



PUC-SP

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
FACULDADE DE DIREITO

ANDRÉ JUNQUEIRA KODJAOGLANIAN

CRIPTOMOEDAS COMO INSTRUMENTO DE LAVAGEM DE DINHEIRO
POR ORGANIZAÇÕES CRIMINOSAS

São Paulo

2024

ANDRÉ JUNQUEIRA KODJAOGLANIAN

**CRIPTOMOEDAS COMO INSTRUMENTO DE LAVAGEM DE DINHEIRO
POR ORGANIZAÇÕES CRIMINOSAS**

Trabalho de Conclusão de Curso
apresentado como requisito parcial para
obtenção do título de bacharel em Direito.

Orientador: Prof. Dr. Motauri Ciocchetti
de Souza.

São Paulo

2024

AGRADECIMENTOS

Agradeço sinceramente a todos que me apoiaram e me motivaram ao longo da minha jornada acadêmica. Primeiramente, sou profundamente grato aos meus pais, André e Ana Paula, por sempre me oferecerem tudo o que eu precisava para o meu desenvolvimento pessoal e acadêmico. Eles estimularam minha ambição e me deram infinitas possibilidades para alcançar tudo o que almejo.

Agradeço também ao meu irmão, Pedro, pela parceria constante; às minhas avós, Angela e Ivonne, pelo apoio e pelos conselhos valiosos; e aos meus avós já falecidos, Sebastião e Krikor, que continuam presentes em meu coração.

Aos meus amigos, expresso minha eterna gratidão pelo incentivo, apoio, lealdade, críticas construtivas, companheirismo e por terem sido meu ponto de equilíbrio em todas as fases dessa jornada. Obrigado por serem ombro amigo nos momentos difíceis e por celebrarem comigo as minhas vitórias. Vittoria Giannelli, Henrique Attuch, Walther Strupeni, Lucas Maltese, Thomas Fusco, Luca Angelis, Guilherme Naufal, João Felipe, Gabriel Casarin e Victor Jorge, vocês são fundamentais em minha vida e não teria chegado tão longe sem o apoio de todos.

Aos meus colegas de trabalho, especialmente aos meus chefes, Drs. Pedro Henrique Partata e Alice Pereira Kok, agradeço pelas inúmeras oportunidades de aprendizado e crescimento; ao meu colega de mesa e amigo, Guilherme Ferraz, por me fazer sentir parte da equipe desde o meu primeiro dia de trabalho; e à Mariana Neves, por tornar meus dias mais leves e agradáveis.

Por fim, expresso minha profunda gratidão aos professores da PUC-SP, que me orientaram ao longo de todo o curso e contribuíram de maneira significativa para minha formação acadêmica e pessoal.

RESUMO

As criptomoedas são ativos digitais desenvolvidos para funcionar como dinheiro eletrônico. Embora ainda não tenham substituído as moedas fiduciárias tradicionais, conquistaram grande popularidade, especialmente na forma de investimentos de alto risco, caracterizados por sua volatilidade e pelo significativo potencial de crescimento. A metodologia adotada neste estudo consistiu na coleta de dados sobre as estratégias utilizadas por agências de segurança pública em um contexto global para combater delitos associados às criptomoedas. Essa abordagem foi complementada por uma revisão de artigos científicos e doutrinas nacionais e internacionais já publicadas sobre o tema. O objetivo é oferecer uma introdução ao contexto histórico dos ativos digitais, esclarecer os mecanismos de transação comercial envolvidos e demonstrar como as organizações criminosas têm explorado esse ambiente virtual. Além disso, propõe-se estabelecer possíveis caminhos para a prevenção e regulamentação, baseando-se na experiência de outros países que, assim como o Brasil, enfrentam desafios semelhantes. O foco central deste trabalho é analisar as formas como o crime relacionado às criptomoedas é praticado, bem como traçar estratégias de combate e políticas criminais que possam reduzir a incidência desse delito. No quadro das finanças contemporâneas, o surgimento das criptomoedas e da tecnologia blockchain representa um marco significativo, transformando a dinâmica dos mercados financeiros e desafiando as práticas bancárias tradicionais. Essas inovações não apenas introduziram uma nova classe de ativos, mas também criaram um ecossistema repleto de oportunidades e riscos que exigem uma análise rigorosa e detalhada. O estudo explora a diversidade de métodos regulatórios, estratégias de conformidade e inovações financeiras, fornecendo insights valiosos sobre práticas bem-sucedidas que podem ser adaptadas e implementadas em diferentes nações e regiões. Essa variedade de abordagens enriquece o campo com experiências diversificadas, que podem beneficiar a formulação de políticas mais eficazes e fornecer maior suporte aos operadores do direito envolvidos nessa área, garantindo uma atuação mais informada e alinhada às necessidades contemporâneas.

Palavras-chave: Criptomoedas. Criminalidade. Combate. Regulação.

ABSTRACT

Cryptocurrencies are digital assets designed to function as electronic money. Although they have not yet replaced traditional fiat currencies, they have gained great popularity, especially as high-risk investments, characterized by their volatility and significant growth potential. The methodology adopted in this study consisted of collecting data on the strategies used by law enforcement agencies in a global context to combat crimes associated with cryptocurrencies. This approach was complemented by a review of scientific articles and national and international doctrines already published on the subject. The objective is to provide an introduction to the historical context of digital assets, clarify the commercial transaction mechanisms involved, and demonstrate how criminal organizations have exploited this virtual environment. In addition, it proposes to establish possible paths for prevention and regulation, based on the experience of other countries that, like Brazil, face similar challenges. The central focus of this work is to analyze the ways in which crime related to cryptocurrencies is practiced, as well as to outline combat strategies and criminal policies that can reduce the incidence of this crime. In the context of contemporary finance, the emergence of cryptocurrencies and blockchain technology represents a significant milestone, transforming the dynamics of financial markets and challenging traditional banking practices. These innovations have not only introduced a new asset class, but have also created an ecosystem full of opportunities and risks that require rigorous and detailed analysis. The study explores the diversity of regulatory approaches, compliance strategies and financial innovations, providing valuable insights into successful practices that can be adapted and implemented in different nations and regions. This variety of approaches enriches the field with diverse experiences, which can benefit the formulation of more effective policies and provide greater support to legal practitioners involved in this area, ensuring a more informed action aligned with contemporary needs.

Keywords: Cryptocurrencies. Crime. Combat. Regulation.

LISTA DE FIGURAS

Figura 1 – Condutas do Banco Central do Brasil diante de condutas ilícitas ou suspeitas	16
Figura 2- Número de Criptomoedas de 2013 a 2021	26

LISTA DE TABELAS

Tabela 1 - Estimativas de lavagem de dinheiro para países da OCDE em 2014 após cinco rodadas de fluxos internacionais.....	19
Tabela 2 - Tratados e acordos internacionais sobre crimes cibernéticos.	46

SUMÁRIO

1 INTRODUÇÃO	9
2.1 LEGISLAÇÃO BRASILEIRA RELACIONADA À LAVAGEM DE DINHEIRO	14
2.2 IMPACTOS SOCIOECONÔMICOS DA LAVAGEM DE DINHEIRO	17
2.3 ORGANIZAÇÕES CRIMINOSAS: CONCEITOS, FORMAÇÃO E ATUAÇÃO	20
3. CRIPTOMOEDAS: DEFINIÇÃO, FUNCIONAMENTO E TIPOLOGIA	24
3.1 REGULAÇÃO DAS CRIPTOMOEDAS NO CONTEXTO INTERNACIONAL	27
3.2 REGULAÇÃO DAS CRIPTOMOEDAS NO CONTEXTO NACIONAL	29
3.3 INTERSEÇÃO ENTRE CRIPTOMOEDAS, CRIMINALIDADE E LAVAGEM DE DINHEIRO	31
4 ESTUDO DE CASO	35
4.1 ANÁLISE DE CASOS REAIS DE UTILIZAÇÃO DE CRIPTOMOEDAS NA LAVAGEM DE DINHEIRO POR ORGANIZAÇÕES CRIMINOSAS	35
4.2 DESAFIOS ENFRENTADOS PELAS AUTORIDADES NO COMBATE DO USO DAS CRIPTOMOEDAS PARA LAVAGEM DE DINHEIRO	38
4.3 TECNOLOGIAS E FERRAMENTAS DE RASTREAMENTO	40
5 ANÁLISE CRÍTICA	44
5.1 AVALIAÇÃO DAS REGULACOES E ESFORÇOS ATUAIS	45
5.2 SUGESTOES PARA APRIMORAR A REGULAMENTACAO DAS CRIPTOMOEDAS; PARA PROFISISONAIS DO DIREITO E AUTORIDADES COMPETENTES	48
6 CONCLUSÃO	51
7 REFERÊNCIAS	53

1 INTRODUÇÃO

A escolha do presente tema para o trabalho de monografia decorre da notável ausência de regulamentação do mercado de criptomoedas no Brasil, bem como da sua viabilidade para a ocultação e dissimulação de valores ilícitos oriundos de atividades criminosas. A natureza anônima e a limitada rastreabilidade dos ativos digitais têm atraído a atenção de organizações criminosas, tanto no contexto nacional quanto internacional, configurando-se como um obstáculo significativo para as forças de segurança pública no combate à lavagem de dinheiro.

Criptomoedas são moedas digitais criadas por algoritmos de computador, que são distribuídas e transacionadas pela internet, utilizando criptografia e tecnologia de rede P2P (peer-to-peer). As criptomoedas são ativos digitais projetados para funcionar como dinheiro eletrônico. Embora ainda não tenham substituído as moedas fiduciárias tradicionais, elas ganharam popularidade, especialmente como investimentos de alto risco, conhecidos por sua volatilidade e pelo grande potencial de crescimento. O mercado de criptomoedas experimentou um crescimento impressionante em 2021, quando seu valor de mercado saltou de US\$ 400 bilhões em novembro de 2020 para US\$ 2,8 trilhões no mesmo período do ano seguinte (Johnson *et al.*, 2023).

Esse crescimento acelerado chamou a atenção de investidores ao redor do mundo. Existem diversas maneiras pelas quais os investidores podem acessar as criptomoedas, incluindo fundos negociados em bolsa (ETFs), a compra direta de moedas em plataformas de venda e, mais comumente, por meio de exchanges de criptomoedas, como Binance e Coinbase. Essas plataformas de negociação têm se tornado cada vez mais populares, com a Coinbase registrando receitas de US\$ 7,4 bilhões em 2021, superando até mesmo a Bolsa de Valores de Nova York (US\$ 7,1 bilhões) e a Nasdaq (US\$ 5,8 bilhões). Essas exchanges permitem que os usuários comprem e vendam uma ampla variedade de criptomoedas, com a Binance oferecendo suporte para mais de 600 moedas diferentes (Johnson *et al.*, 2023).

Considerando-se que se trata de um mercado relativamente novo, caracterizado por uma ampla variabilidade de ativos e sua transnacionalidade, torna-se urgente o desenvolvimento de estratégias de prevenção e regulamentação que impeçam o uso indevido dessa nova realidade por agentes criminosos.

A lavagem de dinheiro é o processo de ocultar a origem de recursos adquiridos de forma ilícita, tornando-os "limpos" ou legais. Em termos tradicionais, isso

geralmente envolve o uso de bancos e outras instituições financeiras para disfarçar a origem de fundos, enquanto no caso das criptomoedas, a ideia é muitas vezes recorrer a transações digitais para obscurecer a origem dos recursos (Zhang *et al.*, 2023; Zhang *et al.*, 2023).

Embora as criptomoedas possam ser usadas para atividades ilícitas, também existem esforços significativos para combater esse tipo de crime. Muitas jurisdições estão introduzindo regulamentações mais rigorosas sobre a identificação de usuários e a monitorização de transações (Zhang *et al.*, 2023; Zhang *et al.*, 2023).

Essas características tornam o combate à lavagem de dinheiro em criptomoedas uma tarefa desafiadora, mas não impossível. As autoridades e as empresas de blockchain estão desenvolvendo ferramentas cada vez mais sofisticadas para monitorar transações e identificar atividades suspeitas, destacando a importância da colaboração entre o setor privado e as agências governamentais (Johnson *et al.*, 2020; Zhang *et al.*, 2023)).

Com este trabalho, buscou-se oferecer uma introdução ao contexto histórico dos ativos digitais, esclarecer os mecanismos de transação comercial envolvidos e demonstrar a frequência e os métodos pelos quais as organizações criminosas exploram esse ambiente virtual.

Além disso, pretende-se estabelecer possíveis caminhos para a prevenção e regulamentação, fundamentando-me na experiência de outros países que, assim como o Brasil, enfrentam desafios semelhantes. O objetivo central deste trabalho é analisar as formas como o crime em questão é praticado, bem como traçar estratégias de combate e políticas criminais que possam reduzir a incidência desse delito.

Este estudo justifica-se pela necessidade de compreender o mercado atual das criptomoedas, verificar quais são as vantagens e desvantagens, bem como analisar, sob a perspectiva legal, de que modo esse mercado está aberto ao cometimento de atos ilícitos e que abordagens podem ser úteis para evitar que isso ocorra e se repita.

A pesquisa se baseou na análise das estratégias predominantes adotadas por países estrangeiros no combate à lavagem de dinheiro por meio de criptomoedas, destacando a importância do monitoramento do ponto de contato entre os ativos digitais e o mundo real, especialmente no momento da compra utilizando essa nova forma de pagamento. A metodologia principal consistiu na coleta de dados sobre os métodos utilizados por agências de segurança pública em um contexto global para enfrentar o

delito em análise, complementada por uma revisão de artigos científicos e doutrinas nacionais e internacionais já publicadas sobre o tema.

2. LAVAGEM DE DINHEIRO: CONCEITOS E FORMAS DE MANIFESTAÇÃO

A lavagem de dinheiro é um meio de manutenção e sobrevivência das organizações criminosas, que gera muito dinheiro a partir de diferentes atividades ilegais que elas têm que introduzir no circuito legal para poder utilizá-lo e se beneficiar dele. Portanto, a luta contra a lavagem de dinheiro tem um escopo mais amplo do que a investigação de tipos específicos de crimes. A lavagem de dinheiro tem que estar vinculada a uma atividade criminosa (tráfico de drogas, tráfico de armas, tráfico de pessoas, terrorismo, fraude fiscal, corrupção, etc.) (Sanz Bas, 2020).

O desmantelamento de uma organização criminosa, materializado apenas na prisão de indivíduos que participaram de delitos, não é a resposta mais completa e eficaz, já que as organizações se reestruturam rapidamente. Analisar, bloquear e intervir no sistema financeiro de uma organização criminosa (redes corporativas, fundos fiduciários, contas bancárias, bens móveis e imóveis, etc.) pode enfraquecer e, em alguns casos, paralisar sua atividade ilícita (Sanz Bas, 2020).

A lavagem de dinheiro pode ser definida como o processamento de produtos criminosos para disfarçar sua origem ilegal. As regulamentações que regem a lavagem de dinheiro podem ser divididas em duas; de um lado, há a preventiva, focada na não prática de infrações e, de outro, a repressiva ou punitiva, que é quando os atos praticados levam a uma infração independentemente do estágio em que o ilícito se encontra (Shier *et al.*, 2019).

Para compreender o crime em análise, é necessário saber que se trata de um crime com diferentes fases desde o momento em que a organização criminosa dispõe do dinheiro em efetivo até que este seja lavado e posto em circulação. A doutrina aceita a divisão teórica da operação de lavagem de capitais em três fases, concordando também que muitas vezes tal divisão pode parecer irreconhecível (Nanez Alonso *et al.*, 2021).

As fases se sobrepõem, são simultâneas e desordenadas, com os métodos de lavagem se tornando cada vez mais complexos, e algumas das fases podem ser repetidas. A doutrina, sobre Lavagem de Dinheiro concorda que esse crime geralmente se desenvolve nos três estágios seguintes: Primeiro, colocação; segundo, estratificação ou intercalação ou diversificação ou conversão; e finalmente, integração ou investimento (Nanez Alonso *et al.*, 2021). As três fases são brevemente descritas a seguir:

Colocação: É a primeira etapa do processo de lavagem, na qual o dinheiro “sujo”, seja em espécie ou materializado em qualquer tipo de bem obtido ilicitamente, muda de local, ficando fora do controle das autoridades (Nanez Alonso *et al.*, 2021).

Layering ou intermixing ou diversificação ou conversão: Esta é a segunda etapa do processo de lavagem de dinheiro e consiste em intermixar o dinheiro ou bens em vários negócios e instituições financeiras. O dinheiro é transportado para outros lugares para disfarçar sua origem ilícita. O importante aqui é adquirir ativos para transferi-los ou trocá-los com outros de origem lícita. Nesta etapa, uma vez que o dinheiro entra nos circuitos financeiros, são feitos movimentos para ocultar sua origem, a fim de erradicar qualquer possível vínculo entre o dinheiro colocado e sua origem. As técnicas mais frequentes são enviar o dinheiro para paraísos fiscais ou centros offshore, para garantir que os fundos circulem por diferentes países, instituições e contas mantidas por diferentes pessoas físicas ou jurídicas (Nanez Alonso *et al.*, 2021).

Integração ou investimento: Esta é a última etapa do processo de lavagem de dinheiro. O dinheiro das atividades criminosas é usado para negócios financeiros, que podem ser legítimos. Nesta etapa, são feitos investimentos comerciais, são concedidos empréstimos a pessoas físicas, são adquiridas mercadorias e são realizadas todo tipo de transações por meio de registros contábeis e fiscais, que justificam o capital de forma legal, dificultando o controle. Portanto, o dinheiro é recolocado na economia, com aparência de legalidade. Nesta fase, uma vez que o capital foi colocado e estratificado, o dinheiro retorna ao circuito financeiro legal misturado a outros elementos lícitos, dando-lhe assim a aparência de legalidade (Albrecht *et al.*, 2019; Nanez Alonso *et al.*, 2021).

A lavagem de dinheiro constitui um dos problemas da nossa sociedade, devido às suas consequências econômicas, políticas e sociais. O desenvolvimento tecnológico é fundamental no surgimento das criptomoedas, surgindo para evitar a dependência dos sistemas financeiros tradicionais. A lavagem de dinheiro pode ser definida como o conjunto de mecanismos ou procedimentos destinados a dar a aparência de legitimidade ou legalidade a bens ou ativos de origem criminosa (Albrecht *et al.*, 2019; CHowdhury, 2019).

Com as criptomoedas, foram desenvolvidas ferramentas e serviços que podem ser utilizados para fins ilícitos. O anonimato ou pseudoanonimato (dependendo do Blockchain utilizado) na titularidade da criptomoeda, utilizando diferentes métodos como “mixers” e “exchanges”, dificultam, em alguns casos, a investigação e rastreabilidade das operações, tornando-se um agente facilitador da lavagem de dinheiro.

As principais características das criptomoedas são a segurança, a rapidez, baseadas em criptografia, pseudoanônimas, descentralizadas, a eliminação de intermediários e a facilitação de transações internacionais. Todas essas características fazem das criptomoedas um produto atrativo e útil para a lavagem de dinheiro (Albrecht *et al.*, 2019).

O tópico a seguir traz dados específicos sobre a legislação brasileira no que tange a lavagem de dinheiro.

2.1 LEGISLAÇÃO BRASILEIRA RELACIONADA À LAVAGEM DE DINHEIRO

Esforços para combater a lavagem de dinheiro se tornaram mais expressivos na década de 1980, quando a sofisticação do narcotráfico ficou mais evidente. Esse momento evidenciou a necessidade “[...] enfrentar o poderio dessas organizações por meio da identificação e do bloqueio de seus fluxos financeiros” (Mattos, 2022, p. 422).

A partir daquele momento, diversas convenções foram conduzidas e geraram documentos sobre o tema, tais como a Convenção de Viena (1988), Convenção de Palermo (2000) e Convenção de Mérida (2003), a criação do Grupo de Ação Financeira contra Lavagem de Dinheiro e Financiamento ao Terrorismo (1989), todas elas voltadas para “[...] impedir que esses grupos reciclassem o dinheiro de origem criminosa” (Mattos, 2022, p. 422).

No cenário brasileiro, a Lei 12.683/2012 alterou vários dispositivos da Lei 9.613/98, tornando-se um marco na luta contra a lavagem de dinheiro. “A principal mudança foi a extinção do rol de crimes antecedentes, o qual era taxativo (legislação de segunda geração)” (Mattos, 2022, p. 423).

A legislação em vigor no país estabelece que qualquer infração penal pode ser avaliada como antecedente em casos de lavagem (legislação de terceira geração).

Para tanto, basta que a peça acusatória aponte indícios de uma infração penal antecedente que gerou recursos, sendo dispensável a demonstração, de antes da reforma legislativa, de que tal infração constituiu alguma das puníveis no antigo rol de crimes antecedentes. O crime de lavagem de capitais pressupõe a prática de uma infração penal antecedente, da qual se extraem bens, direitos ou valores,³⁵ os quais serão introduzidos na economia formal, como forma de ocultar/ dissimular sua origem ilícita. Afinal, se o dinheiro não é sujo, não se cogita a possibilidade de lavá-lo. O injusto possui, então, uma acessoriedade material em relação a um crime que já ocorreu e já produziu seus efeitos – obrigatoriamente financeiros. Nesse ponto, surge o primeiro elemento constitutivo do crime de lavagem de capitais: o delito antecedente (Mattos, 2022, p. 423).

Mattos (2022) afirma que o crime antecedente não exige processo autônomo, mas a certeza da ocorrência e do fato que essa conduta rendeu recursos financeiros que foram ocultados de alguma forma para, mais tarde, serem recuperados, tomando aspecto de valores lícitos. “Assim, os elementos concretos que caracterizam a infração antecedente devem ser descritos com todas as suas circunstâncias” (p. 424).

Outro componente essencial é o núcleo da ação típica (na modalidade do art. 1º, caput da Lei nº. 9.613/98), com relação direta ao ato de ocultar e/ou dissimular. Caberá à acusação evidenciar de que modo as ações típicas ocorreram (fato processual penal), vinculando o fato processual ao fato penal. Deverá ser evidenciada a relação de causalidade entre o crime antecedente e as ações de ocultação, o processo deve comprovar a infração penal antecedente e “[...] o nexo de causalidade entre os valores auferidos ilícitamente e as ações de ocultação/dissimulação. Na prática, definir esta relação não é tarefa fácil, já que, em regra, é difícil diferenciar precisamente os valores” (Mattos, 2022, p. 424).

Por fim, deve ficar evidente o dolo com foco na ocultação e dissimulação dos valores cuja origem seja criminosa, trata-se de delito necessariamente doloso, não ocorrendo responsabilização por culpa. “A rigor, deve haver por parte do sujeito ativo a consciência da origem ilícita dos valores, além da intenção voltada à prática das ações contidas no núcleo do tipo” (Mattos, 2022, p. 424).

Na condenação por lavagem de dinheiro, o infrator poderá ficar recluso pelo período de 3 a 10 anos, além de haver possibilidade de imposição de multa. As penas são maiores, de acordo com a legislação vigente, quando o crime é recorrente ou cometido por organizações criminosas. Caso o acusado opte por colaborar de forma espontânea, prestando esclarecimentos que permitam apurar outras infrações penais, identificar outros participantes ou localizar bens / valores, a redução de sua pena poderá ser de 2/3, o regime prisional poderá ser mais brando, em alguns casos a pena não será aplicada ou, ainda, será substituída por penas alternativas (TJDFT, 2016).

O Banco Central do Brasil atua diretamente visando coibir a lavagem de dinheiro, combatendo o financiamento ao terrorismo, sendo seu papel as seguintes ações:

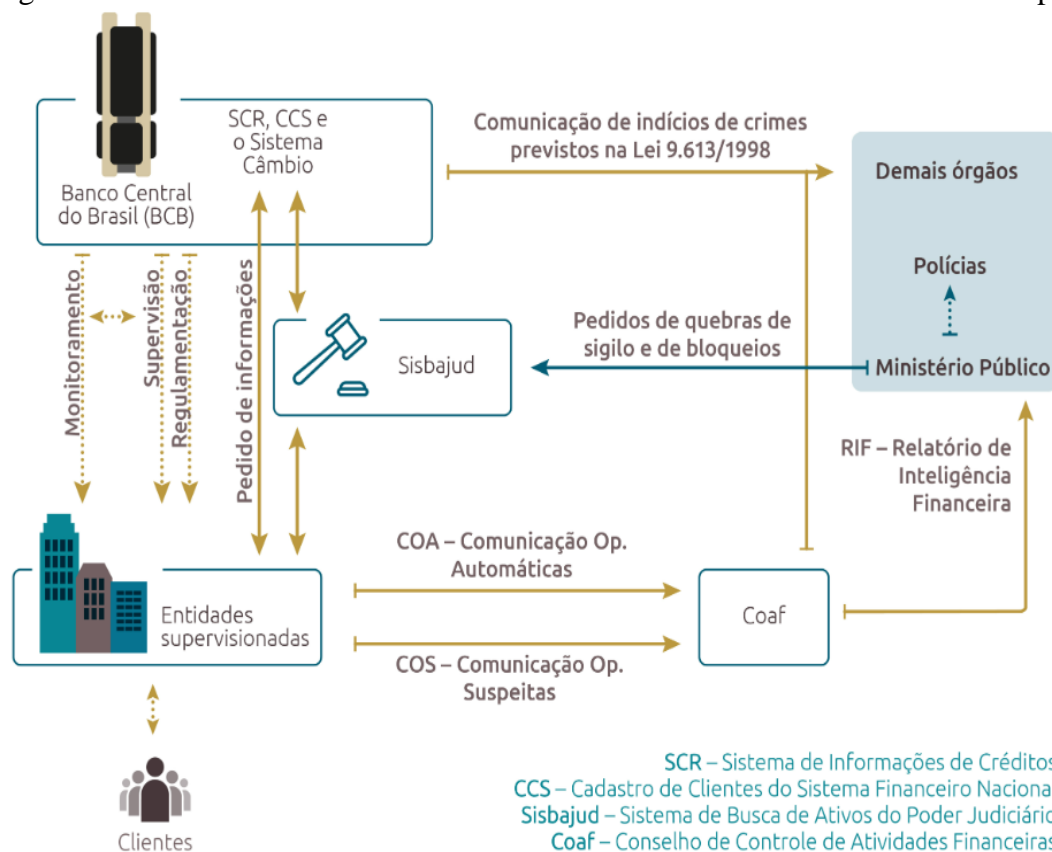
- regulamentar a Lei nº 9.613, de 1998, para que as entidades supervisionadas implementem políticas, procedimentos e controles de PLD/FT e comuniquem ao Conselho de Controle de Atividades Financeiras (Coaf) situações e operações suspeitas que envolvam seus clientes;
- regulamentar a Lei nº 13.810, de 2009, para que as entidades supervisionadas cumpram as sanções impostas pelo Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais

e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;

- monitorar e fiscalizar a aderência às normas por parte das entidades supervisionadas;
- manter o Cadastro de Clientes do Sistema Financeiro Nacional – CCS;
- comunicar:
 - ao Conselho de Controle de Atividades Financeiras (Coaf) indícios de crimes de LD/FT;
 - ao Ministério Público indícios de crimes de ação pública identificados no exercício das suas atribuições; e
 - aos órgãos públicos competentes as irregularidades e os ilícitos administrativos de que tome conhecimento.
- aplicar sanções administrativas quando identificadas infrações às normas por parte das entidades supervisionadas; e
- participar em fóruns nacionais (como por exemplo a ENCCLA) e internacionais, como é o caso do GAFI, do GAFILAT e da CPLD/FT (Brasil, 2024).
-

Quanto às ações do Banco central do Brasil para coibir ou quando da identificação de condutas suspeitas, apresenta-se a Figura 1.

Figura 1 – Condutas do Banco Central do Brasil diante de condutas ilícitas ou suspeitas



Fonte: Brasil (2024).

Verifica-se que no Brasil, além de uma legislação específica destinada aos crimes de lavagem de dinheiro, existem diferentes órgãos públicos envolvidos nos

esforços de coibir, bem como identificar condutas ilícitas ou potencialmente ilícitas, denunciando aos órgãos de investigação para que encontrem as provas e a solução para cada situação.

Na sequência são relatados dados sobre os impactos socioeconômicos da lavagem de dinheiro.

2.2 IMPACTOS SOCIOECONÔMICOS DA LAVAGEM DE DINHEIRO

Os impactos econômicos da lavagem de dinheiro afetam a economia em nível macroeconômico, podendo resultar em uma redução no crescimento econômico, diminuição do investimento estrangeiro direto e distorções nas taxas de câmbio e taxas de juros. Esses efeitos podem enfraquecer a estabilidade financeira e prejudicar a confiança nos mercados (Schmidt, 2024).

Já os impactos sociais incluem uma série de mudanças, especialmente no nível de criminalidade. A lavagem de dinheiro está frequentemente ligada a delitos antecedentes, que geram receitas ilícitas que são posteriormente ocultadas e integradas à economia legal. Além disso, essa prática pode alimentar crimes financiados por esses fundos ilícitos e atrair atividades criminosas para regiões onde a lavagem de dinheiro é prevalente (Schmidt, 2024).

Outro impacto social significativo é o financiamento do terrorismo, que é facilitado pelo processo de lavagem de dinheiro. Os efeitos incluem não apenas os custos financeiros de ataques terroristas, mas também os danos à reputação nacional e o impacto social causado pela violência e instabilidade geradas por esses atos (Schmidt, 2024).

Os impactos setoriais incluem danos à reputação do setor financeiro e de outras entidades regulamentadas, a exclusão de concorrentes legítimos, aumentos artificiais nos preços (por exemplo, preços de imóveis) e perda de receita tributária. Na esfera social, essas perdas podem levar a dificuldades de financiamento de serviços públicos que deveriam ser assegurados aos cidadãos para que tivessem melhores condições de viver com mais dignidade (Schmidt, 2024).

O principal objetivo de muitos crimes, especialmente do crime organizado, é lucrar com atividades ilícitas. Ao disfarçar a origem dos lucros criminosos por meio de transações legítimas, os infratores conseguem fazer com que esses fundos pareçam ter sido obtidos de fontes legais. Se esses recursos fossem diretamente gastos na economia formal, sem o processo de lavagem de dinheiro, seria mais fácil para as autoridades

identificarem os fundos como riqueza inexplicável, originada de atividades ilegais (Schmidt, 2024).

O grande risco para o criminoso é que os fluxos financeiros ilícitos podem ser rastreados pelas autoridades, levando à identificação da atividade criminosa. Isso aumentaria a possibilidade de confisco dos fundos ou ativos e de acusação criminal. A lavagem de dinheiro, portanto, serve como um mecanismo para reduzir esse risco, permitindo que os infratores usufruam dos lucros obtidos, minimizando a chance de perda de bens e evitando a detecção das atividades ilícitas (Loayza *et al.*, 2019; Schmidt, 2024).

Uma grande proporção de partes interessadas se concentrou nessas características da lavagem de dinheiro como centrais para a motivação para cometer crimes. A implicação é que, se a lavagem de dinheiro não for possível (ou mais difícil), o incentivo para cometer crimes e a capacidade de financiar mais crimes são reduzidos e os níveis de criminalidade diminuiriam. Por outro lado, a criminalidade aumentará quando a lavagem de dinheiro for possível. Isso tem implicações óbvias para o custo do crime subjacente (Schmidt, 2024).

Os tipos de custos que são geralmente atribuídos ao crime incluem custos médicos (por exemplo, relacionados ao uso de drogas ilícitas ou crimes contra a pessoa), as perdas diretas incorridas pelas vítimas e os custos de perda de produção. O custo de diferentes tipos de crimes varia dependendo de sua natureza e do impacto sobre as vítimas, governos e a comunidade em geral. Esses custos foram estimados e são significativos; por exemplo, os custos estimados da atividade ilícita de drogas relacionada ao crime sério e organizado na Austrália em 2016-17 foram de US\$ 9,6 bilhões, enquanto o custo da fraude organizada foi de US\$ 8,6 bilhões. Isso é antes dos custos associados às estratégias e respostas de prevenção dos setores público e privado serem incluídos. O que não está tão claro, no entanto, é até que ponto esses crimes — ou qual proporção dos custos desses crimes — podem ser atribuídos à lavagem de dinheiro (Schmidt, 2024).

A lavagem de dinheiro aumentou substancialmente nos últimos anos, tanto em economias desenvolvidas quanto em desenvolvimento. No entanto, a literatura econômica sobre os efeitos de longo prazo da lavagem de dinheiro é limitada, pois apenas alguns artigos consideram a medição e o efeito de atividades ilícitas – e transações de lavagem associadas – na acumulação de capital e no crescimento econômico (Loayza *et al.*, 2019).

Uma estimativa dos valores relacionados à lavagem de dinheiro apenas da Organização para Cooperação e Desenvolvimento Econômico – OCDE encontra-se na Tabela 1.

Tabela 1 - Estimativas de lavagem de dinheiro para países da OCDE em 2014 após cinco rodadas de fluxos internacionais.

País	Lavagem de dinheiro de crime doméstico (A)		Fluxos de dinheiro criminoso (B)		Lavagem de dinheiro estrangeiro criminoso (C)		Lavagem de dinheiro total (A + B + C)	
	Bilhões de dólares americanos	% do PIB	Bilhões de dólares americanos	% do PIB	Bilhões de dólares americanos	% do PIB	Bilhões de dólares americanos	% do PIB
Austrália	25,0	1,7	7,0	0,5	1,8	0,1	33,9	2,3
Áustria	2,5	0,6	7,7	1,7	0,7	0,2	11,0	2,5
Bélgica	8,0	1,5	22,1	4,2	2,5	0,5	32,6	6,1
Canadá	19,8	1,1	14,6	0,8	3,5	0,2	37,8	2,1
Chile	0,8	0,3	3,0	1,2	0,9	0,3	4,7	1,8
República Checa	1,1	0,5	1,8	0,9	0,3	0,1	3,1	1,5
Dinamarca	4,7	1,3	1,6	0,5	0,2	0,0	6,4	1,8
Estônia	0,2	0,6	0,6	2,3	0,1	0,2	0,8	3,1
Finlândia	2,8	1,0	2,7	1,0	0,2	0,1	5,7	2,1
França	27,9	1,0	41,3	1,4	11,2	0,4	80,4	2,8
Alemanha	55,5	1,4	12,6	0,3	1,4	0,0	69,6	1,8
Grécia	1,0	0,4	1,4	0,6	0,3	0,1	2,7	1,1
Hungria	0,7	0,5	2,8	2,0	0,3	0,2	3,8	2,7
Islândia	0,2	1,2	0,2	1,0	0,0	0,1	0,4	2,3
Irlanda	1,0	0,4	5,9	2,3	1,3	0,5	8,2	3,2
Israel	4,0	1,3	9,0	2,9	2,4	0,8	15,4	5,0
Itália	16,6	0,8	10,6	0,5	1,2	0,1	28,5	1,3
Japão	9,6	0,2	5,0	0,1	0,9	0,0	15,4	0,3
Letônia	0,1	0,5	0,7	2,2	0,1	0,3	0,9	3,0
Lituânia	0,2	0,4	0,9	1,9	0,1	0,3	1,3	2,6
Luxemburgo	0,5	0,8	2,8	4,2	0,3	0,5	3,6	5,5
México	6,2	0,5	26,7	2,0	8,4	0,6	41,3	3,1
Holanda	8,8	1,0	4,7	0,5	0,6	0,1	14,1	1,6
Nova Zelândia	3,0	1,5	2,9	1,4	0,7	0,3	6,5	3,2
Noruega	11,0	2,2	1,0	0,2	0,1	0,0	12,2	2,4

País	Lavagem de dinheiro de crime doméstico (A)		Fluxos de dinheiro criminoso (B)		Lavagem de dinheiro estrangeiro criminoso (C)		Lavagem de dinheiro total (A + B + C)	
	Bilhões de dólares americanos	% do PIB	Bilhões de dólares americanos	% do PIB	Bilhões de dólares americanos	% do PIB	Bilhões de dólares americanos	% do PIB
Polónia	4.1	0,8	4.7	0,9	0,6	0,1	9.4	1.7
Portugal	0,9	0,4	7.4	3.2	1.5	0,6	9.7	4.2
Eslováquia	0,3	0,3	1.6	1.6	0,2	0,2	2.1	2.1
Eslovênia	0,3	0,5	0,8	1.6	0,1	0,2	1.2	2.3
Coréia do Sul	1.8	0,1	4.7	0,3	0,7	0,0	7.2	0,5
Espanha	6.5	0,5	16,5	1.2	4.7	0,3	27,6	2.0
Suécia	12.7	2.2	2.8	0,5	0,2	0,0	15.8	2.8
Suíça	11.3	1.6	13.3	1.9	1.6	0,2	26.1	3.7
Peru	1.1	0,1	10.3	1.1	2.3	0,2	13.7	1.5
Reino Unido	37.2	1.2	74,4	2,5	17.8	0,6	129,4	4.3
Estados Unidos	157,8	0,9	66,4	0,4	17.9	0,1	242,1	1.4
Total da OCDE	445,1	0,9	392,5	0,8	87,2	0,2	924,9	1.9
Total mundial	540,6	0,7	1433,6	1.8	358,4	0,5	2332,6	3.0

Fonte: Ferwerda *et al.* (2020)

Estimado pelos autores. Note que os fluxos totais (1433,6 bilhões) são, por definição, 4 vezes o valor total da lavagem de dinheiro criminoso estrangeiro (358,4 bilhões).

É preciso compreender que a lavagem de dinheiro não gera impactos em apenas um setor da sociedade, assim, não repercute apenas a economia, mas pode ser amplamente prejudicial para variadas áreas, dificultando o desenvolvimento local, regional e nacional, em alguns casos com danos que chega à esfera internacional. A seguir são abordadas as facções criminosas, com dados sobre conceitos, sua composição e o modo como atuam.

2.3 ORGANIZAÇÕES CRIMINOSAS: CONCEITOS, FORMAÇÃO E ATUAÇÃO

Em todo o mundo ocorrem práticas relacionadas ao crime organizado, sempre com o intuito de obtenção de lucros que financiam a expansão dessas atividades, tanto dentro das fronteiras da não quanto para outros locais.

O crime organizado é uma questão complexa e multifacetada que afeta sociedades em todo o mundo. As organizações criminosas operam com o objetivo de obter lucros, o que, por sua vez, financia a expansão de suas atividades. Essas organizações são caracterizadas por uma estrutura hierárquica e divisão de tarefas, permitindo que cada membro compreenda seu papel e valor dentro do grupo, o que pode levar a um aumento na gravidade de suas ações.

As atividades do crime organizado são diversas e se adaptam a diferentes contextos, especialmente quando os grupos percebem oportunidades e se sentem seguros em suas operações. Essa criminalidade tende a ocorrer de forma discreta, com poucos indivíduos fora do círculo de interesse conhecendo a identidade dos membros ou como interagir com eles.

O impacto do crime organizado nas sociedades é significativo, comprometendo a segurança pública e a ordem social, além de dificultar o desenvolvimento saudável das comunidades. Portanto, esforços para combater essa criminalidade são essenciais, pois resultam em benefícios diretos para os cidadãos e para a coletividade (Nucci, 2015).

A implementação de leis rigorosas e claras é fundamental para que um país possa efetivamente enfrentar o crime organizado. Embora existam dispositivos legais que abordam essa questão desde o Código Penal de 1940, a introdução de definições e penas mais severas em 2013, através da Lei n. 12.850, representa um avanço importante nesse combate.

Conforme mencionado por Nucci (2015, p. 12), é crucial que as nações reconheçam a gravidade do crime organizado e adotem medidas eficazes para sua erradicação, promovendo assim um ambiente mais seguro e estável para todos.

A organização criminosa é a associação de agentes, com caráter estável e duradouro, para o fim de praticar infrações penais, devidamente estruturada em organismo pré-estabelecido, com divisão de tarefas, embora visando ao objetivo comum de alcançar qualquer vantagem ilícita, a ser partilhada entre os seus integrantes.

A Lei n. 12.850, de 2013, representa um marco significativo no combate ao crime organizado no Brasil, ao estabelecer definições claras e específicas sobre organizações criminosas. Essa legislação não apenas define os conceitos relacionados a essas organizações, mas também estabelece sanções rigorosas para seus integrantes e lideranças, levando em consideração a gravidade das ações cometidas.

Um aspecto importante da lei é que ela também penaliza aqueles que atuam para encobrir ou proteger essas organizações, garantindo que todos os envolvidos, direta ou indiretamente, sejam responsabilizados. Além disso, a legislação prevê penas mais severas para casos que envolvem crianças e adolescentes, a participação de funcionários públicos e a conexão entre diferentes grupos criminosos, refletindo uma preocupação com a gravidade e a complexidade do crime organizado (Lima, 2017).

As lacunas que existiam na legislação anterior a 2013 foram abordadas, permitindo que a lei respondesse de forma mais eficaz às demandas da sociedade por um sistema legal que combata efetivamente o crime organizado. Essa evolução legislativa é um passo importante para fortalecer a segurança pública e a ordem social no país.

Conquanto a revogada Lei 9.034/95 definisse e regulasse meios de provas e procedimentos investigatórios referentes a ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo (art. 1º, caput), não havia, no bojo da referida lei, uma definição legal e organizações criminosas, razão pela qual tal diploma normativo sempre teve aplicação restrita às quadrilhas (CP, antiga redação do art. 288) e às associações criminosas (v.g., Lei nº 11.343/2006, art. 35; Lei nº 2.889/1956, art. 2º) (Lima, 2017, p. 663).

A erradicação das organizações criminosas representa um desafio significativo em escala global, uma vez que essas entidades operam em diversas regiões e têm uma longa história de adaptação às mudanças sociais e aos esforços de combate às suas atividades. A corrupção, em particular, tem se intensificado em muitos países, incluindo o Brasil, levando a população a demandar reformas no sistema jurídico. Essa pressão social visa criar um ambiente legal mais robusto que minimize as oportunidades para a atuação dessas organizações, com o objetivo final de sua eliminação.

As mudanças no ordenamento jurídico são vistas como essenciais para enfrentar a complexidade do crime organizado e a corrupção, refletindo a necessidade de um compromisso contínuo e coordenado entre governos, instituições e a sociedade civil para efetivamente dismantelar essas redes criminosas (Lima, 2017).

A LOC está dividida em três capítulos, contendo 27 artigos: • Capítulo I: cuida do conceito de organização criminosa, traz um tipo penal específico e apresenta efeitos da condenação criminal (arts.1º e 2º); • Capítulo II: trata da investigação e dos meios de obtenção da prova e cria novas condutas típicas relacionadas com condutas que dificultem a investigação (arts.3º a 21); • Capítulo III: estabelece as disposições finais (arts.22 a 27) (Capez, 2017, p. 263).

É verdade que tanto o Brasil quanto outros países enfrentam um longo caminho até a eliminação completa do crime organizado. No entanto, a implementação de leis mais

claras e penas mais severas representa um avanço significativo na luta contra essas organizações. Esses esforços legislativos visam não apenas dismantelar as estruturas criminosas, mas também proteger a sociedade dos abusos que elas perpetuam.

A crescente conscientização sobre a gravidade do crime organizado e a corrupção, juntamente com a pressão da sociedade por mudanças, tem levado a um fortalecimento das políticas de combate a essas práticas. Embora a erradicação total ainda seja um objetivo distante, os progressos feitos até agora indicam um comprometimento em enfrentar esses desafios de forma mais eficaz e coordenada.

3. CRIPTOMOEDAS: DEFINIÇÃO, FUNCIONAMENTO E TIPOLOGIA

David Chaum criou o criptosistema de dinheiro eletrônico em 1983. Doze anos depois, ele criou o DigiCash, outro sistema de criptografia, para ocultar transações financeiras. Wei Dai empregou o criptosistema para criar um novo mecanismo de pagamento com uma característica primária de descentralização em 1998, o mesmo ano em que a palavra “criptomoeda” surgiu pela primeira vez (Zhang *et al.*, 2023).

A primeira e mais proeminente criptomoeda é o Bitcoin, lançado por Satoshi Nakamoto inventou o Bitcoin e disponibilizou o código-fonte para o mundo. Bitcoin, altcoins e tokens são as três principais criptomoedas que estão ativamente ativas no mercado. A tecnologia de criptomoeda está levando os mercados financeiros um passo mais perto do futuro ao descentralizar o dinheiro e liberá-lo das estruturas de poder hierárquicas. Com a tecnologia de criptomoeda, consumidores e empresas executam transações digitalmente por meio de uma rede ponto a ponto (Zhang *et al.*, 2023).

As criptomoedas podem ser compreendidas como ativos digitais desenvolvidos visando seu uso como meio virtual de troca, são descentralizadas, assim, podem ser transacionadas ponto a ponto sem um administrador central. A propriedade e as transações de ativos de criptomoeda são criptografadas e armazenadas em bases eletrônicas virtuais. Nessa sistemática, vários usuários operam e protegem coletivamente a carteira de negócios, permitindo controle descentralizado e manutenção de registros (Johnson *et al.*, 2020).

Bitcoin (BTC) é a maior e mais conhecida criptomoeda, todavia é preciso ressaltar que existem inúmeras outras moedas, cada uma delas com preços ou valor total (capitalização de mercado) variáveis. Os preços podem ser altamente voláteis, com oscilações de 40% em um único dia e retornos de 100-1000x observados em dias ou meses (Delfabro *et al.*, 2021).

A partir dessa tecnologia os desenvolvedores puderam criar diversos descentralizados, especialmente na área de finanças, disponibilizando instrumentos financeiros sem a necessidade de intermediários. As criptomoedas impulsionam as economias por meio dos aplicativos relacionados, atraindo grandes investimentos e atenção como resultado (Johnson *et al.*, 2020).

O interesse em criptomoedas tem relação com sua capitalização no mercado global, ultrapassando três trilhões de dólares americanos em 2021, podem ser comercializadas em bolsas de valores, permitindo que os usuários comprem e vendam

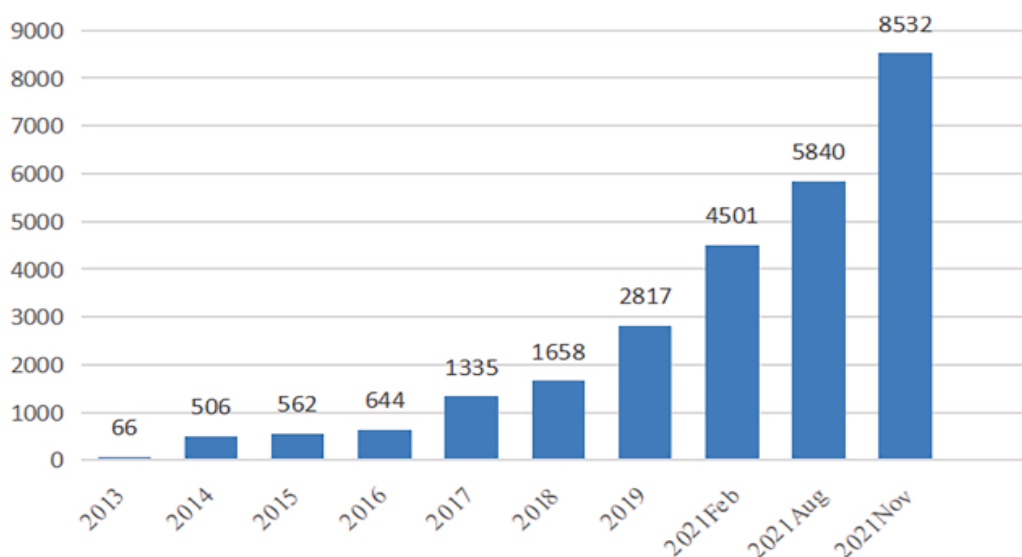
uma variedade de ativos de criptomoeda, de forma contínua e remota, quando for de interesse dos investidos, 24 horas por dia, 7 dias por semana, já que os mercados de criptomoedas e os aplicativos móveis estão sempre disponíveis para negócios (Johnson *et al.*, 2020).

Há que se considerar, porém, que esses aplicativos de negociação podem levar os usuários a se envolver em padrões de negociação arriscados, que lembram jogos de azar. Um exemplo proeminente é a negociação alavancada, oferecida em muitas bolsas, que permite que os traders aumentem o tamanho de sua posição tomando dinheiro emprestado de terceiros. Embora isso amplifique os retornos potenciais, também aumenta o potencial de perda (Johnson *et al.*, 2020).

Sobre o tema, Delfabro *et al.* (2021) enfatizam que ao mesmo tempo em que a criptomoeda adentrou ao mercado financeiro para se tornar um facilitador das operações de mercado nas mais diversas áreas, no âmbito social trouxe problemas consideráveis, levando-se em consideração que sua compra, venda e outras negociações desses ativos em plataforma vistorias podem se tornar um vício para indivíduo com propensão de vício em jogos.

No curto período desde seu nascimento, o mercado de criptomoedas experimentou um crescimento exponencial e popularidade generalizada (Figura 2). Nos últimos anos, as criptomoedas cresceram em popularidade e receberam atenção da mídia global, atraindo investidores, acadêmicos, governos, reguladores e especuladores. O futuro do Bitcoin, ou de qualquer criptomoeda, não se limita a nenhuma disciplina em particular; em vez disso, ele transcende cada domínio (Zhang *et al.*, 2023).

Figura 2- Número de Criptomoedas de 2013 a 2021



Fonte: Zhang *et al.*, (2023).

Estima-se que até 10% do PIB global será armazenado e transacionado via DLT até 2027, com o mercado de transações de criptoativos pelos aplicativos virtuais com o potencial de atingir US\$ 24 trilhões até aquele ano (Tummala, 2020).

Embora a propriedade de criptomoedas não seja tão prevalente quanto os investimentos tradicionais mais estabelecidos, como ações, centenas de milhões de investidores globalmente entraram neste mercado cada vez mais popular, estimulando os ativos criptográficos a um valor coletivo de mais de três trilhões de dólares em 2021. Apesar dos potenciais riscos financeiros para investidores individuais, bem como dos recentes colapsos em larga escala de empresas e mercados de câmbio de criptomoedas (por exemplo, FTX), muitas pessoas continuam a investir e negociar esse tipo de ativos, vendo-os como uma maneira fácil de ganhar dinheiro rápido com investimentos (Faverio; Massarat, 2022; Royal, 2023).

Zhang *et al.* (2020) esclarecem que os dados atuais apontam que investidores negros e hispânicos, que tradicionalmente se mantiveram afastados do mercado de ações, tem visto as moedas digitais mais atrativas devido ao seu potencial para lidar com a desigualdade. Uma pesquisa de 17 de agosto de 2021 aponta que 23% dos negros e 17% dos hispânicos, em comparação com 11% dos americanos brancos, estão atualmente investindo em ativos digitais.

Os dados apresentados evidenciam que as criptomoeda podem ser usadas de forma bastante efetiva para a economia em diferentes áreas, todavia, ao mesmo tempo podem ser utilizadas de forma ilícita ou para o financiamento de atividades ilícitas,

considerando-se a falta de controle absoluto de uma agência estatal, como o Banco Central de cada país. Diante disso, a seguir aborda-se a regulação das criptomoedas no contexto internacional.

3.1 REGULIZAÇÃO DAS CRIPTOMOEDAS NO CONTEXTO INTERNACIONAL

Os criptoativos estão sendo cada vez mais integrados em aplicativos de serviços financeiros para permitir transações quase em tempo real, registro preciso de dados e processos de pagamento mais eficientes. No entanto, uma das principais barreiras para implementar esses ativos é a falta de segurança jurídica (Dutch Banking Association, 2020).

O fato é que qualquer tipo de atividade financeira deve ser regida por leis e normas por meio da qual seja priorizada a proteção dos direitos das partes envolvidas nesses mercados. Além disso, existem deveres a serem cumpridos e a existência de leis evita que esses deveres sejam ignorados.

Em alguns países, as dificuldades em regular as atividades envolvendo criptomoedas são consideradas tão negativas que essas transações foram banidas, tendo-se como exemplo a China, Índia, Egito, entre outras. Todavia, muitos países reconheceram o potencial dessas transações de fomentar a economia e a participação no mercado de valores que nos moldes tradicionais seriam impossíveis para públicos menos favorecidos. Os EUA são pioneiros no desenvolvimento de leis nessa área, com a "Crypto-Currency Act of 2020", cujo texto apresenta uma definição legal dos criptoativos, bem como os órgãos que avaliam essas atividades para evitar fraudes (Joma, 2022).

Em 25 de setembro de 2018, o *Kammergericht Berlin* (o mais alto tribunal de Berlim) anulou a posição do *Bundesanstalt für Finanzdienstleistungsaufsicht* (BaFin, o regulador financeiro federal alemão) sobre criptoativos em um julgamento criminal referente a uma bolsa de Bitcoin não autorizada. Em seu julgamento, o tribunal decidiu que os bitcoins não eram instrumentos financeiros nem unidades de conta, pois não tinham as características definidoras de tais (por exemplo, emissão por uma entidade conhecida e validade estatutária como moeda com curso legal). A negociação de bitcoins, portanto, não exigia autorização do BaFin. O tribunal fez algumas declarações diretas criticando o BaFin por ultrapassar os limites de sua competência ao adotar uma interpretação tão ampla. Dado que o caso foi decidido na jurisdição criminal do tribunal,

o BaFin não está vinculado ao julgamento do *Kammergericht* e atualmente é incerto como os bitcoins serão caracterizados na lei alemã (Blandin *et al.*, 2020).

Dados mostram que, em média, há três órgãos nacionais distintos por jurisdição que emitiram declarações oficiais, incluindo advertências, sobre criptoativos. No entanto, diferenças significativas podem ser observadas entre jurisdições; enquanto em alguns países uma única autoridade reguladora emitiu declarações, esse número sobe para seis em outros países (Blandin *et al.*, 2020).

A razão reside principalmente no fato de que as atividades de criptoativos podem cair dentro do perímetro regulatório de vários reguladores, como na Austrália, onde quatro reguladores têm mandatos para garantir a estabilidade do mercado financeiro. Mesmo quando os reguladores têm objetivos estatutários diferentes, seus poderes regulatórios sobre tais atividades podem se sobrepor. Em tais casos, os reguladores podem escolher cooperar entre si (Blandin *et al.*, 2020).

Embora a cooperação possa ser informal ou *ad-hoc*, os reguladores que enfrentam novos mercados ou novos poderes podem formalizar seus esforços colaborativos por meio de grupos de trabalho, consultas ou forças-tarefa. O Reino Unido, por exemplo, estabeleceu a “Força-Tarefa de Criptoativos do Reino Unido” para coordenar os esforços do regulador financeiro (a Financial Conduct Authority - FCA), o banco central (o Bank of England - BoE) e o Ministério das Finanças (Her Majesty’s Treasury). Os benefícios esperados da coordenação incluem compartilhamento de informações, aprendizado e a reunião de recursos, além de potencialmente fornecer um maior grau de segurança jurídica para a indústria e os consumidores (Blandin *et al.*, 2020).

Uma análise de 40 jurisdições sugere que os bancos centrais geralmente foram o primeiro tipo de autoridade a emitir um aviso ou declaração sobre criptoativos (40% das jurisdições cobertas), seguidos por departamentos governamentais como o Ministério das Finanças (17%) e órgãos de supervisão financeira (17%). Essa observação talvez não seja surpreendente, dado que a primeira geração de criptoativos foi frequentemente projetada e comercializada como “moedas” digitais não soberanas, levando os bancos centrais a esclarecer as leis de curso legal (Blandin *et al.*, 2020).

Compreende-se, assim, que a análise da regulação dos criptoativos no contexto internacional é difícil e muito ampla, considerando-se que algumas nações já trabalham para desenvolver e aplicar leis nesse sentido, enquanto outras ainda não possuem dispositivos legais nesse sentido. A seguir aborda-se a regulação das criptomonedas no cenário brasileiro.

3.2 REGULACÃO DAS CRIPTOMOEDAS NO CONTEXTO NACIONAL

É essencial destacar que o Brasil demorou mais tempo do que algumas nações para desenvolver uma legislação relacionada aos criptoativos, o que indica que o tema, na esfera legal, ainda demanda de esclarecimentos e maior investimento em pesquisas e compreensão para que se chegue a uma regulação verdadeiramente ampla e efetiva (Joma, 2022; Martin, 2023).

Apesar dessa demora, o Brasil ainda está à frente de muitas nações nas quais negócios com criptoativos ocorrem e que desejam, em algum momento, regulamentar essas atividades por meio de legislação específica. Assim, os investidores brasileiros poderão se sentir mais seguros caso desejem investir nesse ramo da economia (Martin, 2023).

Em 20 de junho de 2023 foi regulado o Marco Legal das Criptomoedas, a chamada lei das criptomoedas, que havia sido aprovado em 2022 (*vacatio legis* de 180 dias).

Em 30 de novembro de 2022, a Câmara dos Deputados aprovou a versão final do Projeto de Lei nº 4401/2021 (antigo PL 2303/2015).² Apelidado de “Lei do Bitcoin”, de “Lei dos Criptoativos” ou de “Marco Jurídico das Criptomoedas”, o projeto de lei foi sancionado pelo presidente da República, sem vetos, instituindo o marco regulatório para a criptoconomia no Brasil, um quadro jurídico essencial para a inovação e a segurança jurídica no setor e para a prevenção à lavagem de capitais por meio de ativos virtuais (Aras, 2023, p. 268).

Observa-se que a aprovação e atuação de uma legislação especificamente direcionada para a questão das criptomoedas era uma questão verdadeiramente necessária para regular essas atividades no país. Seu enfoque está na regulação das atividades com criptoativos, bem como na proteção dos consumidores que adentram a esse mercado. Com o Marco Legal, há verdadeira proteção jurídica aos integrantes dos mercados de criptomoedas no país (Aras, 2023; Martin, 2023).

A Lei n. 14.478 (Brasil, 2022) define como ativos virtuais:

Art. 3º Para os efeitos desta Lei, considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento, não incluídos:

I - moeda nacional e moedas estrangeiras;

II - moeda eletrônica, nos termos da Lei nº 12.865, de 9 de outubro de 2013;

III - instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e

IV - representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros.

Parágrafo único. Competirá a órgão ou entidade da Administração Pública federal definido em ato do Poder Executivo estabelecer quais serão os ativos financeiros regulados, para fins desta Lei.

Compreende-se que as criptomoedas, juntamente com outras atividades eletrônicas que envolvem valores, estão nos ativos virtuais. No que tange a prestação de serviços nessa área, o texto legal define:

Art. 4º A prestação de serviço de ativos virtuais deve observar as seguintes diretrizes, segundo parâmetros a serem estabelecidos pelo órgão ou pela entidade da Administração Pública federal definido em ato do Poder Executivo:

I - livre iniciativa e livre concorrência;

II - boas práticas de governança, transparência nas operações e abordagem baseada em riscos;

III - segurança da informação e proteção de dados pessoais;

IV - proteção e defesa de consumidores e usuários;

V - proteção à poupança popular;

VI - solidez e eficiência das operações; e

VII - prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais (Brasil, 2022).

Para que as prestadoras de serviços possam atuar nessa área, deverão obter uma autorização de órgãos federais, o Banco Central é o órgão regulador,

Art. 8º As instituições autorizadas a funcionar pelo Banco Central do Brasil poderão prestar exclusivamente o serviço de ativos virtuais ou cumulá-lo com outras atividades, na forma da regulamentação a ser editada por órgão ou entidade da Administração Pública federal indicada em ato do Poder Executivo federal (Brasil, 2022).

A Comissão de Valores Mobiliários (CVM) supervisiona criptoativos que tenham características de valores mobiliários. Foram definidas, ainda, severas sanções em caso de fraudes e crimes financeiros relacionados aos ativos virtuais. Com isso, eleva-se a segurança jurídica e os investidores têm seus direitos muito mais protegidos (Martin, 2023).

Sobre os órgãos reguladores, a legislação estabelece.

Art. 7º Compete ao órgão ou à entidade reguladora indicada em ato do Poder Executivo Federal:

I - autorizar funcionamento, transferência de controle, fusão, cisão e incorporação da prestadora de serviços de ativos virtuais;

II - estabelecer condições para o exercício de cargos em órgãos estatutários e contratuais em prestadora de serviços de ativos virtuais e autorizar a posse e o exercício de pessoas para cargos de administração;

III - supervisionar a prestadora de serviços de ativos virtuais e aplicar as disposições da Lei nº 13.506, de 13 de novembro de 2017, em caso de descumprimento desta Lei ou de sua regulamentação;

IV - cancelar, de ofício ou a pedido, as autorizações de que tratam os incisos I e II deste caput; e

V - dispor sobre as hipóteses em que as atividades ou operações de que trata o art. 5º desta Lei serão incluídas no mercado de câmbio ou em que deverão submeter-se à regulamentação de capitais brasileiros no exterior e capitais estrangeiros no País.

Parágrafo único. O órgão ou a entidade da Administração Pública federal de que trata o caput definirá as hipóteses que poderão provocar o cancelamento previsto no inciso IV do caput deste artigo e o respectivo procedimento (Brasil, 2022).

Aras (2023) esclarece, ainda, que a Lei das Criptomoedas alterou a Lei nº 9.613/1998, definindo nova causa especial para aumento de pena. Nesse sentido, no §4º do art. 1º da Lei de Lavagem de Dinheiro, haverá majoração da pena em casos nos quais ocorrer o crime de lavagem de capitais utilizando-se o infrator de ativo virtual para essa finalidade.

A pena mais alta se justifica pelo aumento da dificuldade de rastreamento e de arresto ou sequestro de ativos virtuais para eventual confisco, assim como pela extrema volatilidade de tais ativos e pela relativa anonimização de operações que poderão ocorrer de modo descentralizado, em qualquer ponto do globo. A imputação dessa nova causa especial de aumento somente é possível para condutas ocorridas a partir de 20 de junho de 2023, em função da irretroatividade da lei penal mais gravosa (Aras, 2023, p. 279).

O fato é que o Brasil tem caminhado de forma efetiva no sentido de formular uma base legal sólida para reger a questão dos ativos virtuais, como as criptomoedas, elevando a proteção dos consumidores e a expansão da segurança no mercado, além de estabelecer penas severas para crimes cometidos por meio dessas inovações de difícil rastreamento.

3.3 INTERSEÇÃO ENTRE CRIPTOMOEDAS, CRIMINALIDADE E LAVAGEM DE DINHEIRO

A criptomoeda tem crescido em popularidade, é uma forma cada vez mais utilizada de troca de moeda digital e investimento que não é produzida, controlada ou apoiada por nenhum banco central ou entidade governamental. Essas moedas permitem tanto a ocorrência de negociações não regulamentadas quanto transações anônimas, o que

contribuiu, pelo menos parcialmente, para mercados de criptomoedas que são voláteis e propensos a fraudes e falhas (Shayegan *et al.*, 2022; Rosen, 2023).

Dada a volatilidade dos mercados de criptomoedas, o potencial de perda e a falta de supervisão regulatória, muitos especialistas financeiros, bem como membros do público, veem a criptomoeda como um investimento insustentável, com alguns até mesmo comparando-a a jogos de azar ou participação em um esquema Ponzi. Além disso, os governos expressaram preocupação significativa não apenas sobre a capacidade da criptomoeda de levar indivíduos à falência e perturbar os mercados financeiros mundiais, mas também suas potenciais ligações com o crime e o terrorismo (Sonkurt, 2021; Song; Chen; Wang, 2023).

Nos últimos anos, o setor de serviços financeiros tem enfrentado inúmeros desafios, principalmente devido à crise financeira, que exigiu que os bancos trabalhassem arduamente para reconquistar a confiança da sociedade. O uso de novas tecnologias é reconhecido como um método de melhoria das operações financeiras. Se devidamente regulamentados, os criptoativos podem resultar em enormes ganhos de eficiência no setor financeiro, transformando o funcionamento dos mercados financeiros para facilitar a troca de valor sem a necessidade de uma autoridade central ou intermediário.

Estima-se que a tecnologia relacionada às criptomoedas poderia reduzir os custos de infraestrutura em 30% apenas para os dez maiores bancos europeus, resultando em economias de US\$ 8 a US\$ 12 bilhões. O setor de serviços financeiros é o maior usuário mundial de TIC e mais de 5.100 tipos de criptoativos existiam em 2020. No entanto, embora a capitalização de mercado de criptoativos tenha subido para US\$ 2 trilhões em maio de 2021, ela caiu para US\$ 1,3 trilhão em agosto de 2021, destacando tanto o potencial quanto a fragilidade do mercado (Casey *et al.*, 2018; Saulnier, 2020; Kou *et al.*, 2021).

A fraude de criptomoeda se tornou uma preocupação global crescente, com vários governos relatando um aumento na frequência e nas perdas com golpes de criptomoeda. A fraude de criptomoeda se tornou uma preocupação crescente em todo o mundo. Entre 2017 e 2018, a Austrália registrou um aumento de 190% nas perdas para vítimas de golpes envolvendo criptomoedas, em 2019 os relatórios de golpes de criptomoeda triplicaram. Essa trajetória de criminosos fraudando indivíduos que compraram ou fizeram transações usando criptomoedas (usuários de criptomoedas) sugere que o espaço da criptomoeda oferece oportunidades ainda não exploradas para o crime (Trozze *et al.*, 2023).

O fato é que as operações por meio de criptomoedas podem ser mais difíceis de rastrear do que outras operações, nesse sentido, indivíduos com intenções criminosas podem acreditar que encontraram um caminho para ocultar recursos, evitando tributação adequada ou visando a lavagem de ativos (Aras, 2023).

Ocorre que os crimes cometidos a partir das criptomoedas não podem ser considerados menos graves, na verdade, seus impactos sobre o Sistema Financeiro podem ser mais expressivos do que outros crimes na área, levando-se em conta a facilidade encontrada para ocultar recursos, obter vantagens e legalizar recursos que não são legais (Aras, 2023).

Com vistas a essa realidade:

A Lei nº 14.478/2022 introduziu um novo tipo penal, supostamente de estelionato, no art. 171-A do Código Penal, com o título de “fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros”. A conduta estará configurada quando o agente “organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento.” A pena do crime do art. 171-A do CP é de reclusão, de 4 a 8 anos e multa, o que o diferencia drasticamente do estelionato, cuja escala penal é bem mais modesta, de 1 a 5 anos de reclusão na modalidade simples. Pena semelhante só vemos na fraude eletrônica do §2º-A do art. 171 do CP (Aras, 2023, p. 279).

Os antigos tipos de lavagem utilizados pelas organizações, como o uso de dinheiro em espécie, vêm evoluindo. Atualmente, existe um sistema preventivo e repressivo de lavagem de dinheiro, que impede que certas operações sejam realizadas ou, se forem realizadas, certas instituições são avisadas por meio de relatórios automáticos. São estabelecidos limites para comprar produtos e serviços por meio de dinheiro em espécie, o sistema bancário estabeleceu limites ao realizar diferentes transações, o que limita muito o possível pagamento em dinheiro. Diante dessa situação, as organizações criminosas se atualizam, ou contam com pessoal especializado, ou entram em contato com organizações dedicadas à lavagem de dinheiro. Por meio das criptomoedas, novas metodologias para lavagem de dinheiro estão surgindo, dificultando o combate dos países a esse tipo de crime organizado (Trozze *et al.*, 2023).

Os dados coletados apontam que as criptomoedas podem servir como rota para o cometimento de crimes financeiros e é preciso encontrar alternativas cada vez mais modernas e efetivas para o controle dessas operações e para a regulação da forma como as atividades nesse mercado são conduzidas.

Na sequência são elencados dados de casos nos quais as condutas criminosas de lavagem de dinheiro e ocultação de divisas foram verificadas.

4 ESTUDO DE CASO

Esta etapa do estudo tem como foco relatar casos reais de uso de criptomoedas por organizações criminosas de modo a ocultar seus ganhos e legalizar a entrada desses valores no país, ou em outros países.

4.1 ANÁLISE DE CASOS REAIS DE UTILIZAÇÃO DE CRIPTOMOEDAS NA LAVAGEM DE DINHEIRO POR ORGANIZAÇÕES CRIMINOSAS

Dados apontam que em 2021, os crimes envolvendo criptomoedas totalizaram US\$ 14 bilhões (E-investidor, 2022).

Os criminosos utilizam diferentes métodos e serviços que enviam fundos por vários endereços ou empresas para ocultar suas origens. Os ativos são então enviados de uma fonte aparentemente legítima para um endereço de destino ou uma bolsa para serem liquidados. Esse processo torna muito difícil rastrear fundos lavados de volta a atividades ilícitas (Dyntu; Dykyi, 2018).

Serviços aninhados envolvem uma ampla categoria de serviços que operam em uma ou mais bolsas. Esses serviços utilizam endereços hospedados pelas bolsas para explorar a liquidez das bolsas e capitalizar oportunidades de negociação. Algumas bolsas não exigem altos padrões de conformidade para serviços aninhados, permitindo que atores mal-intencionados os explorem para lavagem de dinheiro (Dyntu; Dykyi, 2018).

No livro-razão do blockchain, essas transações de serviços aninhados parecem ter sido conduzidas por suas contrapartes hospedeiras (ou seja, as bolsas) em vez dos serviços aninhados hospedados ou endereços de indivíduos. O tipo mais comum e notório de serviço aninhado é um corretor Over-the-Counter (OTC). Os corretores OTC permitem que os comerciantes negociem facilmente, com segurança e anonimamente grandes quantidades de criptomoeda (Dyntu; Dykyi, 2018).

Plataformas de jogos de azar são populares entre lavadores de dinheiro de criptomoedas. Os fundos são pagos na plataforma por meio de alguma combinação de contas identificáveis ou anônimas. Eles são sacados ou colocados em apostas, geralmente em conluio com afiliados (Dyntu; Dykyi, 2018).

Mixers são serviços que misturam ativos digitais de muitos endereços antes de liberá-los em intervalos aleatórios para novos endereços de destino ou carteiras, aumentando assim o anonimato. Eles são frequentemente usados para ocultar o

rastro de fundos antes que sejam transferidos para empresas legítimas ou grandes bolsas (Dyntu; Dykyi, 2018).

Transações offshore: contas offshore são usadas por criminosos para ocultar a origem dos fundos (Dyntu; Dykyi, 2018).

Serviços baseados em jurisdições de alto risco: Esses serviços estão localizados em áreas sinalizadas por deficiências em seus sistemas de Prevenção à Lavagem de Dinheiro (AML) ou Combate ao Financiamento do Terrorismo (CFT) (Dyntu; Dykyi, 2018).

Bolsas fiduciárias: as bolsas fiduciárias convertem criptomoedas em dinheiro, variando de plataformas tradicionais a peer-to-peer (P2P) ou não compatíveis e, após a conversão do dinheiro, métodos tradicionais de investigação financeira são necessários (Dyntu; Dykyi, 2018).

Troca de exchanges: os criminosos também usam diversas exchanges de criptomoedas para transferir fundos entre diferentes plataformas, dificultando o rastreamento do dinheiro (Dyntu; Dykyi, 2018).

Na sequência são elencados alguns casos de uso das criptomoedas para lavagem de dinheiro.

Em fevereiro de 2011, Ross William Ulbricht, que atendia pelo nome de guerra de “Dread Pirate Roberts”, fundou o site “Silk Road”. A Silk Road abriu com começos modestos, com cogumelos psicodélicos cultivados pelo próprio Ross listados como os primeiros itens à venda. No entanto, Ross promoveu seu site no famoso fórum bitcoin, um ato que atraiu alguns compradores para seus cogumelos, mas que acabou levando à sua queda. No final de fevereiro, vinte e oito transações de narcóticos variando de LSD a mescalina foram realizadas no site. Em dois meses, mais de mil pessoas se registraram. Os servidores da Silk Road não conseguiram lidar com o fluxo, e uma combinação de hackers e aumento do tráfego do site forçou Ross a tirar temporariamente o Silk Road do ar, para reformular e atualizar o site. O verdadeiro fluxo de usuários, no entanto, ocorreu depois que uma coluna de fofocas online, publicou uma história aprofundada sobre a Silk Road. Em poucos meses, Ulbricht recuperou seu investimento inicial e conseguiu criar um mercado virtualmente anônimo e próspero para a venda de narcóticos, completo com uma função de revisão de vendedores, semelhante à Amazon ou eBay (Pinheiro, 2023).

O BTC-e foi uma das principais formas pelas quais criminosos cibernéticos ao redor do mundo transferiram, lavaram e armazenaram os lucros criminosos de suas

atividades ilegais. O BTC-e recebeu lucros criminosos de inúmeras invasões de computador e incidentes de hacking, ataques de ransomware, esquemas de roubo de identidade, funcionários públicos corruptos e redes de distribuição de narcóticos (Pinheiro, 2023).

A Operação Pão Nosso, um desdobramento da Lava Jato no Rio de Janeiro, revelou uma descoberta inédita: pela primeira vez, a força-tarefa identificou um esquema de lavagem de dinheiro que utilizava bitcoin. A confirmação da utilização da criptomoeda foi divulgada pela Receita Federal. Esse episódio é um marco importante na investigação de crimes financeiros, evidenciando como as criptomoedas podem ser empregadas para ocultar a origem de recursos ilícitos. As autoridades estão intensificando seus esforços para monitorar e regular esse tipo de atividade, destacando a necessidade de uma abordagem mais robusta no combate à lavagem de dinheiro em ambientes digitais. A descoberta também levanta questões sobre a eficácia das atuais políticas de segurança financeira e a importância da cooperação internacional em investigar e prevenir tais crimes (Pinheiro, 2023).

A bolsa de criptomoedas Quadriga viu milhões de dólares desaparecerem logo após a morte de seu fundador, atuava como esquema Ponzi. Somente o fundador tinha acesso às contas e senhas para verificar as operações e os clientes perderam seus recursos (Pinheiro, 2023).

Na Operação Daemon foi cuidadosamente investigado um grupo suspeito de desviar mais de R\$ 1,5 bilhão em negociações de criptomoeda, em Curitiba. O montante desviado pode ser ainda maior, já que existem indícios da prática de outros crimes, como lavagem de dinheiro por meio das criptomoedas (Pinheiro, 2023).

A Exchange Bitcoin Banco (BBB) foi investigada pela Polícia Federal por suspeita de lavagem de dinheiro por meio de esquema de pirâmide financeira, os valores eram negociados em criptomoedas, dificultando o rastreamento dos mesmos. Quando os investidos não conseguiram mais sacar os lucros que haviam sido prometidos, ficou evidente a ilicitude das atividades e as investigações confirmaram essa questão (Pinheiro, 2023).

4.2 DESAFIOS ENFRENTADOS PELAS AUTORIDADES NO COMBATE DO USO DAS CRIPTOMOEDAS PARA LAVAGEM DE DINHEIRO

O processo investigatório, no presente, teve que passar por atualizações e alterações importantes, em função das mudanças tecnológicas que permitiram que os crimes tomassem novas formas, como no caso da criptomoedas. De acordo com Zumas (2020), as criptomoedas asseguram bastante privacidade para os investidores nessa tecnologia, porém, ao mesmo tempo envolvem riscos relacionados ao anonimato e à possibilidade de cometimento de crimes diversos fazendo uso dessas criptomoedas.

Horchel (2022) afirma que a sociedade atual está inserida em uma *cyber* pós-modernidade, na qual as características das relações sociais mudaram expressivamente e as tecnologias permeiam a forma como as pessoas trabalham estudam, fazem compras e realizam as demais atividades de seu cotidiano. No âmbito financeiro, com as criptomoedas, surge uma maior liberdade de seleção quanto aos modelos de investimentos, quantidades e demais especificidades. Na mesma direção, os crimes também assumiram novas características e englobam atividades ilícitas financeiras relacionadas a essa modernidade.

Para os investigadores, os desafios são amplos, como os sistemas informatizados misturam as criptomoedas, também dificultam o rastreo das mesmas, de onde vieram, para onde foram, etc. Os órgãos que investigam essas condutas necessitam de constantes esforços de atualização de conhecimentos para que possam compreender as inúmeras alterações relacionadas à circulação de ativos por meio de criptomoedas e, ao mesmo tempo, consigam encontrar caminhos pelos quais poderão encontrar os valores que são movimentados todos os dias (Horchel, 2022).

Na concepção de Rodrigues (2024), um importante desafio a ser considerado refere-se à necessidade de treinamento e desenvolvimento de conhecimentos e habilidades por parte dos investigadores para que possam se atualizar e participar adequadamente dos processos de investigação. “Tratando-se de uma tecnologia relativamente recente, que exige, em alguma medida, conhecimento técnico específico, e dadas suas características” (Rodrigues, 2024, p. 18).

Echarté-Fernandez *et al.* (2021) esclarecem que o combate ao uso de criptomoedas para lavagem de dinheiro apresenta diversos desafios para as autoridades em todo o mundo. Entre os principais desafios, destacam-se:

1. Anonimato e Descentralização: As criptomoedas, por sua natureza, oferecem um alto grau de anonimato. Isso dificulta a identificação dos usuários e a rastreabilidade das transações, tornando mais complicado para as autoridades rastrear atividades ilícitas (Echarté-Fernandez *et al.*, 2021).

2. Falta de Regulação: A regulamentação das criptomoedas ainda está em desenvolvimento em muitos países. A ausência de um marco regulatório claro pode dificultar a aplicação de leis existentes e a implementação de medidas eficazes de combate à lavagem de dinheiro (Echarté-Fernandez *et al.*, 2021).

3. Tecnologia em Evolução: O rápido avanço das tecnologias relacionadas a criptomoedas e blockchain torna difícil para as autoridades acompanharem as novas práticas e métodos utilizados por criminosos. Isso inclui o uso de técnicas como mixers e tumblers, que ofuscam a origem das transações (Echarté-Fernandez *et al.*, 2021).

4. Jurisdicionalidade: As criptomoedas operam em um ambiente global, o que significa que as transações podem cruzar fronteiras facilmente. Isso levanta questões sobre a jurisdição e a cooperação internacional, dificultando a ação coordenada entre diferentes países (Echarté-Fernandez *et al.*, 2021).

5. Capacitação e Recursos: Muitas autoridades enfrentam limitações em termos de capacitação e recursos para investigar crimes relacionados a criptomoedas. A falta de conhecimento técnico e de ferramentas adequadas pode comprometer a eficácia das investigações (Echarté-Fernandez *et al.*, 2021).

6. Evolução das Táticas Criminosas: Os criminosos estão constantemente adaptando suas táticas para explorar as vulnerabilidades do sistema financeiro e das regulamentações. Isso inclui o uso de criptomoedas em esquemas de pirâmide, fraudes e outras atividades ilícitas (Echarté-Fernandez *et al.*, 2021).

7. Percepção Pública e Aceitação: A crescente aceitação das criptomoedas como um meio legítimo de transação pode dificultar a percepção pública sobre os riscos associados ao seu uso. Isso pode levar a uma falta de apoio para medidas regulatórias mais rigorosas (Echarté-Fernandez *et al.*, 2021).

8. Desafios na Colaboração: A colaboração entre agências governamentais, instituições financeiras e empresas de tecnologia é crucial para combater a lavagem de dinheiro. No entanto, diferenças de objetivos, prioridades e abordagens podem dificultar essa cooperação (Echarté-Fernandez *et al.*, 2021).

Esses desafios exigem uma abordagem multifacetada, que inclua a criação de regulamentações adequadas, o fortalecimento da capacitação das autoridades, a promoção

da cooperação internacional e a conscientização pública sobre os riscos associados ao uso de criptomoedas.

Nesse sentido, os maiores desafios relatados englobam tanto a capacitação dos órgãos e investigadores que atuam nos processos investigatórios, como também a necessidade de tecnologias cada vez mais modernas que possam ser utilizadas para essa finalidade de modo efetivo.

As tecnologias existentes em busca do acompanhamento e controle dessas atividades são elencadas no tópico a seguir.

4.3 TECNOLOGIAS E FERRAMENTAS DE RASTREAMENTO

Os métodos tradicionais para contornar a detecção incluem misturar dinheiro ilícito por meio de negócios intensivos em dinheiro para declará-lo como renda legítima, converter os lucros em moeda estrangeira ou canalizar dinheiro por meio de contas ilícitas, cassinos, títulos ou empresas de fachada, entre outros. Todos esses métodos agora estão sendo aprimorados pela adoção generalizada de tecnologias novas e disruptivas (Teicher, 2018; Megaw, 2019).

Tecnologias disruptivas referem-se a inovações que alteram substancialmente mercados e operações existentes devido a atributos vastamente superiores. Os exemplos com os quais este artigo começou destacam os riscos representados por três vertentes específicas de tecnologias, a saber, tecnologias de razão distribuída (criptomoedas), novos métodos de pagamento e tecnologias financeiras (FinTech) (Smith, 2020).

O combate à lavagem de dinheiro com criptomoedas atraiu ampla atenção na comunidade acadêmica, com métodos principalmente divididos em três categorias: métodos baseados em regras, métodos de detecção de anomalias não supervisionados e métodos de aprendizado de máquina supervisionados. Algoritmos baseados em regras normalmente detectam atividades ilícitas construindo sistemas especialistas ou usando algoritmos heurísticos, mas esses algoritmos são limitados pelas regras pseudônimas e em constante mudança das criptomoedas (Jourdan *et al.*, 2018; Liang *et al.*, 2019; Toyoda *et al.*, 2019).

Métodos AML não supervisionados alcançam a detecção por meio de agrupamento, como k -means aparados e agrupamento de comunidades, classificando transações com padrões semelhantes como um grupo para ajudar a detectar transações anômalas. No entanto, pesquisas indicam que a eficácia desses algoritmos não é

comparável com algoritmos AML supervisionados. Portanto, cada vez mais pesquisadores estão se concentrando em métodos de aprendizado supervisionado para abordar esses desafios, usando dados de treinamento com rótulos conhecidos para treinar modelos que aprendem as características de transações normais e suspeitas para ajudar as autoridades regulatórias a detectar potenciais atividades de lavagem de dinheiro (Jourdan *et al.*, 2018; Liang *et al.*, 2019).

Entre estes, algoritmos relacionados a gráficos têm desempenho excepcionalmente bom, incluindo um classificador baseado em node2vec, redes neurais convolucionais de gráficos (GCNs) e suas variações. Desde o lançamento do maior conjunto de dados supervisionado de Bitcoin pela Elliptic, que representa transações como nós e fluxos entre transações como arestas, a detecção de lavagem de dinheiro ilícita pode ser vista como uma tarefa de classificação dos nós (Liang *et al.*, 2019; Toyoda *et al.*, 2019; Alarab *et al.*, 2020).

As tecnologias de livro-razão distribuído (DLT) fornecem uma plataforma de livro-razão digital e descentralizada aberta para um número específico ou ilimitado de usuários. Ao contrário dos livros-razão normais, no entanto, eles não são governados por uma autoridade central, como um governo ou banco (Barone; Masciandaro, 2019).

Em vez disso, o livro-razão (e cópias dele) é mantido por seus usuários, agindo semi-anonimamente por meio de mecanismos de consenso para autenticar e adicionar novas transações usando métodos criptográficos. Blockchain é talvez o exemplo mais proeminente de um livro-razão distribuído, onde os usuários podem negociar criptomoedas (tokens digitais que representam valor) entre si. O DLT também está evoluindo ainda mais para permitir a negociação de outras formas de ativos, representadas digitalmente por meio de criptotokens associados, sem mediadores ou supervisão de autoridade central (Tapscott; Tapscott, 2016; Barone; Masciandaro, 2019; Christie, 2018).

Novos métodos de pagamento (NPMs), que representam formas modernas de concluir transações financeiras, há muito são considerados riscos de ML/FT, particularmente em países em desenvolvimento que não têm serviços financeiros extensivos ou conformidade com regulamentações. Os NPMs incluem transferências de dinheiro móvel e cartões pré-pagos, que permitem aos usuários armazenar, transferir e sacar fundos sem precisar de uma conta bancária. Outros NPMs, como aplicativos de pagamento móvel com recursos de processamento de pagamento no aplicativo mencionados acima (por exemplo, *Uber*), são desenvolvimentos mais recentes que

diversificam as possibilidades disponíveis para criminosos (Barone; Masciandaro, 2019; Christie, 2018).

Enquanto isso, os serviços financeiros são atualmente o foco principal das regulamentações de "antilavagem de dinheiro" (AML) e "combate ao financiamento do terrorismo" (CFT). Elas exigem que as instituições financeiras conduzam "conheça seu cliente" (KYC) e due diligence do cliente (CDD) em clientes para entender padrões de transações "normais", permitindo que transações suspeitas sejam detectadas e relatadas a unidades nacionais de inteligência financeira designadas. No entanto, a inovação da FinTech está digitalizando rapidamente os serviços tradicionais, permitindo acesso cada vez mais remoto e anônimo a serviços bancários on-line, arrecadação de fundos e negociação de títulos (Smith, 2020; Teixeira; Rodrigues, 2022).

Exemplificando seus riscos, o Reino Unido identificou um "crescimento significativo" de relatórios de atividades suspeitas arquivados entre 2017 e 2020 por tais serviços, embora isso possa ser devido a um melhor treinamento de funcionários ou a um impulso preventivo para conformidade com as regulamentações futuras. Este artigo define FinTech como serviços e produtos financeiros habilitados por tecnologia, especificamente distintos de tecnologias de pagamento não bancárias (cobertas em NPMs) e tecnologias de blockchain (cobertas em DLT). Outras pesquisas podem adotar definições diferentes (Barone; Masciandaro, 2019; Christie, 2018; Smith, 2020).

O rastreamento de lavagem de dinheiro envolvendo criptomoedas é um campo em rápida evolução, impulsionado pelo desenvolvimento de tecnologias específicas que visam identificar e monitorar transações suspeitas (Liang *et al.*, 2019; Toyoda *et al.*, 2019). Algumas das principais tecnologias e abordagens utilizadas para esse fim incluem:

Análise de Blockchain: Ferramentas de análise de blockchain permitem que as autoridades e empresas de compliance rastreiem transações em redes de criptomoedas. Essas ferramentas analisam o histórico de transações, identificando padrões e conexões entre endereços, o que pode ajudar a detectar atividades suspeitas. Exemplos de empresas que oferecem essas soluções incluem Chainalysis, Elliptic e CipherTrace (Jourdan *et al.*, 2018; Liang *et al.*, 2019).

Softwares de Monitoramento de Transações: Esses softwares são projetados para monitorar transações em tempo real, identificando atividades que possam indicar lavagem de dinheiro. Eles utilizam algoritmos para detectar comportamentos anômalos,

como transações de grandes valores ou transferências frequentes entre endereços (Barone; Masciandaro, 2019; Christie, 2018).

Inteligência Artificial e Machine Learning: A aplicação de inteligência artificial e machine learning permite a análise de grandes volumes de dados para identificar padrões que podem não ser evidentes em análises manuais. Esses sistemas podem aprender com dados históricos para melhorar continuamente a detecção de atividades suspeitas (Barone; Masciandaro, 2019; Christie, 2018).

Identificação de Endereços: Algumas tecnologias se concentram na identificação de endereços associados a atividades ilícitas, como aqueles listados em bases de dados de endereços "negros" (blacklists). Isso ajuda as instituições financeiras a bloquear transações com endereços conhecidos por estarem envolvidos em lavagem de dinheiro ou fraudes (Liang *et al.*, 2019; Toyoda *et al.*, 2019; Alarab *et al.*, 2020).

Integração com Sistemas de Compliance: Muitas plataformas de criptomoedas e exchanges estão integrando tecnologias de rastreamento em seus sistemas de compliance, permitindo que realizem verificações de due diligence e monitoramento contínuo das transações de seus usuários (Toyoda *et al.*, 2019).

Relatórios de Atividades Suspeitas: As tecnologias também facilitam a geração de relatórios de atividades suspeitas, que podem ser enviados às autoridades competentes. Esses relatórios são essenciais para que as agências de combate à lavagem de dinheiro possam investigar e tomar medidas apropriadas (Liang *et al.*, 2019; Toyoda *et al.*, 2019; Alarab *et al.*, 2020).

Colaboração Internacional: O uso de plataformas que permitem a troca de informações entre diferentes jurisdições e agências de aplicação da lei é fundamental. Tecnologias que suportam essa colaboração ajudam a rastrear transações que cruzam fronteiras, facilitando investigações mais abrangentes (Liang *et al.*, 2019; Toyoda *et al.*, 2019; Alarab *et al.*, 2020).

Análise de Redes: Ferramentas de análise de redes ajudam a visualizar e entender as conexões entre diferentes endereços de criptomoedas, permitindo que os investigadores identifiquem redes de lavagem de dinheiro e suas estruturas (Alarab *et al.*, 2020). O tópico que segue consiste de uma análise crítica dos dados levantados.

5 ANÁLISE CRÍTICA

Existe uma preocupação recorrente em relação aos criptoativos no que diz respeito ao uso potencial e real para a lavagem de dinheiro. Essa relação se deve às características fundamentais das criptomoedas, como a descentralização, o anonimato e a dificuldade de rastreamento das transações, que podem facilitar a movimentação de fundos provenientes de atividades ilícitas.

Os criptoativos, sustentados pela tecnologia blockchain, oferecem um ambiente onde os usuários podem transacionar com um nível de privacidade que não é comum em sistemas financeiros tradicionais. Isso levanta questões sobre a regulamentação e a necessidade de implementar medidas de conformidade mais rigorosas para prevenir crimes financeiros (Amparo, 2022).

Além disso, o fato de as criptomoedas compartilharem essas características permite que a discussão se amplie para todos os criptoativos, ressaltando a importância de entender as implicações legais e éticas associadas à sua utilização. Portanto, o debate sobre a regulação das criptomoedas envolve não apenas considerações econômicas, mas também questões de segurança, privacidade e integridade do sistema financeiro global.

A cooperação internacional e o intercâmbio de informações são fundamentais na luta contra crimes relacionados a criptomoedas. Dada a natureza global e descentralizada das criptomoedas, as atividades criminosas, como lavagem de dinheiro, fraudes e financiamento do terrorismo, frequentemente transcendem fronteiras nacionais.

A colaboração entre países permite a troca de dados e inteligência sobre transações suspeitas, ajudando as autoridades a identificar e rastrear atividades ilícitas. Organizações internacionais, como o Grupo de Ação Financeira (GAFI), desempenham um papel crucial ao estabelecer diretrizes e promover a cooperação entre nações para fortalecer a regulamentação e a supervisão do uso de criptomoedas (Loayza *et al.*, 2019).

Além disso, o desenvolvimento de plataformas e redes de compartilhamento de informações entre agências de aplicação da lei e instituições financeiras é essencial para detectar e prevenir crimes. Essa abordagem colaborativa não apenas melhora a eficácia das investigações, mas também contribui para a criação de um ambiente mais seguro e confiável para o uso de criptomoedas.

Através de acordos bilaterais e multilaterais, as nações podem compartilhar informações sobre transações suspeitas, endereços de carteiras digitais e perfis de usuários, o que é crucial para rastrear e desmantelar operações criminosas. Assim, a

cooperação internacional se torna um pilar essencial na eficácia das estratégias de combate à lavagem de dinheiro envolvendo criptomoedas.

As criptomoedas, embora ofereçam vantagens como descentralização e transações rápidas, também levantam preocupações éticas e de privacidade. Entre os problemas éticos, destaca-se a possibilidade de uso em atividades ilícitas, como lavagem de dinheiro e financiamento do terrorismo, devido ao seu caráter anônimo. Além disso, a volatilidade das criptomoedas pode levar a perdas financeiras significativas para investidores sem conhecimentos aprofundados.

Em relação à privacidade, embora as transações em blockchain sejam transparentes e rastreáveis, a natureza pública dessas informações pode comprometer a privacidade dos usuários. A exposição de dados financeiros pode resultar em riscos de segurança, como roubo de identidade e fraudes. Portanto, é crucial que os usuários e reguladores considerem esses aspectos ao lidar com criptomoedas, buscando um equilíbrio entre inovação e proteção dos direitos individuais (Teixeira; Rodrigues, 2022).

5.1 AVALIAÇÃO DAS REGULAÇÕES E ESFORÇOS ATUAIS

A existência de regulamentações e esforços atuais para coibir a lavagem de dinheiro com criptomoedas é, de fato, um tema de crescente importância no cenário financeiro global. Muitos países têm adotado legislações específicas para aumentar a transparência e a rastreabilidade das transações em criptomoedas (Blandin *et al.*, 2020), sendo as principais:

Registros e Identificação: A exigência de que as exchanges de criptomoedas realizem a verificação de identidade dos usuários (KYC - Know Your Customer) é uma prática comum. Isso ajuda a garantir que as transações possam ser rastreadas até indivíduos ou entidades específicas (Blandin *et al.*, 2020; Teixeira; Rodrigues, 2022).

Relatórios de Transações Suspeitas: Muitas jurisdições exigem que as plataformas de criptomoedas relatem transações que possam ser indicativas de atividades ilícitas. Isso inclui transações de alto valor ou aquelas que envolvem endereços associados a atividades criminosas (Liang *et al.*, 2019).

Colaboração Internacional: A natureza global das criptomoedas exige uma abordagem colaborativa entre países. Organizações como o GAFI (Grupo de Ação Financeira) têm promovido diretrizes que incentivam os países a adotar regulamentações

semelhantes para evitar que jurisdições mais permissivas se tornem refúgios para atividades de lavagem de dinheiro (Loayza *et al.*, 2019).

Educação e Conscientização: Além das regulamentações, há um esforço crescente para educar tanto os usuários quanto os operadores de plataformas sobre os riscos associados à lavagem de dinheiro e a importância de práticas de conformidade (Teixeira; Rodrigues, 2022).

Tecnologia de Monitoramento: O uso de tecnologias avançadas, como análise de blockchain e inteligência artificial, tem se mostrado eficaz na identificação de padrões suspeitos e na prevenção de atividades ilícitas (Teixeira; Rodrigues, 2022).

Embora haja progresso significativo, os desafios permanecem, especialmente devido à natureza descentralizada e anônima de muitas criptomoedas. A adaptação contínua das regulamentações e a implementação de melhores práticas são essenciais para mitigar os riscos associados à lavagem de dinheiro nesse setor.

Na Tabela 2 são citados tratados e acordos internacionais voltados para os crimes cibernéticos de forma geral.

Tabela 2 - Tratados e acordos internacionais sobre crimes cibernéticos.

Nome do instrumento	Descrição	Situação jurídica	
Convenção das Nações Unidas contra o Crime Organizado Transnacional (2000) (Convenção de Palermo)	As disposições do tratado são altamente relevantes, embora não abordem explicitamente o crime cibernético, obrigando as partes a promulgar legislação para cooperação policial e extradição.	Entrada em vigor: 29 de setembro de 2003. Signatários: 117 Partes: 178	
Convenção sobre os Direitos da Criança (1989)	Artigo 34: Os Estados Partes devem proteger a criança de todas as formas de exploração e abuso sexual, incluindo prostituição e pornografia.	Entrada em vigor: 2 de setembro de 1990. Signatários: 140 Partes: 196	
Protocolo Facultativo à Convenção sobre os Direitos da Criança (2001)	O artigo 3(1) (c) proíbe a pornografia infantil e menciona a Internet como meio de distribuição.	Signatários: 121 Partes: 177	
Tratados do Conselho da Europa Convenção sobre o Cibercrime (2001) (Convenção de Budapeste)	O primeiro acordo internacional para reduzir o crime cibernético por meio da harmonização com as leis nacionais. Melhorando as técnicas investigativas e aumentando a cooperação internacional.	Signatários: 2 Ratificações/adesões: 66 (Países não pertencentes à UE: 22)	Países não pertencentes à UE: Argentina, Austrália, Cabo Verde, Canadá, Chile, Colômbia, Costa Rica, República Dominicana, Gana, Israel, Japão,

Nome do instrumento	Descrição	Situação jurídica	
			Maurício, Marrocos, Panamá, Paraguai, Peru, Filipinas, Senegal, África do Sul, Sri Lanka, Tonga, Estados Unidos da América
Protocolo Adicional à Convenção sobre o Cibercrime, relativo à criminalização de actos de natureza racista e xenófoba cometidos através de sistemas informáticos (2003)	Ampliação do escopo da Convenção sobre Crimes Cibernéticos para abranger crimes de propaganda racista ou xenófoba.	N.º de assinaturas não seguidas de ratificações: 12 N.º de ratificações/adesões: 33 (países não membros da UE: 5)	Países fora da UE: Canadá, Marrocos, Paraguai, Senegal, África do Sul.
Convenção sobre a Proteção das Crianças contra a Exploração Sexual e o Abuso Sexual (2007)	A Convenção criminaliza a solicitação de crianças para fins sexuais (“grooming”) e o “turismo sexual”.	Número de ratificações/adesões: 48 Todos os 47 países que são membros do Conselho da Europa e a Tunísia é o único que não é membro.	
Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais (dados em 18/06/2020)	A Convenção foi adotada em junho de 2014 e aborda (i) transações eletrônicas, (ii) proteção de dados pessoais e (iii) segurança cibernética e crimes cibernéticos.	Total de países: 55 De assinaturas: 14 De ratificações: 8 De depósitos: 8	A União Africana (UA) é composta por 55 países.

Fonte: Adaptado de Khan *et al.* (2022).

Não é possível afirmar que não existem esforços regulatórios e legais visando coibir a prática de crimes cibernéticos, inclusive aqueles contra o sistema financeiro. Apesar de muitos países serem signatários desses acordos, porém, a troca de informações de forma ágil, organizada, precisa e tempestiva ainda é um desafio (Khan *et al.*, 2022).

As lacunas nas regulamentações existentes muitas vezes se devem à rápida evolução das tecnologias de blockchain e à falta de um marco regulatório uniforme entre diferentes jurisdições. Atualmente, muitos países estão implementando esforços para coibir a lavagem de dinheiro associada a criptomoedas. Isso inclui a introdução de legislações que exigem que as exchanges de criptomoedas se registrem e sigam normas de Conheça Seu Cliente (KYC) e de combate à lavagem de dinheiro (AML). Além disso, organismos internacionais, como o Grupo de Ação Financeira (FATF), estão promovendo diretrizes que incentivam os países a adotar medidas mais rigorosas (Liang *et al.*, 2019; Blandin *et al.*, 2020; Teixeira; Rodrigues, 2022).

A natureza irreversível das transações em blockchain significa que, uma vez que um pagamento é realizado, não há como revertê-lo, o que pode facilitar fraudes e extorsões, como em casos de ransomware, onde as vítimas são obrigadas a pagar para ter seus dados liberados. Esse desafio se agrava com as dificuldades que as autoridades enfrentam para investigar e interromper atividades ilícitas. A intervenção em máquinas envolvidas nas transações é uma alternativa que, além de exigir autorização legal, demandaria conhecimentos técnicos específicos e, muitas vezes, seria ineficaz dada a natureza descentralizada dos sistemas que operam com criptomoedas. Além disso, a colaboração voluntária de intermediários legítimos, como exchanges de criptomoedas e carteiras digitais, não é garantida, colocando um obstáculo adicional na tentativa de rastrear e combater atividades ilícitas (Teixeira; Rodrigues, 2022).

A complexidade do ambiente das criptomoedas, aliado ao fato de que muitos criminosos podem operar de maneira discreta e em múltiplas jurisdições, torna o combate à lavagem de dinheiro e outras fraudes um desafio significativo para as autoridades. Portanto, a discussão sobre regulamentação, segurança e ética no uso de criptoativos se torna ainda mais urgente, visando não só a proteção dos consumidores, mas também a integridade do sistema financeiro como um todo (Teixeira; Rodrigues, 2022).

Esses esforços visam aumentar a transparência nas transações de criptomoedas e dificultar a utilização dessas tecnologias para atividades ilícitas. No entanto, ainda existem desafios significativos, como a necessidade de colaboração internacional e a adaptação das regulamentações às inovações tecnológicas.

5.2 SUGESTÕES PARA APRIMORAR A REGULAMENTAÇÃO DAS CRIPTOMOEDAS; PARA PROFISISONAIS DO DIREITO E AUTORIDADES COMPETENTES

O ano de 2020 foi um ano desafiador sem precedentes, especialmente da perspectiva do crime cibernético. Não apenas o mundo tem que enfrentar as ameaças do surto de pandemia global, mas também dos ataques cibernéticos cada vez mais sofisticados. O surto de pandemia global resultou em um aumento de mais de 600% no crime cibernético. Quanto mais sofisticada e avançada for a tecnologia, maior será o número de crimes cibernéticos e mais difícil será compreender o problema. Os criminosos cibernéticos usam a tecnologia avançada para realizar atividades criminosas, como hacking, phishing, spam, pornografia infantil e crimes de ódio, resultando em perdas

massivas sofridas por indivíduos e corporações e até mesmo representam perigo para a segurança nacional em alguns casos (Bechara; Schuch, 2021).

Sem dúvida, a Inteligência Artificial - IA trouxe enormes benefícios e vantagens para a humanidade na última década e essa tendência provavelmente continuará nos próximos anos, já que a IA está gradualmente se tornando parte dos serviços digitais que usamos em nossas vidas diárias. Muitos governos ao redor do mundo estão considerando a implantação de sistemas e aplicativos de IA para ajudá-los a realizar suas atividades e, mais concretamente, para facilitar a identificação e a previsão de crimes. Além disso, as agências de segurança nacional e inteligência também perceberam o potencial das tecnologias de IA para apoiar e atingir objetivos de segurança nacional e pública (Burgess, 2020).

Há desenvolvimentos significativos em tecnologias de IA, como o uso de reconhecimento facial na esfera da justiça criminal, o uso de drones, armas autônomas letais e veículos autônomos que, quando não configurados ou gerenciados adequadamente sem mecanismos de supervisão adequados, têm o potencial de serem usados para fins disruptivos e prejudicar os direitos e liberdades individuais (Burgess, 2020; Teixeira; Rodrigues, 2022).

Atualmente, há uma discussão em andamento nos círculos políticos e legislativos internacionais sobre a revisão e melhoria da estrutura e do limite de responsabilidade referentes a sistemas e tecnologias de IA, embora, devido à complexidade do tópico e às diferentes abordagens jurídicas ao redor do mundo relativas à responsabilidade civil, provavelmente não haverá um consenso sobre uma resposta harmonizada e uniforme, pelo menos não em um futuro próximo (Burgess, 2020; Teixeira; Rodrigues, 2022).

O compartilhamento de informações trata-se de uma das melhores formas de obter e ceder informações, assim, tanto dentro dos territórios quanto na esfera internacional, esses esforços podem permitir que haja a possibilidade de rastrear operações, especialmente aquelas que se repetem e, assim, levantar dados para avaliar a possibilidade de fraudes envolvidas, como a lavagem de dinheiro (Tian *et al.*, 2020; Teixeira; Rodrigues, 2022).

O aprimoramento dos conhecimentos sobre criptomoedas e os crimes associados ao seu uso, como a lavagem de recursos, é crucial para que operadores do direito e autoridades possam responder de maneira eficaz às novas ameaças que surgem nesse ambiente digital. A natureza dinâmica e em constante evolução das criptomoedas

exige um compromisso contínuo com a atualização de informações e práticas, bem como a adoção de uma abordagem proativa na prevenção e combate a delitos financeiros.

Desenvolver estratégias de educação voltadas para o combate a fraudes em criptoatividades é uma tarefa fundamental. Isso inclui a capacitação de profissionais do direito, policiais, reguladores e o público em geral sobre os aspectos técnicos das criptomoedas, as diferentes modalidades de fraudes, e a importância da diligência na realização de transações. Programas de formação e conscientização podem ajudar a fornecer as ferramentas e conhecimentos necessários para identificar comportamentos suspeitos e agir de maneira informada em situações de risco.

Além disso, a colaboração entre diferentes setores—governo, indústria financeira, tecnologia e educação—é essencial para a construção de um ecossistema resiliente. O compartilhamento de informações e melhores práticas pode ajudar a desenvolver padrões eficazes de segurança e conformidade, assim como facilitar a identificação e a limpeza das transações.

Por fim, é importante ressaltar que a educação deve ir além dos operadores do direito e das autoridades, alcançando também os usuários de criptomoedas. Consciência sobre os riscos, bem como sobre medidas de segurança para proteger seus ativos digitais, é vital para a construção de um ambiente mais seguro. Assim, enquanto os criminosos se adaptam rapidamente às novas tecnologias, a sociedade em seu conjunto também deve evoluir, com um foco contínuo na educação e na ética no uso de criptomoedas.

6 CONCLUSÃO

No contexto das finanças contemporâneas, o surgimento das criptomoedas e da tecnologia blockchain marca um verdadeiro ponto de inflexão, transformando a dinâmica dos mercados financeiros e desafiando as práticas bancárias tradicionais. Essas inovações não apenas introduziram uma nova classe de ativos, mas também criaram um ambiente repleto de oportunidades e riscos que requerem uma análise cuidadosa e aprofundada.

A intersecção entre criptomoedas e blockchain gerou um leque de possibilidades que podem reconfigurar a forma como as transações financeiras são realizadas, promovendo eficiência, transparência e descentralização. No entanto, essa mesma inovação também vem acompanhada de ameaças significativas, como fraudes, lavagem de dinheiro e a potencial volatilidade dos ativos digitais. A natureza descentralizada e anônima de muitas criptomoedas complica os esforços de regulamentação e fiscalização, exigindo uma abordagem mais robusta e colaborativa por parte de reguladores, instituições financeiras e autoridades competentes.

Diante desse panorama, é imperativo que especialistas, acadêmicos e stakeholders do setor financeiro se dediquem a um estudo aprofundado das interações entre essas forças disruptivas. A compreensão das implicações econômicas, sociais e legais do uso de criptomoedas é fundamental para a formulação de políticas e estratégias que possam mitigar riscos, promover a inovação responsável e garantir a integridade do sistema financeiro global. Assim, enquanto avançamos rumo a um futuro cada vez mais digitalizado, a necessidade de um conhecimento abrangente e adaptável sobre criptomoedas e blockchain torna-se não apenas uma prioridade, mas um requisito essencial para a sustentabilidade e segurança do ecossistema financeiro, bem como para a organização e evolução do ordenamento jurídico.

À medida que o sistema financeiro mundial passa por uma transformação radical, este estudo contribui para análises variadas, como uma análise abrangente sobre como as criptomoedas influenciam a dinâmica dos mercados financeiros, permitindo que investidores, instituições financeiras e reguladores compreendam melhor os efeitos colaterais e as oportunidades decorrentes dessa nova era digital. Compreender essas interações possibilita que esses stakeholders naveguem de maneira mais eficaz no ambiente de investimento em constante evolução, auxiliando na tomada de decisões informadas e na mitigação de riscos associados à volatilidade dos ativos digitais.

Além disso, a pesquisa investiga as diferentes abordagens que estão sendo adotadas globalmente para enfrentar os desafios e aproveitar as oportunidades apresentadas pelas criptomoedas e tecnologia blockchain. Ao explorar a diversidade de métodos regulatórios, estratégias de compliance e inovações financeiras, o estudo oferece insights valiosos sobre práticas bem-sucedidas que podem ser adaptadas e implementadas por outros países e regiões. Essa diversidade de abordagens pode enriquecer o campo com experiências variadas, auxiliando na formulação de políticas mais eficazes, além de dar maior suporte aos operadores do direito que optem por uma atuação relacionada à referida área.

Por último, o estudo também enfatiza a importância da educação e da conscientização em torno das criptomoedas, tanto para investidores quanto para o público em geral. Ao disseminar informações sobre como funcionam esses ativos e os riscos envolvidos, a pesquisa contribui para uma cultura de responsabilidade financeira, ajudando os usuários a realizar transações mais seguras e informadas. Dessa forma, a pesquisa não só amplia a base de conhecimento sobre criptomoedas e blockchain, mas também promove um ambiente de investimento mais robusto e resiliente, capaz de enfrentar os desafios e mudanças que estão por vir.

7 REFERÊNCIAS

AGUIAR, RDA. **Bitcoin como meio no crime de lavagem de dinheiro e o papel da regulamentação**. 2021. 40 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022.

ALARAB, I. et al. Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain; **Proceedings of the 2020 5th International Conference on Machine Learning Technologies**; Beijing, China. 19–21 June 2020; pp. 23–27.

ALBRECHT, C. et al. The Use of Cryptocurrencies in the Money Laundering Process. **Journal of Money Laundering Control** 22: 210–16, 2019.

AMPARO, ALS. **A regulação de criptoativos no Brasil e suas implicações no combate ao crime de lavagem de dinheiro: uma breve análise do projeto de lei n. 4.401/2021**. Artigo Científico apresentado à Universidade Federal de Lavras, como parte das exigências do Curso de Programa de Pós-Graduação Latu Sensu em Detecção de Fraudes, para a obtenção do título de Especialista. Lavras, 2022.

ARAS, V. Os aspectos penais da Lei Brasileira dos Criptoativos. **Revista do Ministério Público do Estado do Rio de Janeiro** nº 88, abr./jun. 2023.

BBC. **Thodex cryptocurrency boss jailed for 11,196 years in Turkey for fraud**. 8 set. 2023.

BECHARA, FR.; SCHUCH, SB. Cybersecurity and Global Regulatory Challenges. **Journal of Financial Crime**. 2021;28(2):359–374. 10.1108/JFC-07-2020-0149

BLANDIN, A. *et al.* University of Cambridge. **The Global Cryptoasset Regulatory Landscape Study**. 2020.

BRASIL. **Lei n. 14.478 de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições.

BRASIL. **Lei n. 12.850 de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112850.htm. Acesso em: 1 dez. 2022.

BRASIL. **Lei n. 13.964 de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113964.htm. Acesso em: 1 dez. 2022.

BRASIL. Banco Central do Brasil. **Prevenção à lavagem de dinheiro e ao financiamento do terrorismo**. 2024.

BURGESS, M. Police built an AI to predict violent crime. It was seriously flawed, **WIRED**, August 6, 2020.

CAPEZ, Fernando. **Curso de direito penal legislação especial 4**. 12. ed. São Paulo: Saraiva, 2017.

CASEY, M. et al. **The Impact of Blockchain Technology on Finance: A Catalyst for Change**. Geneva Reports on the World Economy 21. International Center for Monetary and Banking Studies (ICMB). 2018.

CHAVEZ-DREYFUSS, G.; PRICE, M. How hackers stole \$613 million in crypto tokens from Poly Network. 13 ago. 2021.

CHOWDHURY, N. Crime, Criminals and Cryptocurrencies. In *Inside Blockchain, Bitcoin, and Cryptocurrencies*. Edited by Niaz Chowdhury. London: CRC Press, pp. 295–316, 2019.

COLLIER, R. NHS ransomware attack spreads worldwide. **CMAJ**. 2017 Jun 5;189(22):E786-E787. doi: 10.1503/cmaj.1095434. PMID: 28584047; PMCID: PMC5461132.

DELFABBRO, P. et al. Cryptocurrency trading, gambling and problem gambling. **Addict Behav.** 2021 Nov;122:107021. doi: 10.1016/j.addbeh.2021.107021. Epub 2021 Jun 16. PMID: 34171583.

DUTCH BANKING ASSOCIATION. **Crypto-assets in Dutch perspective, Opportunities for a Dutch crypto-asset ecosystem**, 2020.

DYNTU, V.; DYKYI, O. Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies*. Vol. 4, No. 5, 2018.

ECHARTE-FERNANDEZ, MA et al. Central Banks' Monetary Policy in the Face of the COVID-19 Economic Crisis: Monetary Stimulus and the Emergence of CBDCs. **Sustainability** 13: 4242, 2021.

E-INVESTIDOR. **Conheça os 5 crimes mais famosos com criptomoedas**. 21 abr. 2022.

FAVERIO, M.; MASSARAT, N. 46% of Americans who have invested in cryptocurrency say it's done worse than expected. **Pew Research Center** [Internet]. 2022.

FERWERDA, J. et al. Estimating money laundering flows with a gravity model-based simulation. **Sci Rep.** 2020 Oct 29;10(1):18552. doi: 10.1038/s41598-020-75653-x. PMID: 33122829; PMCID: PMC7596494.

HORCHEL, C. Criptomoedas como moeda paralela: apontamentos entre a liberdade financeira e o (des)controle estatal no combate e repressão à lavagem de dinheiro. **Revista Brasileira de Ciências Policiais.** 2022.

JOHNSON, B. et al. Cryptocurrency trading and its associations with gambling and mental health: **A scoping review. Addict Behav.** 2023 Jan;136:107504. doi: 10.1016/j.addbeh.2022.107504. Epub 2022 Sep 24. PMID: 36174424.

JOMA, J.Z. **Criptoativos:** uma breve análise da legislação internacional. 22 ago. 2022.

JOURDAN, M. et al. Characterizing entities in the bitcoin blockchain; **Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW);** Singapore. 17–20 November 2018; Piscataway, NJ, USA: IEEE; 2018. pp. 55–62.

KHAN, S. et al. A systematic literature review on cybercrime legislation. **F1000Res.** 2022 Aug 23;11:971. doi: 10.12688/f1000research.123098.1. PMID: 39258289; PMCID: PMC11384205.

KOU, G. et al. Fintech investments in European banks: a hybrid IT2 fuzzy multidimensional decision-making approach. **Financ Innov.** 2021;7:39. doi: 10.1186/s40854-021-00256-y.

LIANG, J. et al. Targeted addresses identification for bitcoin with network representation learning; **Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI);** Shenzhen, China. 1–3 July 2019; Piscataway, NJ, USA: IEEE; 2019. pp. 158–160.

LIMA, Renato Brasileiro de. **Legislação criminal especial comentada.** Volume único. 5. ed. rev., atual. e ampl. Salvador: JusPODIVM, 2017.

LOAYZA, N. et al. Illicit activity and money laundering from an economic growth perspective: A model and an application to Colombia. **Journal of Economic Behavior & Organization.** Volume 159, March 2019, Pages 442-487

MARTIN, E. **Regulamentação de Criptomoedas:** Um Panorama Global e o Caso Brasileiro. 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/regulamentacao-de-criptomoedas-um-panorama-global-e-o-caso-brasileiro/2024518717>. Acesso em: 1 nov. 2024.

MATTOS, P. H. A imputação e o crime de lavagem de capitais: um estudo crítico sobre a viabilidade da denúncia. **Revista Brasileira de Direito Processual Penal,** v. 8, n. 1, p. 409–440, jan. 2022.

MEGAW, N. Regulator Orders N26 to Improve Anti-Money Laundering Controls. **Financial Times.** 2019.

NANEZ ALONSO, SL. Et al. **Reasons fostering or discouraging the implementation of central bank-backed digital currency**: A review. *Economies* 8: 41, 2020.

NUCCI, Guilherme de Souza. **Organização criminosa**. 2. ed. ver., atual. e ampl. Rio de Janeiro: Forense, 2015.

PINHEIRO, BBP. **Criptomoedas e lavagem de dinheiro**: um estudo sobre os impactos da regulação no Brasil e no mundo. Trabalho de Conclusão de Curso apresentado à Faculdade de Direito, da Universidade Presbiteriana Mackenzie, como requisito parcial à obtenção do título de Bacharel em Direito. São Paulo, 2023.

RODRIGUES, R.S. Uso de Bitcoins em lavagem de dinheiro: dissensos doutrinários. **Boletim IBCCRIM**, ano 32, n. 380, 2024.

ROSEN, A. **What Is Cryptocurrency?** A Guide for Beginners. Nerdwallet [Internet]. 2023. May 22, 2023.

ROYAL, J. **Cryptocurrency Statistics 2023**: Investing In Crypto. Bankrate. Bankrate [Internet]. 2023.

SANZ BAS, D. Hayek and the cryptocurrency revolution. **Iberian Journal of the History of Economic Thought** 7: 15–28, 2020.

SAULNIER, J. **Digital finance: emerging risks in crypto-assets—regulatory and supervisory challenges in the area of financial services, Institutions and Markets**. 2020

SCHMIDT, A. Impacts of money laundering and terrorism financing: Final report. **Special reports**. Canberra: Australian Institute of Criminology. 2024.

SHAYEGAN, MJ. Et al. A Collective Anomaly Detection Technique to Detect Crypto Wallet Frauds on Bitcoin Network. **Symmetry**. 2022;14(2):328. doi: 10.3390/sym14020328.

SHIER, C. et al. Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack. **Journal of Cases on Information Technology** 21: 19–32, 2019.

SONG, Y.; CHEN, B.; WANG, X-Y. Cryptocurrency technology revolution: are Bitcoin prices and terrorist attacks related? *Financial Innovation*. 2023;9(1):29. doi: 10.1186/s40854-022-00445-3.

SONKURT, HAA. Cryptocurrency investment: A safe venture or a new type of gambling? **Journal of Gambling Issues**. 2021;47.

TEICHER, R. How Uber Ghost Rides Are Linked to Online Money Laundering. **The Next Web**. 2018.

TEIXEIRA, T.; RODRIGUES, C.A. **Blockchain e Criptomoedas**: Aspectos Jurídicos. 4. ed. [S. l.]: Juspodivm, 2022.

TIAN, J. et al. Blockchain Information Sharing Mechanism Based on Embedded System in Project Management System. **Comput Intell Neurosci**. 2022 Aug 4;2022:1835626. doi: 10.1155/2022/1835626.

TJDFT - Tribunal de Justiça do Distrito Federal e dos Territórios. **Lavagem de dinheiro**. 2016.

TOYODA, K. et al. A novel methodology for hyip operators' bitcoin addresses identification. **IEEE Access**. 2019;7:74835–74848. doi: 10.1109/ACCESS.2019.2921087.

TROZZE, A. et al. Cryptocurrencies and future financial crime. **Crime Sci**. 2022;11(1):1. doi: 10.1186/s40163-021-00163-8. Epub 2022 Jan 5. PMID: 35013699; PMCID: PMC8730302.

TUMMALA, R. **The 10X Potential Of Tokenisation**. 2020.

ZHANG, H. et al. **Economic principles of PoPCoin, a democratic time-based cryptocurrency**. 2020; arXiv preprint arXiv:2011.01712.

ZHANG, S. et al. "Plus Token and investor searching behaviour – A cryptocurrency Ponzi scheme," **Accounting and Finance, Accounting and Finance Association of Australia and New Zealand**, vol. 63(4), pages 4713-4728, December, 2023.

ZHANG, H. et al. A survey of deep learning applications in cryptocurrency. **iScience**. 2023 Nov 22;27(1):108509. doi: 10.1016/j.isci.2023.108509. PMID: 38111683; PMCID: PMC10726249.

ZUMAS, S.F. Criptomonedas, Críptocrime e Criptoinvestigação. **Revista Eletrônica Direito & TI**, [S. l.], v. 1, n. 12, p. 8, 2020.