LAVAGEM DE DINHEIRO AO LIDAR COM CRIPTOATIVOS: UMA ABORDAGEM BASEADA EM RISCO PARA A PROFISSÃO CONTÁBIL

MONEY LAUNDERING WHEN DEALING WITH CRYPTOASSETS: A RISK-BASED APPROACH FOR THE ACCOUNTING PROFESSION

Jaime Wagner Rodrigues Barbosa

*Mestre em Ciências Contábeis, Programa de Pós-Graduação em Ciências Contábeis, Universidade Federal do Rio de Janeiro, (UFRJ).
Endereço: Avenida Pasteur 250, sala 250, Urca, Rio de Janeiro – RJ. CEP: 22.290-902.
Telefone: (21) 3938-0282
E-mail: jaimewrodrigues@yahoo.com.br*

*Recebido: 10/05/2024 Aprovado: 09/08/20243
Publicado: 20/08/2024*

Pierre Ohayon

*Doutor em Administração, Professor Titular do Programa de Pós-Graduação em Ciências Contábeis, Universidade Federal do Rio de Janeiro, (UFRJ).
Endereço: Avenida Pasteur 250, sala 250, Urca, Rio de Janeiro – RJ. CEP: 22.290-902.
Telefone: (21) 3938-0282
E-mail: pohayon@facc.ufrj.br*

RESUMO

Considerando a inovação na prática de lavagem de dinheiro (LD) com criptoativos, a necessidade de prevenção e combate à LD (PCLD), e o fato de que o profissional da contabilidade é considerado a primeira linha de defesa na PCLD, este estudo tem como objetivo identificar possíveis abordagens que auxiliem o profissional da contabilidade na PCLD por meio de criptoativos. 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 aplicados questionários junto à 62 profissionais com experiência em criptoativos e na prevenção à LD e ao financiamento do terrorismo (PLD-FT). 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 significantes níveis de ocorrência e relevância. Na análise dos comentários deixados pelos respondentes, emergiram temas que reforçam a implementação de uma abordagem baseada em risco (ABR) para PCLD 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.

Palavras-chave: Lavagem de dinheiro. Criptoativos. Profissional da contabilidade. ABR. PLD-FT.

ABSTRACT

Considering the innovation in the practice of money laundering (ML) with cryptoassets, the need to prevent and combat ML (PCML), and the fact that the accounting professional is considered the first line of defense in the PCML, this study aims to identify possible approaches that help the accounting professional in the PCML through cryptoassets. The present study is classified as documentary, with a qualitative approach and an exploratory and descriptive character, based on content and documentary analysis. Questionnaires

were applied to 62 professionals with experience in cryptoassets and in the prevention of ML and terrorist financing (AML-FT). In general, respondents understand that all assertions related to the risks and challenges of ML crime faced when dealing with cryptoassets have significant levels of occurrence and relevance. In the analysis of the comments left by the respondents, themes emerged that reinforce the implementation of a risk-based approach (RBA) to PCML by professionals who come to get 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.

Keywords: Money laundering. Cryptoassets. Accounting Professional. RBA. AML-FT.

1 INTRODUÇÃO

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 o estudo de 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. Esses crimes impedem o crescimento sustentável e inclusivo, reduzindo os recursos disponíveis para fins produtivos como a construção de estradas, escolas e hospitais (WEEKS-BROWN, 2018). Provocam, também, o aumento nas taxas de emigração de mão de obra qualificada, especialmente nos países em desenvolvimento (SCHANEIDER, 2018).

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, 2017). Por consequência, esse mercado está introduzindo uma nova realidade repleta de ameaças, como a inovação na prática de LD, por meio da utilização de criptoativos, como as criptomoedas. 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.

Considerando a necessidade de PCLD, e o fato de que o profissional da contabilidade é considerado a primeira linha de defesa na PCLD, 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 LD? Os objetivos, tanto geral como específico, são, respectivamente, identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na LD, e identificar possíveis aplicações dos criptoativos nos crimes de LD.

Os criptoativos estão em contínua evolução, e as expectativas e experiências de partes interessadas podem mudar de acordo. Profissionais da contabilidade precisam ficar a par dos desenvolvimentos dos criptoativos e considerar as implicações desses desenvolvimentos, como a inovação na prática de LD, justificando, assim, a realização da presente pesquisa. Sua relevância 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 PCLD. 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 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 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 PLD-FT e experiência com criptoativos, com a finalidade de seguir uma ABR para a profissão contábil.

2 REFERENCIAL TEÓRICO

Nesta seção são abordadas as bases teóricas que sustentam o estudo proposto, cuja intenção é fornecer os subsídios mínimos para a compreensão da pesquisa e seu contexto.

2.1 Criptoativos

Não há uma definição única para os criptoativos, variando significativamente em cada país e contexto, devido sua fase inicial de desenvolvimento e seu acelerado processo de mudanças. Sua definição está numa 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). Abrangem todos os ativos desenvolvidos em um registro distribuídos, incluindo as criptomoedas, os *security token* e *utility/access token* (ICAEW, 2019). No presente estudo será tratado somente das criptomoedas, graças ao seu histórico de utilização em atividades ilícitas como a LD.

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 com transferências de valor digital *peer-to-peer* (P2P), sem envolver instituições terceirizadas para fins de certificação de transações (DANIEL; GREEN, 2018; GIUDICI; MILNE; VINOGRADOV, 2020). A criptomoeda BTC surgiu em 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*”, como *Monero* (XMR), *Dash* (DASH), *Zcash* (ZEC), dentre muitas outras.

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. Suas transações 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*, 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 P2P, de transferências, entre outros. 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 ENCCCLA (2017, 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*. Uma carteira 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 conectada à Internet. As entidades que fornecem carteiras de criptomoedas, os provedores de carteira (*wallet providers*), ajudam no aumento da liquidez dos criptoativos, permitindo aos usuários, *exchanges* e comerciantes realizarem mais facilmente suas operações em criptomoedas (FATF, 2014).

2.2 A responsabilidade do contador

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 atividades e profissões não financeiras designadas (APNFDs) no rol de atividades também sujeitas aos deveres de PLD e combate aos FT (CFT) (CABELLO, 2011). Tal fato ocorreu em 2003, quando o Grupo de Ação Financeira Internacional (GAFI) incluiu 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, 2020; NDUKA; SECHAP, 2021).

Os profissionais da contabilidade, como 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 três riscos principais (IFAC, 2020a): (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.

No Brasil há uma legislação específica para o assunto, a Lei nº 9.613 de 1998 (Lei de Lavagem de Dinheiro), alterada pela Lei nº 12.683 de 2012. Como primeiro dispositivo legal que tipifica o crime de LD no Brasil, a Lei de LD, em seu artigo 9º, define como um dos sujeitos submetidos às medidas de 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 PCLD (CFC, 2017).

2.3 Abordagem baseada em risco (ABR)

Conforme o GAFI, a ABR para PLD significa que as APNFDs, devem identificar, avaliar e compreender os riscos de LD a que estão expostas e tomar as medidas de PLD necessárias para mitigar e gerir os riscos de forma eficaz e eficiente (FATF, 2019). O princípio geral de uma ABR está na implantação de medidas proporcionais aos riscos identificados (FATF, 2020). Como APNFDs, os profissionais da contabilidade devem seguir uma ABR, ou seja, precisam aplicar 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, 2019). Dentre os principais elementos de uma ABR está a **Identificação e avaliação de riscos** – Identificação de riscos de LD/FT enfrentados por uma organização, considerando seus clientes, serviços e países de atuação (FATF, 2019, p. 14).

Portanto, 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 (FATF, 2019): (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, 2019; IFAC, 2020b); (ii) **Risco de cliente**: Certos tipos de clientes podem representar maior risco do que outros. O conhecimento sobre os clientes e seus negócios se desenvolverá durante 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, 2019; IFAC, 2020b); e (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, 2019).

3 METODOLOGIA

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 LD, é um tema complexo. A caracterização do estudo como exploratório geralmente ocorre quando há pouco conhecimento sobre a temática a ser abordada, e pretende-se preencher uma lacuna no conhecimento sobre essa temática, ou abordá-la por uma perspectiva diferente para gerar percepções novas e emergentes (RAUPP; BEUREN, 2013; LEAVY, 2017). Quanto ao caráter descritivo do estudo, conforme Leavy (2017), quando se deseja descrever grupos, atividades, eventos ou situações, a pesquisa descritiva é apropriada.

O estudo segue abordagem qualitativa que, segundo Sutton e Austin (2015) 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.

A pesquisa é caracterizada como uma pesquisa documental, que 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, 1995). 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. 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.

A seleção de possíveis participantes considerou a amostragem intencional, com algumas características predeterminadas pelo pesquisador, como experiência na PLD-FT e criptoativos, sendo desejável, mas não obrigatório, formação em Ciências Contábeis. Os contatos foram iniciados na data de 04/2021, com profissionais via plataforma *LinkedIn*. Por meio de seu recurso de pesquisa, procuraram-se profissionais de organizações cuja atividade estava de alguma forma relacionada aos criptoativos, conforme Rodrigues e Kurtz (2019), 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. Dentre as diferentes combinações de palavras-chave utilizadas durante os contatos para seleção de possíveis participantes da pesquisa, as combinações “contador; *bitcoin*”, “contador; BTC”, “contador; criptomoedas”, “contabilidade; *bitcoin*”, “contabilidade; *cryptocurrency*”, “contabilidade; criptomoedas; PLD” e “contabilidade; *blockchain*” foram as primeiras a serem aplicadas.

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: Elaboração própria com base nos dados da pesquisa (2023).

Os instrumentos de coleta dos dados foram a análise documental e questionário. 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. 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.

Quadro 1 – Referências relacionadas às perguntas da Parte 2 do questionário da pesquisa

Perguntas	Referências	Análise
<i>Em que medida as seguintes vulnerabilidades associadas às práticas e serviços oferecidos são exploradas nos crimes de LD com criptomoedas?</i>	CFC (2017, p. 2); FATF (2018, p. 58); FATF (2019, 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 quais estão expostos e implementar as medidas de mitigação mais apropriadas (FATF, 2019, p. 5, item 1).
<i>Qual a relevância dos seguintes fatores de risco de LD ao lidar com criptomoedas?</i>	FATF (2019, 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, 2019, p. 22, item 61).

Fonte: Elaboração própria (2023).

No questionário, o objetivo de sua aplicação foi verificar a percepção dos profissionais que atuam na área PLD-FT 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. O questionário utilizado na pesquisa 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, 2020), conforme **Quadro 1**.

Na Parte 1 (Perfil dos respondentes) do questionário, o objetivo foi a identificação qualitativa dos respondentes através de perguntas fechadas de múltipla escolha de resposta única. Na Parte 2 (Riscos e desafios de crime de LD enfrentados ao lidar com criptoativos) procurou-se obter a percepção dos respondentes por meio de perguntas do tipo matriz, com abertura para comentários.

A coleta de dados por meio de questionário teve início em 15/12/2021 e término em 20/04/2022, com aproximadamente 5% dos questionários enviados respondidos, conforme demonstrado na **Tabela 2**.

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.

Tabela 2 – 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: Elaboração própria com base nos dados da pesquisa (2023).

Os dados coletados por meio de questionários, com exceção dos comentários deixados pelos participantes no “Espaço aberto para comentários referentes à pergunta”, foram tabulados com o auxílio do *software Microsoft Excel* e organizados de forma sistematizada para análise no *software IBM SPSS*. Nesta etapa foi utilizada a análise descritiva dos dados coletado, a fim de se obter a frequência relativa percentual das percepções dos respondentes em relação a cada assertiva a eles indicadas. 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.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Na **Tabela 3** estão expostas as informações a respeito dos participantes da pesquisa.

Ao analisar o perfil dos 62 participantes, evidenciou-se que aproximadamente 67% (40% + 27%) dos respondentes possuem elevado nível de conhecimento a respeito das regras e regulamentos domésticos de AML, cerca de 56% (31% + 25%) mantem elevado nível de conhecimento a respeito das Recomendações do GAFI e em torno de 57% (26% + 31%) possuem mais de 5 anos de experiência em PLD-FT. Sobre a familiaridade dos respondentes com os criptoativos, aproximadamente 39% dos respondentes possuem bom conhecimento a respeito dos criptoativos, sendo que a maioria, cerca de 66%, têm de 1 a 5 anos de experiência com criptoativos.

Os riscos e desafios de crime de LD enfrentados ao lidar com criptoativos, foram abordados apresentando as percepções obtidas dos respondentes por meio das perguntas apresentadas a seguir:

Tabela 3 – Perfil dos respondentes

		Formação acadêmica				n	%			
Administração.						7	11%			
Ciências Contábeis.						20	32%			
Ciências Econômicas.						5	8%			
Direito.						24	39%			
Biblioteconomia*; Ciências da Computação*; Comércio Exterior*; Engenharia Civil*; Engenharia Mecânica*; Sistema de Informação*.						6	10%			
Segmento do setor de serviços ou órgão da Administração Pública que se concentra a experiência dos respondentes com PLD-FT e criptoativos						n	%			
Escritório de advocacia.						7	11%			
Escritório de contabilidade.						5	8%			
Exchange de criptoativos.						11	18%			
Instituição financeira.						23	37%			
Instituição de pesquisa**; Administração Pública (AP)**.						4	6%			
Contabilidade Forense*; Empresa EUA que paga salários em criptomoedas*.						2	3%			
Empresas de auditoria e consultoria.						4	6%			
Investigação e processamento de empresas privadas envolvidas em casos de corrupção na AP.						1	2%			
Órgão de persecução penal*; Polícia Civil – Laboratório de Tecnologia contra LD*; Polícia Federal – Setor de perícia criminal*.						3	5%			
Polícia Judiciária, Representação em Delegação Brasileira perante o GAFI.						1	2%			
Unidade de Inteligência Financeira (UIF).						1	2%			
Familiaridade	Pouca		Regular		Boa		Muito boa		Excelente	
	n	%	n	%	n	%	n	%	n	%
Regras e regulamentos domésticos de <i>anti-money laundering</i> (AML).	2	3%	4	6%	14	23%	25	40%	17	27%
Recomendações do GAFI.	7	11%	11	18%	9	15%	19	31%	15	25%
Criptoativos.	5	8%	14	23%	24	39%	11	18%	7	11%
Experiência	Até 1 ano		De 1 até 5 anos		De 5 até 10 anos		Mais de 10 anos			
	n	%	n	%	n	%	n	%	n	%
PLD-FT.	4	6%	23	37%	16	26%	19	31%		
Criptoativos.	15	24%	41	66%	6	10%	0	0%		

Legenda: Com 1 respondente: (*); Com 2 respondentes: (**).

Fonte: Elaboração própria com base nos dados da pesquisa (2023).

Em que medida as seguintes vulnerabilidades associadas às práticas e serviços oferecidos são exploradas nos crimes de LD com criptomoedas?

Na Tabela 4 são apresentados os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa sobre as vulnerabilidades associadas às práticas e serviços oferecidos que são comumente explorados por criminosos nas atividades de LD por meio do uso de criptomoedas. Todas as assertivas foram consideradas com significativo nível de ocorrência, onde as assertivas 1.6 e 1.4 são as que aparecem com maiores oportunidades de serem exploradas.

Ao analisar os comentários deixados pelos respondentes observou-se que para R1 “[...] 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”. Segundo R17, “[...] a maior vulnerabilidade seja a criação de empresas de fachada, com negociações forjadas, para fluxo de recursos ilícitos”, enquanto para R31, nas “[...] questões ligadas ao setor financeiro, [...] os casos mais clássicos para Lavagem de Dinheiro foram as empresas de consultoria de fachada e formação de empresas fantasmas [...]”.

R26 relata que a LD por meio de “[...] pagamento de serviços de assessoria/consultoria financeira e tributária associa-se a formação de empresas e trustes [...]”, quando “[...] 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” (R26). Nesse sentido, R26 ao declarar “*Desta forma, considero a opção 9.1 com frequência ocasional [...]*”, entende que a assertiva 9.1, que no presente trabalho é 1.1, guarda poucas chances de exploração por parte de clientes que procuram fazer uso indevido de serviços legítimos para fins de LD com criptomoedas.

Tabela 4 – Frequência com que as vulnerabilidades associadas às práticas e serviços oferecidos são exploradas nos crimes de LD com criptomoedas

Assertiva	1	2	3	4	5	6
1.1 Assessoria/consultoria financeira e tributária.	3%	16%	26%	23%	21%	11%
1.2 Formação de empresas e <i>trustes</i> .	5%	11%	19%	21%	27%	16%
1.3 Compra/venda de imóveis e estabelecimentos comerciais/industriais.	3%	18%	20%	30%	20%	10%
1.4 Gestão de fundos, valores mobiliários e outros ativos.	0%	23%	16%	23%	31%	7%
1.5 Prestação de serviços não presenciais (internet, correio, telefone).	5%	16%	20%	26%	20%	13%
1.6 Transferência eletrônica de fundos e valores mobiliários.	5%	11%	13%	40%	26%	5%
1.7 Realização de apresentações para instituições financeiras, com profissionais específicos como intermediários.	11%	13%	11%	15%	19%	31%
1.8 Prestação de serviços a clientes residentes no exterior.	6%	8%	23%	21%	23%	19%
1.9 Privilégio profissional legal e confidencialidade do cliente.	8%	13%	19%	23%	18%	19%
1.10 Obrigações <i>anti-money laundering</i> (AML) limitadas para Atividades e Profissões Não-Financeiras Designadas (APNFDs).	3%	8%	20%	28%	18%	23%

Legenda: 1-Numca; 2-Raramente; 3-Ocasionalmente; 4-Frequentemente; 5-Muito frequente; e 6-Não saberia optar.

Fonte: Elaboração própria com base nos dados da pesquisa (2023).

Contudo, R27 considera que “[...] *as maiores vulnerabilidades estão nos setores de assessorias, consultorias e ambientes não regulados [...]*”, devido ao fato de que “[...] *os ambientes regulados contam com robustos (mas, não por isso, absolutamente suficientes) controles de conhecimento normativo e de tendências, prevenção, monitoramento e resposta*” (R27). Da mesma forma, para R52, a prática de crimes de LD através de operações com criptomoedas está diretamente relacionada aos “[...] *sistemas de cryptocurrency de rastreabilidade e com registro em países de baixo aspecto regulatório [...]*” (R52).

Quanto à assertiva 1.3 na **Tabela 4**, R26 entende que sua ocorrência seja rara, devido a necessidade de “[...] *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*” (R26). Nesse cenário, 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 a inviabilidade de um dos possíveis caminhos para a execução dessa etapa, a declarar que “*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*” (R26). R26 discorre, ainda, sobre outro possível caminho para a execução das etapas de “*ocultação*” e “*integração*” no crime de LD, onde “[...] *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*” (R26).

De acordo com R21, “[...] *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*”, “[...] *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*” (R52). Em outras palavras,

a associação dos serviços oferecidos ao sistema financeiro tradicional com o mercado de criptomoedas criará diferentes opções de serviços antes inexistentes no cenário das medidas de AML tradicionais.

Em relação a assertiva 1.6 na **Tabela 4**, R20 expõe que “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 [...]”, e R54, sob o mesmo ponto de vista, relata que a “[...] transferência eletrônica de fundos (normalmente valores mobiliários) traz uma grande preocupação (vulnerabilidade) em razão do caráter anônimo das transferências que envolvem criptoativos”, “[...] 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” (R20).

Por consequência, R32 entende que 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 [...]”. É “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” (R21). A “[...] utilização de criptoativos para fins de lavagem de dinheiro, em sua grande maioria, está associada a pagamentos ocultos, de difícil identificação” (R11), e a existência de “[...] 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 GAFT” (R32).

Qual a relevância dos seguintes fatores de risco de LD ao lidar com criptomoedas?

Na **Tabela 5** são demonstrados os resultados obtidos a partir das assertivas indicadas aos respondentes da pesquisa acerca dos fatores de risco de LD ao lidar com criptomoedas. Todas as assertivas foram consideradas com significativo nível de relevância, onde as assertivas 2.2 e 2.5 possuem maior grau de importância.

Tabela 5 – Relevância dos fatores de risco de LD ao lidar com criptomoedas

Assertiva	1	2	3	4	5	6
2.1 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%
2.2 Clientes que conduzem seu relacionamento comercial em circunstâncias incomuns/não convencionais.	0%	0%	5%	29%	61%	5%
2.3 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%
2.4 Clientes residente em um país/região geográfica de alto risco.	2%	3%	10%	32%	48%	5%
2.5 Clientes em que o relacionamento dificulta a identificação oportuna do verdadeiro beneficiário final.	2%	0%	3%	18%	71%	6%
2.6 Serviços em relação a ofertas iniciais de moedas (<i>Initial Coin Offering – ICO</i>).	2%	6%	21%	24%	34%	13%
2.7 Cliente com beneficiário final residente em um país/região geográfica de alto risco.	2%	3%	6%	23%	61%	5%
2.8 Clientes com negócios intensivos em dinheiro/equivalente, como corretores e outros prestadores de serviços em ativos virtuais.	0%	10%	19%	23%	44%	5%
2.9 Uso de ativos virtuais em transações sem aparente motivo legal, tributário, comercial e econômico.	2%	2%	8%	23%	58%	8%

Legenda: 1-Sem importância; 2-Pouco importante; 3-Razoavelmente importante; 4-Importante; 5-Muito importante; e 6-Não saberia optar.

Fonte: Elaboração própria com base nos dados da pesquisa (2023).

Ao analisar os comentários deixados pelos respondentes é possível entender que, de acordo com 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”. “A natureza transfronteiriça dos ativos virtuais apresenta risco adicional pois aumenta o potencial de transferências de ativos de/para contrapartes e/ou jurisdições sancionadas” (R56). No entanto, R24 relata 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”. “Frequentemente os usuários maliciosos de criptomoedas utilizam exchanges e hash’s [sic] com IP’s [sic] de paraíso fiscal (suíça [sic], ilhas Cayman [sic] e etc...)” (R58). Portanto, “A geolocalização é um fator importante e relevante na prevenção à lavagem de dinheiro [...]” (R32), na medida em que “[...] nem todos os países seguem diretrizes e boas práticas de transparência, seja em moeda fiduciária ou em criptoativos [...]” (R32).

Nesse sentido, com relação a assertivas 2.1 na **Tabela 5**, R55 relata que “Em grande maioria as instituições não realizam operações com clientes que possuem fundos em jurisdição com deficiência de controles para AML”. Sinalizando, também, sobre a assertiva 2.4 na **Tabela 5**, uma vez que “O mesmo se repete para cliente residente em país de alto risco para Lavagem de Dinheiro, eles são barrados no processo de checagem de listas restritivas na abertura e manutenção da conta” (R55). Conforme R52, “[...] clientes de países de alto risco que solicitam informações sobre procedimentos de compra de imóveis [...] utilizando criptomoedas” são classificados como de alto risco. No entanto, R28 entende que “[...] existe uma preocupação exacerbada com países percebidos em alto risco, eles quase nunca aparecem, a participação é irrisória e gera trâmites quase inexistentes”.

Tendo em vista a declaração de R44, de que “O fator mais importante acredito que esteja relacionado à dificuldade de identificação do beneficiário final, especialmente quando se trata de privilégio profissional”, a assertiva 2.5 na **Tabela 5**, no entendimento de R44, é um importante fator de risco de LD ao lidar com criptomoedas, que pode aumentar quando do privilégio profissional legal. Segundo R52, os clientes familiares entre si e pessoas expostas politicamente (PEPs) são classificados como de alto risco, conforme suas próprias palavras: “Ainda, colocávamos como de alto risco clientes familiares entre si, clientes PEP [...]” (R52).

De acordo com 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”) [...]”. R26 explica que “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”. Nesse sentido, para R26 “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”.

Ainda sobre a dificuldade de rastrear transações financeiras envolvendo criptomoedas, R31 expõe que “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 [...]”. Igualmente, R37 relata que “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”. Mediante o exposto, R58 afirma que “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”.

R37 sinaliza, também, como fator de risco de LD ao lidar com criptomoedas, as “Transações de alto valor realizadas num único pagamento ou recorrentes em valores pequenos e que possam caracterizar fracionamento” (R37). Devido essas transações poderem ser realizadas entre diferentes

carteiras virtuais, R54 traz a informação de que *“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”*.

Para R20, a questão a respeito dos fatores de risco de LD ao lidar com criptomoedas *“[...] é uma questão extremamente sensível”*. De acordo com R20 *“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”*. Em outras palavras, R20 entende que numa análise ampliada, é possível concluir como inadequada, a análise isolada de cada assertiva apresentada na **Tabela 5** durante o cumprimento de uma política de PLD envolvendo criptomoedas. Desse modo, R27 explica que *“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”* (R27). No entendimento de R27, *“O papel das áreas de Governança/Compliance/Auditoria/PLD-FTP é de análise e não de julgamento”*. Para 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”*.

4.1 Discussão

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 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 1.3 *“Compra/venda de imóveis e estabelecimentos comerciais/industriais”* da **Tabela 4** 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 1.3, assim como as demais assertivas, guarde significativo nível de ocorrência, os respondentes da presente pesquisa entendem a ocorrência da assertiva 1.3 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 discussão 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 na 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, aproximadamente 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), onde os setores que envolvem transferências internacionais são considerados como vulneráveis às práticas de LD com criptomoedas, 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 2.8 “Clientes com negócios intensivos em dinheiro/equivalente, como corretores e outros prestadores de serviços em ativos virtuais” da **Tabela 5**. 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.

Sobre as questões concernentes ao risco de transação/serviços e canal de entrega associado, considera-se 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. 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 da importância da regulamentação AML/CFT ao lidar com criptomoedas. Por conseguinte, 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 de essas organizações facilitarem atividades ilícitas.

5 CONSIDERAÇÕES FINAIS

Mediante uma 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), não se repetiu, dada a predominância de respondentes com formação acadêmica em Direito, aproximadamente 39% (24/62), contra aproximadamente 32% (20/62) dos respondentes com formação em Ciências Contábeis. Por consequência, o objetivo específico de identificar possíveis aplicações dos criptoativos nos crimes de LD foi alcançado por meio da análise das percepções dos participantes da pesquisa acerca dos riscos e desafios de crime de LD enfrentados ao lidar com criptoativos. 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 significante níveis de ocorrência e relevância.

Servindo o objetivo específico de subsídio para alcançar o objetivo geral de identificar possíveis abordagens que auxiliem o profissional da contabilidade na prevenção e combate aos crimes relacionados à utilização dos criptoativos na LD, 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 apresentadas aos participantes da pesquisa, que estão diretamente relacionadas aos elementos de uma ABR, 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. 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. Esse conhecimento traz questões para uma conformidade em ALM no contexto das criptomoedas, que foram discutidas neste trabalho. 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 Provedores de Serviços de Ativos Virtuais (PSAVs), ou se envolverem com ativos virtuais 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 presente pesquisa está na possibilidade, quando do envolvimento com criptoativos, de: (i) Trazer às teorias, práticas e políticas existentes um debate mais aprofundado sobre os dilemas na PLD; (ii) Apresentar informações sobre a importância e abrangência dos elementos de uma ABR; (iii) Fornecer uma atualização sobre as causas e efeitos específicos de um ambiente de negócios cada vez mais voltado para as criptomoedas; e (iv) 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.

Como sugestão de pesquisas futuras, com vista na continuidade das pesquisas envolvendo o uso dos criptoativos nos crimes de LD, recomenda-se: (i) 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, sobre os requisitos AML; (ii) Uma análise das percepções dos profissionais da contabilidade acerca da importância da Contabilidade como instrumento de PCLD; (iii) Uma pesquisa sobre a conformidade do regime AML em diferentes países com as Recomendações do GAFI para as APNFDS, como as organizações contábeis; (iv) Procurar identificar as vulnerabilidades no regime AML do Brasil por meio da não conformidade com as Recomendações do GAFI sobre a regulamentação das APNFDS; (v) Um estudo sobre os diferentes normativos que foram emitidos pelos órgãos reguladores dos setores mais propícios para a prática de LD, como as APNFDS, em nível nacional e internacional; (vi) Um estudo sobre a possibilidade da existência de uma lacuna de conhecimento sobre o mercado de criptoativos entre os profissionais da contabilidade; (vii) Uma abordagem a respeito dos possíveis *red flag indicators* sobre LD; e (viii) Investigar deficiências como a ausência ou falha nos controles internos e governança sobre LD nas organizações contábeis.

REFERÊNCIAS

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

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.

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

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.

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. 2023.

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. 2023.

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.

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.

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.

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.

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. 2023.

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

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.

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.

ESTELLITA, H. Criptoedas 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). **Glossário**. São Paulo: ENCCLA, 2017.

FINANCIAL ACTION TASK FORCE (FATF). **Concealment of Beneficial Ownership**. Paris: FATF, 2018.

FINANCIAL ACTION TASK FORCE (FATF). **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**. Paris: FATF, 2020.

FINANCIAL ACTION TASK FORCE (FATF). **Risk-Based Approach for the Accounting Profession**. Paris: FATF, 2019.

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.

FRANCO, M. L. P. B. **Análise de Conteúdo**. 3 ed. Brasília: Liber Livro Editora, 2008.

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. 2023.

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. Pesquisa Qualitativa: tipos fundamentais. **Revista Administração de Empresas**, São Paulo, v. 35, n. 3, p. 20-29, jun. 1995.

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.

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.

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.

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, Sept. 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 FEDERATION OF ACCOUNTANTS (IFAC). **Anti-Money Laundering, The Basics: Installment 1 – Introduction to Anti-Money Laundering for Professional Accountants**. New York: IFAC, 2020a.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). **Anti-Money Laundering, The Basics: Installment 2 – A Risk-Based Approach**. New York: IFAC, 2020b.

JEANS, N. **A Tranche Too Hard?** The AML/CFT Regulation of Australian Designated Non-Financial Businesses and Professions. Melbourne: Initialism AML Compliance Solutions, 2019.

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.

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.

LEAVY, P. **Research Design – Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches**. New York: The Guilford Press, 2017.

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.

MARQUES, M. L. **Tratamento 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.

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.

MOSER, A.; KORSTJENS, I. Series: Practical guidance to qualitative research. Part 1: Introduction. **European journal of General Practice**, Abingdon, v. 23, issue 1, p. 271-273, 2017.

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. 2023.

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.

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.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB). **Audits Involving Cryptoassets Information for Auditors and Audit Committees**. Washington, DC.: PCAOB, 2020.

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.

RODRIGUES, G.; KURTZ, L. **Cryptocurrencies and anti-money laundering regulation in the G20**. Belo Horizonte: Institute for Research on Internet and Society – IRIS, 2019.

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.

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.

SHARMA, A. M. **Cryptocurrency and Financial Risks**. 2020. 191 f. Tese (Doutorado em Administração de Empresas) – Liberty University. Lynchburg, 2020.

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.

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.

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.

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. 2023.

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.

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.