Desafíos regulatorios y tecnológicos de los oráculos aplicados a los *smart contracts*[1]

Eduardo Andrés Calderón-Marenco
Universidad Cooperativa de Colombia
eduardo.calderon@campusucc.edu.co
https://orcid.org/0000-0002-7840-6495

Víctor H. Aristizabal-Tique
Universidad Cooperativa de Colombia
victor.aristizabalt@campusucc.edu.co
https://orcid.org/0000-0002-7880-5883

Juan Guillermo Agón López
Universidad Cooperativa de Colombia
juan.agon@campusucc.edu.co
https://orcid.org/0000-0002-2335-4739

Paola Arenas
Universidad Cooperativa de Colombia
proyectosp44@gmail.com
https://orcid.org/0009-0000-5592-0064

Ana Valeria Romero Guido
Universidad Americana (Nicaragua)
ana.romero@uamv.edu.ni
https://orcid.org/0000-0001-7794-3718

Gabriel Ravelo-Franco
Universidad Continental, Huancayo (Perú)
gravelo@continental.edu.pe
https://orcid.org/0000-0003-0212-312X

https://doi.org/10.26422/RJA.2025.0602.cal

Recibido: 27/03/2025
Aceptado: 06/11/2025

1 El presente artículo es derivado de los proyectos "Desafíos jurídicos y tecnológicos de la Tokenización de activos para la innovación en América Latina", con código INV3707 (ejecutado por la Universidad Cooperativa de Colombia –sedes Medellín y Bogotá–, la Universidad de Salamanca, la Universidad Continental y la Universidad Americana) e "Implementación de acciones para la protección de cuencas de agua y suelos a partir de reforestación con tecnologías emergentes y biotecnología en la región Llanos Orientales en los departamentos de Meta y Arauca", con código BPIN2022000100005 (ejecutado por la Universidad Cooperativa de Colombia –sedes Medellín, Villavicencio y Arauca– y financiado por el Ministerio de Ciencia y Tecnología de Colombia mediante el Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías).

Resumen
El objetivo de este estudio es analizar los desafíos regulatorios y tecnológicos asociados a los oráculos en *blockchain*, con énfasis en su papel en la automatización de contratos inteligentes y la *tokenización* de activos. La metodología utilizada combina una revisión sistemática de la literatura con el análisis de un caso de estudio, el Oráculo Terrasacha, aplicado a la gestión ambiental y compensación de emisiones de carbono. Los resultados evidencian que los oráculos son esenciales para integrar datos externos en *blockchain*, pero presentan riesgos relacionados con la fiabilidad de la información, la seguridad y la falta de un marco normativo específico. Se identifican distintas tipologías de oráculos según su fuente de datos, modelo de confianza y patrón de diseño, lo que permite evaluar su aplicabilidad en diversos contextos. Se destaca también la necesidad de establecer estándares regulatorios claros para la gobernanza de los oráculos que contemplen la asignación de responsabilidades y que promueva modelos descentralizados de validación de datos.

Palabras clave: oráculos en *blockchain*, contratos inteligentes, *tokenización* de activos, gobernanza de oráculos, validación de datos descentralizada, regulación de *blockchain*, seguridad de datos.

Regulatory and Technological Challenges of Oracles Applied to Smart Contracts

Abstract
This paper examines the regulatory and technological challenges of blockchain oracles, emphasizing their role in enabling smart contract automation and asset tokenization. The research employs a literature review alongside a case study of Oráculo Terrasacha, an oracle applied to environmental management and carbon emission offsetting. The findings highlight the critical role of oracles in bridging blockchain systems with external data, while also exposing vulnerabilities related to data integrity, security, and regulatory gaps. The study categorizes oracles based on data sources, trust models, and design patterns, offering insights into their suitability for different applications. It also emphasizes the urgency of establishing robust regulatory frameworks for oracle governance, ensuring accountability, and fostering decentralized data validation mechanisms to enhance transparency and security in blockchain ecosystems.

Key words: blockchain oracles, smart contracts, asset tokenization, oracle governance, decentralized data validation, blockchain regulation, data security.

1. Introducción

Esta investigación se centra en la necesidad de establecer un marco conceptual claro sobre los oráculos en *blockchain*, debido a su importancia en la tecnología y economía digital, particularmente en el auge de DeFi, la *tokenización* de activos y los contratos inteligentes (Hierro Viétiez, 2021). La *blockchain*, aunque segura, es un sistema cerrado que depende de los oráculos para interactuar con

datos externos, lo que permite la automatización y una descentralización efectiva (Condon et al., 2023).

El análisis también aborda los retos operativos y legales asociados con los oráculos, como la fiabilidad de los datos y la asignación de responsabilidades en caso de errores, lo que subraya la necesidad de un marco normativo que garantice la seguridad y la transparencia (Chung y Adriaens, 2024; Diago Diago, 2021). Este trabajo busca contribuir tanto al conocimiento académico como a la regulación, estableciendo bases sólidas para el uso seguro y eficiente de oráculos en la economía digital.

En consonancia con lo relevante de este estudio, se tiene que el avance acelerado de la tecnología *blockchain* ha dado lugar a la creación de aplicaciones innovadoras que prometen transformar diversas industrias, particularmente a través del uso de contratos inteligentes y la *tokenización* de activos. Los contratos inteligentes, programas autoejecutables que se hacen efectivos cuando se cumplen ciertas condiciones, y la *tokenización*, que convierte activos físicos en representaciones digitales, han sido celebrados como mecanismos que pueden revolucionar la forma en que se manejan las transacciones y la propiedad. No obstante, estas aplicaciones dependen fundamentalmente de la integración de datos externos para funcionar de manera efectiva. Aquí es donde surge la necesidad crítica de los oráculos, sistemas que actúan como intermediarios, permitiendo que *blockchains* —que, por diseño, son cerradas y autosuficientes— interactúen con el mundo exterior al proporcionar los datos que no están intrínsecamente disponibles en la cadena (Cong y He, 2019).

El principal desafío que enfrenta la implementación de los oráculos radica en garantizar la integridad y fiabilidad de los datos transmitidos. Dado que los contratos inteligentes se ejecutan automáticamente basándose en la información que reciben, cualquier error o manipulación de estos datos podría tener consecuencias legales y financieras graves. Este riesgo es especialmente alto en aplicaciones críticas, como la *tokenización* de activos, donde la precisión de la información es fundamental para mantener la integridad de los *tokens* y, por ende, la confianza en los mercados digitales.

Además, el uso de oráculos introduce otros conjuntos de retos legales y regulatorios que aún no han sido abordados de manera exhaustiva en la literatura jurídica. Por ejemplo, surge la cuestión de la responsabilidad legal en casos donde los datos proporcionados por un oráculo son incorrectos o falsificados, lo que podría llevar a la ejecución errónea de contratos inteligentes. Este es un problema complejo, ya que los oráculos pueden ser operados por terceros que

no están directamente vinculados a las partes involucradas en un contrato, lo que complica la asignación de responsabilidades legales (Diago Diago, 2021).

El problema del oráculo se refiere a la incapacidad inherente de las *blockchains* para acceder directamente a información externa, lo que limita su capacidad para interactuar con el mundo real. Este aislamiento asegura que las *blockchains* mantengan su seguridad y transparencia, pero, a su vez, impide su aplicación en escenarios que requieren datos externos, como precios de mercado o condiciones climáticas (Warwick, 2019). Los oráculos surgen como una solución a este problema, actuando como puentes que permiten que los contratos inteligentes accedan a datos externos que no están disponibles en la *blockchain*.

La falta de consenso sobre la mejor manera de gobernar estos sistemas ha dado lugar a debates dentro de la comunidad *blockchain* sobre cómo asegurar que los datos transmitidos sean precisos y no estén sujetos a manipulaciones. Estos debates son particularmente relevantes en el contexto de la *tokenización*, un área emergente que tiene el potencial de transformar la economía digital al permitir la representación digital de activos del mundo real (Chung y Adriaens, 2024).

Así, el fenómeno de los oráculos ha ganado relevancia como un tema central de discusión y análisis. Estos se han vuelto necesarios para la expansión de las aplicaciones de contratos inteligentes, ya que permiten que estos programas automatizados interactúen con eventos y condiciones del mundo real. No obstante, la teorización sobre los oráculos sigue siendo un área en desarrollo, con numerosas lagunas conceptuales y técnicas que necesitan ser abordadas para garantizar su implementación segura y efectiva.

La problemática central de esta investigación es el abordaje sobre la falta de un marco teórico y técnico sólido que explique de manera exhaustiva qué son los oráculos, cómo funcionan y cuáles son los principales desafíos y oportunidades que presentan en el contexto de la tecnología *blockchain*. Este marco no solo debe abordar los aspectos técnicos, sino también los legales y regulatorios, considerando que la integración de oráculos en aplicaciones críticas como la *tokenización* requiere de un entorno normativo que proteja a las partes involucradas y asegure la transparencia y la justicia en las transacciones. Por lo que esta investigación dará respuesta a la siguiente interrogante: ¿cuál es la taxonomía teórica y técnica del oráculo en el proceso de *tokenización* para ser integrado en la comprensión de las legislaciones nacionales?

Por otra parte, debe agregarse que la *tokenización*, que convierte activos físicos en representaciones digitales gestionadas en una *blockchain*, es una de las

áreas más prometedoras de la economía digital. Sin embargo, también está plagada de desafíos técnicos y regulatorios, como la validez legal de los *tokens* y la protección de los derechos de los propietarios; la necesidad de desarrollar un marco jurídico adecuado que regule tanto la operación de los oráculos como la validez de los activos *tokenizados* en los mercados legales (Chung y Adriaens, 2024).

Es así como la presente investigación acoge como objetivo general establecer un marco teórico y técnico sobre los oráculos en el proceso de *tokenización* que permita su integración adecuada en las legislaciones nacionales, por lo que se tienen como acciones específicas establecer el marco conceptual de oráculos y el proceso de *tokenización*, desarrollar una taxonomía técnica de los oráculos y elaborar recomendaciones para la regulación de oráculos en las legislaciones nacionales.

Respecto de la metodología para la selección de los textos analizados, se debe tener presente que la literatura sobre oráculos en *blockchain* aún se encuentra en una fase inicial de desarrollo, por ello, la presente investigación no se configuró como una revisión sistemática, sino como una revisión exploratoria de carácter descriptivo. De este modo, se consultaron bases de datos académicas de alta visibilidad, principalmente Scopus, complementadas con fuentes institucionales y repositorios especializados en ingeniería, informática y derecho tecnológico.

La búsqueda se orientó hacia estudios relativos a la taxonomía de los oráculos, abarcando oráculos de *hardware* y *software*, así como modelos centralizados, descentralizados e híbridos. También se incluyeron trabajos vinculados al patrón de diseño *immediateread* y a la interacción entre *blockchain* e IoT. Se aplicó una estrategia de bola de nieve, tomando como punto de partida publicaciones de referencia como Beniiche (2020), Condon et al. (2023) y Ezzat et al. (2022), que permitieron identificar nuevas contribuciones relevantes sobre gobernanza de oráculos, validación descentralizada y desafíos regulatorios. Las fuentes se seleccionaron con base en su pertinencia temática, actualidad (20182025) y rigor metodológico. De este modo, el enfoque metodológico privilegia la amplitud conceptual y la diversidad de perspectivas técnicas con el propósito de sentar las bases para futuras revisiones sistemáticas, que podrán realizarse conforme se consolide el cuerpo teórico y empírico en torno a los oráculos *blockchain*.

2. Fundamentos de los oráculos y la *tokenización*

Los oráculos se entienden como sistemas o mecanismos que proveen información o predicciones basadas en datos y algoritmos complejos. Estos sistemas funcionan como intermediarios entre un conjunto de datos y una decisión automatizada o semiautomatizada, y son importantes en áreas como la predicción de tendencias de mercado, la climatología y, más recientemente, en la tecnología *blockchain* (Corvalán, 2020).

En el ámbito del derecho, los oráculos algorítmicos se han convertido en herramientas clave, utilizando IA para procesar grandes volúmenes de datos jurídicos y ofrecer predicciones sobre posibles resultados judiciales. Estos sistemas ayudan a los profesionales a tomar decisiones más informadas al identificar patrones y correlaciones en datos históricos (Ashley, 2017).

En el ámbito de la tecnología *blockchain*, los oráculos se definen como sistemas que permiten que las cadenas de bloques (*blockchains*), que están inherentemente aisladas del mundo exterior, interactúen con datos externos que no están intrínsecamente disponibles en la cadena. Y es que, para que los contratos inteligentes (*smart contracts*) en la *blockchain* sean útiles en aplicaciones del mundo real, deben ser capaces de interactuar con datos externos como precios de mercado, resultados de eventos deportivos o condiciones climáticas. Aquí es donde los oráculos juegan un papel fundamental (Antonopoulos y Wood, 2018).

Los oráculos en *blockchain* pueden clasificarse en varios tipos según su origen y función, entre ellos, oráculos de *software*, que obtienen datos de fuentes digitales como API o sitios web; oráculos de *hardware*, que recopilan datos del mundo físico mediante dispositivos como sensores; oráculos *inbound*, que introducen datos externos en la *blockchain*; y oráculos *outbound*, que permiten que la *blockchain* envíe datos hacia el exterior (Buterin, 2015).

Hasta el día de hoy, siendo que los contratos inteligentes ejecutan automáticamente acciones basadas en los datos que reciben, cualquier error o manipulación en estos datos puede tener consecuencias graves, como la ejecución incorrecta de transacciones financieras o la creación de *tokens* que no representen adecuadamente los activos subyacentes (Chainlink, 2017). Es decir que este problema atañe a los oráculos, particularmente para que puedan proporcionar datos fidedignos.

Ahora, para comprender el concepto, pueden señalarse algunos ejemplos: oráculos que suministran datos que provienen de fuentes privadas específicas, como certificados académicos o identificaciones gubernamentales. En estos casos, la fuente de los datos, como una universidad o un departamento guber-

namental, es considerada completamente confiable, y la veracidad de los datos es subjetiva, ya que la verdad depende de la autoridad de la fuente emisora. Los datos que proporcionan generalmente se presentan en forma de atestaciones, como pasaportes o registros de logros académicos. Las atestaciones están destinadas a convertirse en un componente importante para el éxito de las plataformas *blockchain* en el futuro, especialmente en lo que respecta a la verificación de identidad o reputación, por lo que es esencial explorar cómo estas plataformas pueden integrar y manejar dichas atestaciones (Antonopoulos y Wood, 2018).

Otros ejemplos que pueden resaltarse son oráculos que proporcionan información desde números aleatorios utilizados en loterías hasta datos de mercados de capitales y tasas de cambio que anclan criptomonedas a monedas fiduciarias. Además, facilitan la activación de contratos inteligentes vinculados a eventos como catástrofes naturales o fluctuaciones meteorológicas, lo que demuestra su importancia en la automatización y precisión de procesos dentro del ecosistema digital. Asimismo, los oráculos gestionan datos críticos para la resolución de mercados de predicción, la verificación de daños en seguros y la interoperabilidad entre *blockchains.* También proveen información relevante como estadísticas de vuelos y precios de mercado del éter, que son fundamentales para diversas aplicaciones descentralizadas (Antonopoulos y Wood, 2018). Ahora bien, es importante conocer los patrones de diseños para obtener una mejor comprensión del estudio, sumado a los conceptos ya analizados.

3. Taxonomía de los oráculos

La clasificación de los oráculos en distintas categorías permite comprender mejor sus capacidades, limitaciones y ámbitos de aplicación. Sin una clasificación clara, los desarrolladores y diseñadores de *blockchain* pueden enfrentar dificultades al elegir el modelo de oráculo adecuado para sus aplicaciones. De igual forma, abogados y reguladores pueden encontrar barreras para evaluar el cumplimiento normativo de los oráculos, especialmente en lo que respecta a la privacidad de los datos y la responsabilidad legal en la validación de información externa. A continuación, se presenta una estructura de clasificación de los oráculos basada en sus fuentes de datos, modelos de confianza, patrones de diseño y formas de interacción con *blockchain*, basada en los trabajos de Al-Breiki et al. (2020), Ezzat et al. (2022) y Sadawi et al. (2022). Así, los oráculos en las cadenas de bloques pueden clasificarse tal como se muestra en la Figura 1:

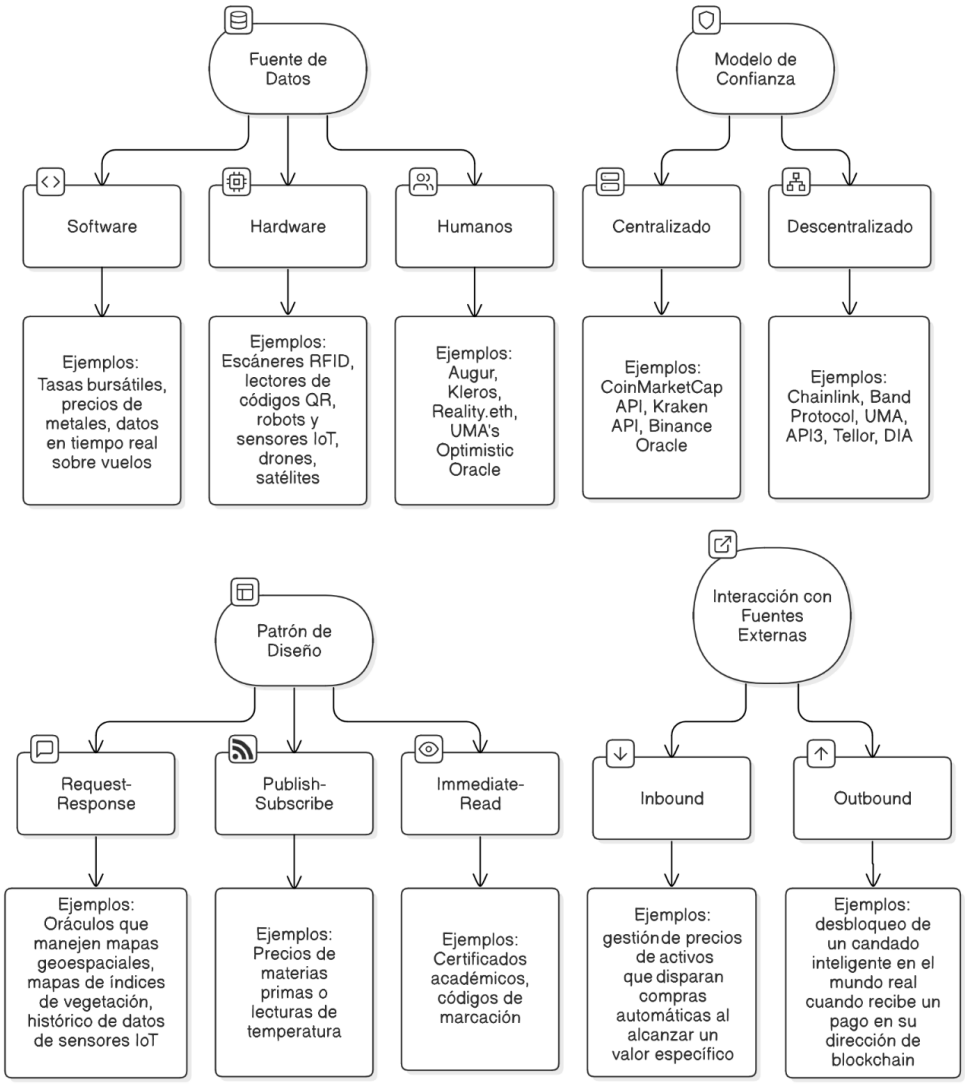

Figura 1. Diagrama de la taxonomía de los oráculos en *blockchain*.
Fuente: elaboración propia.

3.1 Fuentes de datos

3.1.1 Oráculos de *software* y de *hardware*

Dentro de la taxonomía de oráculos en *blockchain*, los oráculos de *software* y los de *hardware* constituyen dos categorías distintas, pero complementarias, cuya interacción resulta esencial para el ecosistema. Los oráculos de *software* o determinísticos se encargan de interactuar con fuentes de datos en internet e integrar la información obtenida en contratos inteligentes. Utilizan bases de datos, servidores y sitios web como principales fuentes, lo que les permite transferir datos en tiempo real a la *blockchain*. Gracias a esta capacidad, se han convertido en una de las opciones más empleadas actualmente, proporcionando información que va desde tasas bursátiles y precios de metales hasta valores de activos digitales o datos en tiempo real sobre vuelos y otros eventos (Beniiche, 2020). No obstante, como advierten Adams y Tomko (2018), esta dependencia de datos externos plantea problemas significativos de representación espacial y de incertidumbre. La información procedente de sensores o servicios web puede no reflejar con precisión la realidad física, lo que podría desencadenar ejecuciones erróneas de contratos inteligentes o disputas legales en transacciones que involucren activos físicos. Estos autores subrayan que el uso de oráculos de *software* para regular procesos ambientales o espaciales exige una validación rigurosa de los datos y una reflexión sobre la gobernanza, pues la simple automatización mediante *blockchain* no resuelve los problemas de precisión geoespacial ni las implicaciones sociales y regulatorias de su aplicación.

Adicionalmente, Adams y Tomko (2018) sintetizan varias complicaciones surgidas en su escenario de transferencia de tierras mediante *blockchain*: (1) problema de propiedad, cuando vecinos cuestionan los límites y generan disputas; (2) problema de trazabilidad, ya que la incertidumbre en las mediciones puede alterar superficies, afectar impuestos y zonas protegidas; (3) propagación de errores, donde una representación numérica imprecisa puede activar bloqueos automáticos en las transferencias; (4) problema de incentivos, al carecer de un tercero de confianza que garantice acuerdos voluntarios y verificados; (5) brecha digital, que pone en riesgo la legitimidad en sociedades con baja alfabetización digital; y (6) problema de gobernanza, pues se debe asegurar el bien común y la protección de áreas de valor especial frente a intereses individuales potencialmente conflictivos.

Por otro lado, los oráculos de *hardware* operan en el mundo físico, recopilando datos a través de tecnologías IoT. Entre los dispositivos que utilizan se encuentran escáneres RFID, lectores de códigos de barras o QR, robots,

sensores ambientales, drones y satélites (Beniiche, 2020). Estos oráculos son especialmente relevantes en aplicaciones críticas como las cadenas de frío en la industria farmacéutica y de alimentos, donde la confiabilidad de las mediciones es esencial. Investigaciones recientes han propuesto arquitecturas seguras para transferir datos de IoT a *blockchain*, integrando módulos de seguridad de *hardware* (HSM) y una infraestructura de clave pública basada en *blockchain* para garantizar autenticidad, trazabilidad, integridad, confiabilidad y frescura de los datos (Gómez-Marín et al., 2023).

A pesar de estos avances, se trata aún de una tecnología en desarrollo. Tal como señalan las conclusiones del trabajo de Gómez-Marín et al. (2023), la operación de las soluciones propuestas depende en gran medida de la infraestructura de Ethereum y de la disponibilidad de sensores seguros con arquitecturas de *hardware* específicas. Este carácter emergente implica que, antes de su adopción masiva, deberán realizarse investigaciones adicionales para extender su uso a otras *blockchains* (como Hyperledger Fabric o Arbitrum), mejorar los tiempos de respuesta y explorar mecanismos de preprocesamiento de datos en IoT antes de su envío a la *blockchain*. Estas limitaciones tecnológicas también abren un espacio para el debate regulatorio: las conclusiones sugieren la necesidad de marcos legales que aborden la responsabilidad de los fabricantes de sensores, la auditoría de oráculos y la trazabilidad de datos en escenarios transfronterizos para evitar riesgos de manipulación o retrasos en las mediciones que afecten contratos inteligentes sensibles.

Finalmente, Adams y Tomko (2018) recomiendan actuar con cautela y no consideran que el momento sea propicio para una "cripto-gobernanza" ambiental plenamente descentralizada. Subrayan que, especialmente en lo referente a la relación de las personas con su entorno, la propiedad de la tierra y la conservación de bienes comunes naturales son imprescindibles marcos institucionales sólidos, certeza jurídica y un mayor entendimiento de la relación entre representación espacial y tecnologías de registro distribuido antes de avanzar hacia una adopción generalizada.

3.1.2 Oráculos humanos

Según Beniiche (2020), los oráculos humanos dependen de individuos con conocimientos especializados para recopilar, verificar y proporcionar información a las redes *blockchain*. Estos expertos certifican datos provenientes de diferentes fuentes y los integran en contratos inteligentes. Utilizan criptografía

para autenticar su identidad, lo que reduce significativamente las posibilidades de fraude. Como ejemplos se tienen a Augur, la cual es una plataforma de predicción descentralizada donde los usuarios actúan como oráculos humanos al reportar los resultados de eventos específicos para liquidar apuestas o predicciones; Kleros, plataforma que utiliza jurados humanos para resolver disputas y validar información en contratos inteligentes, los jurados evalúan las pruebas presentadas y llegan a un consenso; Reality.eth, un oráculo que les permite a los usuarios humanos responder preguntas específicas en la red Ethereum, donde las respuestas son validadas por la comunidad o pueden ser disputadas si hay desacuerdos; UMA's Optimistic Oracle, aunque este oráculo es mayormente automático, los humanos pueden intervenir para verificar datos si hay una disputa sobre la información inicial enviada. Estos oráculos dependen de la honestidad y participación de los humanos para garantizar la precisión de los datos en la *blockchain*. Además, Zhang et al. (2025) comparan estos oráculos con su propuesta LPEA, un enfoque automatizado de aprendizaje por refuerzo que optimiza la selección y validación de datos para contratos inteligentes, diseñado para superar las limitaciones de dependencia humana y reducir sesgos y costos. Resaltan que, aunque los expertos humanos a veces logran un buen desempeño en *recall*, su precisión, costo y consistencia son superados por enfoques automatizados como LPEA. Este contraste sugiere implicancias regulatorias significativas: si los sistemas automatizados ofrecen mayor fiabilidad y menores costos, los marcos legales podrían evolucionar para exigir estándares mínimos de validación automatizada, auditorías de datos y protocolos de intervención humana solo cuando existan disputas complejas. Asimismo, las políticas públicas deberían equilibrar la innovación con la protección de derechos, garantizando transparencia en los algoritmos y mecanismos de apelación para evitar que la sustitución de oráculos humanos comprometa principios de equidad o rendición de cuentas.

3.2 Modelo de confianza

3.2.1 Modelos centralizados y descentralizados

Los oráculos *blockchain* pueden clasificarse según su estructura de gestión en modelos centralizados y descentralizados, cada uno con ventajas y desafíos específicos (Beniiche, 2020). En el modelo centralizado, una sola entidad gestiona el oráculo, actuando como el proveedor de datos. Aunque ofrece mayor eficiencia y rapidez en la transmisión de información, introduce un único punto de

fallo, lo que aumenta los riesgos de confianza y dependencia en la entidad que lo controla. Ejemplos de este tipo son CoinMarketCap API (2025), utilizada como oráculo para proporcionar precios de criptomonedas cuya confiabilidad depende de su control interno; Kraken API (2025), que entrega datos de precios de activos directamente desde el exchange Kraken a contratos inteligentes; y Binance Oracle (2025), ofrecido por el exchange Binance para transmitir datos de mercado a aplicaciones *blockchain*.

Por su parte, el modelo descentralizado distribuye la validación de datos entre múltiples oráculos, eliminando la dependencia de un único punto de fallo. Aunque mejora la confiabilidad y la resistencia a manipulaciones, genera mayor latencia y menor eficiencia en comparación con el modelo centralizado. Los oráculos descentralizados, también llamados "oráculos de consenso", recopilan información de múltiples fuentes para validar los datos, lo que resulta especialmente útil en aplicaciones como la predicción de mercados. Entre sus ejemplos se destacan Chainlink (2025), una red ampliamente utilizada que conecta contratos inteligentes con datos del mundo real mediante múltiples nodos para garantizar precisión y descentralización; Band Protocol (2025), que emplea su propia *blockchain* (BandChain) para conectar datos externos con contratos inteligentes; UMA (Universal Market Access) (2025), que usa un enfoque optimista en el cual los datos se asumen correctos salvo disputa, reduciendo la dependencia de una sola fuente; API3 (2025), el cual permite que las API descentralizadas (dAPIs) se conecten directamente a contratos inteligentes eliminando intermediarios; Tellor (2025), un sistema donde los mineros proporcionan datos y son recompensados o penalizados según su precisión; y DIA (Decentralized Information Asset) (2025), enfocado en datos financieros descentralizados recopilados y validados por su comunidad. Estos sistemas utilizan múltiples fuentes y mecanismos de consenso para asegurar la integridad y confiabilidad de la información. Además, Xiao et al. (2023) destacan que el uso de oráculos descentralizados con modelos de confianza distribuidos entre componentes *on-chain* y *off-chain* es esencial para mantener la correlación de valor entre activos reales *tokenizados* y su representación digital, lo cual aporta mayor seguridad y confiabilidad en ecosistemas complejos como el metaverso.

Esta diferencia entre modelos también tiene implicancias normativas: los reguladores deberán considerar estándares mínimos para la auditoría de datos, mecanismos de supervisión y protocolos de responsabilidad compartida cuando los datos erróneos de un oráculo generen efectos legales o financieros. En modelos centralizados, la supervisión puede enfocarse en la transparencia

y la gobernanza corporativa de la entidad controladora, mientras que en entornos descentralizados se requieren marcos que equilibren la autonomía de los nodos con garantías de integridad, trazabilidad y protección de los usuarios, especialmente en jurisdicciones donde la *tokenización* de activos reales impacta mercados regulados.

3.3 Patrones de diseño

3.3.1 Diseño solicitud-respuesta *(request-response)*

Este tipo de diseño resulta especialmente complejo de implementar porque se emplea para gestionar grandes volúmenes de datos que no pueden almacenarse directamente en un contrato inteligente, como mapas geoespaciales, índices de vegetación o históricos de datos provenientes de sensores IoT. Por ello, dichos datos deben mantenerse fuera de la *blockchain*. Además, el cliente suele requerir solo una fracción específica de toda la información disponible.

Para llevar a cabo este diseño, se utilizan dos componentes principales: *on-chain* y el *off-chain*. El componente *on-chain* corresponde a un contrato inteligente que recibe la solicitud del cliente junto con los argumentos necesarios para definir con precisión la información requerida. Una vez validada la solicitud por el contrato oráculo, los datos se envían fuera de la *blockchain*, ya sea como un evento o mediante una actualización en el estado del contrato.

El componente *off-chain* abarca un *script* que procesa los eventos del oráculo y herramientas externas como bases de datos o aplicaciones para manejar la consulta. Los datos recuperados son firmados por el propietario del oráculo para garantizar su autenticidad y luego enviados de regreso a la *blockchain* en forma de transacción. Dado que estas transacciones se procesan fuera de la cadena, es habitual incluir en la solicitud detalles sobre los permisos del cliente para acceder a los datos solicitados. Además, este tipo de mecanismos, al proteger las rutas de solicitudes y emplear técnicas de ofuscación de tráfico, tienen implicancias regulatorias: podrían requerir normas sobre anonimato de las consultas y estándares de transparencia para equilibrar la privacidad con la auditabilidad de las transacciones de datos en *blockchain* (Gao et al., 2024).

3.3.2 Diseño publicación-suscripción *(publish-subscribe)*

Este patrón de diseño ofrece un servicio de difusión de información a intervalos regulares para suscriptores que han pagado por el servicio. De este modo, los

contratos suscritos reciben actualizaciones de manera periódica cada vez que los datos se modifican. Existen dos principales modalidades de implementación.

La primera es el contrato *on-chain*, donde un contrato inteligente mantiene tanto la lista de suscriptores como los datos almacenados en sus variables. El propietario del oráculo decide el momento de actualizar la información y, cuando lo hace, envía una transacción a los contratos suscritos con los datos renovados.

La segunda es el sistema híbrido. En este caso, el cliente se suscribe enviando una solicitud al oráculo, el cual genera un evento con la información del suscriptor. Estos datos se guardan fuera de la *blockchain*, lo que permite que los suscriptores reciban notificaciones cada vez que se actualizan los datos.

Este patrón es especialmente útil para oráculos que manejan datos dinámicos, como precios de materias primas o mediciones de temperatura. Cada vez que el oráculo actualiza su información, alerta a los usuarios sobre la disponibilidad de nuevos datos. Además, Wang et al. (2019) proponen el esquema AKPS (siglas en inglés para *attribute-keyword based encryption scheme for data publish-subscribe service*), un modelo basado en atributos y palabras clave que emplea cifrado de políticas duales para reforzar la privacidad en sistemas *publish-subscribe*. AKPS les permite a los publicadores cifrar datos de manera que solo los suscriptores con atributos y palabras clave coincidentes puedan descifrarlos, protegiendo así tanto el contenido como las condiciones de acceso. Asimismo, el esquema incluye pruebas de seguridad mejoradas bajo el supuesto DDH (Decisional Diffie-Hellman), garantizando resistencia frente a ataques y fortaleciendo la difusión segura de datos en plataformas en la nube. Esta sofisticación técnica plantea implicancias regulatorias relevantes: las autoridades podrían exigir estándares claros para la protección de datos en sistemas *publish-subscribe*, incluyendo requisitos de auditoría y trazabilidad para garantizar la rendición de cuentas, así como normas que equilibren el anonimato de las consultas con la transparencia necesaria para prevenir abusos o fraudes en entornos descentralizados.

3.3.3 Diseño de lectura inmediata *(immediate-read)*

Este diseño es ideal para gestionar datos pequeños y operaciones rápidas, como certificados académicos o códigos de marcación, que se almacenan directamente en la memoria permanente de un contrato inteligente. Los datos se actualizan mediante transacciones al contrato y, una vez almacenados, quedan disponibles para otras aplicaciones *blockchain* a través de solicitudes directas al oráculo, lo que permite un acceso inmediato a la información requerida.

Al respecto, Wu et al. (2025) proponen mecanismos avanzados de verificación multicapa que combinan firmas umbral de Shamir, árboles de Merkle, cadenas de firmas y filtros *cuckoo*, lo que refuerza la integridad de los datos y previene ataques de falsificación. Además, introducen un sistema de reputación dinámica para las fuentes de datos, incentivando el buen comportamiento y reduciendo riesgos de datos maliciosos. También destacan optimizaciones de rendimiento que disminuyen el tiempo de verificación y la latencia de transmisión en comparación con métodos existentes, particularmente útiles en escenarios de lectura inmediata para datos críticos pequeños. Estas innovaciones sugieren implicancias regulatorias: podrían exigirse auditorías y trazabilidad de las fuentes, así como estándares mínimos de seguridad y mecanismos de verificación independientes para garantizar la confiabilidad de datos sensibles en sectores como la educación o la salud.

3.4 Interacciones con fuentes externas

Los oráculos de entrada (*inbound*) capturan datos del mundo externo y los integran en la *blockchain*. Por ejemplo, gestionan precios de activos que disparan compras automáticas al alcanzar un valor específico.

Por su parte, los oráculos de salida (*outbound*) permiten que los contratos inteligentes envíen datos hacia el mundo externo. Un ejemplo típico es un contrato que desbloquea un candado inteligente cuando recibe un pago en su dirección de *blockchain*.

Un oráculo de entrada podría proporcionar lecturas de sensores a un contrato inteligente, mientras que un oráculo de salida podría activar mecanismos físicos, como desbloquear un dispositivo. Un mismo oráculo puede combinarse en múltiples categorías. Por ejemplo, uno que suministra datos desde el sitio web de una organización se clasifica como un oráculo de *software*, centralizado y de entrada.

4. Los oráculos y la Lex Criptográfica: implicaciones regulatorias

El concepto de Lex Criptográfica se refiere a un sistema legal emergente en el ámbito de la tecnología *blockchain*, basado en la autorregulación mediante algoritmos, códigos, contratos inteligentes y criptografía. Este marco normativo desafía las concepciones tradicionales del derecho al promover la libertad individual y la emancipación. La Lex Criptográfica se percibe como una evolución

de la Lex Mercatoria y la Lex Informática, pero con una autonomía propia derivada de su origen en el entorno digital descentralizado (Calderón Marenco et al., 2024). En el contexto de los oráculos en *blockchain*, plantea preguntas fundamentales sobre cómo regular estos sistemas que, en esencia, son códigos que gobiernan flujos de datos y decisiones automatizadas (Reidenberg, 1998).

Los oráculos, al introducir datos externos en la *blockchain*, deben cumplir con estándares rigurosos de seguridad, transparencia y responsabilidad. Sin embargo, la ausencia de un marco regulatorio específico que aborde los desafíos únicos que plantean los oráculos genera un vacío legal. Este vacío puede ser específicamente problemático cuando los oráculos son utilizados en aplicaciones críticas, como los mercados financieros o la automatización de contratos legales (Antonopoulos y Wood, 2018).

Desde la perspectiva de la Lex Criptográfica, los oráculos podrían considerarse reguladores de facto en el ecosistema *blockchain*, ya que determinan qué información es considerada válida y, por lo tanto, qué transacciones o contratos son ejecutados. Esta capacidad de influir en las decisiones automatizadas subraya la necesidad de establecer un marco legal que supervise tanto la tecnología subyacente como las reglas y principios que guían la operación de los oráculos (Reidenberg, 1998).

Hasta la fecha, no existe una legislación específica a nivel nacional en la mayoría de los países que regule directamente los oráculos para contratos inteligentes. Sin embargo, algunas jurisdicciones han comenzado a abordar aspectos relacionados con la tecnología *blockchain* y los contratos inteligentes, lo que indirectamente podría influir en la regulación de los oráculos. Por ejemplo, la Unión Europea, a través del Reglamento de Mercados de Criptoactivos (MiCA, por sus siglas en inglés), establece un marco regulatorio para los criptoactivos y servicios asociados, lo que podría incluir aspectos relacionados con los oráculos, especialmente en contextos donde los datos suministrados por estos son cruciales para la validez y ejecución de contratos inteligentes.

El Reglamento (UE) 2023/1114 sostiene que la tecnología de registro distribuido (TRD) tiene aplicaciones y modelos de negocio que aún no han sido completamente explorados, lo que podría generar nuevas actividades económicas y oportunidades de empleo en la Unión. No obstante, advierte que la ausencia de un marco general para los mercados de criptoactivos puede generar desconfianza y fragmentación normativa, obstaculizando el desarrollo de mercados innovadores en Europa. Se enfatiza que un marco regulatorio claro y equilibrado es esencial para fomentar la innovación y garantizar que los criptoactivos

se utilicen de manera segura, evitando riesgos para la estabilidad financiera, el buen funcionamiento de los sistemas de pago y la soberanía monetaria.

Además, algunas jurisdicciones como Mónaco y Suiza han avanzado en la creación de marcos legales que reconocen y regulan parcialmente el uso de tecnología *blockchain* y contratos inteligentes, lo que podría allanar el camino para la futura regulación de los oráculos. Sin embargo, una regulación específica y detallada sobre oráculos como entidades autónomas que interactúan con contratos inteligentes aún está en desarrollo y sigue siendo un área de interés emergente en la legislación tecnológica global.

Por lo tanto, mientras la legislación específica sobre oráculos sigue siendo limitada, es probable que, a medida que estos sistemas se desarrollen e integren más profundamente en los entornos legales y financieros, las jurisdicciones consideren la creación de normas más precisas y detalladas para regular su uso. A continuación, se desarrollan los tópicos orientadores de ese proceso.

4.1 Contratación clásica versus contratos autoejecutables

Es posible establecer conexiones entre la taxonomía descrita y los desarrollos doctrinales del derecho informático clásico, especialmente en torno a la formación, existencia y validez de los contratos. Así, los contratos inteligentes autoejecutables, al depender de los oráculos para acceder a información externa, plantean retos respecto a principios jurídicos tradicionales. En el derecho civil y comercial, la validez contractual se sustenta en la autonomía de la voluntad, la causa lícita y el cumplimiento de requisitos formales. Sin embargo, en la Lex Criptográfica, la ejecución automática condicionada por datos oraculares transforma la noción de consentimiento y desplaza el centro de gravedad hacia la fiabilidad tecnológica.

Los hallazgos muestran que este desplazamiento no implica la desaparición de los marcos normativos clásicos, sino la necesidad de reinterpretarlos a la luz de las nuevas dinámicas digitales. Por ejemplo, los oráculos centralizados presentan un único punto de fallo que concentra riesgos de confianza, lo cual recuerda la doctrina de los intermediarios en el derecho informático tradicional. A su vez, los modelos descentralizados, basados en consensos distribuidos, obligan a pensar en equivalentes funcionales a la fe pública registral, pero en un entorno algorítmico.

De igual forma, los patrones de diseño identificados (*request-response*, *publish-subscribe*, *immediate-read*) muestran la manera en que la estructuración técnica

de los oráculos impacta la forma en que se transmiten, validan y auditan los datos. En este punto, el derecho informático clásico ofrece categorías sobre seguridad de la información, integridad de datos y asignación de responsabilidades que resultan fundamentales para interpretar la operación de los oráculos y sus implicancias legales.

En atención a lo expuesto, la Lex Criptográfica no se erige en ruptura absoluta frente al derecho informático, sino en una capa de especialización que exige un diálogo constante con doctrinas tradicionales. La taxonomía de los oráculos sirve, en este sentido, como puente conceptual para comprender cómo los mecanismos técnicos de acceso y validación de datos reconfiguran la teoría general del contrato y los principios de responsabilidad.

4.2. Asignación de riesgos en sistemas descentralizados

Otra dimensión de análisis se relaciona con la responsabilidad y asignación de riesgos en los ecosistemas descentralizados de oráculos. La dependencia de múltiples fuentes de datos, así como la implementación de mecanismos de verificación multicapa, no elimina los problemas de responsabilidad cuando se producen errores, retrasos o manipulaciones en la provisión de información. En el derecho informático clásico, doctrinas como la responsabilidad de los intermediarios y la diligencia debida han servido para asignar riesgos en la prestación de servicios digitales. La taxonomía expuesta, al incorporar modelos centralizados, descentralizados e híbridos, ofrece un marco para reevaluar estas doctrinas.

En los modelos centralizados, la concentración del control en un solo proveedor aproxima su papel al de los prestadores de servicios de certificación digital, quienes históricamente han debido asumir obligaciones de transparencia, seguridad y reparación en caso de fallos. En contraste, los modelos descentralizados distribuyen la validación de los datos entre múltiples nodos, lo que dificulta atribuir responsabilidades individuales y plantea el desafío de diseñar mecanismos de responsabilidad compartida o solidaria.

Los patrones de diseño como el *publish-subscribe* o el *request-response* muestran que la naturaleza de los flujos de datos impacta directamente en la trazabilidad y, por ende, en la posibilidad de auditar y asignar responsabilidades. En este sentido, la doctrina clásica sobre integridad y autenticidad de los datos se convierte en un referente útil para discutir la pertinencia de auditorías obligatorias, esquemas de reputación de oráculos y la posible implementación de seguros tecnológicos que cubran daños ocasionados por fallas en la provisión de datos.

De este modo, la Lex Criptográfica no solo hereda los dilemas clásicos del derecho informático, sino que los intensifica al introducir un grado mayor de autonomía técnica en la ejecución de contratos inteligentes. Se vuelve indispensable entonces un marco regulatorio que combine la experiencia acumulada en la gestión de riesgos digitales con nuevas fórmulas que contemplen la descentralización, la gobernanza algorítmica y la necesidad de salvaguardar principios de seguridad jurídica y confianza legítima en entornos *blockchain*.

4.3 Estandarización y *soft law* en la gobernanza de datos

Se trata de un aspecto que conecta la práctica tecnológica emergente con los marcos normativos del derecho informático clásico. Los resultados de la investigación muestran que la diversidad de modelos y patrones de diseño de oráculos (centralizados, descentralizados, híbridos, *request-response*, *publish-subscribe*, *immediate-read*) plantea desafíos en términos de interoperabilidad y seguridad que trascienden la capacidad regulatoria de los marcos estatales tradicionales.

En este contexto, la experiencia del derecho informático ofrece paralelismos útiles. Así como la Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil (UNCITRAL) o la estandarización de certificados digitales bajo la infraestructura de clave pública (PKI, por sus siglas en inglés) aportaron seguridad y confianza en las primeras etapas del comercio electrónico, la taxonomía de oráculos sugiere la necesidad de estándares internacionales que armonicen principios mínimos de integridad, auditabilidad y transparencia. Estos estándares pueden surgir no necesariamente de la legislación estatal, sino de mecanismos de *soft law* impulsados por organismos internacionales como la International Organization for Standardization (ISO), la International Telecommunication Union (ITU) o entidades sectoriales como la Cámara de Comercio Digital.

Los hallazgos también resaltan que la ausencia de criterios uniformes puede generar fragmentación regulatoria, lo que incrementa los costos de cumplimiento y limita la interoperabilidad entre ecosistemas *blockchain*. De ahí que la Lex Criptográfica deba concebirse no como un marco autónomo y aislado, sino como un sistema que dialoga con instrumentos de *soft law* capaces de establecer reglas de juego claras y compartidas. Dicho diálogo es fundamental para garantizar la confianza transnacional en aplicaciones críticas de oráculos, tales como la *tokenización* de activos, la ejecución de contratos financieros o la certificación de datos en sectores sensibles como salud y educación.

En definitiva, la estandarización técnica y regulatoria no solo favorece la seguridad jurídica, sino que también permite potenciar la innovación al ofrecer un terreno común sobre el cual distintos actores pueden interactuar sin perder certeza normativa. Este hallazgo confirma que la Lex Criptográfica, en su dimensión regulatoria, debe concebirse como una extensión del derecho informático clásico, enriquecida mediante el desarrollo de estándares globales y prácticas de *soft law* que acompañen la rápida evolución tecnológica.

4.4 Responsabilidad civil y protección de datos

La introducción de los oráculos en la automatización de contratos inteligentes no solo redefine las dinámicas de confianza tecnológica, sino que también plantea desafíos jurídicos vinculados a la responsabilidad civil y a la protección de datos personales. Los oráculos, al actuar como intermediarios entre la *blockchain* y el mundo real, pueden generar efectos jurídicos directos cuando suministran datos erróneos o manipulados, afectando la validez y ejecución de contratos inteligentes. Estos escenarios exigen repensar la imputación de responsabilidad y la aplicación de los principios clásicos del derecho civil a contextos descentralizados y automatizados.

En los modelos centralizados, donde el control y la operación del oráculo recaen en un único proveedor, la atribución de responsabilidad resulta más clara. En estos casos, la responsabilidad podría asimilarse a la de los prestadores de servicios de certificación digital o a la de los intermediarios de la sociedad de la información, de acuerdo con la Directiva 2000/31/CE. Este marco impone deberes de diligencia reforzada, transparencia y reparación en caso de fallos, dado que el proveedor centralizado controla tanto la fuente como la transmisión de los datos.

Por el contrario, en los modelos descentralizados o híbridos, la asignación de responsabilidades se complejiza. La validación distribuida de datos entre múltiples nodos dificulta la identificación de un responsable único, por lo que se plantea la pertinencia de aplicar regímenes de responsabilidad objetiva por riesgo tecnológico. Este enfoque reconoce que el daño puede provenir no de un acto ilícito, sino de la autonomía funcional del sistema. Así, las obligaciones de diligencia se trasladan hacia los desarrolladores, operadores y auditores del oráculo, quienes deben implementar protocolos verificables de seguridad y trazabilidad.

Asimismo, el Reglamento (UE) 2022/868 (Reglamento de Gobernanza de

Datos) ofrece un referente útil al establecer mecanismos de gobernanza compartida y responsabilidad distribuida en entornos de datos descentralizados. Su aplicación analógica al caso de los oráculos permitiría asignar deberes de transparencia, conservación de registros y auditoría independiente para prevenir daños derivados de errores o manipulaciones algorítmicas.

Ahora, desde la perspectiva de la protección de datos, los oráculos enfrentan el desafío de cumplir con los principios establecidos en el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), especialmente en lo relativo a la licitud, finalidad, minimización y seguridad del tratamiento (artículos 5, 24, 25 y 32). En sistemas híbridos como Oráculo Terrasacha, que integran sensores IoT, imágenes satelitales y bases de datos institucionales, la posibilidad de tratamiento incidental de datos personales obliga a definir con claridad los roles de responsable del tratamiento (*controller*) y encargado del tratamiento (*processor*).

El Comité Europeo de Protección de Datos (European Data Protection Board, 2025) ha señalado que, en entornos de *blockchain*, los principios de responsabilidad conjunta resultan esenciales, dado que múltiples actores pueden determinar los fines y medios del tratamiento. En este sentido, los desarrolladores y operadores de oráculos deben garantizar la anonimización efectiva de los datos, la aplicación de técnicas de seudonimización y la adopción de medidas de protección desde el diseño (*privacy by design*), conforme al artículo 25 del GDPR.

En cuanto a las transferencias internacionales de datos, los sistemas basados en infraestructura *cloud* —como los alojados en Amazon Web Services o Google Drive— deben observar las restricciones impuestas por el artículo 44 del GDPR, que prohíbe el traslado de datos personales a países sin un nivel adecuado de protección. Esta obligación cobra relevancia en proyectos como Terrasacha, donde el flujo transfronterizo de datos ambientales puede incluir información asociada a personas o comunidades locales, requiriendo salvaguardias contractuales y técnicas específicas.

Por otro lado, el artículo 32 del GDPR exige la implementación de medidas de seguridad apropiadas, como el cifrado y la capacidad de garantizar la integridad, disponibilidad y confidencialidad de los datos. En este sentido, los oráculos deberían adoptar mecanismos criptográficos verificables, auditorías periódicas y registros inmutables para demostrar el cumplimiento de estos requisitos.

4.5 Discusión del caso de estudio: Oráculo Terrasacha

El caso Oráculo Terrasacha constituye una aplicación de las tecnologías emergentes en la gestión ambiental, pues integra en un mismo sistema datos satelitales, consultas catastrales y sensores IoT para el seguimiento y verificación de bonos de carbono. Entre sus principales fortalezas destaca su naturaleza híbrida: combina fuentes de información heterogéneas y niveles de validación cruzada que fortalecen la trazabilidad de los datos ambientales. Esta integración multidimensional permite ofrecer resultados de alta precisión, mitigar el riesgo de errores en una fuente específica y facilitar la auditoría de la información, alineándose con las exigencias de transparencia que demanda la gobernanza de los mercados de carbono.

No obstante, los resultados también exponen limitaciones que deben abordarse para consolidar la fiabilidad y sostenibilidad del sistema. En primer lugar, el carácter centralizado de la gestión de datos plantea un riesgo de concentración de poder informacional, lo cual contrasta con los principios de descentralización y verificabilidad distribuida que sustentan la filosofía *blockchain*. Ello sugiere la necesidad de avanzar hacia modelos de gobernanza de datos basados en consorcios interinstitucionales, que distribuyan la validación y promuevan la interoperabilidad entre distintos actores públicos y privados.

En segundo lugar, la dependencia de servicios de terceros, como Amazon Web Services o Google Drive, introduce vulnerabilidades asociadas a la soberanía tecnológica y la protección de datos sensibles. Estos entornos, aunque robustos, imponen límites de control sobre la información almacenada y pueden generar dependencia estructural en infraestructuras foráneas. La adopción de arquitecturas *cloud* híbridas o de soluciones locales interoperables podría mitigar estos riesgos y fortalecer la autonomía tecnológica del sistema.

En tercer lugar, el caso revela la urgencia de establecer protocolos estandarizados de control y calidad de datos que aseguren la idoneidad en cada etapa del ciclo de información. La heterogeneidad de las fuentes exige mecanismos de verificación automatizada y auditorías independientes que garanticen la integridad de los registros. Sin una estructura formal de validación, el sistema podría enfrentar dificultades para mantener la coherencia y trazabilidad de los datos en procesos regulatorios o financieros.

Otro aspecto crítico se vincula con la alfabetización digital de los usuarios, tanto del sector público como del privado. La complejidad técnica de Terrasacha exige capacidades institucionales para interpretar los indicadores generados y gestionar los contratos inteligentes vinculados a los créditos de carbono.

Sin un fortalecimiento de las competencias digitales y regulatorias, la adopción de la tecnología podría limitarse a usos superficiales o depender de intermediarios tecnológicos, lo que debilita el principio de autonomía y transparencia.

Por último, el marco regulatorio vigente no contempla aún directrices específicas sobre la interoperabilidad de datos ambientales en *blockchain* ni sobre la certificación de oráculos híbridos. Esta ausencia de regulación integral dificulta la homologación de metodologías y puede generar incertidumbre jurídica en torno a la validez de la información oracular en procesos de compensación de emisiones. Por ello, el desarrollo de normas técnico-jurídicas que armonicen la gestión descentralizada de datos con las exigencias de verificación ambiental constituye un reto prioritario.

En síntesis, el caso Terrasacha demuestra el potencial de los sistemas híbridos para fortalecer la trazabilidad y confiabilidad de los datos ambientales mediante la integración de fuentes diversas, pero también evidencia la necesidad de avanzar en la regulación, la alfabetización digital y la soberanía tecnológica para consolidar un modelo de gobernanza de datos realmente sostenible y transparente.

5. Conclusiones

Este estudio analiza tópicos regulatorios y tecnológicos vinculados a los oráculos en *blockchain*, con énfasis en su importancia para la operatividad de los contratos inteligentes y la *tokenización* de activos. A lo largo de la investigación, se ha demostrado que los oráculos son un elemento clave en la integración de datos externos en la *blockchain*.

En primer lugar, se identificó que los oráculos son esenciales para el funcionamiento de los contratos inteligentes, ya que facilitan la automatización de procesos a partir de información externa. Sin embargo, su implementación está asociada a vulnerabilidades relacionadas con la integridad de los datos, la manipulación de información y la dependencia de terceros, lo que exige mecanismos adecuados de supervisión y auditoría.

Desde el punto de vista regulatorio, se detectó una brecha normativa en la gobernanza de los oráculos, lo que dificulta la asignación de responsabilidades en casos de errores o manipulación de datos. En este sentido, la ausencia de marcos normativos específicos propicia incertidumbre jurídica, lo que refuerza la necesidad de desarrollar regulaciones adaptadas a la naturaleza descentralizada y transfronteriza de la *blockchain*. La Unión Europea lidera iniciativas des-

tinadas a incluir disposiciones generales sobre *blockchain* y criptoactivos, pero aún falta avanzar en la regulación específica de los oráculos.

Asimismo, se constató que existen distintos modelos de oráculos, clasificados según su origen de datos (*software*, *hardware*, humanos), su modelo de confianza (centralizado o descentralizado) y sus patrones de diseño (solicitud-respuesta, publicación-suscripción, lectura inmediata). Cada uno de estos modelos presenta ventajas y desventajas en términos de eficiencia, seguridad y confiabilidad, lo que implica la necesidad de elegir el tipo de oráculo más adecuado según el caso de uso.

En el ámbito de la economía digital, los oráculos han demostrado ser fundamentales en la *tokenización* de activos, al permitir la representación digital de bienes físicos en la *blockchain*. Sin embargo, su eficacia depende de la precisión y confiabilidad de los datos que suministran, lo que resalta la importancia de contar con mecanismos que garanticen la veracidad de la información transmitida.

El análisis del caso de estudio Oráculo Terrasacha evidenció cómo la combinación de tecnologías emergentes, inteligencia artificial y *blockchain* puede mejorar la transparencia y eficiencia en la verificación de activos ambientales. No obstante, también mostró la necesidad de establecer marcos regulatorios claros para la validación y gestión de datos externos en *blockchain*.

En conclusión, la implementación de oráculos en *blockchain* requiere un equilibrio entre innovación tecnológica y regulación efectiva. La estandarización de prácticas, el desarrollo de mecanismos de auditoría y la promoción de modelos descentralizados de validación de datos son aspectos esenciales para garantizar la seguridad y confiabilidad en la interacción entre *blockchain* y el mundo real. Por lo tanto, es fundamental que tanto desarrolladores como reguladores trabajen en conjunto para diseñar soluciones que mitiguen los riesgos asociados y fomenten el crecimiento de un ecosistema *blockchain* confiable y transparente.

Bibliografía

Adams, B. y Tomko, M. (2018). A Critical Look at Cryptogovernance of the Real World: Challenges for Spatial Representation and Uncertainty on the Blockchain. *Conference: 10th International Conference on Geographic Information Science (GIScience 2018).* http://doi.org/10.4230/LIPIcs.GIScience.2018.18

Antonopoulos, A. M., y Wood, G. (2018). *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media.

Al-Breiki, H., Rehman, M. H. U., Salah, K. y Svetinovic, D. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access*, *8*, 85675-85685. http://doi.org/10.1109/ACCESS.2020.2992698

API3. (2025). *API3 – Decentralized APIs for Web 3.0*. https://old-docs.api3.org/api3-whitepaper-v1.0.3.pdf

Ashley, K. D. (2017). *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*. Cambridge University Press.

Band Protocol. (2025). *Band Protocol – Unified Data Layer for AI & Web3*. https://www.bandprotocol.com/

Beniiche, A. (2020). A Study of Blockchain Oracles. *Arxiv, 2004.07140*. http://doi.org/10.48550/arXiv.2004.07140

Binance Oracle. (2025). Binance Oracle. https://oracle.binance.com/

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1). https://doi.org/10.1177/2053951715622512

Buterin, V. (2015). *On Public and Private Blockchains*. Ethereum Foundation Blog. https://blog.ethereum.org/2015/08/07/on-public-and-private-Blockchains

Calderón Marenco, E. A., Rodríguez Palacios, T. S., Garzón Solano, J. E. y Ravelo-Franco, G. (2024). Construyendo la delimitación de la Lex Criptográfica. *Revista Jurídica Austral, 5*(1), 551-575. https://doi.org/10.26422/RJA.2024.0501.cal

Chainlink. (2025). *Chainlink 2.0 and the future of Decentralized Oracle Networks*. https://chain.link/whitepaper

Chainlink. (2017). *DevHub CCIP Concepts*. https://docs.chain.link/ccip/concepts#decentralized-oracle-network-don

Chiu, J., y Koeppl, T. V. (2019). *The Economics of Cryptocurrencies- Bitcoin and Beyond*. Staff working papers 19-40. Bank of Canada.

Chung, K. H. Y. y Adriaens, P. (2024). Blockchain technology for pay-for-outcome sustainable agriculture financing: implications for governance and transaction costs. *Environmental Research Communications*, (6), 1-11. https://doi.org/10.1088/2515-7620/ad16f0

CoinMarketCap. (2025). *CoinMarketCap API Documentation*. https://coinmarketcap.com/api/

Condon, F., Franco, P., Martínez, J. M., Eltamaly, A. M., Kim, Y. C. y Ahmed, M. A. (2023). EnergyAuction: IoT-Blockchain architecture for local peer-to-peer energy trading in a microgrid. *Sustainability, 15*(17), 1-28. https://doi.org/10.3390/su151713203

Cong, L. W. y He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies, 32*(5), 1754-1797. https://www.jstor.org/stable/10.2307/48568940

Corvalán, J. G. (2020). Inteligencia Artificial GPT-3, PretorIA y oráculos algorítmicos en el Derecho. *Revista Nuped, 1*(1), 11-52. https://journal.nuped.com.br/index.php/revista/article/view/corvalanv1n1

Decentralized Information Asset. (2025). *Trustless Blockchain Oracles for Any Asset*. https://www.diadata.org/

Diago Diago, M. P. (2021). Ciberactivismo, «Lex» informática, «Blockchain» y oráculos: desafíos en la era digital. En Castelló Pastor, J. J. (Ed.), *Desafíos jurídicos ante la integración digital as-*

pectos europeos e internacionales (pp. 1-15). Thomson Reuters Aranzadi. https://www.millenniumdipr.com/archivos/1624954554.pdf

Doshi-Velez, F. y Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv:1702.08608*. https://arxiv.org/abs/1702.08608

European Data Protection Board. (2025). *Guidelines 02/2025 on processing of personal data through blockchain technologies*. https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf

Ezzat, S. K., Saleh, Y. N. M. y Abdel-Hamid, A. A. (2022). Blockchain Oracles: State-of-the-Art and Research Directions. *IEEE Access*, *10*, 67551-67572, http://doi.org/10.1109/ACCESS.2022.3184726

Gao, R., Xue, Y., Wang, W., Lu, Y., Gui, G. y Xu, S. (2024). Improved Scheme for Data Aggregation of Distributed Oracle for Intelligent Internet of Things. *Sensors, 24*(17), 5625. https://doi.org/10.3390/s24175625

Gómez-Marín, E., Parrilla, L., Tejero López, J. L. y Castillo, E. (2023) Toward Sensor Measurement Reliability in Blockchains. *Sensors, 23*(24), 9659. https://doi.org/10.3390/s23249659

Hierro Viétiez, G. (2021). Introducción al Blockchain, los contratos inteligentes y su relación con el arbitraje. *THEMIS Revista De Derecho*, (79), 299-309. https://doi.org/10.18800/themis.202101.016

Kraken. (2025). *Kraken API Center*. https://docs.kraken.com/api/

Parke, H. W. y Wormell, D. E. W. (1956). *The Delphic Oracle: Its Responses and Operations*. Oxford University Press.

Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review, 76*(3), 553-593.

Risius, M. y Spohrer, K. (2017). A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering, 59*(6), 385-409. http://doi.org/10.1007/s12599-017-0506-0

Sadawi, A. A., Hassan, M. S. y Ndiaye, M. (2022). On the Integration of Blockchain With IoT and the Role of Oracle in the Combined System: The Full Picture. *IEEE Access*, *10*, 92532-92558, http://doi.org/10.1109/ACCESS.2022.3199007

Supra. (2023). *Blockchain Oracles: The Complete Guide*. https://supra.com/academy/Blockchain-oracles/

Tellor. (2025). *Tellor Introduction*. https://docs.tellor.io/tellor

Wang, S., Zhang, Q., Zhang, Y., Sun, J., Chen, J., Sun, X. (2019). Improving the proof of "Privacy preserving attribute-keyword based data publish subscribe service on cloud platforms". *Plos One 14*(2), e0212761. https://doi.org/10.1371/journal.pone.0212761

Warwick, K. (2019). *Synthetix Response to Oracle Incident Our response to today's Oracle incident*. Synthetix. https://blog.synthetix.io/response-to-oracle-incident/

Wu, R., Chen, L., Song, G., Xu, Y. y Wang, X. (2025). Multi-layered retrieval integrity verification mechanism for blockchain oracle. *Peer-to-Peer Networking and Applications*, 18. https://link.springer.com/article/10.1007/s12083-025-01987-w

Xiao, Y., Zhang, N., Lou, W. y Hou, T. (2023). A Decentralized Truth Discovery Approach to the Blockchain Oracle Problem. *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications*, 1-10, http://doi.org/10.1109/INFOCOM53939.2023.10229019

Zhang, S., Song, H., Wang, Q., Shen, H. y Pei, Y. (2025). *A Test Oracle for Reinforcement Learning Software based on Lyapunov Stability Control Theory*. IEEE/ACM 47th International Conference on Software Engineering (ICSE). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=11029785

Legislación citada

Parlamento Europeo y el Consejo de la Unión Europea. (2000). *Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)*. Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, Gobierno de España. https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295

Parlamento Europeo y el Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Parlamento Europeo y el Consejo de la Unión Europea. (2022). Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80835

Parlamento Europeo y el Consejo de la Unión Europea. (2023). 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. Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, Gobierno de España. https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80808

Anexo técnico

Caso de estudio: Oráculo Terrasacha para el manejo de bonos de carbonos de la compensación de emisión mediante soluciones basadas en la naturaleza.

1. Información sobre el Oráculo Terrasacha

Terrasacha (Universidad Cooperativa de Colombia, 2023) representa un caso de estudio relevante para comprender los desafíos regulatorios y tecnológicos en la aplicación de soluciones basadas en la naturaleza para la compensación de emisiones. Esta iniciativa es liderada por la Universidad Cooperativa de Colombia (UCC) en colaboración con la Corporación Innprende, Gobernación del Meta y Arauca, con financiamiento del Sistema General de Regalías (SGR) y el Ministerio de Ciencia, Tecnología e Innovación de Colombia (Minciencias).

El proyecto, titulado *Implementación de acciones para la protección de cuencas de agua y suelos a partir de reforestación con tecnologías emergentes y biotecnología en la región de los Llanos Orientales en los departamentos de Meta y Arauca*, tiene una duración de cuatro años y está diseñado para impulsar la protección de activos ambientales y la descarbonización en estas regiones.

Uno de sus productos, Oráculo Terrasacha (Universidad Cooperativa de Colombia, 2023), busca integrar tecnologías emergentes y biotecnología en proyectos de reforestación, generando modelos de protección y monetización de bosques naturales y cultivos forestales. Su objetivo principal es mitigar los impactos negativos del cambio climático mediante estrategias de compensación de emisiones de gases de efecto invernadero y reforestación, y la creación de incentivos para inversiones sostenibles en mercados de carbono. En este sentido, el oráculo cumple un papel fundamental al proveer información confiable para la automatización de procesos a través de contratos inteligentes en *blockchain*, garantizando transparencia y eficiencia en la verificación de activos ambientales.

La plataforma Oráculo Terrasacha se distingue por integrar múltiples fuentes de datos, incluyendo imágenes satelitales, consultas catastrales y sensores IoT, con el fin de ofrecer un análisis completo del territorio bajo seguimiento. Esto permite les a los usuarios realizar comparaciones del estado de los espacios terrestres en diferentes períodos de tiempo, facilitando la toma de decisiones fundamentadas en proyectos de reforestación y conservación ambiental.

Además, la plataforma cuenta con una API documentada que posibilita la integración de sus servicios en otras aplicaciones, automatizando procesos

y proporcionando acceso a datos en tiempo real. Esta capacidad permite garantizar la transparencia y eficiencia en la gestión de bonos de carbono y otros instrumentos de compensación de emisiones.

Este caso de estudio permite conectar los debates teóricos y normativos abordados en este trabajo con una aplicación concreta de los oráculos en *tokenización*. A partir de Oráculo Terrasacha, se examina cómo los oráculos pueden mejorar la trazabilidad y verificación de datos en proyectos ambientales, alineándose con la necesidad de garantizar la fiabilidad y precisión en sistemas descentralizados. A partir de la taxonomía de los oráculos desarrollada en este trabajo, se identifican las características específicas de Oráculo Terrasacha, como su modelo híbrido de *software* y *hardware*, su enfoque centralizado en la gestión de datos y su integración con fuentes de información externas. Asimismo, el análisis de esta plataforma permite abordar los desafíos legales y técnicos derivados de la integración de fuentes de datos externas a *blockchain*, la automatización de validaciones mediante contratos inteligentes y la asignación de responsabilidades en caso de errores o manipulación de datos. Estos aspectos resultan fundamentales para el desarrollo de un marco normativo adecuado que garantice la seguridad, la transparencia y la confianza en el uso de tecnologías descentralizadas para la compensación de emisiones, en concordancia con la discusión sobre la regulación de los oráculos en este trabajo.

2. Caracterización basada en la taxonomía

Según la taxonomía de los oráculos en *blockchain* descrita anteriormente, y con base en la arquitectura expuesta en la Figura 2 de la plataforma Oráculo Terrasacha, esta se puede clasificar como un oráculo híbrido de *software* y *hardware* con un modelo centralizado y un diseño solicitud-respuesta. En primer lugar, se ajusta a la categoría de oráculo de *software* porque interactúa con fuentes de datos en internet, como ArcGIS REST API y motores de imágenes satelitales. Por otro lado, también puede ser considerado un oráculo de *hardware*, ya que recopila datos directamente del mundo físico mediante sensores IoT, drones y terminales móviles, que posteriormente son procesados y registrados en la *blockchain*. Desde las categorías de los modelos de confianza, y observando la Figura 2, a primera vista el Oráculo Terrasacha pareciera que sigue un modelo descentralizado, puesto que la validación de los datos proviene de múltiples fuentes, reduciendo la dependencia de una única entidad. Sin embargo, sigue un modelo centralizado debido a que una única entidad gestiona el oráculo, ac-

tuando como el único proveedor de datos. En términos de patrones de diseño, el sistema sigue un modelo solicitud-respuesta, ya que les permite a los usuarios generar consultas específicas sobre imágenes satelitales y análisis ambientales, las cuales son procesadas *off-chain* antes de ser registradas en la *blockchain*. Finalmente, es un oráculo de entrada, ya que introduce datos del mundo real en la *blockchain*, facilitando la automatización de contratos inteligentes ambientales con relación al seguimiento de los créditos de carbono.

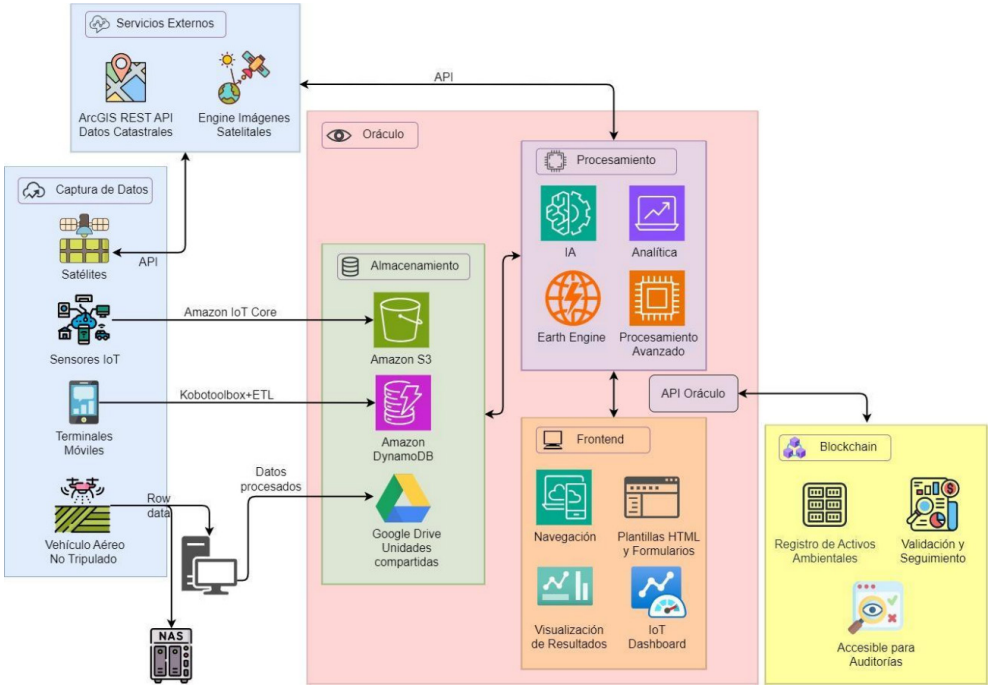

Figura 2. Arquitectura Oráculo Terrasacha. Fuente: elaboración propia.

Desde el punto de vista del funcionamiento, la plataforma Oráculo Terrasacha está orientada a ofrecer una solución robusta para la captura, procesamiento y análisis de datos provenientes de diversas fuentes, tales como satélites, sensores IoT, vehículos aéreos no tripulados (VANT) y dispositivos móviles. Su arquitectura está organizada en módulos claramente diferenciados que trabajan en conjunto para proporcionar análisis y seguimiento precisos y actualizados so-

bre el estado ambiental de regiones bajo estudio. Dichos nódulos son: captura de datos, almacenamiento, procesamiento, frontend, API oráculo y *blockchain*.

2.1 Captura de datos

En la fase de captura de datos, Oráculo Terrasacha se apoya en diversas fuentes de información externas y dispositivos. Los satélites proporcionan imágenes a través de API específicas, como ArcGIS REST API, para obtener datos catastrales y Engine para imágenes satelitales. Además, los sensores IoT, gestionados a través de Amazon IoT Core, recogen datos ambientales en tiempo real, como temperatura, humedad del suelo, y otros parámetros relevantes. El sistema también integra información proveniente terminales móviles y de vehículos aéreos no tripulados (drones o VANT), que recopilan datos en el terreno (*in situ*), gestionados y procesados (ETL: *Extract, Transform, Load*) mediante el uso de herramientas como Kobotoolbox o terminales de procesamiento (*workstation*) ubicados en la región de estudio donde se cargan y procesan la gran cantidad de datos en crudo que capturan los drones y sus sensores, tales como cámara multiespectrales, cámara RGB, cámara hiperespectral y LiDAR, entre otros.

2.2 Almacenamiento

Una vez recopilados, los datos se almacenan en plataformas de almacenamiento en la nube, como Amazon S3, Amazon DynamoDB y Google Drive, los cuales facilitan la gestión y accesibilidad de los datos, asegurando su disponibilidad para análisis posteriores. Esta infraestructura de almacenamiento se complementa con el uso de NAS (Network-Attached Storage) para almacenar grandes volúmenes de datos en crudo que se obtiene de los drones y sus sensores, listos para ser procesados por la *workstation*.

2.3 Procesamiento

Este módulo es crucial para la plataforma Oráculo, donde se llevan a cabo análisis complejos mediante tecnologías avanzadas. Este componente utiliza herramientas como Google Earth Engine para el procesamiento geoespacial y algoritmos de inteligencia artificial y analítica en Python para realizar análisis predictivos y optimización de resultados. Los resultados de estos análisis, tales como índice NDVI (Índice de Vegetación de Diferencia Normalizada, en espa-

ñol), estimaciones de biomasa, carbono capturado por los diferentes ecosistemas monitoreados, se gestionan y se exponen a través de la API Oráculo, la cual actúa como el nexo entre los diversos componentes del sistema y los usuarios externos.

2.4 Frontend

Este módulo les permite a los usuarios interactuar con la plataforma a través de interfaces web que incluyen funcionalidades de navegación, visualización de resultados (métricas históricas, mapas, etc.) y *dashboards* IoT, lo que proporciona una visualización intuitiva de los análisis realizados. Además, se ofrece la posibilidad de integrar formularios HTML y plantillas para facilitar la entrada de datos y la personalización de consultas.

2.5 API Oráculo y *blockchain*

Un aspecto clave de esta arquitectura es su integración con *blockchain*, que garantiza la validación y seguimiento de los datos, asegurando la trazabilidad de las consultas y los resultados. Para este objetivo, la plataforma Oráculo incluye una interfaz de programación de aplicaciones (API, *Application Programming Interface*, por sus siglas en inglés) que permite la interacción entre los usuarios externos y el sistema. Entre algunas funciones, esta API facilita la creación y validación de consultas satelitales, basadas en parámetros como la cédula catastral y las coordenadas geográficas en formato GeoJSON. Tras la creación de la consulta, el sistema genera un análisis que incluye la comparación de datos como la biomasa antes y después de un evento específico, ajustando factores como la nubosidad y la selección de satélites. La información es luego registrada en un sistema *blockchain* externo, asegurando la trazabilidad y confiabilidad de los datos a lo largo del tiempo. Este registro, por ejemplo, usando los Merkle tree, también permite realizar auditorías de los datos procesados, garantizando su integridad y validación ante cualquier posible manipulación. Esta capa asegura que todos los análisis realizados sean confiables y verificables, lo que es esencial para el uso en aplicaciones científicas y de monitoreo ambiental a largo plazo.

En resumen, la arquitectura de Oráculo Terrasacha constituye un sistema robusto que combina tecnologías de vanguardia para el manejo de grandes volúmenes de datos ambientales. Su capacidad para integrar datos de diversas fuentes, procesarlos mediante IA, herramientas de analítica y geoespaciales, y

garantizar la integridad de los resultados a través de *tokenización*, lo convierte en una herramienta poderosa para la gestión, análisis y trazabilidad de datos ambientales, especialmente los relacionados a los bonos o créditos de carbono originados de la compensación de emisión mediante soluciones basadas en la naturaleza.

Roles de autoría y conflicto de intereses

Los autores manifiestan haber cumplido los siguientes roles de autoría: **Calderón Marenco, E. A.:** conceptualización, metodología, investigación; **Aristizabal-Tique, V. H.:** conceptualización, curaduría de datos, validación, escritura, borrador original; **Arenas, P.:** conceptualización, curaduría de datos, validación, escritura, borrador original**. Agón López, J. G.:** escritura, investigación, revisión. **Romero Guido, A. V.:** escritura, investigación, revisión. **Ravelo-Franco, G.:** escritura, investigación, revisión.
Los autores declaran no tener conflicto de interés.