Estado da publicação: O preprint não foi publicado em outro meio.

Criptoativos e cadeia de custódia da prova

Diogo Erthal Alves da Costa

https://doi.org/10.1590/SciELOPreprints.18789

Submetido em: 2026-11-06
Postado em: 2026-11-10 (versão 1)
(AAAA-MM-DD)

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

CRIPTOATIVOS E CADEIA DE CUSTÓDIA DA PROVA

Crypto-Assets and the Chain of Custody of Evidence

Diogo Erthal Alves da Costa

Doutorando na UERJ. Mestre em Raciocínio Probatório pela Universidade de Girona. Mestre em Direito Penal e Ciências Criminais pela Universidade de Lisboa. Certificado *Mastering Web3* pela Universidade de Nicósia. *Advanced Crypto Investigator* (certificado TRM e Chainalysis). Membro do Grupo de Trabalho sobre criptoativos (Hemisfério Ocidental) do *U.S. Department of Justice* – Promotor de Justiça do MPRJ
https://orcid.org/0000-0002-7611-347X

Resumo

O crescimento do mercado de criptoativos e sua popularização no Brasil trouxeram esses ativos para o centro de demandas judiciais, especialmente na persecução patrimonial. Ainda assim, falta teoria consolidada sobre o tratamento probatório das evidências a eles relacionadas. Este artigo examina a aplicação da cadeia de custódia, prevista nos artigos 158-A a 158-F do Código de Processo Penal, às provas envolvendo criptoativos. O marco teórico é a concepção racional da prova. Sustenta-se que a cadeia de custódia se relaciona à fiabilidade do elemento probatório, e não à sua admissibilidade. Por isso, sua inobservância não gera nulidade e deve ser considerada no momento da valoração. A tese central é que a prova sobre criptoativos não constitui categoria unitária: suas modalidades apresentam problemas epistêmicos e jurídicos próprios e se distinguem pelo grau de autonomia do dado em relação a mecanismos externos de verificação. Os dados gravados em blockchains públicas suficientemente descentralizadas se autenticam por simples conferência pública, o que afasta a lógica da cadeia de custódia. Nos dados fornecidos por prestadoras de serviços de ativos virtuais centralizadas, a fiabilidade depende da idoneidade institucional da fonte e da forma de recebimento e manutenção do dado. Nas ferramentas de inteligência de blockchain, o agrupamento de endereços exige validação metodológica da heurística empregada. Já a atribuição desses endereços a entidades do mundo real depende de evidências off-chain, cada uma submetida ao seu próprio regime de custódia. Por fim, quando os dados sobre criptoativos estão vinculados a outras provas digitais, a cadeia de custódia tem aplicação plena e exige

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

cautelas adicionais no manuseio de chaves privadas e frases de recuperação (seed phrases).

Palavras-chave: criptoativos, blockchain, cadeia de custódia, prova digital, fiabilidade

Abstract

The growth of the crypto-asset market and its widespread adoption in Brazil have placed these assets at the center of judicial proceedings, particularly in asset recovery. Even so, there is still no consolidated theory on the evidentiary treatment of crypto-related evidence. This article examines how the chain of custody, governed by Articles 158-A to 158-F of the Brazilian Code of Criminal Procedure, applies to evidence involving crypto-assets. Its theoretical framework is the rationalist conception of evidence. The article argues that the chain of custody concerns the reliability of evidence, not its admissibility. Consequently, failure to comply with it does not render the evidence null and should instead be taken into account in the assessment of the evidence. The central thesis is that crypto-asset evidence is not a unitary category: each type raises its own epistemic and legal problems, and the types differ in how far the data can stand on its own without external verification mechanisms. Data recorded on sufficiently decentralized public blockchains is self-authenticating through simple public verification, so the chain-of-custody framework does not apply. For data provided by centralized virtual asset service providers (VASPs), reliability depends on the institutional trustworthiness of the source and on how the data is received and preserved. For blockchain intelligence tools, address clustering requires methodological validation of the heuristic used. Attributing those addresses to real-world entities, in turn, depends on off-chain evidence, each piece subject to its own custody regime. Finally, when crypto-asset data is linked to other digital evidence, the chain of custody applies in full and requires additional safeguards in handling private keys and recovery phrases (seed phrases).

Keywords: crypto-assets, blockchain, chain of custody of evidence, digital evidence, reliability of evidence

1. Introdução

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

Desde o surgimento da rede Bitcoin em 2008, o mercado de criptoativos experimentou crescimento vertiginoso, atualmente acima dos 2 trilhões de dólares[1]. O Brasil figura como o principal país do mundo em adoção de criptomoedas pela população[2], com mais de 4,5 milhões de CPFs ativos figurando em transações reportadas à Receita Federal[3]. Tamanha popularização inevitavelmente trouxe os criptoativos para o centro de demandas judiciais nas mais variadas áreas, especialmente as que envolvem persecução patrimonial.

Apesar da recente densificação do marco regulatório[4], inúmeras questões surgidas da interseção entre o universo blockchain e o direito permanecem carentes de enfretamento. Se destaca neste cenário a cadeia de custódia das provas relacionadas aos criptoativos. A arquitetura descentralizada e distribuída da blockchain exige abordagem própria, não bastando mera analogia com outros tipos de prova. A inexistência de teoria robusta cria cenário fértil para a má solução dos problemas surgidos nos casos concretos.

Este estudo visa jogar luzes sobre o tema e contribuir para o preenchimento desta lacuna teórica, desenvolvendo a compreensão de que *prova de blockchain ou criptoativo* não é categoria unitária e cada modalidade de evidência levanta problemas epistêmicos e jurídicos próprios.

2. A tecnologia blockchain

Antes de adentrarmos o tema da cadeia de custódia da prova, é indispensável trazer à lume algumas informações básicas sobre a tecnologia relacionada às redes blockchain[5].

Em meio à crise econômica e financeira global de 2008, ativistas da comunidade tecnológica, que já combatiam ataques à privacidade na internet, passaram a se opor à conduta adotada pelos Bancos Centrais para resgatar bancos privados em falência. Em 31 de outubro de 2008, em um portal de comunicações

---

[1] A maior marca histórica ocorreu em outubro de 2025, quando o mercado atingiu 4,4 trilhões de dólares, segundo relatório do Fundo Monetário Internacional (*Crypto Monitor Q1 2026*).
[2] CHAINALYSIS. *2026 Global Crypto Adoption Index*.
[3] https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos.
[4] Formado, entre outros diplomas, pela Lei nº14.478/2022, IN RFB 2.291/2025 e as resoluções BCB nº 519, 520 e 521.
[5] A abordagem se limitará ao estritamente necessário para análise da cadeia de custódia da prova.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

utilizado por *Cypherpunks*, uma pessoa ou grupo de pessoas, autointitulado Satoshi Nakamoto[6], publicou o artigo *Bitcoin: A Peer-to-Peer Electronic Cash System,* considerado a certidão de nascimento da referida rede[7]. Em janeiro de 2009, Satoshi Nakamoto efetuou a primeira transferência de *bitcoin*, nome com o qual batizou o criptoativo circulante na referida rede**.**

A proposta foi de implementação da primeira blockchain pública mundial. Uma infraestrutura digital de pagamento disponível a todos, não sendo propriedade de nenhuma instituição. Um sistema que permitisse a transferência de valores diretamente entre as partes envolvidas, demandando apenas acesso à internet, sem a necessidade de um terceiro interveniente (*trusted third party*), diferenciando-se do sistema financeiro tradicional, que conta com os bancos como emissores de moedas e garantidores das transações. Ela funciona com base em regras incorporadas ao software e a confiança conferida usualmente pelas instituições bancárias foi substituída nesse novo sistema por assinaturas digitais, criptografia, armazenamento descentralizado das informações, transparência e consenso distribuído. Ao invés de os dados serem registrados em um servidor, são arquivados em diversos pontos da rede, cada um deles considerado um nó *(node)*[8].

Além disso, os chamados mineradores (*miners*) "empregariam seu poder computacional em um sistema de incentivos para garantir a integridade da rede, aglutinar as transações válidas em 'blocos' e ligá-los por funções *hash* ao bloco anteriormente finalizado"[9]. Quando um usuário executa uma transação com criptoativos, os dados são transmitidos para a rede. Cada nó individual, de forma isolada, verifica se ela atende às regras do protocolo. O nó checa se a assinatura digital é válida (via criptografia de chave pública) e se os valores a serem transferidos ainda não foram gastos e são suficientes para cobrir o valor da transação. Se for inválida, será descartada**.** Uma transação validada é agrupada com outras em um bloco*,* que, após minerado, será registrado em cada um dos nós da rede. O bloco

---

[6] A identidade de Satoshi Nakamoto ainda é ignorada.
[7] O documento é conhecido como *Bitcoin White Paper*. Bitcoin foi o primeiro criptoativo, mas atualmente há milhares de outras redes e tokens. Weisheimer, Evandro *et al*. *Criptolavagem e compliance: tipologias de lavagem de dinheiro por meio de criptoativos e sua prevenção*. São Paulo: Rideel, 2022, p. 39-42 e 49-50.
[8] Disponível em <https://bitcoin.org/en/how-it-works>, acesso em 21/07/2026.
[9] Weisheimer, Evandro *et al*. *Criptolavagem e compliance: tipologias de lavagem de dinheiro por meio de criptoativos e sua prevenção*. São Paulo: Rideel, 2022. p. 43.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

seguinte conterá, entre outras informações, dados de novas transações, assim como o *hash*[10] do bloco anterior. As transações vão sendo arquivadas de forma cronológica, em blocos conectados uns aos outros, formando-se, então, uma cadeia de blocos, característica que confere o nome a tal tecnologia (*blockchain*). Todos estes dados são públicos, disponíveis na internet e facilmente acessíveis por qualquer interessado.

Assim, o sistema funciona como um livro-razão público, replicado em múltiplos pontos da rede, o que garante a inviabilidade de alteração dos dados registrados. Por conta do vínculo entre os blocos, a tentativa de alteração do conteúdo de um deles teria repercussão em todos os seguintes, o que não seria validado pelo sistema[11].

Apesar de as transações serem públicas, as partes não são representadas por seus nomes ou qualquer outro dado qualificativo, mas por endereços, consistentes em sequências alfanuméricas derivadas de chaves criptográficas, como ilustrado no exemplo abaixo[12]:

"Hash da transação: a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

Bloco: 57043

Hora: 2010-05-22 18:16:31 UTC

Endereço remetente: 1XPTgDRhN8RFnzniWCddobD9iKZatrvH4

Endereço destinatário: 17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ

Quantidade recebida: 10.000 BTC"

Analisando os dados armazenados na blockchain, percebe-se que não há qualquer informação vinculando os endereços envolvidos na transação aos sujeitos que negociaram. Um mesmo indivíduo pode ser o responsável por incontáveis endereços. Para transferir os ativos, o usuário precisa informar a chave privada vinculada ao endereço público, o que, em termos simples, pode ser comparado ao

[10] *Hash* criptográfico é um algoritmo matemático usado para transformar um conjunto de dados digitais em uma série de caracteres de comprimento fixo, conforme disponível em https://csrc.nist.gov/glossary/term/hash_function, acesso em 21/07/2026.
[11] Disponível em <https://bitcoin.org/en/how-it-works>, acesso em 21/07/2026.
[12] Disponível em <https://explorer.btc.com/btc/block/57043>, acesso em 21/07/2026.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

uso de uma senha para efetivar a transação. A chave privada não fica arquivada na rede, mas nas chamadas carteiras (*wallets*), que são mantidas sob o controle do usuário[13]. Na prática, quem possui a chave privada tem o poder de transferir os ativos vinculados ao endereço público correspondente. Percebe-se pelo exemplo acima que a transação é pública, mas a identidade das pessoas nela envolvidas não, o que confere o caráter pseudoanônimo a este tipo de criptoativo.

Entretanto, o rastreio da movimentação dos recursos e o emprego de heurísticas para vincular endereços diversos ao mesmo usuário, atrelados a dados não constantes da blockchain, podem permitir a identificação do detentor das chaves relacionadas a determinados endereços e, por consequência, os personagens envolvidos nas transações investigadas. Os dados acima se referem ao que é considerada a primeira "compra" de bens físicos realizada com bitcoins[14]. Em 22 de maio de 2010, Laszlo Hanyecz adquiriu duas pizzas transferindo 10.000 BTC para Jeremy Sturdivant. A identidade deles é conhecida pois foi amplamente divulgada de forma voluntária, não pelo que constou no bloco. A transação ficou famosa, sendo celebrada anualmente, no que é conhecido como *dia da pizza*[15].

O Bitcoin inaugurou o universo das moedas digitais descentralizadas de alcance global. A partir da sua arquitetura, surgiram inúmeras outras redes blockchain com propósitos e funcionalidades distintas. O Ethereum, por exemplo, introduziu a possibilidade de contratos inteligentes autoexecutáveis[16]. Outras focaram na busca por escalabilidade, tokenização de ativos e finalidades específicas. Esse processo de expansão resultou na atual pluralidade de redes e ativos, cada qual dotada de características técnicas, funcionais e jurídicas próprias, de modo que o bitcoin deve ser compreendido não como sinônimo do universo cripto, mas como seu precursor histórico e conceitual.

3. Cadeia de custódia de provas

---

[13] Disponível em <https://bitcoin.org/en/how-it-works>, acesso em 21/07/2026.
[14] A aquisição dos criptoativos pode ocorrer de diversas formas, como recompensa pela mineração, por meio de transações diretas entre usuários ou junto às prestadoras de serviço de ativos virtuais (exchanges), reguladas no Brasil pela Lei 14.478/22.
[15] Disponível em <https://forbes.com.br/forbes-money/2024/05/bitcoin-pizza-day-entenda-o-que-significa-a-data-para-o-mercado-cripto/>, acesso em 21/07/2026.
[16] Disponível em <https://ethereum.org/>, acesso em 21/07/2026.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

A disciplina específica da cadeia de custódia da prova penal foi introduzida no ordenamento jurídico pela Lei nº 13.964/2019 (Pacote Anticrime), que acrescentou os artigos 158-A a 158-F ao Código de Processo Penal, definindo cadeia de custódia como o "conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte".

O regramento, entretanto, não esclarece qual o efeito jurídico da eventual inobservância desses procedimentos. A resposta a tal questão exige análise da função do instituto no sistema processual penal.

No presente estudo adota-se como marco teórico a concepção racional da prova. Sem olvidar do inafastável respeito aos direitos e garantias dos acusados e de terceiros, o processo é compreendido como instrumento voltado para a obtenção de elementos de conhecimento que permitam, ao final, dar ou não como provada a proposição sobre a ocorrência de um fato com relevância criminal[17]. Tal entendimento deriva da constatação de que a "verdade sobre os fatos condiciona e determina a correção jurídica da solução da controvérsia, pois nenhuma norma se aplica de forma justa a fatos errôneos"[18].

Entretanto, sendo a certeza racional uma impossibilidade, busca-se a maior aproximação possível da verdade, com lastro em probabilidade lógica[19]. Cabe ao julgador adotar esquema valorativo racional das evidências, com decisões apoiadas no grau de confirmação das hipóteses, empregando o conceito de probabilidade indutiva[20].

Corolário desta compreensão é a adoção da relevância como primeiro filtro para admissão da prova. Cuida-se de critério de ordem epistêmica, sendo relevante todo elemento de prova que conferir "apoyo o refutación de alguna de las hipótesis

---

[17] Badaró, Gustavo Henrique. *Epistemologia Judiciária e Prova Penal.* São Paulo: Thomson Reuters Brasil, 2019. p. 62-68.

[18] Taruffo, Michele. *Simplemente la verdad: el juez y la construcción de los hechos*. Madrid: Marcial Pons, 2010. p. 134.

[19] Taruffo, Michele. *A prova.* São Paulo: Marcial Pons, 2014. 29-32.

[20] Abellán, Marina Gascón. *Los hechos en el derecho: bases argumentales de la prueba*. Madrid: Marcial Pons, 2010. p. 158-159.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

fácticas del caso a la luz de los principios generales de la lógica y de la ciencia"[21]. Devem ser admitidas e valoradas pelo julgador apenas as evidências que ostentem uma conexão lógica com os fatos em litígio, aquelas que permitam uma justificação racional da decisão[22]. Nesse sentido, o artigo 400, §1º, do Código de Processo Penal, dita que o juiz pode indeferir as provas consideradas irrelevantes, impertinentes ou protelatórias.

A epistemologia indica, ainda, que a probabilidade de erros, seja a condenação de inocentes ou a absolvição de culpados, é reduzida à medida que mais provas relevantes são aportadas ao conjunto de elementos a serem valorados pelo julgador, pois estas permitem maior grau de corroboração objetiva das hipóteses[23]. Assim, a admissão de provas relevantes não é mera faculdade do magistrado. Ao contrário, há que se reconhecer a existência do princípio da relevância que, ao mesmo tempo que prescreve a inadmissibilidade de provas inúteis, pois desprovidas de capacidade de apoio ou refutação racional das hipóteses, determina a admissão de todo elemento que permita uma maior aproximação da verdade e não seja excluído pela aplicação de critério adicional imposto por regras jurídicas[24].

Como a busca pela verdade não é absoluta no contexto do processo penal, há que se reconhecer a existência de um segundo filtro, o da admissibilidade jurídica, normalmente moldado como regra de exclusão da prova[25] e voltado para a proteção por parte do Direito de valores distintos da averiguação da verdade, como os direitos e garantias fundamentais dos investigados e de terceiros[26]. Na Constituição Federal há regra de exclusão expressa ditando que "são inadmissíveis, no processo, as provas obtidas por meios ilícitos" (artigo 5º, inciso LVI). O Código de Processo Penal também estabeleceu a inadmissibilidade das provas ilícitas e delas derivadas, esclarecendo

---

[21] Beltrán, Jordi Ferrer. *La Valoración Racional de la Prueba*. Madrid: Marcial Pons, 2007. p. 42.

[22] Taruffo, Michele. *A prova*. São Paulo: Editora Marcial Pons, 2014. p. 36.

[23] Ramos, Vitor de Paula. As duas faces do erro da decisão sobre os fatos no processo penal, ou quantos culpados absolvidos valem um inocente condenado. In: Salgado, Daniel de Resende, Kircher, Luís Felipe Schneider Kircher e Queiroz, Ronaldo Pinheiro de (coord.). *Altos Estudos Sobre a Prova no Processo Penal.* Salvador: Editora JusPodivm, 2020. p. 769.

[24] Taruffo, Michele. *A prova*. São Paulo: Editora Marcial Pons, 2014. p. 39 e 52-53 e Beltrán, Jordi Ferrer. *La Valoración Racional de la Prueba*. Madrid: Marcial Pons, 2007. p. 42-43.

[25] Taruffo, Michele. *A prova*. São Paulo: Editora Marcial Pons, 2014. p. 39.

[26] Beltrán, Jordi Ferrer. *La Valoración Racional de la Prueba.* Madrid: Marcial Pons, 2007. p. 43.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

que a ilicitude advém da obtenção em violação a normas constitucionais ou legais (artigo 157).

Sendo certo que a admissão de evidências relevantes reduz a probabilidade de decisão errada, decorrente da equivocada reconstrução dos fatos, as regras de exclusão devem ser analisadas com cautela. Serão justificáveis apenas quando os prejuízos que causam à busca da verdade forem, em correto juízo de proporcionalidade, suplantados por ganhos de outra natureza, como a proteção de direitos e garantias dos acusados[27].

Importante ter em conta que os momentos da admissibilidade e da valoração não se confundem. Naquele, a análise da relevância do meio de prova em relação ao objeto da prova deve ser abstrata e *ex ante.* Posteriormente, na valoração, haverá a análise concreta *ex post* do que foi produzido[28]*.* A relevância, portanto, deve ser avaliada com lastro nas alegações da parte e resolvida hipoteticamente[29].

Após admitida, já no momento da valoração, é necessário verificar a fiabilidade do elemento de prova, perquirindo sua solidez, sua qualidade epistêmica[30], analisando se há razões para tomar o conteúdo da prova como verdadeiro em algum grau de probabilidade[31].

A relevância, relembre-se, depende de juízo hipotético, que dá ensejo à conclusão categórica, do tipo “tudo ou nada”. Afinal, ou uma prova é relevante ou não é, não há gradação entre estas duas conclusões possíveis. A fiabilidade, por sua vez, desperta análise dos diferentes graus de confiança que pode ser depositada em determinado elemento probatório. Salgado leciona que a aferição da fiabilidade probatória deve estar inserida em um contexto de valoração, pois “o nível de

---

[27] Laudan, Larry. *Truth, Error, and Criminal Law: An Essay in Legal Epistemology.* Nova Iorque: Cambridge University Press, 2006. p. 19.

[28] Kircher, Luís Felipe Schneider. *Standards de prova no processo penal: em busca de um modelo controlável*. São Paulo: Editora Juspodivm, 2024. p. 213.

[29] Taruffo, Michele. *A prova*. São Paulo: Editora Marcial Pons, 2014. p. 36.

[30] Salgado, Daniel de Resende. *A Metaprova no Processo Penal: seu perfil conceitual e funcional e o controle racional da fiabilidade da prova*. São Paulo: Editora Juspodivm, 2023. p. 148-149.

[31] Kircher, Luís Felipe Schneider. *Standards de prova no processo penal: em busca de um modelo controlável*. São Paulo: Editora Juspodivm, 2024. p. 220.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

fiabilidade é o resultado de inferências direcionadas à comprovação gradual de que a prova, a partir da análise de determinados atributos, possui qualidade epistêmica”[32].

Nesse contexto, a cadeia de custódia da prova, compreendida como as providências para garantir a autenticidade e integridade do elemento de prova, possui natureza meramente instrumental e se relacionam à sua fiabilidade, não à sua admissibilidade. Sempre que o elemento de prova puder trazer dados úteis para a reconstrução histórica dos fatos que são objeto do processo (filtro da relevância) e não tiver sido obtido com violação de direitos fundamentais do investigado ou terceiros (filtro da admissibilidade jurídica), deve ser admitido.

Trata-se, portanto, de questão de valoração da prova, não de admissão/exclusão. A baixa fiabilidade não se confunde com nulidade, não sendo, assim, apta a justificar exclusão do elemento de prova. Nesse sentido, utilizando o conceito de *mismidad*, a jurisprudência do Tribunal Supremo espanhol assevera que a não observância das providências para devida custódia da evidência não leva à nulidade, pois tal circunstância “puede afectar a la credibilidad del análisis pero no a su validez”[33]. O Superior Tribunal de Justiça já decidiu que a violação da cadeia de custódia dos vestígios digitais “não guarda relação com as nulidades processuais, mas, sim, com a eficácia da prova, a ser analisada na situação concreta e à luz dos demais elementos produzidos na instrução”[34].

Da mesma forma que a observância estrita das providências legais não é garantia absoluta desta fiabilidade, o descumprimento de alguma delas também não retira automaticamente a fiabilidade. Cabe ao magistrado, no caso concreto, de forma fundamentada, conferir o grau devido de fiabilidade ao elemento de prova, sem prescindir do cotejo da prova em análise com as demais. Nada impede que a autenticidade e a higidez da evidência sejam demonstradas por outros elementos de prova disponíveis nos autos.

---

[32] Salgado, Daniel de Resende. Fundamentos à admissibilidade da metaprova no processo penal. Quaestio facti: revista internacional sobre razonamiento probatorio, nº 5, 2023, Girona, p. 97.
[33] Sala Segunda de lo Penal, STS 53/2014, 21 de Enero de 2014. Disponível em <http://www.poderjudicial.es/search/openCDocument/cac2ec927df2 ac24a0bb78e44820713e55160ae6742f0272>, acesso em 22/07/2026.
[34] Inq n. 1.674/DF, relatora Ministra Nancy Andrighi, Corte Especial, julgado em 6/5/2026, DJEN de 14/5/2026.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

Por sua vez, a prova relacionada às transações com criptoativos possui peculiaridades técnicas que, por vezes, afastam a aplicação do instituto da cadeia de custódia. É justamente esse fator que orienta a classificação proposta nas seções seguintes. O fato de a blockchain, fonte primária de uma das modalidades de dado a ser tratada, ser virtualmente imutável, projeta reflexos diretos sobre a lógica da cadeia de custódia: a integridade dos dados inseridos em blocos confirmados é garantida pela própria arquitetura tecnológica que sustenta a rede, não por providências de acondicionamento, lacração ou documentação equivalentes às exigidas para vestígios físicos ou para outras modalidades de prova digital. É essa constatação que fundamenta a tese central deste estudo, segundo a qual a prova relacionada a transações com criptoativos não constitui categoria unitária: cada modalidade de dado analisada a seguir relaciona-se de modo distinto com a lógica da cadeia de custódia.

4. Provas sobre criptoativos

Os dados relacionados às transações com criptoativos podem ser de natureza diversa, permitindo a sua classificação em categorias, com o tratamento jurídico próprio de cada uma delas. Na sequência, serão abordados (1) os dados gravados na blockchain, (2) os fornecidos por prestadoras de serviço de ativos virtuais centralizadas, (3) os advindos de ferramentas dotadas de inteligência de blockchain e (4) dados vinculados a outras provas digitais.

4.1 Dado gravado na blockchain pública (*on-chain*)

A ausência de autoridades centrais ou intermediários financeiros nas arquiteturas de registro distribuído desloca a confiança do sistema para a descentralização, transparência e imutabilidade da rede. Sob essa perspectiva teórica, dados gravados em redes consolidadas como as blockchains Bitcoin e Ethereum podem ser tidos como inalteráveis por estarem protegidos por criptografia e serem publicamente verificáveis.

Ressalva-se, contudo, que essa premissa de imutabilidade prática não constitui um atributo absoluto da tecnologia, mas pressupõe alto grau de descentralização, que exige tamanho poder computacional a ponto de tornar a adulteração do histórico de transações economicamente inviável. Conforme

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

demonstra estudo de revisão sistemática[35], enquanto redes maduras e amplamente distribuídas como o Bitcoin exigiriam um custo de ataque superior a US$ 6 bilhões, redes recentes ou pouco povoadas podem ser comprometidas por valores que oscilam entre US$ 50 mil e US$ 1 milhão. Esse abismo de segurança demonstra que a higidez e a inalterabilidade dos dados *on-chain* dependem estritamente das condições de segurança de cada protocolo específico. Por tal razão, os fundamentos desenvolvidos ao longo desta seção estão expressamente condicionados ao preenchimento desse pressuposto de descentralização, rejeitando-se qualquer generalização abstrata sobre a blockchain enquanto categoria tecnológica homogênea.

Justificada tal premissa, passa-se à análise da obtenção de tais dados. Sendo um livro-razão público disponível na internet, é livre o acesso ao que está gravado na cadeia de blocos. Conforme já decidido pelo Superior Tribunal de Justiça, quando o ambiente virtual é público, são compartilhados dados que qualquer interessado pode obter. O acesso a eles não configura invasão a espaço privado ou interceptação de comunicações que exigiria prévia autorização judicial, mas mera “coleta de informações disponíveis em ambiente compartilhado”[36].

Sendo a transparência um dos fundamentos do sistema, não há que se falar em proteção de privacidade dos usuários que voluntariamente transacionam ativos na rede. Desnecessária, assim, anuência dos envolvidos na transação ou exigência de autorização judicial para acesso. Qualquer interessado pode fazer uma cópia de todo o histórico de dados *on-chain* diretamente da rede descentralizada. Por conta da facilidade e agilidade, é mais comum que seja feita apenas uma consulta aos dados gravados, utilizando exploradores de blocos (*block explorers*). São plataformas gratuitas acessíveis pela internet que mantêm nós das respectivas redes blockchain e disponibilizam os dados por meio de interface amigável.

Em redes como Bitcoin e Ethereum, os principais tipos de dados acessíveis são os relacionados à transação (ativo transferido, quantidade, endereços envolvidos, data e hora exatas e taxas descontadas em favor dos mineradores/validadores), ao

---

[35] Sello, Buti; Yong, Jianming; Tao, Xiaohui. *51% attack vulnerability of nascent blockchains: a comprehensive review*. Complex & Intelligent Systems, v. 12, 120 (2026).

[36] STJ, Informativo nº 870, 11/11/2025. Processo em segredo de justiça, Rel. Ministro Rogerio Schietti Cruz, Sexta Turma, por unanimidade, julgado em 14/10/2025.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

bloco (número do bloco, *hash* e tamanho) e aos contratos inteligentes (código de programação e interações).

Ressalte-se que a extensão da verificabilidade pública varia conforme o protocolo. Em redes como *Monero* e *Zcash* são empregadas camadas extras de privacidade. Assim, a consulta por qualquer interessado ao explorador de blocos permanece possível, preservando-se, por exemplo, o uso do *hash* para verificação da existência, validade e inclusão da transação na cadeia. Entretanto, o conjunto de dados tornados públicos é sensivelmente menor. Elementos como remetente, destinatário e, a depender do protocolo, o próprio valor transacionado, permanecem ocultos, ainda que a integridade criptográfica da operação seja publicamente atestável[37].

Após a consulta livre, para utilizar como elemento de prova, cabe ao interessado apenas documentar de modo auditável os dados relevantes que encontrou registrados na blockchain. Para tal, não há necessidade de laudo pericial, pois basta relato descrevendo os dados individualizadores das transações relevantes, preferencialmente os respectivos códigos *hash.*

Quanto à fiabilidade, é oriunda do próprio processo de criação do dado. Como cada transação registrada na rede é inalterável em virtude da criptografia, a autenticação da prova é feita pela simples conferência, possível a qualquer interessado, do que está registrado na blockchain. Assim, fica garantida a plena correspondência entre o que é tido no processo como elemento de prova e os dados *on-chain,* sendo indiferente o autor ou formato de apresentação do relato (narrativa em petição, *print* de explorador de blocos, relatório do investigador com ou sem gráfico, com ou sem ferramenta paga etc.).

Como não há coleta, posse ou manuseio de vestígios, mas mera documentação que permite acesso aos dados que permanecem na blockchain, não se aplica nesta hipótese a lógica da cadeia de custódia disciplinada no artigo 158-A e seguintes do Código de Processo Penal. Havendo divergência entre o documentado

[37] A resolução BCB nº 520 veda explicitamente a oferta e intermediação de ativos desta natureza por prestadoras de serviço de ativos virtuais (PSAVs) por conta das características que facilitam o anonimato e favorecem práticas de lavagem de dinheiro, financiamento de terrorismo e proliferação de armas de destruição em massa.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

nos autos e os dados *on-chain*, não se tratará de quebra de cadeia de custódia, mas falha na apresentação dos dados em juízo, remediável pela correção após verificação.

Destaque-se, entretanto, que tal fiabilidade advinda da autoautenticação abrange apenas o que está documentado na blockchain, não alcançando qualquer interpretação que extrapole esse espaço de objetividade, nem a correlação de tais dados com outros não documentados na cadeia (*off-chain*). Relembre-se o pseudoanonimato existente, pois os dados se referem à movimentação de ativos entre endereços públicos formados por chaves alfanuméricas, que, isoladamente, não permitem atribuir as transações a pessoas ou entidades.

4.2 Dados fornecidos por prestadoras de serviço de ativos virtuais centralizadas (*exchanges*)

Distinta é a hipótese dos dados fornecidos por prestadoras de serviços de ativos virtuais centralizadas que intermedeiam a relação entre o usuário e o ecossistema blockchain[38]. Nesse contexto, as transações realizadas pelo cliente não estarão necessariamente registradas na rede. Isso porque a movimentação interna de ativos dos usuários de uma mesma prestadora tende a ser processada e refletida apenas no sistema contábil próprio da *exchange*, sem gerar necessariamente, para cada operação, uma correspondente transação *on-chain*. O saldo que o usuário ostenta junto à prestadora de serviços de ativos virtuais constitui, assim, mera anotação contábil interna desta, que pode não encontrar correspondência ou espelhamento na blockchain, na medida em que os ativos dos clientes são tipicamente mantidos em carteiras agregadas de titularidade da própria prestadora, movimentadas de forma consolidada e não segregada por operação individual[39].

Dessa distinção decorrem consequências relevantes para a prova. Enquanto a hipótese tratada na seção anterior tem como objeto dados públicos, autoautenticáveis e verificáveis por qualquer interessado diretamente na rede, os dados relativos à movimentação de ativos e saldo do usuário junto à prestadora são registros privados, não expostos a consulta pública e desprovidos da garantia de

[38] Ressalte-se que a distinção ora tratada se aplica especificamente às exchanges centralizadas (CEXs) e demais PSAVs que operam sob modelo de custódia própria, não se estendendo às exchanges descentralizadas (DEXs), cujas operações, por prescindirem de intermediário custodiante, permanecem sujeitas ao regime de prova *on-chain* tratado no item anterior.

[39] Zetzsche, Dirk; Nikolakopoulou, Areti, *Crypto Custody: An Empirical Assessment*, Journal of Financial Regulation, Volume 11, Issue 1, April 2025, Pages 73–97.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

imutabilidade própria do registro distribuído. A obtenção de tal prova, portanto, depende da cooperação das prestadoras de serviço.

A Lei nº 14.478/2022 definiu em seu artigo 5º a prestadora de serviços de ativos virtuais (PSAV) como sendo a pessoa jurídica que executa, em nome de terceiros, pelo menos um dos seguintes serviços de ativos virtuais: I - troca entre ativos virtuais e moeda nacional ou moeda estrangeira; II - troca entre um ou mais ativos virtuais; III - transferência de ativos virtuais; IV - custódia ou administração de ativos virtuais ou de instrumentos que possibilitem controle sobre ativos virtuais; ou V - participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda de ativos virtuais. Além disso, alterou a Lei nº 7.492/1996 para equiparar à instituição financeira a pessoa jurídica que ofereça serviços referentes a operações com ativos virtuais, inclusive intermediação, negociação ou custódia (art. 1º, parágrafo único, I-A).

O Conselho Monetário Nacional, por sua vez, por meio da Resolução nº 5.280/2026, incluiu as sociedades prestadoras de serviços de ativos virtuais no escopo da Lei Complementar nº 105, de 10 de janeiro de 2001, que dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

Assim, salvo os dados de cadastro, que podem ser requisitados diretamente pela autoridade policial ou membro do Ministério Público às referidas entidades (Lei nº 9.613/1998, art. 17-B e Lei nº 12.965/2014, art. 10, §3º), será indispensável prévia decisão de afastamento do sigilo nos moldes da legislação mencionada para acesso aos dados relacionados às movimentações do usuário junto à exchange.

Nessa hipótese, a fiabilidade não deriva de uma característica intrínseca e criptograficamente verificável do dado, mas do processo institucional que o produziu. Isso significa que a valoração probatória de tais dados não pode prescindir da aferição de elementos como a idoneidade regulatória da prestadora de serviço.

Ademais, é preciso demonstrar a autenticidade e integridade dos dados apresentados em juízo, de modo a comprovar que foram fornecidos pela fonte correta e não foram alterados. Neste ponto, ganha relevo a criação de canais institucionais de comunicação entre o Judiciário e as *exchanges.* Espera-se que, em futuro próximo, os dados oriundos das PSAVs tramitem por canais ágeis e seguros como o SISBAJUD. Até lá é aconselhável que o recebimento destas informações seja

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

devidamente documentado, para evitar discussões sobre autenticidade e integridade dos dados.

4.3 Dados advindos de ferramentas dotadas de inteligência de blockchain

4.3.1 Admissibilidade e fiabilidade das ferramentas

Outra categoria que pode ser identificada é a das provas advindas do emprego de ferramentas especializadas em rastreio de criptoativos, que não se limitam a informar os dados públicos da blockchain, mas os processam por meio de heurísticas proprietárias para gerar conclusões sobre agrupamento de endereços e sua atribuição a entidades. Diferentemente do dado *on-chain*, cuja fiabilidade decorre da autoautenticação garantida pela própria arquitetura da rede, o produto dessas ferramentas resulta de processo analítico, que agrega, ao dado público subjacente, metodologia própria cuja idoneidade não pode ser verificada pela simples conferência do *hash* da transação.

Descortinam-se neste ponto dois problemas distintos: a admissibilidade do emprego destas ferramentas em geral, que não se confunde com a fiabilidade das provas produzidas em cada caso concreto. A primeira questão foi objeto de artigo específico[40]. Na oportunidade, a análise partiu do estudo de jurisprudência norte-americana. No caso nº 20-sc-3310 (ZMF), o juiz Zia M. Faruqui reconheceu a fiabilidade das ferramentas de rastreio a partir do emprego reiterado com resultados corretos, corroborados por diligências subsequentes. Já em *United States v. Sterlingov*, submetida a ferramenta Chainalysis Reactor ao crivo dos critérios *Daubert*, a Corte concluiu, entre outros fundamentos, que a heurística de agrupamento de endereços pode ser testada e replicada por peritos independentes ou por outras ferramentas concorrentes, precisamente porque os dados subjacentes são públicos.

A fiabilidade das ferramentas de análise de blockchain foi reconhecida pelo Grupo de Ação Financeira Internacional (GAFI) ao afirmar sua imprescindibilidade para auxiliar nas investigações e reduzir riscos relacionados a diversas atividades ilícitas[41].

---

[40] Costa, Diogo Erthal Alves da. *Análise da admissibilidade do uso de ferramentas especializadas em rastreio de criptoativos na persecução penal no Brasil*. Revista de Direito e as Novas Tecnologias, São Paulo: Revista dos Tribunais, v. 8, n. 27, p. 50-68, abr./jun. 2025.

[41] FATF, *Targeted Report on Regulatory Challenges from Decentralised Finance*, Paris, France, 2026.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

Soma-se a isso a contribuição da própria indústria de rastreio de criptoativos, que recentemente formalizou, em ontologia própria, distinção conceitual importante: a de que o produto dessas ferramentas não constitui categoria unitária, mas conjunto de proposições analíticas distintas, cada qual com sua própria natureza probatória e seu próprio padrão de fiabilidade[42]. Tal formalização é particularmente útil ao presente estudo, na medida em que reforça, também no âmbito das ferramentas de inteligência de blockchain, a tese central de que a prova sobre criptoativos não é categoria unitária. A partir desse referencial, distinguem-se, nas subseções seguintes, (a) o agrupamento de endereços sob controle comum e (b) a atribuição desse agrupamento a uma entidade nomeada, com a determinação de sua condição de operadora ou mera beneficiária.

4.3.2 Agrupamento de endereços (*wallet segment/clustering*)

O agrupamento de endereços decorre da conclusão de que múltiplos endereços públicos estão sob controle de uma mesma chave ou infraestrutura criptográfica, a partir de heurísticas aplicadas sobre dados *on-chain*. A técnica mais consolidada é a heurística de gasto conjunto (*co-spending*), segundo a qual endereços que figuram simultaneamente como remetentes em uma mesma transação necessariamente compartilham controle da chave privada correspondente.

Tem como base remota dados *on-chain*, mas não se beneficia da autoautenticação direta pelo *hash* da transação, pois a conclusão de que dois ou mais endereços pertencem à mesma carteira não está registrada, como tal, na blockchain, mas decorre de inferência sobre os dados nela registrados. A fiabilidade decorre da validação metodológica da heurística empregada, não de qualquer providência de acondicionamento, lacração ou preservação física do vestígio. Tampouco há, nessa hipótese, coleta ou manuseio de vestígio em sentido próprio, aproximando-se, nesse aspecto, do regime do dado *on-chain,* não sendo aplicada a lógica da cadeia de custódia disciplinada nos artigos 158-A e seguintes do Código de Processo Penal. Exige-se, na verdade, validação metodológica da heurística empregada para aferir a fiabilidade da prova. Este controle de idoneidade científica da técnica vai se dar no plano abstrato da metodologia e, excepcionalmente, no caso concreto.

---

[42] CHAINALYSIS. *Defining the Cluster: A Formal Ontology for Blockchain Address Analysis and Intelligence Claims*. 2026.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

No primeiro, de natureza geral e prévia, afere-se a solidez da heurística em si, com base em inúmeros critérios como: documentação da metodologia para avaliação independente; enumeração dos modos de falha conhecidos capazes de gerar falso positivo (por exemplo, transações colaborativas como *CoinJoin* ou *PayJoin*, em que múltiplos usuários assinam conjuntamente sem compartilhar controle da chave); existência de salvaguardas específicas para cada modo de falha identificado; e reprodutibilidade do resultado por perito independente a partir dos mesmos dados e da mesma metodologia. Preenchidos tais requisitos, e demonstrada a ampla adoção da metodologia por instituições financeiras e agências de persecução penal, dispensa-se, como regra, nova demonstração da fiabilidade geral da heurística a cada agrupamento concreto, tal como reconhecido pela jurisprudência norte-americana mencionada.

No segundo nível, o questionamento da fiabilidade de agrupamento apresentado no caso concreto depende de impugnação específica da parte interessada, apontando a existência de falha. Não basta a impugnação genérica da metodologia empregada, pois esta já foi reconhecida como fiável no plano abstrato. Exige-se demonstração pontual de sua eventual incorreção no caso concreto, ônus que recai sobre quem impugna a prova. Neste caso, pode se revelar necessária a produção de prova pericial para controle da fiabilidade da prova oriunda da ferramenta.

4.3.3 Atribuição a entidade nomeada e determinação operador/beneficiário

Questão diversa é a atribuição desse agrupamento a uma entidade nomeada do mundo real. Enquanto o agrupamento deriva de inferência sobre dados *on-chain*, a atribuição é dependente de dados *off-chain.* Qualquer que seja a quantidade de dados públicos da blockchain analisados, não será possível identificar a pessoa física ou jurídica titular de determinado conjunto de endereços apenas com base neles. Tal vínculo depende de evidências externas, como as advindas de interação com prestadores de serviço, informações de fontes abertas (OSINT), dados de outras investigações, apreensão de dispositivos, dados digitais arquivados em nuvem etc.

Peculiaridade de especial relevância prática é o risco de confusão entre o operador da infraestrutura de determinada carteira e o mero beneficiário mediado por aquele operador. Por exemplo, o endereço de depósito de um usuário em uma

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

exchange centralizada pode ser corretamente atribuído, a partir de informações fornecidas pelo prestador, àquele usuário específico. No entanto, o endereço integra a infraestrutura de carteira agregada operada pela *exchange*, não pelo usuário. Estender tal atribuição a todo o agrupamento de endereços da *exchange* constituiria erro grave.

Assim, a fiabilidade da atribuição não poderá ser aferida por autoautenticação, nem poderá ser verificada pela solidez em abstrato de heurísticas, como as que permitem os agrupamentos de endereços. Vai depender das particularidades do caso, da fonte do dado externo e do cotejo com os demais elementos de prova, cada qual submetido ao regime de cadeia de custódia que lhe for próprio, conforme sua natureza e origem específica.

4.4 Dados vinculados a outras provas digitais

Além das hipóteses já tratadas, dados referentes a transações com criptoativos podem chegar ao processo por outros elementos incidentalmente obtidos no curso da investigação, como arquivos extraídos de dispositivo móvel ou documentos obtidos em cumprimento de busca e apreensão.

Nesse caso, tais elementos podem ser fonte de dados verificáveis na blockchain, como ocorre com um arquivo de imagem que foi extraído de um telefone e contém o *hash* de uma transação. Quanto à existência e integridade da transação, aplica-se a mesma lógica de autoautenticação já desenvolvida para dados *on-chain*, dispensando, quanto a esse aspecto específico, qualquer aferição de idoneidade do processo de coleta e preservação. A autoautenticação, contudo, é limitada à verificação da transação, não se estendendo ao arquivo de imagem. A rede nada esclarece sobre o arquivo ter sido ou não encontrado no aparelho, nem sobre eventual adulteração após a apreensão do dispositivo. Uma coisa é verificar na rede se a transação ocorreu, outra é a análise de fiabilidade da prova digital de onde adveio a informação. A autenticidade e integridade do arquivo de imagem permanecem sujeitas à lógica geral de análise de fiabilidade, assim como à cadeia de custódia disciplinada nos artigos 158-A e seguintes do Código de Processo Penal, tal qual ocorre com os demais elementos extraídos do aparelho telefônico.

São aconselháveis, em qualquer dessas hipóteses, algumas adaptações decorrentes de peculiaridades do ambiente cripto, especialmente em razão da

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

sensibilidade de determinados dados. Destaca-se o cuidado exigido na eventual apreensão ou documentação de frases de recuperação (*seed phrases*) e chaves privadas, cuja exposição indevida pode comprometer a apreensão de ativos virtuais, permitindo a terceiros o esvaziamento da carteira antes mesmo da conclusão do procedimento, cenário de extrema gravidade em razão da irreversibilidade das transações em blockchain. Mostra-se recomendável a adoção de protocolo de atuação para evitar, por exemplo, que tais elementos sejam fotografados com dispositivos pessoais e posteriormente compartilhados em grupos de trabalho, devendo haver célere e segura comunicação apenas entre os agentes diretamente envolvidos na obtenção dos dados e os responsáveis por empregá-los para a pronta apreensão dos criptoativos a eles relacionados. Seguindo tal lógica, também não é aconselhável que sejam armazenados em envelopes transparentes ou de fácil violação, pois esta prática multiplica as possibilidades de exposição indevida e compromete a rastreabilidade de eventual acesso não autorizado.

A cadeia de custódia, nessas hipóteses, deve ensejar, além da documentação sobre cada agente que teve contato com a informação sensível e o momento e a finalidade do acesso, as medidas de segurança empregadas para restringir sua circulação. Deste modo, abre-se a possibilidade de, em sendo verificado posterior desvio dos ativos, a reconstrução do trajeto da informação e a identificação de eventual responsabilidade.

Nestes casos, a cautela e adequação no manuseio e a robustez da documentação assumem uma função dupla: não apenas atestam a idoneidade da obtenção dos dados, como também operam como salvaguarda preventiva contra o risco, inerente aos ativos digitais, de subtração indevida.

5. Considerações finais

O presente estudo partiu da constatação de que a crescente popularidade dos criptoativos e seus naturais reflexos nas contendas judiciais não encontraram, até o momento, correspondente desenvolvimento doutrinário sobre o tratamento probatório da evidência a eles relacionada. Buscou-se, a partir desse diagnóstico, demonstrar que *prova de blockchain* não constitui categoria unitária, mas conjunto heterogêneo de evidências, cada qual com problemas epistêmicos e jurídicos próprios, que

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

reclamam tratamento diferenciado quanto à sua fiabilidade e à aplicação da cadeia de custódia disciplinada pelos artigos 158-A e seguintes do Código de Processo Penal.

A análise conduzida ao longo do estudo revelou que essa heterogeneidade se organiza em torno de um eixo comum: o grau de autonomia do dado em relação a mecanismos externos de verificação. O dado gravado *on-chain*, em redes que preencham o pressuposto de descentralização adequada, é autenticado pela simples conferência pública, dispensando a lógica da cadeia de custódia. Já o dado fornecido por prestadora de serviços de ativos virtuais centralizada desloca a fiabilidade para a idoneidade institucional de terceiro, dependente de cooperação e de canais adequados de comunicação entre o Judiciário e essas entidades.

O produto das ferramentas de inteligência de blockchain, por sua vez, revelou-se categoria de natureza dual: o agrupamento de endereços tem a fiabilidade aferida por controle de idoneidade científica da heurística empregada, e não pela lógica da cadeia de custódia. A atribuição de endereços ou vinculação de uma carteira a determinada entidade, e a determinação de sua condição de operadora ou beneficiária, dependem de evidências *off-chain* variadas, cada qual submetida ao regime de cadeia de custódia que lhe for próprio, conforme sua natureza e origem específica. Por fim, os dados vinculados a outras provas digitais representam o campo em que a cadeia de custódia encontra sua aplicação mais necessária, exigindo, ademais, cautelas adicionais em razão da sensibilidade de dados como chaves privadas e *seed phrases*.

Espera-se, desta forma, contribuir para o preenchimento da lacuna teórica identificada na introdução deste estudo, oferecendo aos operadores do Direito parâmetros metodológicos para o enfrentamento adequado de um contencioso que, tudo indica, continuará a crescer na mesma velocidade do mercado que lhe dá origem.

Referências

ABELLÁN, Marina Gascón. *Los hechos en el derecho: bases argumentales de la prueba*. Madrid: Marcial Pons, 2010.

BADARÓ, Gustavo Henrique. *Epistemologia judiciária e prova penal*. São Paulo: Thomson Reuters Brasil, 2019.

BELTRÁN, Jordi Ferrer. *La valoración racional de la prueba*. Madrid: Marcial Pons, 2007.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

CHAINALYSIS. *2026 Global Crypto Adoption Index*. 2025. Disponível em: https://www.chainalysis.com/blog/2026-global-crypto-adoption-index/. Acesso em 19/10/2026.

CHAINALYSIS. *Defining the Cluster: A Formal Ontology for Blockchain Address Analysis and Intelligence Claims*. 2026. Disponível em: https://www.chainalysis.com/reports/defining-the-cluster/. Acesso em 22/07/2026.

COSTA, Diogo Erthal Alves da. Análise da admissibilidade do uso de ferramentas especializadas em rastreio de criptoativos na persecução penal no Brasil. *Revista de Direito e as Novas Tecnologias*, São Paulo: Revista dos Tribunais, v. 8, n. 27, p. 50-68, abr./jun. 2025.

FATF, *Targeted Report on Regulatory Challenges from Decentralised Finance*, Paris, France, 2026. Disponível em https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Virtualassets/targeted-report-decentralisedfinance-2026.html. Acesso em 22/07/2026.

FUNDO MONETÁRIO INTERNACIONAL. *Crypto Monitor Q1 2026*. Disponível em: https://www.imfconnect.org/content/dam/imf/News%20and%20Generic%20Content/GMM/Special%20Features/Crypto%20Monitor%20Q1%202026.pdf. Acesso em 22/07/2026.

KIRCHER, Luís Felipe Schneider. *Standards de prova no processo penal: em busca de um modelo controlável*. São Paulo: Editora Juspodivm, 2024.

LAUDAN, Larry. *Truth, error, and criminal law: an essay in legal epistemology*. Nova Iorque: Cambridge University Press, 2006.

NAKAMOTO, Satoshi. *Bitcoin: a peer-to-peer electronic cash system*. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em 22/07/2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Computer Security Resource Center Glossary: hash function*. Disponível em: https://csrc.nist.gov/glossary/term/hash_function. Acesso em 21/07/2026.

RAMOS, Vitor de Paula. As duas faces do erro da decisão sobre os fatos no processo penal, ou quantos culpados absolvidos valem um inocente condenado. In: SALGADO, Daniel de Resende; KIRCHER, Luís Felipe Schneider; QUEIROZ, Ronaldo Pinheiro de (Coord.). *Altos estudos sobre a prova no processo penal*. Salvador: Editora JusPodivm, 2020, p. 754-775.

SALGADO, Daniel de Resende. *A metaprova no processo penal: seu perfil conceitual e funcional e o controle racional da fiabilidade da prova*. São Paulo: Editora Juspodivm, 2023.

SALGADO, Daniel de Resende. Fundamentos à admissibilidade da metaprova no processo penal. *Quaestio Facti: revista internacional sobre razonamiento probatorio*, Girona, n. 5, 2023.

SELLO, Buti; YONG, Jianming; TAO, Xiaohui. 51% attack vulnerability of nascent blockchains: a comprehensive review. *Complex & Intelligent Systems*, v. 12, art. 120, 2026. Disponível em: https://link.springer.com/article/10.1007/s40747-026-02256-w. Acesso em 21/07/2026.

TARUFFO, Michele. *A prova*. São Paulo: Marcial Pons, 2014.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/SciELOPreprints.18789

TARUFFO, Michele. *Simplemente la verdad: el juez y la construcción de los hechos*. Madrid: Marcial Pons, 2010.

WEISHEIMER, Evandro *et al*. *Criptolavagem e compliance: tipologias de lavagem de dinheiro por meio de criptoativos e sua prevenção*. São Paulo: Rideel, 2022.

ZETZSCHE, Dirk; NIKOLAKOPOULOU, Areti. Crypto Custody: An Empirical Assessment. *Journal of Financial Regulation*, v. 11, n. 1, p. 73-97, abr. 2025. Disponível em: https://doi.org/10.1093/jfr/fjaf004. Acesso em 22/07/2026.

Declaração de originalidade

O autor assegura que o texto aqui publicado não foi publicado anteriormente em nenhum outro meio e que eventual republicação futura somente ocorrerá com a indicação expressa da referência desta publicação original. Atesta, ainda, a inexistência de plágio de terceiros ou de autoplágio.

Declaração sobre o uso de inteligência artificial

O autor declara estar ciente de que o uso de inteligência artificial não deve substituir a originalidade humana da pesquisa e de que a responsabilidade por eventuais erros ou plágio recai integralmente sobre ele. Declara que a IA Claude (Anthropic) foi usada para revisão gramatical, ortográfica e linguística. O conteúdo substantivo, ou seja, a conceituação, a tese central, a análise jurídica, os parâmetros propostos e os juízos interpretativos, é produto exclusivo do trabalho humano do autor, que permanece integralmente responsável por quaisquer erros, omissões ou plágio.

Declaração sobre conflito de interesses

O autor declara não haver conflito de interesses. Não recebeu financiamento, remuneração ou qualquer outra forma de apoio para a elaboração deste trabalho, e não mantém vínculo empregatício, contratual ou societário com as empresas mencionadas no texto. Para fins de transparência, informa que possui certificações de investigação de criptoativos emitidas pela TRM Labs e pela Chainalysis, obtidas no contexto de capacitação profissional, sem relação com a elaboração deste artigo. As opiniões expressas são de responsabilidade exclusiva do autor e não representam necessariamente a posição das instituições às quais está vinculado.

Disponibilidade de dados de pesquisa

Todo o conjunto de dados que dá suporte aos resultados deste estudo está contido no próprio artigo. Por se tratar de pesquisa teórica, não foram gerados nem analisados conjuntos de dados de pesquisa. As fontes utilizadas (legislação, jurisprudência, doutrina, relatórios técnicos e dados públicos registrados em blockchain) estão integralmente indicadas no texto e nas referências.

Este preprint foi submetido sob as seguintes condições:

- Os autores declaram que os necessários Termos de Consentimento Livre e Esclarecido de participantes ou pacientes na pesquisa foram obtidos e estão descritos no manuscrito, quando aplicável.
- Os autores declaram que a elaboração do manuscrito seguiu as normas éticas de comunicação científica.
- Os autores declaram que estão cientes que são os únicos responsáveis pelo conteúdo do preprint e que o depósito no SciELO Preprints não significa nenhum compromisso de parte do SciELO, exceto sua preservação e disseminação.
- Os autores declaram que os dados, aplicativos e outros conteúdos subjacentes ao manuscrito estão referenciados.
- O manuscrito depositado está no formato PDF.
- Os autores declaram que a pesquisa que deu origem ao manuscrito seguiu as boas práticas éticas e que as necessárias aprovações de comitês de ética de pesquisa, quando aplicável, estão descritas no manuscrito.
- Os autores declaram que uma vez que um manuscrito é postado no servidor SciELO Preprints, o mesmo só poderá ser retirado mediante pedido à Secretaria Editorial do SciELO Preprints, que afixará um aviso de retratação no seu lugar.
- Os autores concordam que o manuscrito aprovado será disponibilizado sob licença Creative Commons CC-BY.
- O autor submissor declara que as contribuições de todos os autores e declaração de conflito de interesses estão incluídas de maneira explícita e em seções específicas do manuscrito.
- Os autores declaram que o manuscrito não foi depositado e/ou disponibilizado previamente em outro servidor de preprints ou publicado em um periódico.
- Caso o manuscrito esteja em processo de avaliação ou sendo preparado para publicação mas ainda não publicado por um periódico, os autores declaram que receberam autorização do periódico para realizar este depósito.
- O autor submissor declara que todos os autores do manuscrito concordam com a submissão ao SciELO Preprints.