principais Definições e Riscos Potenciais de AML/CFT (FATF, 2014)	• Desenvolver uma matriz de risco para moedas virtuais; • Promover uma compreensão mais ampla das partes envolvidas nos sistemas de moeda virtual conversível e a maneira como a moeda virtual pode ser usada para operar os sistemas de pagamento; e; • Estimular uma discussão sobre a implementação de regulamentos AML/CFT baseados no risco nesta área.
Orientação para uma Abordagem Baseada em Risco para Moedas Virtuais (FATF, 2015)	• Explicar a aplicação da abordagem baseada em risco (ABR) às medidas AML/CFT no contexto das moedas virtuais; • Identificar as entidades envolvidas com produtos e serviços de pagamento de moedas virtuais; e; • Esclarecer a aplicação das Recomendações do GAFI relevantes para as *exchanges* de moedas virtuais conversíveis.
Orientação para uma Abordagem Baseada em Risco para Ativos Virtuais e Provedores de Serviços de Ativos Virtuais (FATF, 2019b)	• Expandir a Orientação para moedas virtuais de 2015 e explicar ainda mais a aplicação da ABR para medidas AML/CFT para ativos virtuais (AVs); • Identificar as entidades que conduzem atividades ou operações relacionadas aos AVs, ou seja, provedores de serviços de ativos virtuais (PSAVs); e; • Esclarecer a aplicação das Recomendações do GAFI aos AVs e PSAVs.
Indicadores de Bandeira Vermelha de Lavagem de Dinheiro e Financiamento do Terrorismo Associados a Ativos Virtuais (FATF, 2020b)	• Auxiliar as entidades relatoras, incluindo instituições financeiras (IFs), atividades e profissões não financeiras designadas (APNFDs) e PSAVs na identificação e no relato de atividades potenciais de LD e FT envolvendo AVs; e • Facilitar a aplicação por parte das entidades relatoras de uma ABR para seus requisitos de *customer due diligence* (CDD).
Revisão de 12 meses das Normas do GAFI Revistas Sobre Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (FATF, 2020c)	• Apresentar as conclusões das seguintes ações: ✓ Formação de um Grupo de Contato de Ativos Virtuais (VACG em inglês) para promover a implementação, identificar problemas e se envolver com o setor privado para monitorar o progresso; ✓ Revisão de 12 meses para medir a implementação dos Padrões revisados por jurisdições e pelo setor privado; e; ✓ Monitoramento de quaisquer mudanças nas tipologias, riscos e estrutura de mercado do setor de AVs.
Segunda Revisão de 12 meses das Normas Revistas do GAFI Sobre Ativos Virtuais e Prestadores de Serviços de Ativos Virtuais (FATF, 2021b)	• Apresentar as conclusões das seguintes ações: ✓ Segunda revisão de 12 meses para medir a implementação dos Padrões revisados por jurisdições e pelo setor privado; e; ✓ Monitoramento de quaisquer mudanças nas tipologias, riscos e estrutura de mercado do setor de AVs.

Fonte: Elaborado pelo autor.

Em nível nacional os trabalhos efetuados pela ENCCLA são realizados nas chamadas "Ações", que são elaboradas e pactuadas anualmente pelos membros da ENCCLA. Para cada Ação é criada um grupo de trabalho composto por vários órgãos e instituições, que procuram alcançar uma ou mais metas predefinidas. No **Quadro 33** são expostos os resultados das Ações 8 do período de 2017 a 2019, que foram evidenciados no *site* oficial da ENCCLA.

Quadro 33 – Resultados das Ações 8 ENCCLA (2017 – 2019)

Ações	Resultados
Ação 8/2017: Elaborar diagnóstico sobre a atual conjuntura da utilização de moedas virtuais e meios de pagamento eletrônico (ENCCLA, 2017b).	• Glossário com termos relacionados a Moedas Virtuais (ENCCLA, 2017a); • Levantamento de tipologias de LD e corrupção mediante o uso de moedas virtuais e meios de pagamento eletrônico (ENCCLA, 2017c); e; • *Workshop* sobre utilização de moedas virtuais.
Ação 8/2018: Aprofundar os estudos sobre a utilização de moedas virtuais para fins de lavagem de dinheiro e eventualmente apresentar propostas para regulamentação e/ou adequação legislativa (ENCCLA, 2018).	• Minuta de proposta de alteração da Lei n.º 9.613, de 3 de março de 1998, com foco no segmento de AVs; • Coletânea de jurisprudência; e; • Proposta de nova Ação para a ENCCLA 2019, com foco no âmbito penal.
Ação 8/2019: Aprofundar os estudos sobre a utilização de ativos virtuais para fins de lavagem de dinheiro e financiamento do terrorismo, apresentando (i) levantamento de boas práticas relacionadas com a investigação do delito em diversas esferas; (ii) eventual proposta de adequação normativa em matéria investigativa e de persecução penal (ENCCLA, 2019).	• Elaboração do produto "Roteiro de Boas Práticas de Investigação Relacionada a Criptoativos"; • Solicitação/consulta ao Instituto Brasileiro de Geografia e Estatística (IBGE)/Comissão Nacional de Classificação (CONCLA) sobre a possibilidade de criação de classe ou subclasse de Classificação Nacional de Atividades Econômicas (CNAE) para as corretoras ou *exchanges* de criptoativos; e; • Elaboração de modelo de comunicação/notificação de transação suspeita por corretores ou *exchanges*.

Fonte: Elaborado pelo autor.

Por meio das Ações 8, seu grupo de trabalho realizou estudos e diagnósticos legais-normativos, elaborou propostas legislativas e aprofundou estudos sobre os criptoativos. Abordou a utilização dos criptoativos no crime de LD, por meio de pesquisas e compartilhamento das experiencias dos participantes do grupo de trabalho em atuações relacionadas as práticas de PLD envolvendo criptoativos.

Outras abordagens, como emissão de orientações ou publicação de avisos sobre criptoativos e atividades relacionadas dentro de suas jurisdições, foram realizadas pelos órgãos públicos, conforme **Quadro 34**.

Quadro 34 – Trabalhos nacionais relacionados aos criptoativos

Organizações Nacionais	Trabalhos relacionadas aos criptoativos
Banco Central do Brasil (BCB)	• No ano de 2014 foi divulgado o Comunicado nº 25.306, esclarecendo sobre os riscos decorrentes da aquisição das chamadas "moedas virtuais" ou "moedas criptográficas" e da realização de transações com elas (BCB, 2014); e; • Em 2017 foi divulgado o Comunicado nº 31.379, alertando sobre os riscos decorrentes de operações de guarda e negociação das denominadas moedas virtuais (BCB, 2017).
Receita Federal do Brasil (RFB)	• No ano de 2017 foi divulgado o documento "Perguntas e Respostas – Imposto de Renda Pessoa Física" informando sobre a declaração da posse de criptomoedas e eventuais ganhos de capital em sua negociação (RFB, 2017); e; • Em 2019 foi editada a instrução normativa da Receita Federal do Brasil – RFB de Nº 1.888, de 3 de maio de 2019, que institui e disciplina a prestação de informações relativas às operações realizadas com criptoativos (RFB, 2019).
Comissão de Valores Mobiliários (CVM)	• Em outubro de 2017 foi emitida Nota CVM a respeito das *Initial Coin Offerings* (ICOs) tratando sobre a competência regulatória sobre as ICOs, que se enquadrem na definição de valor mobiliário (CVM, 2017a); • Em novembro de 2017, foi publicado o documento "**FAQ** – Perguntas Frequentes a respeito do tema Initial Coin Offering (ICO)" (CVM, 2017b). • Em janeiro de 2018 foi emitido Ofício Circular nº 1/2018/CVM/SIN, cujo assunto refere-se ao investimento, pelos fundos de investimento regulados pela Instrução CVM nº 555/14, em criptomoedas" (CVM, 2018c); • Em maio de 2018 foi publicado o material educacional Criptoativos – Série Alertas (CVM, 2018a); • No mês de setembro de 2018 foi emitido Ofício Circular nº 11/2018/CVM/SIN, com o objetivo de complementar o Ofício Circular nº 1/2018/CVM/SIN (CVM, 2018b); e; • Em 2020 foi editada a Instrução CVM nº 626, que institui e disciplina regras para constituição e funcionamento de ambiente regulatório experimental (**sandbox** regulatório) (CVM, 2020).

Fonte: Elaborado pelo autor.

Por meio do Comunicado nº 25.306 de 2014, o BCB firmou sua posição sobre as moedas virtuais (criptomoedas), esclarecendo que elas não se confundem com as moedas eletrônicas. Posteriormente, através do Comunicado nº 31.379 de 2017, o BCB reforça sua preocupação com as criptomoedas.

A instrução normativa RFB de nº 1.888 de 2019, é a primeira regulação governamental para o mercado de criptomoedas no Brasil, que obriga a prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil.

No ano 2017, a CVM emitiu dois documentos relacionados às operações de ofertas de ativos virtuais (AVs), as *Initial Coin Offerings* (ICOs). Nesses documentos ela esclarece que

está atenta às recentes inovações tecnológicas nos mercados financeiros global e brasileiro, buscando compreender os benefícios e os riscos associados, através de fóruns internos, como o Comitê de Gestão de Riscos (CGR) e o *Fintech Hub*, ou por meio de discussões no âmbito internacional, como em trabalhos desenvolvidos pela *International Organization of Securities Commissions* (IOSCO). Alertando para os riscos relacionados à participação de potenciais investidores em operações envolvendo ICOs, como o risco de operação de LD nas operações envolvendo a oferta de um criptoativo no mercado (CVM, 2017a, 2017b).

A CVM apresentou, ainda, alguns esclarecimentos sobre determinadas diligências e governança esperadas de administradores, gestores e auditores independentes no desempenho de suas atribuições junto aos fundos durante a aquisição de criptoativos. É levada em conta a exigência de PCLD imposta pela Instrução CVM nº 301 de 1999 (revogada pela Instrução CVM nº 617 de 2019), devido à possibilidade de financiamento, direto ou indiretamente, de operações ilegais nesse mercado. Nesse contexto o papel dos auditores independentes contratados pelo fundo deve ser capaz de conduzir diligências adequadas e proporcionais em relação a eventuais criptoativos adquiridos pelo fundo (CVM, 2018b).

A CVM editou a instrução normativa CVM nº 626 de 2020, na procura em alinhar-se com a Estratégia Brasileira para a Transformação Digital (E-Digital), com ações estratégicas para tornar o Brasil um ambiente amigável ao empreendedorismo digital. O *sandbox* regulatório tem sido uma alternativa ao atraso regulatório frente as inovações tecnológicas (RFB, 2019; CVM, 2020; AHERN, 2020).

Nesse contexto, os comentários dos respondentes foram associados ao tema correspondente às questões referentes a fontes de informação sobre avaliação de risco de LD ao lidar com criptomoedas.

8. Mitigação de riscos

De acordo com o GAFI, os profissionais da contabilidade devem identificar e aplicar medidas para mitigar e gerenciar de maneira eficaz e eficiente os riscos de LD/FT (FATF, 2019a, p. 14). Ao avaliar o risco, os profissionais da contabilidade devem considerar todos os fatores de risco relevantes antes de determinar o nível de risco geral e o nível apropriado de mitigação a ser aplicado (FATF, 2019a, p. 22). Nesse sentido, os profissionais da contabilidade devem ter políticas, controles e procedimentos que lhes permitam gerenciar e mitigar efetivamente os riscos que identificarem (FATF, 2019a, p. 33).

No contexto dos AVs, como as criptomoedas, as APNFDs que se envolverem em atividades de AVs ou fornecerem produtos ou serviços de AVs, devem avaliar os riscos de LD/FT associados e aplicar uma ABR para garantir que as medidas adequadas para gerenciar ou mitigar esses riscos sejam implementadas (FATF, 2019b, p. 20). Para as APNFDs que se envolverem em atividade de PSAVs, o GAFI orienta que essas APNFDs devem estar sujeitas a todas as medidas para os PSAVs estabelecidas em suas Recomendações (FATF, 2019b, p. 34).

Nesse contexto, os comentários dos respondentes foram associados ao tema correspondente aos fatores e medidas para gerenciar e mitigar efetivamente os riscos de LD ao lidar com criptomoedas.

9. Medidas preventivas

Por meio de sua Recomendação Nº 10 – Devida diligência acerca do cliente, o GAFI orienta que os profissionais da contabilidade devem elaborar procedimentos de *customer due diligence* (CDD) que lhes permitam determinar a verdadeira identidade de seus clientes, conhecer os tipos de negócios e transações que o cliente provavelmente realizará (FATF, 2019a, p. 34). No Parágrafo 7 da Nota Interpretativa da Recomendação Nº 15 (NIR – 15) é possível evidenciar que às medidas preventivas contidas nas Recomendações Nº 10 se aplicam aos PSAVs no contexto de AVs e atividades financeiras de AVs (FATF, 2019b, p. 55).

O GAFI explica que a condução de uma *due diligence* contínua sobre o relacionamento comercial tem como objetivo garantir que os documentos, dados ou informações adquiridas no processo de CDD sejam mantidos atualizados e relevantes por meio de revisões de registros existentes (FATF, 2019a, p. 36). A condução de uma *due diligence* contínua no contexto dos AVs torna-se um procedimento de CDD de suma importância, tendo em vista a velocidade com que o mercado de criptoativos evolui e se desenvolve, exigindo maiores esclarecimentos a respeito das atividades envolvendo criptomoedas e dos PSAVs.

Os profissionais da contabilidade quando solicitados por clientes envolvidos no mercado de criptoativos, além de uma análise dos possíveis riscos de LD, se necessário, devem realizar verificações de *due diligence* e ALM aprimoradas (ICAEW, 2019). Devido ao alcance global, liquidez, capacidade de permitir transações ponto a ponto, potencial de maior anonimato e ofuscação de fluxos de transações de AVs e desafios associados à realização de identificação e verificação eficazes do cliente, os AVs e PSAVs, em geral, podem ser considerados como de alto risco de LD/TF, podendo exigir a aplicação de medidas de CDD aprimoradas (FATF, 2019b, p. 24).

O **Quadro 35** apresenta uma lista não exaustiva de medidas de CDD aprimoradas que podem ser aplicadas para relacionamentos comerciais de alto risco.

Quadro 35 – Medidas de CDD aprimoradas

Exemplos de medidas de CDD aprimoradas
• Identificação do cliente e, quando aplicável, do beneficiário efetivo do cliente;
• Verificação da identidade do cliente com base no risco e com base em informações, dados ou documentação confiáveis e independentes, pelo menos na medida exigida pela legislação ou regulamentação aplicável;
• Sendo possível, rastrear o endereço de protocolo da Internet (IP) do cliente;
• Pesquisa na Internet para corroborar informações de atividades consistentes com o perfil de transação do cliente, desde que a coleta de dados esteja de acordo com a legislação nacional de privacidade;
• Obtenção de informações adicionais sobre o cliente (por exemplo, ocupação, volume de bens, informações disponíveis em banco de dados públicos, internet etc.), e atualização regular dos dados de identificação do cliente e real beneficiário;
• Compreensão da finalidade e da natureza pretendida do relacionamento comercial;
• Obtenção de informações adicionais e, conforme apropriado, documentação comprovativa sobre a natureza pretendida do relacionamento comercial;
• Obtenção de informações sobre a fonte de recursos e/ou fontes de riqueza do cliente e evidenciá-las claramente através da documentação apropriada obtida;
• Obtenção de informações sobre os motivos das transações pretendidas ou realizadas;
• Obtenção de aprovação da alta administração para iniciar ou continuar o relacionamento comercial;
• Condução de monitoramento aprimorado do relacionamento comercial, aumentando o número e o tempo dos controles aplicados e selecionando padrões de transações que precisam de exame mais aprofundado;
• Exigência de que o primeiro pagamento seja realizado através de uma conta em nome do cliente com um banco sujeito a padrões de CDD semelhantes; e
• Maior conscientização sobre clientes e transações de maior risco, em todos os departamentos com um relacionamento comercial com o cliente, incluindo a possibilidade de um *briefing* aprimorado das equipes de engajamento responsáveis pelo cliente.

Fonte: Adaptado pelo autor (FATF, 2019a; FATF, 2019b).

Ainda, em concordância com a Recomendação Nº 12 – Pessoas expostas politicamente, os profissionais da contabilidade devem adotar medidas razoáveis para determinar se um cliente ou benificiário é uma PEP ou membro da família ou próximo de uma PEP (FATF, 2019a, p. 38).

No ecossistema dos criptoativos, as organizações contábeis com atividades ou operações financeiras envolvendo criptomoedas ou que forneçam produtos ou serviços relacionados às

criptomoedas, devem ter sistema de gerenciamento de risco capaz de determinar se um cliente/beneficiário final é uma PEP, além das medidas normais de CDD, para determinar se e quando as organizações contábeis estão fazendo negócios com PEPs, incluindo a identificação da fonte de fundos/riquezas quando relevante (FATF, 2019b, p. 27).

Nesse contexto, os comentários dos respondentes foram associados ao tema correspondente as medidas de *customer due diligence* aprimoradas ao lidar com criptomoedas.

10. Controles internos e governança

Procurando atender a Recomendação Nº 18 – Controles internos e filiais e subsidiárias estrangeiras, elaborada pelo GAFI, as organizações contábeis devem criar uma cultura de *compliance* de AML/CFT, assegurando que seus funcionários cumpram as políticas, procedimentos e processos da organização projetados para limitar e controlar os riscos de LD/FT. Os controles internos da organização devem incorporar o processo baseado em risco adequado ao tamanho e complexidade da organização (FATF, 2019a, p. 40).

Uma vez que a vigência de controles adequados nas organizações de contabilidade depende fundamentalmente de treinamento e conscientização, todos os funcionários relevantes devem ter acesso, no mínimo, as informações gerais sobre leis, regulamentos e políticas internas de AML/CFT. O treinamento direcionado para profissionais da contabilidade que fornecem atividades específicas para clientes de alto risco e para os que realizam trabalhos de alto risco, pode ser feito por meio de: (i) Estudos de caso baseados em fatos ou hipotéticos; (ii) Treinamento de documentação falsa; e (iii) Treinamento sobre *red flags* (FATF, 2019a, p. 43).

No contexto dos criptoativos, o treinamento deve permitir que os profissionais da contabilidade formulem sólidos julgamentos sobre a qualidade das avaliações dos riscos associados às atividades envolvendo criptomoedas e ao fornecimento de produtos ou serviços por PSAVs, que podem ser potencialmente mais elevados, e que os profissionais da contabilidade sejam capazes de considerar a adequação e proporcionalidade dos controles de AML/CFT. Dessa forma, a revisão periódica dos serviços oferecidos e avaliação periódica da estrutura AML aplicável ao profissional, permitirá ao profissional da contabilidade determinar se o risco de LD/FT com o uso das criptomoedas aumentou, provocando, assim, a necessidade do aprimoramento ou melhoria dos controles que permitem gerenciar e mitigar efetivamente os riscos, caso o profissional da contabilidade entenda que os controles são fracos ou ineficazes.

Conforme Katarzyna (2019), as criptomoedas, que estão constante evolução, devem ser abordadas de maneira holística, onde as políticas, procedimentos e processos da organização

projetados para limitar e controlar os riscos de LD/FT devem abordar todas as áreas que possam estar em risco. Nesse sentido, uma maior atenção nas operações da organização que são mais vulneráveis ao abuso por LD utilizando criptomoedas, somente será possível após a organização contábil ter realizado a avaliação de risco em toda a organização, considerando os riscos (país/geográfico, cliente e transação/serviço) associados aos AVs e PSAVs.

Nesse contexto, os comentários dos respondentes foram associados ao tema correspondente às políticas, procedimentos e controles da organização projetados para limitar e controlar os riscos de LD ao lidar com criptomoedas.

ANEXO A – FOLHA DE ROSTO DA PESQUISA

Plataforma Brasil MINISTÉRIO DA SAÚDE - Conselho Nacional de Saúde - Comissão Nacional de Ética em Pesquisa – CONEP

FOLHA DE ROSTO PARA PESQUISA ENVOLVENDO SERES HUMANOS

1. Projeto de Pesquisa: PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: UMA ABORDAGEM BASEADA EM RISCO PARA A PROFISSÃO CONTÁBIL			
2. Número de Participantes da Pesquisa: 0			
3. Área Temática:			
4. Área do Conhecimento: Grande Área 6. Ciências Sociais Aplicadas			
PESQUISADOR RESPONSÁVEL			
5. Nome: Jaime Wagner Rodrigues Barbosa			
6. CPF: 042.916.047-00	7. Endereço (Rua, n.º): Rua Sambé, nº 81, Santa Cruz RIO DE JANEIRO RIO DE JANEIRO 23520445		
8. Nacionalidade: BRASILEIRO	9. Telefone: 21976960358	10. Outro Telefone:	11. Email: jaimewrodrigues@yahoo.com.br

Termo de Compromisso: Declaro que conheço e cumprirei os requisitos da Resolução CNS 466/12 e suas complementares. Comprometo-me a utilizar os materiais e dados coletados exclusivamente para os fins previstos no protocolo e a publicar os resultados sejam eles favoráveis ou não. Aceito as responsabilidades pela condução científica do projeto acima. Tenho ciência que essa folha será anexada ao projeto devidamente assinada por todos os responsáveis e fará parte integrante da documentação do mesmo.

Data: 23 / 08 / 2021

Assinatura

INSTITUIÇÃO PROPONENTE		
12. Nome: Universidade Federal Do Rio de Janeiro	13. CNPJ: 33.663.683/0010-07	14. Unidade/Órgão: Faculdade de Administração e Ciências Contábeis
15. Telefone: (21) 3938-5121	16. Outro Telefone:	

Termo de Compromisso (do responsável pela instituição): Declaro que conheço e cumprirei os requisitos da Resolução CNS 466/12 e suas Complementares e como esta instituição tem condições para o desenvolvimento deste projeto, autorizo sua execução.

Responsável: ANTONIO J. B. OLIVEIRA CPF: 471382786/68

Cargo/Função: DIRETOR

Data: 23 / 8 / 2021

Assinatura

Antonio José Barbosa de Oliveira
Diretor
Matrícula SIAPE 2124782
FACC/UFRJ

PATROCINADOR PRINCIPAL

Não se aplica.

ANEXO B – PARECER CONSUBSTANCIADO DO CEP

UFRJ - CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: PREVENÇÃO E COMBATE AO CRIME DE UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: UMA ABORDAGEM BASEADA EM RISCO PARA A PROFISSÃO CONTÁBIL

Pesquisador: Jaime Wagner Rodrigues Barbosa

Área Temática:

Versão: 1

CAAE: 52267921.3.0000.5582

Instituição Proponente: Faculdade de Administração e Ciências Contábeis

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.157.673

Apresentação do Projeto:

O surgimento da Internet trouxe um aumento na circulação e na velocidade do acesso às informações de diversas naturezas, possibilitando maior facilidade nas relações pessoais, profissionais e comerciais. Nesse ambiente global, novos modelos de negócios tornam-se viáveis, trazendo contribuições significativas para um sistema financeiro mais eficiente, mas possibilitando, também, o surgimento de novos riscos, como os relacionados à lavagem de dinheiro. No Brasil há uma legislação específica para o assunto, a "Lei de Lavagem de Dinheiro", onde seu artigo 9º define como um dos sujeitos submetidos às medidas de prevenção à lavagem de dinheiro, o profissional de contabilidade, atribuindo-lhe maiores responsabilidades como uma participação mais efetiva na prevenção e acompanhamento de qualquer atividade que possa estar relacionada a esse crime. Dentro desse contexto têm-se os serviços desenvolvidos para o mercado de criptoativos, cuja operação traz maior liquidez ao mercado com diferentes pontos de interseção entre o ambiente virtual e o ambiente físico. Esse mercado está introduzindo uma nova realidade com muitos desafios e ameaças, como a inovação na prática de lavagem de dinheiro, por meio da utilização de criptoativos. Considerando a necessidade de prevenção e combate à lavagem de dinheiro, este estudo tem como objetivo identificar possíveis abordagens que auxiliem o profissional de contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro. Classificado como documental, com uma abordagem de

Endereço: Av Pasteur, 250-Praia Vermelha, prédio CFCH, 3º andar, sala 30
Bairro: URCA **CEP:** 22.290-240
UF: RJ **Município:** RIO DE JANEIRO
Telefone: (21)3938-5167 **E-mail:** cep.cfch@gmail.com

UFRJ - CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Continuação do Parecer: 5.157.673

natureza qualitativa e de caráter descritivo, a partir de uma análise de conteúdo, o estudo analisa os documentos de domínio público, referentes às abordagens regulatórias e de supervisão emitidos por organizações nacionais e internacionais, a respeito das questões decorrentes dos criptoativos, e aplicação de questionário junto aos profissionais com experiência na Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo (PLD-FT) e experiência com criptoativos.

Objetivo da Pesquisa:

1.3 OBJETIVO GERAL

O objetivo geral do presente estudo é identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro.

1.4 OBJETIVOS ESPECÍFICOS

a) Identificar possíveis aplicações dos criptoativos nos crimes de lavagem de dinheiro;

b) Verificar como as partes interessadas (instituições e atores) na prevenção e combate à lavagem de dinheiro estão tentando coibir a utilização dos criptoativos na prática desse crime; e

c) Verificar o tratamento contábil aplicado aos criptoativos.

Avaliação dos Riscos e Benefícios:

A avaliação de riscos e benefícios está adequada.

Comentários e Considerações sobre a Pesquisa:

O projeto apresentado propõe investigar "possíveis abordagens que auxiliem o profissional de contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na lavagem de dinheiro". Além do levantamento bibliográfico amplo, o pesquisador propõe o uso de questionários a serem enviados a profissionais com experiências relevantes (combate à lavagem de dinheiro e criptoativos). Como a aplicação do questionário será digital (através de e-mail), o projeto trata adequadamente das questões éticas envolvidas.

Considerações sobre os Termos de apresentação obrigatória:

O RCLE apresentado está adequado.

Conclusões ou Pendências e Lista de Inadequações:

Projeto aprovado.

Considerações Finais a critério do CEP:

Endereço: Av Pasteur, 250-Praia Vermelha, prédio CFCH, 3º andar, sala 30
Bairro: URCA **CEP:** 22.290-240
UF: RJ **Município:** RIO DE JANEIRO
Telefone: (21)3938-5167 **E-mail:** cep.cfch@gmail.com

UFRJ - CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Continuação do Parecer: 5.157.673

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1790575.pdf	02/09/2021 11:59:20		Aceito
Folha de Rosto	FolhaDeRosto_JaimeWagnerRodriguesBarbosa.pdf	02/09/2021 11:54:38	Jaime Wagner Rodrigues Barbosa	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	RCLE_JaimeWagnerRodeiguesBarbosa.pdf	02/09/2021 11:53:31	Jaime Wagner Rodrigues Barbosa	Aceito
Projeto Detalhado / Brochura Investigador	ProjetoDePesquisa_JaimeWagnerRodriguesBarbosa.pdf	02/09/2021 11:50:15	Jaime Wagner Rodrigues Barbosa	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

RIO DE JANEIRO, 09 de Dezembro de 2021

Assinado por:
ERIMALDO MATIAS NICACIO
(Coordenador(a))

Endereço: Av Pasteur, 250-Praia Vermelha, prédio CFCH, 3º andar, sala 30
Bairro: URCA **CEP:** 22.290-240
UF: RJ **Município:** RIO DE JANEIRO
Telefone: (21)3938-5167 **E-mail:** cep.cfch@gmail.com

ANEXO C – IFRIC *UPDATE JUNE 2019: HOLDINGS OF CRYPTOCURRENCIES*

Holdings of Cryptocurrencies—June 2019

The Committee discussed how IFRS Standards apply to holdings of cryptocurrencies.

The Committee noted that a range of cryptoassets exist. For the purposes of its discussion, the Committee considered a subset of cryptoassets with all the following characteristics that this agenda decision refers to as a 'cryptocurrency':

a. a digital or virtual currency recorded on a distributed ledger that uses cryptography for security.
b. not issued by a jurisdictional authority or other party.
c. does not give rise to a contract between the holder and another party.

Nature of a cryptocurrency

Paragraph 8 of IAS 38 *Intangible Assets* defines an intangible asset as 'an identifiable non-monetary asset without physical substance'.

Paragraph 12 of IAS 38 states that an asset is identifiable if it is separable or arises from contractual or other legal rights. An asset is separable if it 'is capable of being separated or divided from the entity and sold, transferred, licensed, rented or exchanged, either individually or together with a related contract, identifiable asset or liability'.

Paragraph 16 of IAS 21 *The Effects of Changes in Foreign Exchange Rates* states that 'the essential feature of a non-monetary item is the absence of a right to receive (or an obligation to deliver) a fixed or determinable number of units of currency'.

The Committee observed that a holding of cryptocurrency meets the definition of an intangible asset in IAS 38 on the grounds that (a) it is capable of being separated from the holder and sold or transferred individually; and (b) it does not give the holder a right to receive a fixed or determinable number of units of currency.

Which IFRS Standard applies to holdings of cryptocurrencies?

The Committee concluded that IAS 2 *Inventories* applies to cryptocurrencies when they are held for sale in the ordinary course of business. If IAS 2 is not applicable, an entity applies IAS 38 to holdings of cryptocurrencies. The Committee considered the following in reaching its conclusion.

Intangible Asset

IAS 38 applies in accounting for all intangible assets except:

a. those that are within the scope of another Standard;
b. financial assets, as defined in IAS 32 *Financial Instruments: Presentation*;
c. the recognition and measurement of exploration and evaluation assets; and
d. expenditure on the development and extraction of minerals, oil, natural gas and similar non-regenerative resources.

Accordingly, the Committee considered whether a holding of cryptocurrency meets the definition of a financial asset in IAS 32 or is within the scope of another Standard.

Financial asset

Paragraph 11 of IAS 32 defines a financial asset. In summary, a financial asset is any asset that is: (a) cash; (b) an equity instrument of another entity; (c) a contractual right to receive cash or another financial asset from another entity; (d) a contractual right to exchange financial assets or financial liabilities with another entity under particular conditions; or (e) a particular contract that will or may be settled in the entity's own equity instruments.

The Committee concluded that a holding of cryptocurrency is not a financial asset. This is because a cryptocurrency is not cash (see below). Nor is it an equity instrument of another entity. It does not give rise to a contractual right for the holder and it is not a contract that will or may be settled in the holder's own equity instruments.

Cash

Paragraph AG3 of IAS 32 states that 'currency (cash) is a financial asset because it represents the medium of exchange and is therefore the basis on which all transactions are measured and recognised in financial statements. A deposit of cash with a bank or similar financial institution is a financial asset because it represents the contractual right of the depositor to obtain cash from the institution or to draw a cheque or similar instrument against the balance in favour of a creditor in payment of a financial liability'.

The Committee observed that the description of cash in paragraph AG3 of IAS 32 implies that cash is expected to be used as a medium of exchange (ie used in exchange for goods or services) and as the monetary unit in pricing goods or services to such an extent that it would be the basis on which all transactions are measured and recognised in financial statements.

Some cryptocurrencies can be used in exchange for particular good or services. However, the Committee noted that it is not aware of any cryptocurrency that is used as a medium of exchange and as the monetary unit in pricing goods or services to such an extent that it would be the basis on which all transactions are measured and recognised in financial statements. Consequently, the Committee concluded that a holding of cryptocurrency is not cash because cryptocurrencies do not currently have the characteristics of cash.

Inventory

IAS 2 applies to inventories of intangible assets. Paragraph 6 of that Standard defines inventories as assets:

a. held for sale in the ordinary course of business;
b. in the process of production for such sale; or
c. in the form of materials or supplies to be consumed in the production process or in the rendering of services.

The Committee observed that an entity may hold cryptocurrencies for sale in the ordinary course of business. In that circumstance, a holding of cryptocurrency is inventory for the entity and, accordingly, IAS 2 applies to that holding.

The Committee also observed that an entity may act as a broker-trader of cryptocurrencies. In that circumstance, the entity considers the requirements in paragraph 3(b) of IAS 2 for commodity broker-traders who measure their inventories at fair value less costs to sell. Paragraph 5 of IAS 2 states that broker-traders are those who buy or sell commodities for others or on their own account. The inventories referred to in paragraph 3(b) are principally acquired with the purpose of selling in the near future and generating a profit from fluctuations in price or broker-traders' margin.

Disclosure

In addition to disclosures otherwise required by IFRS Standards, an entity is required to disclose any additional information that is relevant to an understanding of its financial statements (paragraph 112 of IAS 1 *Presentation of Financial Statements*). In particular, the Committee noted the following disclosure requirements in the context of holdings of cryptocurrencies:

a. An entity provides the disclosures required by (i) paragraphs 36–39 of IAS 2 for cryptocurrencies held for sale in the ordinary course of business; and (ii) paragraphs 118–128 of IAS 38 for holdings of cryptocurrencies to which it applies IAS 38.
b. If an entity measures holdings of cryptocurrencies at fair value, paragraphs 91–99 of IFRS 13 *Fair Value Measurement* specify applicable disclosure requirements.
c. Applying paragraph 122 of IAS 1, an entity discloses judgements that its management has made regarding its accounting for holdings of cryptocurrencies if those are part of the judgements that had the most significant effect on the amounts recognised in the financial statements.
d. Paragraph 21 of IAS 10 *Events after the Reporting Period* requires an entity to disclose details of any material non-adjusting events, including information about the nature of the event and an estimate of its financial effect (or a statement that such an estimate cannot be made). For example, an entity holding cryptocurrencies would consider whether changes in the fair value of those holdings after the reporting period are of such significance that non-disclosure could influence the economic decisions that users of financial statements make on the basis of the financial statements.