IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Artigo elaborado a partir de Mapeamento Sistemático da Literatura, versão final para entrega via SIGAA em template IEEE.

Digital Object Identifier

Mapeamento Forense para Identificação, Análise e Tratamento de Evidências de Criptomoedas Baseado em Blockchain

SHELTON BARBOSA OLIVEIRA[1], THAYS DHANDARAH R. SÁ[1]
[1]Universidade Federal do Sul e Sudeste do Pará – UNIFESSPA, Canaã dos Carajás, PA, Brasil
E-mails: shelton@unifesspa.edu.br; thays.dhandarah@unifesspa.edu.br

Orientadores: Profa. Dra. Fernanda Ferreira, Prof. Dr. Vitor de Souza Castro e Prof. Dr. Hugo Pereira Kuribayashi.

ABSTRACT Este artigo apresenta um Mapeamento Sistemático da Literatura sobre evidências digitais relacionadas a criptomoedas em blockchain, com foco em métodos, técnicas, ferramentas e desafios aplicados à identificação, rastreamento, análise, preservação e admissibilidade dessas evidências na perícia digital. A revisão foi conduzida com base no protocolo PRISMA 2020, contemplando as etapas de identificação, triagem, elegibilidade e inclusão dos estudos. As buscas foram realizadas nas bases Scopus e IEEE Xplore, resultando em 58 registros inicialmente identificados, dos quais 41 foram considerados elegíveis e 25 compuseram o corpus final da análise. Os resultados indicam convergência para abordagens híbridas, combinando análise de grafos, subgrafos, heurísticas de clusterização, *taint analysis*, aprendizado de máquina, redes neurais em grafos, análise temporal, visualização interativa, OSINT e procedimentos de preservação da prova digital. Entre as ferramentas e técnicas mais recorrentes destacam-se Neo4j, Dgraph, RevTrack, RevClassify, RevFilter, BitAnalysis, Dakar, Raphtory, Chainalysis, Crystal, AMLBot, *flow maps*, *wallet glyphs*, identificação de CoinJoin, *peeling chains*, heurística *multi-input* e detecção de *change address*. Também foram identificados desafios associados ao pseudonimato, mixers, movimentações multichain, ausência de dados rotulados, risco de falsos positivos, alto custo computacional, cadeia de custódia e admissibilidade jurídica. Conclui-se que a blockchain possui elevado potencial investigativo por registrar transações públicas e auditáveis, mas sua utilização como evidência exige métodos reproduzíveis, validação técnica, documentação adequada, preservação da integridade e correlação com dados externos.

INDEX TERMS Criptomoedas, blockchain, perícia forense, evidência digital, investigação digital, mapeamento sistemático da literatura.

I. INTRODUÇÃO

À medida que as criptomoedas e outros criptoativos ganham popularidade, uma mudança de paradigma mais ampla em torno da natureza das transações digitais surgiu através de transações descentralizadas e transfronteiriças na blockchain. Embora a tecnologia ofereça transparência, imutabilidade e o potencial para auditoria pública das transações, ela também é cada vez mais utilizada para atividades ilegais, incluindo lavagem de dinheiro, ransomware, fraude financeira, sextorsão, golpes de investimento, uso de mixers, CoinJoin e movimentações entre carteiras digitais. Nesse contexto, a blockchain é ambígua para análise forense porque, embora publique fluxos financeiros, impede a atribuição direta de endereços e carteiras a pessoas reais devido ao pseudonimato, fragmentação de transações e uso de métodos de obfuscação.

Dakar, RevTrack/RevClassify e análise de subgrafos e mixers têm sido usados para resolver os problemas trabalhando na classificação, rastreamento de fluxo e busca por tendências suspeitas, conforme relatado em trabalhos recentes [1]–[3].

Na investigação forense digital, o exame de evidências de criptomoedas consiste na identificação, preservação, correlação e interpretação de diferentes tipos de vestígios digitais: transações, endereços, carteiras, hashes, metadados, arquivos de artefatos, artefatos de software de carteira e fluxos de informação de e para entidades ou arquivos off-chain.

De acordo com a literatura, métodos de grafos, heurísticas de agrupamento, *taint analysis*, análise temporal, aprendizado de máquina, visualização de fluxo e coleta de OSINT têm sido usados na investigação de criptoativos. Sistemas como o BitAnalysis sugerem visualizações interativas para explorar carteiras de Bitcoin, e estudos encontram que programas como Electrum e Bitcoin Core recuperam artefatos úteis pela

memória dos processos do cliente Bitcoin [4], [5].

Embora esses avanços sejam significativos, ainda há uma lacuna considerável a ser preenchida no que diz respeito à conversão dos traços técnicos da blockchain em evidências digitais válidas e legalmente defensáveis. Este artigo explora a questão de quais métodos, técnicas e ferramentas foram desenvolvidos para detectar, mapear e analisar evidências digitais de criptomoedas na blockchain, juntamente com os desafios técnicos, forenses e legais que afetam sua preservação, rastreabilidade e aceitação, conforme destacado acima. Os principais desafios são o pseudonimato, o uso de mixers, movimento multichain, escassez de dados rotulados, o risco de falsos positivos, falta de padronização metodológica, cadeia de custódia e a necessidade de provar a confiabilidade dos métodos usados em tribunal. A pesquisa relacionada à admissibilidade, desanonimização e registro de evidências eletrônicas chama a atenção para a medida em que a veracidade da prova depende de sua autenticidade, integridade, documentação do processo, taxa de erro conhecida e auditabilidade [6], [7].

Há uma clara necessidade de organizar um campo de pesquisa recente, técnico e com validação, o que justifica o desenvolvimento deste Mapeamento Sistemático da Literatura. O trabalho traz valor adicional cientificamente nesta área, pois oferece uma visão geral das abordagens, ferramentas e lacunas existentes na literatura sobre criptoforense. Do ponto de vista técnico, essa abordagem apoia os investigadores, peritos e analistas na seleção das técnicas necessárias para a avaliação de transações, carteiras, movimentações de fundos e comportamentos suspeitos. Do ponto de vista social e legal, também é importante, pois a identificação e preservação adequadas de evidências digitais podem aprimorar as investigações criminais, reduzir incertezas probatórias e impulsionar a implementação de procedimentos mais transparentes, reprodutíveis e auditáveis. Em artigos sobre os regimes de prova eletrônica e gestão de evidências digitais com blockchain, também são necessários protocolos padronizados para coleta, preservação e análise [8], [9].

O objetivo deste artigo é mapear sistematicamente a literatura científica sobre métodos, técnicas, ferramentas e desafios na descoberta, análise e gestão de evidências digitais de criptomoedas em blockchain no âmbito da perícia forense digital. Um conjunto de objetivos específicos inclui a seleção das técnicas de rastreamento e análise mais prevalentes; ferramentas e técnicas de coleta de informações empregadas em investigações de criptoativos; categorização das evidências digitais analisadas; discussão de questões técnicas em torno do pseudonimato, mixers, CoinJoin, moedas focadas em privacidade e movimentos através de múltiplos blockchains; além de discutir preocupações forenses e legais em relação à preservação, cadeia de custódia, validação de abordagens metodológicas e aceitação de evidências digitais.

Assim sendo, este Mapeamento Sistemático da Literatura é orientado pelas seguintes questões de pesquisa:

QP1: Que métodos, técnicas e ferramentas são utilizados para identificar, mapear e analisar evidências digitais de criptomoedas em blockchain?

QP2: Quais desafios técnicos, forenses e jurídicos envolvem o tratamento, a preservação, a rastreabilidade e a admissibilidade dessas evidências digitais?

Esse mapeamento ajudará a entender melhor não apenas a possibilidade de investigar na blockchain, mas também as limitações que impedem que seus registros sejam usados como evidência em investigações forenses e judiciais. Portanto, o estudo visa propor uma inter-relação mais abrangente entre análise técnica, metodologia forense e a validade legal de evidências digitais para investigação de criptoativos.

II. METODOLOGIA

Este trabalho foi realizado como um Mapeamento Sistemático da Literatura (MSL) para identificar, estruturar e avaliar estudos científicos em relação à identificação, análise e tratamento de evidências digitais de criptomoedas operando em blockchain. O protocolo PRISMA 2020 orientou o processo de revisão, delineando as etapas de identificação, triagem, elegibilidade e inclusão de estudos. Com base no resumo da pesquisa, o corpus final consistiu em 25 artigos selecionados, principalmente das bases de dados Scopus e IEEE Xplore.

A. ESTRATÉGIA DE BUSCA

A estratégia de busca foi estabelecida de acordo com as questões de pesquisa do estudo, optando por focar em estudos relacionados à perícia forense digital, evidências digitais, rastreamento de transações, análise de carteiras, lavagem de dinheiro, fraude e investigação de criptoativos em blockchains. As bases de dados Scopus e IEEE Xplore foram selecionadas para as buscas, pois possuem ampla cobertura de publicações científicas em Ciência da Computação, Segurança da Informação, Engenharia, Blockchain e Perícia Digital.

O idioma utilizado foi o inglês, já que a maioria das publicações relevantes para o tema eram internacionais. O método envolveu uma combinação de terminologia relacionada a criptomoedas, blockchain e análise forense. As strings de busca foram estruturadas como grupos temáticos:

Grupo 1: criptoativos

cryptocurrency OR crypto assets OR virtual currency OR bitcoin OR blockchain

Grupo 2: perícia e evidência digital

digital forensics OR forensic analysis OR digital evidence OR electronic evidence OR blockchain forensics

Grupo 3: rastreamento e investigação

transaction tracing OR wallet investigation OR address clustering OR taint analysis OR money laundering OR ransomware OR fraud detection

A partir desses grupos, foram utilizadas combinações como:

cryptocurrency AND blockchain AND digital forensics
blockchain AND forensic analysis AND digital evidence
bitcoin AND transaction tracing AND money laundering
crypto assets AND wallet investigation AND forensic evidence

blockchain forensics AND evidence admissibility

Em geral, os filtros foram configurados para filtrar documentos com relevância em Ciência da Computação, Segurança da Informação, Engenharia, Ciências da Decisão e domínios relacionados. Artigos de revistas e artigos de conferências também foram utilizados para a pesquisa, com preferência por documentos completos e de acesso aberto para garantir uma cobertura abrangente. O período de tempo foi estabelecido cobrindo publicações de 2017 a 2026, com a maioria das pesquisas realizadas recentemente no período de 2024 a 2026, quando as técnicas de análise de blockchain, mixers, fraudes em criptomoedas e ferramentas forenses estão mudando continuamente.

B. CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Após a busca, os critérios de inclusão e exclusão foram construídos de forma que os artigos incluídos tivessem uma relevância direta para o objetivo do MSL. Foram considerados artigos que discutem métodos, técnicas, ferramentas ou desafios da investigação de criptomoedas e evidências digitais em blockchain.

Foram adotados como **critérios de inclusão**:

a) artigos publicados entre 2017 e 2026;
b) estudos escritos em inglês;
c) artigos científicos completos, publicados em periódicos ou anais de conferências;
d) trabalhos relacionados à investigação digital, rastreamento de transações, AML, ransomware, fraudes, mixers, carteiras digitais ou evidências eletrônicas;
e) estudos que apresentassem métodos aplicáveis à perícia, como análise de grafos, heurísticas, aprendizado de máquina, OSINT, taint analysis, visualização, análise de memória, preservação ou admissibilidade de evidências.

Foram definidos como **critérios de exclusão**:

a) estudos sobre blockchain sem relação direta com evidências digitais ou investigação de criptoativos;
b) artigos focados apenas em previsão de preço, volatilidade, mercado financeiro ou sentimento de investidores;
c) publicações sem texto completo disponível;
d) documentos duplicados entre as bases;
e) trabalhos voltados a aplicações de blockchain fora do recorte forense, como agricultura, saúde, DRM, smartphones, DAOs ou aplicações genéricas sem vínculo com investigação digital;
f) estudos sem contribuição clara para responder às questões de pesquisa.

Portanto, esse processo foi necessário para garantir que o corpus não fosse inflado com trabalhos que apenas utilizavam a tecnologia blockchain como infraestrutura tecnológica, sem qualquer relação com perícia, evidência digital ou a investigação de crimes envolvendo criptomoedas.

C. PROCESSO DE SELEÇÃO

Usando o funil metodológico fornecido pelo PRISMA 2020, os estudos foram escolhidos de acordo com as fases descritas no guia, os registros foram coletados de bases de dados científicas, que foram triados por títulos e resumos, artigos considerados potencialmente relevantes foram analisados quanto à elegibilidade, e apenas os estudos que melhor se adequavam às questões de pesquisa foram selecionados.

Com base nas fontes consultadas, foram identificados 58 registros. Após a remoção de duplicatas e a aplicação de critérios de triagem preliminares, 41 artigos estavam disponíveis para análise posterior. Para isso, os artigos foram triados por título, resumo, palavras-chave e referências ao tema forense. Em seguida, foi realizada uma leitura técnica focada e uma leitura completa das obras mais relevantes para avaliar suas contribuições para metodologias, ferramentas, evidências e desafios. Vinte e cinco artigos foram selecionados para servir como o corpus central do Mapeamento Sistemático da Literatura, e 16 foram classificados como não centrais ou de menor suporte.

O processo de seleção pode ser descrito da seguinte forma:

Identificação: busca nas bases Scopus e IEEE Xplore, resultando em 58 registros iniciais.

Triagem: análise de título, resumo e palavras-chave, com exclusão de duplicados e estudos fora do recorte.

Elegibilidade: avaliação dos artigos completos ou parcialmente completos, verificando aderência à perícia forense digital e à análise de evidências de criptomoedas.

Inclusão: seleção final de 25 artigos diretamente relacionados às questões de pesquisa.

A Figura 1 apresenta o fluxograma do processo de seleção dos estudos, conforme a lógica do protocolo PRISMA 2020, destacando os registros inicialmente identificados, os estudos triados, os trabalhos excluídos e o corpus final incluído neste MSL.

Essa organização permitiu preservar a rastreabilidade do processo de seleção e reduzir o risco de escolhas arbitrárias, garantindo maior transparência metodológica ao MSL.

D. APOIO COMPUTACIONAL E VALIDAÇÃO DOS DADOS

Durante a etapa final de organização do Mapeamento Sistemático da Literatura, foi utilizado apoio de inteligência artificial generativa para auxiliar na sistematização das informações, estruturação do protocolo PRISMA 2020, revisão textual, padronização do manuscrito e organização dos dados extraídos dos estudos. Esse apoio teve caráter instrumental, atuando como recurso de apoio à organização, síntese e clareza textual, sem substituir a análise crítica dos autores.

A aplicação dos critérios de inclusão e exclusão, a seleção final dos estudos, a interpretação dos resultados, a categorização temática e a validação final das informações permaneceram sob responsabilidade dos autores. Dessa forma, o uso da ferramenta contribuiu para a melhoria da apresentação metodológica e textual do artigo, enquanto as decisões científicas, analíticas e interpretativas foram conduzidas e conferidas pelos pesquisadores.

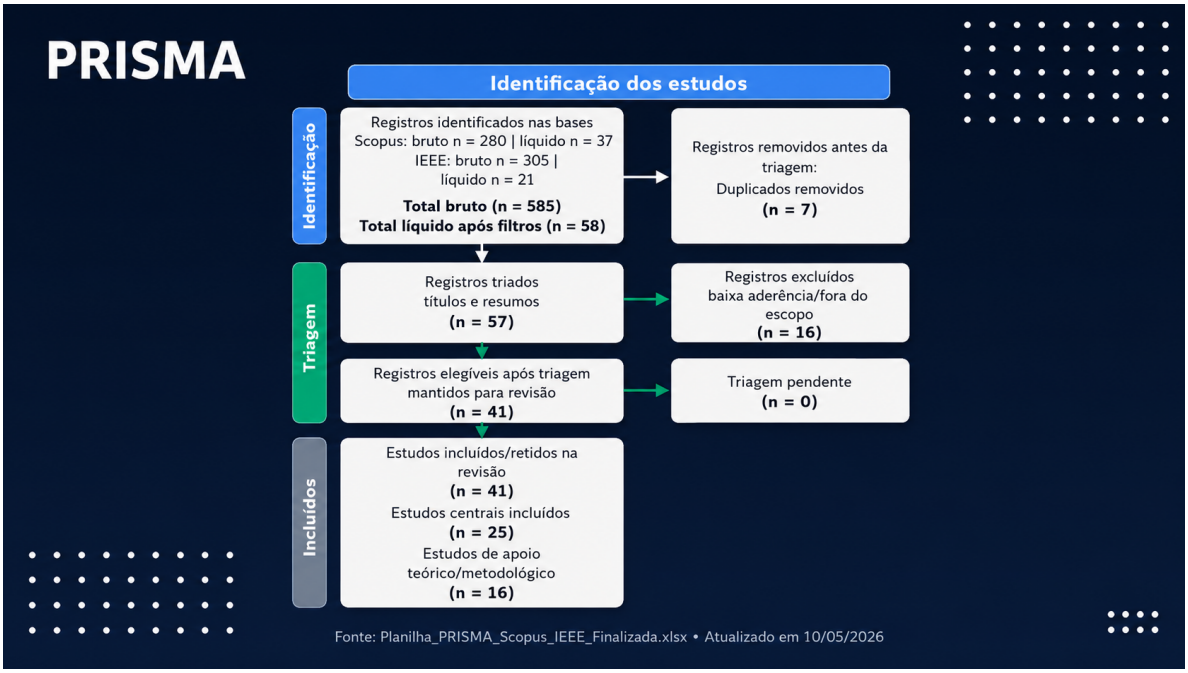

FIGURE 1. **Fluxograma do processo de seleção dos estudos com base no protocolo PRISMA 2020.**

E. EXTRAÇÃO E ANÁLISE DE DADOS

Uma vez estabelecido o corpus final, foi realizada uma extração sistemática dos componentes relevantes de cada artigo. A extração focou-se em diferenciar na pesquisa QP1, que eram métodos, técnicas e ferramentas, e QP2, que eram desafios técnicos, forenses e legais de evidências digitais no campo da blockchain. Os extratos de cada estudo foram os seguintes:

Identificação do artigo: título, autores, ano de publicação, base de dados e tipo de publicação.

Método/técnica aplicada: análise de grafos, subgrafos, heurísticas de agrupamento, *taint analysis*, ML, redes neurais de grafos, OSINT, análise temporal, análise de memória, visualização ou preservação de evidências.

Tipo de evidência examinada: transações, endereços, carteiras, clusters, NFTs, hashes, logs, metadados, artefatos de software de carteira e fluxos financeiros.

Ferramentas referenciadas ou sugeridas: BitAnalysis, Dakar, RevTrack, RevClassify, Chainalysis, Elliptic, BlockSci, Neo4j, Dgraph, scrapers, parsers, sistemas de visualização.

Desafios identificados: pseudonimato, mixers, CoinJoin, moedas de privacidade, movimentos multichain, escassez de dados rotulados, falsos positivos, cadeia de custódia, preservação, validação técnica e admissibilidade legal.

Relevância para as questões de pesquisa: categorização do artigo como respondendo a QP1, QP2 ou ambos.

Este mapeamento foi categorizado de acordo com um eixo temático. Os artigos foram classificados em quatro categorias principais: 1. Análise de grafos e transações: isso inclui estudos que cobrem o uso de grafos, subgrafos, ciclos, redes temporais, grafos de carteiras e mapas de fluxo para estudar ou entender os movimentos na blockchain. 2. Fraude, lavagem de dinheiro e crimes digitais: ransomware, sextorsão, HYIP, phishing de aprovação, golpes, AML, cash-out e movimentos suspeitos. 3. Ferramentas, coleta e visualização: trabalhos que recomendam ou analisam ferramentas, incluindo BitAnalysis, Dakar, scrapers, parsers, dashboards e métodos de análise de carteiras. 4. Preservação, cadeia de custódia e admissibilidade: a pesquisa sobre a validade de evidências digitais, documentação de procedimentos, integridade, autenticidade, taxa de erro, confiabilidade dos métodos e aceitação judicial.

Os dados foram revisados qualitativa e descritivamente, refletindo a descoberta de temas recorrentes, similaridades na metodologia, lacunas de pesquisa, limitações mencionadas pelos autores. Assim, os artigos estão diretamente ligados às questões de pesquisa, o que nos permitiu encontrar os métodos e ferramentas mais visíveis na área, bem como os desafios que ainda dificultam a utilização de registros de blockchain como evidência digital em investigações forenses.

III. RESULTADOS

Esta seção destaca os resultados da Revisão Sistemática de Mapeamento da Literatura. Os dados foram apresentados em duas partes: análise quantitativa para observar a distribuição por base de dados, período e estágio de seleção dos estudos, e análise temática para categorizar as contribuições dos estudos em relação às questões de pesquisa. Esta última compreendeu 25 estudos principais, sendo os estudos escolhidos com base na concordância com os temas relacionados a evidências digitais de criptomoedas em blockchain, técnicas de análise forense, ferramentas de investigação, desafios na preservação, rastreabilidade e admissibilidade.

TABLE 1. Síntese do processo de seleção

Etapa do processo	Qtd	Descrição
Registros identificados	58	Total inicial obtido nas buscas em bases científicas
Artigos elegíveis	41	Estudos mantidos após triagem por título, resumo e aderência temática
Corpus central	25	Artigos efetivamente analisados no MSL
Estudos não centrais / apoio menor	16	Trabalhos com baixa aderência ou contribuição complementar

TABLE 2. Distribuição dos artigos por base

Base	Qtd	Característica predominante
Scopus	18	Estudos aplicados recentes, AML, mixers, preservação, admissibilidade e frameworks
IEEE Xplore	7	Ferramentas técnicas, segurança, visualização, análise de carteiras e modelos computacionais
Total	**25**	Corpus final do MSL

A. RESULTADOS QUANTITATIVOS

Para este propósito, 58 registros foram inicialmente recuperados dos registros de busca obtidos usando bancos de dados pesquisados durante o processo de seleção. Seguindo os critérios de seleção que foram impostos após a exclusão da triagem anterior (ou seja, excluindo estudos não incluídos e que cumprem com o quadro forense e avaliação e garantindo os seguintes critérios de exclusão), 41 artigos foram considerados elegíveis. Destes, a amostra de revisão: 25 artigos foram o corpus central desses estudos e 16 estudos foram considerados não centrais ou de apoio menor (Tabela 1).

Por exemplo, a distribuição de artigos indica que o Scopus tinha 18 artigos; depois disso, o IEEE Xplore tinha 7 artigos. Dito isso, essa diferença mostra que o Scopus apresenta uma coleção mais robusta de estudos aplicados sobre criptoforense, lavagem de dinheiro, mixers, preservação de evidências e admissibilidade, enquanto o IEEE continha uma forte proporção de literatura técnica sobre ferramentas, visualização, segurança, análise de carteiras e modelos computacionais.

A distribuição temporal mostrou uma alta concentração de novos estudos em pesquisas recentes. Dos 25 estudos selecionados, 21 foram publicados entre 2024 e 2026, enquanto 4 pertencem ao período de 2017 a 2023. Isso indica que o tema é muito dinâmico e está mudando rapidamente devido ao aumento de crimes relacionados a criptomoedas, mistura, proliferação multichain, popularização de NFTs, ferramentas forenses e o debate sobre a admissibilidade forense de evidências digitais.

O IEEE Xplore também demonstrou que o refinamento progressivo foi necessário de acordo com o processo de busca. Uma das strings de busca retornou 364 resultados da busca extensiva, que posteriormente foram filtrados para 26 por tipo de documento, período e acesso aberto. Em uma string semelhante baseada em termos como forense de criptomoeda, forense de criptoativos, forense de blockchain e forense de ativos virtuais, foram obtidos 34 resultados, que finalmente foram filtrados para 5 resultados em revistas de acesso aberto. Esses achados corroboram a noção de que a primeira busca geralmente retorna numerosos estudos que são semanticamente próximos, mas nem todos estão diretamente relacionados ao escopo forense do MSL.

TABLE 3. Distribuição temporal dos estudos selecionados

Período	Qtd	Interpretação
2017–2023	4	Base conceitual e metodológica inicial
2024–2026	21	Produção recente, com foco em técnicas avançadas e desafios atuais
Total	**25**	Corpus final analisado

A partir de uma classificação dos 25 artigos, também foi possível ver a relação de cada um dos estudos com as questões de pesquisa. Alguns dos artigos aplicaram principalmente os métodos, técnicas e ferramentas para a RQ1. Uma seção respondeu à RQ2 abordando desafios técnicos, cadeia de custódia, validação, preservação e admissibilidade. E vários responderam a ambas as perguntas ao mesmo tempo, particularmente aqueles que ofereceram uma explicação técnica, bem como uma discussão sobre a confiabilidade dos resultados.

B. ANÁLISE TEMÁTICA

A análise temática revelou que os estudos incluídos estão agrupados em quatro áreas principais: análise de grafos e transações, fraude, golpes e lavagem de dinheiro, ferramentas, coleta e visualização, e preservação, cadeia de custódia e admissibilidade. Essas áreas foram definidas com base nas contribuições dos artigos para as questões de pesquisa e nos tipos de evidências, métodos e desafios recorrentes identificados na literatura.

A análise de grafos e transações foi o primeiro foco e um dos mais comuns. Os autores demonstram que um blockchain pode ser descrito como uma espécie de rede de nós e arestas, com os nós atuando como endereços, carteiras, transações ou entidades, e as arestas representando fluxos de valor. Este método pode ser usado para mapear relações entre carteiras, comunidades, subgrafos suspeitos, ciclos temporais e estruturas de lavagem de dinheiro. Projetos de pesquisa como o RevTrack, por exemplo, tratam a lavagem de dinheiro como subgrafos dentro da blockchain, utilizando aprendizado de máquina e redes neurais em gráficos para classificar estruturas como legítimas ou suspeitas.

O segundo foco, fraudes, golpes e lavagem de dinheiro, reuniu artigos relacionados a crimes digitais e financeiros que utilizam criptoativos como meio de movimentar ou esconder valores. Neste grupo, aparecem estudos sobre ransomware, sextorsão, HYIP, phishing de aprovação, wash trading em NFTs, mixers, CoinJoin, cash-out e carteiras ilícitas. A literatura mostra que analisar uma única transação raramente

TABLE 4. Exemplos de refinamento das buscas na IEEE Xplore

String / estratégia	Resultado bruto	Resultado após filtros	Observação
String ampla sobre cryptocurrency, blockchain e forensic/evidence/investigation	364	26	Redução após filtros de tipo, período e acesso aberto
String específica sobre cryptocurrency forensics / blockchain forensics	34	5	Redução com foco em periódicos e acesso aberto

TABLE 5. Relação geral dos artigos com as questões de pesquisa

Relação com as questões	Característica
QP1	Estudos sobre grafos, heurísticas, ferramentas, ML/IA, OSINT, visualização e análise de carteiras
QP2	Estudos sobre pseudonimato, mixers, preservação, cadeia de custódia, admissibilidade, confiabilidade e taxa de erro
QP1 + QP2	Estudos que apresentam técnica de análise e também discutem limitações, rastreabilidade ou validade forense

é suficiente para caracterizar um comportamento suspeito. Em muitos casos, as evidências aparecem no conjunto de movimentos, na sequência temporal, na repetição de padrões, na passagem por serviços intermediários ou na combinação de dados on-chain e informações off-chain.

O terceiro eixo, ferramentas, coleta e visualização, consolidou estudos que recomendam ou estudam ferramentas para tornar a investigação mais viável. BitAnalysis, por exemplo, transforma dados brutos de blockchain em visualizações de carteiras, conexões, fluxos de Bitcoin e padrões temporais para investigadores. Dakar, no entanto, descreve uma ferramenta forense, que pode analisar CoinJoin em blockchains UTXO utilizando bancos de dados grafos, classificando transações e visualizando o fluxo de mistura. Além disso, o corpus também consiste em ferramentas e processos como BlockSci, Chainalysis, Elliptic, Crystal, AMLBot, scrapers, parsers, dashboards, análise de memória e bancos de dados grafos.

O quarto eixo, preservação, cadeia de custódia e admissibilidade, respondeu mais diretamente à segunda questão de pesquisa. A pesquisa neste grupo também destaca que a prova da blockchain, embora pública e auditável, não necessariamente a torna uma evidência válida. Para que os registros tenham valor probatório, é necessário garantir a autenticidade, integridade, rastreabilidade do procedimento, documentação adequada, controle de acesso, preservação de metadados e a possibilidade de auditoria. O registro de evidências eletrônicas em crimes relacionados a criptomoedas, segundo estudos, cópias bit a bit, hashing, arquivamento, registro cronológico de transações, proteção de frases-semente e o envolvimento de especialistas são medidas para aumentar a admissibilidade das evidências.

Em relação ao QP1, os métodos mais recorrentes foram análise de grafos, grafos temporais, subgrafos, heurísticas de agrupamento, *multi-input*, *change address*, *taint analysis*, análise temporal, aprendizado de máquina, redes neurais de grafos, visualização de fluxo, OSINT e análise de artefatos de carteira. Entre as ferramentas e ambientes mencionados, destacam-se BitAnalysis, Dakar, RevTrack, RevClassify, RevFilter, BlockSci, Chainalysis, Elliptic, CipherTrace, Crystal, AMLBot, Neo4j, Dgraph, scrapers e parsers.

Para o QP2, os desafios comuns são o pseudonimato, a ofuscação por mixers e CoinJoin, o uso de moedas de privacidade, movimentos cross-chain e multichain, falta de dados rotulados, dificuldade de validação, potencial para falsos positivos, alto custo computacional, dependência de ferramentas proprietárias, necessidade de métodos explicáveis e exigência de cadeia de custódia. A literatura também menciona que endereços e carteiras não representam pessoas diretamente, mas requerem correlação com dados externos, registros de câmbio, KYC/CDD, metadados de comunicação, OSINT ou evidências obtidas de dispositivos.

Também identificou uma tendência clara para abordagens híbridas na análise temática do estudo. A maioria dos estudos recentes combina gráficos, heurísticas, aprendizado de máquina, visualização e fontes externas de informação. É uma combinação útil, pois cada técnica cobre apenas parte do problema, gráficos funcionam para representar fluxos, heurísticas permitem inferências práticas, aprendizado de máquina apoia a detecção em escala, visualizações tornam os achados compreensíveis e dados fora da cadeia ajudam a vincular endereços a identidades ou entidades reais.

De acordo com a pesquisa, os resultados mostram que a investigação forense de criptomoedas é guiada por uma cadeia analítica composta por quatro etapas: coleta, mapeamento, interpretação e preservação. Os dados são primeiro coletados de blockchains, carteiras, exploradores, ferramentas OSINT ou dispositivos. Em seguida, são organizados em gráficos, tabelas, fluxos ou subgráficos. Isso é então interpretado por meio de métodos técnicos, heurísticas, classificadores ou análise visual. Finalmente, deve ser preservado com documentação, hashing, registro cronológico, cadeia de custódia e validação por especialistas.

No geral, no entanto, as descobertas mostram que, embora a blockchain possa oferecer um grande potencial investigativo através do registro de transações públicas e auditáveis, esse potencial não está isento de desafios forenses. As evidências na blockchain precisam ser tratadas com cautela, pois o pseudonimato, as técnicas de ofuscação, a escala de dados, a falta de padronização e muitos outros fatores tendem a minar inferências precipitadas. A literatura, portanto, converge para

TABLE 6. Eixos temáticos identificados no corpus

Eixo temático	Descrição	Relação com as QPs
Análise de grafos e transações	Estudo de fluxos, subgrafos, ciclos, carteiras, NFTs, padrões temporais e redes transacionais	QP1
Fraudes, scams e lavagem de dinheiro	HYIP, ransomware, sextortion, approval phishing, mixers, AML e cash-out	QP1 + QP2
Ferramentas, coleta e visualização	BitAnalysis, Dakar, RevTrack, scrapers, parsers, dashboards e análise de memória	QP1
Preservação e admissibilidade	Cadeia de custódia, hashing, integridade, taxa de erro, validação e aceitação judicial	QP2

TABLE 7. Principais métodos e ferramentas identificados para a QP1

Categoria	Métodos, técnicas ou ferramentas
Grafos e redes	Grafos transacionais, grafos temporais, subgrafos, ciclos, motifs, wallet graphs e flow maps
Heurísticas	Multi-input, change address, clustering, taint analysis, hops, peeling chains e regras de mistura
ML / IA	Classificação, detecção de anomalias, GNNs, seleção de atributos, multiagentes e detecção precoce
Visualização	BitAnalysis, dashboards, flow maps, connection diagrams e wallet glyphs
Ferramentas forenses	Dakar, RevTrack, RevClassify, RevFilter, Chainalysis, Elliptic, CipherTrace, Crystal e AMLBot
Coleta e apoio	OSINT, web scraping, parsers, BlockSci, btc-csv, Neo4j e Dgraph
Artefatos digitais	Análise de carteiras, memória de clientes Bitcoin, hashes, logs e metadados

TABLE 8. Principais desafios identificados para a QP2

Desafio	Efeito na prova digital
Pseudonimato	Endereços e carteiras não identificam automaticamente pessoas
Ofuscação	Mixers, CoinJoin, bridges, DeFi, privacy coins e multichain dificultam rastreabilidade
Validação	Falta de ground truth, taxa de erro desconhecida e risco de falsos positivos
Escalabilidade	Grande volume de transações exige automação, grafos e ferramentas especializadas
Interpretabilidade	Modelos complexos podem ser difíceis de explicar em contexto pericial
Preservação	Exige hash, cópia íntegra, documentação, metadados e cadeia de custódia
Admissibilidade	Requer método confiável, auditável, reproduzível e juridicamente defensável
Correlação off-chain	Necessidade de vincular dados on-chain a registros externos, VASPs, dispositivos ou OSINT

a exigência de métodos reprodutíveis, explicáveis, documentados e validação humana quando os resultados técnicos são aplicados em processos judiciais.

IV. DISCUSSÃO

Este mapeamento sistemático da literatura sugere que a investigação forense de criptoativos em blockchain depende, entre outras abordagens, de vários tipos de métodos técnicos, ferramentas computacionais e processos legais-forenses. Em relação ao QP1, uma esmagadora maioria das abordagens foi baseada em gráficos, heurísticas, análise temporal, aprendizado de máquina, visualização de fluxo, OSINT e análise de artefatos de carteira. Do QP2, os estudos destacam dificuldades comuns ligadas ao pseudonimato, uso de mixers, CoinJoin, pontes, movimentos multichain, falta de dados rotulados, risco de falsos positivos, cadeia de custódia, validação técnica e admissibilidade de evidências digitais. Assim, a literatura examinada converge em torno de uma ideia, a blockchain fornece rastros públicos e auditáveis; mas, tais rastros não podem se transformar em evidências forenses válidas.

No QP1, os métodos mais bem documentados são aqueles que modelam o blockchain como uma rede de relacionamentos. A análise de grafos permite o mapeamento de endereços, carteiras, transações, entidades, fluxos e subgrafos suspeitos para revelar padrões complexos que seriam difíceis de ler manualmente. A maturidade técnica neste ponto, como a capacidade do BitAnalysis e do Dakar de transformar dados brutos em visualizações, clusters, mapas de fluxo e classificações de transações CoinJoin, é um exemplo primordial. Ferramentas como RevTrack, RevClassify e RevFilter sugerem uma evolução em direção a modelos automatizados capazes de detectar subgrafos suspeitos em grande escala. Esses trabalhos respondem fortemente à primeira questão de pesquisa, porque mostram como a literatura propôs mecanismos para descobrir, mapear e analisar evidências digitais na blockchain.

Em relação à resposta QP1, também é evidente que não existe um método único capaz de resolver o problema investigativo de ponta a ponta. Heurísticas simples, como múltiplas entradas, *change address*, *peeling chains* e *taint analysis* são boas, mas dependem de suposições sobre o comportamento do usuário e a operação da carteira. Modelos de aprendizado de máquina e redes neurais em grafos fornecem novas fontes para detecção, mas utilizam grandes bases de dados, alto poder computacional e requerem validação humana. Ferramentas de visualização tornam os resultados mais interpretáveis, mas não garantem de forma independente a identidade real dos envolvidos. Como resultado, os métodos identificados funcionam melhor quando combinados em

uma abordagem híbrida, com análise on-chain, validação off-chain, interpretação especializada e documentação técnica trabalhando juntas.

A literatura nos diz que o maior desafio no QP2 não é apenas encontrar a trilha, mas convertê-la em evidências confiáveis. A blockchain permite a verificação de transações, hashes, endereços e fluxos, mas o pseudonimato impede a conexão automática entre uma carteira e uma pessoa ou entidade legal. Além disso, a utilização de metodologias de ofuscação, incluindo mixers, CoinJoin, moedas de privacidade, pontes e movimentos entre cadeias, reduz a capacidade de rastrear trilhas. Pesquisas sobre mixers também demonstram que, quando há transações públicas, a entrada e a saída podem ser propositalmente e deliberadamente embaralhadas, exigindo análise de valor, tempo, gráficos, transações de teste e correlação com dados externos.

A preservação e a admissibilidade aparecem como uma das áreas mais sensíveis do corpus. O estudo das provas eletrônicas sob regimes de combate à lavagem de dinheiro enfatiza que as provas devem manter autenticidade, validade e integridade. A pesquisa sobre como as provas eletrônicas podem ser registradas em crimes envolvendo criptomoedas foca na cópia bit a bit, geração de hash, arquivamento, registro cronológico de transações, preservação de metadados, proteção de frases-semente e o envolvimento de peritos. Essas investigações revelam que a robustez das provas depende tanto do método de análise quanto de como a coleta e a preservação são documentadas.

Uma grande lacuna na literatura é a ausência de padronização dos métodos. Numerosos trabalhos também sugerem ferramentas, modelos ou frameworks específicos, mas nem sempre apresentam protocolos completos para a coleta, validação, preservação e apresentação de evidências. Nesse sentido, há uma barreira entre a dimensão técnica e a dimensão legal-probatória. Em outras palavras, parte da literatura foca na detecção e rastreamento, enquanto outra parte discute a admissibilidade e a cadeia de custódia, mas ainda há poucos trabalhos que integram todo o ciclo forense: identificação, coleta, análise, preservação, validação, documentação e apresentação em tribunal.

Outra lacuna é a limitada abundância de conjuntos de dados rotulados ou verdadeiros. Numerosos modelos dependem de dados previamente reconhecidos como legais ou ilegais, mas no contexto da blockchain, confirmar a natureza criminosa de uma transação nem sempre é uma tarefa fácil. Isso pode impactar particularmente os métodos de aprendizado supervisionado, detecção de anomalias e classificação de carteiras. De acordo com a literatura, conjuntos de dados desequilibrados podem produzir métricas enganosas, já que transações ilícitas representam uma fração do volume total. Assim, um modelo que é excelente em precisão geral pode falhar nos casos mais importantes para uma investigação específica, precisamente.

E também havia inconsistências sobre o papel das heurísticas. Enquanto alguns estudos consideram regras que incluem múltiplas entradas e mudança de endereço como recursos críticos para agrupamento e desanonimização, outros destacam associações com potenciais, particularmente em casos com CoinJoin, mixers ou carteiras modernas. Essa tensão é significativa, as heurísticas são úteis porque são interpretáveis e práticas, mas também resultam em conclusões frágeis na ausência de validação complementar. Para fins forenses, deve-se ter cautela ao redigir relatórios, evitando afirmar identidade ou controle de carteira com base apenas em inferências probabilísticas.

No que diz respeito à maturidade científica, é perceptível que algumas áreas estão mais desenvolvidas. A análise de grafos, visualização de transações de Bitcoin, detecção de mixers e a identificação de padrões de lavagem de dinheiro demonstram uma maior consolidação metodológica. Os tópicos possuem suas próprias ferramentas específicas, estudos empíricos, modelos computacionais e métricas de avaliação. Em contraste, áreas como admissibilidade legal, padronização internacional, análise multichain, preservação de evidências em ambientes DeFi e a vinculação de dados on-chain com identidades reais mostram menos maturidade. Nesses domínios, os trabalhos tendem a ser mais conceituais, exploratórios ou dependentes de contextos nacionais específicos.

Das novas tendências que surgem com base em diferentes estratégias, a dos grafos temporais se destaca. Vários estudos sobre NFTs e atividades suspeitas mostraram que a ordem, frequência e ritmo das transações podem revelar padrões que não aparecem em grafos estáticos. Essa tendência é relevante, muitos crimes digitais não ocorrem em uma única transferência isolada, mas sim através de sequências repetidas, ciclos, movimentos coordenados e mudanças temporais no comportamento das carteiras. Assim, o tempo é tratado como uma dimensão nas evidências digitais.

Aprendizado de máquina, redes neurais em grafos ou modelos híbridos e a abordagem cada vez mais utilizada é outra tendência importante. Eles melhoram significativamente o estudo de blockchains em larga escala, onde a leitura manual se torna inviável. Mas o risco de que esses modelos possam ser potencialmente altamente interpretáveis também é trazido por essas abordagens, baixa interpretabilidade, dependência de dados rotulados, risco de viés, dificuldade em relação à auditoria e necessidade de validação humana. No contexto forense, modelos automatizados devem ser vistos como ferramentas de triagem e apoio, não simplesmente como alternativas à análise altamente especializada.

A pesquisa também destaca a crescente correlação entre dados on-chain e off-chain. A identificação de endereços e fluxos na blockchain raramente é suficiente para atribuir responsabilidade a uma pessoa. Consequentemente, investigações mais robustas combinam registros de blockchain disponíveis publicamente com informações de exchanges, KYC/CDD, VASPs, OSINT, metadados de comunicação, artefatos de dispositivos, memória do cliente Bitcoin e registros de infraestrutura. Essa integração é promissora, mas levanta questões sobre cadeia de custódia, jurisdição, privacidade e documentação.

Os riscos de cada método identificado são categorizados

em quatro grandes dimensões. Existe o risco técnico na forma primária, que envolve alto volume de dados, ferramentas desatualizadas e uma incompatibilidade com novas estruturas de transação, bem como limitações computacionais. O segundo é o risco analítico, relacionado a falsos positivos, heurísticas frágeis, falta de rótulos confiáveis e inferências excessivas. O risco legal, relacionado à coleta irregular, falta de documentação e violação da cadeia de custódia, dificuldade em demonstrar autenticidade e integridade, é o terceiro. O quarto é o risco em nível operacional, que está enraizado na dependência de ferramentas proprietárias, cooperação internacional lenta, perda de registros por VASPs e a necessidade de especialistas altamente qualificados.

À luz desses riscos, as descobertas sugerem que os métodos dos especialistas em blockchain precisarão adotar uma abordagem metodologicamente conservadora. A presença de uma carteira em um fluxo suspeito, por si só, não transmite conclusivamente a impressão de autoria criminosa. O fato de uma transação passar por um mixer não prova que seja ilegal. Da mesma forma, um modelo de aprendizado de máquina que classifica um determinado subgrafo como suspeito deve ser interpretado, explicado e validado. As evidências em blockchain são robustas com um método reprodutível, documentação completa, preservação adequada, validação técnica e correlação com outras fontes.

Consequentemente, a discussão geral sobre o corpus indica que a perícia em criptomoedas está amadurecendo. Há avanços significativos em ferramentas, gráficos, detecção automatizada, visualização e análise temporal. No entanto, ainda existem lacunas na padronização, integração entre técnica e lei, avaliação de erros, explicabilidade de modelos e admissibilidade judicial. A principal contribuição deste MSL é destacar que a investigação de criptomoedas em blockchain não deve permanecer apenas como um rastreamento financeiro, mas sim um processo forense abrangente, onde a qualidade das evidências depende da interação entre a tecnologia, método, documentação e validade legal.

V. CONSIDERAÇÕES FINAIS

Este Mapeamento Sistemático da Literatura foi realizado para identificar, organizar e analisar estudos científicos relacionados à identificação, mapeamento, análise e tratamento de evidências digitais de criptomoedas em blockchain, com foco na perícia forense digital. A partir da seleção e análise dos artigos, foi possível verificar que esse objetivo foi alcançado, pois o estudo permitiu a coleta de métodos, técnicas, ferramentas e desafios recorrentes na literatura, relacionando-os diretamente às duas questões de pesquisa propostas.

A primeira questão de pesquisa mostrou que a literatura possui muitas maneiras de encontrar, mapear e analisar evidências digitais em blockchain. Além disso, alguns dos métodos comuns são análise de grafos, subgrafos, grafos temporais, heurísticas de agrupamento, *taint analysis*, análise de fluxo, aprendizado de máquina, redes neurais em grafos, OSINT, visualização interativa e análise de artefatos de carteiras. Ferramentas e frameworks: BitAnalysis, Dakar, RevTrack, RevClassify, RevFilter, Neo4j, Dgraph, Chainalysis, Crystal, AMLBot e exploradores de blockchain tornam-se essenciais na conversão de transações, endereços, carteiras e fluxos em entidades investigáveis.

Para o estudo sobre a segunda questão de pesquisa, as principais questões técnicas, forenses e legais destacadas por meio desta análise e descobertas foram: pseudonimato, mixers, CoinJoin, moedas de privacidade, movimentos entre cadeias, falta de dados rotulados, alto volume de transações, risco de falsos positivos, baixa interpretabilidade de modelos automatizados, preservação inadequada, cadeia de custódia e admissibilidade de evidências digitais. Este trabalho demonstra que a blockchain fornece trilhas públicas e auditáveis, mas que essas trilhas devem ser coletadas, preservadas, interpretadas e documentadas adequadamente para que possam ter valor forense e legal. A pesquisa sobre evidências eletrônicas ressalta a necessidade de autenticidade, integridade, validade, hashing, cópia bit a bit, registro cronológico e o papel dos especialistas.

A contribuição desta revisão é organizar um campo que ainda está fragmentado e em rápida evolução. O artigo mostra que a perícia em criptomoedas não depende de uma única técnica ou ferramenta, mas de uma abordagem híbrida capaz de combinar análise on-chain, dados off-chain, visualização, aprendizado de máquina, heurísticas, OSINT e procedimentos formais de preservação. Tal esforço pode dar a pesquisadores, especialistas, estudantes e profissionais do direito uma noção de quais caminhos metodológicos já estão estabelecidos, quais ferramentas são mais citadas e quais limitações ainda precisam ser abordadas.

Outras contribuições úteis estão relacionadas à integração dos componentes técnicos e legais-probatórios. Vários trabalhos revisados melhoram a detecção, o rastreamento e a classificação de transações suspeitas, enquanto outros se concentram na preservação, cadeia de custódia e admissibilidade. Ao combinar esses eixos, o MSL proposto demonstra que a força da evidência digital em blockchain não depende apenas da identificação de uma transação suspeita, mas também da confiabilidade do método, da documentação do procedimento, da integridade dos dados e da possibilidade de explicação técnica em um contexto investigativo ou judicial.

Apesar das vantagens, são apresentadas limitações em nosso trabalho. Primeiro, as limitações dos bancos de dados referidos, que são dominados pelos bancos de dados Scopus e IEEE Xplore. Embora esses bancos de dados sejam relevantes para Ciência da Computação, Segurança da Informação e Engenharia, há outros registros importantes e relevantes que não são comumente listados, por exemplo, indexados na ACM Digital Library, ScienceDirect, SpringerLink, Web of Science ou outras bibliotecas. A segunda limitação é o tamanho do corpus final, composto por 25 artigos primários, o que levou a uma concentração da análise, mas não alcança uma produção científica exaustiva sobre criptoforense. A terceira limitação é a rápida evolução do tema, à medida que novas técnicas, ferramentas, crimes e modelos de blockchain surgem constantemente, potencialmente alterando o cenário em pouco

tempo.

Deve-se notar que a análise foi realizada nas publicações científicas e materiais selecionados com base nos critérios MSL. As ferramentas comerciais, relatórios policiais, documentos técnicos de empresas de análise de blockchain e decisões judiciais particulares podem não ter sido investigados extensivamente. Além disso, existem limitações em alguns dos estudos envolvidos, como dependência de conjuntos de dados específicos, falta de dados rotulados, ausência de validação externa, ênfase em uma única blockchain ou falta de discussão legal sobre admissibilidade.

Para esse propósito, sugere-se aumentar o número de bases de dados consultadas e apresentar estudos de caso reais de investigação de criptomoedas, especialmente na transição de evidências técnicas para o processo judicial. Além disso, o trabalho na padronização da cadeia de custódia em blockchain, validação de ferramentas forenses, cálculo da taxa de erro de heurísticas de agrupamento, explicabilidade de modelos de aprendizado de máquina e análise multichain deve ser continuado. Uma possível via também poderia ser explorar a integração de evidências on-chain e off-chain, incluindo dados de exchanges, VASPs, dispositivos apreendidos, metadados, comunicações e fontes abertas.

A evidência digital de criptomoedas em blockchain tem um grande potencial para investigação forense, especialmente porque facilita o rastreamento de transações, fluxos financeiros, carteiras, padrões temporais, bem como estruturas suspeitas. No entanto, a evidência desse potencial não é robusta até que a presença de um método técnico sólido, preservação adequada, documentação detalhada, validação por especialistas e atenção legal andem de mãos dadas. Dessa forma, a expertise específica em blockchain é um campo interdisciplinar, e está localizada entre tecnologia, investigação, ciência de dados e direito probatório.

AGRADECIMENTOS

Os autores agradecem à Universidade Federal do Sul e Sudeste do Pará (UNIFESSPA) e ao Programa de Pós-Graduação em Ciências Forenses pelo apoio acadêmico no desenvolvimento deste trabalho. Agradecem também à Profa. Dra. Fernanda Ferreira, ao Prof. Dr. Vitor de Souza Castro e ao Prof. Dr. Hugo Pereira Kuribayashi pelas orientações, contribuições e acompanhamento durante a elaboração do Mapeamento Sistemático da Literatura.

Os autores registram ainda o uso de ferramenta de inteligência artificial generativa como apoio auxiliar na organização textual, estruturação metodológica, sistematização das informações e revisão do manuscrito. Todas as decisões científicas, a seleção dos estudos, a interpretação dos resultados, a análise crítica e a validação final do conteúdo foram realizadas pelos autores.

REFERENCES

[1] M. H. Ziegler, M. Nowostawski, and B. Katt, "Dakar: A coinjoin forensic software," *SoftwareX*, 2026.

[2] K. Song, M. A. Dhraief, M. Xu, L. Cai, X. Chen, A. Mithal, and J. Chen, "Identifying money laundering subgraphs on the blockchain," in *Proceedings of the 5th ACM International Conference on AI in Finance*, 2024.

[3] P. Tippe and C. Deckers, "Unmixing the mix: Patterns and challenges in bitcoin mixer investigations," *Forensic Science International: Digital Investigation*, 2025.

[4] Y. Sun, H. Xiong, S. M. Yiu, and K. Y. Lam, "Bitanalysis: A visualization system for bitcoin wallet investigation," *IEEE Transactions on Big Data*, vol. 9, no. 2, pp. 621–636, 2023.

[5] L. van der Horst, K.-K. R. Choo, and N.-A. Le-Khac, "Process memory investigation of the bitcoin clients electrum and bitcoin core," *IEEE Access*, vol. 5, pp. 22 385–22 402, 2017.

[6] D. Deuber, J. Gruber, M. Humml, V. Ronge, and N. Scheler, "Argumentation schemes for blockchain deanonymisation," *FinTech*, vol. 3, pp. 236–248, 2024.

[7] V. Kozii, I. Kalancha, H. Vlasova, and A. Orlean, "Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in ukraine using cryptocurrencies," *IDP. Internet, Law and Politics Journal*, no. 42, 2025.

[8] J. R. Latuihamallo, Pujiyono, and I. Cahyaningtyas, "Electronic evidence of anti-money laundering regimes: A comparative study between united kingdom, united states and indonesia," *The Law, State and Telecommunications Review*, vol. 16, no. 1, pp. 189–220, 2024.

[9] P. Dhulavvagol, S. Totad, and A. Anagal, "Shard-femf: Adaptive forensic evidence management framework using blockchain sharding and ipfs," *The International Arab Journal of Information Technology*, vol. 21, no. 2, pp. 179–190, 2024.

[10] W. Sliti, F. Cuadrado, L. C. Hernaez, and J. C. Duenas, "Detecting suspicious activity in the nft ecosystem using temporal graph analysis," *IEEE Transactions on Network Science and Engineering*, vol. 13, pp. 8684–8701, 2026.

[11] K. Sankaewtong, T. Kim, C. J. Tessone, and Y. Ikeda, "Sok: Advances in anomaly detection techniques for cryptoasset transactions," *IEEE Access*, 2025.

[12] Y. Gong, K. P. Chow, and S. M. Yiu, "Improved bitcoin simulation model and address heuristic method," *Forensic Science International: Digital Investigation*, vol. 53, p. 301935, 2025.

[13] X. Hu, M. Gui, G. Cheng, R. Li, and H. Wu, "Multi-class bitcoin mixing service identification based on graph classification," *Digital Communications and Networks*, vol. 10, pp. 1881–1893, 2024.

[14] X. F. Liu, X.-J. Jiang, S.-H. Liu, and C. K. Tse, "Knowledge discovery in cryptocurrency transactions: A survey," *IEEE Access*, vol. 9, pp. 37 229–37 254, 2021.

[15] M. L. Tsai, C. Y. Kuan, C. L. Lin, C. H. Shih, and F. C. Tsai, "The investigation of illicit tron wallet based on temporal behaviour analysis," *Procedia Computer Science*, vol. 246, pp. 5294–5303, 2024.

[16] K.-S. Choi, M. Chawki, and S. Basu, "Uncovering cryptocurrency-enabled sextortion: A blockchain forensic analysis of transactions and offender laundering tactics," *Information*, vol. 17, p. 236, 2026.

[17] B. Mawhayi, J. Botha, and L. Leenen, "A web scraping approach towards cryptocurrency investigations," in *Proceedings of the 24th European Conference on Cyber Warfare and Security*, 2025, pp. 445–454.

[18] "Forensic analysis of cryptocurrencies: A comprehensive overview," 2025, dados bibliográficos a completar conforme a base de origem.

[19] "Cashing out crypto: state of practice in ransom payments," 2024, dados bibliográficos a completar conforme a base de origem.

[20] "A novel methodology for hyip operators' bitcoin addresses identification," 2019, dados bibliográficos a completar conforme a base de origem.

[21] "Dissection of an approval-based trusted-token fraud scheme used across multiple blockchain systems," 2025, dados bibliográficos a completar conforme a base de origem.

[22] "Enhanced identification of illicit bitcoin transactions through genetic algorithm-based feature selection," 2025, dados bibliográficos a completar conforme a base de origem.

[23] "Blockchain forensics and regulatory technology for crypto tax compliance: A state-of-the-art review and emerging directions in the south african context," 2026, dados bibliográficos a completar conforme a base de origem.

[24] "A hybrid multi-agent system for early scam detection in crypto-assets," 2026, dados bibliográficos a completar conforme a base de origem.

[25] "A lawful metadata-driven framework for linking encrypted communication behavior and cryptocurrency wallet activity in digital investigations," 2026, dados bibliográficos a completar conforme a base de origem.