

Criptoativos e Lavagem de Capitais: Limites epistêmicos da prova digital e standard probatório necessário para o édito condenatório

Lara de Macêdo Velasco Fernandes Brito¹

Fábio Moreira Ramiro²

Resumo: Esse trabalho analisa se as provas digitais (*stricto sensu*), no delito de lavagem de capitais praticado por meio de criptoativos, marcadas por anonimato relativo, fragmentariedade e limitações intrínsecas à rastreabilidade, revelam-se, por si só, aptas a alcançarem o standard probatório à condenação? Para desenvolver esse propósito são apresentados: (i) o ecossistema tecnológico e a definição dos criptoativos; (ii) sua inserção nas fases de ocultação, dissimulação e integração patrimonial; e (iii) os limites epistêmicos da prova digital e o standard probatório exigido para o édito condenatório. O objetivo principal é demonstrar a necessidade de uniformização regulatória dos criptoativos, cuja arquitetura tecnológica dificulta a identificação da origem ilícita dos recursos e a atribuição de autoria penal a partir de vestígios digitais.

Palavras-chave: Criptoativos. Lavagem de capitais. *Blockchain*. Prova digital. Standard probatório. Limites epistêmicos.

INTRODUÇÃO

Convém, inicialmente, compreender que o Direito Penal Econômico se desenvolve em paralelo às transformações estruturais das relações econômicas, especialmente no contexto da progressiva globalização econômico-financeira e da crescente integração transnacional dos

¹ Graduanda em Direito pela Universidade Católica do Salvador (UCSal).

² Mestre em Direitos Fundamentais e Alteridade pela Universidade Católica do Salvador (UCSal). Juiz Federal Titular da 2ª Vara Criminal Especializada da Justiça Federal da Bahia. <http://lattes.cnpq.br/8572217840439077>.

mercados. Nesse processo histórico de reestruturação das formas de organização do capitalismo, observam-se constantes adaptações dos sistemas econômicos, financeiros e regulatórios a novos contextos políticos, institucionais e tecnológicos, circunstância que repercute diretamente sobre as formas de manifestação da criminalidade econômica contemporânea (Schmidt, 2018).

Sob essa ótica, à medida que as relações econômico-financeiras se tornam mais complexas e tecnologicamente integradas, observa-se que o delito de lavagem de capitais acompanha as próprias transformações estruturais dos mecanismos de circulação de riqueza, assumindo contornos progressivamente mais sofisticados diante da incorporação de novas ferramentas tecnológicas aos sistemas de movimentação de valores, ampliando significativamente a complexidade das operações de ocultação e dissimulação patrimonial, dificultando a identificação da origem, circulação e destino dos recursos ilícitos.

Nesse contexto, emerge o problema de pesquisa do presente estudo: a prova digital produzida para apurar o delito de lavagem de capitais realizado com criptoativos³ é suficiente para embasar uma condenação quanto à autoria, ou há lacunas probatórias intransponíveis decorrentes da própria arquitetura tecnológica e dos mecanismos de anonimato desses ativos?

Para compreender adequadamente essa problemática, impõe-se, inicialmente, a análise do próprio objeto da investigação. Inseridos nesse novo contexto de transformação e complexificação do sistema financeiro contemporâneo, especialmente no âmbito da criminalidade econômica, surgem os criptoativos, os quais se estruturam como ativos virtuais criptografados baseados em tecnologia descentralizada de validação e circulação de transações, operando sob regime de pseudoanonimato.

No rol dos criptoativos, tem-se as criptomoedas, em especial o Bitcoin, criado em 2008⁴, que se consolidou como o primeiro sistema de pagamento integralmente descentralizado, inaugurando uma nova dinâmica de circulação digital de valores e introduzindo uma categoria inovadora de ativos financeiros no ambiente econômico contemporâneo (Ulrich, 2014).

³ Criptoativos podem ser compreendidos, em síntese, como ativos virtuais criptografados estruturados a partir de tecnologias de registro descentralizado, permitindo a circulação digital de valores sem a necessidade de intermediação direta por instituições financeiras tradicionais. Em razão de sua relevância para a compreensão das dinâmicas contemporâneas da lavagem de capitais, o conceito será analisado de forma mais aprofundada em tópico próprio ao longo do presente trabalho.

⁴ Sobre a estrutura de pagamento descentralizado do Bitcoin, que permite transações diretas entre pares sem intermediários financeiros, veja-se NAKAMOTO, Satoshi. *Bitcoin: a peer-to-peer electronic cash system*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 4 maio 2025.

Assim, diante da crescente inserção dos criptoativos nas dinâmicas de circulação de valores, observou-se progressiva repercussão desses ativos no âmbito da criminalidade econômica, especialmente em operações relacionadas à ocultação e dissimulação de recursos ilícitos no contexto da lavagem de capitais prevista na Lei nº 9.613/1998 (Brasil, 1998), em razão de suas características, como a descentralização das transações, o pseudoanonimato dos usuários e a elevada capacidade de circulação transnacional de ativos digitais.

Nesse sentido, no ordenamento jurídico brasileiro, a Lei nº 14.478/2022 (Brasil, 2022), que altera a Lei nº 9.613/1998 para incluir no sistema antilavagem os prestadores de serviços de ativos virtuais, representou importante avanço regulatório ao incorporar os prestadores de serviços de ativos virtuais ao sistema preventivo antilavagem brasileiro, submetendo os agentes a deveres específicos de controle, conformidade e comunicação de operações suspeitas, além de estabelecer parâmetros normativos voltados à atuação das plataformas de intermediação de criptoativos (Callegari; Linhares, 2025).

Contudo, a despeito desse avanço normativo, subsiste um desafio central para a persecução penal. Embora as operações realizadas com criptoativos permaneçam registradas em *blockchain*⁵, a identificação da pessoa natural vinculada aos endereços virtuais não decorre automaticamente desses registros, sobretudo diante da utilização desses ativos nas fases de ocultação e dissimulação da lavagem de capitais, marcadas pela circulação fragmentada de valores, pela multiplicidade de transações e pela utilização de mecanismos voltados à redução da identificabilidade dos agentes envolvidos (Estellita, 2020).

Nesse contexto, a persecução penal envolvendo criptoativos passa a demandar novas formas de investigação e valoração probatória, especialmente quanto à vinculação entre registros de transações em *blockchain* e a atribuição de autoria penal.

Diante das dificuldades de identificação da titularidade dos endereços virtuais e de reconstrução das operações realizadas, o presente artigo tem por objetivo analisar os limites epistêmicos da prova digital e o standard probatório necessário à imputação penal nos delitos de lavagem de capitais envolvendo criptoativos, partindo da compreensão de que, embora a rastreabilidade em *blockchain* constitua relevante instrumento investigativo, ela não é, por si só, suficiente para fundamentar um juízo seguro de autoria penal.

⁵ *Blockchain* (cadeia de blocos) é uma tecnologia de registro distribuído que organiza transações em blocos sequenciais, criptograficamente encadeados, garantindo integridade, transparência e imutabilidade dos dados sem a necessidade de uma autoridade central. O conceito e o funcionamento detalhado da *blockchain* serão definidos e conceituados no item 1.3 deste artigo.

Para tanto, o trabalho divide-se em três capítulos. No primeiro, examina-se o ecossistema dos criptoativos, abordando seu conceito, estrutura tecnológica, principais características e modalidades, bem como os instrumentos digitais utilizados na circulação de ativos virtuais, incluindo *exchanges*⁶, *fintechs*⁷ e *mixing services*⁸.

No segundo capítulo, analisa-se a inserção dos criptoativos na dinâmica da lavagem de capitais, com ênfase na utilização desses ativos em cada fase do processo criminoso. Demonstra-se como as propriedades tecnológicas dos criptoativos, notadamente a descentralização das transações, a ausência de intermediários obrigatórios, o pseudonimato dos titulares de endereços e a possibilidade de fracionamento em múltiplas carteiras virtuais, potencializam, simultaneamente, dois efeitos distintos, porém complementares: (i) de um lado, o distanciamento entre o produto do crime e sua origem ilícita, ao dificultar o rastreamento linear dos valores, (i) de outro, a dissociação entre a conduta criminosa e a identificação do agente, ao impedir ou dificultar a atribuição automática dos registros em *blockchain* a uma pessoa natural determinada.

Ao final, o terceiro capítulo dedica-se à análise dos limites epistêmicos da prova digital e do standard probatório exigido para o edito condenatório, notadamente quanto à atribuição de autoria, examinando a distinção entre os standards probatórios nas diferentes fases da persecução penal, desde os meros indícios na fase investigativa e a justa causa para o recebimento da denúncia até o grau de certeza exigido para a condenação, com o fim de demonstrar que, embora a rastreabilidade em *blockchain* seja útil nas fases iniciais, a prova digital isolada não se mostra suficiente para lastrear um edito condenatório.

Para a realização do presente artigo, empregou-se pesquisa de natureza teórico-descritiva, com abordagem qualitativa, desenvolvida a partir de levantamento bibliográfico, doutrinário, legislativo e documental. Adotou-se o método dedutivo, por meio do qual se buscou, a partir da análise dos dados e referenciais examinados, compreender as novas dinâmicas de lavagem de capitais no contexto dos criptoativos, bem como os limites probatórios decorrentes do uso de tecnologias *blockchain* no âmbito da imputação penal.

⁶ *Exchanges*: plataformas de negociação que atuam como intermediárias na compra, venda e armazenamento de criptoativos, convertendo moeda digital em moeda fiduciária e vice-versa.

⁷ *Fintechs*: empresas que aplicam inovação tecnológica à prestação de serviços financeiros, operando com estruturas digitais em substituição ao sistema bancário tradicional.

⁸ *Mixing services* (serviços de mistura ou *tumblers*) são plataformas que misturam criptoativos de diferentes usuários, rompendo a ligação entre o remetente e o destinatário.

O referencial teórico fundamenta-se em construções doutrinárias e normativas, em âmbito nacional e internacional, voltadas ao Direito Penal Econômico, à lavagem de capitais, aos criptoativos e à teoria da prova penal, com ênfase na análise dos limites epistêmicos da prova digital e do standard probatório aplicável à persecução penal.

Por fim, esta pesquisa não pretende oferecer soluções definitivas, mas sim contribuir para o aprofundamento do debate acerca dos desafios probatórios na lavagem de capitais com criptoativos, dos avanços normativos e tecnológicos no Direito Penal Econômico e, especialmente, do standard probatório exigido para a prova digital de operações financeiras no contexto da persecução penal.

1. CRIPTOATIVOS

1.1. Definição e delimitação terminológica

De início, é importante delimitar os principais conceitos utilizados na análise dos criptoativos, tendo em vista a ausência de uniformidade terminológica na doutrina e nos documentos regulatórios. Nessa linha, em sentido amplo, os criptoativos são descritos pela *Financial Conduct Authority* (FCA), como representação digital de valor em ambiente eletrônico, protegida por criptografia e sustentada por tecnologias de registro distribuído, o que permite sua transferência, armazenamento e negociação em redes descentralizadas (FCA, 2019).

Para fins regulatórios, FCA, classifica os criptoativos em três categorias principais: (i) *tokens* de câmbio, como Bitcoin e Litecoin, concebidos como meio de troca descentralizado e sem respaldo de autoridade central, geralmente fora do perímetro regulatório; (ii) *tokens* de segurança, que se assemelham a instrumentos financeiros tradicionais (ações ou títulos de dívida), conferindo direitos como dividendos ou participação nos lucros, situando-se dentro do perímetro regulatório; e (iii) *tokens* de utilidade, que concedem acesso a produtos ou serviços de forma similar a vales de pré-pagamento, normalmente fora do perímetro regulatório, salvo quando se qualificam como moeda eletrônica.

Em outras palavras, trata-se de ativos que existem apenas no meio digital, cuja segurança e funcionamento dependem de criptografia e de um livro-razão compartilhado (DLT), circulando sem a necessidade de intermediários centrais como bancos ou governos⁹.

Embora existam outras denominações para os criptoativos, a Instrução Normativa RFB nº 1.888/2019, da Receita Federal do Brasil, adotou oficialmente esse termo, definindo-o no art. 5º, inciso I, em suma, como a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionada eletronicamente por meio de criptografia e tecnologias de registro distribuído, podendo ser utilizada como forma de investimento, instrumento de transferência de valores ou acesso a serviços, mas sem constituir moeda de curso legal (Brasil, 2019).

Por sua vez, é importante destacar a delimitação terminológica adotada pelo Banco Central do Brasil (BACEN). A autoridade monetária diferencia as chamadas moedas virtuais da "moeda eletrônica" definida na Lei nº 12.865/2013¹⁰.

Ainda, nos termos do Comunicado nº 25.306/2014 do BACEN, as chamadas moedas virtuais possuem forma própria de denominação, ou seja, são expressas em unidade de conta distinta das moedas emitidas por governos soberanos, e não se caracterizam como dispositivo ou sistema eletrônico de armazenamento em reais (Brasil, 2014).

Assim, para fins didáticos, o presente trabalho adota o termo "criptoativos" em sentido amplo, abrangendo todas as categorias de ativos virtuais, com foco nos ativos de pagamento utilizados como instrumento de troca, reserva de valor ou unidade de conta em transações econômicas digitais, independentemente de sua classificação técnica, em razão de sua função como meio de circulação de valor no ambiente digital e de sua relevância para os delitos econômicos.

1.2. Infraestrutura tecnológica

Quanto à sua estrutura e funcionamento, os ativos virtuais têm como principal característica a criptografia¹¹. A partir dela, são viabilizados mecanismos de segurança,

⁹ As noções de criptografia, livro-razão distribuído (DLT) e ausência de intermediários centrais serão detalhadas no subitem 1.3, que trata especificamente da estrutura e funcionamento dos criptoativos.

¹⁰ Art. 6º, inciso VI da Lei nº 12.865, de 9 de outubro de 2013: "moeda eletrônica: recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento."

¹¹ A criptografia é uma técnica de segurança milenar que codifica informações, assegurando que apenas o emissor e o destinatário autorizados possam acessá-las e mantê-las em sigilo. Conforme Sidhpurwala (2023), seus

autenticação e integridade das informações, assegurando que as transações realizadas no ambiente digital não possam ser facilmente adulteradas ou falsificadas.

Nos criptoativos, emprega-se especificamente a criptografia assimétrica (ou de chave pública), que opera com duas chaves matematicamente vinculadas, (i) a chave pública é um endereço visível a todos na rede, (ii) chave privada, mantida em sigilo pelo titular, é a única capaz de autorizar transações e comprovar a propriedade dos ativos (Camillo, 2023).

Essa tecnologia de proteção de dados é combinada com uma arquitetura de rede descentralizada baseada no modelo *peer-to-peer* (P2P), definido como um sistema de transações eletrônicas diretas entre partes, sem instituição financeira central, no qual todos os nós da rede se comunicam em igualdade de condições, sem hierarquia ou servidor central (Nakamoto, 2008). O que, por sua vez, o que confere maior autonomia e rapidez às movimentações financeiras, e, paralelamente, dificulta o controle e a rastreabilidade por parte das instituições reguladoras.

Ou seja, até aqui define-se os ativos virtuais como representações digitais de valor criptograficamente asseguradas, que funcionam dentro de uma arquitetura descentralizada baseada no modelo P2P – transações eletrônicas diretas entre partes –, prescindindo de intermediários estatais ou de qualquer autoridade central para validar as transações. Toda essa arquitetura repousa no sistema de registros distribuídos (*Distributed Ledger Technology* – DLT)¹², cuja manifestação mais consolidada é a *blockchain* (FCA, 2019).

Quanto ao aspecto do *blockchain*, pode ser compreendido como uma infraestrutura digital composta por uma cadeia de blocos organizados em ordem cronológica, cada qual contendo um conjunto de transações validadas e uma referência criptográfica ao bloco imediatamente anterior, o que assegura a integridade e a imutabilidade do registro. Essa cadeia de blocos é armazenada simultaneamente em milhares de computadores distribuídos mundialmente, prescindindo de qualquer servidor central. Desse modo, o *blockchain* funciona como um livro-razão distribuído, transparente e compartilhado, que registra e permite a verificação de todas as transações realizadas com o ativo virtual.

primeiros registros históricos datam de cerca de 1900 a.C., em inscrições no túmulo do nobre egípcio Khnumhotep II.

¹² A tecnologia de registro distribuído (DLT) pode ser descrita como um conjunto de soluções tecnológicas que permite que um único registro sequencial, padronizado e criptograficamente seguro de atividades seja distribuído com segurança a uma rede de participantes variados, que podem atuar sobre ele. Esse registro pode conter transações, posições de ativos ou dados de identidade, diferindo de um sistema centralizado tradicional, operado por uma única entidade confiável.

Cada bloco contém um conjunto de transações validadas, um carimbo de tempo (*timestamp*)¹³ e um código criptográfico (*hash*)¹⁴ que referencia o bloco anterior, formando uma cadeia inalterável. Para que um novo bloco seja adicionado à cadeia, exige-se a realização de prova de trabalho (*proof-of-work*), mecanismo de consenso que demanda poder computacional para resolver um problema matemático, o que torna computacionalmente inviável a modificação de registros pretéritos, pois alterar um bloco antigo forçaria o atacante a refazer todo o trabalho matemático dos blocos seguintes, exigindo poder computacional absurdo e assegurando, assim, a imutabilidade e a confiabilidade da *blockchain* (Nakamoto, 2008).

Em síntese, cada conjunto de transações é agrupado em blocos, que são verificados por meio de algoritmos criptográficos e, uma vez validados, ligam-se cronologicamente ao bloco anterior, formando uma cadeia contínua e imutável de registros, daí o termo *blockchain* (“cadeia de blocos”).

Assim, entende-se que a estrutura do criptoativo é baseada em três elementos interligados: (i) a criptografia, que garante segurança e pseudonimato; (ii) o modelo *peer-to-peer* (P2P), que elimina intermediários centrais; e (iii) a *blockchain*, que funciona como um livro-razão distribuído, imutável e descentralizado.

Ainda, dessa estrutura, extraem-se duas propriedades fundamentais, a descentralização, que decorre do modelo (i) *peer-to-peer*, que consiste na ausência de intermediários centrais das transações, da (ii) *blockchain*, entendida como um distribuído sem autoridade central, e o pseudoanonimato, que deriva da criptografia assimétrica, na qual as transações são associadas a chaves públicas, com endereços visíveis, enquanto as chaves privadas permanecem em sigilo.

Essas duas características atuam como verdadeiros catalisadores para a lavagem de dinheiro, uma vez que a descentralização elimina qualquer instância obrigatória que pudesse examinar, reportar ou bloquear transações suspeitas (Estellita, 2020). O pseudoanonimato, por sua vez, impede que as autoridades, a partir apenas do registro público na *blockchain*, vinculem um endereço a uma pessoa física ou jurídica específica, sendo necessária a quebra voluntária do sigilo ou a intermediação de terceiros (como *exchanges*).

¹³ *Timestamp* (carimbo de tempo) é um registro que indica a data e a hora exatas em que determinado evento ocorreu, no caso do *blockchain*, o momento em que o bloco foi criado e validado.

¹⁴ *Hashes* são funções matemáticas que produzem uma sequência única e de tamanho fixo para cada bloco ou transação. Essa tecnologia permite identificar de forma inequívoca cada elemento da cadeia. Além disso, as *hashes* colaboram para a privacidade, pois as informações são codificadas e somente as chaves privadas das partes envolvidas podem acessar os dados originais.

Assim, embora legítimas sob o ponto de vista da autonomia e da segurança do usuário, a descentralização e o pseudoanonimato conferem ao ecossistema dos criptoativos um ambiente estruturalmente favorável à ocultação da origem criminosa dos recursos e à movimentação de capitais ilícitos sem supervisão estatal, criando obstáculos significativos à persecução penal e à identificação dos agentes envolvidos em esquemas de lavagem de dinheiro.

1.3. O ecossistema de intermediação e circulação

Para que os criptoativos transitem entre o ambiente digital descentralizado e o sistema financeiro tradicional — convertendo-se em moedas fiduciárias ou sendo trocados entre si —, tornam-se necessários agentes intermediários que viabilizem essas operações. Esses agentes, conhecidos globalmente como provedores de serviços de ativos virtuais (*Virtual Asset Service Providers* – VASPs), incluem as *exchanges* (centralizadas – CEX, e descentralizadas – DEX), as *fintechs* que oferecem serviços com criptoativos e os *mixing services* (também chamados de *tumbling services* ou *mixers*),

Cada um desses atores opera com diferentes níveis de centralização, exigências de identificação dos usuários e exposição à regulação, influenciando diretamente a rastreabilidade das transações e a vulnerabilidade à lavagem de capitais. A seguir, analisam-se os principais tipos de intermediários e formas de circulação.

1.3.1. *Exchanges*

O ecossistema dos criptoativos estrutura-se com base no princípio da descentralização, que dispensa intermediários centrais e confere maior autonomia aos usuários. Entretanto, as *exchanges* desempenham papel relevante ao viabilizar a compra, a venda e a custódia de criptoativos. Embora a descentralização constitua um de seus principais pilares tecnológicos, as *exchanges* tornaram-se essenciais para a liquidez e o funcionamento do mercado de ativos digitais.

Ainda, as *exchanges* podem existir em diferentes formas e modelos de negócio e geralmente prestam serviços a terceiros, permitindo a seus clientes comprar e vender ativos virtuais em troca de moeda fiduciária tradicional, de outro ativo virtual ou de outros ativos¹⁵.

¹⁵ Sobre o tema, veja-se em FATF (2019).

Os modelos de câmbio e/ou transferência podem incluir *exchanges* "tradicionais" ou serviços de transferência que facilitam ativamente a troca de ativos virtuais por moeda real ou outras formas de ativos virtuais e/ou por metais preciosos mediante remuneração (por exemplo, taxa, comissão, *spread* ou outro benefício)¹⁶.

Há dois tipos principais de *exchanges* de criptoativos: as centralizadas (CEX), com sede e registro em um determinado país, e as descentralizadas (DEX), que são entidades independentes de autoridades estatais e instituições, e não permitem o armazenamento de tokens, quais devem permanecer em uma carteira não custodial (Ciesielska-Maciągowska; Spyra, 2025).

As *exchanges* centralizadas atuam como intermediárias entre compradores e vendedores, obtendo receita por meio de comissões e taxas de transação. Funcionam de maneira semelhante às bolsas de valores tradicionais e são geralmente a primeira etapa no processo de compra de criptoativos, pois aceitam transferências em moeda fiduciária e permitem saques de volta para uma conta bancária¹⁷, em particular, que permitiram a conversão criptoativos e moedas fiduciárias, ajudaram a impulsionar a alta dos preços ao atrair novos participantes em um ciclo de auto-reforço (Ciesielska-Maciągowska; Spyra, 2025).

Uma das principais vantagens das DEXs em relação às CEXs é que permitem aos usuários manter o controle de suas chaves privadas. Nas *exchanges* centralizadas, os criptoativos ficam sob custódia da plataforma, expondo os investidores a riscos como ataques cibernéticos e perdas decorrentes de falhas da própria *exchange*. Além disso, a negociação em CEXs exige confiança em um intermediário, característica que contrasta com os princípios das finanças descentralizadas (Ciesielska-Maciągowska; Spyra, 2025).

Assim, as *exchanges* ocupam posição ambivalente: por um lado, os modelos centralizados (CEX), quando submetidos à regulação, permitem ao Estado exercer controle sobre a entrada e saída de recursos, mediante identificação de usuários (*Know Your Client* – KYC), monitoramento de transações suspeitas e comunicação às autoridades competentes (unidade de inteligência financeira). Por outro lado, os modelos descentralizados (DEX) operam sem intermediação identificável, representando um desafio regulatório ainda não totalmente enfrentado.

¹⁶ Ibid., p. 15.

¹⁷ Sobre o tema, veja-se mais em FATF (2019).

No Brasil, a Lei nº 14.478/2022 representou um marco regulatório para o setor de ativos virtuais. Pela primeira vez, o ordenamento jurídico brasileiro definiu legalmente o conceito de ativo virtual e estabeleceu diretrizes gerais para o funcionamento das prestadoras de serviços que operam com criptoativos, bem como condicionou a operação dessas entidades à prévia autorização de órgão da Administração Pública federal, submetendo-as, assim, ao crivo estatal antes de poderem atuar no mercado nacional.

Para além, a referida lei incluiu as *exchanges* expressamente no rol de entidades obrigadas pela Lei nº 9.613/1998, em seu art. 9º, inciso XIX. Com isso, as plataformas de troca de criptoativos passaram a ter o dever legal de implementar mecanismos de prevenção à lavagem de capitais, entre os quais se destacam a identificação rigorosa de seus clientes (procedimentos de *Know Your Client* — KYC¹⁸) e a comunicação de operações suspeitas ao Conselho de Controle de Atividades Financeiras (COAF).

Dessa forma, as *exchanges* assumem, no ambiente criptoativos, o papel de *gatekeepers*¹⁹ — intermediários encarregados de filtrar e reportar transações potencialmente ilícitas, funcionando como uma extensão do sistema estatal de supervisão dentro de um ecossistema originalmente concebido para ser descentralizado e anônimo²⁰.

Em síntese, as *exchanges* também desempenham papel protagonista já na fase inicial de colocação (*placement*) da lavagem de capitais, pois, por meio delas, os valores provenientes de infrações penais antecedentes ingressam no sistema criptoativos, seja pela conversão do produto do crime em criptoativos por meio da aquisição direta nas plataformas de câmbio, seja pela utilização das *exchanges* como intermediárias para a obtenção de ativos virtuais com recursos ilícitos.

Ou seja, essa dependência da colaboração das *exchanges* revela uma face sensível do problema da prova digital em matéria de lavagem de capitais, pois, se a plataforma não implementa procedimentos de identificação (KYC) ou não coopera com as autoridades, os rastros deixados na *blockchain* tornam-se insuficientes para vincular a transação a uma pessoa natural.

¹⁸ KYC (Know Your Client) – procedimento de identificação e verificação de clientes obrigatório para instituições financeiras e prestadores de serviços de ativos virtuais,

¹⁹ O termo *gatekeepers* (intermediários vigias) é utilizado pela FATF (2019) para designar as entidades obrigadas a implementar medidas de prevenção à lavagem de capitais, incluindo identificação de clientes (KYC) e comunicação de operações suspeitas, funcionando como porta de entrada controlada do sistema financeiro.

²⁰ Para uma análise mais detalhada das funções de vigilância das *exchanges* e das medidas preventivas contra a lavagem de capitais, consulte as páginas 14 a 17 do guia da FATF (2019).

1.3.2. *Fintechs*

Dentro do ecossistema de intermediação e circulação de criptoativos, as *fintechs* ocupam um lugar de destaque, atuando como pontes tecnológicas entre o sistema financeiro tradicional e os ativos virtuais. Embora originalmente associadas a serviços bancários digitais e pagamentos, muitas *fintechs* passaram a oferecer também serviços de custódia, compra e venda de criptoativos, ampliando o acesso desses ativos ao público não especializado.

Conforme, o termo “Fintech” consolidou-se para designar startups que aplicam tecnologia à oferta de produtos e serviços financeiros, promovendo maior eficiência em transações, pagamentos e intermediação, sendo entidades não bancárias e independentes que utilizam soluções tecnológicas para tornar as operações financeiras mais ágeis e acessíveis, incluindo aquelas que envolvem criptoativos. Em um arranjo típico, a fintech fornece a plataforma tecnológica para pagamentos ou concessão de empréstimos sem expor seu próprio capital ao risco, enquanto o banco parceiro entra com o financiamento e assume a exposição creditícia (Eichengreen, 2021).

No Brasil, as *fintechs* que operam como Instituições de Pagamento já estavam sujeitas a obrigações de prevenção à lavagem de dinheiro previstas na Circular BCB nº 3.978/2020 (Brasil, 2020) e na Resolução BCB nº 80/2021 (Brasil, 2021), normas que determinam a implementação de políticas de identificação de clientes (KYC), monitoramento de transações e comunicação ao COAF de operações suspeitas.

Para além, o marco regulatório mais recente relevante para as *fintechs* no âmbito da circulação de criptoativos veio com a Instrução Normativa RFB nº 2.278/2025, a norma passou a exigir das *fintechs* e instituições de pagamento as mesmas obrigações fiscais e de reporte já aplicadas aos bancos tradicionais (Brasil, 2025)²¹.

Dessa forma, as *fintechs* inserem-se no ecossistema de circulação de criptoativos não apenas como facilitadoras tecnológicas, mas também como agentes obrigadas ao controle de lavagem de dinheiro. Ao terem de reportar operações suspeitas ao COAF e transmitir dados à Receita Federal (e-Financeira), elas se tornam pontos de vigilância na cadeia de movimentação

²¹ Ao equiparar formalmente as *fintechs* às instituições financeiras tradicionais, a IN RFB nº 2.278/2025 reduziu significativamente a lacuna regulatória até então existente, impondo a obrigatoriedade de transmissão de dados financeiros por meio do sistema e-Financeira e submetendo as operações das *fintechs* ao controle do COAF.

dos ativos virtuais, reduzindo o anonimato e a informalidade que antes favoreciam a ocultação de recursos ilícitos.

1.3.3. Serviços de mixagem (*mixing services*)

Há, ainda, serviços de *mixing* especializados cuja função é criar um encobrimento entre o remetente e o receptor de criptoativos. Cada usuário envia suas moedas virtuais para o *mixer* e designa um ou mais endereços de destino, geralmente para receber a mesma quantia, descontada a taxa cobrada pelo serviço. Em termos metafóricos, os fundos são lançados em uma "piscina" com os ativos de outros usuários, misturados e, então, remetidos para os endereços designados, podendo ainda ser fracionado em diversas pequenas transações, utilizando múltiplas operações de *mixing* em sequência (Estellita, 2020).

No ecossistema de circulação, os *mixers* (misturadores) potencializam a lavagem de dinheiro ao reunir ativos de diferentes usuários, fracioná-los em múltiplas transações de pequeno valor e, ao final, restituir a cada participante montante equivalente, porém com criptoativos oriundos de fontes diversas. Esse processo tem por objetivo obstruir o rastreamento público das transações (Callegari; Linhares, 2025).

No Brasil e em diversas jurisdições, a utilização de mixers vem sendo crescentemente associada a esquemas de lavagem de capitais. A recente regulação do Banco Central (Resolução BCB nº 520/2025) veda expressamente que exchanges e demais prestadoras de serviços de ativos virtuais utilizem ou se conectem a serviços de mixagem, embaralhadores ou robôs destinados a ocultar a identidade de autores ou beneficiários²².

Em síntese, os serviços de *mixing*, exploram a principal lacuna deixada pela pseudonimidade dos criptoativos: eles transformam a rastreabilidade potencial da *blockchain* em uma ferramenta inócua para a investigação, ao fragmentar e embaralhar propositalmente as transações, tornando impossível ou extremamente difícil o seguimento do fluxo de valores.

Em outras palavras, os *mixers* não apenas dificultam o rastreamento; eles o inviabilizam, pois atuam deliberadamente para quebrar o elo entre o endereço de origem – que poderia estar vinculado a um ilícito – e o endereço de destino – que recebe os valores “limpos” (Arbabi;

²² Art. 90 da Resolução BCB nº 520/2025: "É vedado às sociedades prestadoras de serviços de ativos virtuais utilizar misturadores, embaralhadores ou robôs que visem a ocultar os autores ou beneficiários de transações com ativos virtuais."

Shojaeinasab; Najjaran, 2025). Assim, a evidência da transação permanece registrada, mas o nexo probatório essencial para a demonstração da autoria é propositalmente obliterado.

2. A LAVAGEM DE CAPITAIS POR MEIO DE CRIPTOATIVOS

2.1. Crime de Lavagem de Dinheiro

O crime de lavagem de capitais recebe, no ordenamento jurídico brasileiro, a denominação “lavagem de dinheiro”. O verbo “lavar”, que tem origem no latim *lavare*, transmite a noção de expurgo, purificação ou reabilitação, na tentativa de dar feição legal a ativos oriundos de infrações penais, devolvendo-os ao mercado financeiro como se lícitos fossem. No direito comparado, as palavras utilizadas para designar a infração também carregam, em sua raiz etimológica, a ideia de “limpeza”, justamente porque o cerne do delito é a ocultação da origem ilegal do patrimônio (Callegari; Weber, 2017).

Seja qual for a terminologia adotada, a literatura especializada aponta certos padrões que se repetem nas operações de lavagem de capitais, entre os quais se destacam: (i) a reduzida possibilidade de seguir o rastro dos valores para além da origem das movimentações; (ii) o caráter transnacional das transações; (iii) o emprego de técnicas cada vez mais sofisticadas e especializadas, que denotam certa profissionalização do ilícito; e (iv) o volume expressivo de recursos financeiros movimentados (Callegari; Weber, 2017).

No Brasil, o diploma legal que trata especificamente do delito é a Lei nº 9.613/1998, e em seu artigo 1º tipifica a lavagem de dinheiro como a conduta de ocultar ou dissimular a natureza, a origem, a localização, a disposição, a movimentação ou a propriedade de bens, direitos ou valores que provenham, direta ou indiretamente, de infração penal (Brasil, 1998).

Nessa linha, a conduta criminosa prevista na Lei nº 9.613/1998 exige que a ocultação ou a dissimulação recaia sobre determinados aspectos do bem, direito ou valor: sua natureza (características intrínsecas e particularidades); sua origem (procedência ou modo de aquisição); sua localização (lugar onde se encontra); sua disposição (destinação, emprego ou utilização, seja a título oneroso ou gratuito); sua movimentação (deslocamento, transferência ou circulação); ou sua propriedade (titularidade, domínio e os direitos de usar, gozar, dispor e recuperar a coisa de quem injustamente a detenha) (Prado, L.R., 2019).

Para mais, quanto a construção técnico-legislativa do delito de lavagem de dinheiro pode seguir dois modelos principais: o modelo dependente, em que a lavagem surge como

desdobramento da receptação, e o modelo autônomo, em que o crime é tipificado de forma independente, com configuração própria e desvinculada de delitos antecedentes. Em ambos os casos, o foco está na proveniência ilícita de bens ou valores decorrentes de infração penal, direta ou indiretamente, sem distinção quanto à natureza do crime originário (Prado, L.R., 2019).

Desse modo, a norma descreve um comportamento orientado a esconder a origem ilícita de bens ou valores, valendo-se de operações sucessivas que visam a lhes atribuir uma aparência lícita.

O processo de lavagem de capitais, em linhas gerais, desenvolve-se em três fases interdependentes. Na colocação (*placement*), os valores de origem criminosa ingressam no sistema financeiro, frequentemente por meio de conversão, fracionamento ou aquisição de ativos. Na ocultação (*layering*), também chamada de estratificação ou dissimulação, promovem-se sucessivas operações para afastar os recursos de sua origem ilícita, dificultando o rastreamento. Na integração (*integration*), os ativos já aparentam legitimidade e retornam à economia formal, momento em que se busca justificar a riqueza aparentemente lícita (Callegari; Weber, 2017).

Nesse contexto, torna-se evidente que a constante sofisticação dos meios de ocultação patrimonial e o avanço das tecnologias financeiras, em especial os criptoativos, que ampliam os desafios enfrentados pelos mecanismos tradicionais de rastreio e fiscalização. Assim, na sequência, examina-se a prática da lavagem de dinheiro com o uso de criptoativos, observando seus aspectos técnicos, jurídicos e os riscos que apresenta para o sistema de prevenção e repressão penal.

2.2. Fases da lavagem e a inserção dos criptoativos

A estrutura descentralizada e o pseudoanonimato dos criptoativos criam obstáculos específicos em cada uma das três fases do ciclo da lavagem de capitais: ocultação (*placement*), dissimulação (*layering*) e integração (*integration*).

2.2.1. Ocultação

Nesta fase inicial da lavagem de capitais, denominada colocação (*placement*), o agente procura introduzir o produto do crime no sistema financeiro ou converter o recurso ilícito em

um ativo de aparência lícita, sendo quatro são os principais canais de escoamento de capitais nessa etapa: instituições financeiras tradicionais, instituições financeiras não tradicionais, a inserção nos movimentos financeiros cotidianos e outras atividades que transfiram dinheiro para além das fronteiras nacionais (Callegari; Weber, 2017).

No contexto dos criptoativos, a colocação pode ocorrer pela obtenção de ativos virtuais com valores provenientes de infração penal antecedente, o que se viabiliza por meio de *exchanges*, *fintechs*, plataformas de transações diretas (*peer-to-peer*) ou transferências entre carteiras (Estellita, 2020, apud Grzywotz, 2019). Nesse caso, a transação pode ser verificada pela *exchange* ou *fintech*, diante de atividade suspeita, devem, se estiverem sujeitas à regulação, tem o dever legal de comunicar o fato ao Conselho de Controle de Atividades Financeiras (COAF), nos termos da Lei nº 9.613/1998 e da Lei nº 14.478/2022.

Ainda, a simples aquisição de bitcoins mediante pagamento em espécie, realizada em uma transação pessoal ou por intermédio de plataforma de negociação, já pode configurar essa fase inicial. Isso porque o ingresso do valor ilícito no sistema cripto se dá justamente por meio da conversão do dinheiro (físico ou bancário) em ativo virtual, sem que haja, nesse momento, qualquer mecanismo de identificação obrigatória do adquirente (Silva, 2024).

Nesse processo, a atribuição de identidade aos endereços virtuais, elemento essencial para a persecução penal, depende exclusivamente das *exchanges*, uma vez que o código registrado na *blockchain* não contém dados pessoais dos titulares (Estellita, 2020).

2.2.2. Dissimulação

Uma vez inserido no sistema financeiro, o capital de origem criminoso precisa perder qualquer traço de ilicitude — daí a doutrina também denominar essa etapa de mascaramento. Trata-se, agora, de conferir aparência lícita aos recursos, razão pela qual essa fase é chamada de dissimulação (Callegari; Weber, 2017).

No universo dos criptoativos, a dissimulação pode assumir formas simples ou complexa. Na versão simples, o titular é capaz de criar ilimitadas chaves públicas e realizar transferências sem jamais perder o domínio de seus ativos, podendo ainda lançar mão de chaves pertencentes a terceiros ou a intermediários financeiros. Em todas essas situações, a rota seguida e os rastros das operações continuam perfeitamente identificáveis, em razão da natureza transparente do *blockchain*. No entanto, os dados armazenados na cadeia de blocos não revelam diretamente

quem são os proprietários dos endereços virtuais (Estellita, 2020). Essa dualidade, de um lado, a elevada capacidade de rastreamento, de outro, a ausência de identificação imediata do responsável, é precisamente o que configura o pseudoanonimato, distinto do anonimato pleno.

Nessa fase, os *mixing services* (serviços de mistura) são utilizados para apagar os vestígios dos criptoativos no *blockchain*. Esses serviços especializados ocultam a relação entre remetente e receptor: os ativos são misturados com os de outros usuários e redirecionados para os endereços indicados pelo cliente, podendo ainda ser fragmentados em pequenas transações. Como resultado, o rastreamento das moedas torna-se extremamente difícil, senão impossível (Estellita, 2020).

Ademais, o *mixer* opera no sentido de obscurecer o rastro público das movimentações, gerando uma camada de opacidade que inviabiliza, na prática, o rastreamento forense tradicional. Além dessa técnica, empregam-se ainda o *chain hopping* (conversão célere entre diferentes *blockchains*) e a utilização de *exchanges* descentralizadas (DEX), que dispensam a identificação de seus usuários. Em termos práticos, é na fase de dissimulação que a arquitetura dos criptoativos mais compromete a atividade investigativa, uma vez que neutraliza a pretensa transparência do livro-razão distribuído (Callegari; Linhares, 2017).

2.2.3. Integração

Na fase de integração, o objetivo é conferir uma justificativa aparentemente lícita para o patrimônio acumulado. Utilizando-se mecanismos de reinserção no sistema econômico, os produtos da lavagem são transformados em investimentos aplicados em diversos setores da economia (Callegari; Weber, 2017).

Nesse momento, inevitavelmente, o agente precisa recorrer a intermediários – como *exchanges centralizadas* ou *fintechs*, que realizam a conversão de criptoativos para moeda nacional. Por outro lado, se o criminoso optar por gastar os criptoativos diretamente em bens ou serviços (onde esses ativos são aceitos) ou mantê-los indefinidamente como reserva de valor, o ciclo da integração não se completa, e o delito pode permanecer oculto.

Nesse momento, o curso natural da operação exige que o criminoso converta os criptoativos em moeda fiduciária para que possa usufruir do valor sem levantar suspeitas. Essa conversão, inevitavelmente, depende da atuação de intermediários, como *exchanges centralizadas* ou *fintechs*, que realizam a troca de ativos virtuais por moeda nacional,

destacando-se que, em países com controle sobre essas *exchanges*, a operação pode levar à descoberta da transação (Estellita, 2020).

É precisamente nesse ponto que a regulação moderna impõe às plataformas obrigações de identificação dos usuários (*Know Your Client* – KYC), manutenção de registros detalhados e comunicação de operações suspeitas ao COAF, criando um ponto de controle estatal sobre a entrada dos recursos no sistema financeiro tradicional.

Assim, a fase de integração revela uma dupla face: se, por um lado, representa o momento em que o criminoso busca legitimar o patrimônio, por outro, é onde as vulnerabilidades da lavagem com criptoativos se reduzem significativamente. Isso porque, ainda que o agente tenha logrado ocultar e dissimular com sucesso nas fases anteriores, ao tentar transformar seus ativos em dinheiro de curso legal expõe-se inevitavelmente aos mecanismos de fiscalização e controle estatal.

Em contrapartida, o agente pode optar por uma via alternativa, como a aquisição direta de bens e produtos com os criptoativos, nos setores em que esses ativos são aceitos como forma de pagamento, ou mantê-los indefinidamente como reserva de valor, sem jamais convertê-los em moeda fiduciária. Nessas hipóteses, o ciclo da integração não se completa, e o delito pode permanecer oculto, impondo obstáculos adicionais à persecução penal para rastrear e comprovar a destinação final dos recursos ilícitos.

3. LIMITES EPISTÊMICOS DA PROVA DIGITAL E O STANDARD PROBATÓRIO NA LAVAGEM COM CRIPTOATIVOS

Diante do quadro analisado, impõe-se agora um exame mais detido dos desafios probatórios que emergem da interseção entre a arquitetura tecnológica dos criptoativos e as exigências do processo penal. Para tanto, é necessário, inicialmente, delimitar as provas digitais em suas distintas etapas no curso da persecução penal, desde a investigação preliminar até a formação do convencimento judicial, para, em seguida, examinar o standard probatório necessário à condenação pelo crime de lavagem de capitais. Esse percurso metodológico permite isolar, de um lado, os limites epistêmicos impostos pela própria tecnologia (pseudoanonimato, descentralização, uso de *mixers*), e, de outro, as exigências de certeza que o sistema jurídico demanda para além de qualquer dúvida razoável.

3.1. Os limites epistêmicos da prova digital: rastreabilidade versus identificação do agente

No processo penal, o objeto de conhecimento não é o fato bruto, mas a narrativa que se constrói a respeito dele. Assim, a decisão judicial sobre o ocorrido exige que se estabeleça uma coerência entre o discurso e os acontecimentos do mundo concreto, ou seja, aquilo que se convencionou chamar de “passado a ser reconstruído”. Dito de outro modo, o juízo de verdade no âmbito processual consiste em averiguar se a alegação de que o acusado praticou determinada ação corresponde aos fatos narrados (Badaró, 2019).

Para tanto, a atividade probatória e a busca da verdade no processo penal são regidas por critérios e métodos próprios da esfera jurídica, que envolvem não apenas opções técnicas, mas também escolhas valorativas do legislador. Nesse contexto, a epistemologia judiciária dedica-se a examinar o que é a prova, como se organiza e quais fatores a tornam mais ou menos sólida, mais ou menos frágil (Badaró, 2019).

Nesse ponto, ainda no âmbito dos limites da prova, impõe-se considerar a garantia da integridade do elemento probatório desde sua obtenção até sua apresentação em juízo, ou seja, cuja ruptura pode comprometer irremediavelmente a credibilidade do vestígio (Prado, G., 2019)²³, como também, a prova digital pode ser comprometida por obstáculos tecnológicos intrínsecos à arquitetura dos criptoativos, como a mistura deliberada de transações na *blockchain*, que inviabiliza a identificação real do autor da operação (Estellita, 2020)²⁴.

Para os fins deste trabalho, impõe-se diferenciar os dois planos de limitação epistemológica que incidem sobre a prova digital na lavagem de capitais com criptoativos: (i) o limite tecnológico, inerente à arquitetura da *blockchain*, que, embora assegure imutabilidade e rastreabilidade dos fluxos, não contém, em sua estrutura nativa, qualquer elemento que identifique o controlador efetivo da chave privada, reduzindo-se os endereços a meros identificadores numéricos dissociados da pessoa natural; e (ii) o limite jurídico-processual, que exige, para o édito condenatório, um conjunto probatório suficiente para formar convicção além da dúvida razoável, patamar que a mera correlação entre endereços e transações, desacompanhada de outros elementos corroborativos, não é capaz de alcançar.

²³ Sobre o tema da cadeia de custódia e sua ruptura, especialmente no que se refere às provas digitais, confira-se a análise aprofundada de Geraldo Prado (2014).

²⁴ Para os fins deste trabalho, os “limites epistêmicos” examinados não decorrem de falhas na preservação ou na admissibilidade da prova digital, matéria relacionada à cadeia de custódia e aplicável às provas digitais em sentido amplo, mas das restrições informacionais inerentes à própria arquitetura dos criptoativos. O foco da pesquisa recai sobre características tecnológicas como o pseudoanonimato, os *mixers* e as exchanges descentralizadas (DEX), que podem dificultar a identificação do titular dos ativos e, conseqüentemente, a imputação de autoria em crimes de lavagem de capitais.

Aplicando esses pressupostos epistemológicos ao universo da lavagem de capitais realizada por meio de criptoativos, impõe-se examinar como a prova digital é definida, classificada e obtida no ordenamento brasileiro, para então avaliar se os vestígios deixados na *blockchain* são capazes de atingir o standard probatório exigido para a condenação.

3.1.1. Conceito de prova digital e seus limites estruturais nos criptoativos

Os meios de prova são os instrumentos que levam ao processo um elemento apto a revelar ao juiz a verdade de um fato, e servem diretamente para provar a veracidade da hipótese fática e convencer o julgador (Andrade, 2025). Nesse contexto, antes de examinar os instrumentos probatórios disponíveis e seus limites no âmbito do delito de lavagem de capitais com criptoativos, impõe-se, inicialmente, conceituar a prova digital.

Entretanto, na doutrina, não há uniformidade terminológica quanto à prova digital. De todo modo, as provas digitais (ou *digital evidences*) são os dados binários armazenados em suporte eletrônico ou transmitidos em rede, que representam fatos ou ideias, possuindo natureza de fonte de prova real, assemelhada ao documento (Minto, 2021), sendo imaterial e indivisível, composta por uma sequência de *bits* que existe independentemente do suporte físico (Minto, 2021).

Há ainda as noções de prova eletrônica (suporte físico), prova informática (dados processados por computador) e prova tecnológica (qualquer instrumento tecnológico), que são mais amplas que a prova digital (Minto, 2021).

No âmbito dos criptoativos, essa imaterialidade da prova digital se manifesta na *blockchain*: o registro das transações é público, descentralizado e inalterável, permitindo a qualquer participante da rede verificar a ocorrência, o valor e o endereço de origem e destino de cada operação. Contudo, esse mesmo registro é desprovido de quaisquer dados pessoais dos titulares dos endereços, não há nomes, documentos, nacionalidade ou qualquer elemento que, por si só, permita associar a movimentação a uma pessoa natural. A *blockchain* guarda o quê, o quando, o quanto e entre quais endereços, mas não o quem.

De modo análogo, no plano estritamente tecnológico e imaterial da prova digital, os serviços de mistura (*mixers* ou *tumblers*) impõem um limite epistêmico adicional: ao embaralhar deliberadamente as transações na *blockchain*, eles suprimem a rastreabilidade que, em tese, caracterizaria o sistema, tornando impossível vincular o endereço de destino ao

remetente original e, por consequência, inviabilizando a identificação do autor da operação (Estellita, 2020).

Dessa forma, a prova digital dos criptoativos padece de uma limitação epistêmica estrutural: (i) a ausência de dados pessoais na *blockchain*, embora tenha registro público, não contém qualquer elemento que vincule o endereço a uma pessoa natural; (ii) a ação dos serviços de mistura (*mixers/tumblers*) que embaralham deliberadamente as transações, rompendo a rastreabilidade e inviabilizando a identificação do autor; (iii) a criptografia assimétrica (chave privada), cuja posse é essencial para comprovar a titularidade do endereço, mas que não consta do registro público²⁵; (iv) a existência de *exchanges* descentralizadas (DEX) e transações *peer-to-peer* (P2P), que não coletam dados de identificação dos usuários, tornando impossível a obtenção de KYC, e (v) a fragilidade da cadeia de custódia, qualquer ruptura na coleta, preservação ou transferência do vestígio pode comprometer irremediavelmente sua credibilidade ²⁶.

Nesse sentido, busca-se examinar as fases da persecução penal (investigação, instrução e julgamento) e os meios de obtenção de prova disponíveis no ordenamento brasileiro, Relatório de Inteligência Financeira (RIF)²⁷, perícia em *blockchain*, cooperação internacional, busca e apreensão, bem como os limites específicos que cada um desses instrumentos enfrenta diante da tecnologia dos criptoativos.

Delimitado o conceito de prova digital, passa-se a examinar como as obrigações legais impostas a intermediários financeiros e prestadores de serviços de ativos virtuais contribuem para a obtenção de elementos probatórios. Isso porque as entidades sujeitas à regulação antilavagem devem atuar na prevenção e no combate ao delito, destacando-se, entre esses deveres, a identificação de clientes (KYC) e o monitoramento de transações financeiras suspeitas (Estellita, 2020).

3.1.2. Obrigações legais e o início da persecução penal

²⁵ A criptografia assimétrica (ou de chave pública) foi detalhada no item 1.3 deste artigo: a chave pública é um endereço visível a todos na rede; a chave privada, mantida em sigilo pelo titular, é a única capaz de autorizar transações e comprovar a propriedade dos ativos (Camillo, 2023).

²⁶ cadeia de custódia, que assegura a integridade do vestígio desde sua coleta até o juízo, é tema relevante para toda e qualquer prova digital, não apenas para criptoativos. Por essa razão, não será aprofundada neste trabalho, limitando-nos a reconhecer sua importância para a credibilidade probatória

²⁷ Documento que expõe as operações atípicas e as razões da suspeita, sem formular acusações.

No plano internacional, o Grupo de Ação Financeira Internacional (GAFI)²⁸ sistematiza uma série de sinais de alerta (*red flags*) aplicáveis a transações com criptoativos, sendo como valores atípicos, fragmentação de quantias, uso reiterado de serviços de anonimato (*mixers*, *tumblers*) e criação irregular de carteiras digitais, mas, que não configuram, por si sós, prova de ilícito, e sim, servem como parâmetros objetivos para que as entidades obrigadas e as autoridades identifiquem operações que merecem análise aprofundada (FATF, 2019). Assim, a presença de um ou mais *red flags* desencadeia, nos prestadores de serviços regulados, o dever de comunicar a suspeita à unidade de inteligência financeira local, no Brasil, ao COAF.

No ordenamento brasileiro, as *exchanges* e *fintechs* sujeitas à Lei nº 14.478/2022 e à IN RFB nº 2.291/2025 devem adotar procedimentos de identificação de clientes (KYC) e reportar operações suspeitas ao COAF. Uma vez recebida a comunicação, o COAF consolida os indícios em RIF, que é encaminhado às autoridades de persecução penal, e, com base nesses elementos, podem instaurar investigação preliminar.

Superada a fase de inteligência financeira (RIF), a investigação preliminar propriamente dita tem por finalidade angariar elementos que indiquem a probabilidade da existência do crime e de sua autoria, para viabilizar o oferecimento da denúncia. Ainda, a atividade investigatória orienta-se pela busca de indícios suficientes de materialidade e autoria, sem a exigência de prova plena (Lopes Jr., 2019).

Nessa busca, são produzidas provas mais robustas, como: (i) perícia em *blockchain* (para rastrear a cadeia de transferências), (ii) cooperação internacional, com intuito de obter dados de *exchanges* sediadas no exterior, (iii) busca e apreensão de dispositivos eletrônicos, para acessar chaves privadas e carteiras, e (iv) quebra de sigilo telemático e bancário, a fim de cruzar informações entre o sistema tradicional e o ambiente cripto.

Cada qual tem seus limites específicos diante da tecnologia dos criptoativos, como exemplo: a quebra de sigilo pode revelar a materialidade, pela existência da transação e os valores envolvidos, mas nem sempre a autoria, pois os dados bancários nem sempre estão vinculados diretamente ao endereço virtual suspeito. Já a perícia em *blockchain* identifica o fluxo dos ativos, mas pode ser frustrada por serviços de mistura (*mixers*). Por fim, a busca e

²⁸ O GAFI (*Financial Action Task Force – FATF*) é uma organização intergovernamental criada em 1989 no âmbito do G7, sediada em Paris, com o mandato de formular padrões globais e promover políticas para combater a lavagem de capitais, o financiamento do terrorismo e a proliferação de armas de destruição em massa.

apreensão, quando bem-sucedida, pode capturar chaves privadas armazenadas em dispositivos físicos, o que permite associar o endereço à pessoa natural.

Nessa linha, para o oferecimento da denúncia por lavagem de capitais, a Lei nº 9.613/1998 exige apenas indícios suficientes da existência da infração penal antecedente, não sendo necessário o detalhamento pormenorizado do crime-fonte, nem mesmo o conhecimento da autoria ou a punibilidade do autor do crime anterior. Em outras palavras, o órgão acusatório deve identificar, ao menos, as infrações penais antecedentes, mas pode prescindir de uma descrição exaustiva de todas as suas circunstâncias.

Logo, a prova com base em indícios, também chamada de prova indiciária, indireta, circunstancial ou por presunções, é admitida nessa fase, desde que obedeça a certas condições, como: (a) pluralidade de indícios (excepcionalmente um só, se dotado de força incriminatória singular); (b) possibilidade de confirmação posterior por prova direta; (c) estreita relação entre os indícios; (d) concomitância e univocidade incriminatória; (e) enlace preciso e direto entre os indícios e o fato a ser provado, conforme as regras de lógica e de experiência (Callegari; Linhares, 2025).

Outrossim, havendo elementos mínimos que apontem para a ocorrência de crime antecedente e para a movimentação suspeita de criptoativos identificada pelo RIF, a denúncia pode ser oferecida, ainda que a autoria da lavagem não esteja integralmente desvendada. Entretanto, a investigação preliminar não se encerra com o recebimento da denúncia, e sim continua como base para a produção de provas mais aprofundadas na instrução processual, onde se exigirá o padrão de certeza além de dúvida razoável para a condenação.

3.2. O standard probatório necessário para o édito condenatório

De início, cabe conceituar que os standards de prova, no âmbito jurídico, podem ser entendidos como parâmetros que expressam ideais de razoabilidade, normalidade e isonomia, servindo de orientação para a conduta esperada e para a aplicação da lei com racionalidade e justiça, e traduzem-se em níveis de suficiência da prova: definem o grau de convencimento exigido para que uma alegação sobre os fatos seja tida por verdadeira, permitindo ao julgador formar sua convicção de forma controlada e evitar decisões baseadas em meras suposições pessoais (Andrade, 2025).

Como visto, o recebimento da denúncia por lavagem de capitais com criptoativos pode fundar-se em indícios suficientes da infração antecedente e em movimentações suspeitas detectadas pelo RIF, não se exigindo, nessa fase, standard probatório robusto, apenas elementos mínimos para a investigação e o início da ação penal. Contudo, a superação da mera suspeita e o avanço para uma condenação demandam um patamar de comprovação muito mais rigoroso.

Partindo-se de certas premissas, de que a justiça depende da reconstrução dos fatos, de que essa reconstrução pode ser objetiva (não meramente subjetiva) e de que é possível, na maioria dos casos, alcançar um conhecimento verdadeiro sobre os acontecimentos em litígio, impõe-se estabelecer critérios objetivos que permitam distinguir uma prova robusta de uma frágil.

Assim, a epistemologia tem, entre suas tarefas, fornecer parâmetros para aferir quando um conhecimento pode ser considerado verdadeiro, formulando standards de prova variados que sejam objetivamente controláveis ou, no mínimo, intersubjetivamente verificáveis (Badaró, 2019).

Nesse contexto, os standards probatórios no processo penal organizam-se em uma escala gradual de suficiência. A mera suspeita, suficiente para determinadas medidas investigativas iniciais, situa-se entre 15% e 25% de confirmação da hipótese. Medidas mais invasivas exigem grau de corroboração em torno de 30% a 40%. Para o recebimento da denúncia, o patamar necessário alcança cerca de 50% a 60%, enquanto a prisão preventiva demanda aproximadamente 70% de convencimento. Já a condenação penal, por seu caráter definitivo e gravoso, pressupõe um nível de confirmação significativamente superior, estimado entre 95% e 99%, em sintonia com o standard da prova além de qualquer dúvida razoável (Andrade, 2025).

Dessa forma, a fim de que se possa proferir um édito condenatório no crime de lavagem de capitais perpetrado mediante criptoativos, impõe-se que as provas produzidas em contraditório judicial satisfaçam o standard de certeza além de qualquer dúvida razoável, conforme estabelece o art. 155 do Código de Processo Penal (CPP).

Nessa linha de intelecção, os meios de obtenção de prova disponíveis no âmbito da lavagem de capitais com criptoativos, com perícia em *blockchain*, cooperação internacional, busca e apreensão de dispositivos eletrônicos e quebra de sigilo telemático e bancário, raramente produzem um encadeamento probatório robusto o suficiente, cada qual com seus limites técnicos e legais.

Com efeito, por se tratar de um crime que deixa vestígios, especificamente o rastro do dinheiro na *blockchain*, em tese seria possível produzir prova pericial sobre os criptoativos, uma vez que os registros são distribuídos e permanentemente armazenados na rede. Para os criptoativos provenientes de *fintechs* e *exchanges* que realizam a identificação de clientes (KYC) e comunicam operações ao COAF, é possível ao menos atestar a materialidade da transação. Contudo, as dificuldades estruturais dos criptoativos, como o pseudoanonimato e uso de *mixers*, somadas à ausência de previsão legal específica e de jurisprudência consolidada sobre como realizar a perícia digital, nos termos do art. 158 do CPP, fragilizam sobremaneira a prova.

Ademais, em razão da globalidade e transnacionalidade das transações, a cooperação internacional, frequentemente necessária para obter dados de *exchanges* sediadas no exterior, constitui meio demorado, sujeito à discricionariedade dos Estados parceiros e à eficácia dos tratados bilaterais ou multilaterais²⁹. Além disso, esbarra em diferentes níveis de proteção de dados e de sigilo bancário, o que pode inviabilizar ou atrasar sobremaneira a obtenção das informações.

Outrossim, a busca e apreensão de dispositivos eletrônicos destina-se a capturar a chamada prova digital estática, ou seja, evidências armazenadas localmente no equipamento do investigado. Entre elas incluem-se arquivos de carteira como *wallet.dat* para Bitcoin, arquivos *.json* ou *keystore* para a rede *Ethereum*, e arquivos similares de outras *blockchains*, em chaves privadas, frases de recuperação (*seed*³⁰), aplicativos de criptomoedas (como carteiras de software ou extensões de navegador) com histórico de transações, conversas em aplicativos de mensagem que mencionem endereços virtuais e registros de navegação em *exchanges*.

Todavia, a eficácia dessa medida depende fundamentalmente de que o titular tenha armazenado fisicamente esses elementos em seus dispositivos. Logo, se os ativos forem mantidos exclusivamente em carteiras não custodiais ou em *exchanges* descentralizadas que não exigem custódia local, a busca e apreensão pode ser infrutífera, pois não haverá o que apreender fisicamente.

²⁹ O GAFI, por meio de suas Recomendações 37 a 40, estabelece padrões para a cooperação internacional, incluindo a assistência jurídica mútua (Recomendação 37), o compartilhamento de informações entre autoridades (Recomendação 39) e outras formas de cooperação (Recomendação 40). A efetividade dessa cooperação, contudo, depende da vontade política do Estado requerido, da compatibilidade entre os ordenamentos jurídicos e da existência de acordos bilaterais ou multilaterais operacionais.

³⁰ A *seed* (ou frase de recuperação) é uma sequência de palavras (geralmente 12 ou 24) que permite restaurar todas as chaves privadas de uma carteira; sua obtenção equivale ao controle total sobre os ativos.

A mera comunicação de operações suspeitas e o cumprimento das obrigações legais por *exchanges* e *fintechs* – KYC, monitoramento e reporte ao COAF –, embora indispensáveis para a fase investigativa e para o oferecimento da denúncia, não são suficientes, por si sós, para a condenação, pois, muito embora comprovem que uma transação ocorreu, tendo sua materialidade, não é possível atribuir autoria à pessoa natural que detém a conta seja a autora da operação criminosa. Isso porque o titular da conta pode ser um interposto (laranja), as chaves privadas podem estar sob controle de terceiros, e o próprio endereço virtual pode ter sido utilizado por múltiplas pessoas.

Ainda, a depender das características empregadas pelo criminoso, como o uso de *mixers* (*tumblers*), *exchanges* descentralizadas (DEX) que não exigem KYC, carteiras não custodiais ou endereços descartáveis, a capacidade de rastreamento e de identificação do autor pode ser reduzida a zero. Nessas hipóteses, o que se tem é a certeza de que algo foi movimentado, mas não quem movimentou.

Destarte, as provas que legitimam a fase investigativa e o recebimento da denúncia, não são aptas a respaldar um édito condenatório. Isso porque, o standard exigido para a condenação é a certeza para além de qualquer dúvida razoável, patamar que a prova digital, por si só, não alcança.

Com efeito, a *blockchain* registra a movimentação, mas não identifica os titulares dos endereços. *Mixers*, *exchanges* descentralizadas (DEX) e carteiras não custodiais rompem deliberadamente a rastreabilidade. Ainda, os meios complementares de prova, cada qual com seus limites técnicos e legais, raramente conseguem suprir essa lacuna estrutural.

Em suma, a identificação de um endereço virtual e de suas movimentações na *blockchain*, embora constitua elemento probatório relevante, não é suficiente, por si só, para fundamentar um juízo condenatório. Na ausência de elementos adicionais capazes de vincular, de forma segura, o endereço investigado a uma pessoa natural determinada, não se alcança o grau de certeza exigido para a atribuição da autoria no processo penal. Por essa razão, a responsabilização por lavagem de capitais envolvendo criptoativos demanda um conjunto probatório mais amplo, integrado por elementos independentes e convergentes que permitam estabelecer, com segurança, o vínculo entre a atividade registrada no ambiente digital e o acusado.

Por fim, a definição de um standard de prova objetivo, ainda que não quantificável numericamente, é tarefa espinhosa. E a dificuldade reside em estabelecer um critério que sirva

como guia para o juízo axiológico sem produzir ambiguidades no texto legal, na jurisprudência ou na doutrina, porque, até recentemente, o tema era pouco explorado no Brasil, e limitava-se a invocar o princípio do *in dubio pro reo*, como se bastasse dizer que, ignorando-se a necessidade de analisar os diferentes graus de convencimento exigidos ao longo do processo (Badaró, 2019).

Por fim, conclui-se que prova digital produzida no âmbito da lavagem de capitais com criptoativos, embora detenha significativa relevância investigativa e probatória, não se revela, em regra, suficiente para atingir, isoladamente, o standard de certeza além da dúvida razoável exigido para a condenação. Isso porque os limites epistêmicos inerentes a essa tecnologia são múltiplos e frequentemente dificultam a adequada demonstração da autoria delitiva, destacando-se o pseudoanonimato da *blockchain*, a utilização de serviços de mistura (*mixers*) e de exchanges descentralizadas (DEX), a criptografia assimétrica que impede o acesso às chaves privadas e as dificuldades relacionadas à obtenção, preservação e validação da prova digital.

Assim, os registros extraídos da *blockchain* devem ser compreendidos como elementos integrantes de um quadro probatório mais amplo, cuja suficiência dependerá da existência de provas complementares aptas a vincular, de forma segura, o endereço virtual investigado ao seu efetivo controlador. Nesse sentido, a apreensão de chaves privadas, a extração forense de dados de dispositivos eletrônicos, a interceptação telemática regularmente autorizada, os registros mantidos por prestadores de serviços de ativos virtuais e demais elementos de corroboração assumem papel fundamental, na medida em que permitem estabelecer o nexo entre os vestígios digitais e a pessoa natural submetida à persecução penal. Somente a partir da convergência desses elementos probatórios será possível atingir o grau de certeza necessário à prolação de um édito condenatório.

4. CONSIDERAÇÕES FINAIS

Por fim, o presente artigo não teve a pretensão de esgotar o debate sobre a prova digital na lavagem de capitais com criptoativos. Buscou-se, contribuir para a discussão acadêmica e, com ela, vislumbrar por uma regulamentação minimamente adequada.

A pesquisa demonstrou que a prova digital em delitos de lavagem de capitais cometidos com criptoativos apresenta uma limitação epistêmica intransponível: a *blockchain* registra com

transparência e imutabilidade a movimentação patrimonial, mas não contém dados pessoais dos titulares dos endereços, impedindo a identificação direta do agente. Além disso, o uso de *mixers* (*tumblers*), exchanges descentralizadas (DEX) e carteiras não custodiais anônimas rompe deliberadamente o encadeamento rastreável, inviabilizando a atribuição de autoria com o grau de certeza exigido pelo art. 155 do CPP.

Dito isso, no Brasil é regulamentado, ainda que parcialmente, o ecossistema de circulação de criptoativos. A partir da Lei nº 14.478/2022 e a Instrução Normativa RFB nº 2.291/2025 impõem a *exchanges* e *fintechs* o dever de adotar procedimentos de identificação de clientes (KYC) e de comunicar operações suspeitas ao COAF, e, a mesma legislação veda os serviços de mistura (*mixers*), reconhecendo que essas ferramentas tornam praticamente impossível a identificação da transação e de seu autor (Callegari; Linhares, 2025).

Seguindo essa linha, os meios complementares de prova igualmente se mostram sujeitos a limitações epistêmicas, de modo que a prova digital extraída de registros em *blockchain* não pode ser tomada, isoladamente, como fundamento suficiente para a atribuição de responsabilidade penal. Embora os elementos permitam reconstruir fluxos transacionais com elevado grau de precisão, eles não são capazes, por si sós, de estabelecer a identidade do efetivo controlador dos endereços envolvidos.

Por essa razão, a imputação da autoria demanda um conjunto probatório mais abrangente e corroborativo, formado por elementos independentes e convergentes que permitam vincular, de maneira segura, a atividade registrada no ambiente digital à pessoa natural submetida à persecução penal, em observância às exigências constitucionais inerentes ao édito condenatório.

Para superar esse déficit, são necessárias três medidas regulatórias coordenadas: (i) a vedação expressa e a responsabilização penal pelo uso de *mixers* e *tumblers*, ferramentas cuja finalidade é obstruir a rastreabilidade e que, por essa natureza, integram a própria fase da lavagem de capitais; (ii) a padronização pericial, com a instituição de procedimento vinculante para coleta, cadeia de custódia e valoração da prova digital, suprimindo a lacuna da prova digital atualmente existente no art. 158 do CPP; e (iii) a criação de mecanismos eficazes para obtenção de dados cadastrais junto às *exchanges*, com procedimento judicial ágil e garantia de contraditório, sem, contudo, instituir presunções automáticas de titularidade que possam comprometer o standard probatório da dúvida razoável.

Contudo, a efetividade dessas medidas depende de sua inserção em uma estrutura normativa coerente e sistematizada, necessitando, portanto, de uma disciplina legal específica e integrada para a produção e utilização da prova digital no contexto dos criptoativos evidencia a necessidade de uma reforma legislativa abrangente, destinada a estabelecer parâmetros claros para a obtenção, preservação, autenticação e valoração desses elementos probatórios. A construção de um marco regulatório unitário mostra-se indispensável para conferir previsibilidade, segurança jurídica e legitimidade à atuação estatal diante dos desafios impostos pela criminalidade econômica digital.

Por fim, a complexidade tecnológica e o pseudoanonimato inerentes ao ambiente das criptomoedas impõem à persecução penal da lavagem de capitais um duplo desafio, exige-se, de um lado, um arcabouço probatório particularmente robusto, apto a superar a opacidade digital sem recorrer a atalhos que comprometam a garantia de ampla defesa, e, de outro, procedimentos específicos, capazes de conferir segurança jurídica à coleta e à valoração da prova, sem os quais o juízo condenatório se expõe a um risco permanente de ilegitimidade.

Assim, a regulamentação futura, nesse sentido, ultrapassa o plano da eficiência investigativa, ela se impõe como condição de legitimidade democrática do sistema penal, na medida em que a tutela penal dos bens jurídicos só se justifica quando exercida com estrito respeito às garantias fundamentais que conferem ao processo sua razão de ser.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Flávio da Silva. **Standards de prova no processo penal**: quanto de prova é necessário para deferir medidas cautelares, receber a denúncia, pronunciar e condenar? 4. ed. rev. e atual. São Paulo: Juspodivm, 2024. 336 p.

ANTONPOULOS, Andreas M. **Mastering Bitcoin**: programming the open blockchain. 2. ed. Sebastopol: O'Reilly Media, 2017.

ARBABI, Alireza; SHOJAEINASAB, Ardeshir; NAJJARAN, Homayoun. **Mixing Services in Bitcoin and Ethereum Ecosystems: A Review**. IET Blockchain, 2025. Disponível em: https://www.researchgate.net/publication/394451249_Mixing_Services_in_Bitcoin_and_Ethereum_Ecosystems_A_Review. Acesso em: 03 nov. 2025.

BADARÓ, Gustavo Henrique. **Epistemologia judiciária e prova penal**. São Paulo: Revista dos Tribunais, 2019.

BADARÓ, Gustavo Henrique. **Processo Penal**. 9. ed. São Paulo: Thomson Reuters Brasil, 2021.

BANCO CENTRAL DO BRASIL. **Comunicado nº 25.306, de 19 de fevereiro de 2014**. Alerta sobre os riscos decorrentes da aquisição e da guarda de moedas virtuais. *Diário Oficial da União*, Brasília, DF, 19 fev. 2014. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/comunicado25306>. Acesso em: 02 nov. 2025.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 519, de 10 de novembro de 2025**. Disciplina os processos de autorização relacionados ao funcionamento das sociedades prestadoras de serviços de ativos virtuais. *Diário Oficial da União*, Brasília, DF, 11 nov. 2025.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 520, de 10 de novembro de 2025**. Disciplina a constituição e o funcionamento das sociedades prestadoras de serviços de ativos virtuais e a prestação de serviços de ativos virtuais por outras instituições autorizadas a funcionar pelo Banco Central do Brasil. *Diário Oficial da União*, Brasília, DF, 11 nov. 2025.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 521, de 10 de novembro de 2025**. Altera a Resolução BCB nº 277, de 31 de dezembro de 2022, a Resolução BCB nº 278, de 31 de dezembro de 2022, e a Resolução BCB nº 279, de 31 de dezembro de 2022, para incluir as prestadoras de serviços de ativos virtuais no mercado de câmbio. *Diário Oficial da União*, Brasília, DF, 11 nov. 2025.

BOTTINI, Pierpaolo Cruz; BADARÓ, Gustavo Henrique. **Lavagem de dinheiro: aspectos penais e processuais penais: comentários à Lei 9.613/1998, com as alterações da Lei 12.683/2012**. São Paulo: Revista dos Tribunais, 2012.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941** – Código de Processo Penal. *Diário Oficial da União*, Rio de Janeiro, RJ, 13 out. 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 02 nov. 2025.

BRASIL. **Instrução Normativa RFB nº 1.888, de 3 de maio de 2019**. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Brasília, DF, 2019.

BRASIL. **Instrução Normativa RFB nº 2.278, de 28 de agosto de 2025**. Altera a Instrução Normativa RFB nº 1.571, de 23 de julho de 2015, para dispor sobre a obrigatoriedade de

prestação de informações relativas às operações financeiras pelas instituições de pagamento. *Diário Oficial da União*, Brasília, DF, 29 ago. 2025.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores. *Diário Oficial da União Brasília*, DF, 1998.

BRASIL. **Lei nº 12.683, de 9 de julho de 2012**. Altera a Lei nº 9.613/1998, e dá outras providências. *Diário Oficial da União Brasília*, Brasília, DF, 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014** (Marco Civil da Internet). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes para a prestação de serviços de ativos virtuais e para a atuação de prestadores desses serviços no Brasil. *Diário Oficial da União Brasília*, Brasília, DF, 2022.

BRASIL. Comissão de Valores Mobiliários (CVM). **Ofício-Circular nº 1/2018/CVM/SIN, de 12 de janeiro de 2018**. Comunicado sobre os riscos e o enquadramento jurídico de investimentos em criptoativos. *Diário Oficial da União Brasília*, Brasília, DF, 2018.

CALLEGARI, André Luís; LINHARES, Raul Marques. **Lavagem de dinheiro**: com a jurisprudência do STF e do STJ. 3. ed. São Paulo: Marcial Pons, 2025.

CALLEGARI, André Luís; WEBER, Ariel Barazzetti. **Lavagem de dinheiro**. 2. ed. rev., atual. e ampl. São Paulo: Atlas, 2017.

CAMILLO, Carlos Eduardo da Silva. Criptoativos – Cryptoassets. *ReJuB - Revista Judiciária Brasileira*, Edição Especial Direito Digital, Brasília, 285-308, 2023.

CIESIELSKA-MACIĄGOWSKA, Dorota; SPYRA, Łukasz. Cryptocurrency exchanges in the decentralized finance system. **Kwartalnik Nauk o Przedsiębiorstwie**, v. 75, 2025. DOI: DOI: 10.33119/KNOP.2025.75.1.2.

EICHENGREEN, Barry. Financial regulation in the age of the platform economy. *Journal of Banking Regulation*, v. 23, p. 40–51, 2022. DOI: 10.1057/s41261-021-00178-w.

ESTELLITA, Heloisa. Criptomoedas e lavagem de dinheiro. [Resenha de] GRZYWOTZ, Johanna. **Virtuelle Kryptowährungen und Geldwäsche**. Berlin: Duncker & Humblot, 2019. *Revista Direito GV*, São Paulo, v. 16, n. 1, p. 1-13, jan./abr. 2020.

FATF – FINANCIAL ACTION TASK FORCE. **Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers**. Paris: FATF, 2019.

FCA (FINANCIAL CONDUCT AUTHORITY). **Guidance on Cryptoassets**: Consultation Paper CP19/3. London: FCA, jan. 2019.

GRUPENMACHER, G. T. **As plataformas de negociação de criptoativos**: uma análise comparativa com as atividades das corretoras e da Bolsa sob a perspectiva da proteção do investidor e da prevenção à lavagem de dinheiro. Fundação Getúlio Vargas, São Paulo, 2019.

IBM. **Blockchain**: o que é e como funciona. São Paulo, 2024. Disponível em: <https://www.ibm.com/br-pt/think/topics/blockchain>. Acesso em: 03 maio 2026.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 01 nov. 2025.

NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven. **Bitcoin and Cryptocurrency Technologies**. Princeton: Princeton University Press, 2016.

PRADO, Geraldo. **Prova Penal e Sistema de Controles Epistêmicos**: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. 1. ed. São Paulo: Marcial Pons, 2014.

PRADO, Luiz Regis. **Direito Penal Econômico**. 8. ed. Rio de Janeiro: Forense, 2019.

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. DOI: 10.5281/zenodo.11175344. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1052. Acesso em: 06 mai. 2025.

SCHMIDT, Andrei Zenkner. **Direito Penal Econômico**: parte geral. Porto Alegre: Livraria do Advogado, 2018.

SIDHPURWALA, Huzaifa. **Uma breve história da criptografia**. Red Hat, 12 jan. 2023. Disponível em: <https://www.redhat.com/pt-br/blog/brief-history-cryptography>. Acesso em 04. mai. 2026

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain revolution**: how the technology behind bitcoin is changing money, business, and the world. New York: Penguin Random House, 2016.

TELLES, Christiana Mariani da Silva. **Sistema bitcoin, lavagem de dinheiro e regulação**. 2018. 144 f. Dissertação (Mestrado em Direito) – Fundação Getúlio Vargas, Rio de Janeiro, 2018. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/578db535-ac77-4b1c-857b-d472484ff8a8/content>. Acesso em: 01 nov. 2025.

ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.