

Identidad cifrada con descriptación judicial: una solución jurídica para la responsabilidad en entornos *blockchain*

Javier Martínez Boada
Universidad Camilo José Cela (Madrid)

Fecha de presentación: septiembre 2025

Fecha de aceptación: noviembre 2025

Fecha de publicación: marzo 2026

Resumen

La tecnología *blockchain* se posiciona como una de las tecnologías que mayor interés genera en la sociedad actual. Entre sus mayores atractivos se encuentran las características que aporta a las transacciones que efectúan los usuarios en sus sistemas; sin embargo, junto a sus ventajas, también emergen inconvenientes que pueden poner en jaque los ordenamientos jurídicos tal y como están pensados actualmente. En este sentido, la anonimidad con la que son capaces de actuar los usuarios en algunas *blockchain* dificulta la aplicación del derecho, lo que plantea la necesidad de ofrecer alternativas como la implantación de una identidad cifrada que pueda revelarse en determinadas circunstancias y situaciones para garantizar la seguridad jurídica y el cumplimiento de las normas.

Palabras clave

blockchain; identidad; tecnología; anonimidad; derecho

Encrypted identity with judicial decryption: a legal solution for liability in Blockchain environments

Abstract

Blockchain technology is considered one of the most intriguing innovations in today's society. Its key appeal lies in the unique features it offers for user transactions within its systems. However, alongside its benefits, there are also disadvantages that could pose risks to current legal frameworks. In this context, the anonymity that enables users to operate in some Blockchains complicates the application of existing laws. This highlights the need for alternatives, such as implementing an encrypted identity that can be disclosed under certain circumstances to ensure legal certainty and rule compliance.

Keywords

blockchain; identity; technology; anonymity; law

Introducción

Actualmente, las nuevas tecnologías están acaparando el interés del conjunto de la sociedad. Entre ellas, la tecnología *blockchain*, de la cual se espera que durante este año 2026 las transacciones efectuadas en sus sistemas alcancen los 19.900 millones de dólares a nivel mundial, se posiciona como uno de los sistemas más disruptivos, no solo por su capacidad para descentralizar procesos y garantizar la integridad de la información contenida en el sistema, sino también por los desafíos jurídicos y éticos que puede llegar a plantear (Zhang, Xue y Liu, 2019, pág. 2).

Originalmente, la *blockchain* fue creada como base técnica para la criptomoneda Bitcoin con el propósito de evitar el doble gasto en este sistema desarrollado por Satoshi Nakamoto. Gracias a su evolución tecnológica y funcional, la *blockchain*, que inicialmente servía como base de datos distribuida para registrar transacciones, dio paso a las versiones 2.0 y 3.0, lo que la transformó en una infraestructura transversal con aplicaciones en sectores tan diversos como las finanzas, la salud, la energía, la logística, las ciudades inteligentes y la industria 4.0 (Martínez Boada y Rejas Muslera, 2024, pág. 6).

Sin duda, el desarrollo tecnológico y funcional de la *blockchain* permite a los usuarios efectuar transacciones como nunca antes habían imaginado; sin embargo, estos avances no están exentos de desafíos (Torres Cazorla, 2019, pág. 94).

Uno de los más significativos es la dificultad para compatibilizar algunas características técnicas de *blockchain*, como el anonimato, con los marcos jurídicos existentes. En este sentido, dentro de las redes *blockchain*, la información fluye de forma descentralizada y los participantes pueden operar sin revelar su identidad real, lo que genera un entorno ideal para preservar la privacidad, pero, por contrapartida, también puede facilitar conductas ilícitas de difícil persecución, pues si no puede conocerse la identidad digital real de los sujetos, difícilmente podrán aplicarse las normas y atribuir responsabilidades (Andola, Raghav, Yadav, Venkatesan y Verma, 2021, pág. 1).

La capacidad que tienen los usuarios en *blockchain* para actuar de forma intrazable utilizando seudónimos que impiden conocer su identidad plantea serias preocupaciones al mundo jurídico, ya que impide, en diversos casos, la aplicación efectiva de los ordenamientos jurídicos. De este modo, deviene imprescindible la propuesta de algún tipo de mecanismo que permita compatibilizar el atractivo que supone la privacidad que poseen los usuarios dentro de los sistemas *blockchain* con la posibilidad de identificarles cuando ocurran actividades ilícitas o, sin ocurrir estas, algún usuario desee entablar acciones legales contra otro por no haber visto respetados sus derechos e intereses (Sun Yin, Langenheldt, Harlev, Mukkamala y Vatrappu, 2019, pág. 37).

La solución no debe consistir simplemente en desmantelar las características básicas de esta tecnología, como,

por ejemplo, prohibir aquellos sistemas en los que no existan identidades tasadas, sino que deben desarrollarse mecanismos o estrategias que permitan equilibrar los caracteres atractivos de la *blockchain* y los derechos y obligaciones de los usuarios.

Ante esta situación, surge la propuesta de implementar dentro de las estructuras *blockchain* un sistema de identidad cifrada capaz de ser descifrado cuando existan condiciones judiciales o legales debidamente autorizadas que lo justifiquen. En este sentido, lo que se busca es continuar garantizando el anonimato en *blockchain* protegiendo la identidad de los usuarios mediante técnicas de cifrado robustas, de manera que dicho anonimato se mantenga en condiciones normales de uso, pero se pueda acceder a su información identificativa bajo condiciones determinadas y con autorización judicial.

1. Panorama general de *blockchain*

1.1. Definición de *blockchain*

Hoy por hoy, no existen normas que se encarguen de definir en qué consiste la tecnología *blockchain* y qué modalidades pueden encontrarse o utilizar los usuarios. En el caso de España, tan solo disponemos de la Proposición de Ley 122/000148 para la Transformación Digital de España¹ que, como la propia palabra indica, únicamente es una declaración de intenciones, pues carece de fuerza normativa al no haber sido debidamente aprobada (Martínez Boada, 2025).

Como ya se ha adelantado, la tecnología *blockchain* emergió durante el año 2008 como el sistema que almacenaba la información de las transacciones efectuadas dentro del protocolo bitcoin con el fin de evitar el doble gasto, pues, sin un registro que archivase las transacciones, los usuarios podían utilizar y gastar las monedas de forma ilimitada (De Filippi y Wright, 2018, pág. 205).

De este modo, y según establece la doctrina, inicialmente *blockchain* fue el sistema que permitió el funcionamiento de la criptomoneda Bitcoin (Ammous, 2016, pág. 1). Sin embargo, es una innovación relativamente reciente que ha cobrado protagonismo en los últimos años, pues ha

extendido su uso más allá de las criptomonedas y, por lo tanto, su definición podría variar (Rayenizadeh y Rafsanjani, 2025, pág. 3).

Como se puede observar, la definición de *blockchain* va a depender de la funcionalidad a la que se destine el sistema, por lo que, brevemente a continuación, deberá estudiarse la evolución que ha sufrido esta tecnología y cómo, en consecuencia, varía su concepto (Zile y Strazdina, 2018).

La tecnología *blockchain* ha pasado por tres generaciones denominadas Blockchain 1.0, 2.0 y 3.0, en las que ha sufrido diferentes evoluciones que han variado la manera de concebir este tipo de sistemas (Xu, Chen y Kou, 2019).

Las Blockchain 1.0 se destinaban a almacenar datos y servir como libros de contabilidad distribuidos en los que se registrasen las informaciones de las transacciones de los usuarios, siendo el ejemplo más claro Bitcoin. Posteriormente, surgen las Blockchain 2.0, en las que se va a permitir codificar programas informáticos denominados *smart contracts*, lo que permite observar que la definición de estos sistemas irá un paso más allá de una simple base de datos distribuida. Por último, emergen las Blockchain 3.0 que, sin implementar funcionalidades específicas, permiten a los usuarios utilizar este tipo de ecosistemas en diversos sectores (Sarmah, 2018, pág. 26).

Ante tal evolución, podrá decirse que, dependiendo de cada sistema, la definición podrá variar. Por un lado, existen aquellos que la definen como una base de datos distribuida para registrar informaciones de cualquier tipo (Ibáñez Jiménez, 2018, págs. 36-37). Por otro, quienes la entienden como una enorme computadora mágica en la que pueden codificarse condiciones preestablecidas que, en caso de cumplirse, despliegan unos efectos jurídicos (Davidson, De Filippi y Potts, 2016, pág. 6).

1.2. Estructuras y modalidades de *blockchain*

Junto a la gran variedad de definiciones que puede adoptar esta tecnología, también debe prestarse atención a los tipos de sistemas que pueden constituirse. De igual modo, fruto de los avances tecnológicos que han sufrido estos

1. Vid. Congreso de los Diputados. *Proposición de Ley para la Transformación Digital de España*. BOCG-14-B-173-1. 14.ª Legislatura. https://www.congreso.es/public_oficiales/L14/CONG/BOCG/B/BOCG-14-B-173-1.PDF

sistemas, además emergen nuevos entornos con permisos y características diferentes.

Inicialmente, la *blockchain* fue creada para ser un sistema público, abierto y descentralizado en el que los usuarios pudieran transaccionar bajo seudónimos que dificultaran trazar su identidad o, incluso, si se diseñaban expresamente para ello, ser totalmente anónimas (Preukschat y Kuchkovsky, 2017, pág. 27).

Posteriormente, surgen otros entornos que dan lugar, principalmente, a tres tipos de sistemas: públicos, privados e híbridos (Tourinho Pena *et al.*, 2022, pág. 16).

Según la doctrina, los entornos *blockchain* públicos pueden estar diseñados para ser completamente anónimos. En los sistemas privados, los usuarios normalmente se encuentran debidamente identificados, y los accesos y permisos se encuentran centralizados en una autoridad central; sin embargo, pueden existir entornos privados en los que los usuarios puedan actuar desde el anonimato, si así ha sido diseñado el sistema. En cuanto a los sistemas híbridos, estos combinan características tanto de la *blockchain* pública como de la privada, lo que hace posible configurar el entorno para que los usuarios operen también de manera anónima (Preukschat y Kuchkovsky, 2017, págs. 28-30).

Como puede observarse, a este estudio le interesan todas aquellas arquitecturas *blockchain* que han sido diseñadas para actuar de forma anónima con independencia de su tipología, pues, como ya se ha dicho, cualquiera de los entornos puede haber sido diseñado para que se desconozca la identidad digital fehaciente de los usuarios que operan en este.

2. Características de la tecnología *blockchain*: especial alusión a la anonimidad

La tecnología *blockchain* posee diversos atributos que la diferencian de cualquier otro sistema y que atraen los intereses del conjunto de la sociedad. En general, la doctrina mantiene que las características de *blockchain* son la autonomía, la independencia, la distribución, la inmutabilidad, la seguridad, la transnacionalidad, la rapidez y el pseudoanonimato o anonimato en función del sistema

o la intención de los usuarios (Bedecarratz Scholz, 2018, págs. 86-69).

Conviene explicar brevemente cada una de ellas con la finalidad de que el lector entienda los grandes atractivos de este tipo de sistemas y comprenda por qué la tecnología *blockchain* ha despertado tanto interés en diversos sectores.

2.1. Desintermediación

La autonomía o desintermediación permite a los usuarios actuar sin depender de ningún tipo de intermediario o autoridad central. En este sentido, cada nodo actúa de manera independiente cumpliendo con las normas preestablecidas del protocolo, lo que garantiza la confianza entre los usuarios de la red y posibilita que no existan autoridades que regulen sus actuaciones (Pinto Arboleda, Fajardo Bravo, Ortega Mènde, Zambrano Toapanta y Zambrano Recalde, 2025, pág. 500).

2.2. Independencia

La independencia se encuentra estrechamente relacionada con la característica anterior; sin embargo, se centra en la autogestión que poseen los nodos dentro de la red. A este respecto, cada usuario es dueño de sus activos digitales y de su información sin depender de terceros que validen sus transacciones o custodien sus datos (Bedecarratz Scholz, 2018, pág. 86).

2.3. Rapidez

Asimismo, la tecnología *blockchain* aporta rapidez a las transacciones de los usuarios debido a la eficiencia con la que se pueden validar y registrar estas sin la intervención de intermediarios. Aunque el tiempo de confirmación varía según el protocolo y la congestión de la red, en comparación con sistemas tradicionales de transferencia de valor, especialmente en contextos transfronterizos, *blockchain* suele ofrecer mayor velocidad y disponibilidad, incluso operando fuera del horario bancario convencional (Rueda Castañeda, Gallego Gómez, Estanling Cárdenas, Tello y García Pineda, 2024, pág. 10).

2.4. Distribución

La distribución en *blockchain* permite que la información se replique en múltiples nodos, lo que garantiza que todos

accedan al mismo registro, reforzando la transparencia y eliminando un único punto de fallo, lo que, a su vez, incrementa la seguridad (Yaroshenko, Puntus, Chanysheva, Moskalenko y Sliusar, 2025, pág. 248).

2.5. Inmutabilidad

Toda vez que las transacciones se han validado y añadido a la *blockchain*, se vuelven inmutables debido al uso de funciones criptográficas de *hash*² y la estructura encadenada de los bloques. En otras palabras, los datos no pueden ser alterados, modificados ni eliminados sin el consenso de la mayoría de la red, lo que ofrece un alto grado de confianza y veracidad a la información almacenada (Hofmann, Wurst, Ron y Böhmecke-Schwafert, 2017, pág. 1).

2.6. Seguridad

Cuando los usuarios eligen utilizar *blockchain* para efectuar sus transacciones, es, entre otras cuestiones, por la seguridad que garantiza este tipo de sistemas. Esta seguridad se sustenta en algoritmos criptográficos avanzados y protocolos de consenso, que dificultan enormemente la alteración de registros o la creación de transacciones fraudulentas (Zhang y Lee, 2020, págs. 94-95).

2.7. Transnacionalidad

La tecnología *blockchain* contribuye a la eliminación de barreras geográficas, regulatorias e institucionales, lo que facilita la interacción directa entre personas y promueve la interoperabilidad entre países y sistemas (Padilla Sánchez, 2020, pág. 187).

2.8. Anonimidad

Como característica más interesante para este estudio, debe destacarse la anonimidad con la que los usuarios pueden actuar dentro de este tipo de sistemas (Huang, Zhang, Mu, Rezaeibagha y Du, 2021, pág. 25).

Precisamente, esta característica genera diversas cuestiones que van más allá de lo meramente tecnológico, abriendo un amplio debate en el ámbito jurídico acerca de la identificación de los intervinientes, la atribución de

responsabilidades y la adecuación de estos sistemas a las normativas vigentes en materia de protección de datos, prevención del delito y cumplimiento legal.

En lo que respecta a las normativas sobre protección de datos, la anonimidad y desintermediación que caracteriza a los sistemas *blockchain* imposibilitan enormemente el cumplimiento de las obligaciones de protección de datos como la existencia obligatoria de los denominados responsables del tratamiento y encargados de tratamiento. Al operar sin intermediarios y bajo un modelo descentralizado y anónimo, estos sistemas desdibujan algunas figuras tradicionales previstas en los marcos regulatorios, lo que genera vacíos y desafíos que exigen nuevas soluciones jurídicas (Fink, 2019, pág. 91).

Como puede observarse, aun sin intermediarios ni autoridades, como se viene diciendo, dentro de *blockchain* no existen jerarquías, podrían establecerse estas dos figuras esenciales. Sin embargo, aun existiendo, los nodos no sabrían a quién acudir para ejercer sus derechos de acceso, rectificación, cancelación u oposición, pues, al actuar de forma anónima, se desconocen los datos de identificación de los usuarios y no se puede saber qué usuario asume el papel de responsable o encargado de tratamiento (Pardo Prado, 2022, págs. 153-160).

Por contraparte, puede pensarse que, si los usuarios actúan de forma anónima, la legislación de protección de datos no entra en juego debido a que un dato debidamente anonimizado no se encuentra sujeto a las disposiciones sobre protección de datos por no poderse atribuir a ninguna persona concreta. Sin embargo, sí quedan registrados datos de transacciones asociadas a los usuarios y, en algunas ocasiones, pueden llegarse a vincular a personas concretas, como, por ejemplo, mediante el uso de su dirección IP u otros datos adicionales.

Como ya se ha señalado, en ciertos casos puede llegarse a identificar a los usuarios mediante el uso de información adicional; sin embargo, la anonimidad con la que se actúa en *blockchain* dificulta enormemente, en la gran mayoría de supuestos, la determinación del autor real que se entromete dentro de los derechos e intereses del resto de usuarios (Gimeno Beviá, 2023, pág. 6).

2. Una función *hash* es un algoritmo que convierte datos de cualquier tamaño en una cadena única de longitud fija, lo que permite verificar su integridad al detectar cualquier modificación. Vid. González González, 2015, pág. 172.

Adicionalmente, el uso de la tecnología *blockchain* no se encuentra exenta de riesgos, debido a que su estructura puede utilizarse también como mecanismo para cometer delitos, incumplir obligaciones contractuales o vulnerar derechos como, por ejemplo, la propiedad. En este contexto, *blockchain* no escapa a la posibilidad de originar conflictos de naturaleza social o jurídica, tanto en el ámbito privado como en el público, derivados de su uso o de las actividades que en ella se desarrollen (Gimeno Beviá, 2023, pág. 2).

Ante esta situación, la anonimidad desempeña un papel fundamental, ya que puede favorecer la comisión de dichas actuaciones ilícitas y contrarias a los derechos e intereses de las personas, pues, si se desconoce al autor verdadero de los hechos, se dificulta enormemente la atribución de responsabilidades y la posibilidad de emprender cuantas acciones legales sean necesarias. En este sentido, surge la duda de cómo los usuarios van a ser capaces de reclamar responsabilidades ante un entorno anónimo en el que se desconocen las identidades de los usuarios y en el que no hay autoridades centrales que velen por el cumplimiento normativo y el respeto de los derechos e intereses de las personas (Calaza López *et al.*, 2023, págs. 3-5).

A su vez, las transacciones en *blockchain* son transnacionales, lo que permite operar sin fronteras y puede implicar la aplicación del derecho internacional, público o privado, según la naturaleza de las partes involucradas (Ortega Giménez, 2019, pág. 60).

Actualmente, las normas que se encargan de regular los fueros de competencia en caso de conflicto entre usuarios, en los que al menos uno de ellos sea de carácter extranjero, gravitan en torno al denominado *criterio tradicional de conexión por proximidad*, cuyo eje es la localización. Es decir, dichas reglas necesitan de una identidad fehaciente y de una ubicación geográfica concreta para poder surtir efectos, lo que es prácticamente imposible cuando la celebración de los acuerdos y las transacciones se realiza en un sistema digital, descentralizado, transnacional y anónimo (Jiménez Blanco y Espinella Menéndez, 2021, pág. 28).

Igualmente, las situaciones críticas pueden surgir desde el inicio, pues Blockchain permite celebrar contratos digitales automáticos, inmutables y anónimos, válidos siempre que cumplan con consentimiento, objeto y causa (Fetsyak, 2020, págs. 208-210).

Ahora bien, verificar si el consentimiento otorgado en un *smart contract* celebrado en *blockchain* es válido o no es relativamente complicado: ¿cómo podrá verificarse que el consentimiento que aportan las partes del contrato es válido jurídicamente si se desconoce la identidad de los usuarios?

Como se puede concluir, resulta difícil observar y garantizar si el consentimiento es plenamente válido o si, por el contrario, se encuentra viciado. A modo de ejemplo, puede ser que en la relación contractual alguna de las partes sea menor de edad o, incluso, que alguna se encuentre incapacitada judicialmente para contratar, lo que se desconocerá en todo momento porque no existen identidades reales.

A su vez, en ocasiones, existen mecanismos de resolución de conflictos dentro de los sistemas *blockchain*. En este sentido, existen plataformas que ofrecen los servicios de arbitraje en línea mediante tecnología *blockchain*; sin embargo, más allá de solucionar los problemas, parecen incrementarse. Dentro de estos sistemas, los árbitros actúan de forma anónima; se desconoce si poseen conocimientos sobre la materia que se está discutiendo o si ni siquiera pueden actuar en este tipo de procesos (Yépez Idrovo, Vela Sevilla y Haro Aillón, 2020, pág. 21).

Además, ya se ha dicho que las partes son anónimas, por lo que vuelve a surgir la duda: ¿cómo podrá verificarse que el consentimiento que aportan las partes a someterse a arbitraje es válido jurídicamente si se desconoce la identidad de los usuarios? y ¿cómo puede comprobarse si el convenio arbitral se ha celebrado respetando los requisitos del debido proceso si las partes son anónimas? (Tasende, 2020, pág. 143).

Considerando estas situaciones, parece necesario un mecanismo que preserve el anonimato en *blockchain* y, al mismo tiempo, ofrezca seguridad jurídica. Por ello, se propone implementar una identidad cifrada que pueda ser legalmente descifrada en caso de controversia o riesgo.

3. Identidad cifrada en *blockchain*: equilibrio entre anonimato y responsabilidad

Según lo señalado, uno de los ejes fundamentales de la tecnología *blockchain* es la capacidad que otorga a los

usuarios para actuar dentro de un entorno anónimo, descentralizado y sin necesidad de autoridades o intermediarios (Nespral y Fernández Hergueda, 2021, pág. 23).

Ante este disruptivo diseño aparecen importantes desafíos para el ámbito jurídico, concretamente en lo referente a la imputación de responsabilidades, al acceso a mecanismos judiciales y la tutela efectiva de derechos. Aunque actualmente se recurre a mecanismos alternativos de resolución de conflictos dentro del ecosistema *blockchain*, como el arbitraje automatizado mediante contratos inteligentes, estos carecen de obligatoriedad, presentan ciertas fallas y, por supuesto, no pueden sustituir al derecho a acceder a la justicia ordinaria (Pérez Campillo, 2025, págs. 2 y 6).

3.1. Propuesta de identidad cifrada

Frente a esta situación, los sistemas *blockchain* que permiten que los usuarios puedan ser completamente anónimos deben evolucionar sin contradecir su esencia, y dotar a sus arquitecturas de soluciones que garanticen seguridad jurídica y mecanismos de verificación que permitan responsabilizar a los actores cuando sea necesario sin comprometer la descentralización ni la privacidad.

Así las cosas, como posible solución a las fallas encontradas, se sugiere la implementación de una identidad cifrada con desenscriptación judicial como un modelo intermedio entre la garantía del anonimato que ofrece la *blockchain* y la posibilidad de desvirtuarlo cuando lo exijan los derechos o intereses legítimos de las personas.

Una identidad cifrada es un mecanismo que permite a los usuarios de *blockchain* mantener su anonimato funcional, al interactuar en la red sin revelar sus datos personales reales, pero de manera que exista un método seguro para identificar al titular de la identidad en casos puntuales.

La propuesta de identidad cifrada parte de una premisa clara: preservar el anonimato funcional del usuario dentro del ecosistema *blockchain* y, a su vez, permitir su identificación plena en casos excepcionales debidamente justificados por orden judicial. De este modo, se establece un modelo que persigue el equilibrio entre privacidad y responsabilidad (Pfitzmann y Köhntopp, 2001, pág. 9).

Con ello, se garantiza el anonimato, pues los usuarios no se encuentran obligados a revelar sus datos personales

para observar la cadena, participar en transacciones, celebrar *smart contracts* o cualesquiera otras actuaciones que deseen efectuar y, al mismo tiempo, se respetan las exigencias de las normas que, como ya se ha visto, requieren conocer la identidad del sujeto para bien imputar responsabilidades por actos ilícitos o dañosos, o bien comprobar ciertos requisitos contractuales en aras de verificar que las relaciones mantenidas son conforme a derecho (Merchán Murillo, 2022, pág. 1388).

3.2. Beneficios jurídicos y aumento de la seguridad jurídica

Asimismo, dado que los usuarios serían anónimos en todo momento salvo cuando se extralimiten en sus actuaciones, podría reducirse la comisión de delitos como el fraude, el blanqueo de capitales, la evasión fiscal o la financiación ilegal del terrorismo; aspectos fundamentales que cuerpos legales como el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 (MiCA) abordan con estricto celo por razón de la necesidad de proteger a los usuarios y prevenir actividades ilícitas (Martí Miravalls, 2021, pág. 475).

Además, gracias a la implementación de una identidad encriptada, se respetaría mayormente el derecho a la tutela judicial efectiva, consagrado en muchos ordenamientos constitucionales y en instrumentos internacionales, que exige que las personas puedan acceder a un recurso judicial efectivo y que sus derechos sean protegidos en el ámbito de los procedimientos legales, sin que, por ello, el anonimato de los usuarios que actúan en *blockchain* pueda interferir en la posibilidad de establecer responsabilidades en caso de disputas o delitos (Marcheco Acuña, 2020, pág. 93).

3.3. Implementación técnica de la identidad cifrada

A la hora de implementar la identidad cifrada en los entornos *blockchain*, pueden utilizarse las tecnologías ya disponibles en estos sistemas, particularmente las relacionadas con el cifrado asimétrico, los *smart contracts* y los mecanismos descentralizados de almacenamiento (Soledad Cabrera, 2019, págs. 33-36).

Antes de nada, conviene recalcar que el cifrado asimétrico es una técnica criptográfica que utiliza un par de claves: la clave pública, que sirve como identificador del usuario en el *blockchain* y puede compartirse abiertamente, y la clave privada, que permite firmar digitalmente transacciones y *smart contracts*, debiendo mantenerse en secreto.

Para generar la identidad digital cifrada, cada usuario del sistema debe crear este par de claves asimétricas. Con ello, cada usuario deberá crear una clave pública y una clave privada, siguiendo el estándar criptográfico de claves asimétricas: la clave pública servirá como identificador de la identidad del usuario en la *blockchain* y será la que se almacene y utilice para interactuar con otros usuarios o participar en la red, mientras que la clave privada deberá mantenerse en secreto, nunca se revela ni se almacena en la red y permitirá firmar digitalmente las transacciones y *smart contracts* dentro del sistema, garantizando así la seguridad y privacidad de las acciones de los usuarios dentro de la *blockchain* (González y Martínez, 2007, pág. 420).

Tal y como puede observarse, estas claves asimétricas serán la base para mantener el anonimato funcional, porque los usuarios pueden interactuar sin necesidad de revelar su identidad real, lo que garantiza la filosofía de *blockchain* de descentralización y anonimato (Valderrama Hoyos y Araque Cely, 2024, pág. 93).

Toda vez que se ha generado el bloque que contiene la identidad digital del usuario, los datos personales se cifran y se almacenan en una entidad pública o descentralizada que garantice seguridad, integridad y trazabilidad, pudiendo utilizarse como ente custodio una DAO que, mediante contratos inteligentes, gestione el acceso a los datos, preservando la automatización y reduciendo la intervención humana.

Por otro lado, podría recurrirse a una fórmula más tradicional utilizando un notariado criptográfico público o privado, que actúe como un nodo de confianza dentro de la red y pueda certificar, sin revelar su contenido, que los datos cifrados pertenecen a un usuario concreto (García-Ramos Lucero, 2023, pág. 49).

3.4. Descriptación judicial de la identidad cifrada y posibles desafíos

A la vista de todas las cuestiones planteadas en los sistemas *blockchain* públicos y toda vez que se ha desarrollado

su implementación técnica, conviene destacar que la descriptación judicial es un procedimiento mediante el cual los datos cifrados de un usuario pueden ser revelados solo bajo orden judicial válida, para permitir identificar al titular de la clave pública en casos específicos.

Este mecanismo constituye la propuesta central de este trabajo: un modelo que permite preservar el anonimato funcional dentro de la *blockchain* y, al mismo tiempo, garantizar la responsabilidad jurídica de los usuarios cuando sea necesario. En este sentido, la propuesta se basa en un equilibrio entre privacidad, descentralización y trazabilidad legal, lo que asegura que el acceso a la identidad real del usuario se realice únicamente bajo condiciones estrictamente justificadas y controladas judicialmente (Goel, Bisht, y Chaudhary, 2023, pág. 476).

Uno de los desafíos principales que enfrenta este modelo es el acceso a la identidad cifrada en situaciones en las que se requiere imputar responsabilidad jurídica, realizar una investigación judicial u observar si los requisitos de validez contractual del *smart contract* son conformes a derecho. En este sentido, el sistema debe diseñarse de manera que la descriptación de los datos solo sea posible mediante una orden judicial válida emitida por una autoridad judicial competente, lo que garantiza que el acceso a la información se haga de acuerdo con la ley y solo en los casos estrictamente necesarios.

En este contexto, la tutela judicial efectiva adquiere un papel central, porque la descriptación de la identidad cifrada implica inevitablemente la afectación de derechos fundamentales como la privacidad, la protección de datos personales y, en algunos casos, la libertad individual frente al poder del Estado. Por ello, el acceso judicial a la identidad de un usuario solo debería autorizarse cuando existan indicios razonables y proporcionados de la comisión de un delito o una vulneración grave de derechos de terceros (Vidal Fernández, 2025, págs. 221 y ss.).

El juez, como garante último del equilibrio entre seguridad y libertad, debería evaluar la necesidad, idoneidad y proporcionalidad de la medida, verificando que no existan alternativas menos intrusivas. Además, la autorización debería constar en una resolución motivada, dictada conforme a los principios de legalidad y debido proceso, y ejecutarse bajo un sistema de control técnico seguro, como el modelo de firma múltiple propuesto a continuación, que asegure que la descriptación se realiza exclusivamente

en los términos ordenados judicialmente. En este sentido, la decisión judicial se basaría en la existencia de indicios razonables que justifiquen la intervención, asegurando que la medida solo se adopte cuando haya evidencia fundada de un ilícito, un conflicto contractual o una amenaza a derechos de terceros. De este modo, se protege la privacidad y el anonimato funcional del usuario, limitando la exposición de datos únicamente a lo estrictamente necesario para cumplir con un fin legal concreto, garantizando a la vez la tutela efectiva de los derechos fundamentales involucrados, como la protección de datos, la seguridad jurídica y el acceso a la justicia (Martín Diz, 2025, pág. 57).

Además, como propuesta, el mecanismo de desenscriptación debe ser implementado mediante un sistema de firma múltiple o *multisig*, que significa que la identidad cifrada no podrá ser desenscriptada sin la intervención de varias partes autorizadas. En este caso, las firmas necesarias podrían incluir las de un juez, un representante del ente que custodia los datos y un auditor independiente o defensor de derechos. De este modo, se asegura que la operación sea supervisada y validada por varias entidades, evitando abusos y garantizando la legalidad del acceso (Goel, Bisht, y Chaudhary, 2023, pág. 476).

Por otra parte, debe tenerse en cuenta que el uso de contratos inteligentes automatizados en *blockchain* puede facilitar la ejecución de este proceso sin necesidad de intermediarios manuales. Al respecto, la orden judicial que activa el mecanismo de desenscriptación puede ser programada como un *smart contract* que ejecute el desbloqueo de los datos cifrados bajo condiciones específicas, asegurando eficiencia, rapidez, transparencia y trazabilidad de la acción (Castellano García, 2021, pág. 10).

Toda vez que se ha propuesto la implementación de este sistema y se ha sugerido la forma en la que puede llevarse a cabo, conviene repasar de forma breve las anomalías jurídicas anteriormente expuestas y estudiar cómo este sistema puede resolverlas.

La incorporación de un sistema de identidad cifrada con desenscriptación judicial no solo es compatible con los principios fundamentales de la tecnología *blockchain*, como la descentralización, la privacidad y el anonimato, sino que además permite enfrentar de manera eficaz los principales desafíos jurídicos que actualmente obstaculizan la plena integración legal de esta tecnología en los sistemas normativos tradicionales.

Uno de los principales desafíos jurídicos en *blockchain* es la dificultad para determinar quiénes son los encargados y responsables del tratamiento de los datos personales contenidos en la cadena, dado que, en un entorno descentralizado, no existen jerarquías o autoridades que puedan asumir este papel (Espuga Torné, 2021, pág. 2).

El sistema propuesto mitiga este riesgo mediante la custodia externa de los datos cifrados. En este sentido, como ya se ha comentado, la custodia puede recaer en una organización autónoma descentralizada (DAO) o en una entidad confiable de carácter más tradicional que actúe bajo criterios de notariado criptográfico, que pueden asumir el papel de responsable o encargado del tratamiento, según el caso, y garantizar así el cumplimiento de la normativa sobre protección de datos.

No debe olvidarse que el anonimato en *blockchain* puede favorecer la comisión de actividades ilícitas, como el blanqueo de capitales, la evasión fiscal, el fraude o la financiación del terrorismo; sin embargo, la fórmula de identidad cifrada parece proporcionar una solución equilibrada. Por una parte, garantiza el anonimato funcional de los sistemas *blockchain*, y, por otra, permite que, en situaciones de riesgo o delito, las autoridades puedan acceder a la identidad real del usuario mediante un proceso transparente y controlado, manteniendo la privacidad sin que esta se convierta en un obstáculo para la preservación de los derechos e intereses de los usuarios (Aránguez Sánchez, 2020, págs. 75-76).

Asimismo, las normas que conforman el ordenamiento jurídico necesitan que las personas puedan ser identificadas para poder aplicarse e imputar hipotéticas responsabilidades. En este sentido, el sistema propuesto parece permitirlo, pues, mediante una orden judicial, se podrá identificar al titular de una clave pública en la *blockchain*, desvelando su identidad real, lo que abre la puerta a iniciar acciones judiciales, y resolviendo el problema de la inimputabilidad jurídica de sujetos anónimos.

Por otro lado, se ha visto que la *blockchain* carece de fronteras y, por lo tanto, posee carácter transnacional, lo que, junto al anonimato, impide determinar la jurisdicción aplicable cuando existan en la relación elementos extranjeros. En defecto de acuerdo de sumisión a una jurisdicción determinada o juez competente, con la identidad cifrada asociada a un ente que la custodie, se crea

un vínculo jurídico trazable que facilita aplicar las normas del derecho internacional privado. En este sentido, podrá revelarse judicialmente que un sujeto está domiciliado en cierto país y, por tanto, podrá aplicarse el criterio de proximidad geográfica o de conexión significativa, tal y como exigen los principios de territorialidad y competencia en los conflictos internacionales (Calvo Caravaca y Carrasosa González, 2012, pág. 582).

A su vez, se estudió cómo los *smart contracts* se ejecutan automáticamente sin verificación de la voluntad real de las partes, lo que puede generar dudas sobre la validez del consentimiento prestado. Ahora, asociando cada clave pública a una identidad cifrada, evidentemente respaldada por datos reales, será posible verificar, en caso de controversia, si el consentimiento fue prestado por una persona jurídica o física válida y, por supuesto, bajo qué condiciones. De esta manera, el sistema permitirá revisar la formación del contrato conforme a los requisitos legales del consentimiento (capacidad, ausencia de vicios, libre voluntad), y reforzar así la seguridad jurídica de los procedimientos y el cumplimiento de las normas aplicables (Cáceres Malagón, 2024, págs. 164-166).

Además, muchos entornos *blockchain* proponen mecanismos alternativos de resolución de disputas, como, por ejemplo, arbitrajes automáticos en línea, pero sin que sea posible verificar si existe un acuerdo válido entre las partes identificadas o si los árbitros se encuentran capacitados para actuar en el proceso, lo que pone en duda su eficacia legal y el respeto de los requisitos del debido proceso. Mediante la propuesta de identidad cifrada, si una de las partes impugna el acuerdo arbitral, el juez podrá verificar, mediante desenscriptación judicial, si los usuarios que suscribieron el convenio de arbitraje son plenamente capaces y si actuaron conforme al debido proceso, para garantizar la validez del pacto y, por tanto, la legitimidad del procedimiento arbitral (Gonzalo Quiroga, 2023, pág. 545).

Igualmente, debe decirse que, al igual que responde a los riesgos concretos señalados, el sistema de identidad cifrada con desenscriptación judicial también parece representar una vía intermedia entre dos extremos. Por un lado, el absolutismo del anonimato y el hipercontrol estatal, porque este modelo no impone una vigilancia masiva ni vulnera el principio de privacidad que inspira la Web3, y, por otro, tampoco permite que esa privacidad se convierta en una zona de impunidad digital, porque, en

su lugar, habilita un sistema de responsabilidad condicionada, controlado, con garantías procesales y trazabilidad técnica, que puede constituir una referencia normativa para futuras regulaciones internacionales sobre identidad digital (Ramos Gil de la Haza, 2022, págs. 51-52).

En aras de que este sistema funcione de manera efectiva y cumpla con sus objetivos de privacidad, trazabilidad y responsabilidad jurídica, su implementación debe estar necesariamente respaldada por una regulación específica que establezca los límites de acceso a la identidad cifrada, los procedimientos de autorización y las medidas de control técnico. Esta regulación garantizará que la desenscriptación judicial solo se realice en situaciones extraordinarias, previamente justificadas por la ley, y deberá articularse bajo las normas existentes, como el Reglamento (UE) 2023/1114 (MiCA), las Directivas 2013/36/UE y 2019/1937, la normativa de protección de datos (RGPD) y los principios de tutela judicial efectiva, para asegurar la compatibilidad del sistema con el marco legal vigente.

Asimismo, hay que tener presente que la *blockchain* es transnacional, lo que permite a los usuarios transaccionar sin limitarse a un solo país o continente. Por ello, para que la desenscriptación judicial de la identidad cifrada funcione de manera efectiva y segura, no basta con la regulación europea; es necesario que se creen mecanismos de homogeneidad entre legislaciones, de manera que los criterios de acceso, custodia de datos, autorización judicial y medidas de control técnico sean compatibles en distintas jurisdicciones.

De este modo, el sistema podrá operar en el ámbito global, asegurando que la responsabilidad jurídica se pueda ejercer en cualquier jurisdicción en las que surjan conflictos o delitos, sin que las diferencias entre marcos normativos comprometan la eficacia del procedimiento; cuestión que está ocurriendo actualmente debido a la ausencia de criterios uniformes dentro de este tipo de sistemas.

Conclusiones

La creciente inserción de la tecnología *blockchain* en diversos ámbitos plantea desafíos inéditos para el derecho, especialmente en la atribución de responsabilidad, la protección de derechos fundamentales y el cumplimiento efectivo de la legislación vigente.

Las distintivas características de *blockchain*, como el anonimato, el seudonimato funcional y la transnacionalidad, representan significativos retos para los ordenamientos jurídicos contemporáneos. Sin embargo, estas particularidades no deben convertirse en barreras que imposibiliten la acción del derecho, pues la privacidad que aportan las nuevas tecnologías puede y debe coexistir con la exigencia de responsabilidad jurídica.

En este contexto, el modelo de identidad cifrada con descriptación judicial se presenta como una propuesta concreta y factible, tanto técnica como legalmente. Su implementación se basa en claves asimétricas, custodia descentralizada de datos cifrados y mecanismos de validación jurídica, como la firma múltiple o *multisig*, activables únicamente bajo una orden judicial válida. Esto permite preservar el anonimato funcional de los usuarios, y evitar la creación de bases de datos centralizadas que concentren riesgos o vulneren derechos, al mismo tiempo que habilita la identificación legal cuando sea estrictamente necesario.

Desde el punto de vista técnico, las herramientas y los actuales estándares criptográficos son capaces de soportar este modelo, y, desde el punto de vista legal, se alinea con normas como el Reglamento MiCA, el RGPD, directivas europeas de supervisión y tutela judicial efectiva y puede ser escalado mediante acuerdos de armonización transnacional, es decir, mediante convenios y tratados internacionales.

A su vez, no debe olvidarse que el anonimato es una de las características más atractivas en el mundo *blockchain*, por lo que, en términos de aceptación por parte de los usuarios que operan en este tipo de sistemas, este modelo ofrece un valor significativo: protege el anonimato en la mayoría de las interacciones cotidianas, preserva la descentralización de la red y solo introduce intervención

jurídica en casos excepcionales, lo que podría favorecer aún más la confianza y la adopción del sistema.

Además, la implementación de esta solución podría incentivar la integración institucional y empresarial de este tipo de sistemas, pues, recordemos que actualmente nos encontramos en la etapa Blockchain 3.0, en la que se pretende aplicar a diversos sectores muy regulados, como las finanzas, la salud y la contratación pública, ámbitos en los que la seguridad jurídica constituye un requisito ineludible y, aunque se pudieran usar *blockchain* privadas en estos sectores, no debe olvidarse la importancia de preservar la desintermediación que caracteriza a los sistemas públicos y que también atrae el interés de los usuarios.

Propositivamente, se sugiere que futuras regulaciones incluyan criterios claros de autorización de descriptación, límites de acceso, supervisión de terceros independientes y mecanismos transnacionales de coordinación, para garantizar que la responsabilidad jurídica pueda aplicarse globalmente sin comprometer la privacidad de los usuarios ni la efectividad de la tecnología. Junto a ello, también sería recomendable promover estándares técnicos interoperables y auditorías externas para validar la ejecución segura de los procesos de descriptación judicial y la trazabilidad de los datos.

En conclusión, el modelo de identidad cifrada con descriptación judicial no solo permite integrar la esencia descentralizada y anónima de *blockchain* con la exigencia de seguridad jurídica, sino que también ofrece soluciones técnicas, legales y operativas concretas que podrían ser aceptadas por los usuarios y aportar un valor real al ecosistema. Se trata de una vía equilibrada que protege los derechos de los usuarios, facilita la atribución de responsabilidades y fortalece la confianza institucional en un entorno tecnológico disruptivo.

Referencias bibliográficas

- PREUKSCHAT, A.; KUCHKOVSKY, C. (2017). *Blockchain: la revolución industrial de internet*. España: Gestión 2000.
- AMMOUS, S. (2016). «Blockchain Technology: What is it Good for?». *SSRN* 2832751, págs. 1-5. DOI: <http://dx.doi.org/10.2139/ssrn.2832751>
- ANDOLA, N.; RAGHAV; YADAV, V.; VENKATESAN, S.; VERMA, S. (2021). «Anonymity on blockchain based e-cash protocols—A survey». *Computer Science Review*, vol. 40, 100394. DOI: <https://doi.org/10.1016/j.cosrev.2021.100394>
- ARÁNGUEZ SÁNCHEZ, C. (2020). «El bitcoin como instrumento y objeto de delitos». *Cuadernos de Política Criminal*: 131, II, págs. 75-103.
- BEDECARRATZ SCHOLZ, F. (2018). «Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal». *Revista chilena de derecho y tecnología*, vol. 7 n.º 1, págs. 79-106. DOI: <https://doi.org/10.5354/0719-2584.2018.48515>
- CÁCERES MALAGÓN, J. A. (2024). «¿Sueñan las máquinas con contratar? Un estudio sobre smart contracts y consentimiento algorítmico». *Revista de derecho Privado*, n.º 46, págs. 155-185. DOI: <https://doi.org/10.18601/01234366.46.07>
- CALAZA LÓPEZ, S.; ANGUIANO JIMÉNEZ, J. M.; FERNANDEZ-TRESGUERRES GARCÍA, A.; FELIU REY, J.; GIMENO BEVIÁ, J.; MADRID PARRA, A.; VILALTA NICUESA, A. E. (2023, junio). «Smart Contract: ¿Contrato inteligente o programa informático? ¿Qué son —exactamente— los Smart Contracts? ¿Cuál es su naturaleza, filosofía y principios inspiradores?». *Actualidad Civil*, n.º 6, págs. 1-23. Editorial LA LEY.
- CALVO CARAVACA, A. L.; CARRASCOSA GONZÁLEZ, J. (2012). *Derecho del comercio internacional*. Madrid: San Fernando de Henares: Colex.
- CASTELLANO GARCÍA, A. (2021). «Conceptualización de los contratos inteligentes o autoejecutables basados en la tecnología blockchain y su encuadre en el ordenamiento jurídico español». *Revista Estudios Jurídicos. Segunda Época*, n.º 21, e6756, págs. 1-41. DOI: <https://doi.org/10.17561/rej.n21.6756>
- DAVIDSON, S.; De FILIPPI, P.; POTTS, J. (2016). «Economics of Blockchain». *SSRN* 2744751, págs. 1-23. DOI: <http://dx.doi.org/10.2139/ssrn.2744751>
- De FILIPPI, P.; WRIGHT, A. (2018). *Blockchain and the Law. The Rule of Code*. Cambridge: Harvard University Press. DOI: <https://doi.org/10.2307/j.ctv2867sp>
- ESPUGA TORNÉ, G. (2021, octubre). «Compatibilidad y encaje legal de la tecnología blockchain con la normativa sobre protección de datos personales». *La Ley mercantil*, ISSN-e 2341-4537, n.º 84.
- FETSYAK, I. (2020). «Contratos inteligentes: análisis jurídico desde el marco legal español». *Revista electrónica de Derecho de la Universidad de La Rioja, REDUR*, n.º 18, págs. 197-236. DOI: <https://doi.org/10.18172/redur.4898>
- FINK, M. (2019). «Smart Contracts as a Form of Solely Automated Processing Under the GDPR». *International Data Privacy Law*, vol. 9, n.º 2, págs. 78-94. DOI: <https://doi.org/10.1093/idpl/ipz004>
- GIMENO BEVIÁ, J. (2023). «La resolución de los conflictos «en blockchain» o cuando el código es la ley: difícil reto desde la justicia penal». *La Ley. Mediación y arbitraje*, n.º 16, págs. 1-8.

- GOEL, A.; BISHT, V.; CHAUDHARY, S. (2023). «Multisignature Crypto Wallet Paper». *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, págs. 476-479. Coimbatore, India: IEEE. DOI: <https://doi.org/10.1109/ICCES57224.2023.10192591>
- GONZÁLEZ, S.; MARTÍNEZ, C. (2007). «Las matemáticas de la seguridad». *Arbor Ciencia Pensamiento y Cultura*, vol. 183, n.º 735, págs. 419-425. DOI: <https://doi.org/10.3989/arbor.2007.i725.114>
- GONZALO QUIROGA, M. (2023). «La inteligencia artificial en el arbitraje internacional 2.0. Oportunidades y desafíos en un futuro que ya es presente». *CUADERNOS DE DERECHO TRANSNACIONAL*, vol. 15, n.º 2, págs. 516-550. DOI: <https://doi.org/10.20318/cdt.2023.8067>
- HOFMANN, F.; WURSTER, S.; RON, E.; BÖHMECKE-SCHWAFERT, M. (2017). «The immutability concept of blockchains and benefits of early standardization». *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*. IEEE., págs. 1-8. DOI: <https://doi.org/10.23919/ITU-WT.2017.8247004>
- HUANG, K.; ZHANG, X.; MU, Y.; REZAEIBAGHA, F.; DU, X. (2021). «Scalable and redactable blockchain with update and anonymity». *Information Sciences*, vol. 546, págs. 25-41. DOI: <https://doi.org/10.1016/j.ins.2020.07.016>
- IBÁÑEZ JIMÉNEZ, J. W. (2018). *Derecho de Blockchain*. Navarra: Aranzadi. DOI: <https://doi.org/10.2307/j.ctv346qc0>
- JIMÉNEZ BLANCO, P.; Espinella Menéndez, Á. (2021). *Nuevos escenarios del derecho internacional privado de la contratación*. Asturias: Tirant lo Blanch.
- MARCHECO ACUÑA, B. (2020). «La dimensión constitucional y convencional del derecho a la tutela judicial efectiva (no penal) desde la perspectiva jurisprudencial europea y americana». *Estudios constitucionales: Revista del Centro de Estudios Constitucionales*, vol. 18, n.º 1, págs. 91-142. DOI: <https://doi.org/10.4067/S0718-52002020000100091>
- MARTÍ MIRAVALLS, J. (2021). «La propuesta de reglamento del parlamento europeo y del consejo relativo a los mercados de criptoactivos: la propuesta mica». *Revista de Derecho del Sistema Financiero: mercados, operadores y contratos*, n.º 1, págs. 473-480.
- MARTÍN DIZ, F. (2025). «Derechos y garantías procesales penales fundamentales: una lectura en clave tecnológica». *Ius et Scientia*, vol. 10, n.º 1, págs. 52-81. DOI: <https://doi.org/10.12795/IESTSCIEN-TIA.2024.i01.03>
- MARTÍNEZ BOADA, J. (2025, marzo). «Transformación digital del transporte marítimo: Blockchain para la ventanilla única europea». *Cuadernos de Derecho Transnacional*, vol. 17, n.º 1, págs. 1234-1244. DOI: <https://doi.org/10.20318/cdt.2025.9365>
- MARTÍNEZ BOADA, J.; REJAS MUSLERA, R. J. (2024). «Protección jurídica de Blockchain: Un análisis desde su funcionalidad y naturaleza jurídica según el ordenamiento jurídico español». *Revista Chilena de Derecho y Tecnología*, vol. 13, págs. 1-20. DOI: <https://doi.org/10.5354/0719-2584.2024.73869>
- MARTÍNEZ BOADA, J.; SANTAMARÍA RAMOS, F. J. (2024). «Blockchain: la nueva era de la identificación digital en internet». *Teoría & Derecho. Revista De Pensamiento jurídico*, n.º 37, págs. 258-283. DOI: <https://doi.org/10.36151/TD.2024.114>
- MERCHÁN MURILLO, A. (2022). «La identidad digital en la contratación electrónica: una mirada desde el derecho internacional privado». *Actualidad jurídica iberoamericana*, n.º 16, págs. 1386-1411.
- NESPRAL, D.; FERNÁNDEZ HERGUEDA, R. (2021). *Blockchain: El modelo descentralizado hacia la economía digital*. Bogotá: Ra-ma (España) - Ediciones de la U (Colombia).
- ORTEGA GIMÉNEZ, A. (2019). *Smart Contracta y Derecho Internacional Privado*. Pamplona: Aranzadi.

- PADILLA SÁNCHEZ, J. A. (2020). «Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos». *Revista de Derecho Privado*, n.º 39, págs. 175-201. DOI: <https://doi.org/10.18601/01234366.n39.08>
- PARDO PRADO, S. (2022). «Las repercusiones de Blockchain en los derechos de los consumidores». *Hacia una tutela efectiva de consumidores y usuarios*, cap. 7, págs.153-160. Tirant lo Blanch Online.
- PÉREZ CAMPILLO, L. (2025). «Implementación de blockchain en el sistema judicial público y en los ADR». *IDP. Revista d'Internet, Dret i Política*, n.º 42, págs. 1-12. DOI: <https://doi.org/10.7238/idp.v0i42.429135>
- PFITZMANN, A.; KÖHNTOPP, M. (2001, septiembre). «Cómo alcanzar un equilibrio entre la prevención del ciberdelito y la privacidad». *Vlex*, n.º 57, págs. 9-18.
- PINTO ARBOLEDA, R. A.; FAJARDO BRAVO, N. J.; ORTEGA MÈNDE, J. X.; ZAMBRANO TOAPANTA, A. Y.; ZAMBRANO RECALDE, P. E. (2025). «Análisis del uso de software contable y tecnologías como blockchain». *Sinergia Académica*, vol. 8, especial 2, págs. 499-513. DOI: <https://doi.org/10.51736/sa505>
- POLO ROCA, A. (2021). «Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos». *Estudios de Deusto: revista de Derecho Público*, vol. 69, n.º 1, págs. 165-194. DOI: [https://doi.org/10.18543/ed-69\(1\)-2021pp211-240](https://doi.org/10.18543/ed-69(1)-2021pp211-240)
- RAMOS GIL de la HAZA, A. (2022). «La web3: una aproximación jurídica». *Revista Jurídica Pérez-Llorca*, vol. 8, n.º 24, págs. 36-59.
- RAYENIZADEH, M.; RAFSANJANI, M. (2025). «Chapter 1 - Introduction to blockchain technology». *Digital Twin and Blockchain for Sensor Networks in Smart Cities*, págs. 3-16. DOI: <https://doi.org/10.1016/B978-0-443-30076-9.00002-9>
- RUEDA CASTAÑEDA, J. E.; GALLEGÓ GÓMEZ, N.; ESTANLING CÁRDENAS, E.; TELLO, J. S.; GARCÍA PINEDA, V. (2024). «Identificación de variables relacionadas a la seguridad informática a partir de tendencias investigativas de la tecnología Blockchain». *Revista Politécnica*, vol. 20, n.º 40, págs. 9-29. DOI: <https://doi.org/10.33571/rpolitec.v20n40a1>
- SARMAH, S. S. (2018). «Understanding blockchain technology». *Computer Science and Engineering*, vol. 8, n.º 2, págs. 23-29.
- SOLEDAD CABRERA, C. (2019). «Aproximación a los conceptos de blockchain, smart contracts y su relación con la función notarial». *Revista De Derecho Notarial Y Registral. Universidad Blas Pascal*, n.º 6, págs. 29-40.
- SUN YIN, H.; LANGENHELDT, K.; HARLEV, M.; MUKKAMALA, R.; VATRAPU, R. (2019). «Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain». *Journal of Management Information Systems*, vol. 36, n.º 1, págs. 37-73. DOI: <https://doi.org/10.1080/07421222.2018.1550550>
- TASENDE, I. (2020). «Blockchain y arbitraje: un nuevo enfoque en la resolución de disputas. Especial énfasis en smartcontracts y criptodivisas». *Revista de Derecho (Universidad Católica Dámaso A. Larrañaga, Facultad de Derecho)*, n.º 22, págs. 138-159. DOI: <https://doi.org/10.22235/rd22.2127>
- TORRES CAZORLA, M. I. (2019). «Cuestiones jurídicas Emergentes: Un análisis a Vista De pájaro». *Estudios De Deusto*, vol. 67, n.º 2, págs. 87-102. DOI: [https://doi.org/10.18543/ed-67\(2\)-2019pp87-102](https://doi.org/10.18543/ed-67(2)-2019pp87-102)
- TOURIÑO PENA, A.; VILLASANTE, C.; ARNAIZ, J.; CAMARASA, P.; DÍEZ, J.; GALÁN, J.; TÉLLEZ, H. (2022). *Blockchain y Smart Contracts*. Madrid: Francis Lefebvre.

- VALDERRAMA HOYOS, M.; ARAQUE CELY, J. A. (2024). «Aplicación de blockchain en diferentes sectores: revisión literaria». *Revista Ingeniería, Matemáticas y Ciencias de la Información*, vol. 11, n.º 21, págs. 81-98. DOI: <https://doi.org/10.21017/rimci.1024>
- VIDAL FERNÁNDEZ, B. (2025). «Independencia judicial y proceso penal europeo. El derecho a un juez independiente y su incidencia en el espacio de libertad, seguridad y justicia». *Revista de Estudios Europeos*, n.º 85, págs. 221-252. DOI: <https://doi.org/10.24197/ree.85.2025.221-252>
- XU, M.; CHEN, X.; KOU, G. (2019). «A systematic review of blockchain». *Financial Innovation*, vol. 5, n.º 1, págs. 1-14. DOI: <https://doi.org/10.1186/s40854-019-0147-z>
- YAROSHENKO, O.; PUNTUS, D.; CHANY SHEVA, H.; MOSKALENKO, O.; SLIUSAR, A. (2025). «Integration of blockchain technologies into the social security system: transparency and efficiency». *Revista de derecho de la seguridad social. Laborum*, n.º 42, p. 243-257.
- YÉPEZ IDROVO, M. V.; VELA SEVILLA, M. P.; HARO AILLÓN, B. A. (2020, septiembre). «Smart contracts y el arbitraje: hacia un modelo de justicia deslocalizado». *USFQ Law Review*, vol. 7, n.º 1, págs. 1-28. DOI: <https://doi.org/10.18272/ulr.v7i1.1698>
- ZHANG, R.; XUE, R.; LIU, L. (2019). «Security and privacy on blockchain». *ACM Computing Surveys (CSUR)*, vol. 52, n.º 3, págs. 1-34. DOI: <https://doi.org/10.1145/3316481>
- ZHANG, S.; LEE, J.-H. (2020). «Analysis of the main consensus protocols of blockchain». *ICT Express*, vol. 6, n.º 2, págs. 93-97. DOI: <https://doi.org/10.1016/j.icte.2019.08.001>
- ZĪLE, K.; STRAZDIŅA, R. (2018). «Blockchain use cases and their feasibility». *Applied Computer Systems*, vol. 23, n.º 1, págs. 12-20. DOI: <https://doi.org/10.2478/acss-2018-0002>

Cita recomendada

MARTÍNEZ BOADA, Javier (2026). «Identidad cifrada con descriptación judicial: una solución jurídica para la responsabilidad en entornos *blockchain*». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC [Fecha de consulta: dd/mm/aa]. DOI: <http://dx.doi.org/10.7238/idp.v0i44.9800435>



Los textos publicados en esta revista están –si no se indica lo contrario– bajo una licencia Reconocimiento-Sin obras derivadas 3.0 España de Creative Commons. Puede copiarlos, distribuirlos y comunicarlos públicamente siempre que cite su autor y la revista y la institución que los publica (*IDP. Revista de Internet, Derecho y Política*; UOC); no haga con ellos obras derivadas. La licencia completa se puede consultar en: <http://creativecommons.org/licenses/by-nd/3.0/es/deed.es>.

Sobre el autor**Javier Martínez Boada**

Universidad Camilo José Cela (Madrid)

javier.martinez6@ucjc.edu

ORCID: <https://orcid.org/0009-0008-5482-4757>

Graduado en Derecho por la Universidad Camilo José Cela (2019), máster de Acceso a la Profesión de Abogado por la Universidad Camilo José Cela (2021), abogado colegiado en el ICAM (2021), experto en Derecho y *Compliance* de las TIC's por la Universidad Camilo José Cela (2021), doctor en Derecho por la Universidad Camilo José Cela (2025).