PONTIFICIA UNIVERSIDADE CATOLICA DE SÃO PAULO

Armando de Souza Mesquita

Título:

Lavagem de Dinheiro por Meio de Criptomoedas: Desafios Jurídicos e a Cooperação Internacional como Mecanismo de Controle

GRADUAÇÃO EM DIREITO

São Paulo

2025

PONTIFICIA UNIVERSIDADE CATOLICA DE SÃO PAULO

Armando de Souza Mesquita

Lavagem de Dinheiro por Meio de Criptomoedas: Desafios Jurídicos e a Cooperação Internacional como Mecanismo de Controle

Trabalho De Conclusão De Curso À Banca Examinadora Da Pontifícia Universidade Católica De São Paulo, com exigência parcial para finalização da graduação em direito, sob a orientação da Profa. Marina Faraco

São Paulo - SP

2025

AGRADECIMENTOS

Aos meus pais, Armando e Nádia, pelo amor, apoio incondicional e exemplo constante de integridade e perseverança. Obrigado por me ensinarem, ao longo de toda a minha trajetória, a ser uma pessoa cada vez melhor.

À minha irmã, Karime, pela presença cotidiana, pelo incentivo e pela lealdade nas horas difíceis. Sua companhia firme e generosa foi essencial para que eu enfrentasse com serenidade os desafios deste percurso.

À minha namorada, Luana, pelo companheirismo e pela paciência ao longo destes seis anos, oferecendo apoio nos momentos de maior exigência acadêmica e pessoal. Seu cuidado constante fez diferença em cada etapa deste percurso.

Aos meus avós, cuja formação humana e ética deixaram marcas permanentes na minha vida. Os princípios que me transmitiram como respeito, honestidade e dedicação foram e continuam sendo o alicerce das minhas escolhas.

À minha Professora Orientadora, Profa. Mariana Faraco, registro minha profunda gratidão pela orientação. Agradeço, em especial, pela compreensão diante do trajeto percorrido.

RESUMO

Este trabalho investiga a problemática da lavagem de dinheiro por meio de criptomoedas e analisa os desafios enfrentados pela cooperação internacional para o enfrentamento desse fenômeno. O objetivo principal é compreender como os instrumentos jurídicos e institucionais internacionais vêm sendo utilizados para conter práticas ilícitas associadas à crescente utilização de criptoativos. A justificativa do estudo encontra respaldo na expansão global dos ativos digitais e na dificuldade dos Estados em regulá-los de forma uniforme, o que compromete a eficácia no combate aos fluxos financeiros ilícitos. Parte-se da hipótese de que, apesar da existência de tratados multilaterais e da atuação de organismos como o GAFI, ainda há lacunas significativas na coordenação internacional, sobretudo em razão das diferenças legislativas e do caráter descentralizado das tecnologias envolvidas. A pesquisa adota uma abordagem qualitativa, com base em revisão bibliográfica, análise documental e estudo de casos internacionais. Os resultados esperados incluem a identificação dos principais entraves enfrentados pelos Estados, bem como a proposição de caminhos para o aprimoramento da cooperação entre jurisdições.

Palavras-chave: Criptomoedas. Blockchain. Lavagem de dinheiro. Direito Internacional. Cooperação internacional.

ABSTRACT

This undergraduate thesis investigates the problem of money laundering through cryptocurrencies and analyzes the challenges faced by international cooperation in addressing this phenomenon. The main objective is to understand how international legal and institutional instruments have been used to curb illicit practices associated with the growing use of cryptoassets. The rationale for the study lies in the global expansion of digital assets and the difficulty states face in regulating them uniformly, which undermines the effectiveness of efforts to combat illicit financial flows. The study proceeds from the hypothesis that, despite the existence of multilateral treaties and the work of bodies such as the Financial Action Task Force (FATF), significant gaps remain in international coordination, largely due to legislative differences and the decentralized nature of the underlying technologies. The research adopts a qualitative approach based on a literature review, documentary analysis, and case studies of international operations. The expected results include identifying the main obstacles faced by states and proposing pathways to improve cooperation across jurisdictions.

Keywords: Cryptocurrencies. Blockchain. Money laundering. International law. International cooperation.

LISTA DE ABREVIATURAS E SIGLAS

5AMLD — Fifth Anti-Money Laundering Directive (5ª Diretiva AML da UE).

ABCripto — Associação Brasileira de Criptoeconomia.

AMM — Automated Market Maker (formador de mercado automatizado em DeFi).

API — Application Programming Interface (interface de programação de aplicações).

ARIN — Asset Recovery Inter-Agency Network (rede interagências de recuperação de ativos).

BIS — Bank for International Settlements (Banco de Compensações Internacionais).

CARIN — Camden Asset Recovery Inter-Agency Network (rede europeia de recuperação de ativos).

CFTC — Commodity Futures Trading Commission (EUA).

COAF — Conselho de Controle de Atividades Financeiras (UIF/COAF).

CVM — Comissão de Valores Mobiliários.

DAO — Decentralized Autonomous Organization (organização autônoma descentralizada).

DEX — Decentralized Exchange (exchange descentralizada).

DOJ — U.S. Department of Justice (Departamento de Justiça dos EUA).

DRCI/MJSP — Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional / Ministério da Justiça e Segurança Pública.

EGMONT — Egmont Group (rede global de UIFs).

EUROPOL — Agência de Cooperação Policial da União Europeia.

FinCEN — Financial Crimes Enforcement Network (EUA).

GDPR — General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados da UE).

GAFILAT — Grupo de Ação Financeira da América Latina.

IVMS-101 — InterVASP Messaging Standard 101 (padrão de dados para “travel rule”).

JMLIT — Joint Money Laundering Intelligence Taskforce (Reino Unido).

KYT — Know Your Transaction (conheça sua transação).

L1/L2 — Layer 1 / Layer 2 (camadas de base e de escalabilidade em blockchain).

LGPD — Lei Geral de Proteção de Dados (Brasil).

MEV — Maximal Extractable Value (valor máximo extraível por ordenação de transações).

MLAT — Mutual Legal Assistance Treaty (tratado de assistência jurídica mútua).

MPC — Multi-Party Computation (computação multipartidária para chaves).

NFT — Non-Fungible Token (token não fungível).

OFAC — Office of Foreign Assets Control (órgão de sanções do Tesouro dos EUA).

OSINT — Open-Source Intelligence (inteligência de fontes abertas).

OTC — Over-the-Counter (negociação de balcão).

PEP — Pessoa Exposta Politicamente.

PLD/FT — Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

ROS/STR — Relatório de Operações Suspeitas / Suspicious Transaction Report.

RRAG — Rede de Recuperação de Ativos do GAFILAT.

StAR — Stolen Asset Recovery Initiative (UNODC/Banco Mundial).

Tesouro (U.S. Treasury) — U.S. Department of the Treasury (Departamento do Tesouro dos EUA).

TRISA / TRP / OpenVASP — Soluções/Protocolos para intercâmbio de dados da travel rule.

UNODC — United Nations Office on Drugs and Crime (Escritório da ONU sobre Drogas e Crime).

UTXO — Unspent Transaction Output (modelo de saída não gasta, p.ex., no Bitcoin).

VASP — Virtual Asset Service Provider (provedor de serviços de ativos virtuais).

SUMÁRIO

INTRODUÇÃO..... 9

CAPÍTULO 1 – FUNDAMENTOS CONCEITUAIS E NORMATIVOS..... 11

1.1 O que são criptomoedas 11

1.2 Estrutura e funcionamento da tecnologia blockchain 15

1.3 Conceito e fases da lavagem de dinheiro 20

1.4 Cooperação internacional: fundamentos e tratados principais 25

CAPÍTULO 2 – LAVAGEM DE DINHEIRO POR MEIO DE CRIPTOMOEDAS..29

2.1 Ferramentas e técnicas de ocultação digital 29

2.2 Atores e estruturas envolvidas 32

2.3 Casos práticos e operações internacionais relevantes 36

2.4 Riscos regulatórios e impactos transnacionais 41

CAPÍTULO 3 – COOPERAÇÃO INTERNACIONAL E OS CRIPTOATIVOS.....45

3.1 O papel do GAFI e suas recomendações 45

3.2 Mecanismos multilaterais e redes de inteligência financeira 48

3.3 Limitações legislativas e desafios à harmonização normativa 51

3.4 Tendências e aspectos para o combate global à lavagem com criptoativos..55

CONCLUSÕES.....59

INTRODUÇÃO

A expansão global dos criptoativos, impulsionada por inovações como blockchain, exchanges e serviços de custódia, alterou o modo de circulação de valores e desafiou modelos clássicos de prevenção e repressão à lavagem de dinheiro. Se, por um lado, tais tecnologias ampliam eficiência e inclusão financeira, por outro, introduzem vetores de risco associados à pseudonimidade, à desintermediação e à fragmentação regulatória entre jurisdições. Nesse cenário, este trabalho examina a lavagem de dinheiro por meio de criptoativos e o papel da cooperação internacional como mecanismo de controle desse fenômeno transnacional.

O problema de pesquisa que orienta o estudo formula-se nos seguintes termos: em que medida os instrumentos e arranjos de cooperação internacional, sendo eles normativos, institucionais e operacionais, têm sido capazes de conter práticas de lavagem de dinheiro que se valem de criptoativos? A pergunta parte do reconhecimento de que o produto, a prova e os agentes envolvidos frequentemente transcendem fronteiras, exigindo coordenação célere entre autoridades de diferentes países.

Parte-se da hipótese de que, embora exista um arcabouço relevante (padrões do Grupo de Ação Financeira – GAFI, redes de Unidades de Inteligência Financeira e tratados de assistência mútua), a efetividade ainda é comprometida por: (i) assimetrias regulatórias e de supervisão entre países; (ii) desafios técnicos para atribuir titularidade/controle de endereços e rastrear fluxos com ferramentas forenses; e (iii) lacunas de cooperação prática, desde pedidos de assistência jurídica até o intercâmbio tempestivo de informação financeira. No período de 2019 a 2025, o GAFI reiterou e atualizou os padrões internacionais (Recomendação 15), destacando baixa implementação global e riscos emergentes em DeFi e carteiras não custodiadas.

O objetivo geral é avaliar a efetividade da cooperação internacional no enfrentamento da lavagem de capitais com criptoativos. Como objetivos específicos: (i) descrever conceitos essenciais (criptoativos, blockchain, fases da lavagem) e marcos normativos de referência; (ii) identificar técnicas e atores usualmente envolvidos (mixers, serviços de conversão, VASPs, Peer-to-Peer e

DeFi); (iii) analisar casos e operações com repercussão transnacional para evidenciar padrões de atuação e respostas estatais; e (iv) apontar empecilhos e sugerir recomendações para aprimorar a coordenação entre jurisdições.

A justificativa é acadêmica, prática e social. Acadêmica, por mobilizar debates contemporâneos sobre regulação tecnológica, compliance e cooperação penal internacional. Prática, porque reguladores, autoridades de persecução e o setor privado precisam alinhar procedimentos de identificação, monitoramento e congelamento de ativos em ecossistemas digitais. Social e econômica, porque fluxos ilícitos corroem a confiança nos mercados e podem financiar atividades de alto impacto.

Metodologicamente, adota-se abordagem qualitativa, sustentada em revisão bibliográfica e análise documental (legislação nacional e internacional, padrões do GAFI e diretrizes de autoridades) e em estudos de casos com repercussão transnacional. O recorte temporal prioriza 2019 a 2025, período esse de consolidação de padrões internacionais para VASPs e de marcos internos no Brasil. (IN RFB nº 1.888/2019; Lei nº 14.478/2022; Decreto nº 11.563/2023), enquanto o recorte espacial toma o ordenamento brasileiro como eixo, em diálogo com experiências estrangeiras e mecanismos multilaterais.

Para ilustrar a dimensão transfronteiriça e a necessidade de cooperação, serão abordados casos paradigmáticos: a derrubada do Hydra Market em ação conjunta EUA–Alemanha; o desmantelamento do ChipMixer pela Europol e autoridades parceiras; a responsabilização do exchange Bitzlato por operar sem controles adequados; as ações criminais envolvendo o Samourai Wallet; e a oscilação regulatória em torno do Tornado Cash.

Quanto à organização, o Capítulo 1 sistematiza fundamentos conceituais e normativos (criptoativos, blockchain, fases da lavagem e bases da cooperação). O Capítulo 2 examina a operacionalização da lavagem no ecossistema cripto, mapeando técnicas, atores e casos com impactos transfronteiriços. O Capítulo 3 analisa a cooperação internacional, o papel do GAFI e dos mecanismos multilaterais, limitações à harmonização e tendências. Na conclusão apresentam-se respostas à pergunta de pesquisa, implicações para o Brasil e recomendações para políticas públicas e cooperação.

CAPÍTULO 1 – FUNDAMENTOS CONCEITUAIS E NORMATIVOS

O presente capítulo estabelece as bases conceituais e normativas indispensáveis para a compreensão do fenômeno estudado ao longo do trabalho. Parte-se da distinção entre criptoativos (categoria ampla de representações digitais de valor), criptomoedas (subconjunto vocacionado a ser meio de troca), e demais tokens com funções econômicas diversas (pagamento, utilidade, lastro, governança), destacando como essas diferenças importam para fins de identificação de riscos, sujeição regulatória e desenho de controles.

Em seguida, reconstrói-se a arquitetura tecnológica que dá suporte a esses arranjos, sobretudo a blockchain e seus elementos mínimos (transações, mempool, validação/consenso, finalização probabilística), a fim de mostrar por que a pseudonimidade, a composabilidade e a portabilidade transfronteiriça condicionam tanto as tipologias de ocultação quanto as possibilidades de rastreabilidade.

1.1 O que são criptomoedas

As criptomoedas integram o gênero mais amplo dos criptoativos, entendido como representações digitais de valor que empregam técnicas de criptografia e arranjos de registro distribuído para possibilitar a emissão, a transferência e a custódia de unidades digitais sem a necessidade de um emissor central ou de uma arquitetura de confiança baseada exclusivamente em intermediários. Em sua acepção estrita, as criptomoedas são concebidas para desempenhar funções econômicas típicas de moeda, meio de troca, unidade de conta e reserva de valor, ainda que o grau de êxito prático em cada uma dessas funções varie conforme as propriedades do protocolo, a maturidade tecnológica, a adoção social e a regulação vigente.

Em acepção ampla, “criptoativo” abarca categorias diversas de tokens, como os de pagamento, utilidade e aqueles com características de valores mobiliários; as criptomoedas, portanto, constituem espécie dentro desse conjunto.

Do ponto de vista técnico, a maioria das criptomoedas opera sobre blockchains públicas, ou seja, livros-razão distribuídos que mantêm blocos de transações encadeados por funções de hash, cuja integridade e ordenação são

asseguradas por mecanismos de consenso. O desenho mais difundido recorre a algoritmos como o proof-of-work (PoW) e o proof-of-stake (PoS), por meio dos quais participantes descentralizados acordam a inclusão de novos blocos, mitigando o risco de gasto duplo e viabilizando uma noção compartilhada de estado da rede.

Usuários controlam chaves privadas que lhes permitem assinar transações referentes a endereços públicos; tais transações são propagadas, validadas e agregadas em blocos, e a imutabilidade tende a ser econômica: quanto mais confirmações um bloco acumula, mais custoso se torna revertê-lo. Esse desenho favorece liquidação quase imediata, disponibilidade global e resiliência a pontos únicos de falha, ao custo de introduzir novos vetores de risco, como a perda irremediável de chaves, a exploração de vulnerabilidades em carteiras e contratos inteligentes, e dilemas de governança em ecossistemas abertos.

> “As ideias por trás da blockchain são, novamente, bastante antigas e remontam a um artigo de Haber e Stornetta, de 1991. A proposta deles era um método de carimbo de tempo seguro (timestamping) para documentos digitais, e não um esquema de moeda digital. O objetivo do carimbo de tempo é fornecer uma ideia aproximada de quando um documento passou a existir. Mais importante ainda, o carimbo de tempo transmite com precisão a ordem de criação desses documentos: se um surgiu antes do outro, os carimbos de tempo refletirão isso. A propriedade de segurança exige que o carimbo de tempo de um documento não possa ser alterado a posteriori.” (NARAYANAN et al., 2016, p.15, tradução nossa)

No plano jurídico-econômico, criptomoedas não se confundem com moeda de curso forçado emitida pelo Estado. Em termos civis, são bens incorpóreos passíveis de valoração econômica, cujo domínio decorre do controle exclusivo das chaves privadas. No ordenamento brasileiro, a Lei nº 14.478/2022 estabeleceu diretrizes para a prestação de serviços de ativos virtuais, delineando a figura do provedor de serviços de ativos virtuais (VASPs), e preservou o real como única moeda de curso legal. O Decreto nº 11.563/2023 atribuiu competências regulatórias ao Banco Central do Brasil sobre a supervisão de prestadores que se enquadrem, ao passo que a Comissão de Valores Mobiliários incide quando determinados tokens se amoldam ao conceito de valores

mobiliários, e a Receita Federal disciplina obrigações acessórias e aspectos tributários, a exemplo do reporte de operações com criptoativos previsto na IN RFB nº 1.888/2019.

Essa repartição evidencia que a natureza jurídica dos criptoativos é funcional e dependente do caso concreto: um mesmo ativo pode ensejar diferentes regimes conforme seu uso e as promessas econômicas e jurídicas veiculadas ao público.

Para fins analíticos, a literatura especializada adota uma classificação funcional que distingue, de um lado, tokens de pagamento, categoria essa na qual se situam as criptomoedas e, de outro, tokens de utilidade e tokens com traços de valores mobiliários (security tokens). Já as moedas digitais de banco central (CBDC) não se confundem com criptomoedas: embora possam empregar tecnologias de registro distribuído, são passivos do Banco Central, projetados dentro de um marco jurídico-público de política monetária e estabilidade financeira. A distinção, ainda que sutil em alguns aspectos técnicos, é decisiva para o enquadramento normativo e para a compreensão de impactos concorrenciais.

> “Uma CBDC é um instrumento de pagamento digital, denominado na unidade de conta nacional, que constitui um passivo direto do banco central.[1] Este relatório foca nas CBDCs de uso geral amplamente disponíveis (isto é, que podem ser usadas pelo público em pagamentos do dia a dia), em vez de CBDCs restritas a pagamentos de atacado em mercados financeiros.” (BIS, 2020, p. 3, tradução nossa).

No plano da infraestrutura de mercado, a experiência do usuário se dá em dois grandes modelos de custódia. No primeiro, de autocustódia (non-custodial), o titular mantém integralmente suas chaves privadas, maximizando soberania e resistência à censura, mas arcando com responsabilidades operacionais, como o gerenciamento seguro de frases-semente e dispositivos.

No segundo, de custódia por terceiros (custodial), um provedor como uma exchange ou custodiante regulado gerencia chaves em nome do cliente, simplificando a experiência e viabilizando recursos de recuperação de acesso, porém reintroduzindo riscos de contraparte e dependência de controles internos.

Essa malha de prestadores, somada a mercados P2P, mesas OTC e exchanges centralizadas e descentralizadas (DEX), compõe os principais pontos de entrada e saída entre o ecossistema cripto e o sistema financeiro tradicional, conhecidos como on-ramps e off-ramps.

Em termos de compliance e de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT), as propriedades das criptomoedas produzem efeitos ambivalentes. A transparência de dados em redes públicas habilita a análise forense on-chain, permitindo rastrear fluxos, identificar padrões comportamentais e mapear interações com serviços conhecidos; todavia, a pseudonimidade dos endereços, a desintermediação em certos casos de uso e a disponibilidade de técnicas de ofuscação como mixers[1], coinjoins[2], chain-hopping[3] e bridges inter-cadeias aumentam a dificuldade de vincular endereços a identidades civis sem a colaboração de prestadores e sem instrumentos de cooperação internacional.

Por isso, as prestadoras de serviços de ativos virtuais (VASPs), enquanto gatekeepers regulatórios, assumem papel central: políticas robustas de identificação e qualificação de clientes (Know Your Customer ou ‘‘Conheça Seu Cliente’’), monitoramento transacional com ferramentas especializadas, observância da “travel rule”[4] e reporte tempestivo de operações suspeitas são mecanismos decisivos para mitigar riscos e viabilizar medidas de congelamento e confisco, sobretudo quando os ativos e as evidências se encontram fragmentados por múltiplas jurisdições.

A terminologia do campo, por sua vez, permanece em evolução e nem sempre se apresenta de modo uniforme entre regimes jurídicos e comunidades técnicas. Termos como “criptoativo”, “ativo virtual”, “token”, “moeda virtual” e “moeda eletrônica” são empregados com sentidos parcialmente sobrepostos, o que recomenda precisão vocabular ao longo do trabalho.

---

[1] Serviços que recebem criptos de várias pessoas e devolvem valores “misturados”, trocando os vínculos visíveis entre quem enviou e quem recebeu.
[2] Técnica em que vários usuários combinam suas entradas numa única transação e recebem saídas de valores padronizados.
[3] Trocar rapidamente um criptoativo por outro e pular entre diferentes blockchains.
[4]Regra de compliance (do GAFI) que exige que prestadores de serviços de ativos virtuais (VASPs/exchanges) enviem junto com a transferência as informações mínimas do remetente e do destinatário. Pense como o “comprovante de dados” viajando com o dinheiro.

Para os efeitos desta pesquisa, adota-se o uso de “criptoativos” como gênero e “criptomoedas” como espécie, reservando-se “moeda eletrônica” ao conceito de Direito Financeiro aplicável a arranjos centralizados de pagamento e “CBDC” ao passivo digital do banco central. Esse recorte terminológico, além de coeso com a legislação nacional recente, previne confusões conceituais e fornece a base adequada para a análise dos efeitos regulatórios, tecnológicos e de cooperação internacional que serão explorados nos itens subsequentes.

1.2 Estrutura e funcionamento da tecnologia blockchain

A tecnologia blockchain pode ser descrita, em sua forma canônica, como um livro-razão distribuído que mantém um registro cronológico e encadeado de transações por meio de estruturas criptográficas, de modo a tornar economicamente custosa a alteração retroativa de dados e a dispensar um intermediário único de confiança. O núcleo dessa construção repousa em três camadas intimamente relacionadas: a camada de dados, que organiza transações em blocos encadeados por meio de funções hash e, em muitas implementações, árvores de Merkle[1] que sintetizam grandes conjuntos de transações em um único identificador; a camada de consenso, responsável por coordenar participantes não confiáveis a respeito de qual bloco será aceito como extensão legítima da cadeia; e a camada de rede, que propaga transações e blocos entre nós distribuídos com mecanismos de tolerância a falhas e latência variável (NAKAMOTO, 2008; NARAYANAN et al., 2016).

Na prática, cada bloco inclui um cabeçalho que referencia o hash do bloco anterior, metadados relevantes (como carimbo temporal e dificuldade) e o resumo criptográfico das transações ali contidas; esse “apontamento para trás” por hash cria uma cadeia em que a alteração de um bloco antigo exigiria recomputar todos os hashes subsequentes, o que, sob certas suposições de poder computacional ou de participação econômica, torna a manipulação retrospectiva impraticável do ponto de vista econômico.

---

[1] Estrutura de dados que resume um conjunto grande de informações usando hashes em formato de árvore. Cada “folha” é o hash de um item (ex.: uma transação); nós internos combinam hashes das folhas; no topo fica o Merkle root, um único hash que representa todo o conjunto.

O funcionamento cotidiano de uma blockchain pública pode ser compreendido a partir da trajetória de uma transação individual.

O usuário, de posse de uma chave privada, assina digitalmente a transação que movimenta unidades de valor associadas a seu endereço e a transmite à rede, onde ingressa em um “mempool” [1] mantido por nós validadores.

Esses nós verificam a validade formal e semântica da transação, formato correto, assinaturas válidas, inexistência de gasto duplo, saldo suficiente e, em seguida, a transação disputa inclusão em um bloco conforme uma lógica de mercado de taxas, já que, em ambientes de capacidade limitada, taxas mais elevadas tendem a priorizar a inclusão.

Uma vez montado e proposto, o bloco é disseminado pela rede e, se aceito por uma maioria econômica ou computacional de participantes, passa a integrar a cadeia principal, produzindo “confirmações” subsequentes à medida que novos blocos são acrescentados. Esse processo gera finalização probabilística: quanto mais blocos sucedem uma dada transação, menor a probabilidade de reorganizações que a revertam, embora diferentes implementações e camadas de consenso possam buscar finalização econômica forte ou determinística por meio de checkpoints e protocolos específicos.

O consenso, por sua vez, materializa-se por mecanismos como o proof-of-work (PoW) e o proof-of-stake (PoS), os quais, apesar de perseguirem o mesmo objetivo de ordenação compartilhada de transações, o fazem por incentivos e suposições de segurança distintas. No PoW, a produção de blocos exige a resolução de um problema criptográfico assimétrico que demanda custo computacional elevado, controlado por um parâmetro de dificuldade que se ajusta periodicamente para manter o intervalo médio de blocos. Essa exigência, ao amarrar segurança a dispêndio energético e a hardware especializado, desencoraja ataques, pois a tentativa de reescrever a cadeia em retrospecto requereria controlar parcela substancial do poder de hashing, com custos potencialmente proibitivos.

---

[1] É a “fila de espera” de cada nó da rede onde ficam as transações ainda não confirmadas. Cada nó mantém seu próprio mempool e os mineradores/validadores escolhem dali quais transações vão para o próximo bloco (geralmente pelas taxas mais altas).

No PoS, a produção e a validação de blocos são condicionadas ao “aporte” de participação econômica nativa que pode ser penalizada em caso de comportamento desonesto, desenhando uma matriz de incentivos na qual atacar a rede implica arriscar a perda de capital bloqueado. Em ambas as abordagens, a resiliência decorre de hipóteses sobre a honestidade majoritária do recurso escasso subjacente, poder computacional, no PoW, ou participação econômica, no PoS, e sobre a capacidade de a rede manter-se sincronizada dentro de limites práticos de latência.

A modelagem do estado e da transação varia conforme o protocolo. Em arquiteturas do tipo UTXO (unspent transaction outputs), como a do Bitcoin, as transações consomem “saídas não gastas” e produzem novas saídas, compondo um grafo de fluxos de valor em que cada saída é indivisível e somente pode ser totalmente consumida, com troco retornando ao emissor.

Esse modelo favorece verificações locais de saldo e facilita certas heurísticas forenses, mas exige composição específica de múltiplas entradas e saídas para representar pagamentos fracionados. Em arquiteturas baseadas em contas, como a do Ethereum, cada endereço mantém um saldo e um “nonce”[1] que impede reenvio de transações, e a execução de smart contracts se dá por uma máquina virtual que atualiza o estado global conforme regras determinísticas, consumo de recursos (gas) e limites de gastos computacionais por bloco.

A presença de contratos programáveis amplia o espaço de aplicações ao permitir a criação de tokens, a operação de exchanges descentralizadas, de mercados de crédito e de instrumentos complexos de governança, ao custo de introduzir novas superfícies de risco técnico e econômico.

Em ecossistemas programáveis, a questão da ordenação das transações ganha relevo pela possibilidade de extração de valor por agentes que controlam a inclusão e a ordenação, fenômeno conhecido como “maximal extractable value” (MEV).

---

[1] Valor no cabeçalho do bloco que os mineradores ficam alterando até que o hash do bloco fique abaixo do alvo de dificuldade.

Em linhas gerais, a ordem em que transações são postas em bloco pode afetar preços, liquidações e liquidez em protocolos de finanças descentralizadas, criando incentivos para reordenação estratégica que impõe custos a usuários e pode degradar a qualidade do mercado.

Soluções de mitigação incluem leilões de blocos, canais privados de transmissão de transações, mecanismos de comprometimento revelado e ajustamentos de protocolo para reduzir vantagens informacionais de proponentes de blocos, embora tais medidas impliquem trade-offs entre descentralização, eficiência e resistência à censura (NARAYANAN et al., 2016).

A escalabilidade constitui outro eixo central. Blockchains de primeira camada enfrentam limites de throughput[1] decorrentes de parâmetros de bloco e da necessidade de plena verificação por nós distribuídos. Para contornar essas restrições sem sacrificar a verificabilidade pública, proliferaram soluções de segunda camada, com desenhos distintos. Canais de pagamento, como na proposta do Lightning Network[2], deslocam a maior parte das interações para fora da cadeia, ancorando na camada base apenas estados iniciais e liquidações finais; rollups, por sua vez, acumulam transações em lotes cuja validade é provada por mecanismos criptográficos, provas de fraude em rollups otimistas ou provas de validade em rollups de conhecimento zero, publicando dados suficientes na camada base para permitir a reconstrução do estado e a saída segura de usuários mesmo na presença de operadores maliciosos.

Tais arranjos enfatizam o problema da disponibilidade de dados e a necessidade de garantir que informação suficiente permaneça acessível para verificação independente, sob pena de se reintroduzir confiança em operadores centralizados.

> “A blockchain do Bitcoin tem grande potencial para livros-razão distribuídos, mas, como plataforma de pagamentos, por si só, não conseguirá abranger o comércio mundial em um futuro próximo. A blockchain é um gossip protocol (protocolo de disseminação) pelo qual todas as modificações de estado do livro-razão são transmitidas a todos os participantes

[1] Capacidade de uma rede processar operações por tempo — ex.: “X transações por segundo (TPS)”.
[2] Rede de segunda camada do Bitcoin para pagamentos rápidos e baratos via canais; liquida só o saldo final na blockchain.

> A blockchain é um gossip protocol (protocolo de disseminação) pelo qual todas as modificações de estado do livro-razão são transmitidas a todos os participantes. É por meio desse ‘gossip protocol’ que se alcança o consenso sobre o estado — isto é, os saldos de todos. Se cada nó da rede Bitcoin precisar conhecer todas as transações que ocorrem globalmente, isso pode impor um arrasto significativo à capacidade da rede de abarcar todas as transações financeiras do mundo.” (POON; DRYJA, 2016, tradução nossa)

A partir dessa infraestrutura, compõem-se mercados de entrada e saída, exchanges centralizadas e descentralizadas, mesas OTC, provedores P2P, que conectam o ecossistema cripto ao sistema financeiro tradicional e servem de pontos de controle para políticas de identificação, monitoramento e reporte. Por isso, apesar de a blockchain oferecer transparência radical de dados em redes públicas, a efetivação de medidas de congelamento, confisco e rastreio, especialmente quando associadas à repressão à lavagem de dinheiro, passa não apenas pela perícia forense on-chain, mas também pela cooperação com prestadores e pela harmonização internacional de padrões de identificação.

Por fim, é importante ressaltar que blockchains públicas não são inerentemente anônimas, mas pseudônimas: endereços representam chaves e não identidades civis. A vinculação entre endereços e pessoas físicas ou jurídicas ocorre por agregação de sinais, como cadastros mantidos por prestadores, registros públicos, erros operacionais dos próprios usuários e padrões transacionais, de modo que a privacidade, quando desejada, depende de práticas operacionais consistentes e, em alguns casos, de protocolos especializados que empregam provas de conhecimento zero para ocultar remetente, destinatário e valores.

Esses mesmos mecanismos de privacidade, quando utilizados com propósitos ilícitos, impõem desafios adicionais às autoridades e reforçam a necessidade de cooperação célere entre jurisdições, padronização de pedidos de assistência e desenvolvimento de capacidades técnicas para interpretar evidências digitais sem violar garantias fundamentais. A arquitetura da blockchain, portanto, não é por si um antídoto nem uma ameaça definitiva à aplicação da lei; é uma infraestrutura neutra cujo efeito concreto sobre prevenção e repressão a ilícitos dependerá de escolhas de desenho de protocolo, de

incentivos econômicos e de arranjos institucionais que orbitam a camada de aplicação.

1.3 Conceito e fases da lavagem de dinheiro

A lavagem de dinheiro consiste no conjunto de atos orientados a ocultar ou dissimular a natureza, a origem, a localização, a disposição, a movimentação ou a propriedade de bens, direitos e valores provenientes de infração penal, de modo a reintroduzi-los no circuito econômico com aparência de licitude. No plano internacional, a noção se consolidou a partir da Convenção de Viena (1988), com posterior ampliação pela Convenção de Palermo (2000) e pela Convenção de Mérida (2003), que tornaram mais robustas as previsões sobre criminalização, confisco e cooperação.

As três convenções da ONU formam a espinha dorsal da cooperação penal transnacional contra a lavagem e crimes correlatos: a Convenção de Viena (1988), originada no combate ao tráfico de drogas, inaugurou a criminalização do branqueamento de capitais vinculado a entorpecentes e previu confisco e assistência jurídica mútua (v.g., arts. 3, 5 e 7); a Convenção de Palermo (2000) ampliou o alcance para o crime organizado transnacional, exigindo a tipificação da lavagem de dinheiro (art. 6), medidas de confisco (art. 12), extradição (art. 16) e um regime robusto de assistência mútua (art. 18); por fim, a Convenção de Mérida (2003), voltada à corrupção, consolidou a ideia de recuperação de ativos como princípio (cap. V, especialmente art. 51) e detalhou instrumentos de cooperação e medidas assecuratórias (p. ex., arts. 31, 43 e 46), servindo de base normativa para pedidos de bloqueio, sequestro e repatriação em casos que envolvam criptoativos.

No Brasil, a Lei nº 9.613/1998 estabeleceu um sistema de prevenção e repressão de caráter amplo, desvinculado de rol fechado de crimes antecedentes, e estruturado sobre obrigações de diligência e de reporte para setores sensíveis da economia, sob coordenação da Unidade de Inteligência Financeira (UIF/COAF), além de prever medidas assecuratórias e instrumentos especiais de investigação (ONU, 1988; 2000; 2003).

Ainda que o tipo penal descreva condutas de “ocultar” e “dissimular”, a dinâmica empírica da lavagem revela um processo, em geral fragmentado e

iterativo, que se vale de camadas sucessivas de transações, interposição de pessoas e estruturas jurídicas, arbitragens regulatórias e jurisdições de baixa cooperação, a fim de romper ou enfraquecer o nexo probatório entre o proveito do crime e seu titular efetivo.

A literatura clássica organiza esse processo em três fases, a colocação (placement), ocultação ou estratificação (layering) e integração (integration), alertando, contudo, que tais etapas não são estanques nem necessariamente lineares: podem ocorrer em paralelo, repetir-se, inverter-se ou mesmo serem dispensadas conforme a natureza do delito antecedente, os canais de movimentação e a tolerância a risco dos agentes envolvidos.

Conforme esclarece Gustavo Badaró, embora haja diferentes formas de denominação, esse modelo é amplamente aceito:

> Ainda que com variações terminológicas, costuma-se decompor o crime de lavagem de dinheiro em três fases comunicantes denominadas, segundo a tipologia proposta pelo GAFI, ocultação, dissimulação e integração. De modo muito simples, a primeira é aquela na qual se procura tornar os bens ilícitos menos visíveis; a segunda tem por objetivo distanciar o dinheiro de sua origem ilícita; e a terceira se dá quando se converte o capital ilícito em lícito. (BADARÓ, 2016, p. 76).

A colocação corresponde ao ingresso do produto do crime no sistema econômico formal enquanto a ocultação/estratificação refere-se à criação de camadas que dificultem a rastreabilidade por meio de sucessivas conversões, transferências e interposições. Já a integração representa a reapropriação do valor, já “purificado” aos olhos do mercado, por meio de recompras, investimentos legítimos, consumo ostensivo ou reciclagem em atividades empresariais. Em alguns relatos técnico-operacionais, menciona-se ainda uma etapa de “justificação” documental ou contábil, voltada a conferir narrativa plausível à disponibilidade de patrimônio, o que, embora não constitua fase autônoma na tipologia clássica, costuma aparecer como corolário da integração em contextos de fiscalização (NARAYANAN et al., 2016).

A transposição dessas fases ao ambiente dos criptoativos preserva a lógica funcional, mas altera meios e velocidades. Na colocação, observa-se a

conversão de numerário ou de ativos ilícitos em criptoativos por meio de on-ramps: aquisição direta em exchanges (com ou sem controles robustos de KYC), uso de mercados “P2P” e mesas OTC, emprego de terceiros interpostos (“laranjas”) e de contas de fachada, ou ainda a apropriação de criptoativos já produzidos por ilícitos cibernéticos — ataques a protocolos, phishing, ransomware, golpes de investimento e esquemas de pirâmide.

O objetivo é deslocar o valor para uma representação digital cuja circulação transnacional é instantânea, com custos de transferência baixos e pseudonimidade por design, o que torna, desde logo, a qualidade dos controles de entrada (identificação, verificação e restrições de risco) uma variável crítica para a mitigação (FATF, 2023; RFB, 2019).

> “As jurisdições avançaram de forma insuficiente na implementação da Travel Rule, deixando os ativos virtuais (VAs) e os provedores de serviços de ativos virtuais (VASPs) vulneráveis a usos indevidos.” (FATF, 2023, p. 3–4, 18, 21, tradução nossa)
>
> IN 1.888/2019 instituiu a obrigatoriedade de prestação de informações sobre operações com criptoativos; para operações no exterior ou fora de exchange, o declarante é PF/PJ residente quando ultrapassar R$ 30.000/mês (p. 1, 3); as informações dos titulares incluem nome, endereço, CPF/CNPJ ou NIF. (RFB, 2019, p. 1, 3, 7)

Na ocultação/estratificação, multiplicam-se técnicas destinadas a fragmentar trilhas e a confundir a análise forense. São recorrentes as cadeias de “peel” (liberação paulatina de pequenas quantias a partir de um grande saldo), as transferências em cascata entre centenas de endereços controlados por um mesmo agente, o uso de mixers e coinjoins para embaralhar entradas e saídas, a passagem por bridges e swaps inter-cadeias (o chamado chain-hopping), a conversão para moedas com foco em privacidade e a circulação por DEX de alta liquidez.

Em ambientes programáveis, contratos inteligentes permitem roteamentos sofisticados e a composição de estratégias com múltiplos estágios em blocos consecutivos, explorando janelas de tempo curtas, arbitragem e diferenças de políticas de monitoramento entre provedores. Em paralelo, surgem

“camadas off-chain” de dissimulação, como o uso de provedores de hospedagem, VPNs e simulações de geolocalização que tentam enganar filtros de IP, além de redes de mulas financeiras para distribuir recebimentos em contas bancárias espalhadas por diferentes países.

A contrapartida é que a transparência das redes públicas, se combinada com heurísticas robustas (agrupamento de endereços por co-gasto, detecção de endereços de troco, identificação de serviços conhecidos, análise de timing e de padrões de taxa), muitas vezes permite reconstruir fluxos com alto grau de confiança, notadamente quando se obtém, por meios legais, dados cadastrais e de acesso mantidos por prestadores.

> “Considere novamente o exemplo da venda de um carro. Se a ‘cor’ de objetos do mundo real (no sentido de colored coins/‘moedas coloridas’) for conhecida, qualquer pessoa pode examinar a blockchain para ver quando ocorreu a venda de um carro e quanto foi pago por ele, sem necessariamente saber as identidades do comprador e do vendedor. Isso pode ser útil em algumas circunstâncias, e a ‘cor’ pode ser mantida privada quando for prejudicial.” (NARAYANAN et al., 2016, p.297, tradução nossa)

A integração no ecossistema cripto se dá, tipicamente, por off-ramps para moeda fiduciária e por conversões econômicas que conferem aparência lícita aos valores. O repertório inclui saques via exchanges para contas bancárias do próprio agente ou de interpostos; liquidação em mesas OTC com pagamento em espécie; uso de cartões vinculados a cripto emitidos por provedores de pagamento; compras de alto valor (bens duráveis, joias, veículos) com posterior revenda; alongamento de posição em stablecoins como “reserva” com menor volatilidade; e reciclagem empresarial, em que recursos são canalizados a sociedades controladas direta ou indiretamente pelo beneficiário para capitalizar operações ou simular receitas.

Em cenários digitais, também se observam tentativas de integração por meio de jogos, apostas e plataformas de conteúdo, em que micropagamentos e programas de afiliados produzem lastros contábeis para ingressos de difícil

qualificação, exigindo do analista uma leitura integrada de on-chain e off-chain, com atenção a incongruências de perfil, capacidade contributiva e declarações fiscais.

Sob a ótica de prevenção (PLD/FT), as três fases se conectam a pontos de controle distintos e complementares. Na colocação, destacam-se políticas de KYC/KYB consistentes, validação documental com prova de vida e verificação de vínculo bancário, monitoramento de on-ramps com score de risco por origem de recursos e, quando cabível, limites graduais por perfil.

Na estratificação, a chave é o KYT com ferramentas de análise on-chain que identifiquem exposição a tipologias de risco (mixers, serviços ilícitos, moedas de privacidade, bridges de alto risco), variações abruptas de comportamento, chain-hopping acelerado e padrões de valor incompatíveis com a renda declarada ou com o histórico da conta.

Na integração, ganham relevância os relatórios de operações suspeitas à UIF/COAF, a comunicação tempestiva a autoridades competentes, os congelamentos na origem e a coordenação com outros prestadores para evitar a dissipação dos ativos, com documentação de cadeia de custódia e as cautelas probatórias exigidas.

Em todos os estágios, convém evitar a automatização cega: as heurísticas forenses aumentam a eficiência, mas não substituem o juízo crítico e a necessidade de corroboração por evidências externas (registros de acesso, contratos, comunicações, logs de API, dados bancários e fiscais), sob pena de falsos positivos e de violações a garantias fundamentais.

Do ponto de vista investigativo e processual, a velocidade e a transnacionalidade dos fluxos digitais exigem cooperação jurídica internacional para acesso a dados de clientes, registros de transações internas, endereços IP, logs de autenticação e eventual bloqueio de ativos sob guarda de VASPs sediados no exterior. Na prática, pedidos de assistência mútua (MLATs), cartas rogatórias e canais de inteligência financeira podem ser decisivos para romper a pseudonimidade, desde que observados requisitos de necessidade, adequação e proporcionalidade, com fundamentação concreta e delimitação de escopo.

Por outro lado, medidas intrusivas, como a quebra de sigilo bancário/telemático ou a apreensão de dispositivos, devem demonstrar pertinência temática e subsidiariedade, especialmente quando a mesma finalidade pode ser atingida por meios menos restritivos, como o compartilhamento de registros mantidos por prestadores sujeitos a regulação.

Finalmente, uma vez apreendidos criptoativos, a gestão segura, geração de carteiras de custódia institucional, procedimentos de múltiplas assinaturas, segregação por caso e logs imutáveis, integra-se o dever de preservação da prova e de proteção do valor público (NARAYANAN et al., 2016).

Em síntese, as fases da lavagem continuam a oferecer um mapa funcional útil, mas sua aplicação a criptoativos exige lentes técnicas e institucionais específicas: compreender como se dá a colocação em on-ramps de risco heterogêneo, como a estratificação explora a combinatória de mixers, DEX, bridges e moedas de privacidade, e como a integração se materializa em off-ramps, bens reais e estruturas empresariais.

É esse pano de fundo que justifica, no capítulo seguinte, a análise dos fundamentos e instrumentos da cooperação internacional, com ênfase na harmonização regulatória, no papel do GAFI, na rede de UIFs e nos mecanismos multilaterais e bilaterais que tornam viável a resposta estatal a um fenômeno intrinsecamente transfronteiriço.

1.4 Cooperação internacional: fundamentos e tratados principais

A cooperação jurídica internacional (CJI), em matéria penal e administrativa sancionadora, constitui resposta estrutural ao caráter transnacional da lavagem de dinheiro com criptoativos, cuja circulação veloz e fragmentada por múltiplas jurisdições exige coordenação normativa, canais formais de assistência e rotas de inteligência financeira.

Nesse plano, as Recomendações do Grupo de Ação Financeira (GAFI) consolidam um padrão internacional que articula, de um lado, a adesão e a aplicação efetiva de convenções multilaterais centrais e, de outro, a obrigação de prover a “mais ampla assistência jurídica possível” em investigações e processos por lavagem, delitos antecedentes e financiamento do terrorismo, com

desenho institucional claro, inclusive por meio de autoridade central para recepção e tramitação de pedidos e processos de priorização e execução célere.

> Os países e instituições financeiras deveriam identificar e avaliar os riscos de lavagem de dinheiro e financiamento do terrorismo que possam surgir em relação a: (a) desenvolvimento de novos produtos e práticas de negócios, inclusive novos mecanismos de entrega; e (b) o uso de novas tecnologias ou em desenvolvimento para produtos novos ou já existentes. No caso de instituições financeiras, tal avaliação de riscos deveria ocorrer antes do lançamento desses novos produtos, práticas de negócios ou do uso de novas tecnologias ou em desenvolvimento. As instituições deveriam adotar medidas apropriadas para gerenciar ou mitigar tais riscos.(GAFI, 2012, p. 14).

Esse mesmo marco ressalta que o segredo financeiro não pode ser fundamento autônomo de negativa de auxílio, que o foco da dupla tipicidade deve recair sobre a conduta subjacente e que, quando cabível, a assistência deve ser prestada até mesmo na ausência de dupla incriminação, se não houver medidas coercitivas envolvidas.

No eixo dos instrumentos multilaterais, avulta a tríade convencional das Nações Unidas: a Convenção de Viena (1988), a Convenção de Palermo (2000) e a Convenção de Mérida (2003). Elas proveram, em sequência, a base para criminalização da lavagem, medidas de confisco e recuperação de ativos, assistência jurídica mútua e cooperação policial e judicial, hoje incorporadas como “capítulo de cooperação internacional” no padrão GAFI, ao lado de outros instrumentos relevantes, como a Convenção para a Supressão do Financiamento do Terrorismo (1999) e a Convenção do Conselho da Europa sobre o Cibercrime (Budapeste, 2001).

Nesse espectro temático, a Convenção de Viena influenciou debates específicos sobre confisco proporcional em casos de mescla de valores lícitos e ilícitos, ao admitir a apreensão até o limite do produto criminoso efetivamente misturado, solução que evita “contaminação integral” de patrimônios quando a

prova só demonstra a presença parcial de valores ilícitos em contas ou bens agregados.

Para o domínio dos criptoativos, duas frentes merecem destaque. Primeiro, a de tipificação e alcance material: a própria Convenção de Palermo oferece noção ampla de “bens” como ativos de qualquer tipo, corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis, e documentos/instrumentos que atestem propriedade ou direitos, formulação que se ajusta à natureza jurídico-econômica dos criptoativos como bens incorpóreos passíveis de valoração.

Segundo a de cooperação cibernética: a Convenção de Budapeste, primeiro tratado internacional específico sobre criminalidade informática, estabeleceu harmonização tipológica, técnicas investigativas e parâmetros de cooperação entre signatários, reconhecendo a necessidade de fluxos rápidos de dados em delitos que atravessam redes e países. Embora o Brasil tenha sido historicamente não-signatário, o debate interno sobre adesão e internalização do tratado ganhou impulso institucional, justamente pelos ganhos em capacidade probatória e interoperabilidade com autoridades estrangeiras.

Em termos operacionais, a CJI realiza-se por múltiplas vias: assistência jurídica mútua (MLATs), cartas rogatórias, extradição, transferência de procedimentos, reconhecimento e execução de decisões estrangeiras, além de canais informais de inteligência financeira. O padrão GAFI enfatiza que países devem organizar processos claros para priorizar e executar pedidos, com autoridade central capaz de garantir confidencialidade, rastreabilidade e prazos adequados, ao mesmo tempo em que previnem negativas baseadas apenas em matéria fiscal ou em segredo financeiro, e privilegiam o exame da conduta como critério de dupla tipicidade.

Nessa arquitetura, a existência de redes como a das Unidades de Inteligência Financeira (UIFs) e arranjos de partilha de informações complementam os caminhos convencionais, permitindo que evidências técnicas (registros de acesso, dados de carteira custodiada, logs de API, IPs de autenticação) alimentem rapidamente pedidos formais de prova e medidas assecuratórias, inclusive de congelamento e confisco.

A literatura do próprio projeto, ademais, sublinha que a cooperação deve ser acompanhada de harmonização normativa, capacitação técnica e infraestrutura para inteligência compartilhada, premissas particularmente sensíveis quando se lida com ativos digitais programáveis e passíveis de “chain-hopping” em minutos.

O resultado é um padrão de convergência: adesão a convenções-chave, incorporação efetiva de dispositivos de confisco e recuperação de ativos, desenho de autoridades centrais funcionais e cooperação célere com foco em condutas, não em rótulos, tudo sustentado por processos internos de PLD/FT alinhados às Recomendações do GAFI. Essa malha normativa e institucional, que inclui, além das convenções da ONU, tratados setoriais como Budapeste, é reiterada nos materiais do seu projeto como requisito para eficácia diante de ameaças em rápida evolução, inclusive no ecossistema cripto.

CAPÍTULO 2 – LAVAGEM DE DINHEIRO POR MEIO DE CRIPTOMOEDAS

Aqui examinamos, de forma aplicada, como a lavagem de dinheiro se operacionaliza no ecossistema de criptoativos. O capítulo descreve as técnicas de ocultação digital (mixers/coinjoin, chain-hopping, bridges inter-cadeias e riscos de data availability em rollups), mapeia atores e estruturas que viabilizam a estratificação (VASPs, OTC/P2P, ATMs, emissores de stablecoins, DEX/DeFi com captura de taxas e front-ends), e reconstrói casos práticos e operações que evidenciam padrões recorrentes e pontos de controle. A partir desses elementos, avaliam-se os riscos regulatórios e impactos transnacionais, destacando como assimetrias de supervisão, lacunas de travel rule e diferenças de cooperação internacional condicionam a efetividade de prevenção, investigação, bloqueio e recuperação de ativos.

2.1 Ferramentas e técnicas de ocultação digital

A dinâmica de ocultação em criptoativos parte de uma tensão estrutural: blockchains públicas oferecem transparência radical de dados, mas não embutem identidade civil nos endereços, operando sob um regime de pseudonimidade. Essa dissociação permite que agentes tentem “colocar distância” entre o valor e o seu beneficiário final por meio de trilhas encadeadas, enquanto a própria transparência, quando combinada a heurísticas on-chain e a dados fora da cadeia, habilita a reconstituição de fluxos por analistas e autoridades.

> “As identidades no Bitcoin são, portanto, pseudoanônimas: ainda que não estejam explicitamente vinculadas a indivíduos ou organizações do mundo real, todas as transações são completamente transparentes.” (MEIKLEJOHN et al., 2013)

Na prática, o processo começa com a compreensão de que co-gastos, endereços de troco, padrões temporais e rótulos de serviços funcionam como sinais probabilísticos; cruzados com cadastros, IPs, logs de autenticação e registros de API mantidos por prestadores, esses sinais convertem a pseudonimidade em identificabilidade suficiente para finalidades de compliance e prova, desde que observadas as garantias legais aplicáveis.

Entre as técnicas mais conhecidas para elevar a opacidade estão os misturadores e os arranjos de coinjoin. Misturadores custodiais recebem depósitos e redistribuem valores a partir de pools internas, muitas vezes com atrasos e padronizações que tentam desfazer inferências de vinculação entre entradas e saídas; por operarem a custódia, tendem a se enquadrar como provedores de serviços de ativos virtuais, atraindo obrigações de KYC, “travel rule” e reporte tempestivo de operações suspeitas, conforme as Recomendações do GAFI.

O coinjoin, por seu turno, reúne múltiplos usuários em uma mesma transação de N entradas para N saídas com valores idênticos, reduzindo a força de heurísticas de troco; sua efetividade, porém, depende do tamanho do conjunto de anonimato e da disciplina operacional posterior, pois o comportamento subsequente pode “quebrar” o disfarce.

Em paralelo, cadeias de “peel”, que se trata de escoamento granular de pequenas frações a partir de um saldo volumoso ao longo de muitas transações, procuram diluir a saliência de saques relevantes e encarecer o congelamento coordenado em diversos pontos de contato; ferramentas analíticas detectam esses padrões, mas a fragmentação aumenta custos de triagem e de pedidos de assistência internacional (NARAYANAN et al., 2016).

Ganha relevância, também, o chamado chain-hopping, a troca sucessiva entre ativos e redes distintas, que fragmenta a trilha e explora heterogeneidades de monitoramento e de governança. Essa prática pode envolver swaps atômicos não custodiados, que permitem conversões diretas entre pares, e bridges inter-cadeias, em que ativos são bloqueados numa rede e representados noutra por “wrapped tokens”. Falhas de custódia, de governança ou de auditoria nessas pontes já geraram volumes expressivos de fundos ilícitos a circular; do ponto de vista regulatório e de risco, respostas eficazes combinam due diligence sobre a exposição a pontes e ativos de alto risco, listas de observação dinâmicas, oráculos de compliance e monitoramento inter-cadeia com indicadores calibrados (WOOD, 2014).

Outra fonte importante de opacidade são as exchanges descentralizadas e as finanças descentralizadas. Ao permitir trocas não custodiadas, empréstimos

colateralizados e estratégias programáveis com formadores automatizados de mercado, agregadores e roteadores que fracionam ordens por múltiplas pools, o ecossistema DeFi viabiliza estratificação acelerada em janelas temporais muito curtas. Não há um único intermediário passível de ser compelido a bloquear preventivamente a execução, mas todo o fluxo é público, o que desloca a ênfase para análise on-chain em nível de contrato e pool, para políticas de exposição a protocolos e para gatilhos automatizados de mitigação que reajam a padrões de risco previamente definidos (ANTONOPOULOS, 2017; NARAYANAN et al., 2016).

Nesse mesmo contexto, fenômenos como extração máxima de valor (MEV) e reordenação de transações por proponentes de blocos podem interferir na previsibilidade de rotas, criando condições propícias a roteamentos oportunistas e a composições de curto prazo que degradam a visibilidade estatística do percurso.

Criptoativos voltados à privacidade empregam técnicas criptográficas próprias, como stealth addresses, assinaturas em anel, saídas confidenciais e provas de conhecimento zero, para ocultar remetentes, destinatários e valores, reforçando a proteção a dados legítima, mas também elevando a dificuldade investigativa quando combinados a lacunas regulatórias. O consenso regulatório recente tem sido o de calibrar políticas por risco, evitando proibições amplas que empurrem o uso para ambientes totalmente opacos e inibam colaborações institucionais, e privilegiando a integração de metadados periféricos, análise comportamental e foco em pontos de entrada e saída, onde controles de KYC/KYB e de “travel rule” podem operar com maior efetividade.

Nem toda ofuscação é on-chain: fora da cadeia, agentes recorrem a VPN/Tor, hospedagem resiliente, compartimentalização de dispositivos, camadas operacionais com “mulas financeiras” no on/off-ramp bancário e a justificativas documentais simuladas por meio de empresas de fachada. Esse pano de fundo exige abordagem probatória integrada, em que logs de API, IPs, carimbos de tempo e cadastros mantidos por prestadores são combinados a dados bancários e fiscais, sempre sob os parâmetros de necessidade, adequação e proporcionalidade, e frequentemente com apoio de cooperação

jurídica internacional para acesso e congelamento de valores sob guarda de VASPs estrangeiros.

O mesmo raciocínio se aplica a vetores menos convencionais, como a tokenização de itens digitais e os ambientes de jogos e apostas, que viabilizam “micro-lavagem” e “wash trading” por meio de simulações entre identidades coordenadas; nesses cenários, a correlação entre endereços, padrões de lance, horários, vínculos de custódia e clusters econômicos costuma ser mais informativa do que a análise isolada de transações.

Infraestruturas físicas e de balcão, como cripto-ATMs e mesas OTC, completam o quadro. Em ambientes de baixa supervisão, podem tornar-se pontos de colocação e integração com diligência deficiente; em mercados regulados, funcionam como gatekeepers relevantes para congelamentos e reporte, desde que operem controles robustos de identificação, verificação de vínculo bancário e monitoramento transacional, com segmentação de risco e limites compatíveis com perfis.

Em síntese, a caixa de ferramentas de ocultação combina pseudonimidade estrutural, técnicas de embaralhamento e fragmentação, composições programáveis e camadas off-chain que “explicam” fluxos perante o mundo bancário e fiscal; a contrapartida institucional eficaz combina KYC/KYB sólido, KYT com indicadores específicos para mixers, moedas de privacidade, bridges e DEX, observância da “travel rule”, reporte tempestivo à UIF/COAF e o uso de canais de inteligência e de assistência mútua para romper assimetrias temporais entre a velocidade das transações digitais e os prazos de resposta do aparato estatal.

2.2 Atores e estruturas envolvidas

A lavagem de dinheiro por meio de criptoativos mobiliza um ecossistema heterogêneo de agentes e arranjos operacionais que, combinados, permitem transformar proveitos ilícitos em valores com aparência de licitude. No núcleo estão os beneficiários finais, indivíduos ou organizações que derivam receitas de infrações penais e seus operadores, responsáveis por desenhar e executar a engenharia financeira necessária à colocação, estratificação e integração dos recursos.

Em torno desse núcleo gravita uma constelação de facilitadores com perfis distintos: corretores P2P e mesas OTC que oferecem liquidez e discrição na conversão entre moeda fiduciária e cripto; intermediários informais que alugam contas bancárias e perfis verificados em exchanges; consultores tecnológicos e provedores de “lavagem como serviço” que programam roteiros on-chain complexos e automatizados; e redes de “mulas” encarregadas de pulverizar ingressos e resgates, tanto no sistema bancário tradicional quanto em prestadores de pagamento.

No plano da infraestrutura cripto propriamente dita, destacam-se as exchanges centralizadas (com diferentes níveis de governança e conformidade), os custodiantes que administram chaves privadas em nome de clientes, as exchanges descentralizadas e os protocolos DeFi que viabilizam conversões e alavancagem sem custódia, os mixers/coinjoins que elevam a opacidade de trilhas, as bridges que conectam cadeias e tornam trivial o chain-hopping, e as emissoras de stablecoins, cujo papel como “reserva de valor” de baixa volatilidade costuma viabilizar a conservação dos ganhos até que surjam oportunidades de integração. A depender da tipologia, mineradores/validadores também podem desempenhar papel relevante, seja ao aceitar transações com taxas elevadas para acelerar a confirmação de roteiros de estratificação, seja ao operar nós em jurisdições com baixa cooperação, embora, em regra, atuem como participantes neutros de infraestrutura (NARAYANAN et al., 2016).

Do lado institucional, o conjunto de gatekeepers regulatórios previsto em padrões internacionais e no ordenamento brasileiro define os pontos de controle para identificação, monitoramento e reporte. A Lei nº 14.478/2022 delineia o provedor de serviços de ativos virtuais e abriu caminho para a supervisão setorial no Brasil, complementada pelo Decreto nº 11.563/2023, que atribuiu competências ao Banco Central do Brasil para regular e fiscalizar prestadores enquadrados, sem prejuízo da atuação da Comissão de Valores Mobiliários quando determinados tokens ostentam características de valores mobiliários e da Receita Federal do Brasil quanto às obrigações acessórias e ao reporte de operações com cripto (IN RFB nº 1.888/2019.

A arquitetura de PLD/FT coordenada pela Lei nº 9.613/1998 segue estruturando deveres de diligência e comunicação ao sistema de inteligência

financeira (UIF/COAF), essa mesma lei, em seu artigo 9º, traz um rol de agentes que se sujeitam às obrigações de identificação de clientes e manutenção de registros, bem como de comunicação (arts. 10 e 11). Enquanto instituições financeiras, instituições de pagamento e correspondentes bancários seguem sendo pontos críticos de on/off-ramp, devendo calibrar KYC/KYB, monitoramento transacional (KYT) e “travel rule” em linha com as Recomendações do GAFI.

> “A atualização mostra que as jurisdições continuam enfrentando dificuldades para implementar os requisitos fundamentais desta Recomendação. Com base em 98 relatórios de avaliação mútua e de acompanhamento do GAFI, 75% das jurisdições estão apenas parcialmente em conformidade ou não estão em conformidade com as exigências do GAFI. Também há progresso insuficiente na implementação da ‘travel rule’, um requisito-chave do GAFI para proteger contra os riscos de LD/FT/FP (lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação) associados aos ativos virtuais. Mais da metade das jurisdições que responderam à Pesquisa de 2023 do GAFI ainda não havia tomado qualquer medida para implementar a ‘travel rule’.” (FATF, 2023, p.28)

No âmbito da cooperação, a atuação coordenada de autoridades centrais para assistência mútua, do Ministério Público, da Polícia Federal e de agências estrangeiras (FIUs, unidades de cibercrime, autoridades reguladoras e de persecução) é indispensável para romper a pseudonimidade e obter dados sob custódia de prestadores sediados fora do país, inclusive quando se discute congelamento/apreensão e posterior confisco. Também integram a malha de atores as empresas de análise forense on-chain, que produzem inteligência a partir de rotulagem de serviços, clusters econômicos e heurísticas de fluxo; embora privadas, tornam-se peças recorrentes no suporte a investigações públicas e a programas de compliance de VASPs e instituições financeiras.

No nível das estruturas jurídicas e organizacionais, a lavagem com criptoassets reatualiza ferramentas clássicas e incorpora arranjos nativamente digitais. Sociedades de fachada e interpostas pessoas continuam essenciais para “explicar” ingressos e patrimônio perante o fisco e o sistema bancário, funcionando como veículos para capitalização de negócios simulados, emissão

de notas frias, criação de folhas de pagamento artificiais e circulação de empréstimos e dividendos com aparência regular.

Estruturas societárias em cadeia, com camadas em diferentes jurisdições, são utilizadas para deslocar o centro de gravidade regulatório e reduzir o risco de medidas cautelares, ao passo que contas bancárias e perfis de exchange alugados conferem ao operador um estoque de identidades e acessos alternativos que ajudam a contornar travas de diligência e limites transacionais.

No plano cripto, carteiras de autocustódia segmentadas, arranjos de multiassinatura e esquemas de MPC (computação multipartidária) compõem uma camada operacional voltada à continuidade e à resiliência, mitigando riscos de apreensão física de dispositivos ou de "ponto único de falha".

Em ecossistemas programáveis, DAOs e contratos inteligentes podem ser instrumentalizados como "casca" para captação de recursos ou circulação de valores com governança difusa, criando zonas cinzentas de responsabilização quando não há indicação clara de beneficiários e controladores; de igual modo, a infraestrutura DeFi permite arquiteturas de alavancagem, colateralização e roteamento que, combinadas a agregadores e roteadores, resultam em trajetórias de difícil segmentação temporal, especialmente quando encadeadas com flash loans[1] e reordenação de transações (MEV).

A essas estruturas somam-se os arranjos híbridos, nos quais "front businesses" sustentam fluxo de caixa que lastreia ingressos digitais, e circuitos OTC com operadores regionais conectados por confiança pessoal e liquidez em múltiplas moedas, nos quais a precificação reflete risco de exposição, volatilidade e velocidade de rotação de estoques de cripto e numerário.

O retrato não se completa sem a perspectiva de riscos assimétricos entre jurisdições.

---

[1]São empréstimos sem garantia feitos em DeFi que nascem e são quitados dentro da mesma transação. Se, ao final da transação, o valor + a taxa que forem devolvidos, tudo é automaticamente revertido (nada acontece).

Atores maliciosos tendem a arbitrar diferenças de supervisão entrando por prestadores com controles fracos, pulverizando em ambientes DeFi e saindo por canais com integração bancária em países de alta liquidez, muitas vezes aproveitando janelas de tempo entre o acionamento do monitoramento e a execução de medidas assecuratórias.

É nesse ponto que a convergência regulatória, a padronização de formulários de assistência mútua, a existência de pontos de contato 24/7 e a integração entre UIFs e autoridades centrais fazem diferença prática, reduzindo o hiato temporal entre identificação de tipologias de risco e bloqueio eficaz de ativos. Em ambos os lados, tanto preventivo quanto repressivo, o papel de compliance officers e equipes de resposta a incidentes dentro de VASPs e

Instituições financeiras é decisivo para transformar alertas em ações coordenadas, com documentação de cadeia de custódia, governança de chaves em apreensões e segregação por caso, de modo a preservar valor e prova sem violar garantias processuais.

Em síntese, a lavagem com cripto não é um “truque” de um só ator, mas a combinação de pessoas, plataformas e estruturas que espelham a economia digital contemporânea; o enfrentamento eficaz requer ativar, do lado lícito, a mesma integração entre tecnologia, governança e cooperação jurídica que os agentes ilícitos exploram do lado oposto.

2.3 Casos práticos e operações internacionais relevantes

A observação de casos concretos confirma que a lavagem por criptoativos é, antes de tudo, um fenômeno transnacional que explora assimetrias regulatórias, heterogeneidades tecnológicas e janelas de tempo entre o monitoramento privado e a resposta estatal. A queda do Hydra Market, em 2022, ilustra como cooperação policial e judiciária, que combinando investigação americana com execução alemã conseguiu desarticular um hub que, ao longo de anos, canalizava pagamentos em cripto para uma miríade de ilícitos, praticando serviços acoplados de “cash-out” e “mixing”.

O confisco de infraestrutura e a apreensão de grandes quantidades de criptoativos revelaram, em escala, a interdependência entre mercados ilícitos, provedores de ofuscação e on/off-ramps com diligência deficiente (DOJ, 2022).

Na mesma direção, a operação europeia contra o ChipMixer (2023) expôs a centralidade de misturadores custodiais na fase de estratificação: ao bloquear servidores, apreender chaves e mapear fluxos, autoridades conseguiram correlacionar depósitos e saídas com clusters de risco e serviços conhecidos, apontando o papel desses provedores como “ponte” entre crimes cibernéticos e o sistema financeiro tradicional Explica

> “ChipMixer, um mixer de criptomoedas não licenciado criado em meados de 2017, era especializado em misturar ou cortar trilhas relacionadas a ativos de moeda virtual. O software do ChipMixer bloqueava a trilha na blockchain dos recursos, tornando-o atraente para cibercriminosos que buscavam lavar proventos ilícitos de atividades criminosas como tráfico de drogas, tráfico de armas, ataques de ransomware e fraude com cartões de pagamento. Os valores depositados eram convertidos em ‘chips’ (pequenos tokens de valor equivalente), que então eram misturados entre si, e, anonimizando, assim, todas as trilhas que levavam à origem dos recursos.” (EUROPOL, 2023, tradução nossa).

As medidas contra a Bitzlato (2023), plataforma acusada de permitir movimentações com frágil diligência e exposição a mercados ilícitos, adicionam a dimensão regulatória e sancionatória à resposta penal, salientando que prestadores que operam sem controles compatíveis com padrões internacionais atraem, além de risco reputacional, responsabilização por facilitarem a lavagem em larga escala (DOJ, 2023).

No mesmo ciclo de enforcement, o acordo global envolvendo Binance/Changpeng Zhao (2023), com componentes penais e administrativos, marcou a consolidação de um “padrão de expectativas” para VASPs sistêmicos: políticas robustas de KYC/KYB, monitoramento sensível a tipologias cripto (mixers, moedas de privacidade, chain-hopping/bridges, exposição a sancionados), governança de sanções e capacidade de resposta a autoridades.

Ainda que a finalidade primária desses casos seja sancionatória, o resultado prático é a elevação do piso regulatório para gatekeepers globais.

> “A Binance Holdings Limited (Binance), a entidade que opera a maior corretora de criptomoedas do mundo, a Binance.com, declarou-se culpada hoje e concordou em pagar mais de US$ 4 bilhões para encerrar a investigação do Departamento de Justiça sobre violações relacionadas à Lei de Sigilo Bancário (BSA), à falta de registro como empresa de transmissão de dinheiro e à Lei de Poderes Econômicos de Emergência Internacional (IEEPA).” (DOJ; Treasury; CFTC, 2023).

Todos esses casos envolvendo ferramentas orientadas à privacidade mostram a tensão entre proteção de dados legítima e opacidade para fins ilícitos. As sanções da OFAC ao Tornado Cash (2022) e litígios associados, bem como investigações criminais em torno de carteiras com funcionalidades de coinjoin e roteamento ofuscado, como no procedimento contra os desenvolvedores da Samourai Wallet (2024), evidenciam o debate sobre o alcance da responsabilidade de criadores/operadores, a distinção entre código e serviço, e o dever de mitigação de riscos quando há governança e benefícios econômicos capturáveis.

Atuação do Departamento do Tesouro:

> “O Departamento do Tesouro vem atuando para expor componentes do ecossistema de moedas virtuais, como Tornado Cash e Blender.io, que cibercriminosos utilizam para ofuscar os proventos de atividades cibernéticas ilícitas e outros crimes. Embora a maior parte da atividade com moedas virtuais seja lícita, elas podem ser usadas de forma ilícita, inclusive para evasão de sanções por meio de mixers, corretores P2P, mercados da dark web e exchanges. Isso inclui a facilitação de roubos, esquemas de ransomware, fraudes e outros crimes cibernéticos.” (OFAC,2022, tradução nossa)

Atuação do Departamento de Justiça:

> “Federal Bureau of Investigation (“FBI”), anunciou hoje o levantamento do sigilo de uma acusação formal (indictment) contra KEONNE RODRIGUEZ, diretor-executivo e cofundador da Samourai Wallet (“Samourai”),

> e WILLIAM LONERGAN HILL, diretor de tecnologia e também cofundador da Samourai, por conspiração para cometer lavagem de dinheiro e conspiração para operar empresa de transmissão de valores sem licença.”(DOJ, 2024, tradução nossa)

Ainda que os desfechos variem caso a caso, o ponto comum é a leitura funcional: quando há intermediação material, controle de chaves, taxas, interfaces de front-end e suporte operacional, cresce a expectativa de medidas de compliance proporcionais ao risco, especialmente se a ferramenta se converte em rota preferencial para valores vinculados a atores sancionados ou a crimes de alto impacto.

A dimensão cibernética e geopolítica aparece com nitidez nas investigações sobre o grupo Lazarus e ataques a bridges e protocolos, como o comprometimento do Ronin Bridge (2022). A triagem inicial, que ocorre com rotulagem de clusters e endereços, evoluiu para uma corrida de arbitragem e chain-hopping com uso de mixers e serviços descentralizados, exigindo respostas sincronizadas de VASPs globais, acionamento de canais de UIFs e, por vezes, congelamentos coordenados em janelas de tempo muito curtas.

Esses episódios enfatizam dois aprendizados operacionais: primeiro, a necessidade de KYT inter-cadeia (capaz de correlacionar exposições em L1/L2, bridges e wrapped tokens); segundo, a importância de pontos de contato 24/7 e playbooks previamente acordados para pedidos de bloqueio e preservação de evidências (FATF, 2023; Treasury, 2022).

Casos com recorte mais “tradicional” também oferecem lições úteis. Na investigação do ataque de ransomware ao oleoduto Colonial (2021), as autoridades norte-americanas conseguiram recuperar parte do resgate pago em bitcoin, demonstrando que a pseudonimidade não é sinônimo de impunidade quando há cooperação com prestadores, rastreabilidade de fluxos e pronta emissão de medidas assecuratórias. A ação combinou heurísticas on-chain, requisições formais a serviços custodiados e cadeia de custódia na apreensão de chaves, sinalizando um caminho metodológico replicável em contextos de alto impacto social (DOJ, 2021).

No Brasil, a Operação Kryptos (2019–2021), que mirou um conglomerado de investimentos suspeitos ancorado em cripto , evidenciou, por sua vez, a relevância da integração entre perícia on-chain, análise contábil e medidas cautelares patrimoniais, além da necessidade de articulação entre Polícia Federal, Ministério Público, Banco Central, COAF e autoridades estrangeiras para acesso a dados e efetividade de bloqueios.

> Segundo a investigação, uma empresa, com sede na Região dos Lagos/RJ, é responsável pela operacionalização de um sistema de pirâmides financeiras ou “esquemas de ponzi”, calcado na efetiva oferta pública de contrato de investimento, sem prévio registro junto aos órgãos regulatórios, vinculado à especulação no mercado de criptomoedas, com a previsão de insustentável retorno financeiro sobre o valor investido. (PF, 2021).

O caso também mostrou que a “porta de entrada” dos recursos ilícitos no sistema bancário doméstico costuma ocorrer por múltiplas vias: adquirência, instituições de pagamento, contas em bancos de menor porte e carteiras de clientes com perfis declarados incompatíveis com a volumetria transacionada, no caso, todos pontos de controle previstos na Lei 9.613/1998 e nos padrões do GAFI. A triangulação entre essas “pontas” e as trilhas on-chain permitiu robustecer o nexo probatório e fundamentar pedidos de sequestras e arrestos com foco na preservação do valor econômico.

Tomados em conjunto, esses casos reforçam cinco implicações para a política pública e a prática forense no domínio cripto. Primeiro, gatekeepers importam: quando VASPs globais internalizam padrões de KYC/KYB, KYT e sanções, a superfície disponível para a estratificação diminui de modo significativo.

Segundo tempo é prova: a capacidade de acionar autoridades centrais e redes de UIFs com prazos de horas invés de semanas, altera a taxa de sucesso de bloqueios e confiscos. Terceiro, inter-cadeia é o novo normal: sem visibilidade para bridges, L2 e wrapped tokens, boa parte das trilhas permanece invisível. Quarto, governança técnica não é neutra: ferramentas com captura de taxas, governança ativa e front-end próprio tendem a ser tratadas como serviços reguláveis, e não como “código estático”. Quinto, integração probatória decide

casos: heurísticas on-chain precisam ser corroboradas por dados de prestadores, registros de acesso, documentos bancários e fiscais, sob padrões de necessidade, adequação e proporcionalidade previstos em.

2.4 Riscos regulatórios e impactos transnacionais

A regulação de criptoativos opera num cenário de assimetria normativa e velocidade tecnológica que produz, simultaneamente, zonas de risco e externalidades transnacionais. No plano doméstico, o Brasil consolidou um arcabouço mínimo com a Lei nº 14.478/2022 que delineia o provedor de serviços de ativos virtuais, com o Decreto nº 11.563/2023, que atribuiu competências regulatórias e de supervisão, e com a Lei nº 9.613/1998, que estrutura o regime de PLD/FT, além da IN RFB nº 1.888/2019, que disciplina obrigações acessórias de reporte.

Esse arranjo, contudo, convive com lacunas de tipificação e de supervisão de fronteira, especialmente quando a prestação de serviços se dá em arquiteturas descentralizadas (DEX/DeFi), quando há exposição relevante a pontes inter-cadeias (bridges), quando emissores de stablecoins operam com estruturas globais de custódia e quando a intermediação é feita por agentes fora da jurisdição nacional.

O resultado é um mosaico regulatório que incentiva arbitragem: a entrada do capital por prestadores de baixa diligência, a pulverização em contratos programáveis e o retorno por canais bancários de maior liquidez, frequentemente em países distintos. Essa dinâmica pressiona gatekeepers locais, VASPs, instituições financeiras e de pagamento, que passam a administrar risco de exposição indireta a eventos originados fora do perímetro regulado doméstico, exigindo controles de KYC/KYB, KYT e “travel rule” adaptados a tipologias específicas (mixers, moedas com foco em privacidade, chain-hopping, bridges e DEX), sob pena de responsabilização por falhas de governança.

Entre os riscos jurídicos mais relevantes estão o enquadramento funcional e os conflitos de qualificação: o mesmo token pode assumir natureza diversa conforme o uso e o modo de oferta, atraindo esferas regulatórias distintas (valores mobiliários, meios de pagamento, atividades de custódia, crédito colateralizado em DeFi).

A pluralidade de regimes suscita incerteza regulatória e risco de enforcement retrospectivo, especialmente quando há promessa pública de rendimento, governança concentrada e captura de taxas que aproximem o arranjo de um serviço regulável. Some-se a isso o problema da lex situs de ativos digitais para fins de medidas assecuratórias e execução: a ausência de um "lugar" físico do bem desloca a discussão para o locus de controle/custódia (chaves, custodiante, provedor), para a jurisdição da autoridade central acionada e para o efeito extraterritorial de ordens de bloqueio, o que exige coordenação por MLATs/rogatórias e pontos de contato 24/7 para evitar dissipação em minutos.

Nessa trilha, o sigilo financeiro e as leis de proteção de dados (inclusive LGPD) funcionam como salvaguardas, não como barreiras absolutas à cooperação: a legalidade estrita, a necessidade, a adequação e a proporcionalidade delimitam a coleta e o compartilhamento de dados, sem legitimar negativas genéricas de auxílio quando a conduta subjacente encontra dupla tipicidade ou quando o pedido prescinde de medidas coercitivas.

Sob o prisma prudencial, emergem riscos operacionais e de custódia. A segregação de ativos em prestadores, a governança de chaves (MPC/multiassinatura), a política de prova de reservas e a gestão de contrapartes determinam a resiliência frente a insolvência, fraude interna e ataques cibernéticos. Provas de reservas não substituem auditorias completas e podem mascarar mismatch entre ativos e passivos se não acompanhadas de compromissos verificáveis de integridade de passivos e de controles sobre reutilização de colateral.

Em ambientes DeFi, a composabilidade cria risco de contágio técnico e econômico: falhas em oráculos, ataques a bridges, incentivos de MEV e bugs em contratos podem propagar perdas sistêmicas entre protocolos interdependentes, com repercussões extraterritoriais quando liquidez e usuários são globais. Para gatekeepers regulados, a exposição indireta por meio de clientes que interagem com tais contratos requer políticas de apetite a risco e de lista de exposição a protocolos/pontes, além de trilhas documentais que suportem decisões de recusa ou de diligência reforçada.

No eixo tributário, a IN RFB nº 1.888/2019 cria obrigações de reporte que visam reduzir a assimetria informacional entre o contribuinte e a administração fiscal, mas sua eficácia depende do grau de cooperação de prestadores estrangeiros e do nível de conformidade espontânea dos usuários, pois carteiras de autocustódia e mercados P2P desafiam o monitoramento tradicional.

A falta de convergência internacional nessa matéria favorece planejamento agressivo e erosão de base, além de contenciosos sobre valoração, momento de realização e tratamento de perdas em mercados de alta volatilidade. Em paralelo, regimes sancionatórios e de embargos (sanctions) projetam efeitos além-fronteiras: prestadores expostos a jurisdições com “long-arm jurisdiction” precisam conciliar listas e proibições globais sob risco de penalidades severas e exclusão de infraestruturas críticas, o que, por sua vez, incentiva redes ilícitas a orquestrar evasões com uso de mixers, moedas de privacidade e bridges, sendo uma corrida que pressiona ainda mais a necessidade de KYT inter-cadeia e de compartilhamento de inteligência em tempo quase real.

> “O FATF também adicionou dois novos cursos de e-learning sobre sanções financeiras direcionadas e sobre ativos virtuais e provedores de serviços de ativos virtuais ao seu programa abrangente de treinamento, que tem como objetivo ampliar o conhecimento dentro da Rede Global. O programa de treinamento e suporte do GAFI ajuda as jurisdições da rede global a implementar medidas sólidas para enfrentar os fluxos financeiros ilícitos que alimentam o crime e o terrorismo. O programa também as ajuda a se preparar para a próxima rodada de avaliações mútuas, que terá um foco muito mais forte na efetividade.” (FATF, 2023)

Os impactos transnacionais manifestam-se, portanto, em três camadas que se retroalimentam. Na camada micro, o aumento de custo e complexidade para atores ilícitos decorre de gatekeepers que internalizam as Recomendações do GAFI: KYC/KYB robusto, travel rule, KYT sensível a tipologias cripto e resposta a ofícios em horas, não semanas.

Na camada meso, a eficácia de medidas assecuratórias e de recuperação de ativos depende da interoperabilidade entre autoridades centrais e UIFs, do

uso eficiente de MLATs/rogatórias e da capacidade de preservação da prova digital (cadeia de custódia, governança de chaves, segregação por caso). Na camada macro, a convergência regulatória reduz incentivos à arbitragem e estabiliza expectativas de mercado, enquanto lacunas e “sunrise problems” da travel rule criam janelas para desvio de fluxos a jurisdições permissivas.

Nessa dimensão, políticas públicas eficazes combinam harmonização mínima (definições, escopo de VASPs, obrigações de identificação, reporte e sanções), capacitação técnica (perícia on-chain e análise inter-cadeia), arranjos 24/7 para pedidos urgentes e parcerias público-privadas que transformem alertas analíticos em medidas concretas, preservando simultaneamente garantias fundamentais.

Em síntese, o risco regulatório em criptoativos é menos um problema de “ausência de lei” e mais um problema de coordenação entre jurisdições, entre autoridades e entre camadas tecnológicas. Enquanto redes ilícitas exploram tempo e fronteiras, a resposta eficaz exige convergência normativa, execução célere e visibilidade inter-cadeia, sem perder de vista que a legitimidade do sistema depende do respeito à legalidade estrita, à proporcionalidade e à privacidade. É nesse equilíbrio, entre prevenção/repressão efetivas e proteção de direitos, que se decide, em última análise, a sustentabilidade do regime de criptoativos no plano.

CAPÍTULO 3 – COOPERAÇÃO INTERNACIONAL E OS CRIPTOATIVOS

Este capítulo aborda a cooperação internacional aplicada aos criptoativos, articulando o padrão global do GAFI com os instrumentos multilaterais que dão lastro jurídico às trocas de informação e às medidas de constrição transfronteiriças. Partimos do papel das Recomendações do GAFI (abordagem baseada em risco, VASPs, travel rule, confisco e assistência mútua) e avançamos pelos mecanismos e redes de inteligência (UIFs/Egmont, ARINs regionais, Convenção de Budapeste/24×7), mostrando como a inteligência financeira se converte, quando bem estruturada, em prova executável por meio de MLATs e cartas rogatórias.

Na sequência, examinamos as limitações legislativas e os desafios de harmonização (definições de ativo virtual/VASP, diferença de prazos e requisitos, sunrise problem da travel rule, DeFi e pontos de governança), e apresentamos tendências e perspectivas: métricas de efetividade, interoperabilidade de dados, leitura inter-cadeia (L1/L2/bridges/rollups) e respostas 24×7. O objetivo é oferecer um mapa prático de como cooperar rápido e com legalidade, reduzindo arbitragem regulatória e aumentando a taxa de bloqueio e recuperação em casos com criptoativos.

3.1 O papel do GAFI e suas recomendações

O Grupo de Ação Financeira (GAFI/FATF) é o foro intergovernamental que desde 1989 define o padrão global de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação, por meio de um conjunto de Recomendações (atualmente quarenta) e de um processo de avaliações mútuas que mede efetividade (immediate outcomes) e conformidade técnica. A relevância do GAFI para criptoativos é dupla. De um lado, o organismo estabeleceu a abordagem baseada em risco como eixo do regime de PLD/FT, exigindo que países e setores identifiquem, avaliem e mitiguem riscos de acordo com a sua materialidade (Recomendação 1). De outro, desde 2019, o GAFI incorporou ativos virtuais e provedores de serviços de ativos virtuais (VASPs) ao seu perímetro normativo, definindo requisitos de licenciamento/registro, supervisão, KYC/KYB, monitoramento transacional (KYT), travel rule e cooperação internacional.

No plano substantivo, as Recomendações que mais impactam o ecossistema cripto estruturam-se em quatro blocos. O primeiro é o bloco preventivo, que impõe deveres a “entidades obrigadas” (incluídos os VASPs): identificação e qualificação de clientes e beneficiários finais (Rec. 10 e 24), due diligence reforçada por risco (Rec. 1 e 12), conservação de registros (Rec. 11), reporte de operações suspeitas às unidades de inteligência financeira (Rec. 20) e sanções financeiras direcionadas (Rec. 6 e 7).

O segundo é o bloco setorial, com a Recomendação 15, que trata especificamente de novas tecnologias, incluindo ativos virtuais: países devem mitigar riscos antes e durante a introdução de novos produtos/serviços, exigir licenciamento/registro de VASPs, garantir supervisão eficaz e aplicar a travel rule (Rec. 16), isto é, a transmissão segura de informações mínimas do originador e do beneficiário entre prestadores quando há transferência de valor. O terceiro bloco é o institucional, com ênfase na UIF (Rec. 29), na coordenação nacional (Rec. 2) e na confiscação e medidas assecuratórias (Rec. 4), inclusive de bens intangíveis. O quarto é o bloco de cooperação internacional (Recs. 36–40), que exige assistência jurídica mútua ampla, extradição, execução de medidas de confisco e canais ágeis de troca de informações entre autoridades competentes.

Três elementos operacionais merecem destaque quando se transpõe esse padrão ao contexto cripto. Primeiro, a definição funcional de VASP: não importa a etiqueta comercial do serviço, mas sim o que ele faz (troca, transferência, custódia, administração ou participação em ofertas e vendas de ativos virtuais). Sempre que uma pessoa natural ou jurídica intermediar ou facilitar profissionalmente essas funções para terceiros, a expectativa do GAFI é de submissão a regras de licenciamento/registro, supervisão e sanções proporcionais. Essa leitura evita “arbitragem semântica” e é coerente com o tratamento de gatekeepers em outros setores regulados.

Segundo a travel rule o núcleo de interoperabilidade de compliance entre prestadores, cujo desafio principal é o chamado “sunrise problem”: a adoção desfasada entre países cria janelas onde parte do tráfego corre sem metadados exigidos. O GAFI recomenda soluções técnicas interoperáveis, verificação de contrapartes e medidas proporcionais de recusa/mitigação quando a contraparte não cumpre os padrões. Terceiro, a ênfase em supervisão efetiva, o que inclui

testes de governança, avaliação de controles de KYT, métricas de resposta a ofícios e a capacidade de bloqueio tempestivo quando houver ordem legal, inclusive em regimes de 24/7 para solicitações urgentes.

No Brasil, o padrão do GAFI foi internalizado por meio de um mosaico normativo que combina a Lei nº 9.613/1998 (e seu sistema de PLD/FT, com reporte à UIF/COAF), a Lei nº 14.478/2022 (diretrizes para prestação de serviços com ativos virtuais e figura do VASP), o Decreto nº 11.563/2023 (atribuições regulatórias e de supervisão) e a IN RFB nº 1.888/2019 (obrigações acessórias de reporte fiscal).

Em conjunto, esses instrumentos alinham o país às Recomendações ao: (i) reconhecer ativos virtuais e VASPs como objetos de políticas de PLD/FT; (ii) habilitar supervisão setorial (com protagonismo do Banco Central do Brasil para prestadores enquadrados e da CVM quando houver valores mobiliários); (iii) demandar KYC/KYB, conservação de registros e reporte de operações suspeitas; e (iv) estabelecer mecanismos de cooperação para confisco e recuperação de ativos.

As lacunas residuais, como a operacionalização plena da travel rule entre VASPs domésticos e estrangeiros, a supervisão de pontos de exposição inter-cadeia (bridges) e o perímetro regulatório de DeFi em casos com captura de taxas e governança vêm sendo endereçadas por regulação infralegal e por alinhamento com guia interpretativo do GAFI.

Do ponto de vista de efetividade, o GAFI mede não só a aderência formal às Recomendações, mas se o país identifica e mitiga riscos de maneira consistente: se os VASPs são licenciados/registrados e efetivamente supervisionados; se a UIF recebe, analisa e dissemina relatórios de suspeição de boa qualidade; se há congelamentos e confiscos proporcionais; se a cooperação internacional é célere e ampla; e se instituições públicas e privadas entendem e aplicam a abordagem baseada em risco.

Para cripto, isso se traduz em indicadores concretos: tempo de resposta a pedidos internacionais, capacidade de análise inter-cadeia (L1, L2, bridges, wrapped tokens), qualidade dos dossiês de reporte (com narrativas de risco e evidências on-chain), governança de chaves em apreensões

(multiassinatura/MPC, segregação por caso) e documentação de cadeia de custódia. Países e prestadores que não entregam esses resultados são alvo de avaliações negativas e, no limite, de listagens (cinza/negra) que ampliam custo de capital e reduzem acesso a correspondentes.

Por fim, vale notar que o GAFI vem ajustando continuamente sua orientação interpretativa para acompanhar stablecoins, serviços de privacidade, DEX/DeFi, mixers e carteiras não custodiadas. A tônica é evitar tanto a complacência quanto proibições cegas: o padrão global favorece proporcionalidade e calibragem por risco, mirando intermediações com captura de taxas e governança (serviços de fato) e fortalecendo pontos de contato 24/7 e parcerias público-privadas para transformar alertas analíticos em ações coordenadas sem violar garantias fundamentais.

Nesse sentido, o papel do GAFI não é o de “legislador global”, mas o de arquitetar convergência: criar linguagem comum, práticas comparáveis e incentivos reputacionais suficientes para que jurisdições e gatekeepers movam-se, em conjunto, rumo a um nível mínimo de proteção compatível com a natureza transnacional e veloz dos fluxos digitais.

3.2 Mecanismos multilaterais e redes de inteligência financeira

A cooperação internacional aplicada a criptoativos assenta-se em dois trilhos complementares: o trilho judicial-formal, fundado em tratados e instrumentos processuais (assistência mútua, cartas rogatórias, extradição, reconhecimento e execução de decisões, confisco e recuperação de ativos), e o trilho de inteligência financeira, estruturado em redes especializadas de Unidades de Inteligência Financeira (UIFs) e parcerias público-privadas. No primeiro, o paradigma continua sendo os tratados multilaterais da ONU, como o de Viena/1988, Palermo/2000 e Mérida/2003, que exigem tipificação ampla da lavagem, medidas assecuratórias, confisco e assistência jurídica mútua (MLAT) com a “mais ampla assistência possível”, inclusive para obtenção de provas digitais e rastreamento de bens intangíveis.

Esse eixo se articula com instrumentos setoriais, em especial a Convenção de Budapeste sobre Cibercrime (2001), que harmoniza tipos penais informáticos, prevê preservação expedita de dados e opera uma rede 24/7 para

pedidos urgentes de natureza eletrônica, aspecto crucial quando fluxos em cripto podem atravessar fronteiras e cadeias (L1/L2/bridges) em minutos (CONSELHO DA EUROPA, 2001). No Brasil, a Autoridade Central para MLATs é o DRCI/MJSP, encarregado de recepcionar e dar curso a pedidos ativos e passivos; a coordenação com Ministério Público, Polícia Federal, Banco Central, CVM e UIF/COAF é indispensável para transformar inteligência em prova admissível e, quando cabível, bloqueio e confisco de valores sob guarda de VASPs sediados no exterior.

O trilho de inteligência financeira é capitaneado pela Rede Egmont, que integra as UIFs do mundo por meio de padrões, manuais e uma infraestrutura segura de compartilhamento (Egmont Secure Web). Diferentemente do MLAT, a cooperação Egmont não produz prova judicial direta: antecipa sinais, conecta casos, concentra relatórios de operações suspeitas (ROS/STR) e ajuda a localizar prestadores e ativos, para então subsidiar o canal formal (EGMONT, 2021).

Na América Latina, a GAFILAT e a RRAG (Rede de Recuperação de Ativos) funcionam como hubs regionais para recuperação e partilha de boas práticas; na Europa e outras regiões, as Redes ARIN (p. ex., CARIN na UE e seus correlatos regionais) aproximam pontos de contato especializados em confisco e asset tracing, acelerando a identificação de “pontos de apreensão” (GAFILAT, 2020; CARIN, 2016). Em paralelo, iniciativas como StAR/UNODC-Banco Mundial apoiam reformas legais e casos complexos de recuperação transnacional, sobretudo quando valores migram por camadas corporativas e fundos com múltiplas jurisdições. (UNODC/WB, 2007).

Para o domínio cripto, esses mecanismos passaram a absorver três exigências técnicas: visibilidade inter-cadeia, tempo de resposta e interoperabilidade de metadados. A primeira demanda que autoridades e UIFs consigam ler exposição a L2, wrapped tokens e bridges, bem como converter “rótulos” comerciais (exchanges, mixers, OTCs) em contrapartes jurídicas (CNPJ/LEI/endereço/autoridade supervisora).

A segunda remete à capacidade de responder em horas, não semanas, ativando redes 24/7 (Budapeste; Interpol I-24/7; Egmont) para preservar dados

voláteis (logs, IPs, carimbos de tempo, registros internos de custódia) antes do pedido formal. A terceira envolve a travel rule: o intercâmbio de informações mínimas do originador/beneficiário entre VASPs em transferências, cuja adoção descompassada entre países cria o chamado sunrise problem; por isso, o GAFI tem recomendado padrões de dados (v.g., IVMS-101) e soluções interoperáveis (TRISA, TRP, OpenVASP), além de due diligence sobre contrapartes que não implementam a regra.

Na prática, a jornada de um caso com cripto costuma seguir um pipeline híbrido. A detecção nasce no setor privado (VASPs, bancos, instituições de pagamento) por KYT sensível a tipologias (mixers/coinjoins, moedas de privacidade, chain-hopping/bridges, exposição a carteiras sancionadas), gera ROS à UIF nacional e aciona canais Egmont para verificar vínculos transfronteiriços.

Confirmadas materialidade e risco, a autoridade competente estrutura o pedido MLAT com delimitação de escopo, base legal (dupla tipicidade pela conduta, não pelo rótulo “cripto”), justificativa de urgência e medidas solicitadas (preservação, entrega de registros, congelamento), apontando a autoridade supervisora do VASP estrangeiro para facilitar execução.

Em paralelo, aciona-se a rede 24/7 (Budapeste/Interpol) para preservar dados que, por política de retenção, poderiam desaparecer. A execução ideal combina rapidez do trilho de inteligência com formalização probatória do trilho judicial: a primeira evita perda de metadados e dissipações; a segunda dá base para sequestro, arresto e confisco.

Redes público-privadas ampliam a eficácia desse pipeline. Experiências como JMLIT (Reino Unido), FinCEN Exchange (EUA) e Fintel Alliance (Austrália) mostram que fóruns seguros para compartilhamento de tipologias e indicadores entre autoridades e instituições reguladas reduzem o tempo entre alerta analítico e congelamento, sobretudo em casos com alto impacto social (ransomware, hacks de bridges, financiamento ilícito).

O Brasil vem expandindo a Rede LAB-LD (Laboratórios de Tecnologia contra Lavagem de Dinheiro) e iniciativas de cooperação interinstitucional que aproximam perícia on-chain, fiscalização tributária (IN RFB nº 1.888/2019),

regulação prudencial e persecução penal, de modo a encurtar o ciclo “inteligência-prova-constrição” Importa lembrar que inteligência não é prova: relatórios analíticos precisam ser corroborados por meios legais idôneos (ordens judiciais, respostas MLAT, documentos autenticados), sob pena de nulidades e de contaminação de cadeias probatórias.

Há, contudo, limites e fricções. As diferenças de prazos e de requisitos formais entre autoridades centrais; a invocação indevida de segredo financeiro e de proteção de dados como bloqueio absoluto; a dúvida sobre lex situs de ativos digitais para fins de competência; e a dificuldade de enquadrar arquiteturas descentralizadas (DEX/DeFi) no perímetro de VASPs quando há governança difusa e ausência de captura de taxas são pontos que ainda testam a elasticidade do sistema.

O padrão internacional caminha para respostas funcionais e proporcionais: quando há intermediação material, captura de taxas e governança (front-end, operadores, multisig, tesouraria), cresce a expectativa de deveres de prevenção e de cooperabilidade; quando não há, a ênfase volta-se a pontos de entrada e saída (on/off-ramps, emissores de stablecoins, custodiante de wrapped tokens) e a ordens dirigidas a usuários identificados.

De todo modo, a combinação de convergência regulatória mínima (definições, escopo de VASPs, travel rule), capacidade técnica (leitura inter-cadeia, preservação/guarda de chaves e logs, documentação de cadeia de custódia) e canais 24/7 tende a elevar, de forma mensurável, a taxa de sucesso em bloqueios e recuperações no ambiente cripto, sem abdicar das garantias fundamentais que legitimam a cooperação internacional.

3.3 Limitações legislativas e desafios à harmonização normativa

A harmonização normativa no campo dos criptoativos enfrenta um conjunto de tensões estruturais que não decorrem apenas de lacunas textuais, mas de diferenças de filosofia regulatória, de arranjos institucionais e do próprio modo como cada sistema jurídico decide compatibilizar inovação tecnológica com garantias fundamentais. Mesmo quando os países afirmam seguir as Recomendações do GAFI, persistem assimetrias significativas em temas como definição de “ativo virtual” e de “provedor de serviços de ativos virtuais (VASPs)”,

escopo material da “travel rule”, tratamento de arquiteturas descentralizadas e critérios para confisco e recuperação de ativos digitais, o que fomenta arbitragem regulatória e reduz a previsibilidade para gatekeepers e autoridades.

No plano doméstico, o Brasil deu passos importantes com a Lei nº 14.478/2022, que estabeleceu diretrizes e a figura do VASP, e com o Decreto nº 11.563/2023, que atribuiu competências regulatórias e de supervisão, em diálogo com a Lei nº 9.613/1998 e com as obrigações acessórias da IN RFB nº 1.888/2019. Como os artigos 6º e 7º garante a obrigação de transparência de todas as partes da negociações.

Ainda assim, a operacionalização plena desses comandos esbarra em desafios práticos: a adoção descompassada da travel rule por contrapartes estrangeiras, o perímetro de incidência sobre serviços que capturam taxas e exercem governança em ecossistemas DeFi, a identificação de responsáveis por front-ends e “interfaces” que intermediam acesso a contratos inteligentes e a calibragem de expectativas para emissores de stablecoins com custódia e governança fragmentadas em múltiplas jurisdições.

Há, ademais, um problema de linguagem comum. A taxonomia adotada por cada jurisdição quanto a “criptoativo”, “ativo virtual”, “token de pagamento”, “token de utilidade” e “valor mobiliário” segue heterogênea; a mesma representação digital pode migrar de categoria conforme o uso, a promessa econômica e a forma de distribuição ao público, atraindo regimes distintos e, por vezes, conflitantes.

Esse quadro alimenta incerteza jurídica e contenciosos sobre competência de supervisores, sujeição a regras prudenciais e deveres de PLD/FT, com risco de enforcement retrospectivo quando a autoridade entende ex post que a função econômica concreta aproximava o arranjo de um serviço regulável. A recomendação internacional por uma definição funcional de VASP atenua o problema, mas não elimina a fricção em torno de serviços “sem custódia formal” que, mesmo assim, extraem taxas, operam tesouraria, mantêm repositórios de chaves de administração ou controlam parâmetros críticos de contratos, pontos que têm sido tratados, mundo afora, por guias interpretativos e não por tipificações legislativas exaustivas.

No domínio probatório e sancionatório, duas limitações se destacam. A primeira é a da dupla tipicidade e da lex situs de ativos digitais para fins de cooperação: como o bem não tem ancoragem física e o controle efetivo é distribuído entre chaves e custodiantes, a competência e a execução de ordens de congelamento/ confisco dependem da localização do custodiante, do ponto de acesso do usuário, da autoridade supervisora e da efetividade dos canais de assistência mútua, de modo que pedidos amplos e não delimitados tendem a fracassar.

A segunda é a necessidade de compatibilizar legalidade estrita, proporcionalidade e proteção de dados com a urgência operacional de preservar logs, IPs, registros de custódia e chaves sob guarda de VASPs, evitando tanto negativas genéricas com base em segredo financeiro quanto coletas excessivas que contaminem a cadeia probatória.

A orientação do GAFI é clara ao exigir assistência ampla fundada na conduta subjacente e a admitir cooperação mesmo sem dupla incriminação quando não há medidas coercitivas, mas a prática mostra que diferenças procedimentais e prazos internos ainda constituem gargalos relevantes, sobretudo em cenários de chain-hopping e bridges que dissipam valores em minutos.

Do ponto de vista prudencial e de integridade de mercado, a ausência de padrões mínimos e verificáveis de governança de chaves, segregação de ativos, auditoria e prova de reservas cria assimetrias de informação entre clientes, reguladores e VASPs; “provas de reservas” sem escopo sobre passivos e governança podem induzir falsa sensação de solvência.

Em ecossistemas programáveis, a composabilidade entre protocolos multiplica riscos de contágio técnico e econômico, exigindo que supervisores e instituições definam listas de exposição a contratos e bridges, critérios de due diligence por risco e mecanismos de desligamento proporcional que não redundem em censura indiscriminada de contratos, mas que reduzam exposição a falhas estruturais. E, em paralelo, regimes de sanções extraterritoriais e listas divergentes entre jurisdições impõem dilemas de conformidade para prestadores globais: a tentativa de conciliar múltiplos ordenamentos ao mesmo tempo amplia

custos e incentiva atores ilícitos a operar nos interstícios ainda não cobertos por padrões interoperáveis de travel rule e de compartilhamento de metadados.

Há, por fim, um conjunto de desafios ligados à harmonização “de fato”, e não apenas “de direito”. A eficácia do regime depende menos da existência de leis formais e mais da capacidade de implementá-las com recursos técnicos e humanos adequados. Isso envolve formar perícia on-chain capaz de leitura inter-cadeia (L1, L2, wrapped tokens), estabelecer pontos de contato 24/7 para pedidos urgentes, produzir guias operacionais que traduzam as Recomendações em checklists concretos para VASPs e bancos, e incentivar parcerias público-privadas que reduzam o tempo entre alerta analítico e medida assecuratória.

Também exige padronização documental de MLATs e cartas rogatórias, com narrativas de risco factuais, delimitação de escopo, indicação da autoridade supervisora do destinatário e preservação prévia de dados voláteis por redes 24/7. Sem essa camada operacional, o regime “no papel” perde densidade e a harmonização normativa se torna, na prática, irregular e regressiva, pois incentiva a movimentação de fluxos para jurisdições com baixa capacidade de execução, reduzindo o efeito dissuasório e a taxa de recuperação de ativos.

Em síntese, as limitações legislativas e os desafios de harmonização não se resolvem apenas com novas tipificações ou listas mais extensas. O núcleo do problema é coordenar conceitos, competências e procedimentos entre países e entre camadas tecnológicas, adotando uma leitura funcional do papel dos intermediários, impondo deveres proporcionais a quem capta taxas e exerce governança, e reforçando, ao mesmo tempo, os pilares de legalidade, proporcionalidade e proteção de dados.

A convergência que importa, e que dá lastro às Recomendações do GAFI e ao mosaico normativo brasileiro, é aquela que transforma linguagem jurídica comum em capacidade prática de prevenir, investigar, bloquear e recuperar ativos digitais, sem sacrificar as garantias que legitimam a atuação estatal no Estado de Direito.

3.4 Tendências e aspectos para o combate global à lavagem com criptoativos

O combate global à lavagem envolvendo criptoativos caminha para um arranjo de convergência funcional: menos ênfase em rótulos e mais foco no que serviços e protocolos efetivamente fazem, trocar, custodiar, transferir, intermediar ofertas e administrar liquidez, impondo deveres proporcionais a quem capta taxas e exerce governança.

Essa inflexão, já preconizada pelo GAFI desde 2019, tende a consolidar quatro linhas de evolução. A primeira é a profundidade regulatória nos pontos de contato com o sistema financeiro: VASPs com licenciamento/registro, supervisão baseada em risco e métricas de efetividade (qualidade de ROS, tempo de resposta a ofícios, capacidade de congelar/segregar ativos, governança de chaves com MPC/multiassinatura, documentação de cadeia de custódia).

A segunda é a interoperabilidade informacional, com a adoção de padrões de dados e soluções técnicas para travel rule, mitigando o “sunrise problem” por mecanismos de verificação de contrapartes e medidas proporcionais quando o destinatário não cumpre o padrão.

A terceira é a visibilidade inter-cadeia como requisito para compliance e investigação, leitura de L1, L2, wrapped tokens, bridges e swaps atômicos, elevando a maturidade de ferramentas de KYT e perícia on-chain.

A quarta é a resposta 24/7, com redes específicas (Budapeste/Interpol, Egmont, ARINs regionais) para preservação expedita de logs e dados de custódia antes mesmo do MLAT, reduzindo o hiato entre alerta privado e constrição judicial.

No plano tecnológico, três movimentos se impõem. Primeiro, a passagem de um monitoramento centrado em endereços para um monitoramento centrado em contratos e ecossistemas, com listas de exposição a bridges e pools de alto risco, análise de MEV e de roteamentos que degradam a previsibilidade das rotas, e orquestração de respostas automáticas quando a heurística sinaliza mixers, coinjoins, moedas de privacidade e padrões de chain-hopping.

Segundo o amadurecimento de modelos de prova de reservas com prova de passivos, evitando “falsas confortabilidades” prudenciais e integrando auditoria cripto-nativa a testes tradicionais de solvência e segregação de ativos. Terceiro, a experimentação regulatória com cripto-compliance de privacidade, em que provas de conhecimento zero permitem atestar atributos (p. ex., sanções/ PEP/ jurisdição) sem expor dados pessoais, e viewing keys ou controles de acesso calibram o equilíbrio entre proteção de dados e rastreabilidade quando necessário, preservando a proporcionalidade exigida por LGPD/GDPR e pelos padrões do GAFI.

No ambiente de mercado, stablecoins e tokenização deslocam o eixo do risco. Emissões com lastro fiduciário e governança global exigem regras claras sobre reserva, liquidez, custódia e insolvência, e cooperabilidade com autoridades para congelamento/recall quando há base legal, sob pena de se tornarem “meios de integração” rápidos e de baixo atrito.

A tokenização de ativos do mundo real amplia o perímetro de PLD/FT, exigindo identificação granular de beneficiário final e cadeias de titularidade, inclusive quando o ativo subjacente está em jurisdição distinta do emissor do token. Já em DeFi, caminha-se para um teste funcional: se há tesouraria, captura de taxas, multisig, governança ativa e front-end operado por pessoas identificáveis, cresce a expectativa de deveres de VASP; se não, a política pública se concentra em on/off-ramps, emissores de stablecoins, custodiante de wrapped tokens e ordens dirigidas ao usuário identificado, evitando tratar “código estático” como serviço por si.

No vetor cooperação internacional, a tendência é combinar harmonização mínima (definições, escopo de VASPs, travel rule, confisco de bens intangíveis) com capacidade operacional: autoridade central dotada de pessoal técnico, formulários padronizados, pontos de contato 24/7, e integração com a UIF para transformar ROS em pedidos MLAT com narrativa fática, delimitação de escopo, base legal (dupla tipicidade pela conduta, não pelo rótulo “cripto”) e identificação da autoridade supervisora estrangeira.

As redes Egmont e ARINs regionais ampliam o alcance de asset tracing e encurtam o ciclo entre inteligência e prova, sem confundir uma com a outra. Em

paralelo, multiplicam-se parcerias público-privadas (JMLIT, FinCEN Exchange, Fintel Alliance e congêneres) que compartilham tipologias e indicadores de risco em ambientes seguros, elevando a taxa de sucesso de bloqueios em casos de alto impacto (ransomware, hacks de bridges, financiamento ilícito). (FATF, 2019; 2023)

> “Uma UIF (Unidade de inteligência Financeira) deve obter informações adicionais das entidades obrigadas e ter acesso tempestivo às informações financeiras, administrativas e de aplicação da lei necessárias para desempenhar adequadamente suas funções. Alguns fatores centrais moldam a criação de uma UIF: as leis de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, a estrutura existente de aplicação da lei e a necessidade de uma autoridade responsável por receber, avaliar e compartilhar informações financeiras.” (EGMONT, 2021)

Do lado sancionatório, observam-se respostas mais cirúrgicas: ações contra mixers custodiais e plataformas com frágil governança de PLD/FT; exigência de geofencing e bloqueios por exposição a listas; e negociações que internalizam “padrões de expectativa” mínimos para VASPs sistêmicos (KYC/KYB, sanções, KYT inter-cadeia, tempo de resposta, governança de chaves).

A lição prática é que gatekeepers importam: quando grandes prestadores aderem a padrões compatíveis com o GAFI, a superfície de estratificação encolhe de forma mensurável. Ao mesmo tempo, há sinais de deslocamento para periferias regulatórias (P2P, OTC, ATMs, DEX sem governança aparente), o que reforça a importância de políticas proporcionais, que não expulsem o tráfego íntegro para áreas opacas, e de estratégias de redução de danos (onboarding seguro, limites graduais, educação do usuário, triagem por risco).

No campo probatório, a próxima fronteira é metodológica: relatórios de perícia on-chain precisarão explicitar margens de erro, hipóteses e

corroborações off-chain (registros de acesso, documentos bancários, logs de API), sob pena de falsos positivos e de fragilidade em juízo.

A tendência é a adoção de protocolos forenses padronizados (descrição de heurísticas, versões de ferramentas, hashes de evidências, cadeia de custódia digital), capazes de dialogar com as exigências de legalidade estrita, necessidade e proporcionalidade da Lei nº 9.613/1998 e das convenções de cooperação. Conecta-se a isso a padronização de custódia pública de criptoativos apreendidos, com carteiras institucionais segregadas por caso, governança de chaves em múltiplas partes, logs imutáveis e políticas de liquidação conversacional com preservação de valor, pilares sem os quais confisco e recuperação ficam aquém do potencial.

Sob a ótica tributária, a IN RFB nº 1.888/2019 continuará a ser calibrada pela prática: a eficácia do reporte depende da cooperabilidade de prestadores estrangeiros e do grau de conformidade espontânea em autocustódia e P2P. A perspectiva é de maior integração entre fisco, supervisores e UIF, com analytics que cruzam declarações, exposições on-chain e perfis de risco, respeitando a LGPD e priorizando materialidade fiscal em contextos de alta volatilidade e de planejamento agressivo.

Em síntese, o horizonte combina convergência normativa mínima, execução célere e capacidade técnica para leitura inter-cadeia, sem abdicar de garantias fundamentais. A sustentabilidade do regime depende de converter linguagem comum (GAFI) em resultados mensuráveis: VASPs licenciados e supervisionados; travel rule interoperável; ROS de boa qualidade; MLATs eficazes; bloqueios e confiscos proporcionais; e custódia pública segura de ativos apreendidos.

Onde esses elementos coexistem, a pseudonimidade deixa de ser sinônimo de impunidade; onde faltam, a arbitragem regulatória continua a premiar a velocidade dos fluxos ilícitos. O desafio, portanto, não é “cripto versus lei”, mas coordenação: entre países, autoridades e camadas tecnológicas, exatamente o tipo de coordenação que o mosaico normativo brasileiro (Lei nº 9.613/1998; Lei nº 14.478/2022; Decreto nº 11.563/2023; IN RFB nº 1.888/2019) e o padrão internacional pretendem tornar prática cotidiana.

Conclusão.

O conflito central que percorre este trabalho pode ser formulado assim: como compatibilizar a natureza transnacional, pseudônima e tecnicamente dinâmica dos criptoativos com deveres estatais de prevenção, investigação, tributação e repressão, sem sufocar a inovação legítima nem esvaziar garantias fundamentais? A resposta que emerge do conjunto de fontes analisadas indica que nenhuma jurisdição, isoladamente, consegue entregar resultados sustentáveis; é preciso combinar (i) regulação funcional e baseada em risco, (ii) capacidade tecnológica para leitura e constrição em múltiplas cadeias e (iii) comunicação internacional robusta e tempestiva entre autoridades e gatekeepers.

Do ponto de vista doméstico, o Brasil instituiu obrigações acessórias relevantes com a IN RFB nº 1.888/2019, justamente para elevar a arrecadação e aumentar o controle sobre origem, destino e transações com criptoativos, a fim de evitar a evasão fiscal e a lavagem (e outros ilícitos), um reconhecimento explícito de que, sem dados estruturados, a administração tributária perde visibilidade sobre fluxos digitais.

A norma também alcança operações em exchanges estrangeiras ou fora de exchanges, deslocando o dever de informar para pessoas físicas e jurídicas brasileiras, o que procura fechar lacunas usuais de planejamento e arbitragem de reporte.

Ainda assim, a literatura aponta um descompasso de finalidade: a IN 1.888/2019 tem ênfase arrecadatória e não impõe, por si só, o reporte de operações suspeitas à UIF/COAF, o que fragiliza a ponte entre o dado fiscal e a inteligência financeira quando o objetivo é PLD/FT. Esse vazio vem sendo parcialmente suprido por práticas voluntárias de VASPs, com comunicações efetivamente enviadas ao COAF desde 2017, mas em volume ainda distante do universo de plataformas ativas, sintoma de uma governança em transição.

No plano regulatório-setorial, o Decreto nº 11.563/2023 atribuiu ao Banco Central competência para regular e supervisionar prestadores enquadrados, movimento coerente com a exigência de KYC, registros e reporte e com

iniciativas de autorregulação (ABCripto) que buscam elevar padrões mínimos de PLD/FT.

Esse avanço local dialoga com experiências estrangeiras (Austrália, Japão, Estônia), onde as exchanges passaram a cadastrar-se, identificar clientes e manter registros por anos, sinalizando uma convergência funcional sobre o papel de gatekeepers, ainda que por caminhos normativos diferentes.

O limite das soluções domésticas, porém, aparece com nitidez sempre que o rastro depende de cooperação transfronteiriça. Quando valores migram por exchanges situadas em paraísos fiscais ou em países sem tratados de troca de informações com o Brasil, a rastreabilidade e a recuperação tornam-se dramaticamente mais difíceis, sobretudo se a conversão rápida para autocustódia e a pulverização em alto volume ocorrerem antes de qualquer medida constritiva.

Por isso, a conclusão inevitável é que tecnologia sem cooperação internacional é insuficiente: a perícia on-chain precisa vir acompanhada de canais céleres de compartilhamento de dados e de execução de ordens para que a prova seja admissível e o bloqueio, efetivo.

Esse quadro também explica por que fragmentação regulatória é combustível de risco. A literatura mapeia diferenças entre blocos (p. ex., 5AMLD na União Europeia) e jurisdições (EUA, Itália), bem como a oscilação conceitual sobre o que é ativo virtual e quem é VASP, assimetrias que facilitam arbitragem e deslocamento de fluxos para perímetros menos exigentes.

Nessa arena, o papel do GAFI/FATF permanece central: sua orientação pós-2019 pede regulação de ativos virtuais e VASPs, licenciamento/registro, supervisão baseada em risco, KYC/KYB, guarda de dados, reporte de suspeitas, sanções e cooperação internacional, exatamente os pilares que reduzem a vantagem operacional da lavagem em ambiente digital.

Duas implicações normativas se impõem como resposta ao conflito mapeado. Primeiro, a regulação precisa mirar função e governança, e não rótulos: toda intermediação que capta taxas, guarda chaves, opera tesouraria ou controla parâmetros críticos deve se submeter a deveres proporcionais de

diligência, registro, supervisão e cooperação, com incentivos e sanções claras para conformidade.

Isso inclui métricas objetivas de efetividade (qualidade de comunicações, tempo de resposta, capacidade de segregar e custodiar ativos apreendidos) e mecanismos de interoperabilidade de dados que reduzam fricções entre VASPs de diferentes jurisdições. Segundo, é indispensável investir em capacidade tecnológica pública e privada (leitura inter-cadeia, análise de bridges e wrapped tokens, governança de chaves em apreensões) e em comunicação internacional forte e contínua (pontos de contato 24/7, formulários padronizados, rotas rápidas para preservação e entrega de registros), sob pena de transformar a pseudonimidade em oportunidade sistêmica para evasão fiscal e dissimulação patrimonial.

No Brasil, inclusive, a própria exposição de motivos e a doutrina justificam a IN 1.888/2019 como instrumento para evitar evasão fiscal e dar lastro informacional à supervisão, um reconhecimento de que sem dados compartilháveis, não há controle.

Em síntese, sem comunicação, entre países, entre autoridades e entre camadas tecnológicas, o custo de praticar o crime cai e a chance de impunidade sobe. Com convergência mínima de padrões, tecnologia aplicada e cooperabilidade em tempo útil, a pseudonimidade deixa de ser barreira intransponível e volta a ser apenas uma característica técnica administrável, enquanto a tributação e o PLD/FT recuperam capacidade de ver, congelar e confiscar com proporcionalidade e respeito ao devido processo. O mosaico normativo brasileiro, lido à luz das orientações do GAFI, aponta o caminho, o desafio é executá-lo em rede, para que a promessa de inovação não seja capturada pela arbitragem das brechas e pelo silêncio entre fronteiras.

REFERÊNCIAS BIBLIOGRAFICAS:

ANTONOPOULOS, Andreas M. *Mastering Bitcoin: unlocking digital cryptocurrencies*. 2. ed. Sebastopol: O'Reilly Media, 2017.

ANTONOPOULOS, Andreas M.; WOOD, Gavin. *Mastering Ethereum: building smart contracts and DApps*. Sebastopol: O'Reilly Media, 2018.

BADARÓ, Gustavo Henrique. Lavagem de dinheiro: o conceito de produto indireto da infração penal antecedente no crime de lavagem de dinheiro. Revista dos Tribunais – Caderno Especial, São Paulo, v. 967, p. 73-93, 2016

BANK FOR INTERNATIONAL SETTLEMENTS (BIS). *Central bank digital currencies: foundational principles and core features*. Basel: BIS, 2020.

BRASIL. Decreto nº 11.563, de 13 de junho de 2023. Dispõe sobre a competência regulatória e de supervisão de prestadores de serviços de ativos virtuais. Diário Oficial da União, Brasília, DF, 14 jun. 2023.

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, 4 mar. 1998.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes para a prestação de serviços de ativos virtuais e define o provedor de serviços de ativos virtuais (VASP). Diário Oficial da União, Brasília, DF, 22 dez. 2022.

CONSELHO DA EUROPA. *Convenção sobre o Cibercrime (Convenção de Budapeste)*. Budapeste, 2001.

EGMONT GROUP. *About the Egmont Group of Financial Intelligence Units*. Ottawa: Egmont, 2021.

EUROPOL. *Law enforcement disrupts ChipMixer, a cryptocurrency laundering service*. Haia: Europol, 2023.

FATF – FINANCIAL ACTION TASK FORCE. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*. Paris: FATF/OECD, 2012 (atualizadas em 2023).

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

FATF – FINANCIAL ACTION TASK FORCE. *Updated Guidance on Virtual Assets and VASPs / Targeted Updates on Implementation, including Travel Rule and DeFi/Mixers (2019–2023)*. Paris: FATF/OECD, 2023.

GAFI. As Recomendações do GAFI: padrões internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação. Tradução sob coordenação do COAF. [S.l.: s.n.], 2012.

MEIKLEJOHN, Sarah et al. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. *Proceedings of the 2013 Internet Measurement Conference (IMC '13)*, Barcelona, 2013.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

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

POON, Joseph; DRYJA, Thaddeus. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 2016 (white paper).

RECEITA FEDERAL DO BRASIL (RFB). Instrução Normativa RFB nº 1.888, de 3 de maio de 2019. Dispõe sobre a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos. Diário Oficial da União, Brasília, DF, 7 maio 2019.

UNITED NATIONS. *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention)*. Viena, 1988.

UNITED NATIONS. *United Nations Convention against Transnational Organized Crime (Palermo Convention)*. Palermo, 2000.

UNITED NATIONS. *United Nations Convention against Corruption (UNCAC, Mérida)*. Mérida, 2003.

UNITED STATES. Department of Justice (DOJ). *Department of Justice Seizes Ransomware Proceeds from Colonial Pipeline Attack*. Washington, DC: DOJ, 2021.

UNITED STATES. Department of Justice (DOJ). *U.S. and German Authorities Disrupt Hydra Market, the World's Largest Darknet Market*. Washington, DC: DOJ, 2022.

UNITED STATES. Department of Justice (DOJ). *Justice Department Announces Enforcement Action Against Bitzlato* (e outros casos correlatos). Washington, DC: DOJ, 2023.

UNITED STATES. Department of Justice (DOJ); Department of the Treasury; CFTC. *Global resolution with Binance/Changpeng Zhao* (componentes penais e administrativos). Washington, DC, 2023.

UNITED STATES. Department of Justice (DOJ). *Indictment/Case against Samourai Wallet Developers* (mixing/coinjoin). Washington, DC: DOJ, 2024.

UNITED STATES. Department of the Treasury – Office of Foreign Assets Control (OFAC). *Sanctions related to Tornado Cash*. Washington, DC: OFAC, 2022.

UNITED STATES. Department of the Treasury. *Press materials on DPRK/Lazarus Group cyber activities and crypto sanctions*. Washington, DC: Treasury, 2022.

UNODC; WORLD BANK. *Stolen Asset Recovery (StAR) Initiative: Challenges, Opportunities and Action Plan*. Washington, DC: World Bank/UNODC, 2007.

WOOD, Gavin. *Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper)*. 2014.