Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i1.20387

GOVERNANÇA DE CRIPTOATIVOS E COMPLIANCE REGULATÓRIO: DESAFIOS GLOBAIS NA PREVENÇÃO DE ILÍCITOS FINANCEIROS DIGITAIS

CRYPTOASSET GOVERNANCE AND REGULATORY COMPLIANCE: GLOBAL CHALLENGES IN PREVENTING DIGITAL FINANCIAL CRIMES

GOBERNANZA DE CRIPTOACTIVOS Y CUMPLIMIENTO REGULATORIO: DESAFÍOS GLOBALES EN LA PREVENCIÓN DE DELITOS FINANCIEROS DIGITALES

Jaison Sfogia Ricardo[1]

RESUMO: O advento e a rápida ascensão dos criptoativos transformaram o panorama financeiro global, impulsionando a inovação, mas também introduzindo desafios substanciais no combate a ilícitos financeiros, notadamente a lavagem de dinheiro (LD) e o financiamento do terrorismo (FT). Este artigo explora as complexidades da natureza descentralizada e pseudônima dos criptoativos, que são exploradas para fins criminosos, culminando em volumes anuais de lavagem de dinheiro estimados entre US$ 800 bilhões e 2 trilhões globalmente. Por meio de uma análise do arcabouço regulatório brasileiro (Lei nº 14.478/2022 e regulamentações do Banco Central do Brasil) e uma comparação com abordagens normativas internacionais (FATF, União Europeia, Estados Unidos), este estudo identifica lacunas e inconsistências regulatórias. Propomos uma discussão crítica sobre a eficácia das medidas existentes, especialmente diante das limitações técnicas de congelamento de ativos e da persistência de movimentação de fundos por entidades sancionadas. Finalmente, delineamos estratégias futuras, enfatizando a cooperação internacional, o investimento em tecnologias avançadas como análise de blockchain, inteligência artificial (IA) e supervisão embutida, e a necessidade de um equilíbrio estratégico entre fomentar a inovação e garantir a segurança e integridade financeira na era digital.

Palavras-chave: Criptoativos. Lavagem de Dinheiro. Regulamentação. Blockchain.

ABSTRACT: The advent and rapid rise of crypto-assets have transformed the global financial landscape, driving innovation while also presenting substantial challenges in combating financial crime, notably money laundering (ML) and terrorist financing (TF). This article explores the complexities arising from the decentralized and pseudonymous nature of crypto-assets, which are exploited for criminal purposes, resulting in estimated annual money laundering volumes ranging from US $800 billion to US $2 trillion worldwide. Through an analysis of the Brazilian regulatory framework (Law No 14.478/2022 and regulations issued by the Central Bank of Brazil) and a comparison with international normative approaches (FATF, European Union, United States), this study identifies regulatory gaps and inconsistencies. We propose a critical discussion on the effectiveness of existing measures, especially considering the technical limitations of asset freezing and the ongoing movement of funds by sanctioned entities. Finally, we outline future strategies, emphasizing international cooperation; investment in advanced technologies such as blockchain analytics, artificial intelligence (AI), and embedded supervision; and the need for a delicate balance between fostering innovation and ensuring financial security and integrity in the digital era.

Keywords: Crypto-assets. Money Laundering. Regulation. Blockchain.

[1] Pós-graduado em Compliance e Integridade Corporativa pela Pontifícia Universidade Católica de Minas Gerais. Diretor de Secretaria no TRT-9.

RESUMEN: El advenimiento y la rápida expansión de los criptoactivos han transformado el panorama financiero global, impulsando la innovación, pero también introduciendo desafíos sustanciales en la lucha contra los delitos financieros, en particular el lavado de dinero (LD) y la financiación del terrorismo (FT). Este artículo explora las complejidades de la naturaleza descentralizada y pseudónima de los criptoactivos, que son aprovechados con fines ilícitos, generando volúmenes anuales de lavado de dinero estimados entre 800 mil millones y 2 billones de dólares a nivel mundial. A través del análisis del marco regulatorio brasileño (Ley nº 14.478/2022 y regulaciones del Banco Central de Brasil) y una comparación con enfoques normativos internacionales (GAFI, Unión Europea, Estados Unidos), este estudio identifica lagunas e inconsistencias regulatorias. Se propone una discusión crítica sobre la eficacia de las medidas actuales, especialmente frente a las limitaciones técnicas para el congelamiento de activos y la continua movilización de fondos por parte de entidades sancionadas. Finalmente, se delinean estrategias futuras, destacando la cooperación internacional, la inversión en tecnologías avanzadas como el análisis de blockchain, la inteligencia artificial (IA) y la supervisión embebida, así como la necesidad de un equilibrio delicado entre el fomento de la innovación y la garantía de la seguridad e integridad financiera en la era digital.

Palabras clave: Criptoactivos. Lavado de Dinero. Regulación. Blockchain.

1. INTRODUÇÃO

O surgimento e a ascensão vertiginosa dos criptoativos têm reconfigurado o panorama financeiro global, impulsionados por inovações tecnológicas e uma demanda crescente por modalidades alternativas de investimento e transações digitais.

Contudo, essa transformação paradigmática introduziu desafios substanciais no combate a ilícitos financeiros, notadamente a lavagem de dinheiro e o financiamento do terrorismo, que exploram a inerente natureza descentralizada e, por vezes, pseudônima dessas moedas digitais.

A dimensão do problema é alarmante: projeta-se que a lavagem de dinheiro atinja volumes globais anuais de US$ 800 bilhões a 2 trilhões, equivalente de 2 a 5% do Produto Interno Bruto (PIB) mundial, posicionando-a como um dos maiores entraves para agências reguladoras e forças de aplicação da lei (UNODC, 2020).

Além disso, o valor recebido por endereços de criptomoedas ilícitos em 2024 foi de US$ 40,9 bilhões, com uma estimativa de superar os US$ 51 bilhões, dado um crescimento médio anual de 25% desde 2020. A atividade ilícita em blockchain tem se diversificado e profissionalizado, abrangendo desde crimes cibernéticos até o financiamento de ameaças à segurança nacional (CHAINALYSIS, 2025).

Este artigo propõe uma análise aprofundada do complexo cenário dos criptoativos, com particular atenção à Lei nº 14.478/2022 e seu arcabouço regulatório no Brasil, em comparação com as abordagens normativas internacionais.

A pesquisa se desdobra em uma exploração da definição e das características fundamentais dos criptoativos, uma avaliação crítica dos riscos inerentes à sua exploração em atividades ilícitas

e um exame das medidas regulatórias e de supervisão adotadas tanto globalmente quanto no contexto brasileiro.

Serão, ademais, discutidos os desafios persistentes na implementação dessas normativas e delineadas estratégias futuras, bem como recomendações visando ao fortalecimento do regime de combate aos crimes financeiros na era digital.

O objetivo é oferecer uma compreensão mais aprofundada das intersecções entre tecnologia, regulação e a luta contra o crime organizado, o terrorismo e a fraude.

2. Criptoativos: Fundamentos e Vulnerabilidades

Para uma compreensão robusta dos desafios regulatórios, é fundamental delinear a ontologia dos criptoativos e suas características intrínsecas.

2.1. Definição Legal e Ontológica

Para os fins da Lei nº 14.478, de 21 de dezembro de 2022, um ativo virtual é conceituado como uma "representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento" (BRASIL, 2022).

É mandatório, contudo, notar as exclusões explícitas desta definição legal (BRASIL, 2022), que visam diferenciar os ativos virtuais de outras formas de valor digital já regulamentadas ou com propósitos distintos:

> Moeda nacional e moedas estrangeiras [art. 3º, I].
>
> Moeda eletrônica, nos termos da Lei nº 12.865, de 9 de outubro de 2013 [art. 3º, II].
>
> Instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e [art. 3º, III].
>
> Representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros. [art. 3º, IV].

O Banco Central do Brasil (BCB), por sua vez, corrobora a definição de ativo virtual como uma representação digital de valor passível de negociação ou transferência eletrônica.

Embora a conceituação de ativos virtuais possa variar entre diferentes jurisdições, ela tipicamente se refere a uma representação digital de valor que pode ser transacionada ou transferida eletronicamente, caracterizando-se pela sua natureza não tangível e pela capacidade de desempenhar diversas funções econômicas, incluindo meio de troca, reserva de valor ou instrumento de investimento (BANCO CENTRAL DO BRASIL, 2024).

Nesse contexto, é comum que regulamentações internacionais excluam ativos já abrangidos por outras estruturas regulatórias financeiras (UNIÃO EUROPEIA, 2023).

2.2. Principais Características e Implicações

Os criptoativos distinguem-se das moedas fiduciárias por atributos intrínsecos que, embora inovadores, apresentam vulnerabilidades exploráveis para fins ilícitos:

2.2.1. Descentralização e Resistência à Censura

A ausência de um controle centralizado, seja por um banco central, instituição financeira ou outra autoridade, e sua operação em sistemas *peer-to-peer* (Entre Pares - P2P) ou redes globais de computadores, confere resiliência, mas também mitiga a supervisão tradicional.

No contexto acadêmico, Genc e Acikgoz (2025) destacam que a descentralização é frequentemente empregada como sinônimo de resistência à censura. Essa característica intrínseca de evitar o controle de terceiros ou esforços coordenados de terceiros torna a aplicação de modelos regulatórios tradicionais um desafio fundamental.

2.2.2. Pseudonimato, Anonimato e Paradoxo da Rastreabilidade

Embora as transações sejam imutavelmente registradas em um blockchain — um livro-razão público e transparente — as identidades dos usuários permanecem predominantemente pseudônimas.

Certos criptoativos, como Monero e Zcash, recorrem a técnicas sofisticadas de anonimização: o Monero utiliza assinaturas de anel, um mecanismo que mistura várias chaves digitais para ocultar a origem das transações, enquanto o Zcash emprega provas de conhecimento zero (zk-SNARKs) para validar transações sem revelar remetente, destinatário ou valores envolvidos, intensificando o anonimato e complicando sobremaneira o rastreamento da origem e destino dos fundos (KAPPOS et al, 2018).

Esse paradoxo reside no fato de que, apesar de todas as transações serem criptograficamente registradas e publicamente acessíveis, a pseudonimidade pode obscurecer a identificação dos atores reais. Miyamae e Matsuura (2020) destacam que múltiplos endereços de carteira podem ser criados sem verificação de identidade, conferindo um grau de anonimato que dificulta o rastreamento da trilha virtual do dinheiro.

2.2.3. Imutabilidade e Fungibilidade

Todas as transações são criptograficamente registradas no blockchain, tornando-as acessíveis publicamente e inalteráveis após a sua confirmação. Para Yaga et al. (2018), essa imutabilidade é um pilar da segurança blockchain.

Paradoxalmente, a fungibilidade (a intercambialidade das unidades de criptoativos) facilita a eficácia de misturadores de moedas e agitadores (*tumblers*), ferramentas empregadas para obscurecer a trilha transacional (MARIANI e HOMOLIAK, 2025).

Embora possam ter usos legítimos, esses serviços são amplamente empregados em lavagem de dinheiro, combinando e fragmentando transações para ocultar a origem e o destino dos fundos.

2.3. Classificação dos Criptoativos e Plataformas de Negociação

A categorização das moedas virtuais, baseada em sua conversibilidade com moeda legal, é crucial para identificar os riscos inerentes:

2.3.1. Moeda Virtual de Sistema Fechado

Caracteriza-se por não poder ser adquirida ou convertida em moeda de curso legal. A obtenção dessas moedas virtuais ocorre, em regra, por meio do engajamento do usuário, sendo concedidas como recompensa dentro de um ambiente digital específico e restrito à aquisição de bens virtuais.

Seu principal objetivo é incentivar a interação do consumidor com a plataforma e monetizá-lo por meio de vendas adicionais e estratégias publicitárias. Exemplos incluem as moedas leves (*soft*) de jogos, como o ouro do World of Warcraft, as moedas do FIFA21 e o dinheiro ($) do GTA V (SCHEIDEGGER e RAGHUBIR, 2022).

2.3.2. Moeda Virtual Unidirecional

Essa categoria caracteriza-se pela fungibilidade limitada entre usuários e conversão restrita para moeda oficial, frequentemente mediada por plataformas não regulamentadas.

Sua aquisição pode ocorrer por compra direta com moeda estatal ou de forma indireta, mediante gastos realizados em moeda oficial (SCHEIDEGGER e RAGHUBIR, 2022).

Exemplos brasileiros incluem: Milhas aéreas: Programas como MaxMilhas permitem a compra de passagens utilizando pontos Smiles, sem possibilidade de conversão em dinheiro. Jogos digitais: Plataformas como MafaCoin, do Mafagafo NFT, oferecem tokens adquiridos com reais, utilizáveis exclusivamente dentro do jogo. Programas de fidelidade: Iniciativas como o Méliuz oferecem cashback em reais, resgatáveis após atingir um valor mínimo.

2.3.3. Moeda Virtual Bidirecional

Apresenta maior semelhança com a moeda oficial, pois pode ser adquirida com moeda estatal e reconvertida para ela.

Scheidegger e Raghubir (2022) informam que embora não possua curso legal e não seja emitida por autoridade monetária, sua taxa de câmbio é flutuante, regulada pela oferta e demanda do mercado.

Destina-se à aquisição de bens e serviços, tanto virtuais quanto físicos, fora do sistema da entidade emissora. Três principais tipos incluem:

> - *Moeda econômica virtual:* Exemplificada por moedas utilizadas em jogos on-line, como o Robux do Roblox, que permitem aos jogadores adquirir itens e benefícios dentro do jogo, mas não têm valor fora desse ambiente.
>
> - *Moeda corporativa específica:* Um exemplo brasileiro é o WiBX, uma criptomoeda desenvolvida pela startup Wiboo, que permite aos usuários acumular pontos através de interações com marcas e convertê-los em produtos ou serviços de empresas parceiras.
>
> - *Criptomoedas:* Como o Bitcoin, que, embora tenha sido criado fora do Brasil, possui ampla aceitação em território nacional, sendo utilizado como meio de pagamento em diversos estabelecimentos e plataformas de negociação.

2.3.4. Exchanges Centralizadas e Descentralizadas (CEXs e DEXs)

Criptomoedas são transacionadas em plataformas de câmbio (*exchanges*), que se classificam em:

> - *Centralizadas (CEXs):* Operam sob a direção de uma autoridade central, que geralmente demanda o registro formal dos usuários e a verificação de sua identidade com o processo de Conheça Seu Cliente (KYC) (ZHOU, SHEN, 2022).
>
> - *Descentralizadas (DEXs):* Facilitam transações diretas P2P entre usuários, eliminando a necessidade de verificação centralizada, o que as torna significativamente mais difíceis de supervisionar e fiscalizar. A ausência de uma autoridade centralizada dificulta a implementação eficaz de requisitos regulatórios como a identificação e verificação dos clientes (KYC) e a prevenção à lavagem de dinheiro (AML) (ZHOU e SHEN, 2022).

3. Criptoativos e Ilícitos Financeiros

A natureza intrínseca dos criptoativos, marcada pela descentralização e a percepção de anonimato, os torna ferramentas particularmente atraentes para atividades criminosas.

3.1. Lavagem de Dinheiro e Financiamento do Terrorismo

O ciclo da lavagem de dinheiro é facilitado por criptoativos em suas três fases tradicionais:

> - *Colocação:* A conversão de fundos ilícitos em ativos virtuais via *exchanges* on-line (frequentemente em jurisdições com estruturas regulatórias baixas) permite contornar as redes bancárias tradicionais, dificultando a detecção. Plataformas de câmbio de criptomoedas, caixas eletrônicos de criptomoedas e plataformas de oferta inicial de moedas (ICOs) são exemplos de canais usados para a colocação.

- *Ocultação:* Criptoativos com técnicas avançadas de ofuscação, como Monero e Zcash, e a prática de mistura de moedas (*coin mixing*), tornam o rastreamento da origem e movimentação dos fundos consideravelmente mais complexo e de menor custo. Essa fase pode ser realizada por meio de protocolos de Finanças Descentralizadas (DeFi), serviços de mistura, provedores de carteira e emissores/desenvolvedores de moedas de privacidade (MARIANI e HOMOLIAK, 2025).

- *Integração:* Os fundos limpos são reintroduzidos na economia legítima, muitas vezes após a ofuscação do histórico transacional. Isso pode ocorrer através da venda de criptoativos por moeda oficial, compra de bens e serviços ou investimentos em setores tradicionais.

3.2. Riscos Críticos e Técnicas de Ofuscação

Os principais riscos e mecanismos de ofuscação incluem:

-*Anonimato e Pseudonimato:* A dificuldade de vincular pseudônimos a identidades reais permite a operação de atores mal-intencionados sem detecção.

-*Alcance Global e Lacunas Regulatórias:* A natureza transfronteiriça das criptomoedas permite a exploração de inconsistências e lacunas regulatórias entre jurisdições, facilitando a transferência de fundos para ambientes de supervisão mais fraca. Essa seleção regulatória é um desafio significativo, dada a implementação desigual das diretrizes internacionais.

-*Descentralização e Déficit de Supervisão:* Plataformas descentralizadas (DEXs), de acordo com Zhou e Shen (2022), operam sem autoridade central, obstaculizando a fiscalização e a aplicação de requisitos de KYC/AML. A própria essência da descentralização, entendida como resistência à censura, implica uma dificuldade inerente à supervisão tradicional.

-*Tecnologias de Melhoria de Privacidade:* Ferramentas como misturadores fragmentam e combinam transações, obscurecendo a origem e o destino dos fundos (MARIANI e HOMOLIAK, 2025). Para Loporchio et al. (2023), a fragmentação cripto ou "poeirinha digital" (*crypto dusting*) cria múltiplas trilhas minúsculas para confundir as autoridades.

3.3. Casos Notórios e Tendências Recorrentes

Diversos casos emblemáticos demonstram o papel crescente dos criptoativos em esquemas ilícitos, tanto no Brasil quanto globalmente:

-*Lavagem de Dinheiro:* Na Operação Symbolic, a Polícia Federal desarticulou um grupo sediado no RS que, entre 2019 e 2023, movimentou aproximadamente R$ 15

bilhões por meio de fraudes cambiais, evasão de divisas e lavagem em criptomoedas (POLÍCIA FEDERAL, 2024).

-*Financiamento do Terrorismo:* Em 2023, a Polícia Federal deflagrou a Operação Trapiche, mirando o financiamento de terrorismo no Brasil. A investigação aponta que, após sucessivas transferências entre contas de empresas de fachada, recursos ilícitos foram convertidos em criptoativos e destinados a carteiras sancionadas com vínculos a organizações terroristas (POLÍCIA FEDERAL, 2024).

-*Fraudes e Golpes:* A Operação Kryptos, conduzida pela PF, MPF e Receita Federal, expôs uma pirâmide financeira disfarçada de investimento em criptomoedas, responsável por movimentar cerca de R$ 38 bilhões entre 2015 e 2021 e causar prejuízo a mais de 62 mil investidores (POLÍCIA FEDERAL, 2021). Em 2024, golpes de alto rendimento foram as fraudes mais bem-sucedidas, com um aumento exponencial no uso de IA para criar personas falsas e conteúdo convincente, tornando os ataques mais escaláveis e difíceis de detectar. Plataformas como Huione Guarantee ilustram a profissionalização do ecossistema de golpes, oferecendo infraestrutura e serviços de lavagem de dinheiro (ELLIPTIC, 2025).

-*Software de sequestro digital (ransomware):* Em 2021, a JBS, maior processadora de carnes do mundo, sofreu um ataque de *ransomware* e concordou em pagar US$ 11 milhões em Bitcoin, com o objetivo de reduzir problemas relacionados à invasão e evitar o vazamento de dados (REUTERS, 2021). Embora os pagamentos de *ransomware* tenham diminuído 35% em 2024 devido a medidas de repressão e a colaboração internacional, as criptomoedas continuam no centro das extorsões. (CHAINALYSIS, 2025).

-*Mercado Negro e Web profunda (Dark Web):* Em 2019, uma operação internacional da Polícia Federal e do FBI combateu crimes praticados na Web profunda (Dark Web), que indexava mercados ilícitos para tráfico de drogas, armas, contrabando e lavagem de dinheiro, utilizando criptoativos para viabilizar transações (POLÍCIA FEDERAL, 2019).

-*Ataque Hacker ao Sistema Financeiro Brasileiro:* Em 2025, o maior ataque cibernético da história do país desviou cerca de R$ 1 bilhão de recursos mantidos na contas de reserva de uma *fintech* junto ao Banco Central, sendo que parte desses recursos foi convertida em Bitcoin e USDT (BRASIL, 2025).

4. Marcos Regulatórios: Brasil e Cenário Internacional

A resposta global aos desafios dos criptoativos tem sido multifacetada, com diferentes abordagens jurisdicionais.

4.1. Regulação Brasileira: Lei nº 14.478/2022

A Lei nº 14.478, de 21 de dezembro de 2022, constitui o pilar para a prestação de serviços de ativos virtuais no Brasil e a regulamentação das Prestadoras de Serviços de Ativos Virtuais (PSAVs).

É imperativo destacar que esta lei não abrange ativos representativos de valores mobiliários regidos pela Lei nº 6.385/1976 e não altera as competências da Comissão de Valores Mobiliários (BRASIL, 2022).

A operação de PSAVs no Brasil é condicionada à prévia autorização de um órgão ou entidade da Administração Pública federal. O Decreto nº 11.563, de 13 de junho de 2023, regulamentou a Lei nº 14.478/2022, atribuindo ao Banco Central do Brasil (BCB) a competência para regular, autorizar e supervisionar as PSAVs.

O BCB, portanto, é o órgão disciplinador e supervisor para os fins do Art. 6º da Lei nº 14.478/2022 (BRASIL, 2022).

As diretrizes que devem nortear a prestação de serviços de ativos virtuais (BRASIL, 2022), segundo parâmetros a serem estabelecidos pelo BCB, incluem:

> Livre iniciativa e livre concorrência; [art. 4º, I]
>
> Boas práticas de governança, transparência nas operações e abordagem baseada em riscos; [art. 4º, II]
>
> Segurança da informação e proteção de dados pessoais; [art. 4º, III]
>
> Proteção e defesa de consumidores e usuários; [art. 4º, IV]
>
> Proteção à poupança popular; [art. 4º, V]
>
> Solidez e eficiência das operações; e [art. 4º, VI]
>
> Prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais. [art. 4º,VIII]

Uma Prestadora de Serviços de Ativos Virtuais (PSAV) é definida como uma pessoa jurídica que executa, em nome de terceiros, pelo menos um dos seguintes serviços de ativos virtuais (BRASIL, 2022):

> Troca entre ativos virtuais e moeda nacional ou moeda estrangeira; [art. 5º, I]
>
> Troca entre um ou mais ativos virtuais; [art. 5º, II]
>
> Transferência de ativos virtuais; [art. 5º, III]

> Custódia ou administração de ativos virtuais ou de instrumentos que possibilitem controle sobre ativos virtuais; ou [art. 5º, IV]
>
> Participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais. [art. 5º, V]

As atribuições do BCB consolidam seu papel como regulador central do segmento, assegurando governança, integridade e conformidade com padrões de mercado e prevenção a ilícitos.

As Resoluções BCB (Nº 519/2025, 520/2025 e 521/2025) visam detalhar a regulamentação, estabelecendo requisitos de capital social para PSAVs e padronizando processos de autorização, além de focar na regulamentação de transferências internacionais envolvendo ativos virtuais denominados em reais (BANCO CENTRAL DO BRASIL, 2025).

A legislação penal brasileira foi alterada pela Lei nº 14.478/2022, que criminaliza a fraude com utilização de ativos virtuais, valores mobiliários ou ativos financeiros com pena de reclusão de 4 a 8 anos e multa (BRASIL, 2022).

As PSAVs foram explicitamente incluídas no rol de entidades que devem manter registro de transações que ultrapassem limites específicos, e a pena de lavagem de dinheiro é aumentada em caso de reincidência, atuação de organização criminosa ou uso de ativo virtual.

Além disso, as PSAVs deverão consultar o Cadastro Nacional de Pessoas Expostas Politicamente (PEP) em seus procedimentos de registro e comunicação de operações suspeitas.

A proteção ao consumidor é garantida, com a aplicação do Código de Defesa do Consumidor e exigência de transparência e informação clara por parte das PSAVs.

4.2. Abordagens Internacionais e Modelos Comparados

A reação global aos desafios impostos pelos criptoativos tem revelado abordagens distintas e desafios de harmonização.

4.2.1. FATF (Financial Action Task Force)

Instituído em 1989, o FATF é o órgão intergovernamental primordial que estabelece padrões globais para combater a lavagem de dinheiro (AML) e o financiamento do terrorismo (CFT).

A Recomendação 15 do FATF estendeu seus padrões para incluir ativos virtuais e prestadores de serviços de ativos virtuais (PSAVs), impondo requisitos de licenciamento/registro, *due diligence* de clientes (CDD), monitoramento de transações e relatórios de atividades suspeitas (FATF, 2025).

A Regra de Viagem (*Travel Rule*), embora de implementação inconsistente, exige que os PSAVs compartilhem informações sobre transações, sendo que a política Conheça seu Cliente (KYC), que proíbe contas anônimas, é um pilar das exigências AML (FATF, 2025).

Contudo, a FATF, ao focar na extensão do modelo tradicional de controle baseado em intermediários, enfrenta limitações na aplicabilidade a sistemas verdadeiramente descentralizados, forçando uma extensão que é incompatível com a estrutura do blockchain.

Apesar dos esforços, 75% das jurisdições pesquisadas permanecem apenas parcialmente ou não conformes, indicando dificuldades em avaliar riscos e promulgar legislação adequada (FATF, 2025).

4.2.2. União Europeia: AMLDs, MiCA e TFR

Adotou uma abordagem centralizada com as Diretivas Anti-Lavagem de Dinheiro (AMLDs). A 5ª AMLD expandiu o escopo para incluir *exchanges* de criptomoedas e provedores de carteiras de custódia como entidades obrigadas, sujeitando-os a medidas de *due diligence* de clientes (CDD) e monitoramento de transações (UNIÃO EUROPEIA, 2018).

Para a União Europeia (2023), o Regulamento MiCA (*Markets in Crypto-Assets Regulation*) visa criar uma estrutura de desenvolvimento abrangente para mercados de criptoativos não cobertos pela legislação existente. No entanto, MiCA explicitamente exclui serviços oferecidos de forma totalmente descentralizada sem qualquer intermediário.

O Regulamento TFR (*Traceability of Transfer of Funds Regulation*) foi alterado para estender a provisão de informações a PSAVs e transações entre criptomoedas, garantindo a rastreabilidade (UNIÃO EUROPEIA, 2023).

4.2.3. Estados Unidos

Adotam uma abordage]m multiagência.

4.2.3.1. FinCEN

A Financial Crimes Enforcement Network (FinCEN) é uma agência do Departamento do Tesouro e classifica *exchanges* de criptomoedas como negócios de serviços monetários (MSBs), exigindo conformidade com rígidos protocolos KYC e AML (FINCEN, 2019).

A FinCEN (2019) adota uma abordagem tecnologicamente neutra, focando na atividade de transmissão de dinheiro e intensificando o escrutínio sobre serviços de mistura, embora reconheça

que entidades que fornecem serviços de infraestrutura para emissão e negociação de criptomoedas podem estar fora do escopo das regulamentações AML.

4.2.3.2. SEC

A Comissão de Valores Mobiliários (SEC, na sigla em inglês) regula ofertas iniciais de moedas (ICOs) e os criptoativos considerados valores mobiliários, adotando uma política de "regulação por execução" (*regulation by enforcement*), e classificando muitos desses ativos como valores mobiliários segundo o teste de Howey[2] (KAZIMIROV, 2025).

Essa abordagem é criticada por criar ambiguidade e incerteza legal para a indústria, contrastando com a necessidade de uma estrutura regulatória clara e previsível. Expandindo a crítica, decisões judiciais como *Jarkesy v. SEC*[3] e *Loper Bright*[4] limitaram os poderes executivos da agência, reforçando o espaço para contestação jurídica e tornando o regime atual de execução estruturalmente instável. Isso gera incerteza para os agentes regulados e, consequentemente, aumenta os custos de conformidade regulatória e os incentivos à fuga regulatória.

4.2.3.3. CFTC

A Comissão de Negociação de Futuros de Commodities (CFTC), além de supervisionar os derivativos tradicionais, exerce papel central na regulação dos derivativos de criptomoedas, como contratos futuros, opções e *swaps* baseados em ativos digitais tais como Bitcoin e Ethereum.

A agência classifica essas criptomoedas como commodities, segundo o *Commodity Exchange Act* (CEA), supervisionando diretamente as operações desses instrumentos, além de conduzir investigações e ações contra fraudes ou manipulação no mercado de derivativos de criptomoedas (UNITED STATES, 2018).

4.2.3.4. OCC

A Office of the Comptroller of the Currency (2025) é uma agência independente vinculada ao Departamento do Tesouro dos Estados Unidos, desempenha papel crucial na regulamentação

[2] Teste de Howey é uma ferramenta legal usada para determinar se um ativo deve ser classificado como valor mobiliário. Mais detalhes podem ser encontrados no site da SEC: https://www.sec.gov/newsroom/speeches-statements/statement-stablecoins-040425

[3] UNITED STATES. SUPREME COURT. Nº. 22–859. MICHELLE JARKESY, ET AL., PETITIONERS v. SECURITIES AND EXCHANGE COMMISSION. Washington, DC, 27 jun. 2024. Disponível em: https://www.supremecourt.gov/opinions/23pdf/22-859_1924.pdf. Acesso em: 13 jul. 2025.

[4] UNITED STATES. SUPREME COURT. Nº. 22–451. LOPER BRIGHT ENTERPRISES, INC., ET AL., PETITIONERS v. RAIMONDO, SECRETARY OF COMMERCE, ET AL. Washington, DC, 28 jun. 2024. Disponível em: https://www.supremecourt.gov/opinions/23pdf/22-451_7m58.pdf. Acesso em: 13 jul. 2025.

e supervisão de bancos nacionais, associações federais de poupança e filiais de bancos estrangeiros. Historicamente, o OCC tem buscado equilibrar a inovação financeira com a proteção do sistema bancário.

Recentemente, o órgão tem adotado uma postura mais favorável à integração de ativos digitais, permitindo que instituições financeiras sob sua supervisão ofereçam serviços relacionados a criptomoedas (OCC, 2025).

Essa abordagem visa facilitar a convergência entre o sistema financeiro tradicional e as tecnologias emergentes, ao mesmo tempo em que assegura a implementação de controles robustos de risco e conformidade regulatória (OCC, 2025).

5. Limitações Regulatórias e Desafios de Implementação

Apesar dos esforços regulatórios crescentes, persistem obstáculos significativos na implementação eficaz do combate à lavagem de dinheiro (LD) e ao financiamento do terrorismo (FT) no ecossistema de criptoativos.

5.1. Inconsistências Internacionais e Lacunas de Cooperação

- *Inconsistência e Lacunas Regulatórias:* A divergência das regulamentações nacionais cria oportunidades para uma seleção regulatória, onde criminosos exploram as jurisdições com supervisão mais branda. Com efeito, a falta de padronização ainda impede a eficácia plena da cooperação internacional (MANNINEN, 2023).

- *Dificuldade de Cooperação Transfronteiriça:* A natureza global das transações e as diferentes interpretações das leis de AML dificultam a colaboração internacional eficaz e a coordenação de informações (LEUPRECHT, et al., 2023).

5.2. Barreiras Operacionais e Tecnológicas

- *Custos de Conformidade Elevados:* Os requisitos de capital e patrimônio, bem como as exigências de Conheça Seu Cliente (KYC) e Prevenção à Lavagem de Dinheiro (AML), podem gerar altos custos de conformidade, especialmente para *startups* e pequenas empresas. Isso, paradoxalmente, pode empurrar atividades ilícitas para canais ainda menos regulamentados ou para jurisdições menos rigorosas, sufocando a inovação legítima (DRYLEWSKI, et al., 2025).

- *Anonimato e Tecnologias de Melhoria de Privacidade (PETs):* Criptomoedas focadas em privacidade, como Monero e Zcash, continuam a minar os esforços de rastreamento, dificultando a vinculação de pseudônimos a identidades reais (DYSON, et al., 2019).

- *Limitações Técnicas de Congelamento de Ativos e Eficácia das Sanções:* A natureza descentralizada do ecossistema cripto torna o bloqueio ou congelamento de ativos digitais complexo e, em alguns casos, inviável. Sanções funcionam mais como impedimentos do que como mecanismos de bloqueio direto, e a ausência de um registro centralizado de propriedade é um desafio no confisco de fundos ligados a atividades criminosas.

Drylewski et al. (2025) indicam que cerca de metade das entidades sancionadas continuam a movimentar fundos via endereços Bitcoin sancionados, sugerindo uma preferência por táticas mais diretas (como conversão em *exchanges*) em vez de métodos sofisticados de lavagem

O caso Tornado Cash exemplifica essa dificuldade: apesar das sanções e ações legais, seus contratos inteligentes descentralizados permitiram que continuasse operando, com suas entradas aumentando 108% em 2024. A *blacklisting* de endereços é ineficaz, pois carteiras podem ser criadas ilimitadamente sem supervisão central (NADLER e SCHÄR, 2023).

5.3. Stablecoins: Lacunas, Riscos Sistêmicos e Propostas

Além da lacuna na regulamentação específica de *stablecoins*, amplamente utilizadas, e setores como misturadores, mineradores e *traders* que muitas vezes não são adequadamente cobertos, apesar de representarem riscos significativos (BENSON et al., 2024), é crucial aprofundar a discussão sobre os riscos sistêmicos e regulatórios específicos das *stablecoins*.

- *Riscos Sistêmicos e de Liquidez:* Para Aldasoro et al. (2024), estudos do Banco de Compensações Internacionais (BIS) mostram que as *stablecoins* funcionam de forma similar a fundos do mercado monetário, estando sujeitas a riscos de liquidez e retiradas em massa. Gráficos de volatilidade que utilizam *wavelets*, segundo Moura de Carvalho et al. (2025), demonstram padrões de co-movimento entre *stablecoins* e crises macroeconômicas (como COVID-19, Terra-Luna e o colapso do Silicon Valley Bank).

- *Risco de Contágio e Impacto no Sistema Bancário:* O Banco de Compensações Internacionais (BIS) alerta para o risco de contágio via venda forçada de ativos lastreados, a exemplo do Tether. Um artigo de economistas de tecnologia confirma que ajustes nos colaterais de *stablecoins* influenciam os mercados tradicionais (AHMED, et al., 2024).

- *Uso Ilícito e Lacunas de Conformidade:* As *stablecoins* permanecem vulneráveis a canais de lavagem de dinheiro devido à falta de mecanismos robustos de KYC e ao anonimato nas transações (FMI, 2023). Para mitigar esses riscos, propõe-se a implementação de uma execução híbrida de conformidade, integrando processos de AML/CFT realizados dentro e fora da *blockchain*, aliado à certificação independente de conformidade.

- *Propostas de Regulação e Política de Reservas:* O Instituto de Estabilidade Financeira (FSI) do Banco de Compensações Internacionais argumenta que as *stablecoins* devem cumprir requisitos de licenciamento, reservas auditadas, capital mínimo, ciber-resiliência e conformidade AML/CFT (CRISANTO, et al., 2024). Além disso, Wen et al. (2025) propõem modelos híbridos, como *stablecoins* privadas lastreadas em reservas do banco central tipo CBDC.

5.4. Volatilidade do Setor e Viés de Recência

A indústria de Finanças Descentralizadas (DeFi) é excessivamente volátil e prematura, o que dificulta a produção de pesquisas com validade de longo prazo e pode levar a um viés de recência. Para Zhuk (2025), as constantes mudanças no ecossistema tornam o desenvolvimento regulatório um alvo em movimento.

6. Estratégias para o Fortalecimento da Governança de Criptoativos

Para enfrentar os desafios dos crimes financeiros facilitados por criptoativos, é imperativa uma abordagem multifacetada e coordenada, que combine esforços tradicionais com a exploração de soluções tecnológicas inovadoras.

6.1. Cooperação e Harmonização Global

O FATF desempenha um papel central na promoção de padrões AML/CFT consistentes. A criação do Grupo Egmont de Unidades de Inteligência Financeira (UIFs) facilita a troca de informações entre 174 UIFs.

Contudo, a falta de padronização ainda impede a eficácia plena, de modo que a harmonização de padrões e regulamentações entre jurisdições é crucial para maximizar a eficácia e limitar a arbitragem regulatória.

A FATF poderia evoluir para um executor global de conformidade AML em cripto, estabelecendo padrões técnicos vinculantes para análise de blockchain e monitoramento de transações, além de estabelecer um registro global de transações suspeitas para automatizar verificações de conformidade.

6.2. Inovação Tecnológica e Supervisão Inteligente

A integração de ferramentas avançadas é crucial para aprimorar a capacidade regulatória e de execução das leis.

6.2.1. Blockchain Analytics e Inteligência Artificial

Plataformas como Chainalysis e Elliptic, baseadas em IA, auxiliam reguladores e agências na detecção de padrões suspeitos, rastreamento de transações ilícitas e identificação de atores mal-intencionados.

A Chainalysis, por exemplo, oferece soluções de detecção de fraude alimentadas por IA e inteligência de blockchain para melhorar a prevenção e aplicação. De acordo com Ananth e Mittal (2024), o uso de modelos preditivos, como os da Hexagate (adquirida pela Chainalysis), permite a detecção em tempo real de riscos e ameaças, prevenindo ataques cibernéticos antes que ocorram.

6.2.2. Supervisão Embutida (Embedded Supervision)

O uso de tecnologias digitais para conformidade regulatória pode reduzir custos e erros, permitindo a supervisão simultânea de múltiplas entidades e a rápida identificação de riscos.

Um conceito-chave nesse domínio é a supervisão embutida, que se refere à incorporação de pontos de acesso para autoridades reguladoras diretamente na infraestrutura de software blockchain de uma infraestrutura financeira descentralizada ou centralizada (ÇAĞLAYAN AKSOY, 2024).

Isso permitiria que a autoridade reguladora realizasse certas ações diretamente na infraestrutura subjacente aos produtos e atividades regulamentadas.

6.2.2.1. Desafios de Governança e Interoperabilidade

A implementação da supervisão embutida enfrenta desafios significativos.

- *Governança e Interoperabilidade Regulatória:* Para Arner et al. (2020), exige estruturas claras de decisão em casos críticos (como reversão de transações ou bloqueios de ativos) e destaca a necessidade de mapeamento de competências entre jurisdições, uso de Contratos Inteligentes com mecanismos de parada de emergência e fomento a consórcios regulatórios multilaterais (como o BIS e o FMI) para testar estruturas interoperáveis.

- *Técnicos Operacionais:* Incluem múltiplas versões de Contratos Inteligentes, divergências entre provedores de dados externos centralizados e descentralizados, anonimato de usuários e padrões de dados inconsistentes. Para superar isso, de acordo com Arner et al. (2020), são necessários:

  - Desenvolvimento de protocolos padronizados para provedores de dados externos regulamentados;

- Auditorias de segurança periódicas por terceiros especializados;
- Infraestrutura resiliente com testes formais de verificação.

- *Comprometimento de Recursos e Know-how:* A implementação em larga escala exige um comprometimento significativo de recursos e *know-how* técnico por parte dos reguladores, que atualmente carecem disso. Há também uma hesitação em assumir a responsabilidade direta pela coleta e verificação de dados, historicamente atribuída aos intermediários (ARNER, et al., 2020).

6.2.2.2. Estratégias de Implementação

Estratégias para superação desses desafios incluem.

- *Pilotos Regulatórios:* A Autoridade Monetária das Bermudas (BMA) recebeu diversas propostas até abril de 2025 para testar a supervisão embutida em plataformas DeFi, permitindo monitoramento automático de *compliance* via Contratos Inteligentes.

- *Colaboração Público-Privada:* Seguindo a proposta de Arner, Auer e Frost (2020), propõe-se uma sinergia entre reguladores, indústria e academia para a formulação conjunta de padrões técnicos de supervisão embutida.

- *Estruturas de Dados Auditáveis em Blockchain:* Modelos como o de Bluhm et al. (2024) sugerem formatos que garantem transparência e privacidade, com monitoramento em tempo real das reservas e passivos de *stablecoins*.

6.2.2.3. Mecanismos de Ação: Monitoramento e Fiscalização

A supervisão embutida pode se manifestar de diversas formas.

- *Monitoramento Passivo (Tempo Real):* Acesso verificável a dados selecionados (*on-chain*) ou posições consolidadas, mesmo que confidenciais a terceiros. Em *blockchains* públicas, isso já é possível, mas aprimorar a capacidade de leitura e análise de dados *on-chain* pelos reguladores é fundamental (MAFRUR, 2025).

- *Alimentação de Dados:* Permite que autoridades forneçam dados à infraestrutura, como taxas de juros relevantes ou, mais criticamente, listas negras para bloquear partes sancionadas de transações (ZHOU, 2025). A indústria cripto poderia ser receptiva a provedores de dados externos regulatórios que implementem *blacklists* oficiais.

- *Poderes de Fiscalização Ativa:* Embora o mais intrusivo, poderia permitir ações diretas, como o congelamento de ativos ou reversão de transações em casos de atividades ilícitas (ZHOU, 2025). No entanto, isso desafia a natureza de imutabilidade do *blockchain* e a preferência por anonimato dos usuários.

6.2.2.4. Identificação e Privacidade: ZKP e Soulbound Tokens

A questão da identificação e da identidade digital é crucial.

- *Provas de Conhecimento Zero (ZKP):* Ferramentas criptográficas modernas, como ZKP, permitem verificar informações (ex: aprovação em verificação AML) sem revelar a identidade real do usuário, equilibrando a necessidade regulatória de identificação com a demanda por privacidade (KUMARA et al, 2023).

- *Tokens intransferíveis (soulbound tokens):* NFTs não transferíveis que contêm informações de identificação são vistos como uma ferramenta promissora para o gerenciamento de identidade em uma estrutura regulatória (GOLDSTON et al, 2024).

6.2.2.5. Desafios de Implementação da Supervisão Embutida

A implementação em larga escala exige um comprometimento significativo de recursos e *know-how* técnico por parte dos reguladores, que atualmente carecem disso.

Há também uma hesitação em assumir a responsabilidade direta pela coleta e verificação de dados, historicamente atribuída aos intermediários.

Contudo, à medida que as Finanças Descentralizadas (DeFi) crescem, a supervisão embutida pode se tornar mais relevante no futuro (BABEL e SEDLMEIR, 2023).

6.3. Colaboração Público-Privada e Capacitação Técnica

A colaboração entre governos, instituições financeiras e empresas de tecnologia é essencial para o compartilhamento de informações e desenvolvimento de melhores práticas.

É essencial capacitar as autoridades no rastreamento de criptomoedas para enfrentar com eficácia as novas ameaças, especialmente diante da atual deficiência no domínio dessa tecnologia.

6.4. Educação e Conscientização do Público

Campanhas de educação e conscientização são cruciais para informar os consumidores sobre os riscos e benefícios dos criptoativos, e para capacitá-los na identificação e prevenção de golpes.

O crescimento de golpes cada vez mais sofisticados, combinados ao uso de criptomoedas em fraudes, evidencia a urgência de fortalecer mecanismos regulatórios e ampliar a conscientização pública.

6.5. Regulação do Elemento Humano e Inovação

A questão de quem regular em sistemas verdadeiramente descentralizados, onde os intermediários são eliminados, permanece um desafio fundamental. Mirar os desenvolvedores de código para fins regulatórios é uma ladeira escorregadia que pode sufocar a inovação e o desenvolvimento de novas ideias.

A legislação deve atingir um equilíbrio estratégico entre fomentar a inovação e assegurar a segurança, evitando uma regulamentação excessiva que possa sufocar o desenvolvimento legítimo do setor ou, inversamente, impulsionar atividades ilícitas para canais ainda mais obscuros.

A clareza regulatória é mais importante do que a estrita regulação para o crescimento do setor.

CONCLUSÃO

A regulamentação dos criptoativos, notadamente a Lei nº 14.478/2022 no Brasil e as diretrizes internacionais, representa um esforço global para equilibrar a inovação tecnológica com a segurança e a integridade financeira.

A natureza descentralizada e pseudônima dos criptoativos, embora inovadora, favorece a lavagem de dinheiro, o financiamento ao terrorismo e diversas fraudes. Paradoxalmente, as mesmas tecnologias que habilitam essas práticas, como blockchain e inteligência artificial, também proporcionam ferramentas robustas para combatê-las.

A atribuição de competências ao Banco Central do Brasil para regular e supervisionar as PSAVs reflete um alinhamento com as melhores práticas internacionais, visando à proteção do consumidor e à solidez do mercado.

As alterações na legislação penal brasileira, que criminalizam a fraude com ativos virtuais e aumentam as penas para lavagem de dinheiro, representam avanços significativos na coibição do uso ilícito dessas tecnologias.

No entanto, os desafios de implementação permanecem consideráveis, incluindo as inconsistências regulatórias entre jurisdições, a dificuldade intrínseca em congelar ativos digitais devido à descentralização, e a complexidade de rastrear transações que se movem rapidamente através de redes que podem oferecer anonimato.

A eficácia das sanções ainda é um ponto de atenção, com a persistência de movimentação de fundos por entidades sancionadas.

Em uma projeção futura, a colaboração internacional contínua, o investimento ininterrupto em tecnologias avançadas de análise e rastreamento (como a análise de blockchain e IA/ML), o aprimoramento de programas de treinamento para autoridades e a expansão de campanhas de conscientização pública serão elementos cruciais para aprimorar o ambiente regulatório e operacional.

A exploração e eventual adoção de ferramentas como a supervisão embutida, que permitem o monitoramento e a fiscalização de sistemas descentralizados sem a necessidade de intermediários tradicionais, são promissores, embora exijam significativo investimento em recursos e *expertise* por parte dos reguladores.

É essencial que as regulamentações encontrem um equilíbrio estratégico entre incentivar a inovação e garantir a segurança, evitando tanto a imposição de regras excessivas que possam sufocar o desenvolvimento legítimo do setor, quanto a ausência de regulamentação que possa direcionar atividades ilícitas para canais ainda mais obscuros.

A participação proativa da sociedade, o monitoramento contínuo e a adaptabilidade às novas exigências do mercado são indispensáveis para o sucesso da regulamentação no ecossistema de ativos virtuais.

Assim, a transparência regulatória e a clareza sobre o que constitui um sistema verdadeiramente descentralizado são, e continuarão a ser, pilares para o avanço responsável da inovação financeira digital.

REFERÊNCIAS

BRASIL. *Lei nº 14.478, de 21 de dezembro de 2022*. **Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais.** Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm. Acesso em: 13 jul. 2025.

BRASIL. Agência. **PF investigará ataque hacker a empresa que atende bancos**. Brasília, DF, 09 jul. 2025. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2025-07/pf-investigara-ataque-hacker-empresa-que-atende-bancos. Acesso em: 09 jul. 2025.

AHMED, Rashad; ALDASORO, Iñaki; DULEY, Chanelle. **Public information and stablecoin runs**. *BIS Working Papers*, n. 1164, jan. 2024 (rev. jan. 2025). Disponível em: https://www.bis.org/publ/work1164.htm. Acesso em: 13 jul. 2025.

ALDASORO, Iñaki et al. **Stablecoins, money market funds and monetary policy**. *BIS Working Papers*, n. 1219, out. 2024. Disponível em: https://www.bis.org/publ/work1219.pdf. Acesso em: 04 jul. 2025.

BABEL, Matthias; SEDLMEIR, Johannes. **Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs.** arXiv, 3 nov. 2023. Disponível em: https://arxiv.org/abs/2301.00823. Acesso em: 10 jul. 2025.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 520, de 2025.** Disciplina a constituição e o funcionamento das sociedades prestadoras de serviços de ativos virtuais e a prestação de serviços de ativos virtuais por outras instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=520. Acesso em: 07 dez. 2025.

BENSON, Vladlena et al. **Harmonising Cryptocurrency Regulation in Europe: Opportunities for Preventing Illicit Transactions**. *European Journal of Law and Economics*, v. 57, n. 1-2, p. 37-61, abr. 2024. DOI: 10.1007/s10657-024-09797-w. Disponível em: https://repository.lboro.ac.uk/articles/journal_contribution/Harmonising_cryptocurrency_regulation_in_Europe_opportunities_for_preventing_illicit_transactions/25447015. Acesso em: 12 jul. 2025.

BLUHM, Marcel et al. **Real-time Risk Metrics for Programmatic Stablecoin Crypto Asset-Liability Management (CALM).** *arXiv*, 24 jan. 2024. Disponível em: https://arxiv.org/abs/2401.13399. Acesso em: 13 jul. 2025.

CHAINALYSIS, Inc. **The 2025 Crypto Crime Report**. [S.l.]: Chainalysis, mar. 2025. Disponível em: https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf. Acesso em: 09 jul. 2025.

CRISANTO, Juan Carlos; EHRENTRAUD, Johannes; GARCIA OCAMPO, Denise. **Stablecoins: regulatory responses to their promise of stability**. *FSI Insights on policy implementation*, n. 57, abr. 2024. Disponível em: https://www.bis.org/fsi/publ/insights57.htm. Acesso em: 13 jul. 2025.

DRYLEWSKI, Alexander C.; EVANGELISTA, Alessio D.; COHEN, Adam J. Keeping crypto clean: risk-based controls for stablecoins. **Reuters Legal News**, 24 jun. 2025. Disponível em: https://www.reuters.com/legal/legalindustry/keeping-crypto-clean-risk-based-controls-stablecoins-2025-06-24/. Acesso em: 12 jul. 2025.

DYSON, Simon; BUCHANAN, William J.; BELL, Liam. **The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime.** *arXiv*, 29 jul. 2019. Disponível em: https://arxiv.org/abs/1907.12221. Acesso em: 12 jul. 2025.

ELLIPTIC. Huione: **The company behind the largest ever illicit online marketplace has launched a stablecoin**. *Elliptic Research Blog*, 14 jan. 2025. Disponível em: https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin. Acesso em: 09 jul. 2025.

FINANCIAL CRIMES ENFORCEMENT NETWORK – FINCEN. **Advisory on Illicit Activity Involving Convertible Virtual Currency.** Advisory FIN-2019-A003, 9 maio 2019. FinCEN, 2019. Disponível em: https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf. Acesso em: 10 jul. 2025.

FINANCIAL ACTION TASK FORCE (FATF). **The FATF Recommendations**. Paris: FATF, jun. 2025. Disponível em: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html. Acesso em: 12 jul. 2025.

FUND INTERNATIONAL MONETARY. **Review of The Fund's Anti-Money Laundering and Combating The Financing of Terrorism Strategy.** Washington, D.C.: International Monetary Fund, 5 dez. 2023. Disponível em: https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015. Acesso em: 13 jul. 2025.

GENC, Huseyin Oguz; ACIKGOZ, Eray. **Constructing an Evaluation Framework for Full Decentralization**: A Case Study on DeFi's Stable Currency Issuance Services – CDP Protocols. *Stanford Journal of Blockchain Law & Policy*, [S.l.], 2025. Disponível em: https://stanford-jblp.pubpub.org/pub/cdp-protocols. Acesso em: 09 jul. 2025.

GOLDSTON, Justin et al. Digital Inheritance in Web3: **A Case Study of Soulbound Tokens and the Social Recovery Pallet within the Polkadot and Kusama Ecosystems.** *arXiv*, 6 jun. 2024. Disponível em: https://arxiv.org/abs/2301.11074. Acesso em: 12 jul. 2025.

KAPPOS, George et al. **An empirical analysis of anonymity in Zcash.** In: *Proceedings of the 27th USENIX Security Symposium*, Baltimore, MD, USA, 15–17 ago. 2018. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf. Acesso em: 12 jul. 2025.

KAZIMIROV, Alexandros G. **Regulation by Enforcement: A Retrospective of the SEC's Vision for Digital Assets and an Alternative European Model**. *Stanford Journal of Blockchain Law & Policy*, v. 8, n. 2, 30 jun. 2025. Disponível em: https://stanford-jblp.pubpub.org/pub/regulation-by-enforcement/release/1. Acesso em: 10 jul. 2025.

KUMARA, Bryan et al. **Redactable Signature Schemes and Zero-knowledge Proofs: A comparative examination for applications in Decentralized Digital Identity Systems**. *arXiv*, 24 out. 2023. Disponível em: https://arxiv.org/abs/2310.15934. Acesso em: 12 jul. 2025.

LEUPRECHT, Christian; JENKINS, Caitlyn; HAMILTON, Rhianna. **Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency.** *Journal of Financial Crime*, v. 30, n. 4, p. 1036–1054, maio 2023. DOI: 10.1108/JFC-07-2022-0161. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/jfc-07-2022-0161/full/html. Acesso em: 12 jul. 2025.

LOPORCHIO, Matteo et al. **Is Bitcoin gathering dust? An analysis of low-amount Bitcoin transactions.** *Applied Network Science*, v. 8, n. 1, art. 34, 15 jun. 2023. DOI: 10.1007/s41109-023-00557-4. Disponível em: https://doi.org/10.1007/s41109-023-00557-4. Acesso em: 12 jul. 2025.

MAFRUR, Rischan. **Blockchain Data Analytics: Review and Challenges**. *arXiv*, 12 mar. 2025. Disponível em: https://arxiv.org/abs/2503.09165. Acesso em: 12 jul. 2025.

MANNINEN, Heidimaria. **The Anti-money Laundering Challenges of FinTech and Cryptocurrencies.** *Nordic Journal of Legal Studies*, v. 1, n. 2023, art. 26, 2023. DOI: 10.51421/njls-2023-0026. Disponível em: https://njls.eu/index.php/journal/article/download/26/24/49. Acesso em: 12 jul. 2025.

MARIANI, Juraj; HOMOLIAK, Ivan. SoK: **A Survey of Mixing Techniques and Mixers for Cryptocurrencies**. *arXiv*, 28 abr. 2025. Disponível em: https://arxiv.org/abs/2504.20296. Acesso em: 12 jul. 2025.

MIYAMAE, Takeshi; MATSUURA, Kanta. **Privacy Analysis and Evaluation Policy of Blockchain-based Anonymous Cryptocurrencies**. *arXiv*, v. 2012.10563, 19 dez. 2020. DOI:10.48550/arXiv.2012.10563. Disponível em: https://arxiv.org/abs/2012.10563. Acesso em: 13 jul. 2025.

MOURA DE CARVALHO, Rubens; INÁCIO, Helena Coelho; MARQUES, Rui Pedro. **Stablecoin: A Story of (In)Stabilities and Co-Movements Written Through Wavelet.** *Journal of Risk and Financial Management*, v. 18, n. 1, art. 20, 2025. DOI: 10.3390/jrfm18010020. Disponível em: https://www.mdpi.com/1911-8074/18/1/20. Acesso em: 13 jul. 2025.

NADLER, Matthias; SCHÄR, Fabian. **Tornado Cash and Blockchain Privacy:** A Primer for Economists and Policymakers. *Federal Reserve Bank of St. Louis Review*, v. 105, n. 2, p. 122–136, abr. 2023. DOI: 10.20955/r.105.122-136. Disponível em: https://www.stlouisfed.org/publications/review/2023/02/03/tornado-cash-and-blockchain-privacy-a-primer-for-economists-and-policymakers. Acesso em: 13 jul. 2025.

POLÍCIA FEDERAL. P**F deflagra a segunda fase da Operação Trapiche**. Brasília, DF, 08 ago. 2024. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2024/08/pf-deflagra-a-segunda-fase-da-operacao-trapiche. Acesso em: 09 jul. 2025.

POLÍCIA FEDERAL. **PF deflagra operação contra evasão de divisas e lavagem de dinheiro por meio de criptoativos e fraudes cambiais**. Santana do Livramento, RS, 07 fev. 2024. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2024/02/pf-deflagra-operacao-contra-evasao-de-divisas-e-lavagem-de-dinheiro-por-meio-de-criptoativos-e-fraudes-cambiais. Acesso em: 09 jul. 2025.

POLÍCIA FEDERAL. **PF desarticula esquema de fraudes bilionárias envolvendo criptomoedas**. Rio de Janeiro, RJ, 25 ago. 2021. Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2021/08/pf-desarticula-esquema-de-fraudes-bilionarias-envolvendo-criptomoedas. Acesso em: 09 jul. 2025.

POLÍCIA FEDERAL**. PF e FBI combatem a prática de crimes na internet e Dark Web**. Brasília, DF, 30 mai. 2019. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2019/05/pf-e-fbi-combatem-a-pratica-de-crimes-na-internet-e-dark-web. Acesso em: 09 jul. 2025.

REUTERS. **Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack.** [S.l.], 09 jun. 2021. Disponível em: https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/. Acesso em: 09 jul. 2025.

SCHEIDEGGER, Gianluca; RAGHUBIR, Priya. **Virtual currencies: different schemes and research opportunities**. *Marketing Letters*, v. 33, n. 2, p. 351–360, jun. 2022. DOI: 10.1007/s11002-022-09620-z. Disponível em: https://link.springer.com/article/10.1007/s11002-022-09620-z. Acesso em: 01 jul. 2025.

UNITED STATES. Commodity Futures Trading Commission (CFTC). **Bitcoin Basics**. fev. 2018. Disponível em: https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf. Acesso em: 12 jul. 2025.

UNIÃO EUROPEIA. **Directive (EU) 2018/843, de 30 maio 2018, que altera a Diretiva (EU) 2015/849 relativa à prevenção da utilização do sistema financeiro para branqueamento de capitais ou financiamento do terrorismo**. *Official Journal of the European Union*, L 156, p. 43–74, 19 jun. 2018. Disponível em: https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng. Acesso em: 07 jul. 2025.

UNIÃO EUROPEIA. **Regulation (EU) 2023/1113, de 31 maio 2023, sobre informação que acompanha transferências de fundos e determinados criptoativos, alterando a Diretiva (EU) 2015/849.** *Official Journal of the European Union*, L 150, p. 1–39, 09 jun. 2023. Disponível em: https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng. Acesso em: 07 jul. 2025.

UNIÃO EUROPEIA. **Regulation (EU) 2023/1114, de 31 maio 2023, sobre mercados de criptoativos, alterando os Regulamentos (EU) nº 1093/2010 e nº 1095/2010 e Diretivas 2013/36/EU e (EU) 2019/1937.** *Official Journal of the European Union*, L 150, p. 40–..., 09 jun. 2023. Disponível em: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng. Acesso em: 07 jul. 2025.

UNODC – UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Money-laundering: overview**. UNODC, [s.d.]. Disponível em: https://www.unodc.org/unodc/en/money-laundering/overview.html. Acesso em: 06 jul. 2025.

WEN, Hongzhe; LI, Songbai; ZHANG, Jamie. **Hybrid Monetary Ecosystems: Integrating Stablecoins and Fiat in the Future of Currency Systems.** *arXiv*, v. 2505.10997, 11 jun. 2025. DOI: 10.48550/arXiv.2505.10997. Disponível em: https://arxiv.org/abs/2505.10997. Acesso em: 13 jul. 2025.

YAGA, Dylan et al. **Blockchain Technology Overview.** NISTIR 8202. Gaithersburg, MD: National Institute of Standards and Technology, out. 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf. Acesso em: 03 jul. 2025.

ZHOU, Heather Yue. **Regulating Crypto Money Laundering: An Assessment of Current Regulatory Responses and Potentials for Technology-Based Solutions**. *Stanford Journal of Blockchain Law & Policy*, 30 jun. 2025. Disponível em: https://stanford-jblp.pubpub.org/pub/crypto-laundering/release/1. Acesso em: 04 jul. 2025.

ZHOU, Zhixuan; SHEN, Bohui. **Toward Understanding the Use of Centralized Exchanges for Decentralized Cryptocurrency.** *arXiv*, 19 abr. 2022 (v. 2: 15 jun. 2022). Disponível em: https://arxiv.org/abs/2204.08664. Acesso em: 12 jul. 2025.

ZHUK, Alesia. **Beyond the blockchain hype: addressing legal and regulatory challenges.** *SN Social Sciences*, v. 5, art. 11, 2025. DOI: 10.1007/s43545-024-01044-y. Disponível em: http://hdl.handle.net/10230/69254. Acesso em: 13 jul. 2025.