

A UTILIZAÇÃO DE CRIPTOATIVOS NA LAVAGEM DE DINHEIRO: Fundamentos Tecnológicos e Reação Normativa

The use of crypto assets in money laundering.: Technological Foundations and Regulatory Response

João Pedro Motta Pereira ¹

RESUMO

A presente obra analisa os impactos da utilização de criptoativos nas práticas contemporâneas de lavagem de dinheiro, destacando os desafios enfrentados pelo sistema jurídico frente às inovações tecnológicas e à descentralização financeira. Inserido no campo do Direito Penal Econômico e da persecução de crimes financeiros digitais, o estudo tem por objetivo compreender como instrumentos como criptomoedas, mixers, tumblers e NFTs têm sido utilizados para ocultar a origem de valores ilícitos e dificultar a rastreabilidade patrimonial. Adota-se o método dedutivo, com abordagem qualitativa e pesquisa bibliográfica e documental. Os resultados apontam que, embora o ordenamento jurídico brasileiro tenha avançado com a edição da Lei nº 14.478/2022 e normas complementares, a sofisticação dos mecanismos utilizados para lavagem de capitais digitais ainda supera a capacidade regulatória e investigativa das autoridades. Conclui-se que a articulação entre inovação tecnológica, regulamentação normativa e cooperação internacional é essencial para o enfrentamento eficaz da lavagem de dinheiro no ambiente criptoeconômico.

Palavras-chave: Criptomoedas. Lavagem de dinheiro. Direito Penal Econômico.

ABSTRACT

This work analyzes the impacts of the use of crypto-assets in contemporary money laundering practices, highlighting the challenges faced by the legal system in the face of technological innovations and financial decentralization. Situated within the field of Economic Criminal Law and the prosecution of digital financial crimes, the study aims to understand how instruments such as cryptocurrencies, mixers, tumblers, and NFTs have been used to conceal the origin of illicit funds and hinder asset traceability. The deductive method is adopted, with a qualitative

¹ Advogado OAB/SC 70.860, Graduado pela Universidade Federal de Santa Catarina, Pós-Graduado em Direito Penal e Criminologia pela PUC-RS, Pós-Graduado em Defesa em Crimes de Lavagem de Capitais pela FaCiência. Endereço eletrônico: joaopmotta.adv@gmail.com

Artigo recebido em 25/08/2025 e aprovado para publicação em 27/10/2025.

Este é um artigo de Acesso Aberto, distribuído sob os termos da Licença Creative Commons (<http://creativecommons.org/licenses/by/4.0/>), que permite uso, distribuição e reprodução para fins não comerciais, com a citação dos autores e da fonte original e sob a mesma licença.

approach and bibliographic and documentary research. The results indicate that, although the Brazilian legal system has advanced with the enactment of Law No. 14,478/2022 and complementary regulations, the sophistication of the mechanisms used for digital money laundering still exceeds the regulatory and investigative capacity of the authorities. It concludes that the articulation between technological innovation, regulatory framework, and international cooperation is essential for the effective combating of money laundering in the crypto-economic environment.

Keywords: Cryptocurrencies. Money laundering. Economic criminal law.

1. INTRODUÇÃO

O presente artigo apresenta como problema central, a fim de orientar o estudo, a dificuldade de identificação, compreensão e desarticulação do ciclo da lavagem de capitais diante da incorporação dos criptoativos nas práticas ilícitas. A atuação criminosa com o uso de criptomoedas desenvolve-se em distintas fases - muitas vezes sobrepostas - e é dotada de técnicas próprias com elevado grau de sofisticação tecnológica. A despeito dos avanços legislativos, como o marco regulatório brasileiro dos ativos virtuais e do fortalecimento institucional de órgãos fiscalizadores, as práticas de lavagem vêm se adaptando ao ambiente digital e às inovações promovidas pela descentralização das transações, o que exige dos operadores do Direito constante atualização teórica e prática.

Diante desse cenário, o objetivo geral do artigo é examinar a utilização de criptoativos como instrumentos para a prática da lavagem de capitais, a partir de uma abordagem jurídico-penal e tecnológica. O estudo propõe-se a demonstrar a relação das criptomoedas com a lavagem de capitais, destrinchar acerca do pseudoanonimato desses ativos e apresentar algumas ferramentas específicas de dissimulação patrimonial, como *mixers* e *tumblers*, bem como casos práticos e a reação normativa nacional e internacional.

Apesar dos mecanismos legais já existentes, o ecossistema cripto ainda se revela desafiador pela ausência de padronização global, interoperabilidade das plataformas e complexidade das tecnologias envolvidas. Por isso, a compreensão técnico-jurídica dessas práticas se torna essencial à atuação dos operadores do Direito, tanto na investigação e persecução penal, quanto na cooperação internacional e no aprimoramento das políticas de prevenção.

Para tanto, o trabalho está estruturado da seguinte forma: o primeiro capítulo trata da relação entre criptoativos e lavagem, com destaque para os principais instrumentos utilizados para dificultar a rastreabilidade; o segundo capítulo explora casos práticos e medidas de combate, destacando os avanços e limitações na resposta normativa e tecnológica. Ao final,

Este é um artigo de Acesso Aberto, distribuído sob os termos da Licença Creative Commons (<http://creativecommons.org/licenses/by/4.0/>), que permite uso, distribuição e reprodução para fins não comerciais, com a citação dos autores e da fonte original e sob a mesma licença.

são sistematizadas as conclusões, reforçando a importância da atualização doutrinária e da integração institucional como ferramentas indispensáveis para o enfrentamento eficaz da lavagem de dinheiro no ambiente criptoeconômico.

2. A RELAÇÃO ENTRE CRIPTOMOEDAS E LAVAGEM DE DINHEIRO

Primeiramente se destaca que a preocupação em torno dessa relação é genuína, basta entender que, as criptomoedas, sendo criptografadas e com uma capacidade de esconder – ou dificultar – a identificação de seu usuário, acaba por gerar risco para as operações financeiras mal-intencionadas, possivelmente figurando a primeira fase da lavagem de dinheiro (colocação) (Savino, 2020; Silveira, 2018).

No geral, a utilização de criptoativos na lavagem de dinheiro tornou-se um fenômeno de crescente atenção para os operadores do direito penal e da persecução criminal. Criptomoedas como o Bitcoin, embora não tenham sido concebidas com propósitos ilícitos, possuem propriedades que podem favorecer condutas criminosas, especialmente – como mencionado - nas primeiras fases da lavagem de capitais.

No Brasil, para adquirir criptomoedas – Bitcoin mais especificamente – utiliza-se, em regra, *exchanges*, ocupando o papel de corretoras que fazem a intermediação entre as partes interessadas, sendo comissionada por tal serviço.

O serviço se dá, resumidamente, da seguinte forma: realizar um depósito na conta da corretora; enviar o comprovante da transação; relacionar o valor a um nome e CPF indicado; transformar o valor em moedas virtuais.

Após essa transformação na moeda escolhida, o indivíduo pode realizar o armazenamento em um software específico (carteira fria), ou, permanecer utilizando as operações na própria corretora (carteira quente), podendo enviar montantes para qualquer lugar do mundo, de maneira instantânea e discreta.

Inexistem controles próprios ou órgãos de supervisão para conferir esse CPF juntado. Cada empresa age de uma forma própria, o que acaba por figurar-se como um fator de risco

para a lavagem de capitais, devido a possibilidade de uso de pessoas interpostas para as transações (Santana, 2020).

Como um histórico exemplo em nosso país, o caso Lava Jato, especificamente na operação “pão nosso”, no qual o Ministério Público Federal investigou um desequilíbrio entre o valor de alimentos fornecidos ao sistema penitenciário e o custo de produção, as autoridades desconfiavam que os investigados teriam realizados diversas operações, as quais, juntas, totalizaram cerca de R\$300.000,00 (trezentos mil reais), todas em criptomoedas, atuando de uma nova maneira de tentar burlar o sistema da Receita Federal (Lemos, 2018). Nesse mesmo relevante caso, houve a investigação acerca dos doleiros, com o envio ou ingresso de dinheiros em outros países.

Buscando inovações nas práticas, surgem as criptomoedas como grande chamariz, devido à possível anonimidade dos utilizadores e a ausência de regulamentação sólida em âmbito nacional, dificultando a origem e destino dos recursos transacionados (Santana, 2020).

Comparativamente, se no mercado paralelo de moedas fiduciárias tradicionais existe a necessidade desse mencionado “doleiro”, com as criptomoedas qualquer indivíduo consegue transacionar altos valores para qualquer lugar do mundo, sem controle completo das autoridades (Santana, 2020).

Em contrapartida, importante destacar que o uso do Bitcoin apresenta riscos também. Apesar do pseudoanonimato ser uma vantagem para os indivíduos que busquem lavar dinheiro, a rede fornece um registro público de todas as transações feitas na blockchain. Com isso, em determinada transação suspeita, é possível fiscalizar e acompanhar pelas autoridades (Savino, 2020).

Ainda que o usuário do sistema se esconda apoiado em um pseudônimo, um mero descuido pode ser suficiente para que sua identidade venha à tona através de uma transação. Ou seja, ainda que ofereça segurança e esse isolamento da identidade, existem riscos a partir do registro público das transações (Savino, 2020).

Com o intuito de não restarem dúvidas acerca desse mencionado “pseudoanonimato”, constrói-se a seguinte tabela, demonstrando as características próprias desse fator aqui tratado, em comparação com o “anonimato” por completo:

Imagem 1 - Comparação entre anonimato e pseudoanonimato em criptomoedas

ASPECTO	ANONIMATO	PSEUDOANONIMATO
Definição	Identidade do usuário é completamente oculta	Endereço público é visível, mas não diretamente ligado à identidade real
Exemplo de criptomoeda	Monero (XMR), Zcash (modo shielded)	Bitcoin (BTC), Ethereum (ETH)
Rastreamento de transações	Extremamente difícil ou praticamente impossível	Transações podem ser rastreadas publicamente na blockchain
Ligação com a identidade do usuário	Não há vínculo visível com identidade real	Pode ser possível associar endereços à indivíduos com técnicas de análise
Privacidade das transações	Alta privacidade: valores, remetentes e destinatários ocultos	Baixa a moderada: valores e endereços visíveis publicamente
Compliance regulatório	Mais difícil implementar medidas de conformidade (KYC/AML)	Mais fácil aplicar regras de compliance, devido à transparência da blockchain
Percepção pública	Muitas vezes associada a uso malicioso (ainda que tenha usos legítimos)	Vista como tecnologia transparente, mas com riscos à privacidade

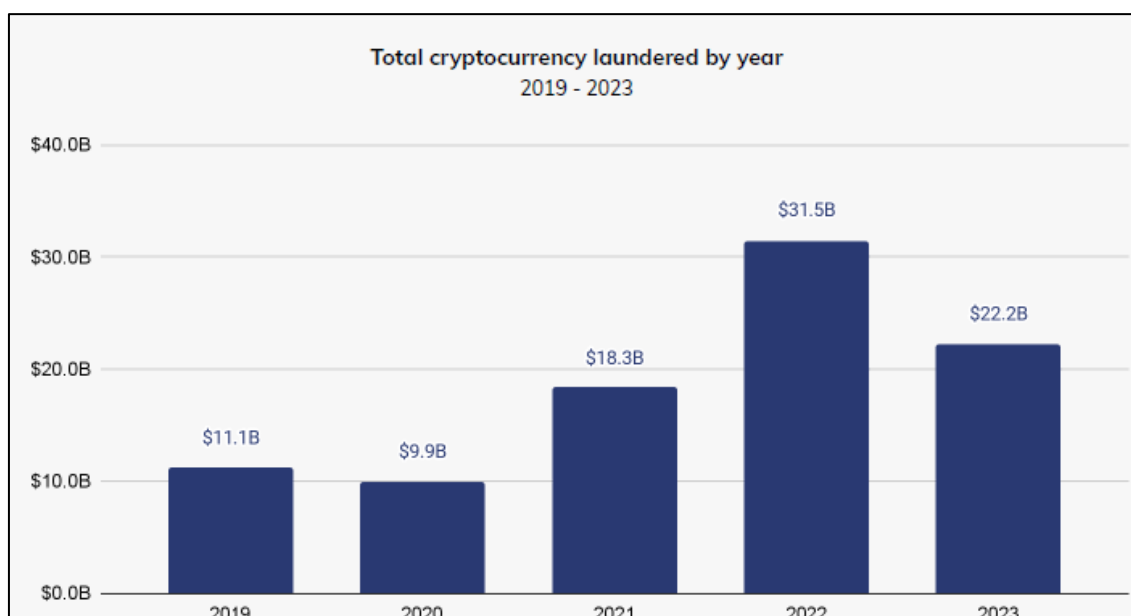
Fonte: Elaboração própria

Posto isso, entende-se como relevante destacar que, dentre todos os entes que participam de uma transação de criptomoeda, as *exchanges* são os únicos que podem ser efetivamente regulados, dependendo, portanto, exercer um papel de cooperação com as autoridades em casos de operações suspeitas ou anormais (Savino, 2020).

Segundo autores, a legislação traz mais segurança aos investidores e clientes, criando exigências para que as operações ocorram, com tipificações específicas para os delitos envolvendo ativos digitais (Junior, 2023).

Tratando de dados práticos, averigua-se os montantes de criptomoedas direcionadas para destinos ilícitos, com o passar dos anos:

Imagem 2 – Total de criptomoedas lavadas por ano (2019–2023)



Fonte: Chainalysis, 2024.

O relatório informa o montante por ano destinado (considerando o mundo inteiro), demonstrando que se tratam de valores de extrema relevância. A queda entre os anos de 2022 e 2023 podem ser associadas a redução geral no volume de criptotransações, ainda que lícitas. Mais especificamente, informam que a queda na atividade de lavagem foi mais impactante, totalizando cerca de 29,5% de diminuição (Chainalysis, 2024).

A grande parte dessas criptomoedas ilícitas teriam sido destinadas para *exchanges* centralizadas. Um dos motivos para tal seria por se configurarem como saídas fiduciárias, ou seja, plataformas que possibilitam a conversão de ativos virtuais (ainda que ilícitos) em dinheiro estatal, como dólar ou real (Junior, 2023).

Mais de 40% desses fundos mencionados são inicialmente direcionados para serviços intermediários, como *mixers* - conforme será tratado no próximo subcapítulo -, e, após isso, enviados para essas empresas para realizarem a conversão em moeda fiduciária, escondendo seu caminho ilegal (Junior, 2023).

Apesar de números elevados, ao ser comparados com a quantia estimada de dinheiro lavado ao redor do mundo em um ano, é possível perceber que a participação das criptomoedas acaba por ser insignificante, proporcionalmente. De acordo com o Escritório de Drogas e Crimes da ONU (2022), estima-se que, durante um ano, ao redor do mundo, a quantia de dinheiro lavado gire entre US\$ 800 bilhões e US\$ 2 trilhões (Junior, 2023).

Em dados mais recentes, o cenário é ainda pior. Segundo o Escritório das Nações Unidas sobre Drogas e Crime (UNODC), estima-se que entre 2% e 5% do Produto Interno Bruto (PIB) global seja lavado anualmente. Com base no PIB global de 2024, isso corresponderia a valores entre US\$ 2,22 trilhões e US\$ 5,54 trilhões por ano (Neopay, 2024).

A sofisticação também faz-se presente nesse meio, sendo possível verificar que os indivíduos estão alterando seus hábitos ilícitos. No ano de 2021, cerca de 70% de todas as transações ilícitas envolveram Bitcoin (BTC), que agora virou para ser dominado por *stablecoins*². O BTC agora responde por cerca de 20% de todas as transações ilícitas, enquanto as *stablecoins* ocupam a maioria com 63% (Knight, 2025).

Vale ressaltar que os números de 2025 podem ser distorcidos para incluir o ether (ETH) devido ao golpe sofrido por hackers que furtaram cerca de US\$ 1,5 bilhão na *Bybit* em fevereiro, que é o maior crime de Cripto até o momento.

² *Stablecoins* = criptomoeda cujo valor está atrelado a uma moeda fiduciária, como o dólar, com o objetivo de reduzir a volatilidade

Como uma das grandes alterações do ano de 2024 tem-se a ascensão do chamado “*Laundering-as-a-Service*”, que se figura como uma modalidade na qual empresas especializadas em lavar dinheiro oferecem seus serviços diretamente para os criminosos, facilitando, ou até possibilitando, as operações fraudulentas e dificultando a detecção pelas autoridades (Rubinstein, 2025).

Conforme o observado, a lavagem de dinheiro dispõe de alta demanda do mundo de criptoativos. A dificuldade das autoridades em interromperem tais ações acaba por dificultar o bloqueio das atividades ilícitas em larga escala. Porém, apesar desse desenvolvimento, tal ecossistema permanece como pequeno (em uma análise comparativa), ainda mais quando comparado com o próprio uso de criptos para outras finalidades. A atividade ilícita envolvendo esses ativos representa cerca de 1% das movimentações totais de criptomoedas (Junior, 2023).

2.1. O USO DE MIXERS E TUMBLERS PARA DIFICULTAR A RASTREABILIDADE

Primeiramente é importante definir os conceitos aqui tratados. Um “misturador de criptomoedas”, chamado de *mixers* ou *tumblers* seria um instrumento para garantir ainda mais privacidade das transações executadas, misturando suas criptomoedas com os fundos de outros indivíduos.

Tais serviços são utilizados frequentemente para ocultar informações das transações e não exigem que os usuários cumpram com o processo estabelecido no *Know Your Customer*.

Esses serviços acabam por embaralhar as transações em um único lote e redistribuir os valores para múltiplas carteiras, de maneira aleatória. Com isso, dificulta-se a reconstituição do fluxo original dos ativos, exigindo análises minuciosas com ferramentas forenses que busquem identificar padrões de movimentação (Tomaz, 2024).

Na prática, especialistas precisam recorrer a algoritmos avançados e ao cruzamento de dados entre múltiplas redes para encontrar pontos de conexão entre carteiras suspeitas.

Em termos práticos, existem dois tipos de misturadores, os centralizados e os descentralizados.

O primeiro tipo envia as criptomoedas de “A” para “B” com o pagamento de uma taxa. No caso do segundo tipo, protocolos específicos são utilizados, como o “CoinJoin”, com o intuito de ofuscar as transações realizadas. Ao depositar as moedas virtuais no sistema, elas são embaralhadas, e, na sequência, são retiradas ou enviadas para outro local a mesma quantia depositada, porém, com a natureza da fonte daquele dinheiro tendo sido alterada.

Analisando o anonimato, os *mixers* descentralizados recebem destaque, por oferecer um grau de sigilo muito maior. Isso ocorre também pelo fato de que, os centralizados detêm acesso aos endereços de IP dos usuários, sendo possível, através de uma investigação, prever qual endereço recebeu ou enviou os ativos (Gonzalez, 2022).

A título de exemplo desses dois tipos de serviços, temos:

Imagem 3 – Exemplos de mixers centralizados e descentralizados utilizados em criptoativos

CENTRALIZADOS (custodiais)	DESCENTRALIZADOS (não custodiais)
Helix Operado por Larry Dean Harmon; usado na darknet; encerrado após investigação do FBI e FinCEN em 2020.	Tornado Cash (Ethereum) Popular por transações anônimas; sancionado nos EUA em 2022 por uso ligado a hackers norte-coreanos
Bitcoin Fog Um dos mais antigos (desde 2011); acusado de lavar mais de US\$ 335 milhões em criptomoedas.	Wasabi Wallet (Bitcoin) Usa protocolo CoinJoin; foco em privacidade; monitorado por autoridades
BestMixer.io Baseado na Holanda; derrubado pela Europol em 2019; prometia anonimato, mas armazenava logs	Samourai Whirlpool (Bitcoin) Baseado em CoinJoin; foco em privacidade total com camadas de proteção.

Fonte: Elaboração própria

Conforme visualizado, existem diversos serviços que fornecem tais ferramentas, contudo, vários envolvidos em escândalos ilícitos.

Em paralelo a isso, um dos grandes desafios da regulamentação dessas ferramentas, além da complexidade técnica, reside na jurisdição e cooperação internacional, tendo em vista

que os misturadores operam, com grande frequência, em diversas jurisdições, o que passaria a exigir uma cooperação internacional para investigar e reprimir tais delitos (Belarmino, 2025).

Além do mais, o equilíbrio entra a privacidade a segurança é delicado, pois a regulamentação deveria buscar a proteção da privacidade dos usuários, mas, também, a prevenção e combate à lavagem de capitais, podendo, por muitas vezes, coexistirem esses âmbitos (Belarmino, 2025).

Conforme citado na tabela anterior, a utilização criminosa destes instrumentos acabou por gerar reações regulatórias internacionais, como os grandes casos de destaque do Tornado Cash (sancionado pelo Departamento do Tesouro dos EUA por facilitar transações de hackers ligados ao grupo Lazarus, da Coreia do Norte) e do ChipMixer (desativado pelo FBI e pela polícia alemã, acusado de movimentar mais de US\$ 3 bilhões em fundos ilícitos, incluindo golpes de *ransomware* e roubo de ativos) (Belarmino, 2025).

Já no aspecto tecnológico, o uso de ferramentas forenses de blockchain faz-se essencial. Soluções como *Chainalysis*, *Elliptic* e *Crystal Blockchain* permitem mapear transações em diferentes redes, identificar padrões suspeitos e rastrear o caminho dos ativos, mesmo após o uso de *mixers* ou *tumblers*. Essas ferramentas funcionam através da análise de metadados e do cruzamento de informações, possibilitando identificar endereços conectados e transações atípicas que podem ser ligadas a atividades ilícitas (Tomaz, 2024).

Dessa forma, ainda que dificultem o processo, a utilização dessas ferramentas não blinda por completo qualquer atividade ilícita que seja desenvolvida. As atividades de respostas para casos como os mencionados são frequentes na história recente, com grandes impactos globais na área.

2.2. CRIPTOATIVOS NÃO FUNGÍVEIS E A COMPLEXIFICAÇÃO DA LAVAGEM DE CAPITAIS

Dentre todo esse elaborado processo de lavagem de capitais, apresenta-se como recente e importante tópico os chamados “NFT’s”. Provenientes de “*non-fungible tokens*”,

essa ramificação dos criptoativos discorre sobre novas camadas de sofisticação nos mecanismos que podem atuar nos crimes financeiros aqui tratados.

Para esclarecer, no universo das criptomoedas, um token seria a representação digital de um ativo, sendo registrada na blockchain (INFOMONEY25, 2022).

Já os bens fungíveis, segundo o art. 85 do Código Civil, seriam aqueles que podem substituir-se por outros da mesma espécie, qualidade e quantidade (Brasil, 2002).

Sendo assim, uma NFT seria a representação digital de um item exclusivo, adquirindo um certificado digital de propriedade, sendo possível verificar, publicamente, sua autenticidade, sendo impossível de ser alterado. Como exemplos clássicos, tem-se obras de arte, músicas, itens de jogos, momentos esportivos, memes ou quaisquer outras transformações únicas (INFOMONEY25, 2022).

Já para diferenciar das criptomoedas, a primeira característica seria referente à fungibilidade.

Moedas clássicas como bitcoin ou ether são fungíveis. Caso você envie uma dessas moedas para um terceiro, ele poderá lhe devolve-la e continuará com o mesmo valor. Além disso, são divisíveis, sendo possíveis criar frações (no caso do bitcoin, suas frações são denominadas “*satoshis*”).

Já no caso de um NFT, ele se figura como único e indivisível, não sendo possível trocar o token de, por exemplo, uma obra de arte específica, por outro igual, tendo em vista que só existe uma unidade (como por exemplo, uma pintura de Pablo Picasso) (INFOMONEY25, 2022).

Fora isso, não é possível transferir apenas uma fração para outro indivíduo, os itens são únicos por completo.

Ao mesmo tempo, esse fator “único” desses ativos acabam por criar, em paralelo, um ambiente com potencial para estratégias de dissimulação patrimonial, com foco na ocultação de valores provenientes de atividades ilícitas.

Se um indivíduo controlar diversas carteiras, é possível simular operações comerciais legítimas através da criação, compra e revenda de NFT’s, atribuindo uma aparência lícita para

tais. Esse processo se assemelha ao *wash trading*, no qual as transações ocorrem sem alteração real da propriedade, apenas com o intuito de encobrir a origem daqueles fundos.

Fora isso, a grande subjetividade na valorização dos NFT's acaba por tornar o rastreamento ainda mais complexo, pois inexitem critérios objetivos de mercado que permitam identificar possíveis operações fraudulentas.

Um ativo digital pode ser registrado e posteriormente vendido por valores exponencialmente superiores, sem que haja um parâmetro claro de precificação, o que dificulta o monitoramento automatizado por órgãos reguladores ou instituições financeiras.

Detalha-se que essa tecnologia em questão funciona como uma assinatura digital capaz de transformar uma mídia em um bem não fungível. Sendo assim, fotos, vídeos, mensagens, domínios de sites, áudios ou quaisquer outros itens podem se tornar uma propriedade exclusiva (Homma, 2022).

Ao tornar-se bastante difundida no mercado de obras de artes, os valores se tornam fluidos, tendo em vista que, costumeiramente, tais itens são vendidos a preços exorbitantes por conta de sua exclusividade (Homma, 2022).

Em 2021, estima-se que a lavagem de dinheiro através de NFT's ultrapassou um milhão de dólares, um aumento de mais de duzentos por cento em relação ao ano anterior (Neopay, 2024).

No caso das *stablecoins* – já definidas anteriormente –, idealizadas para manter um valor mais estável por conta de sua paridade com os preços de moedas fiduciárias que as respaldam, ainda permanecem voláteis (Costa, 2025).

Essas tais podem possibilitar transações internacionais, reduzindo o tempo e os custos associados aos sistemas bancários tradicionais, fazendo com que se transfiram valores de forma quase instantânea, excluindo a presença de intermediários (Costa, 2025). Com isso, os praticantes de lavagem de capitais apoiam-se nesses facilitadores para exercerem etapas de seus delitos.

Outro aspecto relevante que igualmente se encaixa no tema em questão seria da descentralização das plataformas que negociem qualquer um desses ativos mencionados.

Atuando por pseudônimos e distantes de jurisdições tradicionais, acabam por dificultar o compartilhamento de informações com autoridades competentes. Ainda que existem iniciativas internacionais para fomentar o cumprimento de determinadas normas, a falta de harmonização regulatória global gera um entrave para a prevenção eficaz o uso indevido desses instrumentos.

Em síntese, os criptoativos não fungíveis e as *stablecoins* não apenas expandem o universo dos ativos digitais como igualmente impõe novos desafios ao sistema de combate de lavagem de capitais, unindo características tecnológicas, jurídicas e econômicas que fragmentam o controle estatal e demandam atualizações dos marcos legais e mecanismos de fiscalização, caso se busque o pleno controle de tais setores.

3. CASOS PRÁTICOS E IDENTIFICAÇÃO

Conforme discutido nos capítulos anteriores, a expansão do uso das criptomoedas, aliada à natureza descentralizada e à complexidade técnica desses ativos, tem contribuído para a criação de um ambiente propício à prática da lavagem de dinheiro. A opacidade das transações, a ausência de intermediários tradicionais e a constante inovação tecnológica representam desafios significativos para as autoridades na identificação, rastreamento e repressão de condutas ilícitas.

Neste capítulo, serão apresentados casos concretos de crimes financeiros envolvendo criptomoedas, com destaque para os métodos empregados e para as respostas adotadas pelas autoridades nacionais e internacionais. A partir dessas análises, serão discutidas também estratégias e medidas de enfrentamento voltadas à mitigação dos riscos associados a esses ativos digitais, com ênfase não apenas na elaboração jurídica, mas também na atuação prática de órgãos reguladores, fiscalizadores e operadores do direito.

3.1. ESTUDOS DE CASOS REAIS: CRIMES FINANCEIROS ENVOLVENDO CRIPTOMOEDAS

Em 2021, os crimes envolvendo criptomoedas chegaram aos quatorze bilhões de dólares (Crypto Crime Report, 2022), significando um aumento de 79% em relação ao ano anterior.

Ainda que trate-se de valor recorde, as transações ilícitas representam 0,15% das movimentações feitas com criptomoedas ao longo do ano, as quais atingiram a marca de US\$15,8 trilhões, crescendo 567% em relação a 2020 (Lanza, 2022).

De acordo com o relatório *Cryptocurrency Geography* (2021), o Brasil ocupou a 14ª posição dentre o ranking de países que adotaram as criptomoedas, totalizando 157 territórios na lista. Dentre a América Latina, o Brasil ocupa a 4ª posição, atrás apenas de Venezuela, Argentina e Colômbia (Lanza, 2022).

Dentre os crimes mais famosos envolvendo criptomoedas, o vírus “WannaCry” deve ser mencionado (E-Investidor, 2022). Em maio de 2017, mais de duzentos mil computadores distribuídos em 150 países foram infectados com o conteúdo. Dados foram limitados e furtados, sendo devolvidos mediante um pagamento de US\$600, em bitcoins. Estima-se que cerca de 140 mil dólares foram arrecadados, através de pagamentos feitos por vítimas que tentaram salvar seus arquivos.

Também no ano de 2017, a casa de câmbio “Poloniex” foi igualmente um alvo (E-Investidor, 2022). Criou-se um aplicativo falso com o nome da empresa para adquirir indevidamente moedas digitais. Com login de diversos usuários, suas criptomoedas foram acessadas e encaminhadas para outras carteiras. Contando com mais de dez mil downloads do aplicativo falso, mais de US\$140 mil foram desviados.

Outro crime envolvendo criptomoedas foi o “PlusToken Ponzi”, um esquema de pirâmide com falsas promessas de lucro rápido. Diferente dos demais, esse episódio totalizou mais de US\$3 bilhões de perdas em bitcoins (E-Investidor, 2022). Os indivíduos envolvidos coletaram as moedas, desviaram, embaralharam e misturaram, distribuindo em diversos endereços e dificultando suas localizações.

Mais um notável caso ocorreu no ano de 2021, através do site “*Poly Network*”, no qual foram coletados mais de US\$600 milhões de forma ilegal (E-Investidor, 2022). Os criminosos identificaram falhas no protocolo de interoperabilidade do sistema e acabaram por conseguir a permissão para transferir ou converter tokens utilizados em blockchains, acessando os criptoativos. O montante adquirido foi considerado o maior em finanças descentralizadas, envolvendo três criptomoedas: US\$ 267 milhões em ether, US\$ 252 milhões em binance e US\$ 85 milhões em USDC.

O crime também impactou as empresas por trás das moedas citadas, que se viram obrigadas a auxiliar na identificação dos criminosos, obtendo respostas como bloqueio de depósitos na bolsa de valores com esses ativos.

Já em fevereiro de 2025, foi possível visualizar caso de extrema relevância sobre o assunto. O presidente da Argentina, Javier Milei, promoveu, em sua conta pessoal no X, o lançamento de uma criptomoeda (\$LIBRA) (Smink, 2025).

Após esse marketing realizado, a capitalização do ativo ultrapassou os US\$4 bilhões, com mais de quarenta mil compradores. Horas após, o valor da moeda virtual despencou, após um pequeno grupo retirar quase US\$ 90 milhões de investimento.

O presidente chegou a excluir suas postagens e dizer que não conhecia os detalhes do projeto, optando por não divulgar novamente.

Tal atitude foi interpretada como um “*pump and dump*”, que seria uma tática de manipulação de mercado em que o valor de um ativo é inflado artificialmente, atraindo participantes, e, posteriormente, vendido em altos montantes, gerando a quebra de seu valor.

Esse esquema costuma dividir-se em quatro etapas: pré-lançamento, lançamento, bombeamento e despejo, sendo que as três primeiras fases foram projetadas para instigar o medo de ficar de fora nos participantes.

No Brasil, não existe uma estatística específica sobre os prejuízos a partir de crimes envolvendo criptomoedas. Porém, em caso recente, uma das maiores investigações sobre o tema ocorreu (Operação Colossus), a qual revelou um sólido esquema de evasão de divisas e lavagem de dinheiro (Leite, 2024).

Através de empresas de fachada, diversas carteiras eram administradas pelos criminosos, gerindo ativos digitais, e, movimentando, em menos de dois anos, cerca de R\$7 bilhões.

Foi possível entender que um indivíduo oferecia sua carteira de criptomoedas para o grupo criminoso, o qual utilizava-a para receber pagamentos no exterior e, posteriormente, sacar o dinheiro, sem intermediários ou controle bancário formal.

As criptomoedas eram utilizadas para esconder o dinheiro ilegal e movimentá-lo, com maiores dificuldades de rastreá-la.

3.2. MÉTODOS DE RASTREAMENTO: AVANÇOS TECNOLÓGICOS NA IDENTIFICAÇÃO DE TRANSAÇÕES ILÍCITAS

O Brasil ainda se encontra em um estágio inicial de combate aos cibercrimes, em especial à lavagem de capitais, vez que o Estado carece de tecnologias adequadas para investigação, além da vulnerabilidade dos sistemas operacionais e de segurança. Todos esses tópicos são relevantes para o constante avanço do *animus operandi* dos criminosos, os quais se aproveitam das condições gerais para transacionar ilegalmente (Nery, 2025).

Conforme já mencionado, a cooperação internacional figura-se como ferramenta crucial para o combate, devido ao fato de que, ao contrário das transações financeiras tradicionais, as transações com criptomoedas não são regulamentadas por um órgão centralizado e podem ocorrer de forma quase anônima, o que torna difícil rastrear e identificar as partes envolvidas em transações suspeitas (Granado, 2024).

Dentre diversas características a serem desenvolvidas, destacam-se (Granado, 2024):

- (i) Vulnerabilidade Técnica: diversas vezes a legislação não aborda as vulnerabilidades, como *hacks* de *exchanges* ou roubo de chaves privadas, criando lacunas e deixando as vítimas sem os devidos recursos para recuperar seus fundos;

- (ii) Regulamentação Abrangente: desenvolver regulamentações específicas para as criptos, incluindo requisitos de identificação, relatórios de transações suspeitas e conformidade com padrões de segurança cibernética;
- (iii) Aprimoramento da Educação: implementação de programas públicas para aumentar a conscientização sobre os riscos associados a tais ativos, além de orientações para tentar evitar golpes;
- (iv) Monitoramento de Transações Suspeitas: estabelecer sistemas de monitoramento para identificar atividades suspeitas, incluindo análises de padrões ou volumes incompatíveis;
- (v) Responsabilidade das *Exchanges*: possivelmente exigir a implementação de políticas de *Know Your Customer* para verificar identidades e relatar transações suspeitas para os órgãos responsáveis;
- (vi) Legislação Anti-Lavagem de Dinheiro: reforçar as leis para, não só abranger criptos de maneira geral, como também para garantir que empresas cumpram com as obrigações de compartilhar relatórios e *due diligence* (investigação proferida de maneira prévia à uma transação, como uma aquisição ou investimento, para confirmar detalhes e identificar possíveis riscos. Tal processo visa evitar surpresas indesejadas após a finalização da transação. A *due diligence* pode abranger áreas como finanças, leis, operações e conformidade. A realização adequada desse procedimento protege contra perdas, assegura a responsabilidade fiduciária e previne complicações legais);
- (vii) Auditorias Empresariais: Realizar auditorias regulares nas *exchanges* de criptomoedas para garantir que elas estejam em conformidade com as regulamentações e padrões de segurança;
- (viii) Investigação Forense Digital: Desenvolver equipes especializadas rastrear atividades criminosas relacionadas a criptomoedas e identificar os responsáveis;

- (ix) Transparência na Blockchain: promover maior transparência, permitindo que as transações possam ser rastreadas, ainda que o anonimato dos usuários se mantenha, de maneira apropriada;
- (x) Desenvolvimento de Tecnologias: Investir em pesquisa e desenvolvimento de tecnologias de segurança cibernética para proteger as carteiras de criptomoedas e as *exchanges* contra ataques.

Ou seja, para garantir maior transparência e responsabilização na administração pública, é crucial ampliar o acesso à informação, seguido pela garantia de regras claras e transparentes que sejam efetivamente aplicadas em cada decisão, e, por fim, desenvolver a capacidade de rastrear as decisões e ações até os respectivos envolvidos (Rocha, 2022).

Antes da Instrução Normativa nº 1.888 da Receita Federal, não existia uma regulamentação específica em território nacional. Igualmente, a Instrução Normativa nº 1.899 (2019) abordou de maneira clara a definição jurídica de Criptoativo e *Exchange* de Criptoativos (Trindade, 2024).

Tal regulamentação seguiu em progresso ao estipular que todas as plataformas de negociação (*exchanges*) seriam obrigadas a fornecer à Receita Federal dados abrangentes acerca das transações realizadas por seus usuários (nomes dos negociantes, valores, datas, taxas pagas, dentre outros) (Trindade, 2024).

De qualquer forma, é crucial a existência de cursos profissionalizantes que especializem os agentes envolvidos nessas ações, mantendo-os nivelados com o cenário contemporâneo (Rocha, 2022). O aprimoramento contínuo desse arcabouço regulatório e da capacidade de atuação estatal figuram-se como instrumentos de elevada importância.

A Lei nº 14.478/2022 representou um avanço ao estabelecer um marco legal, mas sua efetividade depende crucialmente da regulamentação infralegal a ser editada pelo Banco Central. É fundamental que esta regulamentação detalhe rigorosamente as obrigações de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo para todos os provedores

de serviços, incluindo procedimentos densos, monitoramento transacional baseado em risco, comunicação tempestiva e qualificada de operações suspeitas ao COAF (Nery, 2025).

Essa exigência de fornecimento de dados se aplica também aos investidores individuais que atuam de maneira autônoma, sem depender necessariamente das Exchanges. Isso ocorre nos casos em que ultrapassem o montante de R\$30.000 em transações de criptomoedas mensalmente, conforme previsto no artigo 6º, incisos II, "a" e "b", (IN) nº 1888/2019 (Trindade, 2024).

No caso das leis penais, incluiu-se o termo “ativos virtuais” para delitos que envolvam fraudes, lavagem de dinheiro e crimes contra o sistema financeiro nacional, servindo inclusive como majorante, conforme o artigo 1º, § 4º, da Lei nº 9.613/1998, aumentando de 1/3 a 2/3 caso o crime de lavagem envolva ativos virtuais, sendo equivalente, por exemplo, à reiteração delitiva (Trindade, 2024).

Por fim, observa-se certa resistência por parte de segmentos da indústria cripto à implementação de regras mais estritas, apoiando-se no argumento de que o excesso de regulamentação poderia afastar as inovações ou violar os princípios de privacidade (Nery, 2025).

Apesar dos diversos métodos de rastreamento e combate, encontrar um balanço que controle os riscos sem impedir o desenvolvimento pleno do setor, segue sendo um desafio constante para os reguladores.

4. CONSIDERAÇÕES FINAIS

A presente pesquisa buscou compreender e analisar a utilização de criptoativos como instrumentos de lavagem de dinheiro, diante das inovações tecnológicas que desafiam os mecanismos tradicionais de controle jurídico e financeiro. Inserida no campo do Direito Penal Econômico e da persecução de crimes digitais, a problemática central investigada foi: como os criptoativos têm sido utilizados para ocultar valores ilícitos e quais são os limites e possibilidades da reação normativa frente a essa realidade?

Partindo dessa problemática, formulou-se a hipótese de que os criptoativos não apenas oferecem novas formas de movimentação financeira, mas também são instrumentalizados em esquemas cada vez mais sofisticados de dissimulação patrimonial, aproveitando-se de aspectos como pseudoanonimato, descentralização e interoperabilidade global. Ao longo do estudo, observou-se que mecanismos como mixers, tumblers e NFTs representam não apenas avanços tecnológicos, mas também desafios significativos à rastreabilidade e à repressão de condutas ilícitas.

A análise revelou que, embora o ordenamento jurídico brasileiro tenha evoluído com marcos como a Lei nº 14.478/2022 e normas complementares da Receita Federal, a complexidade técnica e a velocidade de transformação do ecossistema cripto ainda superam a capacidade de atuação estatal em diversas frentes, especialmente no que tange à prevenção, detecção e repressão da lavagem de dinheiro em ambiente digital.

Como contribuição prática, destacou-se a importância do fortalecimento de mecanismos regulatórios, da capacitação técnica dos operadores do Direito e do uso de tecnologias forenses capazes de rastrear transações em blockchains públicas e privadas. Ademais, apontou-se a urgência de cooperação internacional estruturada, capaz de superar os entraves jurisdicionais que dificultam a investigação de crimes com impacto transnacional.

Para futuras pesquisas, sugere-se o aprofundamento dos impactos jurídicos das stablecoins na lavagem de dinheiro, bem como estudos empíricos sobre a efetividade dos instrumentos normativos hoje existentes. Também se recomenda o exame das tensões entre anonimato, privacidade e interesse público na regulação do ambiente criptoeconômico.

Em síntese, esta pesquisa evidencia que o combate à lavagem de dinheiro na era digital exige mais do que adaptação legislativa: impõe uma resposta sistêmica, integrada e permanentemente atualizada. A articulação entre inovação tecnológica, responsabilização institucional e cooperação global é indispensável para que o Direito acompanhe a velocidade da criminalidade digital, sem perder de vista os pilares do Estado de Direito.

REFERÊNCIAS

BELARMINO, Luis Eduardo. Anonimato e lavagem de dinheiro com criptomoedas: papel de mixers e tumblers na legislação. **Consultor Jurídico**, [S. l.], 16 fev. 2025. Disponível em: <https://www.conjur.com.br/2025-fev-16/anonimato-e-lavagem-de-dinheiro-com-criptomoedas-o-papel-de-mixers-e-tumblers-na-legislacao-atual/>. Acesso em: 21 abr. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 11 jan. 2002.

CHAINALYSIS. **The 2024 Crypto Crime Report**. [S. l.]: Chainalysis, fev. 2024. Disponível em: <https://www.chainalysis.com/blog/2024-crypto-money-laundering/>. Acesso em: 20 abr. 2025.

CONHEÇA os 5 crimes mais famosos com criptomoedas. **E-Investidor**, São Paulo, 21 abr. 2022. Disponível em: <https://einvestidor.estadao.com.br/criptomoedas/crimes-mais-famosos-com-criptomoedas/>. Acesso em: 2 maio 2025.

COSTA, Isac. Stablecoins: o dinheiro embaixo do seu colchão virtual. **Consultor Jurídico**, [S. l.], 26 fev. 2025. Disponível em: <https://www.conjur.com.br/2025-fev-26/stablecoins-o-dinheiro-embaixo-do-seu-colchao-virtual/>. Acesso em: 24 abr. 2025.

GONZALEZ, Sol. Mixers de criptomoedas: serviços mantêm o anonimato em transações. **We Live Security**, [S. l.], 25 out. 2022. Disponível em: <https://www.welivesecurity.com/br/2022/10/25/mixers-de-criptomoedas-servicos-mantem-o-anonimato-em-transacoes/>. Acesso em: 21 abr. 2025.

GRANADO FILHO, Flavio; SOZZO, Bruna. Crimes cibernéticos com criptomoedas: análise da legislação brasileira e estudo de casos. **Revista Terra & Cultura: Cadernos de Ensino e Pesquisa**, Londrina, v. 40, ed. especial, p. 303–323, 28 ago. 2024. Disponível em: <http://publicacoes.unifil.br/index.php/Revistatestes/article/view/3168>. Acesso em: 2 maio 2025.

HOMMA, Giovanna Hatsue Alves. **NFTs e o crime de lavagem de dinheiro**: o velho de roupa nova. 2022. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Presbiteriana Mackenzie, São Paulo, 2022.

ILLICIT crypto volume in 2024 hit USD 40B: a record year for stablecoin crime: Chainalysis. **CoinDesk**, [S. l.], 27 fev. 2025. Business. Disponível em: <https://www.coindesk.com/pt-br/business/2025/02/27/illicit-crypto-volume-in-2024-hit-usd40b-a-record-year-for-stablecoin-crime-chainalysis>. Acesso em: 23 maio 2025.

INFOMONEY. O que são NFTs? Entenda como funcionam os tokens não fungíveis. **InfoMoney**, [S. l.], 8 dez. 2022. Disponível em: <https://www.infomoney.com.br/guias/nft-token-nao-fungivel/>. Acesso em: 24 abr. 2025.

JUNIOR, Jeferson Lemos. **Análise da relação entre a utilização de criptomoedas e o crime de lavagem de dinheiro**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Ciências Econômicas) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023.

LANZA, Luíza. Crimes com criptomoedas somam US\$ 14 bilhões em 2021, diz relatório. **E-Investidor**, São Paulo, 14 mar. 2022. Disponível em: <https://einvestidor.estadao.com.br/criptomoedas/crimes-criptomoedas-aumentaram-2021/>. Acesso em: 2 maio 2025.

LAVA Jato no Rio identifica pela 1ª vez lavagem de dinheiro com bitcoins. **UOL**, São Paulo, 13 mar. 2018. Política. Disponível em: <https://noticias.uol.com.br/politica/ultimas-noticias/2018/03/13/lava-jato-no-rio-identifica-pela-1-vez-lavagem-de-dinheiro-com-bitcoins.htm>. Acesso em: 23 maio 2025.

LEITE, Isabela. ‘Novos doleiros’ usam criptomoedas para lavar dinheiro do crime organizado e tentar despistar investigadores. **G1**, São Paulo, 25 nov. 2024. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2024/11/25/novos-doleiros-usam>

[criptomoedas-para-lavar-dinheiro-do-crime-organizado-e-tentar-despistar-investigadores.ghml](#). Acesso em: 2 maio 2025.

NERY, Isaque Augusto Silva; ALMEIDA, Andreia Alves de. A utilização de criptomoedas para lavagem de dinheiro: a prática de ocultação de ativos virtuais na atualidade. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 11, n. 5, 2025. Disponível em: <https://periodicorease.pro.br/rease/article/view/19163>. Acesso em: 12 maio 2025.

ROCHA, Yuri de Mercês. **Prevenção à lavagem de dinheiro**: operações envolvendo criptomoedas. 2022. Trabalho de Conclusão de Curso (Graduação em Direito) – Centro Universitário de Brasília, Brasília, 2022. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/16393>. Acesso em: 7 maio 2025.

SANTANA, Vinicius. **A lavagem de dinheiro por meio de criptomoedas e o risco para Defesa Nacional**. 2020. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) – Escola Superior de Guerra, Rio de Janeiro, 2020.

SAVINO, Felipe Gardelino. Lavagem de dinheiro e bitcoin: a idoneidade da moeda digital como meio para a prática delituosa. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 115, p. 583-614, 2020.

SMINK, Veronica. Entenda o escândalo de criptomoeda envolvendo Javier Milei. **BBC News Brasil**, [S. l.], 17 fev. 2025. Disponível em: <https://www.bbc.com/portuguese/articles/ckg0gle8ydeo>. Acesso em: 2 maio 2025.

THE GLOBAL impact of money laundering in 2024. **Neopay**, [S. l.], 18 jul. 2024. Disponível em: <https://www.neopay.co.uk/the-global-impact-of-money-laundering-in-2024/#:~:text=Global%20Scale%3A%20The%20United%20Nations,%242.22%20trillion%20and%20%245.54%20trillion>. Acesso em: 24 abr. 2025.

TOMAZ, Paulo. Desafios do rastreamento de criptomoedas e como superá-los. **Raphael Souza**, [S. l.], 18 dez. 2024. Disponível em: <https://raphaelsouza.com.br/desafios-do-rastreamento-de-criptomoedas/>. Acesso em: 21 abr. 2025.

TRANSAÇÕES ilícitas com criptomoedas caíram para 0,14% em 2024, segundo Chainalysis. **BlockTrends**, [S. l.], 2025. Disponível em: <https://blocktrends.com.br/transacoes-ilicitas-com-criptomoedas-cairam-para-014-em-2024-segundo-chainalysis/>. Acesso em: 23 maio 2025.

TRINDADE, Guilherme Foschiera. **A importância da regulamentação das criptomoedas para a prevenção do crime de lavagem de dinheiro**. 2024. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2024.