Criptocrimes Financeiros 2024

- Relatório Tributário e Empresarial –

Gilmara Nagurnhak[1]

[1] Advogada tributarista, empresarial e especialista em criptoativos, dedicada a transformar a complexidade do Direito em estratégias inteligentes, seguras e inovadoras para o crescimento de empresas no cenário dinâmico da nova economia. Graduada em Direito pela Universidade da Região de Joinville (UNIVILLE) e especialista em Direito Tributário pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), atualmente é mestranda em Direito dos Negócios e da Tecnologia pela Ambra University. Autora da obra (R)evolução Tributária na Era Blockchain, livros e artigos jurídicos.

Sumário

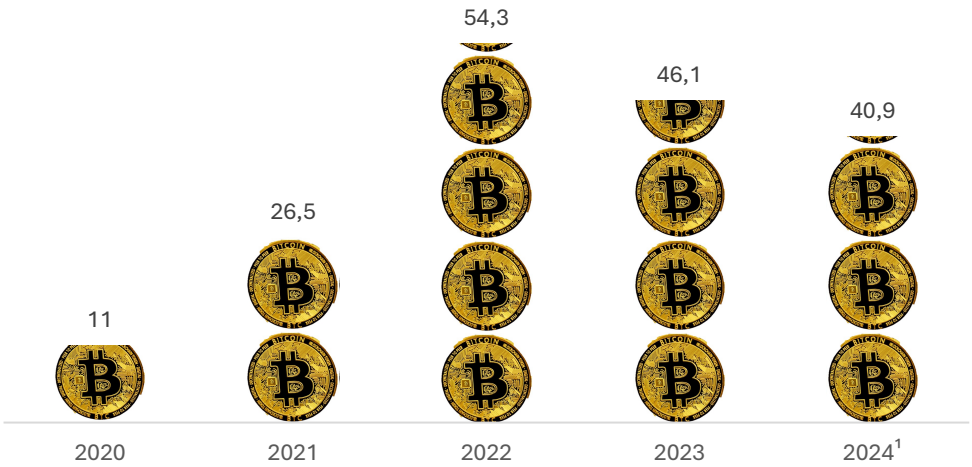
Introdução

No cenário de 2024, o uso ilícito de criptoativos consolidou-se como um ponto de tensão central para o direito penal econômico e empresarial, refletindo os desafios impostos pela crescente digitalização das finanças. Dados robustos, extraídos de relatórios de renome como os publicados pela TRM Labs e ChainAnalysis, revelam que endereços associados a atividades criminosas movimentaram cerca de **US$40,9 bilhões** em criptomoedas ao longo do ano. Importa destacar que projeções atualizadas apontam para a elevação desse montante para aproximadamente **US$51 bilhões**, à medida que novas carteiras ilícitas forem rastreadas e incluídas nas análises.

Do ponto de vista proporcional, observa-se que essas operações ilícitas representaram **apenas 0,14% do total das transações on-chain**, percentual inferior ao registrado em 2023 (0,61%). Ainda assim, o valor absoluto movimentado carrega um peso significativo e supera os números históricos registrados, evidenciando a escalada da criminalidade no ecossistema dos ativos virtuais. Esse contexto revela uma realidade desconcertante: mesmo com o aperfeiçoamento das ferramentas de compliance e das iniciativas de mitigação de risco, a sofisticação dos agentes ilícitos cresce em paralelo, desafiando as autoridades reguladoras, os órgãos de persecução penal e os próprios operadores do mercado cripto.

O panorama histórico reforça a tendência de crescimento. Entre **2020 e 2024**, o volume anual direcionado a endereços ilícitos mais que quadruplicou, saindo de **US$11,0 bilhões** em 2020 para um pico projetado de **US$51,3 bilhões** em 2024, conforme apresentado na Tabela 1. Este crescimento não apenas expõe fragilidades nos mecanismos de controle, mas também lança luz sobre a urgência de estratégias jurídico-regulatórias integradas que combinem direito penal, empresarial, regulatório e tributário, visando à proteção do mercado legítimo e à salvaguarda da integridade do sistema financeiro global.

Esse quadro demanda, dos advogados especializados e dos investidores de alto nível, uma compreensão aprofundada das dinâmicas criminais no universo cripto, tanto para a elaboração de estratégias defensivas quanto para o fortalecimento das práticas de governança corporativa. A sofisticação crescente das fraudes, das estruturas de lavagem de dinheiro e das arquiteturas ilícitas associadas a criptoativos exige atenção redobrada e uma leitura afinada do cenário internacional, uma vez que a natureza descentralizada e transfronteiriça desses ativos desafia fronteiras jurídicas tradicionais.



[1] Os dados de 2024 ainda podem ser revisados e atualizados conforme novas atividades ilícitas sejam identificadas.

A trajetória ascendente do uso ilícito de criptoativos em 2024 não se restringe ao aspecto quantitativo: ela se desdobra também em mudanças qualitativas marcantes no perfil das infrações praticadas. Nos anos anteriores, o protagonismo das criptomoedas vinculava-se predominantemente a delitos cibernéticos clássicos — ataques hackers, phishing, ransomware, pirâmides financeiras digitais, entre outros. No entanto, o cenário atual é significativamente mais amplo e complexo.

Em 2024, os criptoativos passaram a financiar ameaças mais sensíveis, extrapolando o universo cibernético para adentrar áreas tradicionalmente associadas ao direito penal econômico e empresarial: crimes financeiros, crimes contra a ordem tributária, delitos empresariais sofisticados, fraudes corporativas e lavagem de dinheiro integrada a estruturas societárias. Nesse novo contexto, a atenção jurídica recai, com especial ênfase, sobre mecanismos como sonegação fiscal, evasão de divisas e

montagem de arquiteturas empresariais voltadas à ocultação patrimonial.

Essa sofisticação criminosa é acompanhada por um fenômeno relevante: a diversificação dos instrumentos utilizados. Se outrora o Bitcoin reinava absoluto no universo ilícito devido à sua liquidez e reconhecimento global, hoje a narrativa se alterou de forma substancial. Em 2024, as **stablecoins** — criptomoedas de valor estável, vinculadas a moedas fiduciárias ou ativos — assumiram papel central, respondendo por **63% de todo o volume ilícito transacionado**. Essa virada reflete não apenas a popularização legítima desses ativos (cujo uso cresceu 77% no ano), mas também a busca deliberada, por parte de organizações criminosas, por instrumentos menos voláteis e mais facilmente convertíveis em moedas tradicionais.

O deslocamento estratégico para stablecoins tornou-se especialmente visível entre atores sancionados internacionalmente, como entidades vinculadas à Coreia do Norte, que passaram a utilizá-las para driblar restrições financeiras impostas pelo acesso restrito ao dólar norte-americano nos circuitos convencionais. Esse padrão ilustra como a sofisticação criminosa se conecta às dinâmicas geopolíticas globais, ampliando os desafios para os sistemas de controle e vigilância financeira.

Conceitos Gerais e Panorama dos Crimes com Criptoativos

Antes de avançarmos para a análise dos ilícitos específicos envolvendo criptoativos, é essencial estabelecer uma base conceitual sólida que permita compreender os elementos fundamentais deste universo e mapear, com rigor, o panorama da criminalidade que se consolidou ao redor desses ativos em 2024.

Criptoativos: Definições e Características Relevantes

O conceito de **criptoativo** abarca uma ampla gama de ativos digitais assentados em tecnologias de criptografia e em sistemas de registro distribuído, notadamente a **blockchain**. Esse universo inclui, entre outros:

- criptomoedas clássicas, como **Bitcoin** e **Ethereum**;

- stablecoins, como **USDT** e **USDC**, que são tokens atrelados a moedas fiduciárias e mantêm valor estável;

- tokens de plataformas DeFi (finanças descentralizadas);

- **NFTs** (tokens não fungíveis), representações digitais únicas e indivisíveis.

Em essência, os criptoativos representam unidades digitais de valor, passíveis de negociação eletrônica, que possuem uma característica crucial: em grande parte das vezes, operam fora de estruturas centralizadas estatais ou bancárias, funcionando em arquiteturas descentralizadas, autônomas e abertas.

Essas peculiaridades conferem aos criptoativos propriedades altamente atrativas — não apenas para investidores e empresas legítimas, mas também para agentes ilícitos. A literatura especializada salienta que blockchains públicas oferecem um paradoxo singular: **transparência combinada com pseudonimato**. Embora todas as transações fiquem permanentemente registradas em ledgers públicos e imutáveis, os usuários podem ocultar sua identidade real, operando por meio de endereços alfanuméricos sem conexão imediata a seus dados pessoais.

Além disso, as transações envolvendo criptomoedas apresentam atributos de grande apelo:

- caráter transfronteiriço, permitindo circulação irrestrita de valores entre jurisdições;

- rapidez e eficiência, reduzindo tempos e custos operacionais;

- neutralidade geográfica, desvinculando operações de sistemas bancários locais.

Esses mesmos fatores que tornam os criptoativos instrumentos eficientes para a economia legítima também os tornam ferramentas sedutoras para o universo criminoso. O potencial para lavagem de capitais, evasão fiscal, ocultação patrimonial e financiamento ilícito é amplificado justamente pelo conjunto dessas propriedades tecnológicas.

Contudo, é indispensável enfatizar que o termo "criptoativo" não deve ser automaticamente associado a anonimato absoluto ou a um ambiente de impunidade. A imutabilidade dos registros blockchain viabiliza técnicas avançadas de **análise forense de transações**, capazes de mapear fluxos, identificar padrões e estabelecer conexões entre endereços pseudônimos e pontos vulneráveis — especialmente as interfaces onde criptoativos são convertidos em moedas fiduciárias ou em bens tangíveis.

Essa dualidade — entre a **facilidade de movimentação clandestina** e a **rastreabilidade inerente** — coloca as criptomoedas no centro de um terreno jurídico particularmente complexo. De um lado, surgem novas modalidades delitivas que exploram lacunas tecnológicas; de outro, despontam novos instrumentos investigativos que se aproveitam da arquitetura transparente e distribuída das blockchains.

Crimes com Criptoativos: Categorias e Alcance em 2024

A criminalidade envolvendo criptoativos, em 2024, estruturou-se em um espectro amplo e multifacetado, exigindo uma categorização técnica para melhor compreensão. Didaticamente, podemos dividi-la em duas grandes macro-categorias:

a) **Crimes "cripto-nativos"**: trata-se das infrações que surgem no próprio ecossistema dos criptoativos, tendo estes como objeto direto, produto ou meio central do crime. Exemplos característicos incluem:

- golpes de investimento baseados em criptomoedas;

- **rug pulls** (fraudes em projetos DeFi, onde desenvolvedores abandonam subitamente os projetos após captar recursos);

- furtos de criptoativos por meio de ataques hackers a exchanges ou protocolos;

- extorsões cibernéticas, como ransomware, que exigem pagamentos em cripto;

- esquemas Ponzi ou pirâmides financeiras estruturadas com moedas digitais;

- comércio ilícito em marketplaces da dark web operando via criptomoedas.

Esses delitos são intrinsecamente vinculados ao universo criptográfico e, na literatura especializada, frequentemente são chamados de crime criptográfico em sentido estrito.

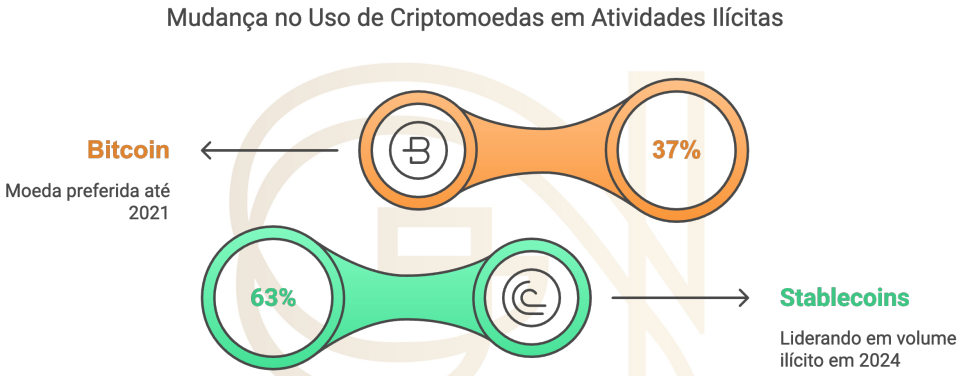
b) **Crimes tradicionais facilitados por criptoativos**: aqui, os criptoativos aparecem como meio de execução, facilitação ou ocultação de crimes clássicos. Em outras palavras, delitos como lavagem de dinheiro, corrupção, tráfico de drogas, evasão fiscal, desvio de ativos corporativos e outros delitos econômicos passaram a incorporar criptomoedas como instrumento para movimentar, transferir ou ocultar valores ilícitos. Nesses casos, a criptomoeda não é o objeto final, mas sim a ferramenta que amplia as possibilidades de evasão de controle, tornando a ação criminosa mais sofisticada.

No panorama de 2024, ambas as categorias experimentaram evoluções relevantes. Sob o prisma quantitativo, conforme já apontado na introdução, o volume absoluto de criptomoedas associado a atividades ilícitas atingiu recordes históricos, superando os valores observados em 2023. Contudo, a participação percentual das transações ilícitas dentro do universo total de operações on-chain permaneceu baixa, situando-se bem abaixo de 1%. Esse dado revela que, embora o crime envolvendo criptoativos tenha aumentado em números absolutos, o uso legítimo

desses ativos também se expandiu significativamente, reduzindo proporcionalmente o peso relativo das operações ilícitas.

Diversificação dos Ativos Ilícitos: Do Bitcoin às Stablecoins

Um traço particularmente marcante do cenário de 2024 foi a **mudança no mix de criptoativos utilizados em atividades ilícitas**. Até 2021, o **Bitcoin** era, de longe, a moeda preferida nos círculos criminosos, valorizado por sua liquidez e aceitação quase universal, tanto nos mercados legítimos quanto nos ilegítimos. No entanto, entre 2022 e 2023, iniciou-se uma migração gradual para outros ativos digitais, fenômeno que se consolidou em 2024: as **stablecoins** assumiram a liderança em volume ilícito movimentado, representando aproximadamente **63% de todas as transações criminosas on-chain**.



De acordo com o relatório da Chainalysis, essa ascensão das stablecoins representa um salto inédito, impulsionado pela funcionalidade desses tokens atrelados ao dólar e sua ampla integração ao ecossistema financeiro digital. Em outras palavras, "**stablecoins now occupy the majority of all illicit transaction volume**" — ou seja, as stablecoins passaram a compor a maior parte do volume ilícito transacionado no espaço cripto.

As razões que explicam essa tendência são múltiplas:

- A **baixa volatilidade** das stablecoins as torna instrumentos preferenciais para armazenar riqueza ilícita, evitando os riscos inerentes a oscilações abruptas de preço;

- A **facilidade de conversão** dessas moedas estáveis em moeda fiduciária ou em outros criptoativos aumenta sua atratividade operacional;

- O **crescimento mainstream** do uso legítimo das stablecoins no comércio e nas finanças descentralizadas acaba servindo de pano de fundo para a exploração ilícita — criminosos simplesmente seguem a maré, tirando proveito da liquidez e da ubiquidade desses tokens.

Como dado ilustrativo, o uso geral de stablecoins no mercado cresceu **77% em 2024**, evidenciando que a adoção criminosa acompanha a ampliação do uso legítimo.

Adicionalmente, o contexto geopolítico exerceu papel relevante. Organizações criminosas e entidades sujeitas a sanções internacionais encontraram nas stablecoins um mecanismo eficaz para contornar restrições impostas ao acesso ao sistema financeiro dolarizado. Com a proibição de diversas instituições financeiras tradicionais em negociar com atores ligados a países como **Coreia do Norte, Irã e Rússia**, consolidou-se uma verdadeira "dolarização paralela" via stablecoins. Como resultado, uma parte significativa das transações associadas a entidades sancionadas migrou para **USDT, USDC** e similares, que oferecem liquidez em dólar fora do circuito bancário tradicional. Em síntese, "**transactions associated with sanctioned entities have shifted primarily to stablecoins**", justamente pela dificuldade de movimentar USD pelos canais formais

Por outro lado, não se pode negligenciar o papel contínuo de outras criptomoedas. O **Bitcoin** permanece amplamente utilizado em nichos específicos, como o pagamento de resgates em ransomware e transações em mercados darknet. O **Ether** (Ethereum) e diversas altcoins continuam sendo ferramentas frequentes em esquemas de fraude, além de figurarem em etapas de lavagem de criptoativos subtraídos. Já as **privacy coins**, como o **Monero**, destacam-se particularmente nos estágios mais avançados de ocultação patrimonial, onde o anonimato extremo é priorizado.

O panorama atual, portanto, é de heterogeneidade estratégica: os criminosos diversificaram seu "portfólio" ilícito, selecionando o criptoativo mais adequado aos seus objetivos específicos — seja buscando estabilidade, anonimato, liquidez ou aceitação em mercados ilícitos determinados. Essa realidade demanda do operador jurídico não apenas um domínio técnico das ferramentas digitais, mas também uma leitura minuciosa das dinâmicas criminais subjacentes, tema que será desdobrado nos mais à frente neste relatório.

Principais Modalidades de Crime com Criptoativos em 2024

O ano de 2024 destacou-se por uma gama diversificada de modalidades delitivas envolvendo criptoativos, evidenciando tanto a criatividade criminosa quanto os desafios regulatórios e investigativos enfrentados no cenário global. A seguir, apresentam-se as principais modalidades observadas, acompanhadas de dados ilustrativos que permitem dimensionar a extensão do fenômeno.

Golpes de investimento e fraudes (scams)

Esses crimes permaneceram como a categoria mais prolífica entre os delitos cripto-nativos. As fraudes abrangeram desde os chamados **High-Yield Investment Programs** (falsas promessas de investimentos de alto retorno) até esquemas conhecidos como **pig butchering** — modalidade na qual a vítima é envolvida emocionalmente, muitas vezes por meio de relacionamentos online, e progressivamente induzida a investir em plataformas fraudulentas, até ser completamente lesada. A metáfora é clara: o golpista engorda o "porco" (vítima) antes do abate final. Em 2024, esses golpes atingiram níveis alarmantes de sofisticação, com destaque para o uso intensivo de ferramentas de **Inteligência Artificial** para automatizar interações, criando falsos consultores financeiros virtuais capazes de estabelecer vínculos de confiança com as vítimas. Embora a quantificação exata dos prejuízos globais seja dificultada pela subnotificação, especialistas apontam que as fraudes e scams superaram todas as demais categorias em número de incidentes, somando prejuízos da ordem de bilhões de dólares.

Furtos e ataques hacker a criptoativos

A subtração de criptomoedas por meio de invasões cibernéticas manteve-se como uma ameaça relevante. Em 2024, estima-se que os fundos roubados de plataformas totalizaram cerca de **US$2,2 bilhões**, um aumento aproximado de 21% em relação ao ano anterior. O foco dos ataques concentrou-se, majoritariamente, em protocolos **DeFi** — exploração de falhas em

contratos inteligentes, invasões a bridges e ataques a exchanges descentralizadas. No entanto, observa-se que, nos segundo e terceiro trimestres de 2024, até mesmo exchanges centralizadas voltaram a ser alvos bem-sucedidos, destacando a vulnerabilidade persistente do ecossistema. Cada ataque de grande escala não apenas gera prejuízo financeiro direto, mas também desencadeia cadeias complexas de **lavagem de ativos**.

Extorsão e ransomware

As operações de ransomware — sequestro de dados mediante criptografia, com exigência de pagamento em criptoativos para liberação — continuaram a movimentar centenas de milhões de dólares em 2024. Relatórios indicam, contudo, que o ritmo de crescimento desse tipo de crime apresentou certo arrefecimento em comparação a anos anteriores. Esse fenômeno deve-se a uma conjugação de fatores: ações multilaterais para desmantelar grupos especializados, prisões de operadores-chave, recuperação parcial de fundos e uma menor disposição das vítimas em pagar resgates. Apesar disso, grupos sofisticados, como os responsáveis pelo malware **Clop** e pelo **LockBit**, permaneceram ativos. O Bitcoin continua a ser a moeda de escolha nesses cenários, devido à familiaridade e liquidez, mas há registros relevantes de exigências em **Monero**, ativo preferido por garantir maior privacidade. Crimes de **extorsão sexual** (sextortion) e ameaças digitais também frequentemente utilizam criptoativos para dificultar rastreamentos.

Mercados ilícitos on-line (darknet markets)

As plataformas clandestinas da dark web, especializadas na comercialização de drogas, armas, dados roubados e outros produtos ilícitos, seguiram movimentando valores expressivos em criptomoedas. Em 2024, esses mercados receberam aproximadamente **US$2,0 bilhões**, uma ligeira queda em relação aos US$2,3 bilhões registrados em 2023. Essa retração decorre, em parte, da derrubada de marketplaces relevantes e da migração de usuários para canais alternativos, mas não elimina a robustez do fluxo financeiro associado ao crime organizado digital. O fechamento do **Hydra Market** em 2022, por exemplo, fragmentou o cenário em múltiplos mercados menores, mantendo a vitalidade do comércio ilícito online. Nesse contexto, **Bitcoin**, **Monero** e, em alguns casos, **Litecoin** permanecem como as moedas predominantes, dada a necessidade de anonimato entre compradores e vendedores.

Lavagem de dinheiro e ocultação de recursos ilícitos

Embora transversal às demais categorias, a lavagem de dinheiro merece destaque específico devido ao seu papel central. Em 2024, tanto crimes cripto-nativos (como hackers que lavam ativos roubados) quanto crimes tradicionais (corrupção, tráfico, fraudes) incorporaram criptoativos em suas operações de lavagem. Praticamente todos os esquemas de grande porte de lavagem

internacional incluíram, em alguma etapa, criptomoedas, explorando sua facilidade de transferência transfronteiriça e a possibilidade de ofuscar rastros por meio de mixers e outras técnicas de anonimização. Segundo levantamento da Chainalysis, cerca de **US$22,2 bilhões** em criptomoedas foram lavados em 2023, e estimava-se um montante ainda mais expressivo em 2024, acompanhando o crescimento geral dos volumes ilícitos.

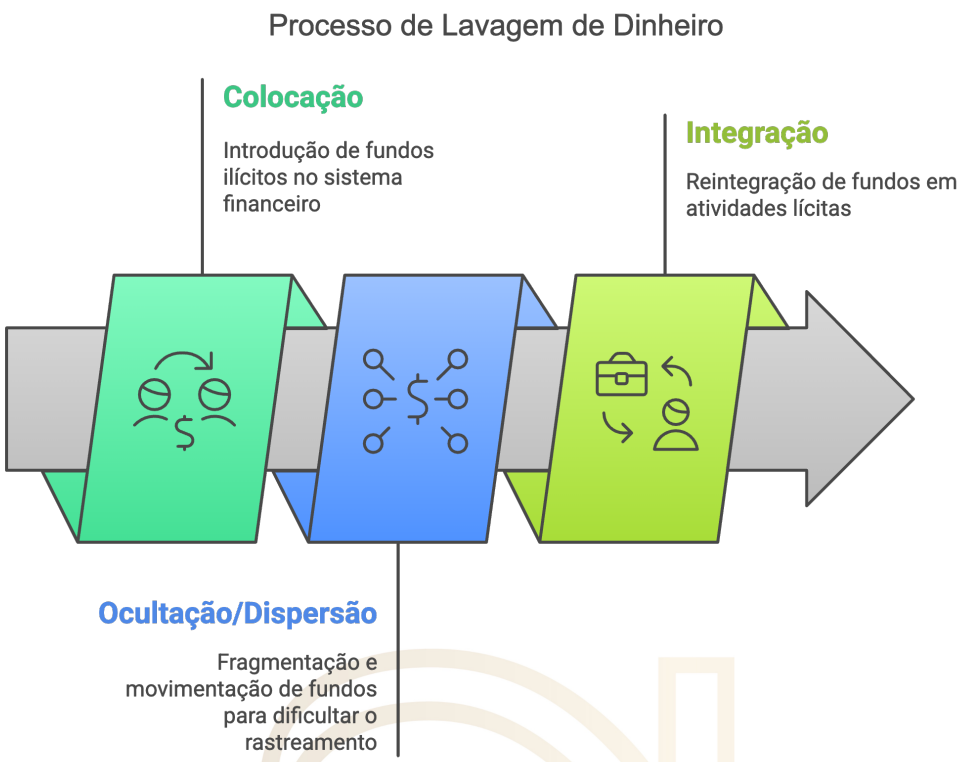
Evasão fiscal e crimes tributários

Por fim, o ano de 2024 evidenciou um aumento relevante no uso de criptoativos para fins de **sonegação fiscal**, **evasão de divisas** e outros ilícitos tributários. Investigações conduzidas em distintas jurisdições revelaram estratégias utilizadas por indivíduos e empresas para ocultar patrimônio em criptoativos e, assim, evitar o pagamento de tributos ou escapar à fiscalização. A natureza descentralizada dos criptoativos, muitas vezes mantidos fora do alcance das autoridades (seja em carteiras privadas, seja em exchanges estrangeiras), criou uma nova fronteira para a sonegação fiscal em larga escala. Casos concretos, como a prisão de um suspeito no Brasil acusado de ocultar bilhões em Bitcoins provenientes de atividades criminosas sem qualquer reporte fiscal, ilustram o potencial criminógeno dessa interface.

Lavagem de Dinheiro com Criptoativos: Mecanismos e Fases

A lavagem de dinheiro, apesar de ser um fenômeno clássico no campo criminal, adquire contornos singulares na era dos criptoativos. Em sua essência, trata-se do conjunto articulado de atos destinados a **ocultar ou dissimular a origem ilícita de recursos**, reintegrando-os ao circuito econômico formal com aparência de licitude. Tradicionalmente, esse processo é segmentado em três fases:

1. **Colocação** — introdução dos recursos no sistema financeiro;
2. **Ocultação/dispersão (layering)** — fragmentação, transformação ou movimentação para dificultar rastreamento;
3. **Integração** — reinserção em atividades ou ativos lícitos, de modo que pareçam originar-se de fontes legítimas.



Quando transposto para o universo dos criptoativos, o processo mantém o arcabouço conceitual, mas assume características próprias, com adaptações de métodos clássicos e surgimento de novos mecanismos específicos da tecnologia blockchain. Esses elementos não apenas ampliam os desafios investigativos, mas também abrem novas possibilidades de rastreamento, dada a transparência inerente aos registros distribuídos. A seguir, exploraremos as nuances da lavagem de dinheiro com criptoativos, analisando fase por fase os mecanismos mais empregados por criminosos em 2024 para ocultar e reinserir ganhos ilícitos.

Fase de Colocação: Entrada de Recursos Ilícitos no Ecossistema Cripto

A fase de colocação corresponde ao momento inicial de introdução de valores ilícitos no sistema financeiro. Em operações tradicionais, isso envolveria, por exemplo, o depósito fracionado de dinheiro em espécie no banco (**smurfing**) ou a aquisição de bens de luxo. Com o avanço das criptomoedas, tornou-se possível converter diretamente dinheiro ilícito em criptoativos, muitas vezes como forma inaugural do esquema de lavagem.

Entre os métodos típicos identificados em 2024, destacam-se:

Uso de Exchanges (Corretoras)

O caminho mais comum passa pela utilização de exchanges centralizadas para adquirir criptomoedas com fundos ilícitos. Criminosos buscam, preferencialmente, exchanges que apresentem falhas nos mecanismos de compliance e **KYC** (know-your-customer), ou que estejam localizadas em jurisdições com regulações permissivas e fiscalização limitada. Ainda que as principais exchanges globais já exijam verificações rigorosas de identidade, persistem corretoras menores ou plataformas **peer-to-peer** que oferecem maior anonimato. Um exemplo recorrente: traficantes recrutam terceiros (**laranjas**) para abrir contas em exchanges, comprando Bitcoin ou outros criptoativos com dinheiro do crime e, assim, inserindo os recursos no ambiente digital.

Corretoras Peer-to-Peer e OTC Brokers

Plataformas **P2P**, como o extinto LocalBitcoins (operante até 2023), ou redes de **OTC brokers** (negociadores de balcão), permitem a compra e venda direta de criptoativos entre particulares, frequentemente sem registro formal. Criminosos aproveitam essas estruturas para adquirir criptomoedas usando dinheiro físico ou transferências de contas de fachada, evitando a detecção por mecanismos de controle tradicionais. Essa colocação peer-to-peer torna o rastreamento significativamente mais complexo, já que muitas transações não transitam por intermediários sujeitos à supervisão regulatória.

Caixas Eletrônicos de Bitcoin (BTMs)

Em determinadas jurisdições, **BTMs** (Bitcoin ATMs) são empregados para converter pequenas quantias em dinheiro vivo para criptoativos. O processo é simples: o operador insere cédulas no terminal e recebe Bitcoins diretamente em seu endereço. Repetindo a operação em diferentes locais, com valores limitados para evitar alertas ou captação por câmeras de segurança, os criminosos conseguem converter moeda física em ativos digitais sem necessariamente vincular a operação a uma identidade real.

Conversão de Valor Ilícito Nativamente Digital

Importante observar que, em alguns casos, a fase de colocação é praticamente automática, dado que o produto do crime já nasce como criptoativo. Fundos obtidos via ataque hacker a uma exchange, ganhos oriundos de esquemas fraudulentos pagos diretamente em criptomoedas, ou Bitcoins extorquidos por ransomware não exigem conversão de dinheiro tradicional: os valores ilícitos já estão inseridos no ecossistema cripto desde a origem. Nesses cenários, a lavagem avança diretamente para a fase de ocultação (**layering**), uma vez que a colocação foi substituída pela própria obtenção criminosa do ativo digital.

Em 2024, autoridades ao redor do mundo identificaram redes altamente organizadas, especializadas em introduzir recursos ilícitos no ecossistema cripto. Casos em que esquemas de lavagem oriundos do tráfico de drogas por meio da conversão de valores em criptomoedas, com operadores adquirindo criptoativos com dinheiro ilícito e os redistribuía entre contas de **shell companies** (empresas de fachada) sob seu controle são cada vez mais comuns. Isso ilustra não apenas a escala que a fase de colocação pode atingir, mas também a sofisticação das estruturas corporativas utilizadas para mascarar a entrada de recursos ilícitos no universo cripto.

Fase de Ocultação (Layering): Táticas de Dissimulação em Série

A fase de **layering** — também denominada ocultação ou estratificação — constitui o núcleo central do processo de lavagem de dinheiro. É nela que os criminosos aplicam múltiplas transações, conversões e estratégias operacionais para dificultar a rastreabilidade do dinheiro ilícito, embaralhando os sinais que permitiriam vincular os ativos atuais à sua origem criminosa. No universo das criptomoedas, o layering não apenas adaptou técnicas herdadas do sistema financeiro tradicional, mas também criou métodos inéditos, potencializados pela estrutura tecnológica das blockchains.

A seguir, descrevem-se as principais táticas de ocultação aplicadas a criptoativos em 2024.

Fragmentação de Valores (Smurfing)

Trata-se de um estratagema clássico, adaptado ao meio digital, que consiste em dividir grandes montantes em pequenas transações sequenciais, de modo a parecerem operações triviais e dispersas. No ambiente das criptomoedas, isso equivale a distribuir, por exemplo, 100 BTC ilícitos em centenas de transações fracionadas (1 BTC, 2 BTC cada) por diversas carteiras. Em vez de uma transferência volumosa, que poderia disparar alertas de compliance, são realizadas micro-operações que passam despercebidas. Em 2024, análises forenses detectaram esse padrão, inclusive em operações ligadas à Coreia do Norte, nas quais quatro transferências totalizando 308 BTC (cerca de US$8 milhões) foram realizadas em valores redondos ao longo de quatro dias. Os investigadores observam que, enquanto carteiras pessoais comuns raramente executam mais que 3 a 5 transações em valores inteiros, sequências com dezenas ou centenas de operações "redondas" sinalizam possíveis serviços automatizados de mixing ou atividades de lavagem profissional.

Hops Entre Múltiplas Carteiras (Chain Hopping Interno)

Diferentemente do chain hopping entre blockchains, aqui falamos de saltos sucessivos dentro da mesma rede. O criminoso transfere os fundos por uma longa cadeia de endereços sob seu controle — as chamadas carteiras intermediárias —, criando um labirinto de transferências. Embora a maioria dos usuários utilize poucas carteiras para movimentar valores, padrões anômalos, como centenas de hops consecutivos, indicam ocultação deliberada. Em muitos casos, bots programados executam essas operações com velocidade, dificultando o acompanhamento em tempo real por analistas humanos.

Uso de Mixers (Misturadores de Criptomoedas)

Os mixers são serviços especializados — centralizados ou descentralizados — que têm como objetivo embaralhar as origens e os destinos das criptomoedas. Funcionam reunindo ativos de múltiplos usuários, misturando-os em um pool comum e redistribuindo quantias equivalentes para novos endereços fornecidos pelos clientes, de forma aleatória. Esse processo quebra a ligação direta entre o endereço inicial e o final, efetivamente embaralhando a trilha auditável. Em 2024, o uso de mixers manteve-se intenso, apesar de sanções regulatórias. O **Tornado Cash**, mixer baseado em contratos inteligentes na rede Ethereum, sancionado pelos EUA em 2022, registrou movimentações expressivas: cerca de 480.328 ETH (US$1,45 bilhão) foram retirados de seus contratos ao longo do ano, representando um aumento anual de 53%. Paralelamente, surgiram novos mixers — como o identificado pelo codinome "**eXch**" — que atraíram especialmente agentes maliciosos afiliados à Coreia do Norte, oferecendo anonimato reforçado e resistência à cooperação com autoridades. Essas plataformas tornaram-se preferidas para ocultação, consolidando-se como peças-chave no ecossistema de lavagem digital.

Chain Hopping (Troca de Blockchain)

Essa técnica envolve a movimentação de valor entre diferentes blockchains, convertendo criptomoedas rastreáveis em outras moedas ou utilizando **pontes cross-chain** para transferir tokens entre redes distintas. O objetivo é fragmentar a trilha de auditoria, exigindo dos investigadores a correlação de dados entre múltiplos livros-razão e, frequentemente, a obtenção de cooperação internacional. Em janeiro de 2024, observou-se um pico recorde, com aproximadamente US$234 milhões em fluxos ilícitos transitando por bridges, resultado direto de hackers que primeiro lavaram ETH via Tornado Cash e, em seguida, movimentaram os ativos para outras blockchains. Embora ferramentas modernas de análise blockchain consigam rastrear esses percursos, a complexidade investigativa aumenta exponencialmente, impondo desafios operacionais às autoridades.

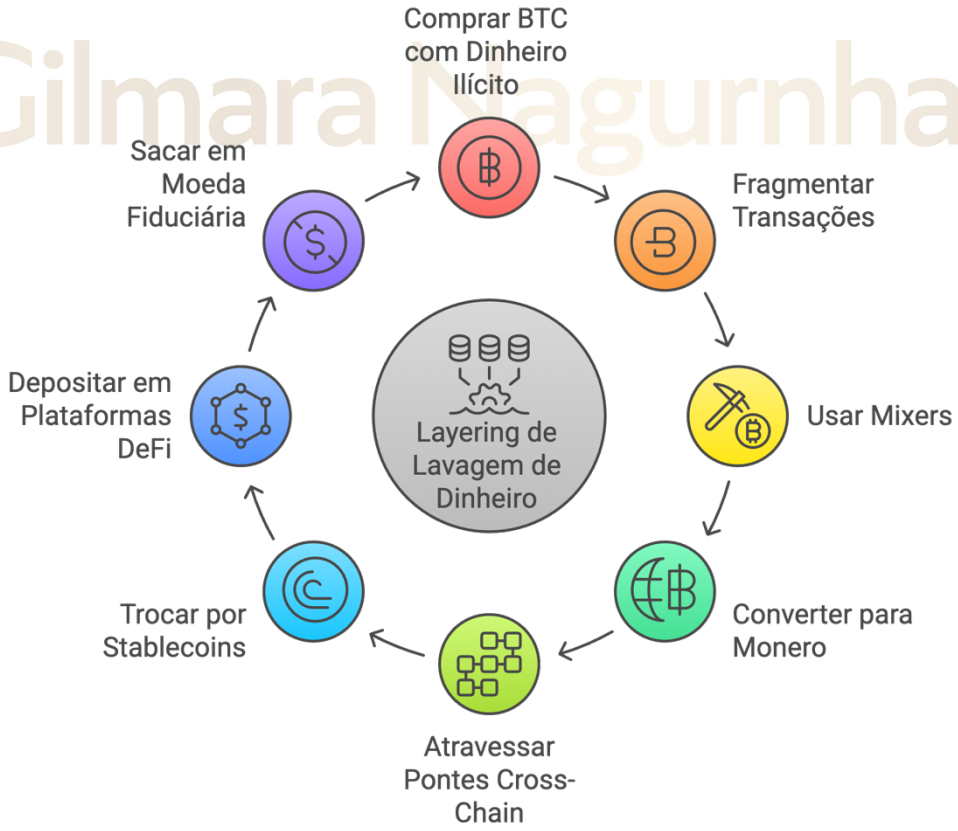
Conversão em Moedas de Alto Nível de Privacidade (Privacy Coins)

Outra estratégia relevante é a conversão de criptoativos rastreáveis, como BTC e ETH, em **privacy coins**, sobretudo **Monero (XMR)**. O Monero emprega mecanismos criptográficos robustos que ocultam remetente, destinatário e valor das transações, tornando praticamente impossível rastrear fluxos dentro de sua blockchain. Em 2024, corretoras instantâneas que não exigem KYC foram identificadas facilitando essa conversão, permitindo que fundos ilícitos fossem convertidos para Monero e, posteriormente, trocados novamente por criptomoedas limpas, sem deixar relação direta com os ativos originais. Em resposta, algumas jurisdições proibiram privacy coins, e exchanges de grande porte, como a Binance, deslistaram o Monero em mercados estratégicos — mas enquanto houver plataformas dispostas a negociar esses ativos anonimamente, eles continuarão sendo instrumentos valiosos de ocultação.

Uso de Plataformas DeFi e Serviços Especializados

Além dos mixers tradicionais, 2024 testemunhou a exploração das **finanças descentralizadas (DeFi)** para fins de lavagem. Os criminosos depositam ativos ilícitos em **pools de liquidez** de exchanges descentralizadas, misturando-os com milhares de outros aportes, ou utilizam plataformas de empréstimo, colateralizando ativos "sujos" para tomar emprestado stablecoins, que saem "limpas". Sites de jogos e apostas online, operando com criptoativos,

Ciclo de Layering de Lavagem de Dinheiro



também foram utilizados, em analogia aos cassinos físicos: tokens são depositados, apostas simuladas são feitas, e os valores são sacados como "ganhos legítimos", dificultando a distinção entre lavagem e operação regular.

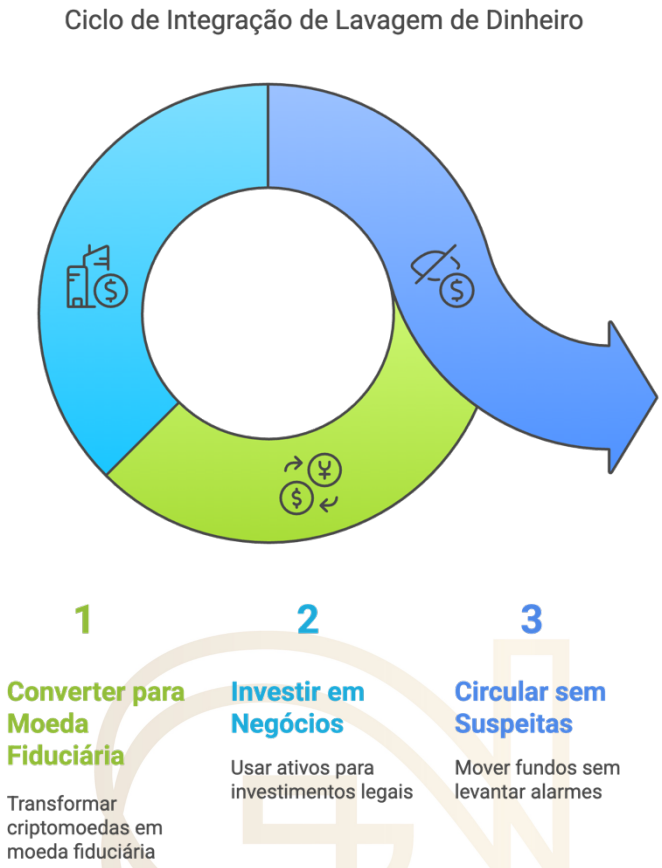
Complexidade e Rastreamento

A fase de **layering** caracteriza-se pela combinação engenhosa dessas múltiplas técnicas. Criminosos profissionais frequentemente encadeiam etapas para construir um labirinto de ocultação: compram BTC com dinheiro ilícito, fragmentam-no em centenas de transações, passam-no por mixers, convertem para Monero, atravessam pontes cross-chain, trocam por stablecoins em redes alternativas, depositam em plataformas DeFi e finalmente sacam em moeda fiduciária via exchange. Cada camada adiciona anonimato e dilui os vínculos com o crime originário.

Contudo, a transparência das blockchains — com seus registros imutáveis — oferece uma vantagem às autoridades: dados permanentes que, embora complexos, permitem reconstituir trilhas, especialmente com o uso de ferramentas forenses avançadas. Por exemplo, picos anômalos de taxas em mixers frequentemente coincidem com grandes ataques hackers, sugerindo que criminosos pagam mais para acelerar suas operações logo após um roubo. Essas análises ajudam a levantar alertas e conectar eventos, demonstrando que, embora o layering com criptoativos tenha elevado a ocultação patrimonial a um patamar sofisticado e veloz, ele não é impermeável — apenas demanda esforços investigativos cada vez mais especializados. Nos próximos tópicos, exploraremos a fase final: a integração dos fundos ilícitos ao sistema econômico formal, completando o ciclo da lavagem de dinheiro digital.

Fase de Integração: Retorno ao Sistema Legal e Uso Empresarial

A etapa de **integração** é aquela em que os recursos ilícitos — já lavados após a fase de ocultação — são finalmente reinseridos no circuito econômico formal, adquirindo aparência legítima. No contexto das criptomoedas, a integração frequentemente se materializa na conversão final para moeda fiduciária ou no emprego dos criptoativos em investimentos e operações ostensivamente legais. Trata-se, portanto, da culminação do ciclo da lavagem, onde o dinheiro "sujo" assume feições documentadas, prontas para circular sem levantar suspeitas.



Entre as formas usuais de integração com criptoativos destacadas em 2024, podemos apontar:

Conversão em Moeda Fiduciária por Meio de Exchanges

Após atravessar as múltiplas camadas do processo de ocultação, o criminoso busca sacar o valor em uma conta bancária ou obter novamente dinheiro em espécie. As exchanges centralizadas são o canal preferencial para esse objetivo, sobretudo aquelas que permitem saques em moedas tradicionais. Estatísticas mostram que mais de 50% dos fundos ilícitos em criptoativos acabam sendo direcionados a exchanges centralizadas, direta ou indiretamente, ao final do ciclo de lavagem. Ou seja, apesar de todas as etapas técnicas no ambiente blockchain, a maior parte do dinheiro sujo termina na interface com uma corretora — muitas vezes após passar por mixers, privacy coins e outras estratégias de despistamento.

Uma vez na exchange, os ativos digitais podem ser convertidos em dólares, euros, reais, entre outras moedas, e então retirados para contas bancárias aparentemente normais. Este é, contudo, o momento mais sensível: exchanges com controles robustos de compliance podem

detectar e congelar ativos suspeitos. Por essa razão, os lavadores preferem exchanges complacentes, menos reguladas, ou recorrem ao uso de contas de terceiros (laranjas) para dificultar a identificação. Ainda assim, grandes volumes de saque em moeda fiduciária tendem a acionar mecanismos de controle bancário, sobretudo em jurisdições com regras rigorosas de antilavagem de dinheiro (AML), o que frequentemente leva os criminosos a fracionar e distribuir saques entre diversas contas e países.

Aquisição de Bens de Alto Valor

Outra via clássica de integração consiste em empregar as criptomoedas já lavadas para adquirir ativos ou investimentos legais, transformando-os em patrimônio ostensivamente lícito. Em 2024, ampliou-se o número de negócios que aceitam pagamentos diretos em criptoativos, incluindo imobiliárias, concessionárias de veículos de luxo, galerias de arte e joalherias. O criminoso, portanto, pode utilizar Bitcoin (já mascarado via mixers e outras etapas) para adquirir um imóvel ou automóvel de alto valor, integrando os recursos por meio da propriedade do bem.

Posteriormente, a revenda desses ativos gera dinheiro "limpo", respaldado por justificativas documentais e aparência formal de licitude. Uma estratégia crescente envolve o investimento empresarial: criminosos injetam capital em startups ou empreendimentos legítimos, tornando-se sócios investidores e mascarando a origem ilícita como se fossem aportes legais. Muitas vezes, isso é feito via stablecoins, que passam despercebidas em processos internos de due diligence, especialmente em empresas pequenas ou necessitadas de capital, que não questionam detalhadamente a proveniência das criptomoedas recebidas.

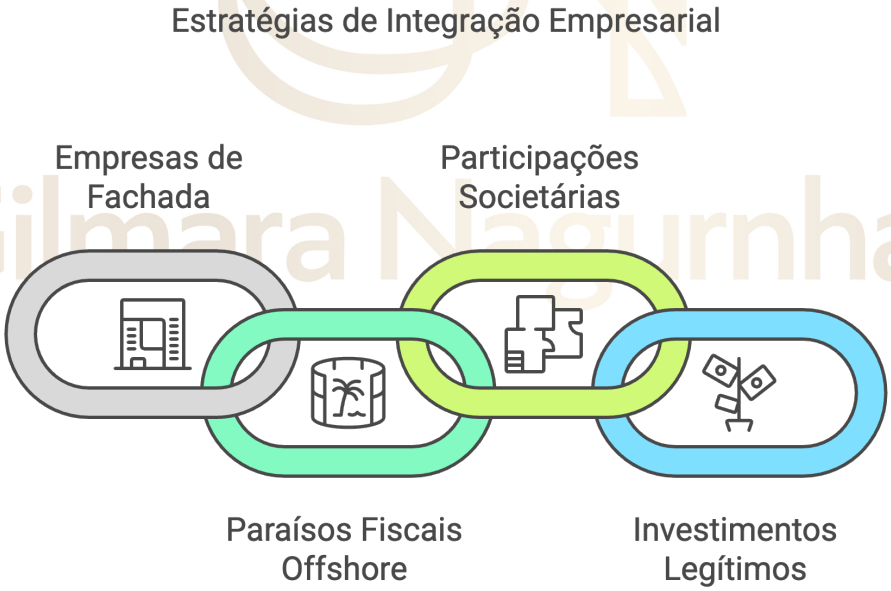
Uso Contínuo no Circuito Cripto

Nem sempre a integração demanda a conversão para moeda fiduciária. Em alguns casos, o criminoso opta por manter os fundos no universo cripto, explorando instrumentos que gerem rendimentos passivos ou valorização patrimonial. Isso inclui estratégias como staking, fornecimento de liquidez em protocolos DeFi (com ganhos derivados de taxas e incentivos legítimos) ou empréstimos em plataformas descentralizadas. Dessa forma, os rendimentos auferidos podem ser declarados como ganhos de investimento lícito, enquanto a origem obscura do capital principal permanece velada. Essa forma de integração, peculiar ao mundo cripto, dispensa os bancos e governos, criando uma economia paralela que dificulta ainda mais os esforços de recuperação estatal.

Estruturas Empresariais e Integração Transnacional

No plano empresarial, a integração frequentemente envolve o uso de empresas de fachada ou laranjas societários, vinculando o capital lavado a pessoas jurídicas para conferir-lhe aparência formal. Essa prática conecta a lavagem de dinheiro aos chamados crimes empresariais. Um exemplo comum é o uso de **offshore companies** em paraísos fiscais combinadas com operações em criptoativos. Criminosos e corruptos podem manter participações societárias abaixo de 25%, por exemplo, em empresas offshore, evitando sua declaração como beneficiários finais, e transferir para essas entidades os criptoativos lavados. A empresa, por sua vez, investe globalmente em negócios legítimos, finalizando o ciclo de branqueamento patrimonial.

Apesar de complexa, a lavagem de dinheiro com criptoativos não é impermeável à investigação. Em 2024, autoridades ao redor do mundo intensificaram o uso de técnicas clássicas de detecção, aplicando-as ao ambiente blockchain. A análise de padrões anômalos — como volumes fracionados repetitivos, uso coordenado de mixers e saltos cross-chain atípicos — permitiu identificar operações suspeitas, evidenciando a convergência entre compliance financeiro e análise cibernética.



Ainda assim, os criminosos demonstraram elevada adaptabilidade, adotando rapidamente novos instrumentos, como mixers descentralizados e protocolos anônimos, para manterem-se à frente da fiscalização. O balanço de 2024 revela que a lavagem de dinheiro com criptomoedas tornou-se um procedimento altamente sofisticado, envolvendo cifras expressivas e redes transnacionais.

Para o jurista especializado, compreender essas dinâmicas é essencial: seja para orientar empresas no cumprimento de obrigações preventivas, seja para atuar em investigações, litígios e processos criminais relacionados à lavagem.

Evasão Fiscal e Sonegação com Criptoativos

A evasão fiscal — compreendida como o conjunto de práticas ilícitas voltadas à supressão ou redução indevida de tributos — adquiriu novos contornos com o advento dos criptoativos. Tradicionalmente, esquemas sofisticados de sonegação envolviam mecanismos como caixa dois, envio de recursos não declarados para offshores, utilização de interpostas pessoas (**laranjas**), entre outros. Contudo, as criptomoedas surgiram como um meio adicional e eficiente para ocultar patrimônio e rendimentos das autoridades fiscais, dadas as características específicas desse mercado: armazenamento fora do sistema bancário, ausência de intermediários estatais e, em muitos casos, a falta de controles diretos sobre transações.

É importante observar que a sonegação por meio de criptoativos frequentemente se entrelaça com práticas de lavagem de dinheiro, uma vez que ocultar ativos do fisco muitas vezes coincide com ocultá-los de outros tipos de escrutínio legal. No entanto, o foco aqui recai exclusivamente sobre os impactos e implicações tributárias — ou seja, o prejuízo direto ao erário e as estratégias empregadas para escapar dos deveres fiscais mediante o uso de ativos virtuais.

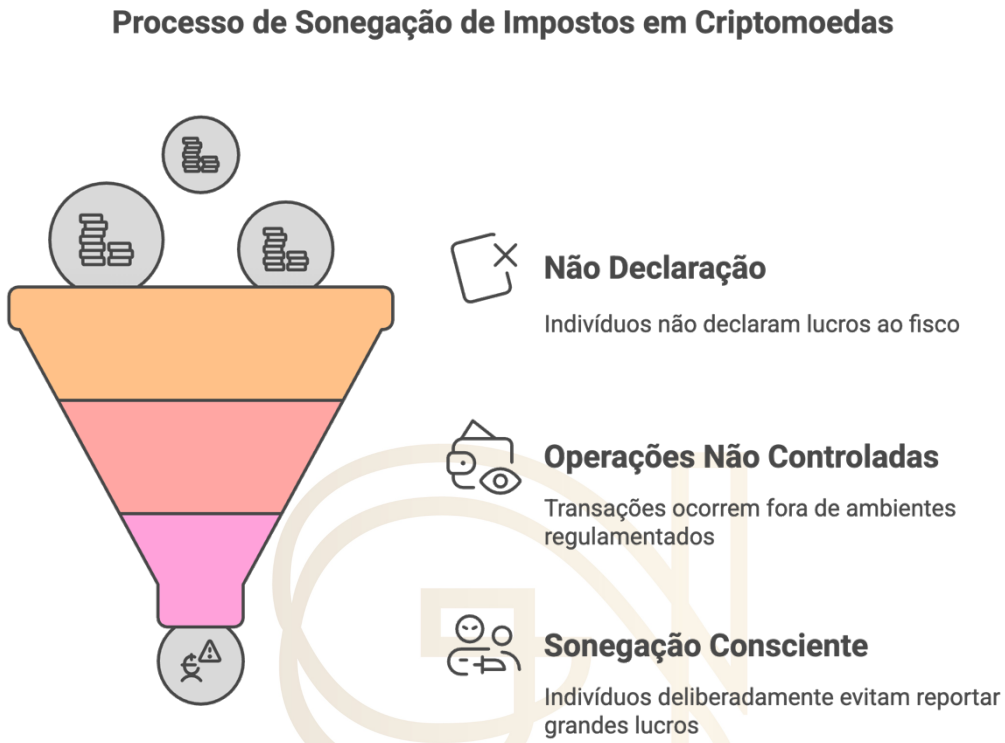
Criptomoedas como Instrumento de Sonegação: Mecanismos Típicos

As estratégias para utilizar criptoativos como ferramenta de evasão fiscal variam em sofisticação e alcance. Em muitos casos, tratam-se de extensões tecnológicas de práticas já conhecidas no mundo físico, agora adaptadas ao ambiente digital:

Não Declaração de Ganhos com Criptomoedas

A forma mais elementar de sonegação ocorre quando indivíduos que obtêm lucros com investimentos em cripto simplesmente deixam de reportá-los ao fisco. Diversas jurisdições, incluindo o Brasil, determinam que ganhos de capital oriundos de transações com criptomoedas sejam declarados e tributados. Contudo, como muitas dessas operações são realizadas fora de ambientes controlados — por exemplo, através de exchanges estrangeiras ou wallets privadas — , muitos contribuintes optam deliberadamente por mantê-las fora do radar fiscal. Em pequenas

somas, isso frequentemente passa despercebido, mas, quando envolvem montantes elevados, configura sonegação consciente. Um exemplo recorrente em 2024 envolve investidores que compraram bitcoins a preços irrisórios em anos anteriores e venderam com enorme lucro recentemente, omitindo a informação à Receita para evitar a tributação sobre ganho de capital.



Pagamento "Por Fora" em Cripto

Empresas e profissionais autônomos podem aceitar pagamentos em criptoativos sem emissão de notas fiscais ou registro contábil, operando fora do sistema formal. Essa prática equivale ao clássico caixa dois, agora em versão digital. Um exemplo simples: um desenvolvedor de software que presta serviços a clientes estrangeiros e solicita pagamentos em stablecoins diretamente para sua wallet pessoal, omitindo essa receita do livro-caixa e, consequentemente, da base tributável. De modo semelhante, empresas podem remunerar fornecedores ou até funcionários com pagamentos em criptomoedas, sem declarar oficialmente tais despesas, alimentando um circuito paralelo não tributado.

Offshores e Exchanges Estrangeiras para Evasão

O uso de contas offshore sempre foi um recurso clássico para ocultação patrimonial. Com os criptoativos, esse processo tornou-se ainda mais ágil e descentralizado. Indivíduos e empresas podem transferir criptomoedas para wallets sob seu controle em outras jurisdições, ou mantê-las em exchanges sediadas em paraísos fiscais, longe do alcance das autoridades locais. Estudos apontam que aproximadamente 20% das exchanges globais operam em locais como Seychelles,

justamente pela combinação de baixa regulação e tributação zero. Muitas vezes, não há sequer necessidade de converter as criptomoedas em moeda fiduciária: basta deixá-las valorizando no exterior ou utilizá-las diretamente em operações comerciais. Ferramentas como cartões de débito cripto, vinculados a exchanges estrangeiras, permitem que esses fundos sejam gastos no dia a dia sem ingressarem formalmente no país de residência, tornando a evasão particularmente difícil de detectar.

Uso de Empresas de Fachada e Interpostas Pessoas

Semelhante aos esquemas tradicionais, mas com um diferencial tecnológico, essa prática envolve a criação de empresas de fachada — nacionais ou offshore — que recebem recursos disfarçados de investimentos em criptomoedas. Por exemplo, uma empresa fictícia adquire criptoativos de um indivíduo ou empresa real a preços artificialmente reduzidos, servindo de veículo para a retirada de lucro não declarado. Outra variante consiste em atribuir a titularidade de wallets a laranjas (familiares, sócios minoritários, etc.), de modo que o verdadeiro detentor dos ativos não figure formalmente como proprietário. Relatórios recentes destacam que, mesmo sem apoio no sigilo bancário tradicional, as criptomoedas oferecem esse mesmo tipo de blindagem: basta não declarar os ativos, contando que a Receita Federal ou órgãos equivalentes não consigam rastreá-los autonomamente.

Conversão de Receitas Lícitas em Cripto para Reduzir Tributação

Em operações empresariais, outra prática envolve a conversão parcial das receitas em criptoativos não registrados. Por exemplo, uma empresa exportadora pode combinar com seu cliente estrangeiro o envio formal de US$70 mil pelo canal oficial (que será tributado) e o envio "extraoficial" de US$30 mil em stablecoins diretamente para os donos ou administradores da empresa, reduzindo artificialmente o faturamento declarado. Essa estratégia de "dupla via" — parte on-book, parte off-book — foi alvo de investigações em 2024, sobretudo no comércio exterior e em serviços transnacionais, destacando-se como uma prática sofisticada de evasão.

Estudos de Caso: Crimes Tributários Envolvendo Criptomoedas em 2024

Para compreender a gravidade e a realidade dos esquemas de evasão fiscal com criptoativos, é essencial analisar casos concretos que ilustram as práticas e os desafios enfrentados pelos órgãos de fiscalização ao redor do mundo.

Caso Brasil – US$ 2,6 Bilhões Ocultos via Bitcoin

Este caso foi alvo de uma grande operação conduzida pela Polícia Federal brasileira em 2024, sob a operação Colossus. Um indivíduo foi acusado de articular um megaprocesso de lavagem de dinheiro e evasão fiscal, ocultando mais de **US$ 2,6 bilhões** provenientes do narcotráfico, utilizando Bitcoin como principal meio de movimentação. Embora o aspecto de lavagem de dinheiro tenha sido central na investigação, ficou evidenciado também o flagrante de sonegação fiscal: empresas de fachada operadas pelo investigado movimentaram centenas de milhões de dólares sem qualquer reporte às autoridades tributárias, sonegando tanto impostos diretos (como IRPJ) quanto obrigações acessórias. Apenas uma das empresas envolvidas registrou **US$ 285 milhões** em transações não declaradas em apenas dez meses. Quando o suspeito foi preso, tentava embarcar para Dubai — uma jurisdição amplamente utilizada por evasores fiscais e conhecida por sua postura mais flexível em relação aos criptoativos e pela ausência de tratado de extradição com o Brasil, reforçando o caráter transnacional e articulado do esquema.

Caso Estados Unidos – Sonegadores Identificados Via Blockchain

Nos Estados Unidos, o Internal Revenue Service (IRS) intensificou investimentos em ferramentas de rastreamento blockchain para identificar contribuintes de alto patrimônio que não declaram corretamente seus ganhos em criptomoedas. Em 2024, com o auxílio de empresas privadas de análise forense, a agência identificou diversos contribuintes que, apesar de terem auferido lucros substanciais em vendas de ativos digitais, não reportaram esses rendimentos em suas declarações fiscais. Um caso emblemático (apresentado de forma anonimizada em conferência) revelou um trader que obteve mais de **US$ 5 milhões** em lucros negociando altcoins entre 2021 e 2022, movimentando os ativos para uma exchange offshore sem declarar nenhum valor à Receita. O rastro on-chain, contudo, permitiu a vinculação dos fundos a endereços identificáveis, resultando na autuação do indivíduo em 2024, com cobrança de impostos, multas e possível encaminhamento para persecução penal por fraude fiscal. Este caso demonstra que, embora as criptomoedas ofereçam anonimato relativo, sua rastreabilidade pode se voltar contra o sonegador quando combinada com dados obtidos de exchanges ou com falhas operacionais, como a reutilização de endereços vinculados a identidades conhecidas.

Caso de Empresa de Tecnologia – Pagamento de Bônus em Cripto no Exterior

Um exemplo oriundo da Europa chamou atenção em 2024: uma empresa de desenvolvimento de software teria remunerado seus executivos com bônus pagos em Bitcoin, diretamente para carteiras fornecidas pelos diretores, evitando o reporte ao fisco local como pagamento de remuneração trabalhista. O esquema foi descoberto quando um dos executivos realizou uma conversão significativa de Bitcoin para euros em uma exchange local, gerando alerta para as autoridades fiscais. Auditorias posteriores constataram que a empresa não havia declarado os bônus pagos, tampouco os beneficiários haviam informado tais rendas em suas declarações individuais. Esse caso revela como as criptomoedas podem ser instrumentalizadas não apenas por indivíduos isolados, mas também por empresas, para fraudar encargos sobre folha de pagamento e impostos sobre renda — configurando, portanto, fraude corporativa e evasão fiscal empresarial. Além disso, destaca como movimentações atípicas de funcionários em exchanges podem servir de pista para desvendar esquemas internos de sonegação.

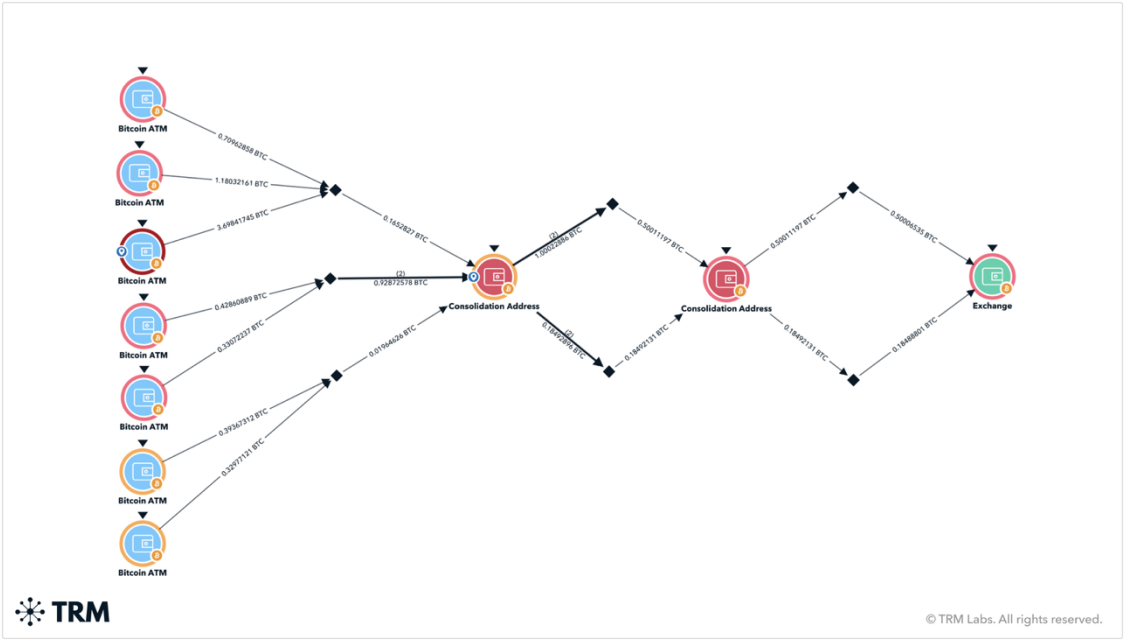
Preocupação Internacional

De forma mais ampla, instituições multilaterais como o Banco Mundial já vinham alertando, desde pelo menos 2018, sobre os riscos crescentes de que os criptoativos servissem como ferramentas de **money laundering, tax evasion, and illicit transactions**. Em 2024, essas preocupações tornaram-se ainda mais urgentes, levando diversos países a implementar medidas robustas, como a obrigatoriedade de reporte de transações em cripto acima de determinados valores e o intercâmbio automático de informações sob padrões da **OCDE** (incluindo a aplicação da Regra de Viagem do **FATF** às exchanges). O entendimento global consolidado é que nenhum país, isoladamente, consegue enfrentar a evasão fiscal viabilizada por criptoativos: trata-se de um desafio transnacional que demanda coordenação internacional efetiva, tanto no plano normativo quanto no operacional.

Desafios Jurídicos e a Resposta às Fraudes Fiscais com Criptomoedas

Sob a perspectiva jurídica, a sonegação fiscal por meio do uso de criptoativos se enquadra, em essência, nas mesmas figuras típicas das fraudes fiscais clássicas: omissão de receitas nos registros contábeis, prestação de informações falsas à autoridade fazendária, evasão de divisas — nos casos em que valores são mantidos clandestinamente no exterior —, entre outras. Ou seja, do ponto de vista normativo, o arsenal jurídico já existe. O verdadeiro desafio reside, portanto, não

tanto na tipificação penal, mas na prova e na detecção dessas condutas, diante das particularidades tecnológicas do ambiente cripto.



Desafios Específicos

Alguns elementos se destacam como obstáculos particularmente relevantes à persecução penal e administrativa:

Anonimato e Dificuldade de Vinculação Pessoal

A identificação do efetivo titular de uma carteira digital é o cerne das dificuldades probatórias. Ao contrário de uma conta bancária, que tem titularidade associada diretamente a CPF ou CNPJ, uma wallet de criptomoedas não carrega, por padrão, a identidade do seu controlador. Para superar essa barreira, investigações precisam recorrer à análise de padrões comportamentais, endereços IP, eventual cooperação de exchanges (quando sujeitas a regulamentação) ou até a erros operacionais cometidos pelos próprios usuários. Esse obstáculo não é trivial: ainda que haja fortes indícios comportamentais, a defesa pode alegar, por exemplo, que aquele endereço não pertence ao acusado, tornando a imputação de propriedade mais desafiadora.

Avaliação Patrimonial e Variação Cambial

Outro ponto crítico reside na volatilidade dos criptoativos. Determinar o exato valor omitido para fins de cálculo tributário, ou mesmo para dosimetria de pena em eventual persecução penal, exige precisão quanto ao momento em que o fato gerador ocorreu e ao valor correspondente na moeda local naquela data. Isso demanda não apenas conhecimentos jurídicos, mas também técnicos e financeiros, incluindo avaliação de cotações históricas, registro de splits e forks, entre outros elementos próprios do universo cripto.

Lacunas Regulatórias e Obrigação de Reporte

Em 2024, muitos países ainda apresentavam legislações fragmentadas ou insuficientes quanto à obrigatoriedade de declarar a posse e as movimentações em criptoativos. No Brasil, por exemplo, a Instrução Normativa RFB nº 1.888/2019 estabelece a obrigatoriedade de reporte de operações acima de certos valores, mas o grau de adesão ainda é desigual. Em jurisdições menos reguladas, o sonegador pode tentar alegar boa-fé, afirmando não saber da obrigação de declarar. Contudo, observa-se uma tendência internacional clara — especialmente em países do G7, da OCDE e da União Europeia — de reforçar os deveres acessórios de exchanges e usuários, aproximando-os progressivamente das obrigações já impostas a instituições financeiras tradicionais.

Respostas das Autoridades Tributárias

Diante desses desafios, a resposta institucional vem se desenrolando em múltiplos níveis, combinando tecnologia, cooperação internacional e inovação jurídica:

Desenvolvimento de Equipes Especializadas

Os fiscos e os ministérios públicos passaram a formar equipes compostas por especialistas em blockchain, que trabalham lado a lado com analistas tributários e peritos contábeis. O cruzamento de dados obtidos por intimação junto a exchanges com registros públicos on-chain permite reconstruir fluxos patrimoniais antes invisíveis. Esse trabalho é essencial para desvendar

esquemas de ocultação sofisticados, muitas vezes distribuídos entre múltiplas jurisdições e blockchains.

Cooperação Internacional

A natureza transnacional das operações com criptoativos impõe uma necessidade premente de articulação internacional. Iniciativas como a **Joint Chiefs of Global Tax Enforcement (J5)** — aliança que reúne EUA, Reino Unido, Canadá, Austrália e Holanda — vêm desempenhando papel central no compartilhamento de inteligência, permitindo rastrear sonegadores globais que utilizam criptoativos como ferramenta para escapar das malhas fiscais nacionais. Essas redes de cooperação têm sido decisivas para enfrentar esquemas que ultrapassam fronteiras e exploram arbitragens regulatórias entre diferentes países.

Medidas Legais Inovadoras

Alguns países passaram a discutir a adoção de inversão do ônus da prova em certos contextos, presumindo como renda não declarada qualquer ativo cripto detectado sem origem conhecida, cabendo ao contribuinte comprovar sua licitude e a quitação de tributos devidos. Embora tais medidas esbarrem em princípios fundamentais de garantias individuais e do devido processo legal, representam um debate em curso relevante. Outro avanço envolve a equiparação formal de endereços e wallets cripto a contas financeiras tradicionais para fins de intercâmbio automático de informações entre fiscos nacionais, fortalecendo a capacidade investigativa e fiscalizatória transfronteiriça.

Os crimes tributários cometidos por meio de criptoativos constituem uma realidade incontornável no cenário contemporâneo. Sonegar impostos usando Bitcoin, Ethereum ou stablecoins não representa um novo crime, mas apenas uma roupagem tecnológica para velhos esquemas de fraude tributária — em suma, o mesmo vinho em odres novos. Cabe à comunidade jurídica, especialmente a advogados tributaristas, promotores, magistrados e reguladores, compreender tanto os aspectos técnicos (como se dão as operações e ocultações via blockchain) quanto as implicações legais e econômicas desses esquemas.

O impacto fiscal desses delitos é significativo, comprometendo a arrecadação estatal e desafiando os princípios de justiça tributária. Como demonstrado, já em 2024, casos bilionários foram expostos, enquanto muitos outros, possivelmente, permanecem ocultos no vasto e opaco universo das blockchains. O fortalecimento dos mecanismos de controle, a adaptação das

legislações e a disseminação da consciência de que os criptoativos não são um refúgio imune à lei representam vetores centrais das respostas futuras.

Fraudes Empresariais e Crimes Corporativos Envolvendo Criptoativos

Além de figurarem como instrumentos para lavagem de dinheiro e evasão fiscal, os criptoativos assumiram, em 2024, um papel central em diversos escândalos empresariais e fraudes corporativas. Aqui, tratamos de ilícitos praticados por agentes no contexto empresarial ou diretamente contra investidores e clientes, envolvendo ativos digitais – seja pela própria natureza do negócio (empresas cuja atividade principal é a operação com criptoativos e que lesaram stakeholders), seja pelo emprego de criptoativos como ferramenta de fraude em corporações tradicionais.

O surgimento e a consolidação das criptomoedas não apenas criaram novos produtos e modelos de negócio, mas também abriram espaço para delitos de colarinho branco, muitas vezes com prejuízos vultosos a investidores, consumidores e ao próprio mercado.

Colapso de Empresas Cripto e Fraudes Contra Investidores

Nos últimos anos, observou-se o colapso de exchanges e plataformas cripto que, até então, figuravam entre os gigantes do setor, ruindo em meio a escândalos de fraude empresarial. Esses episódios revelam como práticas corporativas ilícitas floresceram em um ambiente ainda pouco regulado, até atingirem um ponto de implosão inevitável.

O exemplo mais expressivo – cujos desdobramentos jurídicos ocorreram intensamente entre 2023 e 2024 – foi o da exchange FTX:

Caso FTX (Samuel Bankman-Fried)

A FTX figurava, até novembro de 2022, entre as maiores bolsas de criptomoedas globais. Após sua falência abrupta, revelou-se um sofisticado esquema de apropriação indébita e gestão fraudulenta conduzido pelos executivos da companhia, sob a liderança de Sam Bankman-Fried (SBF). Bilhões de dólares pertencentes a clientes, que deveriam estar segregados e sob custódia, foram desviados para cobrir prejuízos da afiliada Alameda Research e para uso pessoal. Em março de 2024, SBF foi condenado nos Estados Unidos a 25 anos de prisão por fraude, representando o primeiro grande caso de condenação penal de um CEO de empresa cripto por condutas equiparáveis a crimes financeiros tradicionais – um marco comparável a escândalos históricos do mercado de capitais.

O caso FTX evidencia que as fraudes corporativas clássicas – desvio de ativos de clientes, manipulação contábil, falsas declarações a investidores – encontram terreno fértil também nas empresas de criptoativos, especialmente quando operam à margem de regulações claras. O colapso deixou um rombo de mais de US$ 8 bilhões, atingindo clientes e credores, e acentuou discussões sobre a necessidade de reforço de mecanismos de governança, compliance e responsabilização pessoal no setor.

Outro episódio paradigmático, embora anterior a 2024, mas cujos reflexos persistiram, foi o do **PlusToken**. Este esquema Ponzi, estruturado na China e em outros países asiáticos, prometia retornos exorbitantes sobre investimentos em criptomoedas. Estima-se que tenha gerado prejuízos superiores a US$ 6 bilhões entre 2018 e 2019. Os organizadores foram presos e condenados em 2020, mas o caso continuou servindo como referência de como fraudes de investimento envolvendo criptoativos podem alcançar escala global, utilizando estruturas corporativas de fachada para atrair vítimas.

Em 2024, surgiram variações atualizadas desses esquemas, adaptadas a novas tendências, como NFTs e metaverso. Empresas fraudulentas apresentavam-se como startups inovadoras, prometendo lucros elevados em plataformas de arbitragem DeFi ou investimentos em ativos digitais exclusivos, mas, em essência, replicavam modelos de pirâmide financeira sob verniz tecnológico.

Importante notar que diversas fraudes corporativas clássicas passaram a ganhar versões "tokenizadas". Um exemplo recorrente é a prática de **pump and dump**: manipulação do preço de tokens emitidos por determinadas empresas, com o objetivo de inflar artificialmente sua cotação e, posteriormente, vender posições com lucro, deixando os demais investidores no prejuízo. Em 2024, autoridades como a SEC (Securities and Exchange Commission) e o DOJ (Department of Justice), nos Estados Unidos, conduziram investigações envolvendo executivos de empresas blockchain acusados de manipular preços de tokens nativos – condutas comparáveis

a insider trading e fraude contra investidores nos mercados financeiros tradicionais, mas aplicadas ao ambiente de criptoativos.

Esse panorama deixa claro que o universo cripto não apenas reproduz os velhos esquemas de fraude corporativa, mas também os potencializa, dada a velocidade das transações, a falta de transparência em determinados segmentos e a insuficiência de marcos regulatórios globalmente harmonizados. Nos próximos tópicos, aprofundaremos como os crimes empresariais relacionados a criptoativos vêm sendo operacionalizados, destacando suas nuances jurídicas e os desafios específicos que apresentam para advogados, reguladores e autoridades de enforcement.

Empresas Tradicionais Envolvidas em Infrações com Cripto

O fenômeno das infrações corporativas com cripto não é exclusivo das exchanges, startups blockchain ou empresas fintech. Instituições financeiras tradicionais, gestores de fundos e grandes corporações passaram a integrar o ecossistema de riscos, algumas vezes como canais inadvertidos de crimes, outras como responsáveis diretas por condutas omissivas ou ativas ilícitas.

Caso Binance – Violações de AML e Sanções

A Binance, a maior exchange de criptomoedas do mundo, tornou-se símbolo das tensões entre expansão global e cumprimento regulatório. Em 2023–2024, a empresa enfrentou pesadas acusações nos Estados Unidos, sendo alvo de investigações do Departamento do Tesouro (via FinCEN e OFAC) por falhas sistemáticas em seus programas de combate à lavagem de dinheiro (AML) e por violações de sanções internacionais. As acusações envolviam a facilitação de transações com entidades proibidas, incluindo grupos vinculados à Coreia do Norte e mercados darknet, totalizando mais de US$ 900 milhões em movimentações suspeitas.

Em novembro de 2023, a Binance celebrou acordo com as autoridades americanas, aceitando pagar multas bilionárias e implementar melhorias em seus controles internos, em um modelo de acordo administrativo-penal similar a um non-prosecution agreement. Embora não tenha resultado em condenação criminal formal, o caso sinalizou claramente que exchanges cripto de porte global seriam tratadas, pelo enforcement regulatório, como instituições financeiras sujeitas a sanções penais por falhas graves de compliance. Além disso, revelou que executivos da empresa teriam deliberadamente instruído clientes sobre como contornar regras de KYC (know-your-customer), configurando violações corporativas ativas e negligentes — práticas análogas aos históricos escândalos bancários, agora transpostos para o ambiente cripto.

Instituições Financeiras e Gestores de Investimento

Não apenas exchanges enfrentaram dificuldades: bancos tradicionais que ingressaram no mercado cripto também se tornaram alvos de questionamentos. Um exemplo hipotético ilustrativo é o de um banco europeu multado em 2024 por ofertar serviços de custódia de criptoativos a clientes sem estabelecer controles de compliance mínimos, permitindo que contas fossem usadas para movimentação de recursos de origem obscura. Nesses casos, configuram-se ilícitos omissivos: falhas de dever legal de diligência, que acabam por facilitar práticas de lavagem de dinheiro.

Além disso, gestores de fundos hedge focados em cripto foram investigados por fraudes cometidas contra seus próprios investidores, incluindo a falsificação de relatórios de performance e ocultação do real nível de exposição a ativos digitais. Esses episódios reforçam que, independentemente do setor, a incorporação de criptoativos às operações exige rigor absoluto de governança e controles internos, sob pena de incorrer em responsabilidade penal e administrativa.

Uso de Cripto para Corrupção Privada ou Desvio de Recursos

Outra faceta relevante refere-se ao emprego de criptomoedas para corrupção privada e desvio patrimonial dentro de corporações não ligadas diretamente ao setor cripto. Em investigações recentes, surgiram casos de diretores de compras de grandes multinacionais que teriam recebido propinas em Bitcoin, depositadas em carteiras anônimas, como contrapartida por favorecimento em processos de contratação. O raciocínio por trás do uso da cripto nesses contextos é evidente: menor rastreabilidade, maior facilidade de ocultação e ausência de intermediários bancários.

Também foram reportados episódios em que executivos ou tesoureiros desviaram recursos corporativos, transferindo-os para carteiras pessoais sob controle próprio, aproveitando lacunas no monitoramento interno e seu conhecimento técnico superior sobre os ativos. Esses casos configuram crimes empresariais típicos, como apropriação indébita e abuso de confiança, mas com a peculiaridade de envolverem instrumentos digitais que dificultam o rastreamento e a recuperação dos bens.

Estruturas Societárias e Ocultação: Empresas de Fachada, Offshore e Cripto

A utilização de estruturas empresariais para viabilizar esquemas ilícitos envolvendo criptoativos tornou-se prática recorrente, associando elementos de planejamento societário sofisticado a instrumentos digitais.

Empresas de Fachada e Shell Companies

Empresas de fachada, historicamente empregadas em esquemas de lavagem e evasão fiscal, passaram a atuar também no campo cripto. A diferença é que, atualmente, essas entidades não apenas detêm contas bancárias, mas também mantêm carteiras em exchanges e wallets próprias, movimentando valores em criptoativos sob a proteção de uma casca corporativa. Em vez de uma offshore abrir conta em banco X, ela abre conta em exchange Y, movimentando milhões em Bitcoin, Ether ou stablecoins, protegida por estruturas de anonimato corporativo.

Como destaca Subashi (2024), os Offshore Financial Centers, conhecidos pelo sigilo empresarial, passaram a observar crescente uso de criptoativos como instrumentos de ocultação patrimonial. Muitas exchanges globais estão incorporadas nessas jurisdições offshore, o que facilita ainda mais a sobreposição entre anonimato societário e anonimato financeiro. Combater essa arquitetura ilícita exige esforços conjuntos nos âmbitos societário (aumentando a transparência de beneficiários finais) e financeiro (reforçando obrigações de compliance nas exchanges).

Trusts, Veículos Fiduciários e Criptoativos

Outro elemento sofisticado são os trusts e fundações privadas, tradicionalmente utilizados para proteção patrimonial e planejamento sucessório, agora incorporando criptoativos em suas carteiras. Um trust constituído, por exemplo, nas Ilhas Virgens Britânicas pode declarar a posse de criptomoedas custodiadas por terceiros, dificultando esforços de penhora ou execução por autoridades estrangeiras.

Essa camada adicional de opacidade agrava os desafios para a identificação do beneficiário final e complica iniciativas de enforcement internacional. O uso combinado de estruturas fiduciárias e criptoativos é, atualmente, um dos pontos mais sensíveis no combate à evasão fiscal, à lavagem e a outros crimes econômicos transnacionais. Embora governos estejam avançando em regulamentações para exigir a inclusão de criptoativos nas declarações de beneficiário final, a eficácia desses esforços ainda é parcial.

Em síntese, o ambiente empresarial representa, simultaneamente, veículo e vítima das infrações envolvendo criptoativos. As empresas, enquanto entidades, podem ser utilizadas para mascarar operações ilícitas; por outro lado, elas mesmas podem ser alvo de fraudes internas praticadas por agentes oportunistas. A interligação entre os mundos societário, financeiro e digital eleva o grau de complexidade e exige, dos operadores do direito, conhecimento aprofundado das ferramentas, estruturas e práticas que atravessam esse universo.

Governança, Responsabilidades e Medidas Preventivas nas Empresas Cripto

Os eventos ocorridos em 2024 impulsionaram debates consistentes sobre governança e compliance no setor cripto, mesmo que este livro não tenha por foco sugerir políticas públicas ou regulatórias. É essencial, porém, abordar analiticamente como as práticas corporativas evoluíram diante dos escândalos recentes, e quais implicações isso trouxe para advogados, empresários e investidores envolvidos no mercado.

Adoção de Estruturas de Transparência e Auditoria

As empresas cripto de grande porte, abaladas pela queda vertiginosa de confiança após casos como FTX, iniciaram um movimento de aproximação às melhores práticas das instituições financeiras tradicionais. Este movimento incluiu:

Relatórios de prova de reservas: medida destinada a demonstrar que as exchanges detêm, de fato, os ativos que alegam manter sob custódia, fornecendo maior segurança aos usuários.

Auditorias independentes: não apenas sobre o saldo das reservas, mas também sobre os balanços contábeis, estrutura de governança, fluxo operacional e exposição a riscos.

Divulgação clara de riscos: com ênfase nos contratos e termos de uso, tornando mais explícito ao investidor o grau de incerteza e volatilidade do ambiente cripto.

Esses avanços não foram voluntaristas: a condenação de Sam Bankman-Fried (SBF) e a responsabilização administrativa e penal da Binance funcionaram como um aviso contundente de que nem mesmo os líderes do mercado escapariam das consequências legais por má gestão, negligência ou participação deliberada em práticas ilícitas.

Empresas Tradicionais e as Políticas Internas Relacionadas a Cripto

Do lado das empresas fora do núcleo do mercado cripto, houve crescente preocupação em regular o uso de criptomoedas dentro das operações corporativas. Algumas das medidas adotadas incluíram:

Proibição formal do uso de criptoativos em transações corporativas não autorizadas.

Protocolos internos de monitoramento, visando identificar tentativas de pagamento de fornecedores ou recebimento de clientes por meio de ativos digitais, especialmente em setores sob forte regulação.

Treinamentos internos para departamentos financeiros e de compliance, capacitando equipes para reconhecer indícios de fraudes associadas a pagamentos em cripto, como características suspeitas em faturas ou contratos.

Além disso, tornou-se comum que, nas diligências prévias (due diligence) realizadas em operações comerciais, fossem incluídas avaliações específicas quanto ao envolvimento da contraparte com ativos digitais — não apenas para mapear riscos de mercado, mas também para identificar potenciais riscos reputacionais e de compliance regulatório.

Implicações para o Advogado e Operador Jurídico

Para os advogados que atuam na esfera empresarial, o cenário de 2024 trouxe uma lição clara: lidar com criptoativos não é mais um diferencial técnico ou um detalhe periférico, mas sim uma competência indispensável. As implicações incluem:

Revisão criteriosa de contratos e cláusulas específicas sobre ativos digitais, garantindo que estejam cobertos aspectos como compliance, reporte, deveres fiduciários e eventuais garantias.

Avaliação do risco reputacional e jurídico em relações negociais com players do setor cripto, exigindo pesquisas aprofundadas sobre histórico regulatório, reputação e postura frente a sanções.

Capacidade de distinguir elementos técnicos e intencionais, principalmente em litígios envolvendo empresas cripto — onde muitas vezes será necessário diferenciar, do

ponto de vista probatório e argumentativo, um mero insucesso de mercado (não raro em startups) de uma conduta que configure fraude, má-fé ou gestão temerária.

No campo penal, promotores e advogados criminais enfrentam o desafio adicional de enquadrar adequadamente essas condutas à luz do ordenamento vigente, sobretudo na separação entre ilícitos civis, administrativos e penais, evitando confusões conceituais comuns no debate público sobre criptoativos.

Os crimes empresariais envolvendo criptoativos em 2024 revelaram duas faces complementares:

Empresas cripto lesando investidores e clientes, frequentemente por ausência de controles robustos ou por atos fraudulentos deliberados de seus gestores.

Uso de criptomoedas como ferramenta dentro de empresas tradicionais, servindo a esquemas de lavagem, corrupção privada e outras infrações corporativas.

A natureza transnacional, rápida e muitas vezes opaca dos criptoativos cria dificuldades adicionais na prevenção, detecção e repressão desses ilícitos. Porém, os episódios recentes também funcionaram como um catalisador, estimulando avanços em governança, compliance e monitoramento, tanto no setor específico de cripto quanto em corporações que passaram a lidar com ativos digitais.

Para a comunidade jurídica, fica o alerta: episódios como FTX e Binance não são desvios acidentais de startups mal geridas, mas sim escândalos financeiros em escala global, demandando o mesmo rigor, conhecimento técnico e capacidade de atuação que já se exige há décadas nos casos clássicos de colarinho branco e infrações econômicas. Dominar os aspectos regulatórios, operacionais e tecnológicos do mundo cripto tornou-se não apenas desejável, mas necessário para qualquer profissional sério do Direito Empresarial e Penal Econômico.

Exchanges, Mixers, Bridges e DeFi: Ferramentas Tecnológicas do Crime Moderno

Exchanges Centralizadas: Portas de Entrada e Saída

As exchanges centralizadas de criptomoedas (CEXs) são, sem exagero, o epicentro do fluxo entre o mundo dos criptoativos e o sistema financeiro tradicional. Elas desempenham funções essenciais para usuários legítimos e criminosos, operando como mercados globais para a compra, venda e custódia de ativos digitais. Entre os exemplos mais conhecidos estão Binance, Coinbase, Kraken e Huobi.

No contexto criminal, porém, as exchanges centralizadas cumprem um papel especialmente sensível: são os canais privilegiados de **conversão** entre criptoativos e moedas fiduciárias (fiat), funcionando como as principais portas de entrada e saída do ecossistema cripto. Estima-se que mais da metade dos fundos ilícitos gerados ou circulados no universo digital acabem, inevitavelmente, passando por exchanges centralizadas em algum momento. Isso as torna, simultaneamente:

- Um gargalo crucial para a aplicação de políticas antilavagem de dinheiro (AML) e know-your-customer (KYC),

- E, paradoxalmente, um dos pontos preferenciais de exploração por criminosos.

Atração Criminosa: Brechas e Jurisdições Permissivas

Os agentes ilícitos buscam, deliberadamente, exchanges situadas em jurisdições com:

- Regulamentação branda,

- Controles frouxos de identificação,

- Ou reputação de complacência com fluxos suspeitos.

Essas corretoras operam como verdadeiros "bancos paralelos", permitindo a troca de ativos digitais por moeda real com mínima supervisão. Por meio delas, criminosos conseguem:

- Transformar ganhos ilícitos em liquidez convencional,

- Misturar fundos sujos e limpos em grandes volumes de transações,

- E, em alguns casos, até driblar sanções internacionais, transacionando com países ou entidades proibidas.

O caso da Binance é emblemático: sob intenso escrutínio das autoridades americanas em 2023–2024, a empresa enfrentou acusações severas de violações à Bank Secrecy Act, falhas de AML e facilitação indireta de fluxos ilícitos. O acordo bilionário firmado com o Departamento do Tesouro dos EUA, incluindo compromissos de melhoria no compliance, não apagou o fato de que a plataforma havia, por anos, sido um canal de predileção para criminosos e atores sancionados.

O Outro Lado: Cooperação, Fiscalização e Interdição

Por outro lado, nem todas as exchanges são igualmente vulneráveis ou cúmplices. Ao contrário, uma parcela crescente das CEXs vem:

- Cooperando ativamente com autoridades,

- Fornecendo informações sobre usuários e movimentações suspeitas,

- E bloqueando ou congelando ativos quando identificados como frutos de atividades ilícitas.

Essa colaboração torna as exchanges pontos-chave para investigações: trilhar o caminho do dinheiro até a corretora, obter dados de cliente e eventualmente travar os saques em moeda fiduciária passou a ser uma das estratégias prioritárias em operações de enforcement.

Os próprios criminosos, conscientes dessa vulnerabilidade, passaram a fracionar valores, recorrer a intermediários (laranjas) ou movimentar fundos por múltiplas exchanges antes de converter – tentando, assim, pulverizar os rastros.

Tendências e Desafios Regulativos

O movimento global é claro: equiparar progressivamente as exchanges centralizadas às instituições financeiras tradicionais em termos de obrigações legais e regulatórias. Isso inclui:

- Deveres robustos de compliance (KYC, AML),

- Deveres de reporte e retenção de informações,

- Responsabilização civil, administrativa e penal em caso de negligência deliberada ou facilitação consciente de crimes.

Contudo, essa tendência não elimina os desafios:

- Nem todas as jurisdições adotam padrões homogêneos.

- Algumas exchanges migram sedes para regiões mais permissivas.

- E, mesmo com regras mais rígidas, a aplicação prática depende de recursos humanos e tecnológicos adequados – tanto dentro das exchanges quanto nas agências reguladoras.

As exchanges centralizadas ocupam uma posição ambígua e estratégica: para os criminosos, representam uma oportunidade irresistível de escoamento e monetização de capital ilícito; para as autoridades, são pontos privilegiados de interdição, onde o dinheiro sujo pode ser identificado e bloqueado antes de atingir o sistema bancário.

No universo jurídico, entender essas dinâmicas não é opcional: advogados, reguladores e profissionais de compliance precisam conhecer a fundo como essas plataformas operam, quais brechas oferecem, quais controles aplicam e, sobretudo, quais riscos jurídicos estão associados a sua utilização – seja pelo cliente final, seja pela própria empresa. É nesse ponto de interseção entre tecnologia, mercado e direito que se decide quem controla o fluxo: os agentes ilícitos, ou os mecanismos legais e regulatórios.

Diferentemente das exchanges centralizadas, as DEX e os protocolos DeFi funcionam sem intermediários custodiantes, sem registro prévio e, sobretudo, sem exigência de identificação do usuário. Em redes como Ethereum, Binance Smart Chain, Avalanche e outras, os usuários podem realizar trocas anônimas de tokens, fornecer liquidez, contrair empréstimos, operar derivativos e participar de apostas on-chain – tudo orquestrado por contratos inteligentes.

Embora representem uma inovação legítima, eficiente e alinhada ao ethos de descentralização, essas ferramentas também passaram a integrar o arsenal operacional de criminosos digitais. A seguir, destrinchamos as principais facetas desse uso.

Exchanges Descentralizadas (DEX)

As DEX operam por meio de contratos inteligentes que emparelham ordens de compra e venda diretamente entre usuários, eliminando a figura da corretora intermediária. Qualquer pessoa com uma carteira compatível pode interagir com esses protocolos: não há login, não há KYC, não há cadastro.

Os criminosos exploram essas características para:

- Trocar rapidamente tokens de origem ilícita (por exemplo, Ether hackeado) por outros ativos "limpos" (como stablecoins),

- Diluir o histórico contaminado dos tokens originais ao misturá-los em pools de liquidez compostos por milhares de participantes.

Imagine um hacker que rouba 500 ETH: ele pode, em minutos, trocar esses ativos por USDC ou DAI em uma DEX como Uniswap. A transação, embora visível na blockchain, "desaparece" em termos práticos, pois os fundos são embaralhados no fluxo coletivo. Essa prática atua, na prática, como uma forma de mixing descentralizado, dificultando a análise posterior.

Além disso, as DEX possibilitam o chamado **chain-hopping indireto**: por meio de wrappers e bridges, o criminoso pode converter ativos entre diferentes blockchains sem jamais tocar uma exchange centralizada, pulando de Ethereum para Binance Smart Chain, depois para Polygon e assim por diante.

Protocolos DeFi de Empréstimo e Pooling

Os protocolos de empréstimo (como Aave, Compound, MakerDAO) e os pools de liquidez oferecem oportunidades sofisticadas de ocultação. Criminosos podem:

Depositar ativos ilícitos como garantia e contrair empréstimos em outro ativo, limpando o valor, já que ficam com um ativo novo e sem vínculo direto com a origem.

Fornecer liquidez a pools, misturando seus fundos aos de outros usuários, para depois sacar quantias equivalentes, com rastros diluídos.

Essas operações, embora tecnicamente visíveis na blockchain, embaralham a trilha do dinheiro ao fundi-lo em operações legítimas, diluindo o rastro do ativo original.

Outros Protocolos e Técnicas

Outros mecanismos também foram incorporados ao repertório criminal:

Tumbling descentralizado: Serviços como Tornado Cash permitem misturar tokens via contratos inteligentes, cortando o elo entre remetente e destinatário.

Plataformas de apostas on-chain: Assim como cassinos físicos, sites de gambling que aceitam cripto são usados para depositar fundos ilícitos, simular apostas e sacar os ganhos em outro ativo, justificando a origem.

NFTs como ferramenta de lavagem: Um método em ascensão é o chamado **wash trading** com NFTs. O criminoso cria um NFT, compra-o de si mesmo usando fundos ilícitos (movimentando de uma wallet controlada para outra), e declara esses recursos como provenientes da venda de "arte digital". Esse expediente chamou atenção de reguladores justamente pelo potencial de justificar movimentações milionárias sob uma aparência criativa e inovadora.

O Atrativo Central: Ausência de KYC

O verdadeiro chamariz das plataformas DeFi para criminosos reside na ausência de procedimentos obrigatórios de identificação. Ao contrário das exchanges centralizadas, que estão

cada vez mais alinhadas a requisitos AML e KYC, os protocolos DeFi operam em código aberto, permitindo acesso irrestrito.

Contudo, é importante frisar: todas essas interações deixam registros públicos na blockchain. O desafio para autoridades e analistas não está em identificar que a transação ocorreu – mas em vincular os endereços aos indivíduos. Aqui está a grande muralha tecnológica e investigativa.

Inovações para Equilibrar Privacidade e Conformidade

Em 2024, surgiram iniciativas que tentam oferecer um meio-termo: protocolos que utilizam provas de conhecimento zero (ZKPs), como o Railgun, permitindo que usuários provem que seus fundos não advêm de fontes ilícitas sem revelar detalhes de identidade. Tais soluções, ainda experimentais, visam equilibrar a privacidade essencial das finanças descentralizadas com as demandas de compliance regulatório.

As exchanges e protocolos DeFi levantam perguntas inéditas para o direito penal, empresarial e regulatório:

- Quem responde por um protocolo amplamente usado para lavagem, se não há empresa nem pessoa gerindo-o diretamente?

- Desenvolvedores de código-fonte podem ser criminalmente responsabilizados pelas consequências do uso de seus contratos inteligentes?

- Como distinguir entre liberdade de programação (expressão) e facilitação objetiva de ilícitos?

Casos como o de Tornado Cash, cujo desenvolvedor foi preso nos EUA em 2022, demonstram que autoridades vêm tentando enquadrar indivíduos mesmo em sistemas teoricamente descentralizados – gerando debates jurídicos que ainda estão longe de se resolver.

As ferramentas DeFi e as exchanges descentralizadas consolidaram-se como parte do arsenal do crime financeiro moderno, funcionando não apenas como alternativas tecnológicas, mas como verdadeiros multiplicadores de complexidade investigativa. Para juristas e profissionais do setor, compreender essas estruturas é essencial: não apenas para enquadrar condutas ilícitas, mas também para construir sistemas contratuais e empresariais robustos, capazes de mitigar riscos e lidar com as responsabilidades emergentes desse novo ecossistema.

Misturadores de Criptomoedas (Mixers)

Embora já apresentados anteriormente sob o aspecto operacional, os mixers merecem atenção autônoma como serviços especializados historicamente associados à atividade ilícita no ecossistema cripto. Esses serviços, que surgiram com os primeiros anos do Bitcoin, têm como objetivo central garantir anonimato transacional absoluto, embaralhando fluxos financeiros para tornar virtualmente impossível rastrear a origem e o destino de fundos.

Atualmente, coexistem duas vertentes principais:

- **Mixers centralizados**: websites que coletam criptomoedas de múltiplos usuários e redistribuem quantias equivalentes a endereços fornecidos, criando um "pool" comum que quebra a trilha original.

- **Mixers descentralizados**: baseados em smart contracts ou pools CoinJoin (como no Bitcoin), que realizam a mistura sem uma entidade controladora.

Ainda que tais ferramentas tenham argumentos legítimos em defesa da privacidade financeira – como proteger usuários comuns contra vigilância massiva –, estudos recentes apontam que a esmagadora maioria do volume transacionado por mixers está ligada a atividades criminosas, desde fraudes e hacks até lavagem e financiamento ilícito.

Dois mixers ganharam especial proeminência nos relatórios investigativos e de análise financeira no ano de 2024:

Tornado Cash

O Tornado Cash permanece como o caso paradigmático entre os mixers, operando na rede Ethereum para Ether e tokens ERC-20.

Mesmo após ter sido formalmente sancionado pelos EUA em 2022, o Tornado continuou funcional: afinal, trata-se de um contrato inteligente autônomo que reside permanentemente na blockchain, sem controle externo direto ou botão "off". Essa resiliência estrutural tornou-o irresistível para agentes maliciosos.

Dados mostram que, em janeiro de 2024, aproximadamente **US$234 milhões fluíram de Tornado Cash diretamente para bridges**, sugerindo que hackers e lavadores usaram o Tornado como etapa inicial antes de transferir valores entre blockchains, escalonando a ocultação. A opacidade oferecida era tamanha que os poucos sinais visíveis residiam em padrões indiretos,

como **picos anormais de taxas de transação** pagos para acelerar saques logo após grandes hacks.

A resposta das autoridades foi robusta e inovadora: além das sanções, **desenvolvedores foram presos** e formalmente acusados de facilitar lavagem de dinheiro. Esse movimento jurídico abriu debates espinhosos, pois, em tese, o código do Tornado não distingue entre valores lícitos e ilícitos. Contudo, o uso esmagadoramente criminoso do protocolo levou-o a ser tratado pelas autoridades quase como uma entidade criminosa em si.

eXch e Mixers Emergentes

Com o endurecimento sobre mixers estabelecidos, surgiram alternativas menos conhecidas, como o chamado **eXch**, mencionado em relatório da SlowMist.

Em 2024, o eXch teve um crescimento impressionante de **579% em depósitos de tokens**, atraindo atenção por estar vinculado a agentes estatais maliciosos, especialmente norte-coreanos, devido à sua recusa sistemática em cooperar com autoridades. Essa tendência revela um padrão previsível: à medida que repressões caem sobre um mixer, a demanda migra para outro, frequentemente ainda mais descentralizado, automatizado e resistente à censura.

O Dilema Jurídico: Entre Privacidade e Uso Criminoso

Do ponto de vista jurídico, os mixers representam um desafio singular. Eles são serviços cuja arquitetura tecnológica nasceu para proteger a privacidade de qualquer usuário na blockchain, blindando-o contra bisbilhotagem generalizada. No entanto, o abuso criminoso desses serviços é tão dominante que eles se tornaram, aos olhos das autoridades, praticamente sinônimos de lavagem.

Em países como os Estados Unidos, mixers passaram a ser enquadrados como Money Service Businesses (MSBs), ou seja, entidades obrigadas a cumprir normas de combate à lavagem (AML) e de identificação de usuários (KYC). Essa imposição, porém, se choca com a realidade tecnológica: muitos mixers simplesmente não possuem estrutura para implementar tais controles, empurrando-os para a clandestinidade.

Valor Probatório e Presunções Investigativas

Para investigadores e peritos, o uso de mixers é hoje interpretado quase como uma "marca d'água criminal". Um laudo técnico que identifica que determinado ativo saiu recentemente de um mixer tende a afirmar:

"Os ativos nesta carteira têm alta probabilidade de origem ilícita por terem sido misturados, interrompendo a rastreabilidade."

Ou seja, ainda que não seja possível seguir a trilha para além do mixer, o simples uso já levanta suspeita robusta de intenção de ocultação. Essa inversão prática de ônus coloca o usuário sob pressão jurídica para justificar por que precisou usar um serviço notoriamente empregado por agentes ilícitos.

Os mixers são talvez o exemplo mais evidente de como tecnologias de anonimização – criadas sob o pretexto de proteger direitos individuais – podem ser apropriadas massivamente pelo crime organizado. No contexto jurídico, compreender essas ferramentas é essencial não apenas para traçar estratégias processuais, mas também para aconselhar clientes corporativos e investidores sobre os riscos de exposição e as responsabilidades emergentes, inclusive em transações indiretas.

Bridges (Pontes Blockchain) e Ferramentas de Cross-Chain

As bridges, ou pontes blockchain, representam uma das inovações mais poderosas e, ao mesmo tempo, mais desafiadoras no cenário cripto contemporâneo. Elas viabilizam a transferência de ativos digitais entre diferentes blockchains, seja bloqueando tokens em uma rede e emitindo representações equivalentes na outra, seja por mecanismos de swap direto entre partes. Do ponto de vista técnico, bridges são fundamentais para a interoperabilidade entre ecossistemas (por exemplo, conectar Ethereum, BNB Chain, Tron, Polygon), permitindo uma fluidez de capitais até então impossível.

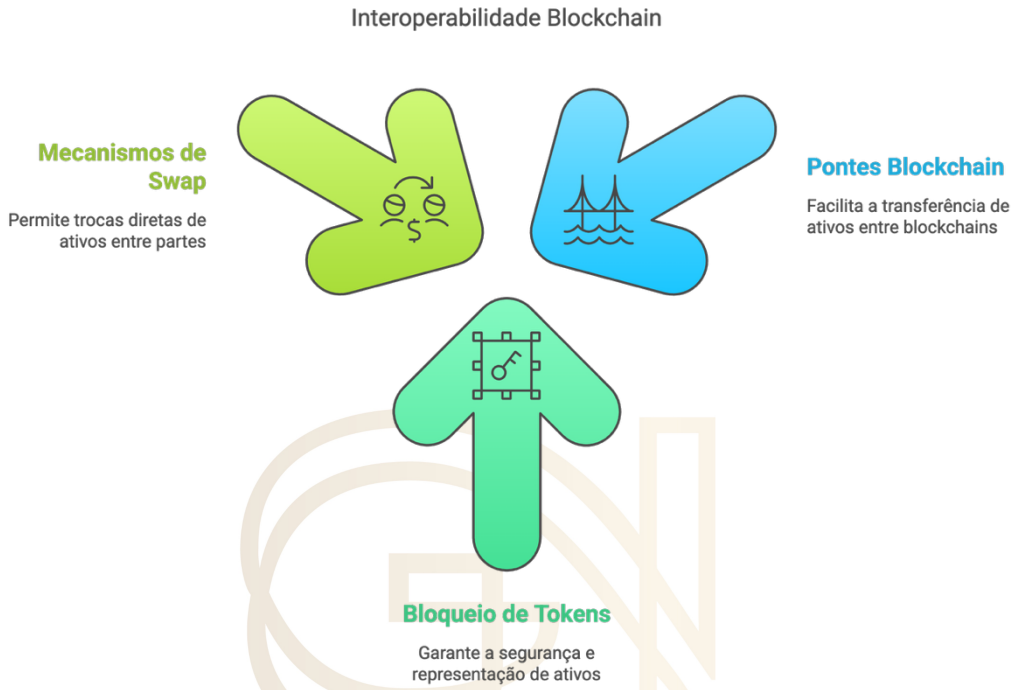
Contudo, essa fluidez foi rapidamente absorvida pelas estratégias ilícitas.

Uso Criminoso e Cenário Atual

Em 2024, o uso ilícito de bridges atingiu patamares recordes. Grupos como o notório Lazarus (ligado à Coreia do Norte) incorporaram sistematicamente pontes em suas operações: após ataques cibernéticos em uma rede, dispersavam os fundos roubados através de múltiplas outras blockchains, dificultando drasticamente o rastreamento.

O caso **Ronin Bridge** (Axie Infinity, 2022) continua emblemático: hackers norte-coreanos, após roubarem ETH, converteram os ativos em outras moedas e os redistribuíram por redes como

BNB Chain e Tron, criando uma teia de hops e conversões que só foi parcialmente desvendada meses depois. Em 2024, o modus operandi seguiu a mesma lógica, com fluxos ilícitos cruzando pontes que processaram, em certos meses, **centenas de milhões de dólares em ativos suspeitos**.



Importante destacar: as bridges, em si, não são ilegais. São, na verdade, ferramentas legítimas de interoperabilidade, amplamente usadas por projetos DeFi. O problema reside na ausência de monitoramento centralizado. Quando fundos ilícitos ingressam em uma ponte descentralizada, saem do outro lado em endereços não vinculados diretamente aos originais, muitas vezes em moedas diferentes. É, metaforicamente, como atravessar fronteiras físicas com dinheiro vivo: a jurisdição muda, as autoridades precisam de novas ferramentas para continuar a perseguição.

Empresas de análise blockchain vêm desenvolvendo técnicas avançadas para mapear fluxos multi-chain, integrando dados de diferentes blockchains e criando trilhas investigativas. Porém, essa tarefa exige perícia sofisticada e um volume enorme de dados inter-relacionados. Além disso, o desafio jurídico vai além do rastreamento:

- Quem é o responsável por uma bridge?

- Quem pode ser compelido a cumprir KYC, se muitas dessas pontes são geridas por DAOs (Organizações Autônomas Descentralizadas), sem entidade jurídica formal?

Diferentemente das exchanges centralizadas, onde há pessoas jurídicas claramente identificáveis, as bridges muitas vezes operam sem "alvo institucional" para ação regulatória.

Em 2024, surgiram propostas que incluem:

- Obrigar exchanges centralizadas a filtrarem depósitos provenientes de bridges de alto risco (assim como já fazem com mixers sancionados);

- Desenvolver "blockchain spiders" – contratos inteligentes ou sistemas de monitoramento que buscam automaticamente padrões suspeitos de lavagem cross-chain e os sinalizam em tempo real.

Entretanto, a efetividade dessas soluções ainda é incipiente. Muitas vezes, os lavadores apenas migram para bridges menos conhecidas ou recém-lançadas, seguindo o ciclo de repressão e adaptação constante.

As bridges transformaram-se em uma peça central do quebra-cabeças investigativo que cerca os crimes financeiros com criptoativos. Elas representam, simultaneamente, o símbolo máximo da promessa cripto – interoperabilidade, liberdade, descentralização – e uma das ferramentas prediletas de lavadores internacionais.

Do ponto de vista jurídico e regulatório, o enfrentamento do abuso de pontes depende menos de ações diretas contra as bridges (dada sua natureza técnica e descentralizada) e mais de inteligência colaborativa, cooperação internacional e, sobretudo, reforço de controles nos pontos finais – ou seja, nas exchanges e serviços onde os fundos, depois de saltarem entre redes, precisam finalmente ser monetizados.

Os blocos tecnológicos que compõem o ecossistema cripto – exchanges (centralizadas e descentralizadas), mixers, bridges e protocolos DeFi – têm, todos, um papel ambivalente. São alicerces de inovação, mas também são explorados intensamente para ocultação de valores, fraudes e lavagem. O ano de 2024 marcou avanços simultâneos: de um lado, criminosos cada vez mais sofisticados em explorar essas ferramentas; de outro, autoridades, empresas e a própria comunidade cripto avançando em técnicas de detecção, bloqueio e autorregulação.

Para advogados, investigadores e empresários, entender esses mecanismos não é mais um diferencial – é um requisito básico para lidar com qualquer operação, contrato ou litígio que envolva criptoativos. A próxima seção trará as conclusões gerais desta análise, destacando as lições aprendidas e as perspectivas para o futuro.

Conclusão

O ano de 2024 cristalizou os criptoativos como peças centrais não apenas no mercado econômico, mas também no ecossistema criminal internacional. Este livro percorreu, com rigor técnico e detalhamento jurídico, os múltiplos aspectos do uso ilícito das criptomoedas — das condutas tributárias e empresariais às sofisticadas estratégias tecnológicas empregadas para lavagem, evasão e fraude.

Ao final desta jornada analítica, algumas conclusões se destacam de forma incontornável:

Onipresença dos Criptoativos no Delito Financeiro Moderno

O que antes parecia domínio restrito de cibercriminosos altamente especializados tornou-se, hoje, um recurso comum para traficantes, corruptos, sonegadores e fraudadores do mais diverso espectro. O volume estimado — entre US$ 40 e 50 bilhões transacionados para endereços ilícitos apenas em 2024 — evidencia que os criptoativos não são apenas uma ferramenta pontual, mas um verdadeiro fio condutor interligando delitos tradicionais em escala global.

Para o advogado tributarista, empresarial ou penalista, essa constatação exige uma reorientação metodológica: não basta mais olhar apenas para movimentações bancárias ou estruturas societárias clássicas; é necessário incluir no radar o ecossistema blockchain como ambiente ordinário das operações financeiras.

Desafios à Investigação e à Responsabilização Jurídica

As dificuldades aqui não surgem primariamente da tipificação penal — a legislação já prevê os crimes em si, como lavagem, sonegação, corrupção ou apropriação indébita. O verdadeiro obstáculo está na prova. Como vincular uma carteira anônima a uma pessoa física? Como rastrear fundos que saltaram por mixers e bridges? Como enquadrar juridicamente condutas distribuídas em protocolos DeFi sem administrador ou controle central?

Em 2024, os avanços tecnológicos mostraram que a blockchain também oferece armas investigativas: registros imutáveis, análises de padrões, e novas técnicas de inteligência artificial para detecção de fluxos suspeitos. Além disso, precedentes marcantes, como a condenação do CEO da FTX, sinalizaram que grandes infratores serão responsabilizados, ainda que operem no setor cripto.

Cooperação Internacional e Atualização Normativa

Nenhuma jurisdição, por mais robusta que seja, conseguirá conter isoladamente os crimes relacionados a criptoativos. A natureza transnacional dessas operações demanda alinhamento regulatório, intercâmbio de informações e esforços conjuntos. A atuação de organismos como o FATF/GAFI, bem como as medidas unilaterais (como sanções aplicadas pelos EUA a mixers), evidenciam uma tendência: trazer os criptoativos para dentro do aparato normativo e de compliance que já rege as instituições financeiras tradicionais.

Exchanges, custodiantes, gestores e até protocolos descentralizados começam a ser incluídos no escopo de obrigações de KYC, AML e reporte tributário. A lacuna, porém, ainda existe — e explorá-la tem sido o jogo preferido de lavadores e sonegadores.

Governança Corporativa e Risco Reputacional

Os casos analisados reforçam que as empresas — tanto do setor cripto quanto de setores tradicionais — não podem mais tratar os criptoativos como uma exceção marginal aos seus sistemas de controle. Muito pelo contrário: pela volatilidade, pseudonimato e complexidade tecnológica, esses ativos exigem governança ainda mais rigorosa.

Segregação patrimonial, auditoria independente, cláusulas contratuais específicas, verificação de parceiros, due diligence reforçada — tudo isso torna-se imprescindível não apenas para evitar colapsos catastróficos (como no caso FTX), mas para proteger dirigentes e conselhos de administração contra responsabilidades pessoais por falhas de gestão.

Evolução Constante e Necessidade de Atualização Contínua

Talvez o ponto mais central: a dinâmica criminal envolvendo criptoativos não é estática. A cada técnica de ocultação mitigada — como os mixers centralizados — surge uma alternativa mais sofisticada, como mixers descentralizados e fluxos cross-chain. Isso impõe ao operador jurídico uma postura de atualização constante, interdisciplinaridade e abertura a conceitos de tecnologia, segurança digital e finanças avançadas.

Doutrinas clássicas permanecem válidas: o tipo penal de lavagem não depende do meio tecnológico, assim como fraude corporativa não deixa de ser fraude porque envolve tokens digitais. Mas os fatos, os meios e as provas mudaram — e compreender blockchain, smart contracts e DeFi deixou de ser diferencial: passou a ser pré-requisito.

Os crimes envolvendo criptoativos em 2024 sintetizam uma dualidade peculiar: de um lado, números alarmantes de atividades ilícitas — bilhões lavados, milhões sonegados, investidores lesados em escala global; de outro, uma mobilização crescente de autoridades, reguladores, técnicos e até da própria comunidade cripto para enfrentar esses desafios. Novas técnicas

investigativas, colaborações público-privadas, regulamentações aprimoradas e medidas internas de compliance começaram a pavimentar um caminho para conter os abusos sem sufocar a inovação.

Para advogados, juristas e investidores, fica clara a necessidade de abandonar qualquer visão futurista ou distante sobre criptoativos: eles já são realidade jurídica, regulatória e econômica presente, e atuar sobre crimes tributários e corporativos nesse cenário demanda domínio técnico, inteligência estratégica e compromisso com um Direito capaz de dialogar com a inovação.

Em última análise, o blockchain é uma tecnologia neutra. Seu potencial construtivo — para inclusão financeira, transparência, eficiência — só será plenamente realizado se os sistemas jurídicos souberem conter seu uso espúrio, garantindo que os avanços tecnológicos sirvam à prosperidade responsável e permaneçam ancorados no Estado de Direito. É este o desafio central que permanece à frente, e que cada profissional da área deve estar pronto a enfrentar.

Referências

BOEHM, Camila. PF prende investigado por lavagem de dinheiro com criptoativos: de 2017 a 2021, homem movimentou mais R$ 13 bilhões. Agência Brasil, São Paulo, 8 jan. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-01/pf-prende-investigado-por-lavagem-de-dinheiro-com-criptoativos. Acesso em: 29 abr. 2025.

CHAINALYSIS. 2024 Crypto Crime Report. Chainalysis, 2025. Disponível em: https://go.chainalysis.com/2025-Crypto-Crime-Report.html. Acesso em: 5 mai. 2025.

CHAINALYSIS. Money Laundering and Cryptocurrency. Chainalysis, 2024. Disponível em: https://www.chainalysis.com/blog/money-laundering-cryptocurrency/. Acesso em: 5 mai. 2025.

G1 SP. Investigado por lavagem de dinheiro com criptoativos é preso pela Polícia Federal ao tentar embarcar para Dubai no Aeroporto de Guarulhos: segundo a PF, homem tinha residência fixa em Dubai e apresentou movimentação bancária superior a R$ 1,4 bilhões em apenas 10 meses; empresa controlada por ele também movimentou R$ 13 bilhões em quatro anos. G1, 8 jan. 2024. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2024/01/08/investigado-por-lavagem-de-dinheiro-com-criptoativos-e-preso-pela-policia-federal-ao-tentar-embarcar-para-dubai-no-aeroporto-de-guarulhos.ghtml. Acesso em: 29 abr. 2025.

ICA ADVANCED. Stablecoins: The New Epicentre of Crypto Fraud. ICA Advanced, 2025. Disponível em: https://www.int-comp.org/insight/stablecoins-the-new-epicentre-of-crypto-fraud/. Acesso em: 5 mai. 2025.

KAMENSKY, Dmitriy; CHERNYAK, Andrii; DUDOROV, Oleksandr; FEDUN, Igor; KLYMENKO, Serhii. Laundering of Criminal Proceeds Through Cryptocurrency Transactions: A Digital Threat to Economic Security. The Law, State and Telecommunications Review, v. 16, n. 2, p. 179-199, out. 2024. Disponível em: https://doi.org/10.26512/lstr.v16i2.52003. Acesso em: 5 mai. 2025.

SLOWMIST. Analysis of the 2024 Blockchain Security and Anti-Money Laundering Annual Report: DPRK & Money Laundering Tools. SlowMist, 2024. Disponível em: https://slowmist.medium.com/analysis-of-the-2024-blockchain-security-and-anti-money-laundering-annual-report-dprk-money-ad8b17bf8e19. Acesso em: 5 mai. 2025.

SUBASHI, Roland. Cryptocurrencies and Money Laundering. Balkan Journal of Interdisciplinary Research, v. 10, n. 1, p. 179-199, maio 2024. DOI: https://doi.org/10.2478/bjir-2024-0005. Acesso em: 5 mai. 2025.

THE STRAITS TIMES. Crypto crime value likely hit a high of $56 billion in 2024. Singapore: The Straits Times, 2025. Disponível em: https://www.straitstimes.com/business/crypto-crime-value-likely-hit-a-high-of-56-billion-in-2024-says-report. Acesso em: 5 mai. 2025.