Revista ARACÊ
ISSN: 2358-2472

TRÍADE DE DESANONIMIZAÇÃO FORENSE: DA PSEUDONIMIDADE À RASTREABILIDADE FORENSE DE CRIMES FINANCEIROS ENVOLVENDO CRIPTOATIVOS

FORENSIC DEANONYMIZATION TRIAD: FROM PSEUDONYMITY TO FORENSIC TRACEABILITY OF FINANCIAL CRIMES INVOLVING CRYPTO ASSETS

TRÍADA DE DESENONANIMIZACIÓN FORENSE: DE LA PSEUDONIMIDAD A LA TRAZABILIDAD FORENSE DE DELITOS FINANCIEROS QUE INVOLUCRAN CRIPTOACTIVOS

https://doi.org/10.56238/arev8n5-071

Data de submissão: 18/04/2026 **Data de publicação:** 18/05/2026

Tullio Henrique dos Santos Souza
Especialista em Contabilidade Forense
E-mail: tullio.thss@pf.gov.br

RESUMO

Este artigo analisa como a assimetria informacional no ecossistema de criptoativos pode ser explorada para mitigar a pseudonimidade das blockchains públicas e transformar rastros técnicos em prova contábil-jurídica. A pesquisa, de natureza qualitativa e exploratória, fundamenta-se em literatura especializada, relatórios técnicos internacionais e normativos nacionais. Propõe-se o modelo Tríade de Desanonimização Forense, composto por três vetores iterativos: (i) vértice *on-chain*, que examina rastros digitais imutáveis; (ii) vértice *off-chain*, que utiliza dados de provedores de serviços de ativos virtuais e fontes abertas; e (iii) vértice de correlação forense-jurídica, que integra os achados técnicos em prova processual auditável. Argumenta-se que a integração iterativa desses vetores fornece subsídios concretos à persecução penal de delitos financeiros, distinguindo-se do rito administrativo-judicial de apreensão e alienação de ativos, pois se concentra na fase probatória anterior.

Palavras-chave: Assimetria Informacional. Pseudonimidade. Criptoativos. Investigação Forense. Desanonimização.

ABSTRACT

This article analyzes how informational asymmetry in the crypto-asset ecosystem can be exploited to mitigate the pseudonymity of public blockchains and transform technical traces into accounting-legal evidence. The research, of a qualitative and exploratory nature, is based on specialized literature, international technical reports, and national regulations. The Forensic De-anonymization Triad model is proposed, composed of three iterative vectors: (i) on-chain vertex, which examines immutable digital traces; (ii) off-chain vertex, which uses data from virtual asset service providers and open sources; and (iii) forensic-legal correlation vertex, which integrates the technical findings into auditable procedural evidence. It is argued that the iterative integration of these vectors provides concrete support for the criminal prosecution of financial crimes, distinguishing itself from the administrative-judicial procedure of asset seizure and alienation, as it focuses on the earlier evidentiary phase.

Revista ARACÊ
ISSN: 2358-2472

Keywords: Information Asymmetry. Pseudonymity. Cryptoassets. Forensic Investigation. De-anonymization.

RESUMEN
Este artículo analiza cómo la asimetría informacional en el ecosistema de criptoactivos puede aprovecharse para mitigar el seudonimismo de las cadenas de bloques públicas y transformar los rastros técnicos en evidencia contable-legal. La investigación, de carácter cualitativo y exploratorio, se basa en literatura especializada, informes técnicos internacionales y regulaciones nacionales. Se propone el modelo de la Tríada de Desanonimatización Forense, compuesta por tres vectores iterativos: (i) vértice en la cadena, que examina los rastros digitales inmutables; (ii) vértice fuera de la cadena, que utiliza datos de proveedores de servicios de activos virtuales y fuentes abiertas; y (iii) vértice de correlación forense-legal, que integra los hallazgos técnicos en evidencia procesal auditable. Se argumenta que la integración iterativa de estos vectores proporciona un apoyo concreto para el enjuiciamiento penal de delitos financieros, diferenciándose del procedimiento administrativo-judicial de incautación y enajenación de activos, ya que se centra en la fase probatoria inicial.

Palabras clave: Asimetría Informacional. Seudonimismo. Criptoactivos. Investigación Forense. Desanonimización.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

Este artigo investiga como a assimetria informacional presente no ecossistema de criptoativos pode ser explorada a fim de ampliar a rastreabilidade e mitigar a pseudonimidade das blockchains públicas e transformar rastros técnicos em provas contábeis e jurídicas. Oriundo da economia, o termo aqui designa a diferença de conhecimento entre usuários leigos e especialistas em blockchain, quanto à fundamental distinção entre anonimato absoluto e pseudonimidade.

A questão central é como transformar ações descuidadas e imprudentes em aprimoramento de método investigativo capaz de reduzir a pseudonimidade e consolidar dados técnicos dispersos em prova contábil-jurídica. Para tanto, sustenta-se a hipótese de que essa transformação é viável mediante a articulação de três vetores, quais sejam, *on-chain*, *off-chain* e de correlação forense-jurídica.

A importância prática do assunto é contemporânea, considerando o aumento do uso de tecnologias de blockchain por grupos criminosos para lavagem de dinheiro, fraudes e evasão de divisas. Esse fenômeno é agravado pela falta de conhecimento técnico tanto das vítimas quanto de algumas autoridades, resultando em uma situação em que a pseudonimidade é erroneamente vista como um anonimato intransponível. Em 2024, o *Crypto Crime Report 2025* da Chainalysis[1] estimou que endereços ilícitos de criptoativos receberam ao menos US$ 40,9 bilhões, podendo o montante ultrapassar US$ 51 bilhões (CHAINALYSIS, 2025).

A literatura especializada confirma a viabilidade da desanonimização tanto na via teórica, por técnicas de análise de grafos e heurísticas de agrupamento (MEIKLEJOHN et al., 2013; NARAYANAN et al., 2016), como na via prática, por metodologias forenses de rastreamento, extração de dados e análise de carteiras (FURNEAUX, 2018). Em paralelo, organismos internacionais como Europol - *European Union Agency for Law Enforcement Cooperation* e FATF[2] - *Financial Action Task Force* enfatizam a crucial importância dos vetores *off-chain*, em especial aquelas obtidas a partir das obrigações *Know Your Customer* - KYC[3], *e Anti-Money Laundering* – AML, a fim de complementar a análise *on-chain* e possibilitar a quebra da pseudonimidade (EUROPOL, 2025; FATF, 2019).

Diante disso, o presente artigo propõe o modelo Tríade de Desanonimização Forense, integrado por três vértices sinérgicos: (i) vértice *on-chain*, que examina os rastros digitais imutáveis

[1] A Chainalysis é uma empresa privada de inteligência e análise de blockchain voltada a compliance KYC/AML e apoio a investigações. No relatório, os valores são estimativas mínimas porque refletem apenas endereços ilícitos já identificados e tendem a ser revisados para cima à medida que novos endereços de carteiras são confirmados.
[2] FATF/GAFI é órgão de fiscalização global de lavagem de dinheiro e financiamento do terrorismo - abandonou a expressão *virtual currency* (“moeda virtual”) por considerá-la tecnicamente imprecisa e juridicamente inadequada.
[3] Normas KYC e AML obrigam a PSAV a identificar clientes e a comunicar operações suspeitas. KYC consiste no processo de identificação de clientes por instituições financeiras e provedores de serviços, enquanto o AML corresponde ao conjunto de normas e práticas, em conformidade FATF/GAFI.

Revista ARACÊ
ISSN: 2358-2472

do *ledger*; (ii) vértice *off-chain*, que explora dados de provedores de serviços de ativos virtuais - PSAVs[4], e *Open Source Intelligence*[5] - OSINT; e (iii) vértice da correlação forense-jurídica, que sintetiza os achados técnicos em prova processual auditável. Defende-se que a integração desses vértices não é linear, mas iterativa, permitindo retroalimentação contínua até a consolidação de um quadro probatório robusto.

É importante ressaltar que a proposta não se mistura com os procedimentos administrativos de apreensão e alienação de ativos virtuais. Em vez disso, ela se apresenta como uma abstração metodológica que organiza os vetores técnicos em uma estrutura probatória, capaz de interagir com os modelos investigativos e probatórios já existentes.

Por fim, ressalta-se a urgência da capacitação, tanto teórica como prática, em blockchain, criptoativos e contratos inteligentes para profissionais de linha investigativa, tais como peritos, policiais e, sobretudo, contadores forenses. Sem isso a resposta institucional permanecerá limitada e ineficaz. Para atingir tais objetivos, este trabalho estrutura-se da seguinte forma: além desta introdução, seção de fundamentos técnicos e normativos; metodologia; análise dos vetores *on-chain* e *off-chain*; aplicação do modelo em estudo de caso; e, por fim, nas conclusões.

2 FUNDAMENTOS TÉCNICOS E NORMATIVOS

2.1 ESTRUTURA DA BLOCKCHAIN: HASH, BLOCOS, LEDGER, POW/POS

A blockchain é uma tecnologia de registro digital distribuído (Distributed Ledger Technology - DLT) criada para armazenar transações em blocos conectados por códigos criptográficos (hash) e validados por protocolos de consenso descentralizado, seja por meio da mineração - Proof-of-Work (PoW), ou por meio da validação - Proof-of-Stake (PoS). Essa tecnologia permite transferências sem depender de instituições tradicionais (CASTELLO, 2019) e dá origem às Finanças Descentralizadas (DeFi), possibilitando a interação por meio de aplicativos descentralizados (DApps) fundamentados em blockchain (ROCHMAN, 2023).

Na prática, funciona como um livro-razão[6] público em que cada transação é registrada de modo sequencial e imutável, replicada em milhares de nós espalhados globalmente. Os três pilares centrais dessa tecnologia, a saber, imutabilidade, transparência e pseudonimidade, constituem os elementos mais relevantes para a perícia contábil e a investigação forense.

[4] PSAVs designa qualquer pessoa física ou jurídica que, no exercício de sua atividade profissional, realize operações de ativos virtuais, em conformidade FATF/GAFI.
[5] OSINT refere-se à coleta e análise de informações obtidas a partir de fontes abertas e publicamente acessíveis, como registros públicos, redes sociais, websites, bases de dados governamentais e reportagens jornalísticas. É amplamente utilizado por agências de segurança e fiscalização para complementar dados sigilosos ou técnicos.
[6] O livro-razão é um livro contábil que organiza e detalha transações controlando seus saldos ao longo do tempo.

Revista ARACÊ
ISSN: 2358-2472

2.2 PSEUDONIMIDADE E ANONIMATO: DISTINÇÃO TEÓRICA E IMPLICAÇÕES PRÁTICAS

No plano conceitual, anonimato é caracterizado como a ausência de qualquer vínculo entre a identidade real de uma pessoa e suas ações. Já a pseudonimidade[7] é definida pelo uso de identificadores, como endereços alfanuméricos, que substituem o nome verdadeiro, mas possibilitam a correlação com outros dados.

Na prática, algumas blockchains, como Bitcoin e Ethereum, apresentam transparência pseudônima. Outras blockchains, como as do Monero, possuem protocolos de privacidade que ocultam remetente, destinatário e valores, o que dificulta a correlação com outros dados.

A crença equivocada de que se trata de anonimato absoluto constitui o elo fraco que deve ser explorado nas investigações forenses, visto que a pseudonimidade pode ser mitigada por meio da correlação entre informações *on-chain* (rastro transacional) e *off-chain* (dados de provedores e fontes abertas). Como afirmou o Procurador da República Alexandre Senra, *"o blockchain é um livro pseudônimo. Abro e consigo ver tudo o que foi movimentado. Não é anônimo"* (GAÚCHAZH, 2025; LIVECOINS, 2025).

2.3 CLASSIFICAÇÃO DOS ATIVOS DIGITAIS

O ecossistema digital exige precisão conceitual, pois frequentemente termos são intercambiados de modo atécnico[8]. Adiante, examinar-se-á as categorias mais controvertidas, separando usos coloquiais de definições técnicas.

A primeira categoria e a mais ampla, é a dos Ativos Digitais[9]. Termo atécnico, que abrange qualquer representação de valor em formato eletrônico, inclusive não financeiro, como arquivos de mídia, é chamado de ativo digital. Por seu turno, o Ativo Virtual, nos termos da Lei nº 14.478/2022 e das diretrizes da FATF, refere-se especificamente à representação digital de valor destinada a investimento ou pagamento, excluídas as moedas oficiais. Dentro desse grupo estão os criptoativos, baseados em blockchain, subdivididos em criptomoedas (Bitcoin, de natureza pseudônima; Monero, de privacidade reforçada), *stablecoins* (USDT, USDC), e tokens, que podem assumir a forma de

[7] Substituição de identificadores pessoais por códigos ou pseudônimos. É uma técnica que, apesar de dificultar a reversão para os dados originais, permite que as obrigações regulatórias de KYC/AML sejam cumpridas, mantendo potencial correlação para fins de análise e *compliance* (MACHADO, 2024, p. 47)

[8] A criptomoeda não pode ser chamada de moeda no sentido legal (estatal) da palavra. Sua utilização ainda encontra interpretações legais pouco padronizadas (STELLA, 2017).

[9] A expressão "ativo digital" deve ser evitada por ausência de rigor técnico, uma vez que se trata de um conceito genérico e não normatizado, que pode abranger qualquer representação digital, por exemplo, documentos, imagens, músicas ou softwares.

Revista ARACÊ
ISSN: 2358-2472

fungíveis ou não fungíveis, estes últimos conhecidos como *Non-Fungible Tokens* - NFTs[10], utilitários, de governança ou de segurança.

Ainda, ressalta-se que o termo moeda digital evoluiu semanticamente: se antes era usada como sinônimo de criptomoeda, agora, na legislação atual, refere-se apenas às Moedas Digitais *Central Bank Digital Currencies* - CBDCs[11], como o Drex[12] (Brasil), o e-CNY[13] (China) e o Euro Digital[14], que possuem natureza soberana e curso forçado[15].

De igual modo, o termo *criptomoeda* é ramo da categoria criptoativos, designando ativos baseados em blockchain, pseudônimos e não emitidos por autoridade central (ex.: Bitcoin, Monero), ao passo que *moeda digital* atualmente designa Moedas digitais emitidas por bancos centrais, representações de moeda oficial.

Por fim, as *stablecoins* (USDT, USDC) também são tipos de criptoativos privados lastreados em ativos de referência, enquanto as moedas digitais de bancos centrais, repisa-se, constituem representação oficial da moeda fiduciária em formato digital.

Ressalta-se, ainda, um caso *sui generis* na taxonomia dos criptoativos: o Ethereum. Em sua camada monetária, o Ether (ETH) funciona como criptomoeda dentro do ecossistema. Contudo, possui infraestrutura programável para contratos inteligentes e para a emissão de tokens (fungíveis - ERC-20, e não fungíveis - ERC-721/1155), possibilitando a criação de *stablecoins*, tokens de governança, NFTs e ativos securitizados. Assim, o Ethereum não se restringe a uma única categoria. É considerado o marco da 2ª geração[16] de criptoativos, diferenciando-se dos criptoativos de 1ª Geração, tais como o

[10] NFTs são registros únicos e indivisíveis em blockchain. Representam a propriedade de um ativo digital (como imagens, músicas, entre outros) ou físico (obras de arte, ingressos, certificados). Diferentemente dos tokens fungíveis (como Bitcoin ou Ether), que são intercambiáveis entre si. Os NFTs possuem identificadores exclusivos que os tornam não substituíveis.
[11] Moedas digitais emitidas por bancos centrais possuem natureza pública de moeda de curso legal forçado, ou seja, de aceitação obrigatória, diferentemente dos ativos virtuais, que possuem natureza privada e não gozam de aceitação compulsória, a exemplo das cédulas e moedas físicas (BANCO CENTRAL DO BRASIL, 2023; BANK FOR INTERNATIONAL SETTLEMENTS, 2020).
[12] O Banco Central do Brasil esclarece que o Drex não substituirá o dinheiro em espécie, sendo apenas uma extensão digital da moeda fiduciária real em ambiente de tecnologia de registro distribuído, e deve obedecer às regras da Lei do Sigilo Bancário e da LGPD (BRASIL, 2025).
[13] e-CNY (Digital Currency Electronic Payment – DCEP) — É a moeda digital de banco central (CBDC) emitida pelo Banco Popular da China (PBoC). Diferencia-se das criptomoedas privadas por ser moeda soberana, com curso legal e lastro direto no renminbi (RMB).
[14] O Banco Central Europeu encontra-se em fase avançada de preparação para a implementação do euro digital (EUROPEAN CENTRAL BANK, 2023).
[15] O conceito de curso legal forçado traduz a característica de aceitação compulsória da moeda emitida pelo Estado, natureza de moeda soberana. Em termos jurídicos, significa que nenhum credor pode recusar o pagamento realizado na moeda oficial em todo o território nacional (Lei nº 9.069/1995, Plano Real).
[16] O Ethereum é considerado de 2ª geração de criptoativos por possibilitar a execução de contratos inteligentes (*smart contracts*), aplicações descentralizadas (*dApps*), emissão de tokens programáveis e protocolos de finanças descentralizadas (*DeFi*), que permitem operações e negociações de forma automática, ampliando funcionalidades econômicas da blockchain, para além de simples transações monetárias.

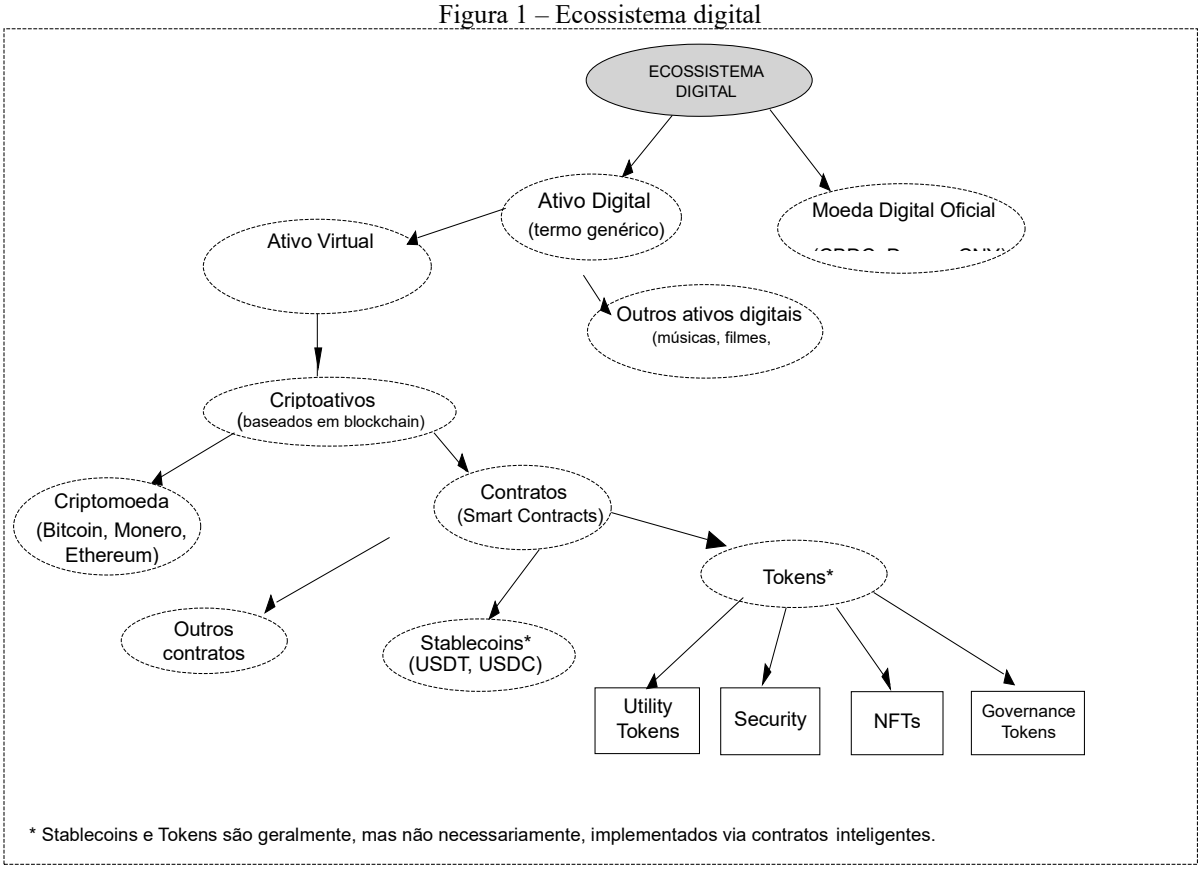
Revista ARACÊ
ISSN: 2358-2472

Bitcoin e do Monero.

2.4 ESTRUTURA DO ECOSSISTEMA DIGITAL

A figura 1 sintetiza o ecossistema digital, organizando as categorias de ativos e ilustrando suas conexões conceituais e funcionais.

Figura 1 – Ecossistema digital



Fonte: Elaboração própria a partir de FATF (2019, 2020, 2025); Europol (2025); Chainalysis (2025); Monero Research Lab (2018); Manual Polícia Federal (2025); Lei nº 14.478/2022; IN RFB nº 1.888/2019; IN RFB nº 2.219/2024; CVM (Parecer de Orientação nº 40/2022); BIS (2022); OECD (2022).

2.5 MARCO CONTÁBIL E REGULATÓRIO

A abordagem jurídica dos criptoativos requer análise em nível internacional e nacional. No nível internacional, as Recomendações 15 e 16 do FATF/GAFI definem a estrutura global de combate à lavagem de dinheiro e financiamento do terrorismo, exigindo que os países apliquem às *exchanges* e PSAVs as mesmas normas destinadas às instituições financeiras convencionais.

Entre essas obrigações, se sobressaem a identificação e verificação da identidade de clientes (*KYC)*, o monitoramento de operações suspeitas e a chamada *Travel Rule*, que exige a transmissão de dados de remetente e destinatário em transações acima de determinados valores (FATF, 2025). Ademais, essas normas favorecem colaboração internacional nas investigações.

Revista ARACÊ
ISSN: 2358-2472

No nível nacional, o Brasil estabeleceu seu marco regulatório por meio da Lei nº 14.478/2022 (Marco Legal dos Criptoativos), introduzindo a definição de ativo virtual no ordenamento jurídico brasileiro. Essa lei foi precedida pela IN - Instrução Normativa RFB nº 1.888/2019, que estabeleceu a obrigação de reportar operações com criptoativos à Receita Federal. Além disso, o Parecer CVM nº 40/2022 complementou-a, estabelecendo os casos em que determinados tokens podem ser classificados como valores mobiliários.

Paralelamente, a Lei nº 9.613/1998, de combate à lavagem de dinheiro, permanece como eixo normativo de suporte, pois a sujeição dos PSAVs a essas regras os insere no rol de entidades obrigadas a colaborar com autoridades administrativas e judiciárias.

Sob a perspectiva contábil, a ausência de pronunciamento específico levou à aplicação, por analogia, de pronunciamento técnico já existente do Comitê de Pronunciamentos Contábeis - o CPC[17] 04 (ativo intangível), de modo que criptoativos são reconhecidos no balanço patrimonial como intangíveis.

Todavia, a rapidez com que esses ativos mudam demonstra as limitações da mensuração pelo custo histórico, o que justifica a relevância do valor justo, de acordo com o CPC 48. Essa falta de regulamentação abre espaço para manipulação patrimonial e sonegação, razão pela qual a classificação contábil e regulatória adequada é fundamental na contabilidade forense e na investigação de crimes financeiros.

3 METODOLOGIA

A pesquisa adota abordagem qualitativa e de caráter exploratório, voltada à análise das vulnerabilidades da pseudonimidade em blockchains públicas e à construção de um modelo aplicável à contabilidade forense. Optou-se por pesquisa bibliográfica e documental, com base em literatura especializada, relatórios técnicos de órgãos internacionais e normativos nacionais.

Do ponto de vista metodológico, utilizou-se o estudo de caso como estratégia, considerando que esse método permite examinar fenômenos complexos no contexto em que ocorrem. O caso examinado é inspirado na Operação Decrypted (Polícia Federal, 2025), que desarticulou uma organização criminosa envolvida em fraudes com criptoativos e lavagem de dinheiro internacional.

[17] A classificação contábil dos criptoativos é objeto de debate: quando destinados à negociação corrente, aproximam-se de estoques (CPC 16, 2009); quando mantidos como reserva ou investimento, podem ser reconhecidos como ativos intangíveis (CPC 04, 2010); parte da literatura ainda sugere sua aproximação com instrumentos financeiros (CPC 39, 2012).

Revista ARACÊ
ISSN: 2358-2472

4 VERTICES DA TRÍADE DE DESANONIMIZAÇÃO

A rastreabilidade de transações em criptoativos baseia-se em três vértices interligados: o *on-chain*, de natureza técnica; o *off-chain*, de natureza contextual e comportamental; e o da correlação forense-jurídica, que integra os anteriores em uma narrativa probatória.

Sua aplicação é iterativa e não linear, permitindo que cada vértice retroalimente os demais até a consolidação da prova. É justamente essa integração, qual seja, o cruzamento entre vértices e vetores, que se constitui o modelo denominado Tríade de Desanonimização Forense.

4.1 VÉRTICE *ON-CHAIN* E SEUS VETORES DE RASTREABILIDADE

Os vetores de rastreabilidade *on-chain* representam a análise direta dos registros públicos da blockchain. Isso envolve rastrear fluxos de ativos virtuais através de técnicas baseadas em busca de grafos transacionais, em heurísticas de *clustering*[18] e em detecção de padrões de reuso de endereços.

Como um desses vetores, os grafos transacionais constituem-se em representações gráficas das transações realizadas em uma blockchain. Cada nó equivale a um endereço ou carteira, enquanto as arestas simbolizam as transferências de ativos entre esses nós. Dessa forma, é possível visualizar a rede de fluxos, identificar hubs de concentração e reconstruir trajetórias de envio e recebimento de criptoativos (MEIKLEJOHN et al., 2013).

As heurísticas de *clustering*, por seu turno, são métodos que agrupam endereços distintos como pertencentes a uma mesma entidade, a partir de padrões observáveis. Além disso, a literatura apresenta, no plano teórico, em Narayanan et al. (2016), a exploração do comportamento recorrente de agrupamentos de endereços e transações em redes de blockchain, e também, no plano prático, em Furneaux (2018), descreve procedimentos de análise de carteiras recuperadas e técnicas de rastreamento de fluxos aplicados à investigação forense.

Finalmente, a detecção de padrões de reuso de endereços examina a frequência com que um mesmo endereço é utilizado em diferentes operações, pois embora a boa prática recomende a geração de novos endereços a cada transação, criminosos e usuários descuidados reaproveitam os mesmos endereços, o que auxilia na identificação do usuário. Esse reuso funciona como ponto de ancoragem para correlacionar atividades e vincular identidades digitais a perfis reais (EUROPOL, 2025).

Apesar da efetividade dessas técnicas, existem mecanismos especificamente desenhados para dificultar a rastreabilidade, como os *mixers*, os protocolos de *CoinJoin* e as chamadas criptomoedas

[18] *Clustering* é termo técnico que designa o agrupamento de itens com características comuns e, no âmbito criptoesfera, corresponde à associação de endereços de blockchain identificados como pertencentes a uma mesma carteira de criptoativos

Revista ARACÊ
ISSN: 2358-2472

de privacidade.

Os *mixers*[19] são serviços que combinam criptomoedas de múltiplos usuários para ofuscar as origens e os destinatários das transações. Rompem com a linearidade dos rastros digitais. Funcionam recebendo criptoativos de diferentes participantes e os redistribuem em novos endereços, embaralhado, a fim de romper a vinculação direta entre remetente e destinatário. Na prática, desfaz parte do rastro digital, dificultando a atribuição de um fluxo a uma pessoa real.

Exemplos notórios incluem o *Tornado Cash*[20] e o *Bitcoin Fog*[21], sendo este um dos *mixers* mais antigos da rede Bitcoin, utilizado para ofuscar grandes volumes de transações suspeitas, enquanto aquele *mixer* da rede Ethereum utiliza contratos inteligentes e *zero-knowledge proof* [22] (e variantes) para permitir depósitos anônimos e retiradas em endereços distintos.

Os protocolos de *CoinJoin*[23], por sua vez, funcionam de modo descentralizado em que vários usuários combinam suas transações em uma única operação conjunta, de modo que as entradas e saídas aparecem mescladas em uma única transação.

Essa técnica, originalmente da rede Bitcoin, tem como efeito a quebra da chamada *multi-input heuristic*, tornando complexa a inferência de quais endereços pertencem a quem. Entre as implementações mais conhecidas estão a *Wasabi Wallet,* que oferece *CoinJoin* integrado com interface voltada à privacidade, e a Samourai *Wallet*, cujo protocolo Whirlpool possibilita ciclos repetidos de *CoinJoin* para ampliar a ofuscação.

Já as criptomoedas de privacidade[24] trazem embutido em seu próprio código protocolo de privacidade. Por exemplo, o *Monero* (XMR) possui recursos de ofuscação nativos[25], que tornam as transações obrigatoriamente ofuscadas. O *Zcash* (ZEC) possibilita transações blindadas (*shielded*), sem expor dados. O *Dash* (DASH), conhecida como *DarkCoin* (ou *Xcoin)*, possibilita realizar transações ofuscadas, chamadas de *PrivateSend.*

[19] Os mixers são serviços externos, programados como sites, scripts ou contratos inteligentes, que recebem criptoativos de vários usuários, misturam esses valores e devolvem em novos endereços, rompendo a ligação direta entre remetente e destinatário. Ele executa a mistura fora da lógica da blockchain e depois devolve os fundos processados.
[20] Em 2022, o serviço *Tornado Cash* foi declarado ilegal pela *Office of Foreign Assets Control* (OFAC). Contudo, essa designação foi revogada judicialmente, e em 2025 o OFAC retirou oficialmente o serviço da proibição.
[21] Bitcoin Fog é um serviço utilizado sistematicamente para disfarçar grandes volumes de transações suspeitas.
[22] Protocolo criptográfico em que uma parte (o provador) convence outra (o verificador) de que uma afirmação é verdadeira sem revelar informações adicionais além da veracidade da afirmação. No contexto da blockchain, tal técnica é aplicada em serviços como o Tornado *Cash*: o usuário deposita fundos vinculados a um compromisso criptográfico e, no saque, apresenta uma prova *zero knowledge* que demonstra conhecer a chave secreta associada a um compromisso válido, sem revelar qual depósito específico originou os fundos.
[23] CoinJoin é um método ou protocolo nativo de organização da transação, no qual múltiplos usuários juntam suas entradas e saídas em uma única operação conjunta. Assim, a própria blockchain registra o embaralhamento no bloco. Ele realiza a mistura dentro do próprio registro, quando a transação é validada.
[24] Criptomoedas de privacidade são projetadas para dificultar o rastreamento de transações, incorporando mecanismos de anonimização em seu protocolo.
[25] Protocolos de ofuscação Monero: *Ring Signatures, Stealth Addresses e RingCT*.

Revista ARACÊ
ISSN: 2358-2472

Registra-se que a utilização dessas criptomoedas aumenta substancialmente as dificuldades da investigação criminal, pois reduzem a efetividade das metodologias de rastreamento *on-chain*, e ampliam o custo analítico exigido para a produção de provas digitais (PF, 2021).

A Tabela 1 apresenta os principais vetores de rastreabilidade presentes no vértice *on-chain*, evidenciando como a análise de grafos transacionais, heurísticas de clustering e detecção de reuso de endereços são técnicas recorrentes na investigação forense.

Destaca-se também os mecanismos dificultadores, como *mixers*, protocolos *CoinJoin* e criptomoedas de privacidade, que reduzem a transparência dos registros públicos da blockchain. E associa, por fim, cada técnica ao seu criptoativos.

Tabela 1 - Vetores de rastreabilidade on-chain

Técnica de rastreabilidade *on-chain*	**Mecanismos dificultadores**	**Criptoativo associado à técnica de rastreabilidade**
Grafos transacionais	Serviços de *Mixers* Exemplo: Tornado Cash, Bitcoin Fog	Bitcoin, Ethereum
Heurísticas de clustering	Protocolos *CoinJoin* Exemplo: Wasabi, Samourai/Whirlpool	Bitcoin
Detecção de reuso de endereços	Endereços de uso único (Stealth Addresses) [26] e Ofuscação de Transações (*Ring Signatures, zk-SNARKs*) notadamente Monero (XMR), Zcash (ZEC) e o Dash (DASH)	Todos os criptoativos

Fonte: Elaboração própria a partir de FATF (2019, 2025); Europol (2025); Chainalysis (2025; 2023); Monero Research Lab (2018); Kappos et al. (2018); TRM Labs (2024); Manual de Apoio à Investigação de Criptoativos - PF (2021); legislação nacional (Lei nº 14.478/2022; IN RFB nº 1.888/2019 e nº 2.219/2024).

Por fim, ferramentas especializadas, a exemplo de Chainalysis[27], TRM Labs[28] e Etherscan[29], operacionalizam as técnicas de análise *on-chain*, tais como grafos transacionais, heurísticas de *clustering* e detecção de reuso de endereços, e fornecem a materialidade digital de condutas suspeitas.

Na prática, não é necessário conhecimento em programação: basta inserir um endereço, transação ou carteira, e a ferramenta realiza automaticamente a consulta nas blockchains públicas. Em

[26] FORÇA a criação de um novo endereço para cada transação, mesmo que o recebedor sempre forneça o mesmo endereço público (o seu endereço principal).
[27] Chainalysis é uma empresa privada desenvolvedora de softwares especializados em análise de blockchain, incluindo o Chainalysis Reactor, Chainalysis Kryptos e Chainalysis Market Intel. Esses softwares são amplamente utilizados por agências de aplicação da lei e instituições financeiras para fins de compliance (conformidade regulatória).
[28] TRM Labs é empresa privada especializada em rastreabilidade e *risk management* em criptoativos, que fornece soluções de monitoramento em tempo real para prevenção de lavagem de dinheiro e financiamento ilícito.
[29] Etherscan é um explorador público da blockchain Ethereum, mantido pela empresa Etherscan, que disponibiliza gratuitamente consultas a transações, endereços, contratos inteligentes e tokens.

Revista ARACÊ
ISSN: 2358-2472

seguida, há cruzamento dessas informações *on-chain* com dados *off-chain*, gerando representações gráficas.

4.2 VÉRTICE *OFF-CHAIN* E SEUS VETORES DE INTELIGÊNCIA

Os vetores *off-chain* complementam o vértice anterior, permitindo atribuir autoria a endereços pseudônimos. Eles se baseiam em informações externas à blockchain, como cadastros PSAVs, dados de *compliance* exigidos pelas normas KYC/AML e evidências obtidas em fontes abertas (OSINT) tais como nomes, endereços eletrônicos e registros de atividades.

Ademais, medidas cautelares judiciais, como quebras de sigilo e apreensão de dispositivos, podem reforçar a vinculação entre transações e indivíduos, fornecendo elementos probatórios, tais como registros de conversas, capturas de tela ou históricos de operações financeiras.

Apesar da efetividade dos vetores *off-chain*, existem mecanismos que dificultam a atribuição direta de autoria, dentre os quais se destacam os pontos de *cash-out*. Este termo nomeia o momento em que os criptoativos são convertidos em moeda fiduciária, funcionando como a ponte entre o ecossistema digital pseudônimo e o sistema financeiro tradicional, dividindo-se em duas modalidades de conversão.

A primeira modalidade ocorre em *exchanges* com regulação insuficientes, que permitem a conversão de criptoativos sem controles rígidos de identificação, fragilizando os mecanismos KYC[30] e AML[31].

A outra modalidade é a negociação *peer-to-peer*[32] (P2P), consiste em formas diretas de trocar ou vender criptoativos entre usuários, sem intermediação de *exchanges*, o que dificulta rastreamento e atribuição de autoria, já que essas transações podem ocorrer em fóruns digitais, aplicativos de mensagens ou até encontros presenciais.

Ressalta-se, ainda, a existência de formas de intermediação de plataforma, exemplificadas pelo serviço Binance P2P[33], no qual a corretora disponibiliza a infraestrutura para aproximar compradores e vendedores, sem, contudo, assumir custódia dos ativos negociados.

[30] Exemplos comuns de informações KYC incluem identificação civil, endereço e comprovante de vínculo bancário.
[31] Exemplos comuns de informações AML incluem volume incomum, fracionamento, uso repetido de endereços novos.
[32] A negociação *peer-to-peer* (P2P, ponto a ponto) refere-se a uma arquitetura de rede onde utilizadores interagem diretamente entre si, sem um servidor central, a exemplo dos protocolos de compartilhamento *Torrents*.
[33] A título ilustrativo, no modelo Binance P2P, o ativo não é transferido imediatamente ao comprador. Ele permanece bloqueado em mecanismo de *escrow* até a confirmação do pagamento pela contraparte, funcionando como salvaguarda contra inadimplemento (Binance, 2020).

Revista ARACÊ
ISSN: 2358-2472

Tabela 2 – Vetores de inteligência *off-chain*

Técnica de inteligência *off-chain*	**Mecanismos dificultadores**	**Exemplos associados**
Cruzamento de dados OSINT (fontes abertas)	Identidades falsas e e-mails descartáveis	Perfis em fóruns, Telegram, redes sociais
Peticionamento de Medidas cautelares (quebra de sigilo, apreensão de dispositivos)	Dispositivos criptografados, uso de mensageria cifrada, jurisdição estrangeira	*Smartphones* e equipamentos computacionais WhatsApp/Telegram, *Soft wallet*s e *hardware wallet*
Cruzamento de dados PSAVs (KYC/AML)	*Cash-out* em *exchanges* pouco reguladas [34]	*Exchanges on-shore e off-shore* com ou sem exigência de KYC/AML
	Conversão via negociação P2P (ausência de intermediário regulado)	Pontos de compra e venda de cripto em WhatsApp/Telegram, Binance P2P

Fonte: Elaboração própria a partir FATF (2019, 2025); Europol (2025); Interpol; Chainalysis (2025); Manual PF (2021); literatura OSINT (Bazzell, 2023); legislação nacional (Lei nº 14.478/2022; IN RFB nº 1.888/2019; nº 2.219/2024).

A Tabela 2 relaciona os principais vetores de inteligência presentes no vértice *off-chain*, demonstrando como a coleta e a intersecção de dados externos ao registro da blockchain enriquecem a investigação forense. Nesse contexto, técnicas de OSINT (fontes abertas), como perfis em redes sociais e fóruns online, são incluídas, além da utilização de medidas cautelares para a coleta de evidências em dispositivos computacionais, notadamente em aplicativos de mensageria e carteiras de criptomoedas.

Ademais, destacam-se os procedimentos de KYC/AML em PSAVs, cuja análise permite identificar tentativas de conversão em *exchanges* – que podem ser pouco reguladas, ou inclusive por meio de negociações P2P.

Por fim, observa-se que a efetividade desses vetores é frequentemente limitada por mecanismos dificultadores, como identidades falsas, jurisdições estrangeiras e canais informais de conversão de criptoativos.

4.3 VÉRTICE DA CORRELAÇÃO FORENSE-JURÍDICA

O vértice da correlação constitui o ponto central da investigação, pois é nessa etapa que se dá a integração dos vetores de rastreabilidade, tanto aqueles constantes no vértice *on-chain*, quanto os do vértice *off-chain*. Rastros técnicos obtidos na blockchain e os dados contextuais externos são articulados para formar uma narrativa probatória coerente.

[34] Atualmente, há transição de paraísos fiscais tradicionais para paraísos digitais de cripto. Este sendo uma jurisdição que oferece condições tributárias e regulatórias muito favoráveis para investidores e empresas de criptomoedas.

Revista ARACÊ
ISSN: 2358-2472

Essa tradução é essencial para que elementos técnicos sejam compreendidos pelo sistema de justiça, transformando-os em subsídios para decisões judiciais, relatórios contábeis ou medidas cautelares.

Nesse procedimento, o analista ou investigador forense emprega vetores de correlação, como conectar registros bancários a transações em blockchain ou relacionar cadastros de *exchanges* a endereços específicos, com o objetivo de estabelecer uma ligação entre a identidade real e a conduta digital. Por outro lado, o perito estabelece essa relação em um laudo ou parecer técnico, atribuindo-lhe valor formal no processo.

De acordo com o *Manual de Procedimento Pericial – Busca e Apreensão de Criptoativos* (2021), "a atuação pericial é indispensável para garantir que a apreensão de criptoativos se dê em conformidade com requisitos técnicos e jurídicos mínimos".

Assim, o vértice de correlação forense-jurídica converte a prova de informação técnica em prova de natureza jurídica e contábil. E a correlação encerra o ciclo de investigação da Tríade. Devido à sua importância, este vértice será abordado de maneira mais aprofundada no item 4.4, onde será apresentada a sistematização completa do modelo de desanonimização forense.

5 ITERATIVIDADE DE VÉRTICES - MODELO TRÍADE DE DESANONIMIZAÇÃO FORENSE

5.1 ESTRUTURA GERAL

Convém destacar que o Manual de Apoio à Investigação de Criptoativos da Polícia Federal (2021), assim como o Manual de Procedimento Pericial - Busca e Apreensão de Criptoativos do Instituto Nacional de Criminalística (2021), já organizam, de forma operacional, procedimentos de identificação, de rastreamento *(on* e *off-chain*), de apreensão, de custódia e de alienação de ativos virtuais.

Todavia, esse fluxo é predominantemente procedimental e não estabelece uma fase autônoma para a conversão de evidências técnicas em fundamentos legais que embasem pedidos judiciais de bloqueio, sequestro ou ulterior alienação de ativos virtuais. A legislação nacional e os procedimentos operacionais exigem autorização judicial para a transferência de fundos, contudo a etapa de formalização da evidência não é uma fase distinta.

Assim, a proposta deste artigo pretende inserir o vértice da correlação forense-jurídica entre as etapas de rastreamento (*on* e *off-chain*) e apreensão e custódia. Desse modo, o modelo dá estrutura ao processo de desanonimização de dados e a posterior conversão de evidências técnicas em prova

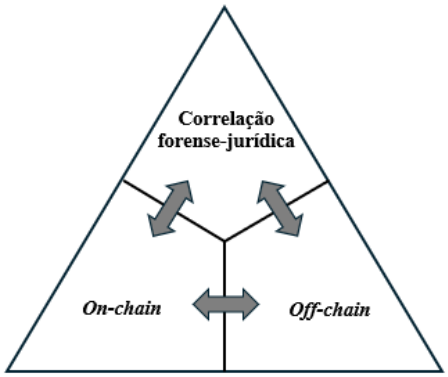
Revista ARACÊ
ISSN: 2358-2472

jurídica. O objetivo fim é lançar luz a um caminho a fim de identificar fluxos de transações, rastrear ativos e, em muitos casos, associar identidades a endereços e carteiras (PF, 2021).

Os vértices ***on-chain*** e ***off-chain*** permitem **ir além da pseudonimidade** ao mapear fluxos e atribuir titularidade, ao passo que o vértice de **correlação forense-jurídica encadeia** esses achados em narrativa probatória conforme às exigências legais (materialidade, autoria, nexo, cadeia de custódia).

A figura 2 elenca os três vértices, que estruturam o modelo da Tríade de Desanonimização.

Figura 2 – Tríade de desanonimização – Integração dos vetores



Fonte: Elaboração própria a partir de FATF (2019, 2020, 2025); Europol (2025); Chainalysis (2025); Monero Research Lab (2018); BRASIL. Instituto Nacional de Criminalística. Manual de Procedimento Pericial – Busca e Apreensão de Criptoativos (2021); BRASIL. Polícia Federal. Manual de Apoio à Investigação de Criptoativos (2021); Lei nº 14.478/2022; Instrução Normativa RFB nº 1.888/2019; Instrução Normativa RFB nº 2.219/2024; CVM. Parecer de Orientação nº 40/2022; BIS (2022); OECD (2022).

Com aplicação iterativa e não linear, as tarefas investigativas podem não ocorrer na ordem apresentada e, talvez, podem até não se aplicar em algum dos casos, permitindo que cada vértice retroalimente os demais, conforme novas informações vão surgindo, até a completa consolidação da prova.

5.2 VÉRTICE ON-CHAIN: RASTREABILIDADE APLICADA E ITERATIVIDADE

O vértice *on-chain* reflete à análise **dos rastros digitais**, isto é, a observação direta dos registros públicos e imutáveis da blockchain. Cada uma das transações registradas na *ledger*[35] constitui um rastro digital verificável, à qual pode ser submetida a técnicas de reconstrução de fluxos e padrões.

[35] Ledger (de blockchain) designa o livro-razão digital, distribuído e imutável, no qual são registradas transações de uma rede blockchain.

Revista ARACÊ
ISSN: 2358-2472

Na prática, a rastreabilidade se dá via ferramentas digitais tais como os exploradores de blocos (*block explorers*[36]) que consultam o histórico de endereço ou *hash* de transação, funcionando como motores de pesquisa sobre blockchains públicas (NARAYANAN et al., 2016). Dentre os exploradores de blocos disponíveis, destacam-se a plataforma *Etherscan*[37], para Ethereum, e a plataforma *Blockchair*[38], para Bitcoin. Ambas as ferramentas constituem a porta de entrada para a construção de provas digitais em investigações forenses.

O **Etherscan dá** acesso a dados públicos de cada transação a partir do *transaction hash* (TXID) ou do identificador de um endereço. É possível, assim, a verificação do histórico de um endereço, o que viabiliza análises de fluxo, conferência de saldos e identificação de padrões. Por sua vez, o Blockchair é um explorador *multichain*, sobretudo utilizado para análise de transações na rede Bitcoin. Permite filtros avançados de busca e também exibe possíveis pontos de vulnerabilidades das transações com relação à privacidade.

Conforme o exposto no item 3.1, os dados brutos extraídos desses exploradores podem ser enviados a outas ferramentas (gráficas) como **Chainalysis Reactor** ou **TRM Forensics**, que aplicam técnicas de grafos e heurísticas de agrupamento, transformando transações isoladas em representações visuais complexas. Essas análises permitem reconhecer conexões entre vários endereços e identificar padrões, como saídas para ***exchanges*** ou *mixers*.

Este vetor corresponde às fases iniciais do rastreamento de criptoativos, sobretudo na localização de evidências de ativos e saldos, e necessita ser complementado pelo vértice *off-chain.*

5.3 VÉRTICE *OFF-CHAIN* - DADOS CONTEXTUAIS APLICADOS E ITERATIVIDADE

O vértice *off-chain* constitui o elo crítico para converter pseudônimos em identidades, identificação pessoal. Ele opera sobre dados externos à blockchain, em especial aqueles mantidos por PSAVs (*exchanges*).

Por força das normas de KYC/AML previstas na Lei nº 14.478/2022 e em normativas da Receita Federal, esses provedores custodiam informações identificáveis (CPF/CNPJ, endereços IP, dados cadastrais, histórico de transações) que permitem associar endereços blockchain a pessoas físicas ou jurídicas. Além das *exchanges*, outras fontes, tais como bancos, operadoras de internet,

[36] Ferramentas on-line que permitem visualizar e consultar dados registrados em blockchains públicas, como blocos, transações e endereços.
[37] Etherscan é uma plataforma de análise que rastreia e classifica os dados da cadeia de blocos Ethereum.
[38] Blockchair é um explorador multichain que indexa e classifica dados de diversas blockchains, com destaque para o Bitcoin, oferecendo filtros avançados de busca e estatísticas agregadas.

Revista ARACÊ
ISSN: 2358-2472

registros públicos ou informações OSINT, podem reforçar a vinculação entre transações digitais e indivíduos concretos.

Na prática, a contextualização de dados *off-chain* pode ser iniciada em duas frentes. A primeira ocorre quando a análise inicial *on-chain* revela indícios técnicos e autoridades oficiais, a partir deles, requisitam informações às PSAVs. A resposta dessas instituições contendo dados cadastrais, registros transacionais e logs de acesso permite vincular endereços pseudônimos a identidades verificáveis e, assim, fundamentar pedidos judiciais de bloqueio ou sequestro (PF, 2021).

A segunda frente começa na etapa de busca e apreensão, momento em que o objetivo do vetor *off-chain* é encontrar artefatos que demonstrem conexões de identidade com endereços e carteiras. Esses artefatos englobam registros de *seed phrases* (frases-sementes), cadastros impressos de PSAVs, além de dispositivos eletrônicos como computadores, smartphones e *hardware wallet*, que hospedam carteiras digitais ativas (BRASIL, INC, 2021).

Ademais, a apreensão de equipamentos computacionais permite, em uma etapa posterior de análise pericial, a identificação de documentos, registros de transações e softwares de carteira digital. Contudo, a natureza transnacional dos criptoativos impõe um desafio[39] crucial no rastreamento: operações transfronteiriças.

5.4 VÉRTICE DA CORRELAÇÃO: TRADUÇÃO PROBATÓRIA E ITERATIVIDADE

O vértice de correlação se inicia quando a investigação técnica alcança validade jurídica. É a etapa em que os resultados dos vetores *on-chain* e *off-chain* se transformam em elementos probatórios aptos a subsidiar medidas cautelares e persecução penal. Essa transformação exige a integração de achados técnicos a uma base jurídica.

No plano internacional, normas jurídicas que se destacam são as Recomendações nº 15 e nº 16 do FATF, que impõem PSAVs as mesmas obrigações de prevenção à lavagem de dinheiro e financiamento ao terrorismo aplicáveis às instituições financeiras tradicionais. Entre essas obrigações figuram o KYC, o monitoramento de operações suspeitas e a *Travel Rule*. No Brasil, norma jurídica destaque é a Lei nº 14.478/2022 (Marco Legal dos Criptoativos), que definiu o conceito de ativo virtual, estabeleceu parâmetros para a atuação de *exchanges* e atribuiu ao Banco Central a competência regulatória.

Complementam esse arcabouço a Lei nº 9.613/1998 (Lavagem de Dinheiro), que prevê medidas como quebra de sigilo e sequestro de bens; a Lei nº 12.846/2013 (Anticorrupção), voltada à

[39] A quebra da pseudonimidade em operações transfronteiriças, especialmente PSAVs sediadas no exterior, exige a cooperação jurídica internacional, que é complexa e lenta, pois demanda o acesso a dados via acordos bilaterais.

Revista ARACÊ
ISSN: 2358-2472

responsabilização empresarial; e a Lei nº 7.492/1986 (Crimes contra o Sistema Financeiro Nacional), aplicável a intermediários não autorizados. Além disso, a Lei nº 13.964/2019 (Pacote Anticrime) reforçou instrumentos de cooperação internacional e constrição patrimonial.

Na área tributária, a IN - Instrução Normativa RFB nº 1.888/2019 instituiu a obrigação de declarar operações maiores que R$ 30.000,00 por mês, inclusive transações *peer-to-peer* ou realizadas em plataformas estrangeiras. A IN RFB nº 2.219/2024 atualizou esses procedimentos, ampliando o nível de detalhamento das informações prestadas.

Paralelamente, são enfatizados os atos normativos do Banco Central e da CVM que tratam da regulação de tokens e *stablecoins*. Já no Banco Central, o Decreto nº 11.563/2023 consolidou a competência da autarquia para supervisionar prestadoras de serviços de ativos virtuais. Por conseguinte, a CVM, via Parecer de Orientação nº 40/2022, dos Ofícios Circulares CVM/SSE 4/2023 e 6/2023 e das Resoluções nº 88/2022 e nº 160/2022, disciplina a caracterização de determinados tokens como valores mobiliários e estabelece regras para *crowdfunding tokenizado* [40]e ofertas públicas digitais.

Em resumo, a correlação forense-jurídica constitui a atividade que transforma indícios em prova juridicamente válida, apta a sustentar medidas cautelares, persecução penal e responsabilização administrativa.

A Tabela 3 mostra vetores de correlação forense-jurídica. A partir desse quadro normativo, é possível compreender que cada legislação não opera de forma isolada, mas se conecta às modalidades delitivas mais recorrentes envolvendo criptoativos.

A Lei de Lavagem de Dinheiro, por exemplo, fundamenta bloqueios e sequestros em investigações de ocultação patrimonial, enquanto as instruções normativas da Receita Federal reforçam a detecção de evasão fiscal. Dessa forma, a Lei Anticorrupção e o Pacote Anticrime como um todo funcionam como elementos de responsabilização empresarial e cooperação internacional, respectivamente.

[40] *Crowdfunding tokenizado* usa a tecnologia de blockchain para representar a participação dos investidores em forma de tokens digitais. é um modelo que combina o financiamento coletivo com a tecnologia blockchain, onde a participação dos investidores é representada por tokens digitais em vez de participações tradicionais. Isso permite fracionar ativos ilíquidos em tokens menores.

Revista ARACÊ
ISSN: 2358-2472

Tabela 3 - Vetores de correlação forense-jurídica

Legislação	Conteúdo-chave	Aplicação prática em crimes com criptoativos
FATF/GAFI – Recomendações 15 e 16	PSAVs equiparados a instituições financeiras; *Travel Rule*; KYC e monitoramento de transações	Fundamenta pedidos de cooperação internacional e exigência de dados de identificação em transações transfronteiriças
Lei nº 14.478/2022 (Marco Legal dos Criptoativos)	Define ativo virtual; atribui competência ao Banco Central; cria diretrizes para *exchanges*	Responsabilização administrativa de PSAVs e exigência de registro/fiscalização pelo Bacen
Lei nº 9.613/1998 (Lavagem de Dinheiro)	Tipificação penal; medidas de sequestro, bloqueio e alienação de bens	Fundamenta pedidos de bloqueio de criptoativos e comunicação de operações suspeitas ao COAF
Lei nº 12.846/2013 (Anticorrupção)	Responsabilização administrativa de empresas	Aplicável a companhias que utilizem criptoativos em esquemas de corrupção ou ocultação patrimonial
Lei nº 7.492/1986 (Crimes contra o SFN)	Tipificação de operações sem autorização do Bacen/CVM	Incidência sobre *exchanges* irregulares ou atuação fraudulenta de intermediários
Lei nº 13.964/2019 (Pacote Anticrime)	Reforço de cooperação internacional e medidas cautelares patrimoniais	Utilizado em sequestro internacional de bens e bloqueio transfronteiriço de criptoativos
IN RFB nº 1.888/2019	Declaração obrigatória de operações acima de R$ 30.000,00	Permite rastreabilidade fiscal e cruzamento de informações com investigações criminais
IN RFB nº 2.219/2024	Atualização e ampliação das informações prestadas à Receita	Reforça transparência tributária e auxilia investigações patrimoniais
Atos do Bacen e da CVM Decreto nº 11.563/2023 (Bacen); Parecer CVM nº 40/2022; Resoluções CVM nº 88/2022 e nº 160/2022; Ofícios Circulares CVM/SSE nº 4/2023 e nº 6/2023	Regulação de tokens como valores mobiliários e impacto das stablecoins	Define enquadramento jurídico de ativos específicos e auxilia na fiscalização de emissões e negociações

Fonte: Elaboração própria a partir de FATF (2019, 2025); BRASIL (Leis nº 9.613/1998, nº 14.478/2022, nº 12.846/2013, nº 7.492/1986, nº 13.964/2019; Decreto nº 11.563/2023; IN RFB nº 1.888/2019, nº 2.219/2024; Resoluções CVM nº 88/2022 e nº 160/2022; Ofícios Circulares CVM/SSE nº 4/2023 e nº 6/2023; Parecer CVM nº 40/2022); BRASIL. Polícia Federal. *Manual de Apoio à Investigação de Criptoativos* (2021); BRASIL. Instituto Nacional de Criminalística. *Manual de Procedimento Pericial – Busca e Apreensão de Criptoativos* (2021).

Com base nesses vetores, apresenta-se a Tabela 4, voltada aos tipos de crimes mais frequentes, seus sinais de alerta, as ações iniciais recomendadas e as ferramentas forenses adequadas. Essa sistematização traduz a legislação em prática investigativa e oferece um guia metodológico para a atuação diante das peculiaridades de cada cenário criminal.

Revista ARACÊ
ISSN: 2358-2472

Tabela 4 - Crimes, sinais de alerta e ferramentas

Crime	Sinais de Alerta[41]	Ação Inicial Recomendada	Criptoativo Mais Usado	Ferramentas Sugeridas
Lavagem de Dinheiro	Altos volumes Origem escondida Fragmentação antes de conversão para *fiat*[42] Uso de *mixers* Ausência de KYC Transações de valores arredondados de múltiplos hops	Mapear ponto de entrada ex.: compra inicial em BTC Buscar acesso à carteira, meio físico ou eletrônico Mapear ponto de saída ex.: ponto saída (*cash-out*)	Monero (XMR)	Exploradores limitados, IPED (apreensão), análises de logs, CIAF-Cripto
		Vetores *on-chain* (Ferramentas) Vinculação de dados PSAV (*off-chain*) Correlação forense Buscar apreensão de carteira (hardware wallet) Quebra de sigilo bancário	Bitcoin (BTC)	Exploradores de blocos Blockchair Etherscan Ferramentas Privadas Chainalysis TRM Ferramenta institucional SIMBA CIAF-Bancário
	Valores recebidos e justificados por vendas de NFTs	Identificar vendas nos sites especializados em NFT (como OpenSea) Relacionar compradores com o vendedor	NFT (*Non Fungible Tokens*)	Etherscan SIMBA
Fraude/Pirâmide Financeira	Tokens de baixa liquidez Promessas de staking, dApps com rug pull Contratos não auditados	Identificar smart contracts envolvidos Apurar a criação de liquidez a destruição de liquidez	Ethereum (ETH)	Etherscan
Ocultação Patrimonial	Patrimônio não declarado Movimentação inconsistente com patrimônio Uso de mixers	Análise do material (frases-semente, anotações) Correlação com bens ocultos	Monero (XMR) Bitcoin (BTC) Stablecoins	Material apreendido IPED SIMBA Declaração de bens

[41] Red flags reconhecidos internacionalmente (FATF, Europol, PF).
[42] Fiat é abreviação de fiat Money. Conversão para fiat significa transformar criptoativos em dinheiro tradicional (real, dólar, etc.), geralmente em *exchanges* ou via negociações *peer-to-peer*.

Revista ARACÊ
ISSN: 2358-2472

Evasão Fiscal	Movimentação internacional sem declaração Valores recebidos de PSAVs estrangeiras	Rastreio *off-chain* Cruzamento com patrimônio declarado	Bitcoin Stablecoins	CIAF-Cripto

Fonte: Elaboração própria a partir de FATF (2019, 2025); Europol (2025); Chainalysis (2025); TRM Labs (2025); Monero Research Lab (2018); BRASIL. Polícia Federal. *Manual de Apoio à Investigação de Criptoativos* (2021); BRASIL. Instituto Nacional de Criminalística. *Manual de Procedimento Pericial – Busca e Apreensão de Criptoativos* (2021); atos normativos nacionais (Decreto nº 11.563/2023; Parecer CVM nº 40/2022).

5.5 ESTUDO DE CASO: APLICAÇÃO DO MODELO TRÍADE DE DESANONIMIZAÇÃO FORENSE NA OPERAÇÃO DECRYPTED

Em 2025, a Operação Decrypted[43], deflagrada pela Polícia Federal em cooperação com a *Homeland Security Investigations* (HSI, dos Estados Unidos), forma-se em estudo de caso, modelo, a fim de explicar a aplicação e iteratividade da Tríade de Desanonimização Forense.

É de se destacar que o presente estudo de caso se baseia exclusivamente em informações divulgadas em veículos de comunicação oficiais e privados (BPMONEY, 2025), sendo possíveis gerir fatos adicionais resultantes de análise acadêmica e da aplicação metodológica do modelo proposto.

Conforme informações oficiais[44], a investigação teve por objetivo desarticular uma organização criminosa suspeita de fraudar e furtar aproximadamente US$ 2,6 milhões em criptoativos de vítimas norte-americanas. A cooperação teve como produto o cumprimento de 11 mandados de busca e apreensão, além de medidas de sequestro de bens nos estados do Maranhão, Tocantins e Goiás.

No vértice o*ff-chain*, o vetor de contextualização de dados se iniciou com a cooperação internacional com a HSI, à qual encaminhou dados sobre o ilícito, tais como vítimas, valores subtraídos, suspeitos localizados em território brasileiro e endereços de carteiras virtuais possivelmente associados à fraude. Esse fato constituiu o vértice de contextualização de dados inicial do modelo, em que informações contextuais e externas são fundamentais para orientar o rastreamento técnico.

A investigação cresceu assim para o vértice *on-chain*, onde os endereços e transações indicados foram analisados em detalhe a partir do *ledger* público das blockchains envolvidas. Ferramentas especializadas puderam restaurar grafos transacionais, detectar clusters de endereços controlados pelos suspeitos e detectar pontos de saída em *exchanges*. Nessa etapa, também se verificaram técnicas de ofuscação, como uso de *mixers*, que buscavam dificultar o rastreamento.

43 POLÍCIA FEDERAL. PF deflagra Operação Decrypted contra fraudes em criptoativos. 26 ago. 2025. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2025/08/pf-deflagra-operacao-decrypted-contra-fraudes-em-criptoativos.
44 A análise reconstrutiva aqui apresentada baseia-se exclusivamente em informações de acesso público (PF, 2025; CNN Brasil, 2025). Detalhes operacionais específicos permanecem sob sigilo processual; portanto, o estudo tem caráter teórico e ilustrativo, voltado a demonstrar a aplicabilidade do modelo Tríade de Desanonimização Forense.

Revista ARACÊ
ISSN: 2358-2472

Os resultados técnicos retroalimentaram o vértice *off-chain* de identificação real, no qual, conforme se infere metodologicamente, ofícios e cartas rogatórias podem ser expedidos a PSAVs. Essas medidas, se fundamentadas em obrigações de KYC/AML, possibilitam quebrar a pseudonimidade, vincular endereços de blockchain a identificadores reais como CPF, nome e dados bancários. Embora não haja divulgação oficial sobre o conteúdo dessas diligências, esse modelo exemplifica como a tríade pode ser aplicada para converter dados técnicos em informação pessoalmente identificável.

Por último, há o correspondente ao vértice de correlação forense-jurídica, consistiu na consolidação dos achados em relatórios técnicos e representações judiciais. Nessa fase, dados (*on-chain*) e elementos contextuais (*off-chain*) foram integrados em uma narrativa probatória clara e auditável, capaz de fundamentar judicialmente os pedidos de mandados de busca, apreensão e sequestro de bens efetuados. O cumprimento das medidas judiciais no Maranhão, Tocantins e Goiás, que resultou na apreensão de veículos, criptoativos e outros bens, representou a materialização do modelo em resultados concretos.

O estudo de caso evidencia, portanto, que a investigação não progrediu de maneira linear, mas sim de modo iterativa, em que cada vértice retroalimentou os demais. Assim, a Operação *Decrypted*, apesar de aqui analisada a partir de dados públicos e reelaborada em modo de tríade, mostra como o vértice de Correlação Forense-Jurídica constitui o fator crítico de transformação, é competente para fazer com que os achados técnicos se tornem provas juridicamente válidas, cruciais para a desarticulação de organizações criminosas no contexto dos criptoativos.

6 CONSIDERAÇÕES FINAIS

Este artigo partiu da hipótese de que é possível ampliar a rastreabilidade de criptoativos explorando ações criminosas descuidadas, decorrentes da assimetria informacional presente no ecossistema digital. A falta de conhecimento técnico leva muitos usuários a acreditarem que estão completamente anônimos, quando, na realidade, existe apenas a pseudonimidade. Essa falsa sensação de invisibilidade os leva a agir sem cautela, deixando rastros que podem ser explorados em investigações.

Depois disso, a tríade apresentada articula três vértices, a saber: (i) *on-chain*, que rastreia fluxos e padrões diretamente nos registros imutáveis da blockchain; (ii) *off-chain*, que cruza informações de prestadores de serviços, dados KYC/AML e fontes abertas; e (iii) correlação forense-jurídica, que organiza os achados técnicos e os transforma em prova jurídica. Essa articulação resulta na chamada Tríade de Desanonimização Forense.

Revista ARACÊ
ISSN: 2358-2472

O modelo complementa o Manual de apoio à investigação de criptoativos (PF, 2021), ao manter os vetores de rastreamento (*on-chain* e *off-chain*) e inserir explicitamente o vértice de Correlação Forense-Jurídica. Essa inclusão é o que distingue o modelo, pois garante o nexo entre a evidência técnica e a prova legal. Adicionalmente, alinha-se ao Manual de Procedimento Pericial (INC, 2021), ao sistematizar a prova e incorporar no vetor *off-chain* a identificação de artefatos técnicos (como *seed phrase* e cadastros em PSAVs).

A principal contribuição deste estudo, contudo, é a consolidação da Tabela 4, que apresenta os tipos de crimes, sinais de alerta e estratégias investigativas específicas. Abordando desde o rastreamento *on-chain* na lavagem de dinheiro (fragmentação de operações, uso de *mixers*), até a correlação *off-chain* na evasão fiscal (transações internacionais e PSAVs estrangeiras) e na ocultação patrimonial.

Além disso, a análise do estudo de caso da Operação Decrypted demonstrou a prática do modelo, confirmando que a combinação entre cooperação internacional, rastreamento e vinculação de dados externos transforma registros digitais diversos em prova contábil-jurídica.

No futuro, há oportunidade de aprofundamento de pesquisas em três frentes: (i) o aprimoramento de heurísticas e ferramentas de análise *on-chain*; (ii) a expansão de protocolos de cooperação para fins de intercâmbio de dados entre autoridades e PSAVs, nacionais e internacionais; e (iii) a consolidação de padrões periciais para a apresentação de provas digitais em juízo.

Por fim, a capacidade de rastreabilidade dos criptoativos pode ser aumentada por meio da análise das atividades ilícitas imprudentes, resultantes da assimetria informacional existente no ecossistema digital. Esse déficit técnico faz com que os usuários acreditem estar completamente anônimos, quando na verdade estão apenas utilizando um pseudônimo, sendo dessa ilusão que se originam indícios importantes para a investigação.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. **Relatório Drex**. Brasília: BCB, 2023. Disponível em: https:/www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/piloto/Relatorio_Drex_piloto_fase_1.pdf. Acesso em: 20 ago. 2025.

BANK FOR INTERNATIONAL SETTLEMENTS (BIS). ***Central Bank Digital Currencies: Foundational Principles and Core Features***. Basel: BIS, 2020. Disponível em: https://www.bis.org. Acesso em: 2 set. 2025.

BANK FOR INTERNATIONAL SETTLEMENTS (BIS). ***BIS Annual Economic Report 2022 – Chapter 3: The Future Monetary System***. Basel: BIS, 2022. Disponível em: https://www.bis.org/publ/arpdf/ar2022e3.htm. Acesso em: 3 set. 2025.

BAZZELL, Michael. ***Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information***. 10. ed. California: IntelTechniques, 2023.

BINANCE. ***How to buy and sell crypto on Binance P2P***. Binance Blog, 2020. Disponível em: https://www.binance.com/en/blog/all/421499824684900825. Acesso em: 3 set. 2025.

BPMONEY. **PF deflagra operação contra esquema de furto de criptoativos nos EUA**. 2025. Disponível em: https://bpmoney.com.br/mercado/cripto/pf-deflagra-operacao-contra-esquema-de-que-furto-de-criptoativos-nos-eua. Acesso em: 28 ago. 2025.

BRASIL. Banco Central do Brasil. **Decreto nº 11.563, de 14 de junho de 2023**. Regulamenta a Lei nº 14.478, de 21 de dezembro de 2022, para estabelecer competências ao Banco Central do Brasil. Diário Oficial da União: seção 1, Brasília, DF, 15 jun. 2023.

BRASIL. Comissão de Valores Mobiliários (CVM). **Ofício Circular CVM/SSE nº 4, de 4 de abril de 2023**. Caracterização de tokens de recebíveis e de renda fixa como valores mobiliários. Rio de Janeiro: CVM, 2023. Disponível em: https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sse1/oc-sse-0423.html.

BRASIL. Comissão de Valores Mobiliários (CVM). **Ofício Circular CVM/SSE nº 6, de 5 de julho de 2023**. Complementa esclarecimentos sobre a caracterização de tokens de recebíveis e de renda fixa como valores mobiliários. Rio de Janeiro: CVM, 2023. Disponível em: https://www.gov.br/cvm/pt-br/assuntos/normas.

BRASIL. Comissão de Valores Mobiliários. **Parecer de Orientação nº 40, de 11 de outubro de 2022.** Trata da classificação jurídica dos criptoativos como valores mobiliários. *Diário Oficial da União*, Brasília, DF, 11 out. 2022.

BRASIL. Comissão de Valores Mobiliários. **Resolução CVM nº 88, de 27 de abril de 2022.** Dispõe sobre ofertas públicas de valores mobiliários via plataformas eletrônicas de investimento participativo. *Diário Oficial da União*, Brasília, DF, 28 abr. 2022.

BRASIL. Comissão de Valores Mobiliários. **Resolução CVM nº 160, de 13 de julho de 2022.** Dispõe sobre ofertas públicas de distribuição de valores mobiliários, registro automático e regimes de oferta. *Diário Oficial da União*, Brasília, DF, 14 jul. 2022.

Revista ARACÊ
ISSN: 2358-2472

BRASIL. **Lei nº 9.069, de 29 de junho de 1995**. Dispõe sobre o Plano Real, o Sistema Monetário Nacional, estabelece as regras e condições de emissão do Real e os critérios para conversão. Diário Oficial da União: Brasília, DF, 30 jun. 1995.

BRASIL. **Lei nº 9.613, de 3 de março de 1998.** Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores. *Diário Oficial da União*, Brasília, DF, 4 mar. 1998.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013.** Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública. *Diário Oficial da União*, Brasília, DF, 2 ago. 2013.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 12 out. 2025.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022.** Dispõe sobre diretrizes para prestação de serviços de ativos virtuais e sobre a atuação de provedores de serviços de ativos virtuais. *Diário Oficial da União*, Brasília, DF, 22 dez. 2022.

BRASIL. Departamento de Polícia Federal. Coordenação-Geral de Repressão à Corrupção, Crimes Financeiros e Lavagem de Dinheiro. **Manual de apoio à investigação de criptoativos**. Brasília: Polícia Federal, 2021. Disponível em: Intranet da Polícia Federal. Acesso em: 3 ago. 2025.

BRASIL. Instituto Nacional de Criminalística. **Manual de Procedimento Pericial - Busca e Apreensão de Criptoativos**. 1. ed. Brasília: Instituto Nacional de Criminalística, 2021.

BRASIL. Receita Federal do Brasil. **Instrução Normativa RFB nº 1.888, de 3 de maio de 2019.** Dispõe sobre a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Receita Federal. *Diário Oficial da União*, Brasília, DF, 7 maio 2019.

BRASIL. Receita Federal do Brasil. **Instrução Normativa RFB nº 2.219, de 9 de abril de 2024.** Altera a Instrução Normativa RFB nº 1.888, de 3 de maio de 2019, ampliando a obrigatoriedade de prestação de informações relativas a operações com criptoativos. *Diário Oficial da União*, Brasília, DF, 10 abr. 2024.

BUTERIN, Vitalik. ***Ethereum White Paper**: A Next-Generation Smart Contract and Decentralized Application Platform*. 2014. Disponível em: https://ethereum.org. Acesso em: 3 ago. 2025.

CASTELLO, Melissa. G. **Bitcoin é moeda? Classificação das criptomoedas para o direito tributário.** Revista de Direito GV, São Paulo, v. 15, n. 2, e1927, 2019. Disponível em: <https://www.scielo.br/j/rdgv/a/vz4x6BdS7znmfYFVmFrCY3C/>. Acesso em: 12 set. 2025.

CHAINALYSIS. ***The 2025 Crypto Crime Report***. New York: Chainalysis, fev. 2025. Disponível em: https://go.chainalysis.com/2025-crypto-crime-report. Acesso em: 7 set. 2025.

CHAINALYSIS. ***Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies***. *Chainalysis* Blog, 2023. Disponível em: https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/. Acesso em: 5 set. 2025.

Revista ARACÊ
ISSN: 2358-2472

CNN BRASIL. **Entenda a diferença entre criptomoeda e moeda digital, como a estudada pelo BC**. CNN Brasil, 19 de agosto. 2023. Disponível em: https://www.cnnbrasil.com.br/economia/financas/entenda-a-diferenca-entre-criptomoeda-e-moeda-digital-como-a-estudada-pelo-bc/. Acesso em: 25 ago. 2025.

COMITÊ DE PRONUNCIAMENTOS CONTÁBEIS (CPC). **CPC 04 (R1)** - Ativo intangível. 2010. Disponível em: https://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos. Acesso em: 25 ago. 2025.

COMITÊ DE PRONUNCIAMENTOS CONTÁBEIS (CPC). **CPC 16 (R1)** - Estoques. 2009. Disponível em: https://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos. Acesso em: 25 ago. 2025.

COMITÊ DE PRONUNCIAMENTOS CONTÁBEIS (CPC). **CPC 39** - Instrumentos. 2012. Disponível em: https://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos. Acesso em: 25 ago. 2025.

COMITÊ DE PRONUNCIAMENTOS CONTÁBEIS. **CPC 48 - Instrumentos Financeiros.** Brasília: CPC, 2017. Disponível em: https://www.cpc.org.br/CPC/Documentos-Emitidos/Pronunciamentos. Acesso em: 25 ago. 2025.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Parecer de Orientação nº 40, de 11 de outubro de 2022**. Brasília: CVM, 2022. Disponível em: https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html. Acesso em: 7 set. 2025.

EUROPEAN CENTRAL BANK. **A digital euro.** Frankfurt: ECB, 2023. Disponível em: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html. Acesso em: 25 ago. 2025.

EUROPOL. ***Internet Organised Crime Threat Assessment (IOCTA) 2025*. The Hague: Europol, 2025**. Disponível em: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2025. Acesso em: 7 ago. 2025

FEDERAL RESERVE. *Money and Payments:* ***The U.S. Dollar in the Age of Digital Transformation***. Washington: Board of Governors of the Federal Reserve System, Jan. 2022. Disponível em: https://www.federalreserve.gov/publications/money-and-payments-discussion-paper.htm. Acesso em: 25 ago. 2025.

FINANCIAL ACTION TASK FORCE (FATF). ***Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*** *(VASPs)*. Paris: FATF/OECD, jun. 2019. Disponível em: https://www.fatf-gafi.org. Acesso em: 2 set. 2025.

FINANCIAL ACTION TASK FORCE (FATF). ***12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs***. Paris: FATF/OECD, jul. 2020. Disponível em: https://www.fatf-gafi.org. Acesso em: 7 set. 2025.

FINANCIAL ACTION TASK FORCE (FATF). ***Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs***. Paris: FATF/OECD, fev. 2025. Disponível em: https://www.fatf-gafi.org. Acesso em: 7 set. 2025.

Revista ARACÊ
ISSN: 2358-2472

FURNEAUX, Nick. ***Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence***. Indianapolis: John Wiley & Sons, 2018.

GAÚCHAZH. "**Euforia com desconhecimento**", GaúchaZH, 2025. Disponível em: https://gauchazh.clicrbs.com.br/economia/noticia/2025/04/euforia-com-desconhecimento-diz-procurador-do-mpf-sobre-vitimas-de-golpes-com-criptomoedas.html. Acesso em: 24 maio. 2025.

INTERPOL. ***Guidelines for the Seizure and Sale of Virtual Assets*****.** Singapore: INTERPOL Innovation Centre, 2020.

KAPPOS, George; YAYLA, Kerim; KATZ, Jonathan; MEIKLEJOHN, Sarah**.** ***An Empirical Analysis of Anonymity in Zcash*****.** ***Proceedings on Privacy Enhancing Technologies***, v. 2018, n. 3, p. 297–316, 2018. DOI: 10.1515/popets-2018-0025. Disponível em: https://arxiv.org/abs/1805.03180. Acesso em: 7 set. 2025.

LIVECOINS. **MPF alerta sobre o uso de criptomoedas no Dia Mundial contra o Tráfico de Pessoas**. Livecoins, 31 jul. 2025. Disponível em: https://livecoins.com.br/mpf-alerta-sobre-o-uso-de-criptomoedas-no-dia-mundial-contra-o-trafico-de-pessoas. Acesso em: 24 jun. 2025.

MACHADO, Rafaela Pinheiro de Andrade**. Crypto assets*:* o equilíbrio entre a necessidade de regulamentação AML/CFT e a proteção de dados**. 2024. Dissertação (Mestrado em Direito e Prática Jurídica – Especialidade em Direito Civil) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2024.

MEIKLEJOHN, Sarah et al**. A fistful of bitcoins: characterizing payments among men with no names**. In: *Proceedings of the 2013 Internet Measurement Conference*. New York: ACM, 2013. p. 127-140. DOI: 10.1145/2504730.2504747.

NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven. ***Bitcoin and cryptocurrency technologies: a comprehensive introduction***. Princeton: Princeton University Press, 2016.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 04 ago. 2025.

NOETHER, Shen; MACKENZIE, Adam; Monero Research Lab. ***Ring Confidential Transactions***. *Ledger*, v. 1, 2016. DOI: 10.5195/LEDGER.2016.34.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Institutionalisation of crypto-assets and DeFi–TradFi interconnectedness**. Paris: OECD Publishing, 2022. Disponível em: <https://doi.org/10.1787/5d9dddbe-en>. Acesso em: 7 set. 2025.

POLÍCIA FEDERAL. **PF deflagra Operação Decrypted contra fraudes em criptoativos**. 26 ago. 2025. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2025/08/pf-deflagra-operacao-decrypted-contra-fraudes-em-criptoativos. Acesso em: 29 out. 2025.

ROCHMAN, Ricardo Ratner. **A Descentralização das Finanças**. GV Executivo, v. 22, p. 20-24, 2023.

Revista ARACÊ
ISSN: 2358-2472

STELLA, Julio César. **Moedas Virtuais no Brasil: como enquadrar as criptomoedas**. Revista da PGBC, Brasília, v. 11, n. 2, p. 33-50, dez. 2017.

TRM LABS. ***Privacy Coins***. TRM Labs Glossary, 2024. Disponível em: https://www.trmlabs.com/glossary/privacy-coins. Acesso em: 7 set. 2025

UNITED STATES**.** Department of the Treasury. ***U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash***. Washington, D.C.: Treasury, 08 ago. 2022. Disponível em: https://home.treasury.gov/news/press-releases/jy0916. Acesso em: 3 set. 2025.

UNITED STATES. Department of Justice. ***Bitcoin Fog Operator Sentenced for Money Laundering Conspiracy***. Washington, D.C.: DOJ, 08 nov. 2024. Disponível em: https://www.justice.gov/archives/opa/pr/bitcoin-fog-operator-sentenced-money-laundering-conspiracy. Acesso em: 3 set. 2025.