CIJur Centro de Información Jurídica
www.cijur.mpba.gov.ar/doctrina
ISSN 3008-718X

# ASPECTOS VINCULADOS A LA PRUEBA EN CASO DE REGISTROS EN BLOCKCHAIN Y CRIPTOACTIVOS

*Alejandro Batista (*)*

## SUMARIO



## 1. INTRODUCCIÓN

La evolución tecnológica ha transformado la forma en que vivimos, trabajamos y nos relacionamos. Dentro de este panorama, blockchain y los criptoactivos emergen como herramientas que plantean nuevos desafíos y oportunidades para el Derecho. La velocidad de las transacciones, la ausencia de una autoridad central y la posibilidad de ofrecer registros inmutables son solo algunos de los rasgos que impulsan su creciente utilización y los ponen bajo la lupa de los operadores jurídicos.

En el ámbito probatorio, donde resulta vital contar con evidencias sólidas y confiables, blockchain y los criptoactivos pueden constituir tanto la fuente de la prueba (por ejemplo, en caso de lavado de activos o estafas) como la propia herramienta para robustecer y garantizar la integridad de la evidencia digital. Por ello, comprender los fundamentos técnicos y jurídicos de esta tecnología es fundamental para una adecuada defensa, acusación o juzgamiento en materia penal y, por extensión, en cualquier rama del Derecho.

## 2. QUÉ ES LA TECNOLOGÍA BLOCKCHAIN

### Definición básica

Blockchain puede describirse como un "libro de contabilidad" o una "base de datos" distribuido en una red de nodos interconectados que valida y registra transacciones de forma secuencial, asegurando que, una vez incluidas en un bloque, la información no pueda alterarse sin que todo el sistema lo detecte.

Así podemos señalar las siguientes características:

- **Descentralización**: No existe una autoridad central o única que controle los datos; los nodos (participantes en la red) comparten la responsabilidad de validarlos. Esto le proporciona a la red una seguridad y resistencia a los ataques que las redes centralizadas no tienen.

- **Inmutabilidad**: Una vez agregados los datos en un bloque, cualquier modificación posterior altera todo el sistema, dejándola al descubierto.

- **Transparencia (en blockchains públicas)**: Cualquiera puede acceder a los registros y verificar transacciones, lo que hace posible rastrear la actividad realizada, así como obtener trazabilidad de las mismas y cómo ello establecer una cronología.

- **Seguridad criptográfica**: Cada bloque se vincula al anterior mediante procedimientos criptográficos (hashes) que garantizan la autenticidad del registro y evitan la manipulación.

En consecuencia, la tecnología blockchain ofrece un medio idóneo para registrar operaciones de forma confiable, proporcionando trazabilidad y robustez en la integridad de la información.

**Aclaración:** Los trabajos de doctrina que se publican en el CIJur no representan necesariamente ni comprometen la opinión de la Institución.

## 3. QUÉ SON LOS CRIPTOACTIVOS

Los criptoactivos por su parte representan un abanico amplio de activos digitales basados en tecnología blockchain. Dentro de ellos se encuentran:

- **Criptomonedas**. Actúan como unidad de medida, medio de intercambio y reserva de valor (ej. Bitcoin o Ethereum). Funcionan de manera descentralizada, sin un banco central emisor.

- **Tokens.** Representan derechos, bienes o servicios en un entorno digital. Pueden ser de ***utilidad*** (servicios dentro de una plataforma), de **seguridad** (similares a acciones o bonos), de ***gobernanza*** (otorgan derecho a voto en un proyecto) o ***no fungibles*** (NFT), utilizados para representar activos únicos (obras de arte digitales, coleccionables, etc.).

- **Stablecoins.** Criptomonedas diseñadas para minimizar la volatilidad de su precio, generalmente vinculadas al valor de una moneda fiduciaria (USDT, por ejemplo) u otros activos.

La **característica esencial** de los criptoactivos es el uso de la criptografía y la tecnología blockchain para garantizar su emisión, su transferencia y su control. Sin embargo, su **pseudonimato** puede facilitar el ocultamiento de la identidad de los operadores, lo cual tiene implicancias cruciales en materia penal (por ejemplo, para fines ilícitos como lavado de dinero). Una excepción a este pseudoanonimato se da cuando los usuarios se valen de *Exchanges Centralizados*[1], ya que en esos casos al tener que cumplir con políticas KYC[2], dichas empresas suelen requerir documentación que acredita la identidad de los titulares de las cuentas.

---

**1.** Un exchange centralizado (o CEX, por sus siglas en inglés) es una plataforma manejada por una empresa que permite comprar, vender o intercambiar criptomonedas. Funciona de forma parecida a un banco o casa de cambio: la empresa actúa como intermediaria, gestiona las operaciones y custodia tus fondos. Esto significa que tenés que confiar en esa empresa para que guarde bien tus criptomonedas y haga correctamente las transacciones. Algunos ejemplos conocidos son Binance, Coinbase o Kraken.

**2.** La política de KYC (siglas en inglés de Know Your Customer, que significa "Conocé a tu cliente") es una norma que obliga a las empresas —como bancos o exchanges de criptomonedas— a verificar la identidad de sus usuarios. Esto incluye pedir datos personales, documentos (como el DNI o pasaporte) y, a veces, una selfie. El objetivo es prevenir delitos financieros, como lavado de dinero o fraude, y asegurarse de que cada usuario sea una persona real y confiable.

Si hablamos en cambio de situaciones de *Exchanges Descentralizados*[3] o de autocustodia[4] de wallets[5] y claves, habrá que apelar a diferentes elementos de prueba que puedan aportar indicios sobre la posible identidad de las personas detrás de esas cuentas.

## 4. IMPORTANCIA PARA EL DERECHO Y MATERIA PROBATORIA

Las características descriptas, hacen de la tecnología blockchain una posibilidad interesante en materia probatoria. Veamos algunas alternativas.

### 4.1. Fuente de evidencia digital

Los registros de transacciones son una fuente muy importante. Toda operación con criptoactivos en una blockchain pública deja rastros (hashes, direcciones o wallets, sellos de tiempo). Estos datos pueden usarse para reconstruir flujos de fondos, probar la existencia de transacciones en un momento dado, etc.

De la misma manera las marcas de tiempo (timestamps), aportan la fecha cierta de realización de una operación, algo de inestimable valor para corroborar cronologías en investigaciones penales o civiles.

### 4.2. Nueva dimensión del delito y la prueba

Por otra parte, es evidente que surgen nuevas problemáticas. Entre ellas tenemos los delitos en los que intervienen criptoactivos. Por ejemplo, el lavado de dinero,

**3.** Un exchange descentralizado (o DEX, por sus siglas en inglés) es una plataforma que permite comprar, vender o intercambiar criptomonedas sin intermediarios, es decir, sin pasar por un banco o una empresa que controle la operación. Funciona a través de tecnología blockchain y contratos inteligentes, que son programas automáticos que se ejecutan cuando se cumplen ciertas condiciones. En lugar de confiar en una empresa para custodiar su dinero, en un DEX la persona el control total de tus fondos. Las operaciones se hacen entre personas directamente, de forma segura y transparente gracias a la tecnología.

**4.** Una billetera fría o autocustodiada es un tipo de billetera para guardar criptomonedas fuera de internet, lo que la hace más segura contra hackers. Al ser autocustodiada, significa que la propia persona tiene el control total de tus claves privadas (la "llave" que permite mover sus criptomonedas). Nadie más puede acceder a tus fondos, solo él. Suele ser un dispositivo físico, como un pendrive especial, o incluso puede ser un papel con códigos, siempre que no esté conectado a la red.

**5.** Wallet o billetera: herramienta que permite guardar, enviar y recibir criptomonedas mediante claves privadas. Puede ser caliente (conectada a internet), fría (sin conexión), custodial (la controla un tercero) o autocustodiada (la controla el usuario).

**Aclaración:** Los trabajos de doctrina que se publican en el CIJur no representan necesariamente ni comprometen la opinión de la Institución.

fraude inversor, estafas electrónicas, secuestro de información (ransomware) y financiación de actividades ilícitas son algunos ejemplos.

Esto a su vez da lugar a cuestiones de jurisdicción. Al ser un sistema descentralizado y transnacional, identificar el lugar donde ocurrió el hecho o al responsable de la operación puede ser complejo.

De la misma manera nos encontramos retos vinculados al anonimato y pseudonimato. Esto es así por cuanto las direcciones de blockchain (wallets) no tienen siempre un nombre asociado, por lo que se requerirá análisis forense y solicitud de datos a "exchanges" si los hubiera, así como otros elementos de prueba para la posible identificación de los titulares.

### 4.3. Aplicación práctica en la cadena de custodia

También puede pensarse el uso de blockchain para resguardar evidencia digital. Registrar la cadena de custodia en una plataforma blockchain permite asegurar la trazabilidad de los elementos probatorios (quién accede, cuándo y con qué finalidad).

A ello sumamos la inmutabilidad de la documentación probatoria. El sello de tiempo y los hashes asociados a cada evidencia impiden su alteración sin dejar rastro, reforzando la fiabilidad ante un tribunal.

### 4.4. Exámenes periciales en blockchain

Asimismo, necesitamos trabajar con peritajes especializados, teniendo en cuenta la complejidad técnica de esta tecnología. Por ende, resulta necesaria la intervención de expertos en criptoanálisis y en análisis de datos de blockchain.

Junto a estos expertos deberemos apelar a herramientas forenses, softwares y metodologías específicas para rastrear transacciones, identificar patrones sospechosos o establecer vínculos entre direcciones de blockchain y usuarios concretos.

## 5. CONTRATOS INTELIGENTES (SMART CONTRACTS) Y SU IMPACTO PROBATORIO

Los *smart contracts*[6] (o contratos inteligentes) son en realidad programas que se ejecutan de manera automática en una red blockchain cuando se cumplen determinadas condiciones preestablecidas. Pueden incorporar cláusulas legales y económicas que se activan sin mediación de terceros, reforzando la trazabilidad y disminuyendo la posibilidad de manipulación humana.

En materia probatoria tenemos que, dado que el contrato es software que funciona de forma autónoma, la mera ejecución o no ejecución de este, registrada en la blockchain, puede evidenciar la conducta de las partes.

Esto nos proporciona una fuente de trazabilidad de fondos y acciones. Cada paso o evento relevante queda plasmado en la cadena de bloques con su correspondiente sello de tiempo, lo que facilita la reconstrucción detallada de los hechos en un proceso judicial.

Estos contratos inteligentes pueden integrarse con otros sistemas. Ciertas plataformas permiten la interacción de los *smart contracts* con fuentes de datos externas llamados oráculos[7], ampliando su utilidad y aumentando la complejidad de su peritaje.

Estas posibilidades vienen acompañadas de nuevos desafíos legales, entre los cuáles podemos mencionar los siguientes:

**6.** Un smart contract o contrato inteligente es un programa que se ejecuta de forma automática cuando se cumplen ciertas condiciones, sin necesidad de intermediarios. Funciona dentro de una blockchain, lo que garantiza que no pueda modificarse ni detenerse una vez activado. Se usa para realizar acuerdos digitales de manera segura y transparente. Hay contratos inteligentes simples, que automatizan tareas básicas como transferencias en fechas determinadas; y otros más complejos, que permiten crear aplicaciones descentralizadas, servicios financieros sin bancos (DeFi), juegos, NFTs y más. También existen contratos inteligentes multifirma, que requieren la aprobación de varias personas para que se ejecuten, lo cual resulta útil en decisiones colectivas.

**7.** Un oráculo en el mundo de los smart contracts es un puente entre la blockchain y el mundo real.
Como los contratos inteligentes no pueden acceder por sí solos a información externa, el oráculo les envía datos del "mundo fuera de la blockchain", como precios, clima, resultados deportivos o cualquier otro dato necesario para que el contrato funcione. Es clave para que los smart contracts puedan tomar decisiones basadas en información actual y confiable.

**Aclaración:** Los trabajos de doctrina que se publican en el CIJur no representan necesariamente ni comprometen la opinión de la Institución.

- **Determinación de la jurisdicción.** Al no requerir de un ente central, se dificulta establecer el marco normativo aplicable cuando las partes y nodos involucrados están en distintas jurisdicciones.

- **Interpretación jurídica.** No todo contrato inteligente equivale a un "contrato legal" en sentido estricto; su validez y eficacia dependerán de si reúne los requisitos legales tradicionales (consentimiento, objeto lícito, etc.) o si se adecua a la normativa vigente.

- **Necesidad de peritos especializados.** La complejidad técnica y la programación de los smart contracts (por ejemplo, en lenguajes como Solidity) demandan peritos capaces de leer y auditar el código para determinar la intención de las partes y si hubo manipulación o errores en su ejecución.

## 6. CUESTIONES LEGALES Y REGULATORIAS

El marco jurídico que regula blockchain y criptoactivos varía según el país. Existen jurisdicciones que los consideran activos digitales sujetos a normativas de lavado de dinero y financiamiento del terrorismo (ej. controles KYC en los exchanges), mientras que en otros lugares hay mayor apertura o incluso prohibiciones parciales o totales.

De esta forma tenemos:

- **Reconocimiento legal**: Algunos países los reconocen como propiedad (con efectos tributarios, sucesorios, etc.).

- **Ausencia de regulación unificada**: Falta todavía una armonización internacional, lo que dificulta el accionar coordinado entre diferentes autoridades en casos transnacionales. Es el caso de Argentina.

- **Necesidad de protocolos claros**: Frente a estos nuevos mecanismos de prueba, se deben crear guías de buenas prácticas para evitar la exclusión de elementos probatorios por defectos formales o vacíos legales.

## 7. DESAFÍOS Y ESTRATEGIAS DE DEFENSA EN CASOS PENALES

Diferentes son los aspectos que habrá que considerar, cuando estemos en el marco de un proceso penal, por ejemplo:

- **Cadena de custodia**: Cualquier desprolijidad o vulneración en la recolección y preservación de evidencia digital puede dar lugar a nulidades y planteos de violación de garantías.

- **Impugnación de la integridad y autenticidad**: La defensa puede cuestionar la validez técnica de los peritajes, así como la fidelidad del método utilizado para la captura de la información de blockchain (herramientas, software, versiones obsoletas, etc.).

- **Falta de identificación del propietario real**: Las billeteras pueden pertenecer a terceras personas no vinculadas al imputado o utilizar identidades falsas (mulas digitales). El pseudonimato plantea interrogantes sobre la autoría real de la operación.

- **Exchanges y jurisdicción**: Si la plataforma de intercambio de criptomonedas se halla en otro país, la cooperación internacional o la ausencia de marcos regulatorios locales puede complicar la investigación y uso de la prueba.

## 8. CONCLUSIONES Y CONSIDERACIONES FINALES

A modo de cierre, podemos concluir que la tecnología blockchain nos presenta:

- **Relevancia creciente**: El uso de blockchain y criptoactivos no solo es un fenómeno financiero o tecnológico, sino un tema jurídico ineludible. Cada vez más casos penales y civiles involucran estos elementos, como fuente de evidencia o como parte del acto delictivo.

- **Robustez y confiabilidad**: En condiciones técnicas y legales adecuadas, el registro en blockchain ofrece altos niveles de fiabilidad (gracias a su inmuta-

**Aclaración:** Los trabajos de doctrina que se publican en el CIJur no representan necesariamente ni comprometen la opinión de la Institución.

bilidad y trazabilidad). También permite optimizar la cadena de custodia de la prueba, evitando manipulaciones.

- **Capacitación y actualización continua**: Para litigar de manera eficaz en un caso que involucre evidencia proveniente de blockchain o criptoactivos, es imprescindible que el abogado, el fiscal y el juez cuenten con conocimientos sólidos, o que se apoyen en peritos debidamente formados.

- **Desafíos regulatorios**: La heterogeneidad normativa y la complejidad propia de las redes globales demandan un trabajo de armonización y cooperación internacional que todavía está en desarrollo.

- **Oportunidades**: Más allá de los delitos asociados, blockchain puede servir para transparentar procedimientos y reforzar la seguridad de datos, lo que abre un abanico de mejoras posibles para el sistema de justicia.

En definitiva, blockchain y los criptoactivos plantean un nuevo paradigma tanto para la comisión de delitos como para la obtención y valoración de las pruebas electrónicas. Conocer sus fundamentos técnicos, normativos y probatorios resulta indispensable en la práctica jurídica contemporánea.

*(*) Abogado. Especialista en Derecho de Alta Tecnología. Magister en Finanzas Públicas. Doctorando en Sociología. Doctorando en Ciencias Jurídicas. Diplomado en Inteligencia Artificial y Derecho.*

*Director de la Diplomatura de Posgrado en Legaltech e IA. Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata.*

*Docente de Grado y Posgrado en la Universidad Nacional de La Plata y en la Universidad del Museo Social Argentino.*

*Director y Profesor en la Especialización en Blockchain, Blockchain, Smartcontracts y Criptocurrency, en Blockchain y la Transformación Digital de la Sociedad, y en Startups, Entrepreneurship y Fundraising Law en ADEN Business School.*

*Prosecretario de Políticas Digitales en la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata.*