Lavagem de criptoativos pela ótica da hipótese investigativa: os mixing-services e a investigação criminal

Laundering of cryptoassets from the perspective of investigative hypothesis: mixing-services and criminal investigation

Fábio Ramazzini Bechara[1]

Universidade Presbiteriana Mackenzie — São Paulo/São Paulo, Brasil

fabio.bechara@mackenzie.br

http://lattes.cnpq.br/6852406985950434

http://orcid.org/0000-0001-9680-537X

Matheus Morelli Sindona Bellizia[2]

Fundação Getúlio Vargas — São Paulo/São Paulo, Brasil

math_bellizia@hotmail.com

http://lattes.cnpq.br/8211969997860175

http://orcid.org/0000-0002-8101-8274

Resumo: O objetivo deste artigo é identificar quais são os elementos necessários à abertura de uma investigação preliminar para apuração do crime de lavagem de capitais praticado por meio de criptomoedas, mais especificamente nos casos em que o agente, na operação de transações financeiras para tanto, vale-se dos chamados *mixing-services* (serviços de mistura, mescla ou *tumblers*) para ocultar, sobretudo, a origem ilícita dos valores ou bens a serem reintegrados na economia formal com

[1] Professor dos Programas de Graduação e Pós-Graduação (Mestrado e Doutorado) em Direito Político e Econômico da Universidade Presbiteriana Mackenzie. Doutor em Direito Processual Penal pela Universidade de São Paulo. Membro do GACINT — Grupo de Análise de Conjunturas Internacionais da USP. Membro do Conselho Orientador da Escola de Segurança Multidimensional do Instituto de Relações Internacionais da USP. Promotor de Justiça em São Paulo/SP.

[2] Pós-graduando em Direito Penal Econômico pela Fundação Getúlio Vargas/SP. Graduado em Direito pela Universidade Presbiteriana Mackenzie. Advogado.

aparência de licitude. Então, busca-se solucionar o seguinte questionamento: o que deve ser aferido pelos agentes de investigação para a formulação de uma hipótese investigativa na criptolavagem manejada pelos serviços de mistura de ativos? A relevância da discussão proposta decorre do fato de que os ativos financeiros digitalizados, criptografados, e registrados em *blockchain*, denominados "criptoativos" para fins desta pesquisa, enfrentam particularidades em seu tratamento jurídico na seara criminal, especialmente em se considerando sua descentralização, (pseudo)anonimidade e globalidade, instituindo-se ambiente propício à ocultação, dissimulação e integração de capital de origem ilícita, que se potencializa com diversas ferramentas digitais de anonimidade (como os próprios *tumblers*) e a lacuna regulatória dos criptoativos no ordenamento jurídico pátrio.

Palavras-chave: Criptoativos; serviços de mistura; investigação criminal.

Abstract: *The objective of this article is to identify the elements necessary to open a preliminary investigation to determine the crime of money laundering carried out through cryptocurrencies, more specifically in cases in which the agent, in the operation of financial transactions for that purpose, uses of so-called mixing-services (mixing services or tumblers) to hide the illicit origin of the values or goods to be reintegrated into the formal economy with the appearance of lawfulness. Therefore, it seeks to answer the following question: what should be measured by the investigating agents to formulate an investigative hypothesis in cryptolaundering handled by the mixing-services? The relevance of the proposed discussion arises from the fact that financial assets digitized, encrypted, and registered on blockchain, or "cryptoassets" for the purposes of this research, face particularities in their legal treatment in the criminal field, especially considering their decentralization, pseudoanonymity and globality, establishing an environment conducive to the concealment, dissimulation and integration of capital of illicit origin, which is enhanced by various digital anonymity tools (such as tumblers themselves) and the regulatory gap for cryptoassets in the Brazilian legal system.*

Key words: *Cryptocurrencies; mixing services; criminal investigation.*

Introdução

O objetivo do presente artigo é identificar quais são os elementos necessários à abertura de uma investigação preliminar para apuração do crime de lavagem de capitais praticado por meio de criptomoedas, mais especificamente nos casos em que o agente, na operação de transações financeiras para tanto, vale-se dos chamados *mixing-services* (serviços de mistura, mescla ou *tumblers*) para ocultar, sobretudo, a origem ilícita dos valores ou bens a serem reintegrados na economia formal com aparência de licitude. Busca-se responder o seguinte questionamento: o que deve ser aferido pelos agentes de investigação para a formulação de uma hipótese investigativa na criptolavagem manejada pelos serviços de mistura de ativos?

A relevância da discussão proposta decorre do fato de que os criptoativos enfrentam particularidades em seu tratamento jurídico na seara criminal, especialmente em se considerando sua descentralização, pseudoanonimidade e globalidade,[3] instituindo-se ambiente propício à ocultação, dissimulação e integração de capital de origem ilícita.

Em linhas gerais, a prática do *mixing* consiste no envio dos ativos a múltiplos endereços eletrônicos com a finalidade de se promover, sucessivamente, remessas aleatórias para novos endereços e se encobrir

[3] ESTELLITA, Heloísa. Criptomoedas e lavagem de dinheiro. Resenha de: GRZYWOTZ, Johanna. Virtuelle Kryptowährungen und Geldwäsche. Berlin: Duncker & Humblot, 2019, p. 02. *Revista de Direito FGV*, v. 16, n. 1, jan./abr. 2020. https://doi.org/10.1590/2317-6172201955; GRZYWOTZ, Johanna. *Virtuelle Kryptowahrungen Und Geldwasch*. Berlim: Duncker & Humblot, 2019, p. 98-100.

rastros percorridos pelos valores. Sua efetividade desafia a constatação do crime de lavagem de dinheiro, notadamente dos elementos que justifiquem a instauração de uma investigação criminal.

Nesse sentido, faz-se necessário compreender a existência de tipologias procedimentais — isto é, padrões de conduta dos agentes observados em *iter criminis* — na ação delitiva dos *mixing-services*, tal como nos sinais de alerta ("*red flags*") na movimentação dos criptoativos, seja para fins de sua qualificação como indícios de materialidade da lavagem de capitais, seja para o aperfeiçoamento do seu controle e fiscalização pelo Estado.

1. Criptoativos

1.1. Notas conceituais

A moeda digital muito difere da concepção de "moeda" cotidiana, que tem em seu manejo financeiro a regulação e controle por autoridades regulatórias centrais. Do contrário, não é emitida por instituições financeiras determinadas e muito menos tem referência em moedas nacionais, surgindo como meio de troca que existe tão somente no sistema eletrônico, sem um equivalente físico, como uma moeda ou cédula.[4]

No rol das moedas digitais, as chamadas criptomoedas — como o Bitcoin, Ethereum, Litecoin e Ripple — figuram como um tipo específico de ativo operado a partir da tecnologia *blockchain*, com um sistema de dinheiro eletrônico transacionável de maneira direta entre os operadores, denominado *peer-to-peer* ("P2P"). O *blockchain*, por sua vez, é a tecnologia de anotação digital que possibilita o registro em cadeia das transações realizadas, funcionando como uma espécie de livro-razão constituído por "blocos" sequenciais e criptografados.[5]

---

[4] GAFI, Grupo de Ação Financeira. Virtual Currencies. Key definitions and potencial AML/CFT risks. Disponível em: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.

[5] KATARZYNA, Ciupa. Cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems. In: *2019 OECD Global Anti-Corruption & Integrity Fórum*, Paris, 20-21 mar. 2019, p. 04-05. Disponível em: https://coincapp.com/corruption/integrity-forum/academic-papers/Ciupa-Katarzyna-cryptocurrencies.pdf.

O aspecto fundamental do *blockchain* é o registro de informações contido nesses blocos. No caso do Bitcoin, por exemplo, as informações que constam no registro são as de entrada (*input*; onde está o valor a ser enviado), do valor remetido (número de Bitcoins) e de saída (*output*; o endereço eletrônico para o qual o montante será remetido). Os blocos são criados a partir de uma "sequência anterior", que armazena informações sobre operações pretéritas, dando-se origem a uma cadeia digital de dados (*ledger*).[6]

Valendo-se de um complexo mecanismo de validação e autorização das informações adicionadas à cadeia de dados, "a tecnologia [*blockchain*] torna dispensável para sua mecânica de operação a necessidade de um agente certificador ou [de] qualquer intermediário".[7] Diferentemente do que ocorre no tráfego do dinheiro eletrônico, em que os bancos desempenham esse papel regulatório central, a operação dos criptoativos é marcada, assim, por sua descentralização.

Em grande parte das plataformas de operação de criptomoedas, não se exige a identificação dos usuários, já que cada unidade do ativo adquirida é monitorada por um conjunto de chaves de acesso digitais que a autenticam, de forma que o "detentor da moeda receba uma chave privada que serve para validá-lo como o proprietário legal dos ativos" (tradução nossa).[8]

---

[6] DE MICHELI, Leonardo Miessa. *Blockchain, criptoativos e os títulos circulatórios do Direito Comercial*. Tese (Doutorado em Direito) — Faculdade de Direito da Universidade de São Paulo, Universidade de São Paulo, São Paulo, 2020, p. 60.

[7] *Ibid*., p. 61.

[8] ELSAYED, Sayid. Cryptocurrencies, corruption and organised crime: Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption. [*s. l.*]. Transparência Internacional, *U4 Helpdesk Answer*, 28 mar. 2023, p. 05. Disponível em: https://www.giz.de/en/downloads/cryptocurrencies-corruption-and-organised-crime.

Autores como Johanna Grzywotz[9], Heloisa Estellita[10], Henry Hillman[11] e Felipe Américo Moraes[12] defendem que a mínima identificação por parte dos operadores cripto (os *traders*), somada ao registro das transações em *blockchain*, permite a conclusão por sua pseudoanonimidade. Isso porque, embora não se faça indispensável a identificação de dados pessoais do *trader* para a operação de criptomoedas — já revestida de certa privacidade garantida pela criptografia inerente a esses ativos —, "o fluxo de transações é todo registrado no *blockchain*, o que dá uma transparência relevante quanto a todo o histórico de transações".[13]

Além do mais, os criptoativos em geral gozam de caráter transacional fundado em sua globalidade, podendo circular livre e indistintamente pelo mundo sem esbarrar em noções geográficas e econômicas de fronteira. Ciupa Katarzyna coloca que "as criptomoedas têm um caráter global e podem circular livremente através das fronteiras e são bastante fáceis de usar" (tradução nossa),[14] bastando para tanto a simples instalação de *software* específico, descartando-se as diversas etapas administrativas e burocráticas exigidas no financeiro tradicional.

A sua descentralização, pseudoanonimidade e globalidade, aliados à simplicidade que envolve sua aquisição e transação, tornam o ambiente dos criptoativos convidativo ao cibercrime, que se sofistica com a adoção de manobras digitais de anonimato.[15] Apesar de a codificação criptográ-

---

9 GRZYWOTZ, Johanna. Virtuelle Kryptowahrungen ... *op. cit*., p. 99-100.

10 ESTELLITA, Heloísa. Criptomoedas e lavagem ... *op. cit*., p. 02.

11 HILLMAN, Henry Daniel. *Money laundering through cryptocurrencies: analysing the response of the United States and Australia and providing recommendations for the UK to address the money laundering risks pose by cryptocurrencies*. Tese (Doutorado em Filosofia — Faculty of Business and Law, University of the West of England, Bristol, 2020, p. 20-21.

12 MORAES, Felipe Américo. *Bitcoin e lavagem de dinheiro*: quando uma transação configura crime. São Paulo: Tirant lo Blanch, 2022, p. 142-143.

13 ESTELLITA, Heloísa. Criptomoedas e lavagem ... *op. cit*., p. 03.

14 KATARZYNA, Ciupa. Cryptocurrencies: opportunities ... *op. cit*., p. 05.

15 MORAIS, Fábio Luiz de; FALCÃO, Rondinelli Melo Alcântara. A regulação de criptomoedas como instrumento de prevenção à lavagem de dinheiro. *Cadernos Técnicos da GCU — Coletânea de Artigos Correcionais*, [*s. l.*], v. 3, p. 110-134, nov. 2022, p. 115-116. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/607.

fica das criptomoedas tender para a segurança no uso de dados, pode se servir para inviabilizar o controle e a regulamentação sobre transações ilícitas com a adoção de diversas técnicas desenvolvidas no campo digital, especialmente quando em função da lavagem de capitais.[16]

1.2. *Mixing-services* e o crime de lavagem de capitais

Define-se o delito de lavagem de capitais como o ato, ou sequência de atos, por meio dos quais se busca "mascarar a natureza, origem, localização, disposição, movimentação ou propriedade de bens, valores e direitos",[17] de origem delitiva ou contravencional, para sua reinserção no sistema econômico formal com a falsa percepção de licitude, procedendo-se em três fases procedimentais, quais sejam: colocação, dissimulação e integração.

Dentre as manobras de anonimato acima referidas, destaca-se os *mixing-services*, plataformas digitais que se prestam à dissociação do dinheiro operado por criptomoedas de sua origem ilícita, forjando transações irrelevantes previamente programadas para, então, proceder-se com a troca aleatória dos ativos designados. O serviço de mistura determina a quantidade fixa de criptoativos que pode ser misturada, conforme o interesse do depositante, enviando os valores para destinos aleatórios. Feita a divisão e remessa dos valores, promove-se a sua volta às chaves geradas pelo remetente, deduzindo-se uma "taxa de mistura".[18]

A principal finalidade dos *tumblers* na lavagem de dinheiro consiste na quebra do elo inicial entre a obtenção ilícita de valores, sua conversão em ativos criptografados e a sua reinserção na economia formal com aparência de licitude. Nesse momento de dissimulação, busca-se misturar os

---

[16] GAFI, Grupo de Ação Financeira. Virtual Currencies ... *op. cit*.

[17] BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. *Lavagem de dinheiro:* aspectos penais e processuais penais. 5. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2022, p. 25.

[18] LIU, Mingdong; CHEN, Hu; YAN, Jiaqi. Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework. *Frontiers in Physics — Section of Social Physics*, v. 9, p. 01-08, jul. 2021, p. 01-02. https://doi.org/10.3389/fphy.2021.665399.

ativos ilicitamente adquiridos para encobrir os registros em *blockchain* de sua ilegalidade e garantir maior anonimidade às transações realizadas.[19]

No modelo tradicional de *mixing*, a plataforma cria endereços de depósito aleatórios para o interessado. A cada vez que a página *web* da solicitação de mistura é atualizada, serão gerados mais endereços. Em seguida, espera-se até que outras solicitações de mistura sejam registradas e outros usuários depositem o dinheiro nos endereços eletrônicos gerados pelo site. Na próxima etapa, tida como intermediária, o serviço "cria transações nas quais essas 'X' entradas são trocadas aleatoriamente e transferidas a 'X' endereços de saída anônimos para limpar o rastro da transferência de dinheiro entre o remetente e o destinatário" (tradução nossa).[20]

Esses serviços apresentam, ainda, variantes operacionais mais modernas. Nelas, o dinheiro é enviado a um endereço de depósito aleatório criado pela plataforma, mas, ao contrário do que ocorre na modalidade tradicional, não se faz necessária a espera pelo recebimento de valores de outras pessoas. Os ativos são embaralhados e remetidos a endereços gerados aleatoriamente, entregando-se os valores já dissimulados ao destinatário final, interessado na mistura. A remessa pode ser fracionada em pequenas transações e direcionada a diversos endereços,

---

[19] WEISHEIMER, Evandro [*et al.*]. *Criptolavagem e compliance*: tipologias de lavagem de dinheiro por meio de criptoativos e sua prevenção. 2. ed. São Paulo: Editora Rideel, 2024, p. 77-79. Não se descarta, entretanto, que o seu uso não necessariamente está relacionado à lavagem de capitais ou a qualquer outra atividade ilícita, podendo se prestar à garantia de anonimidade dos detentores de grandes carteiras de criptoativos e à proteção de sua identidade, tal qual se verá adiante.

[20] SHOJAEENASAB, Ardeshir; MOTAMED, Amir Pasha; BAHRAK, Behnam. Mixing detection on Bitcoin transactions using statistical patterns. *Institution of Engineering and Technology (IET) Blockchain*, [*s. l.*], v. 3, set. 2023, p. 02. https://doi.org/10.1049/blc2.12036. Sobre o funcionamento dos serviços de mistura, ilustra Eric Morse: "Suponha que alguém guardou o número de série de todas as cédulas de dólares que você possui para rastrear seus gastos. Você e três estranhos colocam todo o dinheiro em uma caixa de papelão. Você sacode a caixa e retira o mesmo montante que colocou. Você tem a mesma quantidade de dinheiro que tinha antes, mas você não possui as mesmas cédulas (tradução nossa)" — MORSE, Eric. *Bitcoin*: uma introdução simples. Tradução: João Rossi Parreiras. Nova Jersey: Babelcube Inc., 2017, p. 677.

fazendo com que as transações de envio (inicial) e recebimento (final) não travem relação entre si.[21]

Sobre a rastreabilidade das operações de mescla, Younggee Hong *et al.*[22] ponderam que, muito embora já existam estudos e análises sobre serviços de mistura — que compõe uma literatura científica ainda limitada —, seus resultados propõem soluções de rastreamento das operações aplicáveis a plataformas específicas (processo chamado de *de-mixing*), algumas delas já encerradas por determinação judicial, ou em decorrência da evasão virtual de *mixers*.

Möser, Böhme e Breuker[23], por exemplo, puderam rastrear transações feitas por meio do serviço de mistura '*BitLaundry*', interligando endereços de entrada e saída até a sua fonte ao seguir as poucas operações que esse *mixer* realizava ao ser acionado. Balthasar e Hernandez-Castro[24] elaboraram um algoritmo próprio à plataforma de mescla '*DarkLaunder*' que permitia o rastreamento dos criptoativos misturados e mapeava o seu padrão, ou método, numeral de operação, enquanto Hanbiao Du *et al.*,[25] mais recentemente, propuseram uma análise gráfica de dados próprios da

---

21 VAN WEGBERG, Rolf; OERLEMANS, Jan-Jaap; VAN DEVENTER, Oskar. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime (JFC)*, [*s. l.*], v. 25, p. 419-435, mai. 2018, p. 423. https://doi.org/10.1108/jfc-11-2016-0067.

22 HONG, Younggee [*et al.*]. A Practical De-mixing Algorithm for Bitcoin Mixing Services. In: *ACM Asia Conference on Computer and Communications Security*, Incheon, 4 jun. 2018, p. 16-17. https://doi.org/10.1145/3205230.3205234.

23 MÖSER, Malte; BÖHME, Rainer; BREUKER, Dominic. An inquiry into money laundering tools in the Bitcoin ecosystem. In: *IEEE 2013 APWG eCrime Researchers Summit*, São Francisco, 17-18 set. 2013. Disponível em: https://ieeexplore.ieee.org/document/6805780.

24 RATHORE, Mazhar; CHAURASIA, Sushil; SHUKLA, Dhirendra. Mixers Detection in bitcoin network: a step towards detecting money laundering in crypto-currencies. In: 2022 IEEE International Conference on Big Data, Osaka, 17-20 dez. 2022. Disponível em: https://ieeexplore.ieee.org/document/10020982.

25 DU, Hanbiao [*et al.*]. Breaking the Anonymity of Ethereum Mixing Services Using Graph Feature Learning. IEEE Transactions on Information Forensics and Security, Nova Iorque, v. 19, p. 616-631, out. 2024. Disponível em: https://ieeexplore.ieee.org/document/10292691.

criptomoeda Ethereum que calcula a probabilidade de correlação entre ativos misturados no sistema '*Tornado Cash*'.

No entanto, a análise substancial desses serviços se mostra comprometida pois os seus administradores muito pouco publicam sobre a sua metodologia de funcionamento interno, o que se agrava com diversos outros padrões procedimentais de incremento à anonimidade, como o estabelecimento de *delays* nos endereços de saída do *mixer*, a cobrança de taxas aleatórias dos interessados na mistura e a disponibilidade exclusiva de alguns *tumblers* na *Deep Web* e *Dark Net*.[26]

Isto é, se as transações de mistura são realizadas sem lacunas virtuais que viabilizem o processo de *de-mixing*, efetivamente não se pode aferir conexão entre os ativos depositados e recebidos após a mescla, frustrando-se o rastrear do caminho dos valores transacionados e da 'história de vida' dos criptoativos.[27] A emergência dos *tumblers*, suas variantes procedimentais e a limitada pesquisa empírico-experimental sobre o seu funcionamento fazem difícil o rastreamento da origem dos valores operados, já que, de acordo com o entendimento especializado majoritário, as operações de *mixing* tem o potencial de tornar virtualmente impossível a ligação entre as moedas digitais operadas e a sua fonte ilícita.[28]

Os *mixing-services*, portanto, tem a capacidade de eliminar a transparência da operação de criptomoedas — mesmo que registradas em *blockchain* — tornando difícil a aferição de seus rastros com o significativo aumento de anonimidade e, consequentemente, facilitam a dissimulação da origem ilícita de valores convertidos nesses ativos.

---

[26] CRAWFORD, Jesse; GUAN, Yong. Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy. In: *IEEE 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 15 mar. 2020, p. 38-45, Nova Iorque, p. 41-42. https://doi.org/10.1109/sadfe51007.2020.00013.

[27] *Ibid*.; ELSAYED, Sayid. Cryptocurrencies, corruption ... *op. cit*., p. 05.

[28] Nesse sentido, confira-se: VAN WEGBERG, Rolf; OERLEMANS, Jan-Jaap; VAN DEVENTER, Oskar. Bitcoin money laundering ... *op. cit*., p. 423; LIU, Mingdong; CHEN, Hu; YAN, Jiaqi. Detecting Roles of Money Laundering ... *op. cit*., p. 01-02; ELSAYED, Sayid. Cryptocurrencies, corruption ... *op. cit*., p. 05-06.

2. Persecução penal: da Investigação Preliminar

2.1. Notas conceituais

Sabe-se que, majoritariamente, a persecução penal se divide em duas fases: a investigação preliminar e o processo judicial, que a sucede. A primeira visa a apuração de fatos típicos e ilícitos que chegaram ao conhecimento da autoridade competente — seja por meio de inquérito policial, presidido pelo delegado de polícia, seja através de procedimento investigatório criminal, conduzido pelo Ministério Público —, visando à obtenção de elementos de informação que corroborem uma hipótese investigativa e embasem o oferecimento de uma ação penal.[29]

Aury Lopes Júnior pontua que a finalidade da investigação preliminar não se traduz na plena descoberta ou esclarecimento da existência de um crime, mas na probabilidade da sua existência e autoria, que se prestarão à formação da *opinio delicti* do Ministério Público, ou querelante, cumprindo uma função pré-processual.[30]

Ao contrário do método adotado no processo propriamente dito, em que já há na denúncia uma hipótese fática definida, consistente na prática de um crime de autoria determinada, o contexto da investigação pressupõe a formulação de hipóteses iniciais pelo investigador concebidas a partir de um raciocínio abdutivo, realizando-se inferências das quais se derivam as diligências investigatórias.[31]

O método abdutivo parte de um raciocínio inferencial que permite explicar a ocorrência de um fato desconhecido através da atividade de conjectura, formulando-se uma hipótese explicativa.[32] Do ponto de

---

[29] BADARÓ, Gustavo Henrique. *Processo Penal*. 3. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2015, p. 113-114.

[30] LOPES JÚNIOR, Aury. *Sistemas de investigação preliminar no processo penal*. 2. ed. rev., atual. e ampl. Rio de Janeiro: Lumen Juris, 2003, p. 314-315.

[31] BADARÓ, Gustavo Henrique. *Epistemologia Judiciária e Prova Penal*. 2. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2023, p. 149-150.

[32] TUZET, Giovanni. Razonamiento probatorio: ¿deducción? ¿inducción? ¿abducción? In: AMADO, Juan Antonio García; BONORINO, Pablo Raúl (coord.). *Pruba y razonamiento probatorio em el Derecho. Debates sobre abducción*. Granada: Comares, 2014, p. 123.

vista cronológico, a abdução se desvela dos fatos conhecidos para as suas possíveis explicações, ou seja, do presente para o passado. Sobre tais inferências no âmbito processual penal, Gustavo Henrique Badaró leciona que "enquanto na dedução se conclui algo que tem que ser; e na indução algo que provavelmente será, a abdução simplesmente sugere algo que pode ser".[33]

No ensinamento de Giovanni Tuzet, em se tratando de importante dimensão do racionamento probatório que abrange a primeira fase da reconstrução histórica dos fatos, requer-se uma dose de criatividade do investigador, influenciada pela liberdade na seleção de dados empíricos a serem considerados e sua bagagem cultural, acumulada por experiências anteriores.[34] Justamente por isso, para que se instaure uma investigação preliminar, deve a autoridade responsável se deparar pelo menos com indícios materialidade que despertem a formulação de uma hipótese investigativa inicial referente à ocorrência de um ilícito penal.

Ocorre que, quando um agente se vale dos *mixing-services* para fins de criptolavagem, a verificação desses indícios pelo investigador não só encontra óbice nas noções técnicas e de anonimidade dos *tumblers*, mas na lacuna regulatória dos criptoativos e suas implicações no combate à lavagem de capitais, como se passa a abordar.

2.2. Óbices à formulação de uma hipótese investigativa de criptolavagem

2.2.1. *Mixing-services* e ferramentas de anonimidade

A cadeia de dados registrada em *blockchain* é pública e indica o trajeto dos criptoativos transacionados. Essa transparência viabiliza a obtenção de informações que, sob o olhar das autoridades, poderiam indicar a ocorrência de atos de lavagem, sendo esse aspecto extremamente útil para a instauração e o deslinde de investigações criminais, já que sua efetividade está diretamente vinculada à verificação de chaves-públicas

[33] BADARÓ, Gustavo Henrique. Epistemologia Judiciária ... *op. cit*., p. 103.

[34] TUZET, Giovanni. Razonamiento probatorio: ¿dedución? ... *op. cit*., p. 128.

das carteiras digitais operadas sob suspeita, contendo todo o caminho percorrido pelos valores.[35]

Como o *mixing* é um método de dissimulação capaz de tornar virtualmente impossível a verificação do caminho percorrido pelas criptomoedas embaralhadas, caso se depare com registros de transações de lavagem operadas por meio de um *tumbler*, o investigador ou uma unidade de inteligência financeira não teriam — de imediato, e tão só com base em metadados descobertos — indícios que sustentariam a abertura de uma investigação preliminar, exatamente por não se poder aferir suspeita dos atos de lavagem e sua conexão com o crime que os antecedeu.

Para encobrir ainda mais esses indícios, conforme estudo desenvolvido por Jesse Crawford e Yong Guan, em que foram mapeados dezenas de serviços de mistura, a maioria dessas plataformas aconselham os seus usuários a acessá-las por meio de *softwares* que garantam maior anonimidade e, de tal forma, não despertem suspeita das autoridades — eliminando rastros de operações ilícitas —, como o "TOR" (acrônimo para "*the onion router*"), canal de entrada às camadas da *Deep Web*,[36] comumente associada ao cibercrime.[37]

É dizer, a mistura tem o potencial de suprimir indícios de autoria e materialidade que dariam origem a uma hipótese inicial (abdutiva) de investigação ("uma *ledger* possivelmente contém registros de operações

---

[35] CRAWFORD, Jesse; GUAN, Yong. Knowing your Bitcoin ... *op. cit.*, p. 43-45; MENDONÇA, Lawrence Lino Monteiro de; DIAS, Gabriel Bulhões Nóbrega. Quebra de sigilo telemático como meio de investigação da criptocriminalidade. Disponível em: https://www.migalhas.com.br/coluna/informacao-privilegiada/384513/quebra-de-sigilo-como-meio-de-investigacao-da-criptocriminalidade.

[36] A *Deep Web* é a parte da rede de computadores cujo conteúdo não está disponível ou indexado nos principais mecanismos de pesquisa (Google, Bing e Yahoo), sendo formada por milhões de páginas com larga dimensão e crescimento similar ao da internet visível ("*Surface Web*"). A internet profunda engloba uma rede ainda mais privativa, conhecida como *Dark Net*, que só pode ser acessada com *softwares* específicos para navegação em ambientes criptografados e anônimos, propícios à prática furtiva (abaixo do radar das autoridades) de crimes cibernéticos — SHIMABUKURO, Adriana; SILVA, Melissa Garcia Blagitz de Abreu. Internet, Deep Web e Dark Net. In: SILVA, Ângelo Roberto Ilha da (org.). *Crimes Cibernéticos*. Porto Alegre: Livraria do Advogado, 2018, p. 255.

[37] CRAWFORD, Jesse; GUAN, Yong. Knowing your Bitcoin ... *op. cit.*, p. 42-43.

suspeitas"), levando-se ao esclarecimento de que registros em *blockchain* conteriam, ou não, transações feitas em prol da lavagem de dinheiro. No ambiente dos criptoativos, a supressão desses elementos ganha força com o implemento de ferramentas de incremento de anonimidade, que não seriam realizáveis no sistema econômico tradicional, tornando mais trabalhoso o monitoramento das transações exercido pelas unidades de inteligência.[38]

2.2.2. Lacuna regulatória dos criptoativos

A Lei de Lavagem de Dinheiro (Lei nº 9.613/1998) impõe aos denominados "sujeitos obrigados", entidades privadas que atuam em setores-chave da economia, uma série de obrigações administrativas à sua prevenção e combate. Dentre essas obrigações, destacam-se as diligências para a identificação de clientes e operadores ("*know your client*", ou "KYC"), a compreensão da origem de valores transacionados, tal como a monitoração de transações financeiras e seu reporte aos setores competentes.[39]

No sistema econômico tradicional e centralizado, cabe ao Conselho de Controle de Atividades Financeiras ("COAF"), órgão administrativo de inteligência financeira vinculado ao Banco Central do Brasil, receber dados sobre operações suspeitas, organizá-los e disseminá-los às autoridades competentes para a investigação de delitos eventualmente praticados.[40] No ambiente das criptomoedas, por sua vez, o uso de tecnologia de registros distribuídos ("*distributed ledger technology*", ou "DLT") independe de autoridades centrais, permitindo-se a criação de uma 'comunidade supraestatal' para o armazenamento de metadados referentes às transações cripto, marcadas, sobretudo, pela desintermediação econômica.[41]

---

[38] ESTELLITA, Heloísa; TUMBIOLO, Mariana. Criptomoedas e lavagem de dinheiro: por que regular? *Revista do Advogado (AASP) — Direito e criptoeconomia*, São Paulo, n. 156, p. 157-163, nov. 2022, p. 60.

[39] *Ibid*.

[40] BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. Lavagem de dinheiro ... *op. cit.*, p. 48-49.

[41] COSTA, Isac Silveira da. O futuro é infungível: tokenização, non-fungible tokens (NFT's) e novos desafios na aplicação do conceito de valor mobiliário. *Revista de Direito das Sociedades e Valores Mobiliários*, [*s. l.*], v. Especial, 2022.

Além disso, a mínima necessidade de identificação pessoal dos detentores de carteiras virtuais inviabiliza diligências adotadas para o mapeamento de características do cliente (KYC) que levariam, por exemplo, à identificação do operador e à conclusão pela incompatibilidade econômica da movimentação de recursos e o seu patrimônio, despertando o alerta das autoridades.[42] Nessa linha, Heloisa Estellita e Mariana Tumbiolo asseveram que o fato de o sistema de registros distribuídos não estar sujeito a uma jurisdição determinada — o que redunda da globalidade dos criptoativos — torna possível a circulação de altos valores livremente, "sem quaisquer obstáculos fronteiriços e sem a vigilância de instâncias de controle, supervisão ou monitoramento".[43]

Assim, a falta de uma instância centralizadora, mecanismos de identificação mínima dos operadores, a globalidade dos criptoativos e a anonimidade conferida pelos serviços de mistura afeta diretamente a figura dos *gatekeepers*[44] e, consequentemente, o reporte de movimentações suspeita às autoridades competentes, que dariam base à abertura de uma investigação preliminar e direção às suas diligências. Renato de Mello Jorge Silveira ressalta que as criptomoedas não são em si meios criminosos, mas que "a sua edificação em um universo sem maiores previsões normativas acabou por gerar um sem-número de dúvidas".[45]

De acordo com a novel Lei de Ativos Virtuais (Lei nº 14.478/2022), as *exchanges* devem desempenhar papel na comunicação de operações financeiras e identificação de seus clientes, atuando como *gatekeepers*. No entanto, as transações misturadas com registro em *blockchain*, em razão

---

[42] MORAIS, Fábio Luiz de; FALCÃO, Rondinelli Melo Alcântara. A regulação de criptomoedas ... *op. cit*., p. 115.

[43] ESTELLITA, Heloísa; TUMBIOLO, Mariana. Criptomoedas e lavagem de dinheiro ... *op. cit*., p. 161.

[44] Os *gatekeepers* (ou "torres de vigia"), são entes da esfera privada obrigados a colaborar com a prevenção à lavagem de dinheiro. São responsáveis pelo armazenamento de dados de clientes e suas operações, realização de análises de risco e comunicação de atos suspeitos da prática de crime — BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. Lavagem de dinheiro ... *op. cit*., p. 36-37.

[45] SILVEIRA, Renato de Mello Jorge. Aspectos penais da criptoeconomia. *Revista do Advogado (AASP) — Direito e criptoeconomia*. São Paulo, n. 156, p. 151-157, nov. 2022, p. 155.

da sua limitada rastreabilidade e das ferramentas digitais de anonimidade no uso de *tumblers*, encobririam suspeitas que eventualmente dariam causa a um reporte e à posterior tomada de diligências investigativas.

Muito embora se trate de disposição relevante para o combate à lavagem de dinheiro, a ausência de regulamentação infralegal sobre a atuação das *exchanges* e demais prestadoras de serviços virtuais prejudica o cumprimento do dever em comunicar operações sob as quais recaiam suspeitas.[46] Sem a devida regulação e o controle normativo do universo cripto, que inclui os *mixing-services*, cabe às autoridades investigativas a percepção de que devem ser estruturados novos limites de compreensão entre o suspeito (aparentemente ilegal) e o não suspeito (legal) na operação de criptoativos.[47]

A probabilidade da ocorrência da lavagem de capitais e os elementos que sustentam a abertura de uma investigação para apurá-la, então, encontram base nas nuances técnicas das criptomoedas, advindas dos ideais de privacidade em que sua criação foi baseada, e na identificação de sinais de alerta, que carecem de estudo especializado. A alta anonimidade dos serviços de mistura e a lacuna regulatória dos criptoativos reforçam a importância da compreensão dos sinais de alerta no manejo de ativos virtuais, que antecipam tipologias penais eventualmente verificadas pelas autoridades para a abertura de uma investigação formal.

3. Hipótese Investigativa

3.1. Sinais de alerta no manejo de criptoativos

Os sinais de alerta, ou *red flags*, conforme definição atribuída pelo Grupo de Ação Financeira ("GAFI"), são padrões de conduta verificáveis nas operações de criptolavagem que dão "suporte ou causa a

---

[46] COSTA, Isac Silveira da. Eficácia ineficaz: a Lei 14.478 entrará em vigor sem relevância prática. Disponível em: https://www.conjur.com.br/2023-mai-31/fintech-crypto-lei-144782022-entrara-vigor-relevancia-pratica/.

[47] SILVEIRA, Renato de Mello Jorge. Aspectos penais da criptoeconomia ... *op. cit.*, p. 155.

uma investigação criminal e a interrupção das atividades ilícitas".[48] Esses sinais compõe os múltiplos indicadores de que uma transação, sem lógica financeira[49], tem o potencial de levantar suspeitas quanto a atividades criminosas no manejo de ativos virtuais, de forma que a presença de apenas um, ou alguns, desses indicadores não obrigatoriamente sinaliza a prática de um ilícito penal.[50]

Com base no estudo de centenas de casos de lavagem por criptoativos, o GAFI elenca uma série de *red flags* no manejo de criptoativos, relacionadas, *v.g.*, ao montante e frequência das transações, às características dos ativos transacionados, emprego de ferramentas de anonimidade, irregularidades verificadas na criação de carteiras digitais, perfil do *trader* e fonte dos valores enviados ou recebidos.[51]

Em que pese para cada etapa de lavagem tenham sido vislumbradas novas técnicas de lavagem e anonimato no uso criptomoedas, mostra-se fundamental a identificação de "pontos de interesse" para a abertura de uma investigação sobre criptolavagem, antecipando-se possíveis tipologias penais, muito embora haja divergência doutrinária sobre o tema.[52]

Sem embargo, levando-se em conta que o *mixing* suprime indícios de autoria e materialidade delitiva da lavagem de capitais, e que as lacunas regulatórias do ordenamento jurídico pátrio dificultam o reporte desses indícios às autoridades investigativas, tais pontos de interesse gozam de

---

[48] GAFI, Grupo de Ação Financeira. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, p. 56. Disponível em: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance.

[49] Na redação original: "*without logical business explanation*" (GAFI, 2020, p. 06).

[50] GAFI, Grupo de Ação Financeira. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, p. 07. Disponível em: https://www.fatf-gafi.org/en/publications/Methodsandtrends.

[51] *Ibid*.

[52] Renata da Silva Rodrigues explica que esse dissenso "parece gravitar essencialmente em torno da questão se a tecnologia em si é suficiente para configurar a ocultação e a dissimulação de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal", ou se outras circunstâncias atreladas a uma transação se mostram necessárias para configurar o tipo penal — RODRIGUES, Renata da Silva. Uso de Bitcoins em atos de lavagem: dissensos doutrinários. *Boletim do IBCCRIM*, São Paulo, v. 32, n. 380, p. 18-21, 2024, p. 24. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1052.

especial relevância. Conferindo direção investigativa caso a caso, os *red flags* servem, também, como base para a elaboração de Relatórios de Inteligência Financeira ("RIF") pelo COAF.

O conteúdo de um RIF, documento no qual se expõe as operações e as razões pelas quais o COAF as classifica como suspeitas de lavagem de dinheiro, dá às autoridades investigativas maior direção sobre a materialidade delitiva de transações possivelmente ilícitas, mas sem veicular juízos acusatórios e nem mesmo provas da prática de crimes.[53] A partir disso, a obtenção de elementos de informação que corroborem uma hipótese investigativa (a prática de criptolavagem) se daria através de meios de obtenção de prova como a busca e apreensão e a quebra de sigilo telemático, já que os dados de interesse investigatório no âmbito das criptomoedas são de fonte fechada.

Assim, os sinais de alerta se prestam à identificação e posterior comunicação de operações suspeitas de lavagem, com redobrada relevância no âmbito dos criptoativos, possibilitando maiores esclarecimentos sobre transações de legalidade questionável e dando viabilidade ao conhecimento de elementos que dariam causa à instauração de procedimentos investigatórios.

3.2. Tipologias da criptolavagem

Muito embora os sinais de alerta no manejo de criptoativos figurem como o principal meio de informação pelo qual se concebe uma hipótese investigativa, a sua verificação, por si só, não justifica a tomada de direções investigativas pelos delegados de polícia ou pelo Ministério Público, eis que devem ser sopesados caso a caso.[54] Para fins investigatórios, de nada vale a aferição de *red flags* se deles não se extrai a eventual prática de um crime.

As operações suspeitas de lavagem e as informações correlatas reportadas por um órgão de inteligência, ou eventualmente aferidas pelas

---

[53] BECHARA, Fábio Ramazzini. Natureza jurídica do Relatório de inteligência financeira do COAF. *Revista Fórum de Ciências Criminais — RFCC*, Belo Horizonte, v. 1, n. 1, p. 69-84, jan./jun. 2014, p. 09.

[54] GAFI, Grupo de Ação Financeira. Money Laundering ... *op. cit.*, p. 07.

próprias autoridades investigativas, devem, portanto, conter indicadores de materialidade delitiva que justifiquem a abertura de uma investigação para apurá-los, fazendo-se — também — necessária a compreensão de tipologias procedimentais da criptolavagem.

O *Anti Money Laundering Centre*, associado ao Serviço de Investigações e Informações Fiscais da Holanda, esclarece que o papel das tipologias de criptolavagem é estabelecer formas mais definidas para as atividades que contém traços de lavagem de dinheiro — adequando-se os elementos desse tipo no sistema econômico tradicional ao universo das criptomoedas —, sendo de grande importância a classificação precisa de condutas que levantam suspeitas de sua ocorrência, posteriormente reconstruídas cronologicamente pelo investigador.[55]

Sobre o estabelecimento dessas tipologias, Felipe Américo Moraes disserta que a doutrina pouco avançou na discussão sobre se determinadas operações de criptomoedas configuram a prática da lavagem de capitais. Isso se dá porque algumas conclusões pela tipicidade penal de transações suspeitas apresentam uma escassez que "tem origem metodológica: dizer que determinada conduta configura lavagem de dinheiro porque é uma 'colocação' não encerra — ou sequer inicia — a análise típica necessária".[56]

Afinal, a conversão de dinheiro produto de crime em criptomoedas nem sempre será entendida como ato de lavagem, sendo indispensável que a operação financeira vise tornar mais difícil a identificação de um delito antecedente[57].

Ou seja, a análise de tipologias deve ocorrer com a verificação da (provável) natureza ilícita das criptomoedas, qualidade das transações feitas e a identificação de *red flags*, considerados em conjunto, já que "não há como se falar em investigação de criptoativos sem habilidades para,

---

[55] AMLC, Anti Money Laundering Centre. New money laundering typologies in the fight against money laundering by means of virtual currencies. Disponível em: https://www.amlc.eu/wp-content/uploads/2019/04.

[56] MORAES, Felipe Américo. O que é e o que não é lavagem de dinheiro com Bitcoins. Disponível em: https://www.conjur.com.br/2022-jul-13/felipe-moraes-lavagem-dinheiro-bitcoins/.

[57] RODRIGUES, Renata da Silva. Uso de Bitcoins ... *op. cit.*, p. 20-21.

de fato, empreender ações para seguir o dinheiro (*follow the money*), ou melhor, *follow the crypto*".[58]

Vejamos, abaixo, uma listagem — não exaustiva — de tipologias da criptolavagem e sinais de alerta correlatos, com a indicação de quais elementos seriam suficientes para a instauração de uma investigação preliminar quando observados.

3.2.1. Ocultação

Primordialmente, para constatação de materialidade penal, divide-se a análise das tipologias de criptolavagem em dois momentos: o momento de conversão dos valores de proveniência ilícita em criptoativos, e o de sua subsequente movimentação. Isso pois um dos elementos do tipo penal em questão é o distanciamento dos fundos ilícitos de sua origem, evitando uma associação direta entre eles e o crime antecedente.[59]

Quando se almeja esse distanciamento, costuma-se, na conversão de valores de origem ilícita em ativos virtuais (colocação), adotar métodos simples de transação P2P, o uso de *exchanges* centralizadas e/ou descentralizadas e das chamadas *ATM Machines* ("*any time money*"). No sistema tradicional, enquanto esse momento da lavagem está majoritariamente ligado à utilização de instituições financeiras ou empresas de fechada para a ocultação, no universo cripto está relacionado à inserção de valores em ativos virtuais ou seu recebimento direto como produto de crime.[60]

Assim, os indícios de que as transações enquadradas no conceito de 'colocação', ou 'ocultação', despertando uma hipótese investigativa, podem ser elencados, *v.g.*, como: o depósito ou saque reiterado de valores

---

[58] WEISHEIMER, Evandro [*et al.*]. Criptolavagem e compliance ... *op. cit*., p. 64.

[59] BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. Lavagem de dinheiro ... *op. cit*., p. 120-121.

[60] WEISHEIMER, Evandro [*et al.*]. Criptolavagem e compliance ... *op. cit*., p. 67. As transações ponto a ponto ("P2P") equivalem à qualidade de transação em que não se necessita de um intermediário e se prestam à maior anonimidade das operações. As *exchanges*, centralizadas e descentralizadas, permitem a troca de moedas correntes em criptomoedas — e vice-versa. Os caixas eletrônicos de criptoativos, ou *ATM Machines*, funcionam de maneira similar às *exchanges*, mas, em alguns casos, podem operar dinheiro em espécie — *Ibid*.

altos em períodos curtos, o depósito de valores em *exchange* imediatamente sucedido de saques sem lógica financeira e o recebimento contínuo de criptoativos em quantidades relativamente pequenas ("*smurfing*").[61]

Tais métodos de conversão, quando constatados por uma autoridade investigativa, só justificam a instauração de uma investigação preliminar caso de alguma forma, no seu decorrer, busque-se dissimular ou ocultar a sua origem registrada em *blockchain*.[62] E é aqui em que se insere a problemática dos *tumblers*, capazes de dissimular esses padrões de conversão.

3.2.2. Dissimulação

Inicialmente, sobre a 'dissimulação' como ato de lavagem propriamente dito na criptolavagem, é relevante promover uma distinção entre transações simples e transações complexas.[63] As transações simples são aquelas sem maiores particularidades técnicas e verificáveis pelo registro em *blockchain*. Por outro lado, as transações complexas envolvem ferramentas digitais de anonimato, como as operações em *exchanges* descentralizadas, *privacy wallets* e os próprios *mixing-services*.[64]

Os serviços de mistura, no rol das transações complexas, não tornam possível a aferição direta dos depósitos registradas em *blockchain* e, consequentemente, de elementos que indiquem a ilicitude das operações constantes em uma *ledger*. Em função disso, deve-se atentar ao fato de que as movimentações realizadas por meio de *mixing-services* nem sempre serão entendidas como ato de lavagem, eis que se trata de criada originalmente ferramenta na busca por maior privacidade dos *traders*, considerando que os dados das movimentações cripto se encontram publicamente registrados na cadeia *blockchain*.[65] Nesse sentido, Reinder de

---

61 GAFI, Grupo de Ação Financeira. Money Laundering ... *op. cit*., p. 10.

62 MORAES, Felipe Américo. O que é e o que ... *op. cit*., p. 192.

63 ESTELLITA, Heloísa. Criptomoedas e lavagem ... *op. cit*., p. 03.

64 WEISHEIMER, Evandro [*et al.*]. Criptolavagem e compliance ... *op. cit*., p. 77.

65 Möser, Böhme e Breuker exemplificam: "doadores podem ter interesse legítimo na privacidade financeira. Eles podem usar ferramentas de anonimização de transações para evitar serem observados por invasores monitorando as transações feitas para endereços de Bitcoin publicamente conhecidos das

Jong pondera que existem razões legítimas (lícitas) para o uso dos serviços de mistura, mas, como se observa na prática, os "*tumblers* adotam nomes que descrevem bem o seu propósito, tal qual '*BitLauder',* demonstrando o público-alvo que tem em mente" (tradução nossa).[66]

Como visto, a tipicidade do crime de lavagem depende da constatação de que os valores operados sejam de valor ilícita. Sem a existência de qualquer relação entre valores movimentados por um serviço de mescla e a prática de crime antecedente relacionado, não se consolida materialidade que sustente uma hipótese investigativa. Por isso, apesar de um dos sinais de alerta que indicam a prática de criptolavagem seja a presença de operações realizadas através dos *mixing-services*, o tipo penal de lavagem (e a constatação da materialidade delitiva dessas operações) exige que as condutas adotadas pelo agente no *iter criminis* tenham como finalidade a dissimulação da origem ilícita dos valores.[67]

Então, no âmbito das criptomoedas, a aferição de tipologias de dissimulação pressupõe que a mistura de criptomoedas seja indispensavelmente precedida pela conversão de valores de ordem ilegal em ativos virtuais, ou seu recebimento direto como produto de crime anterior (colocação).[68] Deve-se atentar às transações feitas a partir de endereços, *wallets* ou cartões com conexão a esquemas de fraude, extorsão, jogos de aposta não regularizados *online*, mercados da *Dark Net* e outros sites ilícitos, bem como à falta de transparência e informações insuficientes sobre a origem e os proprietários dos valores e aos fundos diretamente

---

organizações que defendem" — MÖSER, Malte; BÖHME, Rainer; BREUKER, Dominic. An inquiry into money laundering tools ... *op. cit.*, p. 02.

66 DE JONG, Reinder. Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht. *Tijdschrift voor Bijzonder Strafrecht & Handhaving — TBS&H*, [*s. l.*], n. 1, mar. 2017, p. 05. https://doi.org/10.5553/tbsenh/229567002017003001003.

67 BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. Lavagem de dinheiro ... *op. cit.*, p. 122-123.

68 As tipologias relacionadas à reintegração dos valores no sistema econômico formal (integração) não se tornam obrigatórias para a consolidação da materialidade delitiva do crime de lavagem de capitais no uso dos *mixing-services*. Afinal, trata-se de fase posterior à dissimulação dos ativos que, se provenientes de crime pretérito, já tornam criminalmente típicas as operações de mistura por eliminarem a transparência das informações contidas no *blockchain*, mesmo sem a posterior conversão dos valores em moeda corrente, por exemplo.

relacionados a operações de mistura pretéritas ou *privacy wallets*.[69] Esses fatores são fortes indicativos de que os valores mesclados são de origem ilícita e, se verificados em conjunto com a mistura dos ativos e as técnicas de colocação vistas, já confeririam materialidade ao crime de lavagem de capitais, dando origem a uma hipótese investigativa válida.

A anonimidade da qual se vale um agente nas operações de mistura igualmente pode trazer elementos que indiquem a sua tipicidade penal. Dentre eles, menciona-se a troca imediata de criptoativos misturados, como o Bitcoin, por *privacy coins* — ativos virtuais projetados para fornecer transações anônimas e não rastreáveis, como a Monero, Zcash e Verge —, o uso de endereços de protocolo ("IP") relacionados à *Dark Net* ou *softwares* que garantam comunicações anônimas e o emprego de carteiras digitais relacionadas a um mesmo IP, mas registradas em nome de diferentes usuários.[70]

Como exemplo da qualidade informativa que esses sinais de alerta podem conferir às operações de *mixing*, guiando as autoridades públicas na investigação da criptolavagem, tem-se a operação deflagada pelo *Federal Bureau of Investigation* ("FBI") e a Receita Federal estadunidense contra o serviço de mistura Helix. O *tumbler*, que operava na *Dark Net* e travava uma parceria operacional com o mercado clandestino AlphaBay[71], foi interditado pelo governo do Estados Unidos da América e os responsáveis pelo serviço de mistura presos. [72]

No início das investigações, o FBI promoveu por meio de um agente infiltrado a transferência de criptoativos do AlphaBay para o *mixer* Helix, constatando que o seu emprego efetivamente reduzia rastreabilidade e relação direta das movimentações cripto, os crimes cometidos no mercado clandestino (recebimento direto como produto de crime

---

[69] GAFI, Grupo de Ação Financeira. Money Laundering ... *op. cit*., p. 11-12.

[70] *Ibid*., p. 12-13.

[71] O AlphaBay foi um dos maiores mercados clandestinos da *Dark Net*. Ele era usado por centenas de milhares de pessoas para a compra e venda drogas, de documentos falsos, *malware* e outras ferramentas de *hacking*, armas de fogo e produtos químicos tóxicos. O site funcionava a partir de um sistema de transações financeiras baseado na operação de criptoativos e foi interditado em 2017 — *Ibid*., p. 11.

[72] *Ibid*.

anterior) e a reinserção dos valores no sistema economico formal. Em seguida, os investigadores utilizaram o Chainalysis — plataforma de análise de dados em *blockchain* — para identificar inúmeras carteiras de Bitcoin que continham lucro proveniente da operação do serviço Helix. Isso conferiu às autoridades razões suficientes para determinar a busca e apreensão nos endereços dos administradores do serviço de mistura, nos quais em momento posterior foram encontrados documentos e metadados cruciais para a aferição do crime de lavagem de dinheiro.[73]

Ainda sobre os sinais de alerta, uma vez que a origem das criptomoedas está relacionada aos remetentes e destinatários dos valores, também configuram suspeita as operações de *mixing* que os envolvem em determinadas situações, especialmente quando são observadas irregularidades na criação de carteiras digitais, nas diligências de KYC tomadas por *exchanges* ao longo das operações, perfil dos donos das carteiras transacionadas sem conhecimento do ambiente cripto, eventualmente recrutados por operadores especializados em criptolavagem, ou "vítimas de golpes transformados em 'mulas' que são enganadas para transferir rendimentos ilícitos sem conhecimento de suas origens".[74]

O serviço de mistura Tornado Cash, que movimenta a criptomoeda Ethereum e ao todo teria servido para lavar o equivalente a $7 bilhões de dólares,[75] não adotava medidas de KYC. Segundo o FBI, a plataforma ignorou as regras de *know your costumer*, quando deveria ter sido registrada como um serviço de operações financeiras e requerido informações de seus clientes como medida de prevenção à lavagem de dinheiro, despertando suspeitas na agência de inteligência estadunidense que deflagrou uma investigação na qual os criadores do *mixer* foram indiciados por esse delito.[76]

---

[73] CHAINALYSIS. Chainalysis em Ação: Como a Polícia Rastreou Milhões em Bitcoin Ilícito nos Casos dos Irmãos Harmon. Disponível em: https://www.chainalysis.com/blog/helix-mixer-harmon-brothers-investigation/. Acesso em 15 jun. 2025.

[74] GAFI, Grupo de Ação Financeira. Money Laundering ... *op. cit*., p. 13.

[75] DU, Hanbiao [*et al.*]. Breaking the Anonymity of Ethereum Mixing Services ... *op. cit*., p. 01.

[76] Ainda segundo o FBI, existem indícios de que o Tornado Cash foi utilizado para lavar valores ilícitos de wallets do Grupo Lazarus, supostamente comandado

Por fim, a identificação do papel dos agentes e da sua atuação no processo de mistura é ponto fundamental no despertar de suspeita sobre a ilicitude das operações de *mixing*. De acordo com a pesquisa desenvolvida por Mingdong Liu, Hu Chan e Jiagi Yan, pode-se identificar figuras centrais de três operadores nas plataformas de mistura: os 'Organizadores', responsáveis por planejar as etapas de lavagem e fazer contato com potenciais clientes; os 'Comunicadores', que tem como principal atribuição transmitir informações sobre a atividade entre os envolvidos, e os 'Soldados' ("linha de frente"), sem vínculo com o núcleo da organização, que desempenham funções diversas, facilitando a inserção de valores ilegais com aparência de ilicitude no sistema financeiro formal.[77]

Essa "identificação geral" tem o potencial de fornecer às autoridades de investigação e unidades de inteligência informações sobre como os *mixers* atuam — caso a caso —, sendo, inclusive, úteis ao processo de *de-mixing* e conferindo um panorama geral sobre a operabilidade de um serviço de mistura suspeito. Segundo os pesquisadores, essa é uma das chaves para desmistificar a sua anonimidade, para além da elaboração e compreensão de novos algoritmos de operação dos *mixing-services*.[78]

3.2.3. Integração

Quanto às tipologias de integração, os mesmos métodos de ocultação podem ser utilizados no momento de movimentação dos criptoativos,[79] valendo-se o agente do caminho inverso na inserção dos ativos dissimulados no ecossistema econômico tradicional por meio de ações que permitam a sua troca por moeda corrente.[80]

---

pelo governo da Coréia do Norte — FBI, Federal Bureau of Investigation. Tornado Cash Co-Founders Accused of Helping Cybercriminals Launder Stolen Crypto. Disponível em: https://www.fbi.gov/news/stories/tornado-cash-co-founders-accused-of-helping-cybercriminals-launder-stolen-crypto.

77 LIU, Mingdong; CHEN, Hu; YAN, Jiaqi. Detecting Roles of Money Laundering ... *op. cit*., p. 04-05.

78 *Ibid.*

79 WEISHEIMER, Evandro [*et al.*]. Criptolavagem e compliance ... *op. cit*., p. 85-87.

80 GRZYWOTZ, Johanna. Virtuelle Kryptowahrungen ... *op. cit*., p. 109; ESTELLITA, Heloísa. Criptomoedas e lavagem ... *op. cit*., p. 03.

A constatação de tipologias de integração no manejo de criptoativos fica condicionada às transações P2P em que o agente as trocou por moedas correntes — o que também é possível através das *exchanges*, centralizadas e descentralizadas, e de *ATM Machines* — e aos pagamentos de bens e serviços por meio de ativos virtuais, buscando-se a sua liquidação.

Considerações Finais

Em conclusão, tem-se que a instauração de uma investigação preliminar para o crime de lavagem de dinheiro praticado no sistema cripto, com dissimulação a partir dos *mixing-services*, depende da constatação de elementos que indiquem a possível ilicitude dos ativos misturados, precedida de atos que se enquadram nas tipologias de colocação.

Dentre esses elementos que podem qualificar indícios de materialidade do crime de lavagem de dinheiro, vale destacar a forma como os valores são convertidos em criptoativos, o perfil do operador, o *quantum* dos valores transacionados, a divisão e frequência das operações, a estrutura organizacional do serviços de mistura operado, sua relação direta ou indireta com atividades ilícitas da *Dark Net*, sites de aposta não regularizados e ferramentas de anonimidade que encubram rastros verificáveis em *blockchain*, como os próprios *mixing-services*.

A aferição de tais sinais de alerta, que trazem à tona possíveis tipologias da criptolavagem, legitima a abertura de uma investigação formal porque se relevam suficientemente idôneas para a definição de uma hipótese investigatória inicial, consistente no uso dos serviços de mistura em prol da criptolavagem. Sendo o rastreamento das movimentações feitas por um *mixer* de difícil viabilidade, é necessário que esses *red flags* sejam verificados de maneira conjunta, não bastando a simples apuração de operações feitas por um serviço de mistura, eis que a mescla de criptomoedas, por si só, não configura crime.

Com a observância desses indicadores pelas autoridades públicas, torna-se possível uma compreensão mais técnica do papel dos *mixing-services* na lavagem de capitais, que permite a formulação de hipóteses de investigação e a consequente promoção de meios de prova e de obtenção de prova para coleta de elementos de informação indispensáveis à eficácia da diligência investigativa estatal nesses casos.

Referências

AMLC, Anti Money Laundering Centre. New money laundering typologies in the fight against money laundering by means of virtual currencies. Disponível em: https://www.amlc.eu/wp-content/uploads/2019/04. Acesso em: 09 out. 2024.

BADARÓ, Gustavo Henrique. *Epistemologia Judiciária e Prova Penal*. 2. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2023.

BADARÓ, Gustavo Henrique. *Processo Penal*. 3. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2015.

BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. *Lavagem de dinheiro:* aspectos penais e processuais penais. 5. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2022.

BECHARA, Fábio Ramazzini. Natureza jurídica do Relatório de inteligência financeira do COAF. *Revista Fórum de Ciências Criminais — RFCC*, Belo Horizonte, v. 1, n. 1, p. 69-84, jan./jun. 2014.

CHAINALYSIS. Chainalysis em Ação: Como a Polícia Rastreou Milhões em Bitcoin Ilícito nos Casos dos Irmãos Harmon. Disponível em: https://www.chainalysis.com/blog/helix-mixer-harmon-brothers-investigation/. Acesso em: 15 jun. 2025.

COSTA, Isac Silveira da. O futuro é infungível: tokenização, non-fungible tokens (NFT's) e novos desafios na aplicação do conceito de valor mobiliário. *Revista de Direito das Sociedades e Valores Mobiliários*, [*s. l.*], v. Especial, 2022.

COSTA, Isac Silveira da. Eficácia ineficaz: a Lei 14.478 entrará em vigor sem relevância prática. Disponível em: https://www.conjur.com.br/2023-mai-31/fintech-crypto-lei-144782022-entrara-vigor-relevancia-pratica/. Acesso em: 07 jun. 2024.

CRAWFORD, Jesse; GUAN, Yong. Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy. In: *IEEE 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 15 mar. 2020, p. 38-45, Nova Iorque. https://doi.org/10.1109/sadfe51007.2020.00013. Acesso em: 13 jul. 2024.

DE JONG, Reinder. Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht. *Tijdschrift voor Bijzonder Strafrecht & Handhaving — TBS&H*, [*s. l.*], n. 1, mar. 2017. https://doi.org/10.5553/tbsenh/229567002017003001003.

DE MICHELI, Leonardo Miessa. *Blockchain, criptoativos e os títulos circulatórios do Direito Comercial*. Tese (Doutorado em Direito) — Faculdade de Direito da Universidade de São Paulo, Universidade de São Paulo, São Paulo, 2020.

DU, Hanbiao [*et al.*]. Breaking the Anonymity of Ethereum Mixing Services Using Graph Feature Learning. *IEEE Transactions on Information Forensics and Security*, Nova Iorque, v. 19, p. 616-631, out. 2024. Disponível em: https://ieeexplore.ieee.org/document/10292691. Acesso em: 10 jul. 2024.

ELSAYED, Sayid. Cryptocurrencies, corruption and organised crime: Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption. [*s. l.*]. Transparência Internacional, *U4 Helpdesk Answer*, 28 mar. 2023. Disponível em: https://www.giz.de/en/downloads/cryptocurrencies-corruption-and-organised-crime. Acesso em: 08 jun. 2024.

ESTELLITA, Heloísa. Criptomoedas e lavagem de dinheiro. Resenha de: GRZYWOTZ, Johanna. Virtuelle Kryptowährungen und Geldwäsche. Berlin: Duncker & Humblot, 2019. *Revista de Direito FGV*, v. 16, n. 1, jan./abr. 2020. https://doi.org/10.1590/2317-6172201955.

ESTELLITA, Heloísa; TUMBIOLO, Mariana. Criptomoedas e lavagem de dinheiro: por que regular? *Revista do Advogado (AASP) — Direito e criptoeconomia*, São Paulo, n. 156, p. 157-163, nov. 2022.

FBI, Federal Bureau of Investigation. Tornado Cash Co-Founders Accused of Helping Cybercriminals Launder Stolen Crypto. Disponível em: https://www.fbi.gov/news/stories/tornado-cash-co-founders-accused-of-helping-cybercriminals-launder-stolen-crypto. Acesso em: 14 jun. 2025.

GAFI, Grupo de Ação Financeira. Virtual Currencies. Key definitions and potencial AML/CFT risks. Disponível em: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk. Acesso em: 17 jul. 2024.

GAFI, Grupo de Ação Financeira. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets. Disponível em: https://www.fatf-gafi.org/en/publications/Methodsandtrends. Acesso em: 17 jul. 2024.

GAFI, Grupo de Ação Financeira. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Disponível em: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance. Acesso em: 17 jul. 2024.

GRZYWOTZ, Johanna. *Virtuelle Kryptowahrungen Und Geldwasch*. Berlim: Duncker & Humblot, 2019.

HILLMAN, Henry Daniel. *Money laundering through cryptocurrencies: analysing the response of the United States and Australia and providing recommendations for the UK to address the money laundering risks pose by cryptocurrencies*. Tese (Doutorado em Filosofia) — Faculty of Business and Law, University of the West of England, Bristol, 2020.

HONG, Younggee [*et al.*]. A Practical De-mixing Algorithm for Bitcoin Mixing Services. In: *ACM Asia Conference on Computer and Communications Security*, Incheon, 4 jun. 2018. https://doi.org/10.1145/3205230.3205234. Acesso em: 20 jul. 2024.

LIU, Mingdong; CHEN, Hu; YAN, Jiaqi. Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework. *Frontiers in Physics — Section of Social Physics*, v. 9, p. 01-08, jul. 2021. https://doi.org/10.3389/fphy.2021.665399.

KATARZYNA, Ciupa. Cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems. In: *2019 OECD Global Anti-Corruption & Integrity Fórum*, Paris, 20-21 mar. 2019. Disponível em: https://coincapp.com/corruption/integrity-forum/academic-papers/Ciupa-Katarzyna-cryptocurrencies.pdf. Acesso em: 10 jun. 2024.

LOPES JÚNIOR, Aury. *Sistemas de investigação preliminar no processo penal*. 2. ed. rev., atual. e ampl. Rio de Janeiro: Lumen Juris, 2003.

MENDONÇA, Lawrence Lino Monteiro de; DIAS, Gabriel Bulhões Nóbrega. Quebra de sigilo telemático como meio de investigação da criptocriminalidade. Disponível em: https://www.migalhas.com.br/coluna/informacao-privilegiada/384513/quebra-de-sigilo-como-meio-de-investigacao-da-criptocriminalidade. Acesso em: 10 out. 2024.

MORAES, Felipe Américo. *Bitcoin e lavagem de dinheiro*: quando uma transação configura crime. São Paulo: Tirant lo Blanch, 2022.

MORAES, Felipe Américo. O que é e o que não é lavagem de dinheiro com Bitcoins. Disponível em: https://www.conjur.com.br/2022-jul-13/felipe-moraes-lavagem-dinheiro-bitcoins/. Acesso em: 17 jul. 2024.

MORAIS, Fábio Luiz de; FALCÃO, Rondinelli Melo Alcântara. A regulação de criptomoedas como instrumento de prevenção à lavagem de dinheiro. *Cadernos*

Técnicos da GCU — Coletânea de Artigos Correcionais, [*s. l.*], v. 3, p. 110-134, nov. 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/607. Acesso em: 08 jun. 2024.

MORSE, Eric. *Bitcoin*: uma introdução simples. Tradução: João Rossi Parreiras. Nova Jersey: Babelcube Inc., 2017.

MÖSER, Malte; BÖHME, Rainer; BREUKER, Dominic. An inquiry into money laundering tools in the Bitcoin ecosystem. In: *IEEE 2013 APWG eCrime Researchers Summit*, São Francisco, 17-18 set. 2013. Disponível em: https://ieeexplore.ieee.org/document/6805780. Acesso em: 17 jul. 2024.

RATHORE, Mazhar; CHAURASIA, Sushil; SHUKLA, Dhirendra. Mixers Detection in bitcoin network: a step towards detecting money laundering in crypto-currencies. In: *2022 IEEE International Conference on Big Data*, Osaka, 17-20 dez. 2022. Disponível em: https://ieeexplore.ieee.org/document/10020982. Acesso em: 11 jul. 2024.

RODRIGUES, Renata da Silva. Uso de Bitcoins em atos de lavagem: dissensos doutrinários. *Boletim IBCCRIM*, São Paulo, v. 32, n. 380, p. 18-21, 2024. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1052. Acesso em: 06 jun. 2024.

SHIMABUKURO, Adriana; SILVA, Melissa Garcia Blagitz de Abreu. Internet, Deep Web e Dark Net. In: SILVA, Ângelo Roberto Ilha da (org.). *Crimes Cibernéticos*. Porto Alegre: Livraria do Advogado, 2018.

SHOJAEENASAB, Ardeshir; MOTAMED, Amir Pasha; BAHRAK, Behnam. Mixing detection on Bitcoin transactions using statistical patterns. *Institution of Engineering and Technology (IET) Blockchain*, [*s. l.*], v. 3, p. 123-168, set. 2023. https://doi.org/10.1049/blc2.12036. Acesso em: 09 jul. 2024.

SILVEIRA, Renato de Mello Jorge. Aspectos penais da criptoeconomia. *Revista do Advogado (AASP) — Direito e criptoeconomia*. São Paulo, n. 156, p. 151-157, nov. 2022.

TUZET, Giovanni. Razonamiento probatorio: ¿dedución? ¿inducción? ¿abducción? In: AMADO, Juan Antonio García; BONORINO, Pablo Raúl (coord.). *Pruba y razonamiento probatorio em el Derecho. Debates sobre abducción*. Granada: Comares, 2014.

VAN WEGBERG, Rolf; OERLEMANS, Jan-Jaap; VAN DEVENTER, Oskar. Bitcoin money laundering: mixed results? An explorative study on money laundering of

cybercrime proceeds using bitcoin. *Journal of Financial Crime (JFC)*, [*s. l.*], v. 25, p. 419-435, mai. 2018. https://doi.org/10.1108/jfc-11-2016-0067.

WEISHEIMER, Evandro [*et al.*]. *Criptolavagem e compliance*: tipologias de lavagem de dinheiro por meio de criptoativos e sua prevenção. 2. ed. São Paulo: Rideel, 2024.

Authorship information

Fábio Ramazzini Bechara: Professor dos Programas de Graduação e Pós-Graduação (Mestrado e Doutorado) em Direito Político e Econômico da Universidade Presbiteriana Mackenzie. Doutor em Direito Processual Penal pela Universidade de São Paulo. Membro do GACINT — Grupo de Análise de Conjunturas Internacionais da USP. Membro do Conselho Orientador da Escola de Segurança Multidimensional do Instituto de Relações Internacionais da USP. Promotor de Justiça em São Paulo/SP. fabio.bechara@mackenzie.br

Matheus Morelli Sindona Bellizia: Pós-graduando em Direito Penal Econômico pela Fundação Getúlio Vargas/SP. Graduado em Direito pela Universidade Presbiteriana Mackenzie. Advogado. math_bellizia@hotmail.com.

Additional information and author's declarations (*scientific integrity*)

Conflict of interest declaration: the authors confirm that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

- *Fábio Ramazzini Bechara*: writing — review and editing, final version approval.
- *Matheus Morelli Sindona Bellizia*: conceptualization, methodology, data curation, investigation, writing — original draft, validation, writing — review and editing, final version approval.

Declaration of originality: the authors assure that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; they also attest that there is no third party plagiarism or self-plagiarism.

Data Availability Statement: In compliance with open science policies, all data generated or analyzed during this study are included in this published article.

Editorial process dates (https://revista.ibraspp.com.br/RBDPP/about)

- Submission: 24/02/2025
- Desk review and plagiarism check: 10/03/2025
- Review 1: 25/04/2025
- Review 2: 29/04/2025
- Preliminary editorial decision: 11/06/2025
- Correction round return: 20/06/2025
- Final editorial decision: 02/07/2025

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 2

How to cite (ABNT Brazil):

BECHARA, Fábio R.; BELLIZIA, Matheus M. S. Lavagem de criptoativos pela ótica da hipótese investigativa: os mixing-services e a investigação criminal. *Revista Brasileira de Direito Processual Penal*, vol. 11, n. 2, e1173, mai./ago. 2025. https://doi.org/10.22197/rbdpp.v11i2.1173