Fundamentos de la Metodología de análisis y resguardo de potenciales elementos de prueba digital asociados a Criptomonedas y Criptoactivos

Cintia V. Gioia, Emiliano A. Zárate, Serena R. Donato, Mario J. Krajnik, Jorge E. Eterovic

Universidad Nacional de La Matanza (UNLaM), Buenos Aires, Argentina
cgioia@unlam.edu.ar, ezarate@unlam.edu.ar, srdonato@unlam.edu.ar, mkrajnik@unlam.edu.ar, eterovic@unlam.edu.ar

***Resumen*— La Informática Forense aplicada a la tecnología de blockchain y específicamente a las criptomonedas y criptoactivos en general, involucra poseer los conocimientos y herramientas necesarias para encarar una pericia informática como parte de un proceso o investigación judicial, lo cual, posibilita seguir la historia de las transacciones en la cadena de bloques de las principales criptomonedas y otros criptoactivos. Se plantean los fundamentos del diseño de una metodología integral para el análisis y resguardo de posibles elementos de prueba digital asociados a criptomonedas y criptoactivos, la cual fortalece la eficacia y la confiabilidad de los procedimientos forenses a aplicar en pericias informáticas que forman parte de procesos o investigaciones judiciales, asegurando que se generen resultados técnica y legalmente válidos.**

***Abstract*—Forensic Informatics applied to Blockchain technology, and specifically to cryptocurrencies and crypto-assets in general, involves possessing the knowledge and tools required to conduct a digital forensic examination as part of a judicial process or investigation. This enables the tracing of transaction histories within the blockchain of major cryptocurrencies and other digital assets. The paper presents the foundations for designing a comprehensive methodology for the analysis and preservation of potential digital evidence related to cryptocurrencies and crypto-assets. This methodology strengthens the effectiveness and reliability of forensic procedures applied in digital investigations that are part of judicial processes, ensuring that the results obtained are both technically and legally valid.**

I. INTRODUCCIÓN

El desarrollo y la masiva adopción a nivel global, del uso de Internet, de computadoras personales, dispositivos móviles, servicios y plataformas asociadas, ha tenido un vasto impacto sobre la velocidad y naturaleza de las interacciones sociales, del que no están exentos las transacciones comerciales o financieras. Una de las manifestaciones de la transición de la actividad humana desde el mundo físico al virtual ha sido el surgimiento de activos virtuales (AV), entendidos, conforme la definición del Grupo de Acción Financiera Internacional (GAFI[1]), como una representación digital de valor que puede ser intercambiada o transferida digitalmente, y utilizada como forma de pago o instrumento de inversión. En este escenario, el desarrollo más importante ha sido, sin dudas, la creación de las criptomonedas, que desde su nacimiento en 2008 - con la publicación del célebre "White paper" de Satoshi Nakamoto sobre el Bitcoin - se convirtieron en uno de los mercados no regulados más grandes del mundo.

La aparición de las criptomonedas[2], los criptoactivos[3] y de la tecnología de Blockchain[4], constituye un fenómeno que bien puede estar llamado a revolucionar positivamente muchos aspectos del sistema financiero. Pero como muchas innovaciones, también es susceptible de ser explotada para favorecer la actividad ilícita, los cuáles deben ser abordados desde la Forensia Digital.

La tecnología de Blockchain es la tecnología sobre la que se sustentan las criptomonedas y criptoactivos. En términos similares, la Unidad de Información Financiera (UIF)[5], en su resolución 300/2014 "Prevención del Lavado de Activos y de la Financiación Del Terrorismo" [1] definió a las "Monedas Virtuales" como la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de

[1] GAFI (Grupo de Acción Financiera Internacional) es un organismo intergubernamental creado en 1989 por el G7 para establecer estándares y promover políticas destinadas a prevenir el lavado de dinero, la financiación del terrorismo y otras amenazas al sistema financiero global.

[2] Criptomonedas: activos digitales que funcionan como medio de intercambio, basados en criptografía para asegurar las transacciones y controlar la creación de nuevas unidades.

[3] Criptoactivos: categoría más amplia que incluye a las criptomonedas y otros activos digitales tokenizados que representan valor, derechos o bienes en entornos digitales.

[4] BlockChain: tecnología de registro distribuido que almacena transacciones en bloques enlazados y verificables, garantizando transparencia, trazabilidad e inmutabilidad de la información.

[5] UIF: organismo del Estado argentino encargado del análisis, tratamiento y difusión de inteligencia financiera para prevenir el lavado de activos, la financiación del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En ese sentido, la UIF diferenció a las monedas virtuales del "dinero electrónico", entendido este último como un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción. Se define como activo virtual, a una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión, los cuales no incluyen representaciones digitales de monedas fiduciarias.

Las blockchains públicas y privadas se diferencian por su nivel de acceso y control. Las blockchains públicas —como Bitcoin o Ethereum— son redes abiertas, descentralizadas y transparentes, donde cualquier usuario puede participar, validar transacciones y auditar el registro histórico. En cambio, las blockchains privadas restringen el acceso a un conjunto limitado de nodos autorizados, generalmente bajo el control de una organización o consorcio, lo que permite mayor gobernanza, privacidad y eficiencia transaccional, pero reduce la descentralización y la verificabilidad pública de los datos.
Durante la última década, los activos virtuales, en especial las criptomonedas, han pasado a ocupar un lugar central como moneda de cambio en las transacciones ilícitas realizadas, sobre todo, en los mercados ilegales que operan en Internet.

Los principales rasgos que incrementan el riesgo de lavado de dinero y financiación del terrorismo son el anonimato asociado al diseño de los activos virtuales, la posibilidad de que una misma persona controle múltiples "monederos virtuales", el carácter descentralizado de la mayoría de las criptomonedas y el alcance global de muchas de ellas, entre otros. Esto derivó en que se recurriese a las criptomonedas para facilitar el surgimiento de mercados online en la "Dark Web" o "Red oscura" de Internet, en los que hasta el día de hoy se intercambian bienes y servicios (en su mayoría) ilegales a cambio de criptomonedas.

En este escenario de creciente digitalización y expansión de los activos virtuales, se vuelve esencial abordar su impacto desde una perspectiva integral que articule los planos tecnológico, jurídico y forense. El desarrollo del ecosistema cripto ha promovido la creación de nuevos instrumentos financieros y sistemas descentralizados de intercambio, pero también ha introducido desafíos relevantes para las instituciones encargadas de la regulación, la supervisión y la investigación del delito. La combinación entre anonimato, descentralización y alcance global genera un entorno complejo que demanda metodologías especializadas para garantizar la trazabilidad, integridad y validez probatoria de la evidencia digital asociada a estos activos.

La adopción de criptoactivos en Argentina y en el mundo continúa en crecimiento, expandiéndose más allá del uso financiero tradicional y generando nuevos desafíos en materia de trazabilidad, regulación y análisis forense digital. Su expansión trasciende el ámbito del resguardo o reserva de valor: los criptoactivos se utilizan como medio de pago para bienes y servicios, instrumento de inversión, canal de remesas internacionales, mecanismo de financiamiento descentralizado (*DeFi*)[6] y soporte tecnológico para la ejecución de contratos inteligentes[7] y la tokenización de activos digitales[8]. Este patrón, junto con la alta presencia de exchanges[9] centralizados en la región, impulsa la masificación de su uso y genera nuevas superficies de investigación y fuentes de información relevantes para la trazabilidad. Al mismo tiempo, su infraestructura puede ser explotada en esquemas ilícitos —como fraude, *ransomware*, lavado de activos y evasión fiscal— que demandan capacidades específicas de análisis forense digital y cooperación interinstitucional e internacional.

II. DESAFÍOS PERICIALES EN EL ANÁLISIS DE CRIPTOMONEDAS Y CRIPTOACTIVOS

A nivel nacional e internacional, aún no se han consolidado metodologías ni procedimientos específicos que faciliten el trabajo pericial o unifiquen criterios técnicos en el tratamiento de potenciales elementos de prueba digital asociados a criptomonedas y criptoactivos. En tal sentido, las evidencias vinculadas con el uso de criptoactivos se suman como una nueva categoría de elementos que se deben identificar, tanto en el lugar del hecho como en los laboratorios forenses donde se examinan computadoras, unidades de almacenamiento, teléfonos móviles y tabletas, entre otros, para luego poder realizar un análisis forense sobre los mismos.

La investigación criminal ligada a los criptoactivos cobra un rol preponderante. Investigar actividades delictivas relacionadas con criptoactivos puede resultar complejo, ya que muchos casos podrían estar vinculados con compras realizadas o fondos transferidos a través de la cadena de bloques. Por lo tanto, resulta vital comprender con precisión cómo se preparan, transmiten, procesan y almacenan estas transacciones.

Se plantean algunos de los siguientes desafíos: el análisis forense de billeteras físicas o digitales en el sitio (ubicación física), secuestro de criptoactivos, cómo encontrar evidencia en teléfonos móviles y computadoras portátiles y de escritorio, qué métodos aplicar para investigar y realizar análisis forenses de forma remota (usando conexión a Internet) de varias direcciones de criptomonedas maliciosas de la vida real,

[6] Financiamiento descentralizado (DeFi): conjunto de aplicaciones y servicios financieros basados en tecnología blockchain que operan sin intermediarios tradicionales (como bancos o entidades financieras) mediante contratos inteligentes (smart contracts). Permiten ejecutar préstamos, depósitos, intercambios y otros instrumentos financieros de forma automatizada y transparente.

[7] Contrato inteligente (smart contract): programas ejecutados en *blockchain* que automatizan y hacen cumplir condiciones pactadas entre partes sin intermediarios. Se despliegan como código inmutable, se activan ante disparadores definidos y registran sus resultados on-chain, aportando transparencia, trazabilidad y ejecución determinística

[8] Tokenización de activos digitales: proceso mediante el cual un activo físico, financiero o virtual se representa como un *token* dentro de una red *blockchain*. Este token digitaliza el valor o los derechos asociados al activo, posibilitando su fraccionamiento, transferencia y registro seguro en un entorno distribuido y trazable.

[9] Exchanges (casas de intercambio de criptoactivos): plataformas digitales que permiten la compra, venta, conversión y custodia de criptomonedas y otros criptoactivos. Pueden operar de manera centralizada (CEX) bajo la gestión de una entidad que intermedia las transacciones o descentralizada (DEX), donde las operaciones se realizan directamente entre usuarios mediante contratos inteligentes sobre blockchain.

permitiendo rastrear sus transacciones haciendo uso de software libre, entre otros.

Un obstáculo adicional a la hora de requerir información de empresas proveedoras de servicios de intercambio o compraventa de criptoactivos a través de internet es que, por la naturaleza y entorno digital de su negocio, esas empresas podrían estar constituidas y operar en jurisdicciones extranjeras, con lo cual el acceso a este tipo de información y evidencia digital puede resultar más complicado.

La naturaleza pública o privada de una blockchain tiene implicancias sustanciales en la investigación judicial y forense digital.

En las blockchains públicas, la información sobre transacciones y direcciones es abierta, verificable y accesible sin autorización judicial internacional, lo que facilita la trazabilidad de operaciones y el análisis de patrones de flujo mediante herramientas de recopilación y análisis de información disponible públicamente o plataformas de análisis y trazabilidad. No obstante, la pseudonimización de las direcciones impone el reto de vincularlas con identidades reales.

En las blockchains privadas, la visibilidad de los datos depende de los permisos definidos por la entidad administradora, por lo que el acceso a la información requiere cooperación directa con el operador o la autorización judicial correspondiente. Esto puede limitar la transparencia y dificultar la obtención de evidencia digital si la red no garantiza mecanismos auditables de registro y validación.

En síntesis, las blockchains públicas ofrecen mayor trazabilidad técnica, mientras que las privadas ofrecen mayor control institucional, lo que determina estrategias forenses diferenciadas para la recolección y validación de pruebas digitales.

III. Estado actual del conocimiento

En 2021, el Grupo de Acción Financiera de Latinoamérica (GAFILAT[10]) publicó la "*Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales*" [2], La misma tiene como propósito brindar a las autoridades de orden público herramientas para la recuperación de activos delictivos y la cooperación internacional, fortaleciendo sus capacidades para solicitar, investigar e identificar activos virtuales. Además, promueve el desarrollo de habilidades para la identificación, incautación y decomiso de activos ilícitos vinculados al lavado de dinero y la financiación del terrorismo en América Latina, por parte de unidades fiscales, fuerzas de seguridad y agencias de investigación. También advierte sobre las herramientas que utilizan los criminales para obstaculizar la acción de las autoridades y sus consecuencias. Aunque la guía no es de alcance nacional, sino regional —dado que GAFILAT reúne a 17 países de América del Sur, Centroamérica y América del Norte—, su aporte resulta de gran valor para todos los Estados miembros. La guía no profundiza sobre lo referido a análisis forense de las actividades delictivas con activos virtuales. Si bien facilita la cooperación internacional, necesita poder analizarse y adaptarse a marcos legales nacionales y a los avances tecnológicos.

En Argentina, se han producido avances regulatorios recientes, entre ellos la creación del Registro de Proveedores de Servicios de Activos Virtuales[11] (Registro PSAV) por parte de la Comisión Nacional de Valores (CNV), mediante la Resolución General 994/2024 [3] (artículo 4 de la Ley 27.739). Dicho registro está orientado a supervisar y transparentar las operaciones vinculadas con criptoactivos. La Resolución 994/2024 es de interés para que la Argentina pueda cumplir con los estándares fijados en "*Las 40 Recomendaciones de la GAFI*"[12] [4], en particular la Recomendación 15, en lo referente a la lucha contra el lavado de activos y el financiamiento del terrorismo en las transacciones con activos virtuales. Sin embargo, persisten desafíos significativos en materia de jurisdicción y cooperación internacional, especialmente cuando los exchanges o plataformas de intercambio operan desde el exterior y no están sujetos directamente a la normativa nacional.

En este marco, el Convenio de Budapest sobre Ciberdelito[13] [5], suscripto por Argentina, y su Segundo Protocolo Adicional [6] constituyen instrumentos fundamentales, ya que permiten requerimientos directos de información digital entre autoridades judiciales y empresas proveedoras radicadas en los Estados Parte del convenio. Dichos mecanismos garantizan la licitud del acceso a datos públicos, la preservación de la cadena de custodia digital, y fortalecen tanto la cooperación internacional como la eficacia de la investigación forense.

Como parte de los esfuerzos institucionales nacionales por abordar los desafíos vinculados a los criptoactivos, el Ministerio Público Fiscal (MPF[14]) de la Procuración General de la Nación publicó el 12 de mayo de 2023, la Resolución N.° 33/23, mediante la cual se dio a conocer la "*Guía Práctica*

[10] GAFILAT (Grupo de Acción Financiera de Latinoamérica): organismo regional intergubernamental que agrupa a países de América del Sur, Centroamérica y América del Norte, dedicado a promover la implementación de políticas contra el lavado de activos y la financiación del terrorismo, en coordinación con el GAFI.

[11] Las actividades incluidas en la definición de PSAV son i. intercambio entre activos virtuales y monedas de curso legal (monedas fiduciarias); ii. intercambio entre una (1) o más formas de activos virtuales; iii. transferencia de activos virtuales; iv. custodia y/o administración de activos virtuales o instrumentos que permitan el control sobre los mismos; y v. participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo virtual.

[12] Las 40 Recomendaciones del GAFI son los estándares internacionales más reconocidos para combatir el lavado de activos y el financiamiento del terrorismo: https://www.gafilat.org/index.php/es/las-40-recomendaciones

[13] El Convenio de Budapest sobre Ciberdelincuencia es el primer tratado internacional que establece un marco jurídico común para combatir los delitos informáticos y las infracciones cometidas mediante sistemas informáticos o redes. Adoptado por el Consejo de Europa en 2001, promueve la armonización legislativa, el fortalecimiento de las capacidades de investigación y la cooperación internacional entre los Estados Parte para la obtención y preservación de evidencia digital. Los artículos 18 y 19 regulan la obtención, preservación y entrega de datos por parte de proveedores de servicios y autoridades competentes, mientras que el artículo 32 habilita la obtención transfronteriza de información informática cuando se trate de datos públicos o con consentimiento del titular.

[14] MPF (Ministerio Público Fiscal de la Nación): órgano autónomo del Estado argentino responsable de promover la acción de la justicia en defensa de la legalidad y los intereses generales de la sociedad.

para la Identificación, Trazabilidad e Incautación de Criptoactivos" [7], elaborada por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI[15]). La resolución destaca diversas particularidades del entorno digital que dificultan el trabajo del MPF y las investigaciones penales, entre ellas el pseudoanonimato, la complejidad de los procesos informáticos y matemáticos empleados, la alta volatilidad del valor de las monedas virtuales, la localización de las operaciones con criptoactivos y sus actores, la escasa regulación existente, entre otros. Esta guía —una de las primeras de su tipo en Argentina— tiene como objetivo dotar a los organismos públicos de conocimientos y mecanismos actualizados para rastrear transacciones y confiscar activos virtuales que pudieran ser utilizados en actividades delictivas. Asimismo, busca ofrecer a los investigadores un material de referencia accesible para comprender el fenómeno de los criptoactivos y las tecnologías asociadas, con especial énfasis en los aspectos operativos de la investigación criminal, incluida la etapa de incautación. Sin embargo, no proporciona procedimientos específicos de investigación judicial ni aborda las tareas y análisis periciales que competen a los peritos informáticos en su labor. Como su título indica, se focaliza particularmente en la identificación, trazabilidad e incautación de criptoactivos para su investigación penal.

En una línea de acción más general, en marzo de 2023, el Ministerio de Seguridad de la Nación publicó el "*Protocolo para la Identificación, Recolección, Preservación, Procesamiento y Presentación de Evidencia Digital"* [8], elaborado por la Dirección de Investigaciones del Ciberdelito. Este Protocolo General de Actuación (PGA) tiene por objeto establecer las pautas y procedimientos que deben seguir los miembros de las Fuerzas Federales Policiales y de Seguridad durante las etapas de identificación, recolección, preservación, procesamiento y presentación de evidencia digital asociada a cualquier tipo de delito, y en particular a los ciberdelitos, ya sean ciberasistidos o ciberdependientes. El documento se enmarca en los objetivos de la Resolución N.° 86/2022 del Ministerio de Seguridad, dictada en el contexto del Programa de Fortalecimiento en Ciberseguridad e Investigación del Cibercrimen (ForCIC[16]). Su aplicación es de carácter obligatorio en todo el territorio nacional para el personal de la Policía Federal Argentina, Gendarmería Nacional Argentina, Policía de Seguridad Aeroportuaria y Prefectura Naval Argentina, quienes deben ajustar su accionar a la Constitución Nacional, las leyes penales, las normas procesales y los protocolos vigentes.

Este protocolo realiza una referencia general a los conceptos asociados a tecnología de blockchain y criptoactivos, estableciendo que, ante la posible presencia de Potenciales Elementos de Prueba digitales ("PEP digitales")[17] vinculados a los mismos, se coordine con la autoridad judicial los pasos a seguir. No detalla procedimientos de acción específicos, sino que se limita a definiciones y recomendaciones generales. Tampoco profundiza en cómo llevar adelante una investigación judicial o un análisis forense digital que incluya este tipo de evidencia. Definiciones relevantes incluidas en este protocolo:

- Tecnología de blockchain: Libro de contabilidad digital distribuido de transacciones firmadas criptográficamente que se agrupan en bloques. Cada bloque se vincula criptográficamente con el anterior después de su validación y de someterse a una decisión consensuada. A medida que se añaden nuevos bloques, los más antiguos se vuelven más difíciles de modificar (creando una resistencia a la manipulación). Los nuevos bloques se replican en las copias del libro mayor dentro de la red, y cualquier conflicto se resuelve automáticamente utilizando las reglas establecidas.
- Criptoactivos: Representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias.
- Rig de Minería: Conjunto de elementos de hardware instalados y configurados para el minado de criptoactivos.

En el mismo protocolo se establece que, al momento del allanamiento, deberá prestarse especial atención a los siguientes aspectos:

- Presencia de billeteras frías —dispositivos con aspecto similar a un pendrive—, así como a anotaciones que contengan palabras clave (semillas), códigos QR u otros datos que puedan estar asociados a wallets o monederos digitales. Ante la detección de indicadores o identificadores vinculados a actividades con criptoactivos, se deberá consultar de inmediato a la autoridad judicial, quien determinará el criterio de actuación correspondiente.
- Hallazgo de equipos de minería (rigs de minería). El primer interviniente deberá coordinar con la autoridad judicial y con el personal especializado en criptoactivos para definir el procedimiento a seguir. Los rigs de minería pueden presentar distintos aspectos según la tecnología utilizada; actualmente, los más comunes emplean placas de video (GPU) o hardware específico para algoritmos determinados (ASIC). Debe considerarse que algunos rigs representan un alto valor económico, por lo que su detección durante un procedimiento debe ser informada a la autoridad judicial para que evalúe su posible secuestro. El protocolo no detalla las acciones específicas a seguir, sino que en todos los casos recomienda la consulta a la autoridad judicial antes de proceder.

Las criptomonedas constituyen un tipo específico de criptoactivos. Son monedas virtuales de emisión descentralizada, sin respaldo de ningún gobierno o entidad en particular, basadas en la tecnología de blockchain. Funcionan como medios de pago y buscan reproducir las funciones esenciales del dinero. A diferencia del sistema financiero

[15] UFECI (Unidad Fiscal Especializada en Ciberdelincuencia): unidad del Ministerio Público Fiscal de la Nación Argentina encargada de investigar delitos informáticos y coordinar acciones vinculadas con la criminalidad digital y el uso de criptoactivos.

[16] ForCIC (Programa de Fortalecimiento en Ciberseguridad e Investigación del Cibercrimen): creado por el Ministerio de Seguridad de la Nación mediante la Resolución N.° 86/2022, publicada en el Boletín Oficial el 1 de marzo de 2022, orientado a establecer políticas, protocolos y capacidades técnicas para fortalecer la prevención, detección e investigación de delitos informáticos en Argentina.

[17] Potencial Elemento de Prueba (PEP): dispositivos susceptibles de contener información (representación física), los cuales almacenan potencial evidencia digital (representación lógica). Potencial Elemento de Prueba digital (PEP digital): se refiere a cualquier dato (registro y/o archivo) que puede ser generado, transmitido o almacenado por equipos de tecnología informática y que está constituido por campos magnéticos y pulsos electrónicos, los cuales pueden ser recolectados y analizados con herramientas y/o técnicas especiales.

tradicional —basado en la confianza y la intermediación de instituciones financieras—, las criptomonedas operan sobre un sistema de pago electrónico sustentado en pruebas criptográficas, lo que garantiza la autenticidad y seguridad de las transacciones sin necesidad de terceros o autoridades centrales. De este modo, dos partes pueden realizar transacciones directas entre sí mediante mecanismos de criptografía que aseguran la validez de las operaciones.

Actualmente no existe una guía o metodología que esté orientada a cómo proceder específicamente en una pericia informática basada en el análisis y resguardo de potenciales elementos de prueba digital de criptomonedas y criptoactivos para presentar ante la justicia.

Como antecedentes de la presente investigación, en el Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT) de la Universidad Nacional de La Matanza se desarrollaron tres proyectos orientados al diseño de metodologías, procedimientos y a la implementación y gestión de Laboratorios de Informática Forense. Si bien estos trabajos no tuvieron un enfoque específico en criptoactivos o criptomonedas, constituyen el marco metodológico y operativo de referencia que permite avanzar en el desarrollo de la propuesta actual.

En primer lugar, se llevó a cabo el proyecto "*Análisis del Marco Normativo Técnico Legal del Ciclo de Vida de la Evidencia Digital*" en el cual se desarrolló un marco normativo y operativo de referencia para el tratamiento integral de la evidencia digital, incorporando los aspectos legales y procedimentales necesarios para su correcta gestión.

En el contexto del segundo proyecto, "*Implementación y Gestión de un Laboratorio de Informática Forense*" [9], se definió un modelo integral para la creación y gestión de un Laboratorio de Informática Forense (LabIF-UNLaM), abordando tanto la infraestructura tecnológica como los procesos y metodologías de trabajo. De este desarrollo surgió la metodología ForenseUDE [10], alineada con los modelos PURI[18] ("Proceso Unificado de Recuperación de Información") [11], [12] y EDRM[19] ("Electronic Discovery Reference Model") [13]. Su diseño incorpora, además, los lineamientos de la norma ISO/IEC 27037:2012 [14] y su versión traducida al castellano con observaciones, ISO/IRAM 27037:2022, adaptada al contexto nacional, garantizando la validez técnica y legal.

La metodología ForenseUDE fue desarrollada con el propósito de establecer un proceso universal, integral y detallado para el tratamiento de la evidencia digital. Estructura un conjunto de fases interconectadas que guían las actividades forenses desde la identificación hasta la presentación de resultados, garantizando trazabilidad, consistencia y validez técnica en cada etapa.

Como resultado del tercer proyecto impulsado por el DIIT, "*Diseño de un Sistema de Gestión de Calidad y Proceso de Acreditación del Laboratorio Informático Forense (LabIF-UNLaM)*", se logró diseñar, desarrollar e implementar un Sistema de Gestión de la Calidad aplicable al laboratorio, conforme a la norma ISO/IEC 17.025:2017, fortaleciendo la estandarización y la confiabilidad de los procesos periciales [15], [16].

IV. HERRAMIENTAS DE ANÁLISIS Y TRAZABILIDAD

Existe la idea de que, debido a su naturaleza seudónima, es imposible determinar el origen de las criptomonedas o rastrear el camino que han recorrido hasta llegar a la persona que las posee en un momento específico. Sin embargo, las criptomonedas de blockchains públicas son perfectamente trazables, ya que todas las transacciones realizadas están expuestas y son visibles para el público en general. Aunque la red opera de manera seudónima, ya que no hay registro en la blockchain sobre la identidad detrás de cada dirección pública, es posible combinar esa información con otros datos para asociar direcciones a personas y así reconstruir una cadena de tenencias de criptomonedas. Es decir, es viable llevar a cabo una investigación forense para identificar el origen o destino de una criptomoneda.

El análisis forense y la investigación judicial de operaciones con criptoactivos requieren el uso combinado de herramientas especializadas que permitan rastrear, visualizar y documentar transacciones en entornos blockchain.

El proceso investigativo requiere el uso combinado de software libre y plataformas comerciales especializadas en trazabilidad de criptoactivos —tales como Chainalysis [17] y TRM Labs [18] — con el fin de abordar el análisis de grandes volúmenes de transacciones en redes blockchain públicas.

Estas herramientas permiten identificar patrones de flujo financiero, detectar nodos relevantes y visualizar interacciones entre direcciones mediante heurísticas de agrupamiento, técnicas de atribución basada en OSINT (Open-Source Intelligence)[20] y algoritmos de análisis de grafos. OSINT complementa las técnicas de trazabilidad blockchain al permitir contextualizar direcciones, entidades o transacciones mediante información disponible en Internet o detectar infraestructura técnica asociada a actividades ilícitas (por ejemplo, servidores C2[21], exchanges no registrados o clusters de wallets[22]).

[18] PURI (Proceso Unificado de Recuperación de Información): es el resultado de un proyecto de una investigación iniciada en el 2011 en la Facultad de Ingeniería de la Universidad FASTA. El modelo es un esquema de las tareas involucradas en la aplicación forense de las ciencias de la información. Este esquema agrupa las tareas en actividades de mayor abstracción, y a éstas en.

[19] EDRM ("Electronic Discovery Reference Model"): modelo internacional de referencia del descubrimiento electrónico (e-discovery), que se refiere a cualquier proceso en el que se busca, localiza, asegura y examina datos electrónicos con la intención de usarlos como evidencia digital. Este modelo también menciona una serie de etapas o fases en las cuales se brindan mejores prácticas de manera global para el tratamiento de la evidencia.

[20] OSINT: se refiere a la obtención, análisis y correlación de información proveniente de fuentes abiertas y accesibles públicamente, tales como sitios web, redes sociales, registros públicos o foros en línea. Principales herramientas OSINT: Maltego, SpiderFoot, Shodan, Breadcrumbs y Bitquery, entre otras.

[21] Servidores C2 (Command and Control): son infraestructuras utilizadas por atacantes para dirigir, coordinar y controlar sistemas comprometidos o redes de equipos infectados (botnets).

[22] Clusters de wallets: son agrupaciones lógicas de direcciones de criptomonedas que, mediante técnicas de análisis heurístico y de comportamiento en la blockchain, pueden inferirse como controladas por un mismo usuario o entidad.

El empleo conjunto de entornos abiertos y soluciones propietarias fortalece la validez técnica y pericial del proceso, al combinar la transparencia del código abierto con las capacidades avanzadas de procesamiento, correlación y automatización que ofrecen las plataformas comerciales en investigaciones complejas.

Entre las soluciones más utilizadas a nivel internacional se destacan Chainalysis y TRM Labs, plataformas comerciales de inteligencia y trazabilidad blockchain que integran métodos de análisis de grafos, heurísticas de agrupamiento y atribución de direccione.

Chainalysis es una plataforma comercial de inteligencia blockchain diseñada para la trazabilidad y el análisis forense de transacciones con criptoactivos. Permite examinar el flujo de fondos a través de diferentes redes —como Bitcoin, Ethereum y otras blockchains públicas— mediante la aplicación de algoritmos de agrupamiento heurístico, análisis de grafos y técnicas de atribución de direcciones. En el ámbito judicial, su utilización posibilita vincular direcciones de criptoactivos con entidades o actores específicos, detectar operaciones sospechosas, y reconstruir esquemas de lavado de activos, fraude o ransomware. Asimismo, facilita la generación de reportes técnicos admisibles como evidencia digital, compatibles con los principios de trazabilidad y preservación de la cadena de custodia.

Desde una perspectiva forense, Chainalysis aporta capacidad analítica avanzada para el tratamiento de grandes volúmenes de datos y el seguimiento de fondos a través de mixers[23], exchanges o wallets distribuidas globalmente, constituyéndose en una herramienta de apoyo esencial para peritos informáticos y fiscales en investigaciones complejas relacionadas con criptoactivos.

TRM Labs es una plataforma de análisis e inteligencia blockchain orientada al monitoreo de riesgos, cumplimiento normativo y trazabilidad de criptoactivos. Su principal fortaleza radica en la integración de información on-chain[24] y off-chain[25], permitiendo a las autoridades judiciales y forenses identificar, rastrear y analizar transacciones sospechosas en múltiples redes y activos digitales. La herramienta combina modelos de aprendizaje automático con bases de datos de entidades verificadas, lo que posibilita asociar direcciones de billeteras con exchanges, plataformas de servicios financieros y actores ilícitos conocidos. En el contexto forense, facilita la visualización de flujos transaccionales, la detección de patrones de lavado de activos o financiamiento del terrorismo, y la elaboración de reportes probatorios que cumplen con los estándares internacionales de evidencia digital. El uso de TRM Labs en investigaciones judiciales fortalece la cooperación interinstitucional y la eficacia de la respuesta frente a delitos financieros basados en blockchain, al ofrecer un entorno analítico unificado, trazable y técnicamente verificable.

En síntesis, Chainalysis se orienta al análisis forense retrospectivo y judicial de operaciones, mientras que TRM Labs privilegia un enfoque preventivo y de cumplimiento normativo dentro del ecosistema financiero.

El uso conjunto de ambas herramientas —en sinergia con software libre y técnicas OSINT— amplía el alcance del análisis, fortaleciendo la validez técnica y jurídica de las investigaciones, y consolidando un enfoque estandarizado para la trazabilidad forense de activos digitales. Además, ofrecen una cobertura integral que abarca desde la detección temprana de operaciones sospechosas hasta la trazabilidad forense y presentación de evidencia digital.

La admisibilidad judicial de evidencia obtenida en estas herramientas ha sido validada en precedentes internacionales principalmente en los Estados Unidos, los cuales confirmaron su validez probatoria al considerarlas técnicamente confiables, utilizadas por agencias federales y sujetas a verificación pericial independiente. En United States v. Sterlingov [19], el tribunal del Distrito de Columbia admitió los informes de Chainalysis como evidencia válida para vincular direcciones de Bitcoin utilizadas en un servicio de mezcla (*mixer*) con el acusado, estableciendo la confiabilidad técnica de la herramienta y su uso por parte del FBI y el IRS-CI .Por su parte, en *U*.S. v. Harmon [20], la misma corte aceptó los resultados de trazabilidad de Chainalysis que demostraron operaciones ilícitas de lavado de dinero a través de un servicio de "mixing", sentando un precedente relevante para la utilización forense de estos sistemas en delitos financieros y cibernéticos.

Estos antecedentes internacionales sientan base para su aceptación en investigaciones judiciales y pericias forenses de criptoactivos, al demostrar que la trazabilidad basada en blockchain puede cumplir con los estándares de admisibilidad de evidencia digital en el proceso penal.

V. PLANTEO GENERAL DE LA METODOLOGÍA

Se plantea el diseño de una metodología de análisis y resguardo de potenciales elementos de prueba digital vinculados a criptomonedas y criptoactivos, aplicable a pericias informáticas que formen parte de procesos o investigaciones judiciales. El objetivo principal es fortalecer la eficacia, confiabilidad y validez técnica y legal de los procedimientos forenses en el ámbito de los criptoactivos.

La metodología propuesta, orientada al tratamiento de posibles elementos de prueba digital asociados a estos activos, busca asegurar la integridad y trazabilidad de la evidencia digital, promoviendo un desempeño eficiente y estandarizado

[23] Mixers (o tumblers): son servicios o protocolos diseñados para ofuscar el origen y destino de los fondos en una transacción de criptomonedas, mezclando múltiples entradas y salidas de distintos usuarios. Su objetivo declarado suele ser preservar la privacidad, pero en la práctica son utilizados con frecuencia para dificultar la trazabilidad y el rastreo de operaciones ilícitas, como lavado de activos o pago de ransomware. Desde el punto de vista forense, los mixers representan un desafío técnico, ya que rompen la correlación directa entre direcciones y flujos de valor, requiriendo análisis heurísticos avanzados y herramientas de trazabilidad especializadas (p. ej., Chainalysis o TRM Labs).

[24] Información on-chain: comprende todos los datos registrados directamente en la cadena de bloques, como transacciones, direcciones, hashes, bloques y contratos inteligentes. Esta información es pública, inmutable y verificable criptográficamente, lo que permite su análisis mediante herramientas de trazabilidad o inteligencia forense.

[25] Información off-chain: se refiere a datos externos o complementarios que no se almacenan en la blockchain, tales como registros de usuarios en exchanges, metadatos de dispositivos, comunicaciones, archivos, documentos, o datos personales asociados. Su obtención suele requerir órdenes judiciales, cooperación internacional o análisis técnico adicional, y resulta esencial para vincular identidades reales con transacciones pseudónimas.

por parte de los equipos periciales. Asimismo, favorece la cooperación interinstitucional, al propiciar la homologación de criterios y la aceptación de los resultados obtenidos entre diferentes laboratorios forenses.

El desarrollo de esta propuesta metodológica se alinea y especifica a partir de la metodología ForenseUDE, consolidando su adaptación al contexto tecnológico y jurídico de los criptoactivos. Además, se enmarcan en los lineamientos de las normas ISO/IEC 27037:2012 e ISO/IRAM 27037:2022, y sus normas complementarias, como también con las leyes, pautas procesales y protocolos vigentes a nivel nacional e internacional.

Etapa Preliminar de Actualización Metodológica y Tecnológica

Se propone una instancia preliminar y de actualización permanente orientada a fortalecer las capacidades técnicas, analíticas y operativas de los equipos forenses en el tratamiento de evidencia digital vinculada a criptomonedas y criptoactivos. Estas etapas constituyen un marco de referencia dinámico que sustenta la metodología general, asegurando su vigencia y adecuación frente a la evolución tecnológica y delictiva del ecosistema cripto-financiero.

1) Relevamiento y actualización de aspectos teórico-prácticos sobre criptoactivos y tecnología blockchain

Comprende el estudio y actualización de los principales fundamentos técnicos y operativos relacionados con los activos virtuales basados en tecnología blockchain. Incluye el análisis de las transacciones con criptomonedas y criptoactivos, los mecanismos de minería y validación, el funcionamiento de las billeteras virtuales y los métodos de almacenamiento y resguardo de claves privadas. Esta etapa proporciona el sustento conceptual necesario para comprender la naturaleza, estructura y trazabilidad de los criptoactivos en el contexto de la investigación y el análisis forense digital.

2) Investigación y formalización de procedimientos y herramientas para el seguimiento transaccional

Implica el estudio y la definición de procedimientos específicos y herramientas para rastrear y reconstruir el flujo de transacciones (on-chain y off-chain) que involucran criptomonedas y criptoactivos. Su finalidad es establecer criterios de actuación homogéneos que permitan mejorar la trazabilidad y correlación de operaciones a lo largo de la cadena de bloques.

3) Análisis e identificación de nuevas modalidades delictivas asociadas a criptoactivos

Orienta la investigación hacia la detección, clasificación y comprensión de las tipologías delictivas emergentes vinculadas con el uso de criptoactivos, como fraudes, estafas, esquemas de lavado de activos o financiamiento ilícito. Incluye la evaluación de técnicas, actores, patrones de comportamiento y dinámicas de operación que permitan fortalecer la detección temprana y la trazabilidad en el ámbito forense, contribuyendo a la formulación de protocolos de actuación y prevención.

4) Identificación y estudio de métodos antiforenses

Abarca la identificación, análisis y documentación de técnicas antiforenses utilizadas por los ciberdelincuentes para evadir o dificultar la acción de los investigadores. Se consideran herramientas de anonimización, uso de mixers, tumblers, servicios de ofuscación, entre otros mecanismos que alteran la visibilidad de las transacciones o la recuperación de evidencia digital. Incluye la actualización continua de repertorios de amenazas y tipologías antiforenses emergentes.

5) Definición y validación de procedimientos y herramientas forenses aplicables

Consiste en la revisión, selección y validación de metodologías y soluciones tecnológicas aplicables al análisis digital y la investigación de ciberdelitos y cibercrimen vinculados con criptoactivos. Incluye la evaluación comparativa de plataformas de trazabilidad blockchain, software de análisis forense y metodologías de investigación digital, promoviendo la estandarización y compatibilidad entre laboratorios e instituciones.

Tareas Principales de la Metodología

1) Identificación y clasificación de potenciales elementos de prueba digital (PEP) asociados a criptoactivos.

Consiste en la detección, reconocimiento y categorización de indicios o elementos digitales vinculados con criptoactivos que puedan constituir potenciales evidencias en una investigación judicial. Incluye el relevamiento de dispositivos físicos y virtuales —como billeteras frías o calientes, registros de transacciones, equipos de minería, aplicaciones de intercambio (exchanges), y documentación asociada a claves o frases semilla. Esta etapa permite establecer una primera delimitación del alcance de la evidencia, diferenciando entre datos on-chain y off-chain, y asegurando la preservación inicial de la integridad y trazabilidad de la información.

2) Análisis forense y trazabilidad de transacciones con criptoactivos

Tareas orientadas a la aplicación de técnicas de análisis forense digital y trazabilidad en redes blockchain, con el fin de reconstruir el flujo de operaciones y determinar el origen, destino y posible vinculación de los criptoactivos con actividades ilícitas. Se propone emplear una combinación de herramientas de software libre y plataformas comerciales de trazabilidad —como *Chainalysis Reactor* o *TRM Labs*— para el manejo de grandes volúmenes de datos, la detección de patrones transaccionales, la identificación de clusters de direcciones y el rastreo de fondos a través de mixers o servicios de ofuscación. Asimismo, se integran técnicas de OSINT y análisis de información on-chain y off-chain, garantizando la

consistencia metodológica, la documentación del proceso y la preservación de la cadena de custodia digital.

3) Resguardo, preservación y documentación de la evidencia digital.

Comprende el conjunto de procedimientos destinados a asegurar la integridad, autenticidad y trazabilidad de los potenciales elementos de prueba digital (PEP) vinculados a criptoactivos y criptomonedas. Se establecen pautas de recolección, etiquetado, almacenamiento y registro documental que garanticen la cadena de custodia digital durante todas las etapas del proceso forense. La preservación incluye tanto los datos *on-chain* como *off-chain*, así como la protección de metadatos y claves criptográficas asociadas a billeteras o transacciones.

4) Presentación y comunicación de resultados periciales.

Esta fase final se orienta a la elaboración y presentación de informes técnicos periciales que documenten de manera clara, precisa y verificable el proceso de análisis forense realizado sobre los criptoactivos y criptomonedas. Incluye la descripción de los procedimientos aplicados, las herramientas utilizadas, los hallazgos relevantes y las conclusiones obtenidas, en un formato que garantice su comprensión tanto por especialistas técnicos como por autoridades judiciales. El informe debe reflejar el cumplimiento de las normas y protocolos vigentes, mantener la trazabilidad de la evidencia y respaldar la validez técnica, jurídica y probatoria de los resultados.

A partir de la definición de esta metodología adecuada a ForenseUDE se plantea la actualización de los procedimientos y herramientas del Laboratorio Informático Forense (LabIF-UNLaM) para llevarse a cabo pericias informáticas de casos vinculados a criptoactivos y criptomonedas.

VI. Riesgos delictivos asociados al uso de Criptomonedas y Criptoactivos

Así como el mercado criptoactivos y criptomonedas ha crecido y continúa creciendo a pasos agigantados en todo el mundo, en forma paralela, desafortunadamente, también se optimizaron las maniobras delictivas en este innovador ámbito, donde su desregulación, su masiva proliferación o el uso de diversas tecnologías traen aparejados nuevos riesgos, al crear nuevas oportunidades de actividades ilícitas.

Por un lado, nos encontramos con usuarios atraídos, interesados en explorar sus posibles beneficios sociales y económicos, pero también con individuos que desnaturalizan su propósito y evalúan alternativas para explotar la tecnología en el marco de actividades ilícitas.

Las criptos presentan incontables casos de uso beneficiosos para nuestra sociedad. Sin embargo, también es importante destacar que pueden ser utilizadas para cometer distintos tipos de actividades ilícitas. El riesgo de ser víctima de fraude es muy alto, ya que los estafadores a menudo tienen la ventaja en este entorno digital.

Entre los principales delitos se encuentran: estafas con criptomonedas, evasión fiscal, lavado de dinero, coerción y chantaje, especulación, tiendas de dudosa reputación en la dark web, ataques de ransomware/malware, pornografía, fraudes en línea, identidades falsificadas, tráfico de drogas ilegales, financiamiento de organizaciones terroristas o criminales, criminalidad organizada, entre otros.

En todos estos casos los ciberdelincuentes suelen utilizar criptodivisas para dificultar el rastreo y anonimizar sus transacciones. El alto valor económico de estos activos digitales los hace atractivos para todo tipo de delitos, entre ellos los patrimoniales.

Dada su naturaleza digital, las "apropiaciones" de criptomonedas revisten la forma de ataques a los sistemas informáticos de sus tenedores, ya sean empresas o individuos, para lograr tomar el control del sistema y transferir estos bienes digitales a cuentas propias.

La capacidad de realizar operaciones transfronterizas rápidamente y a través de internet no solo permite a los criminales adquirir, mover y almacenar activos digitalmente, a menudo fuera del sistema financiero regulado, sino que también posibilita disfrazar el origen o destino de los recursos, dificultando que los sujetos obligados identifiquen de manera oportuna las actividades sospechosas. Estos factores añaden obstáculos a la detección e investigación de la actividad criminal.

Los casos más frecuentes de comisión de delitos que involucran a las criptomonedas son los de “Ransomware”. Estas son situaciones de ataques informáticos donde se encriptan todos o parte de los archivos de un ordenador o sistema informático de la entidad atacada, ya sea una persona física o una empresa, donde el atacante sólo desencriptará los archivos a cambio de un pago, generalmente en criptomonedas.

En línea con este tipo de ataques informáticos, otra táctica común es la introducción de malware en otros dispositivos. Esto permite que el dispositivo participe sin saberlo en un esquema de minería. Las criptomonedas generadas a través de este malware son dirigidas hacia el ciberdelincuente que infectó el dispositivo, resultando en una suerte de "hurto de uso", aprovechando el tiempo de procesamiento de los sistemas afectados. Además, las criptomonedas son utilizadas como medio para cometer delitos relacionados con la prevención de lavado de activos y el financiamiento del terrorismo, entre otros.

La investigación criminal ligada a los criptoactivos cobra un rol preponderante. Investigar actividades delictivas relacionadas con criptoactivos puede resultar complejo, ya que muchos casos podrían estar vinculados con compras realizadas o fondos transferidos a través de la cadena de bloques. Por lo tanto, resulta vital comprender con precisión cómo se preparan, transmiten, procesan y almacenan estas transacciones.

A esto se suma las “billeteras virtuales” o “monederos virtuales” (wallets) de las cuales existen una gran variedad de implementaciones y permiten almacenar las claves privadas para que los activos virtuales sean seguros y accesibles. Son aplicaciones o software que permite a los usuarios administrar sus criptomonedas y realizar transacciones. Una billetera virtual no almacena criptoactivos, pero sí hará referencia a cualquier transacción en la cadena de bloques que se pueda

vincular con las claves privadas gestionadas por intermedio de esta. En este sentido cabe distinguir las billeteras virtuales de las aplicaciones provistas por diferentes plataformas privadas que proveen servicios de arbitraje y/o compraventa de criptoactivos, conocidas comúnmente como "Exchanges".

Existen monederos con almacenamiento en frío (Cold storage), lo cual alude a los monederos que no están conectados a Internet, como los monederos físicos o de papel. La finalidad de las variantes de "almacenamiento en frío" es ofrecer protección contra el hackeo o robo de las criptomonedas. En contraposición, los monederos con almacenamiento en caliente funcionan online, es decir, con conexión a Internet. Debido a ello, esta forma de almacenamiento es más vulnerable a la piratería/robo que el almacenamiento en frío.

VII. CONCLUSIONES

Disponer de una metodología integral para el análisis y resguardo de posibles elementos de prueba digital asociados a criptomonedas y criptoactivos, fortalece la eficacia y la confiabilidad de los procedimientos forenses a aplicar en pericias informáticas, asegurando que se generen resultados técnica y legalmente válidos.

Dicha metodología puede ser aplicada en organismos judiciales, fuerzas de seguridad, por parte de peritos informáticos en sus diferentes roles y en otros laboratorios de informática forense nacionales e internacionales.

Asimismo, favorece la futura cooperación entre laboratorios de diferentes organismos y entidades, tanto nacionales como internacionales, al generar una mayor confiabilidad y aceptación del trabajo pericial y los resultados obtenidos.

REFERENCIAS

[1] Unidad de Información Financiera (UIF), *Resolución 300/2014 – Monedas* Virtuales, Buenos Aires, Argentina, 2014. [En línea]. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm

[2] Grupo de Acción Financiera de Latinoamérica (GAFILAT), "Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales". GAFILAT, 2021. [En línea]. Disponible en: https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guía-sobre-aspectos-relevantes-y-pasos-apropiados-para-la-investigación-identificación-incautación-y-decomiso-de-AV.pdf

[3] Comisión Nacional de Valores, "Resolución General 994/2024 – Registro de Proveedores de Servicios de Activos Virtuales (PSAV)", Boletín Oficial de la República Argentina, 25-Mar-2024. [En línea]. Disponible en: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-994-2024-397598

[4] Grupo de Acción Financiera Internacional (GAFI), *Las* Recomendaciones del GAFI – Estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y la proliferación (Feb. 2012). [En línea]. Disponible en: https://www.mpf.gob.ar/dafi/files/2017/03/GAFI-Recomendaciones.pdf

[5] Consejo de Europa, Convenio sobre Ciberdelincuencia (Convenio de Budapest), Budapest, 23 de noviembre de 2001. [En línea]. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[6] Consejo de Europa, Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia relativo a la mejora de la cooperación y la revelación de pruebas electrónicas, Estrasburgo, 12 de mayo de 2022. [En línea]. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/224

[7] Ministerio Público Fiscal de la Nación, "Guía Práctica para la Identificación, Trazabilidad e Incautación de Criptoactivos". Dirección de Comunicación Institucional, Buenos Aires, Argentina, 2023. [En línea]. Disponible en: https://www.fiscales.gob.ar/wp-content/uploads/2023/05/Informe_Criptoactivos-1.pdf

[8] Ministerio de Seguridad de la Nación, Dirección de Investigaciones del Ciberdelito, "Protocolo para la Identificación, Recolección, Preservación, Procesamiento y Presentación de Evidencia Digital", Resolución N.° 232/2023. Buenos Aires, Argentina, 2023. [En línea]. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/380000-384999/382307/res232.pdf

[9] C. V. Gioia, J. Eterovic, M. J. Krajnik y E. A. Zárate, "Marco de referencia para la implementación y gestión de Laboratorios de Informática Forense", en CADI 2021 – 5.º Congreso Argentino de Ingeniería, Universidad de Buenos Aires (UBA), Buenos Aires, Argentina, 2021.

[10] C. V. Gioia, E. A. Zárate, M. L. Giménez, M. J. Krajnik y J. E. Eterovic, "Metodología de Informática Forense Universal ForenseUDE", en VI Info-Conf 2022, Universidad FASTA, Mar del Plata, Argentina, p. 51, 2022. [En línea]. Disponible en: https://info-lab.org.ar/extension/info-conf;https://drive.google.com/file/d/1wKJqVbb3vD9ihLyHCWFDuq_km3GxbhQs/view

[11] A. H. Di Iorio, M. Castellote, C. Bruno y J. Waimann, El Rastro Digital del Delito. Mar del Plata, Argentina: Universidad FASTA, Info-Lab, 2017.

[12] A. H. Di Iorio, Guía Integral de Empleo de la Informática Forense en el Proceso Penal, 1.ª ed. Mar del Plata, Buenos Aires, Argentina: Universidad FASTA, 2015. [En línea]. Disponible en: https://info-lab.org.ar/descargas/libros-y-guias

[13] Electronic Discovery Reference Model (EDRM), EDRM Model, 2020. [En línea]. Disponible en: http://www.edrm.net

[14] International Organization for Standardization (ISO), Sitio oficial de la Organización Internacional de Normalización. [En línea]. Disponible en: https://www.iso.org/home.html

[15] M. J. Krajnik, E. A. Zárate, y C. V. Gioia, Implementación de Laboratorios de Informática Forense en base a la norma IRAM/ISO/IEC 17025:2017, ReDDI – Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza, vol. 2, no. 1, ISSN 2525-1333, Univ. Nac. de La Matanza, Buenos Aires, Argentina, 2024. [En línea]. Disponible en: https://reddi.unlam.edu.ar/index.php/ReDDi/article/download/241/434/

[16] M. J. Krajnik, E. A. Zárate, y C. V. Gioia, Requisitos de Infraestructura Edilicia y Tecnológica de Base para la Implementación de Laboratorios de Informática Forense, ReDDI – Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza, vol. 8, no. 2, ISSN 2525-1333, Univ. Nac. de La Matanza, Buenos Aires, Argentina, 2023. [En línea]. Disponible en: https://reddi.unlam.edu.ar/index.php/ReDDi/article/download/215/394/

[17] Chainalysis Inc., Blockchain Data Platform, [En línea]. Disponible en: https://www.chainalysis.com/

[18] TRM Labs Inc., Blockchain Intelligence for Stablecoin Risk Management / Crypto Investigation, Compliance & Risk Solutions, [En línea]. Disponible en: https://www.trmlabs.com/

[19] United States v. Sterlingov, Case No. 1:21-cr-00399, U.S. District Court for the District of Columbia, 2023. [En línea]. Disponible en: https://storage.courtlistener.com/recap/gov.uscourts.dcd.239226/gov.uscourts.dcd.239226.141.0.pdf

[20] United States v. Larry Dean Harmon, Case No. 1:19-cr-00395, U.S. District Court for the District of Columbia, 2021. [En línea]. Disponible en: https://www.justice.gov/opa/pr/operator-darknet-based-cryptocurrency-mixing-service-pleads-guilty