

# **INVESTIGACIONES**



DOI: <http://dx.doi.org/10.4067/S0718-09502025000200009>

## *Blockchain* y contratos inteligentes en el comercio internacional: El rol de los Principios UNIDROIT 2016

Yaritza Pérez-Pacheco\*

### RESUMEN

*Este artículo examina la intersección entre la tecnología blockchain, los contratos inteligentes y los Principios UNIDROIT sobre Contratos Comerciales Internacionales de 2016, evaluando su potencial como marco normativo adaptable ante los retos del comercio digital. Mediante una interpretación sistemática y el análisis de casos como The DAO, se explora la tensión entre la rigidez de los instrumentos autoejecutables y la necesidad de mecanismos de adaptación en contextos de incertidumbre. El estudio identifica tres herramientas jurídicas clave: la autonomía de la voluntad como base para la adaptabilidad, las cláusulas de hardship y fuerza mayor como mecanismos correctivos, y los principios de buena fe y cooperación como salvaguardas éticas frente a la automatización irrestricta. Se proponen soluciones técnicas para su implementación efectiva en entornos digitales y una estrategia de adopción gradual. Se concluye que los Principios funcionan como directrices interpretativas integrables en la lógica contractual automatizada, promoviendo una armonización que combina eficiencia tecnológica con justicia contractual.*

Derecho del comercio internacional; *lex cryptographica*; *soft law*

## *Blockchain and smart contracts in international trade: The role of the 2016 UNIDROIT Principles*

### ABSTRACT

*This article analyzes the intersection between blockchain technology, smart contracts, and the 2016 UNIDROIT Principles on International Commercial Contracts, assessing their potential as an adaptable legal framework in response to the challenges of digital commerce. Through systematic interpretation and the examination of cases such as the DAO, the study explores the tension between the rigidity of self-executing instruments and the need for adaptive mechanisms in contexts of uncertainty. The analysis identifies three key legal tools: party autonomy as a foundation for incorporating adaptability; hardship and force majeure clauses as internal*

---

\* Abogada y Magíster Scientiarum en Derecho Internacional Privado y Comparado, Universidad Central de Venezuela. Doctora en Derecho, Universidad Nacional Autónoma de México. Profesora de Derecho, Universidad Internacional de La Rioja en México, y Universidad Autónoma del Estado de México. ORCID: <https://orcid.org/0000-0003-1435-1517>. Correo electrónico: [yaritzadelcarmen.perez@unir.net](mailto:yaritzadelcarmen.perez@unir.net).

Artículo recibido el 29.10.2024 y aceptado para su publicación el 6.8.2025.

*corrective mechanisms; and the principles of good faith and cooperation as ethical safeguards against unrestricted automation. Technical solutions are proposed for their effective implementation in digital environments, along with a gradual adoption strategy. In conclusion, the principles function as interpretive guidelines that can be integrated into automated contractual logic, promoting a harmonization that balances technological efficiency with contractual justice.*

International trade law; lex cryptographica; soft law

## I. INTRODUCCIÓN

La transformación digital del comercio internacional mediante tecnologías como *blockchain* y contratos inteligentes (*smart contracts*) ha reconfigurado profundamente la organización, celebración y ejecución de transacciones internacionales, introduciendo un modelo descentralizado basado en la ejecución automática de obligaciones previamente estipuladas por las partes<sup>1</sup>. La arquitectura *blockchain*, por su inmutabilidad y transparencia, elimina intermediarios y aporta seguridad y trazabilidad inéditas en operaciones transfronterizas<sup>2</sup>, aunque plantea desafíos jurídicos que requieren revisar los marcos normativos existentes.

En este escenario, la *lex cryptographica* –conjunto de reglas derivadas de protocolos tecnológicos y código computacional– desafía el papel tradicional del Estado en la administración de justicia<sup>3</sup> y acentúa tensiones en los contratos inteligentes, cuya lógica de autoejecución puede entrar en conflicto con la necesidad de adaptación ante circunstancias imprevistas<sup>4</sup>.

Los *Principios UNIDROIT sobre Contratos Comerciales Internacionales* de 2016 (en adelante, Principios UNIDROIT) se perfilan como un instrumento flexible para la armonización jurídica<sup>5</sup>, permitiendo a los operadores jurídicos adaptar sus relaciones contractuales a los retos del entorno digital. Su utilidad se evidenció durante la crisis del COVID-19, cuando facilitaron la adaptación contractual ante situaciones de fuerza mayor y *hardship*<sup>6</sup>.

En el transcurso de más de tres décadas, estos Principios han sido reconocidos por tribunales y árbitros internacionales como herramientas efectivas para resolver controversias complejas<sup>7</sup>, aunque la irrupción de tecnologías descentralizadas exige repensar su alcance y funcionalidad en ecosistema digital que redefine jurisdicción y ejecución contractual.

<sup>1</sup> FETSYAK, 2020.

<sup>2</sup> GARCÍA, 2019.

<sup>3</sup> DE FILIPPI *et al.*, 2022; LÓPEZ, 2021; ORTOLANI 2019, pp. 430-448.

<sup>4</sup> CALDERÓN *et al.*, 2024, pp. 45-78; ORTOLANI 2019, pp. 430-448.

<sup>5</sup> UNIDROIT, 2016.

<sup>6</sup> UNIDROIT, 2020.

<sup>7</sup> MALAGUTI, 2023.

En este sentido, autores como Li (2024) subrayan la urgencia de establecer marcos normativos internacionales más robustos, capaces de abordar problemáticas emergentes como la responsabilidad en sistemas descentralizados<sup>8</sup>. Este diagnóstico es compartido por Singh *et al.*<sup>9</sup> y Gabriel<sup>10</sup>, quienes insisten en la necesidad de conciliar la automatización tecnológica con la seguridad jurídica, propiciando una convivencia funcional entre la *lex mercatoria*, el derecho no estatal y los sistemas jurídicos nacionales e internacionales.

Sobre esta base, el presente artículo examina la aplicabilidad de los Principios UNIDROIT en el contexto de la tecnología *blockchain* y los contratos inteligentes, mediante una interpretación sistemática de algunas de sus disposiciones más relevantes (en particular, los artículos 1.1, 1.4, 1.7, 5.1.3, 6.2.2, 7.1.7 y 7.4.1) y su contraste con las características técnicas de estas innovaciones. Por medio del análisis de casos paradigmáticos –como *The DAO*– y la evaluación de marcos regulatorios seleccionados –como el de Gibraltar y el de Estonia–, se propone un modelo conceptual de “automatización responsable”, orientado a integrar eficiencia tecnológica, flexibilidad jurídica y responsabilidad ética<sup>11</sup>.

Para ello, el artículo se estructura en tres secciones. En primer lugar, se analiza el estado actual de la *blockchain* y los contratos inteligentes, así como los principales desafíos normativos que plantean en el comercio internacional. En segundo lugar, se examina la función interpretativa de los Principios UNIDROIT como herramienta para conciliar ejecución automática y flexibilidad contractual. Finalmente, se propone un marco normativo internacional que promueva una implementación responsable de estas tecnologías, garantizando principios de cooperación transfronteriza, mecanismos de adaptación ante eventos imprevistos y salvaguardas de privacidad, sin sacrificar la equidad contractual.

## II. ESTADO ACTUAL DE LA BLOCKCHAIN Y LOS CONTRATOS INTELIGENTES

### 1. *Fundamentos técnicos y funcionalidad en el comercio internacional*

La tecnología *blockchain* ha creado una infraestructura descentralizada para registrar transacciones, caracterizada por la inmutabilidad, trazabilidad y transparencia de los datos<sup>12</sup>. A diferencia de los sistemas centralizados, opera mediante una red distribuida de nodos que valida bloques criptográficos, impidiendo modificaciones y garantizando un historial verificable de operaciones<sup>13</sup>. Estas características han impulsado su adopción en el comercio internacional, especialmente en contextos con múltiples actores y

<sup>8</sup> LI 2024, pp. 103-130.

<sup>9</sup> SINGH *et al.*, 2020.

<sup>10</sup> GABRIEL 2014, pp. 661-680.

<sup>11</sup> CALDERÓN *et al.*, 2024.

<sup>12</sup> MONRAT *et al.*, 2021.

<sup>13</sup> BECK *et al.*, 2018.

jurisdicciones, donde es esencial asegurar la integridad y autenticidad de la información sin intermediarios<sup>14</sup>.

Los contratos inteligentes constituyen la aplicación más relevante de esta tecnología: son programas que ejecutan automáticamente obligaciones contractuales al cumplirse condiciones previamente establecidas<sup>15</sup>, lo que reduce costos, acelera la ejecución y limita la discrecionalidad, haciéndolos atractivos para operaciones internacionales complejas. Actualmente se aplican en sectores como logística, seguros y compraventa internacional, donde automatizan pagos, penalizaciones y validaciones con precisión<sup>16</sup>. El uso de *oracles* —fuentes externas de datos verificables— amplía su alcance a situaciones contractuales dependientes de hechos objetivos<sup>17</sup>, aunque su adopción generalizada sigue siendo limitada.

## 2. *Problemas estructurales de los contratos inteligentes en el comercio internacional*

La adopción de contratos inteligentes en transacciones internacionales plantea varias dificultades estructurales que afectan su funcionalidad jurídica y operativa. Si bien su valor radica en la ejecución contractual automática y la reducción de intermediarios<sup>18</sup>, su diseño técnico es rígido, lo que impide su adaptación eficaz ante cambios sustanciales en las circunstancias<sup>19</sup>. Esta inflexibilidad adquiere particular relevancia en el contexto del comercio internacional, donde la capacidad de adaptación a condiciones cambiantes constituye un elemento esencial para la viabilidad y sostenibilidad de las relaciones comerciales a largo plazo<sup>20</sup>.

Uno de los principales problemas identificados en la literatura especializada es la dificultad para incorporar mecanismos de modificación o renegociación que respondan a eventos imprevisibles, como desastres naturales, crisis financieras o interrupciones logísticas. En sistemas contractuales tradicionales, estos eventos permiten activar cláusulas que suspenden o ajustan las obligaciones asumidas<sup>21</sup>. Sin embargo, en el entorno digital, el cumplimiento automático de condiciones programadas deja poco margen para soluciones equitativas en tiempo real<sup>22</sup>.

A esta inflexibilidad se suma la complejidad de integrar fuentes externas de información confiable (*oracles*) que permitan detectar automáticamente la ocurrencia de dichos eventos. La dependencia de estas fuentes externas introduce riesgos técnicos y de

<sup>14</sup> UNCTAD, 2023.

<sup>15</sup> FETSYAK, 2020.

<sup>16</sup> MARTÍNEZ y REJAS, 2021.

<sup>17</sup> SÜSS y FRANZCYK, 2021.

<sup>18</sup> FETSYAK, 2020.

<sup>19</sup> SKLAROFF, 2018.

<sup>20</sup> WILLIAMSON, 2021.

<sup>21</sup> FELIU REY, 2018.

<sup>22</sup> WRIGHT y DE FILIPPI, 2015.

gobernanza que comprometen la eficacia de los mecanismos de adaptación<sup>23</sup>. Además, la identificación de un responsable por fallas en la ejecución automatizada plantea problemas adicionales de imputabilidad y reparación en materia de responsabilidad por daño, especialmente en sistemas sin una contraparte claramente definida<sup>24</sup>.

Estas limitaciones no solo afectan la ejecución de las obligaciones contractuales, sino que también ponen en tensión principios fundamentales del derecho comercial internacional, como la equidad, la cooperación entre partes y la revisión por causas sobrevenidas; lo que demanda un análisis normativo que permita responder a estas tensiones sin renunciar a las ventajas operativas de la automatización, lo que será objeto de desarrollo en los apartados siguientes.

### 3. *Experiencias y marcos regulatorios*

La incorporación de tecnologías como la *blockchain* y los contratos inteligentes en el comercio internacional ha generado respuestas regulatorias divergentes y experiencias prácticas que permiten identificar patrones útiles para su gobernanza jurídica. A pesar de la ausencia de un marco internacional uniforme, algunas jurisdicciones han desarrollado modelos normativos incipientes que ofrecen pistas acerca de cómo integrar estas innovaciones sin comprometer la seguridad jurídica.

Uno de los casos paradigmáticos más debatidos es *The DAO*, una organización autónoma descentralizada basada en *blockchain*, lanzada en 2016 en la red Ethereum<sup>25</sup>. El proyecto pretendía funcionar como un fondo de inversión sin intermediarios, administrado mediante votaciones automatizadas de sus participantes. Sin embargo, un fallo en el código permitió la extracción indebida de fondos, lo que obligó a realizar un *hard fork* en la cadena de bloques para revertir la operación<sup>26</sup>. Este caso evidenció que, en ausencia de mecanismos flexibles de revisión o intervención externa, los contratos inteligentes pueden producir consecuencias contrarias al espíritu contractual, aun cuando se ajusten estrictamente al código<sup>27</sup>. También puso en cuestión la aplicabilidad de las categorías tradicionales de responsabilidad en entornos descentralizados.

---

<sup>23</sup> SHELDON, 2021.

<sup>24</sup> FRANKENREITER, 2019.

<sup>25</sup> Para un análisis técnico y normativo del caso *The DAO*, véanse: ATZEI *et al.*, 2017, pp. 164-186; SIEGEL, 2016; DU PONT, 2017. Para el análisis técnico oficial: Ethereum Foundation, 2016: 'The DAO Hard Fork', Ethereum Blog, 20 de julio. Disponible en: <https://blog.ethereum.org/2016/07/20/hard-fork-completed/>

<sup>26</sup> Un *hard fork* es una modificación radical e incompatible del protocolo de una *blockchain* que genera una bifurcación permanente en la red: a partir del cambio, existen dos cadenas independientes que comparten el mismo historial hasta el punto de la bifurcación, pero divergen en adelante. Los nodos que actualizan su *software* siguen la nueva versión, mientras que los que mantienen la versión anterior continúan en la cadena original. Los *hard forks* pueden emplearse para revertir transacciones tras incidentes graves, como ocurrió en *Ethereum* tras el ataque a *The DAO*, o para introducir cambios fundamentales en las reglas de funcionamiento de la red. Véase, ATZEI *et al.*, 2017.

<sup>27</sup> HARVEY, 2019.

A nivel normativo, Gibraltar destaca como una de las primeras jurisdicciones en promulgar legislación específica para regular a los proveedores de servicios basados en tecnologías de registro distribuido, con la *Financial Services (Distributed Ledger Technology Providers) Regulations 2020*<sup>28</sup>. Esta normativa incorpora principios de responsabilidad, seguridad y transparencia, adoptando un enfoque funcional que busca mitigar riesgos sin obstaculizar la innovación<sup>29</sup>.

Otra experiencia relevante es la de Estonia, que ha integrado la *blockchain* en áreas críticas de su administración pública —como los registros notariales, la salud y la identidad digital— bajo el principio de neutralidad tecnológica<sup>30</sup>. Aunque su legislación no regula directamente los contratos inteligentes, su ecosistema digital permite su adopción controlada y jurídicamente segura<sup>31</sup>.

Más allá del ámbito estatal, iniciativas como el *EU Blockchain Observatory and Forum*<sup>32</sup> y las propuestas del *Uniform Law Commission* en Estados Unidos<sup>33</sup> han buscado establecer directrices interpretativas que faciliten la compatibilidad entre los sistemas *blockchain* y los principios del derecho privado. Estas directrices incluyen la elaboración de definiciones precisas para activos digitales y actividades virtuales, la promoción de marcos regulatorios uniformes entre jurisdicciones, la recomendación de *sandboxes* regulatorios para la experimentación controlada, y la formulación de principios generales que permitan aplicar normas de protección de datos, derechos de los consumidores y mecanismos de resolución de disputas en entornos descentralizados. Así, se pretende ofrecer claridad jurídica y seguridad tanto a operadores como a usuarios, facilitando la innovación responsable en el comercio digital internacional<sup>34</sup>.

Estas experiencias muestran que una regulación efectiva no exige necesariamente normas disruptivas, sino una reinterpretación de los principios existentes —autonomía de la voluntad, buena fe, responsabilidad objetiva— a la luz de las nuevas formas de contratación y ejecución descentralizadas. Este enfoque resulta clave para articular soluciones normativas flexibles, donde los estándares internacionales, como los Principios UNIDROIT, puedan dialogar con las prácticas locales y sectoriales en construcción.

---

<sup>28</sup> La versión actualizada de esta ley es del 01/04/2024, se puede consultar su texto completo en el portal oficial *HM Government of Gibraltar, Laws of Gibraltar*, <https://www.gibraltarlaws.gov.gi/legislations/financial-services-distributed-ledger-technology-providers-regulations-2020-4774>

<sup>29</sup> HASSANS INTERNATIONAL LAW FIRM, 2018.

<sup>30</sup> SEMENZIN *et al.*, 2022.

<sup>31</sup> PÁZAITIS y KOSTAKIS, 2018.

<sup>32</sup> EUROPEAN COMMISSION, 2020.

<sup>33</sup> UNIFORM LAW COMMISSION, 2021.

<sup>34</sup> El *EU Blockchain Observatory and Forum* actúa como un centro de conocimiento y diálogo sobre *blockchain* en Europa, emitiendo informes y recomendaciones acerca de tendencias, desafíos regulatorios y mejores prácticas, incluyendo la necesidad de marcos legales adaptativos, interoperabilidad y protección de datos (véase, ELI, 2022; JEREZ *et al.* 2021). La *Uniform Law Commission* ha desarrollado propuestas de leyes modelo para regular actividades con activos digitales y monedas virtuales, con el objetivo de armonizar la legislación estatal y proporcionar mayor certeza jurídica en la economía digital estadounidense (véase, TAUB, 2017).



### III. ASPECTOS ÉTICOS Y LEGALES DEL USO DE LA *BLOCKCHAIN* Y LOS CONTRATOS INTELIGENTES EN EL COMERCIO INTERNACIONAL

#### 1. *Adaptabilidad contractual ante circunstancias imprevistas*

La aplicación de los Principios UNIDROIT a entornos regidos por *blockchain* y contratos inteligentes permite abordar una de las tensiones más significativas del comercio internacional contemporáneo: la que existe entre la rigidez técnica de la ejecución automática y la necesidad de flexibilidad contractual ante eventos imprevistos. La principal ventaja de estos contratos –su capacidad de ejecutar automáticamente términos previamente acordados sin intervención humana– se convierte en una limitación estructural cuando las condiciones de ejecución se ven alteradas por factores externos no previstos por las partes.

Desde una perspectiva de derecho comparado, esta problemática adquiere particular relevancia. Como advierte Li (2024), los contratos inteligentes presentan una rigidez incompatible con la flexibilidad que caracteriza a los ordenamientos jurídicos tradicionales<sup>35</sup>. Tanto el *common law* como el derecho continental disponen de figuras como la imprevisión, el *hardship* o la fuerza mayor, que permiten la revisión, suspensión o incluso la extinción de las obligaciones contractuales cuando circunstancias extraordinarias alteran sustancialmente el equilibrio de las prestaciones. En contraste, este tipo de contratos operan bajo una lógica binaria y determinista, sin contemplar mecanismos internos para adaptar sus efectos jurídicos frente a eventos disruptivos, lo que pone de relieve la necesidad de integrar soluciones híbridas que combinen seguridad tecnológica con adaptabilidad jurídica.

La pandemia por COVID-19 constituye un caso paradigmático que ilustra estas tensiones. Como documenta Dreyzin de Klor<sup>36</sup>, los contratos tradicionales pudieron ajustarse mediante renegociaciones y la aplicación de cláusulas de fuerza mayor o *hardship*. En cambio, los contratos inteligentes, al carecer de canales para la interpretación contextual o la intervención humana, mostraron una rigidez operativa que impidió adaptarlos eficazmente a las nuevas condiciones impuestas por restricciones gubernamentales, cierres de fronteras y disrupciones logísticas. Esta experiencia puso en evidencia la necesidad de incorporar, desde el diseño, mecanismos que habiliten respuestas jurídicas proporcionales ante crisis sistémicas.

---

<sup>35</sup> Véase Li, 2024, quien realiza un estudio comparado donde destaca cómo las limitaciones de los contratos inteligentes, en términos de adaptabilidad ante cambios de circunstancias, ponen de relieve las diferencias entre estos y los contratos tradicionales en diversos sistemas jurídicos. Mientras que en el derecho continental y el *common law* se dispone de principios que facilitan la reinterpretación o anulación de obligaciones bajo circunstancias imprevistas, los contratos inteligentes, al depender de una ejecución estricta y automatizada, carecen de mecanismos que permitan la renegociación o adaptación, evidenciando una necesidad de protocolos híbridos que integren flexibilidad normativa con las ventajas de la tecnología *blockchain*.

<sup>36</sup> DREYZIN DE KLOR, 2021, pp. 145-172.

En este contexto, los Principios UNIDROIT ofrecen un marco conceptual robusto para lo que se podría denominar una automatización responsable. Lo que implica que, lejos de limitar el uso de la tecnología, se promueve su perfeccionamiento jurídico al permitir la integración de cláusulas de flexibilidad, revisión y renegociación que pueden ser programadas *ex ante* y activadas mediante condiciones específicas verificables. Este enfoque se articula en tres niveles normativos:

**Nivel preventivo** (programación de flexibilidad): El principio de autonomía de la voluntad (art. 1.1)<sup>37</sup>, permite a las partes incluir desde la etapa precontractual “cláusulas de escape”, que permitan a una o ambas partes desvincularse o modificar ciertas obligaciones en caso de que ocurran circunstancias excepcionales previamente definidas; posibilidades de “adaptabilidad” contractual, entendida como la capacidad del contrato inteligente para ajustar automáticamente sus condiciones ante determinados cambios en el entorno o en las circunstancias de las partes, como por ejemplo la actualización de precios, plazos de entrega o cantidades, en función de parámetros objetivos y verificables; o “suspensión condicional” para prever la posibilidad de detener temporalmente la ejecución de ciertas obligaciones contractuales cuando se produce un evento específico, sin que ello implique la terminación del contrato, lo que se puede activar automáticamente si, por ejemplo, una autoridad declara estado de emergencia, una cadena logística se interrumpe por causas ajenas a las partes, o se produce un desastre natural<sup>38</sup>.

Estos mecanismos preventivos —cláusulas de escape, adaptabilidad y suspensión condicional— permiten que los contratos inteligentes sean flexibles y resilientes, anticipando respuestas ante imprevistos y asegurando que la ejecución automática no sacrifique la justicia ni la funcionalidad contractual.

**Nivel correctivo** (*hardship* y fuerza mayor como moderadores de la automatización): La cláusula de *hardship* (art. 6.2.2)<sup>39</sup> y la disposición sobre fuerza mayor (art. 7.1.7)<sup>40</sup> actúan como principios correctivos frente a la ejecución automática irrestricta<sup>41</sup>. La cláusula de *hardship* está diseñada para situaciones en las que, debido a acontecimientos extraordinarios e imprevisibles, el cumplimiento del contrato se vuelve excesivamente oneroso para una de las partes, alterando gravemente el equilibrio contractual. En estos casos, la cláusula permite suspender temporalmente la ejecución y abre espacio para la renegociación, de modo que las partes puedan ajustar las condiciones contractuales para restablecer la equidad. Por ejemplo, en un contrato inteligente de suministro internacional, una crisis financiera global que cause una devaluación abrupta de la moneda podría activar la cláusula, permitiendo renegociar los precios o las condiciones de pago.

Por su parte, la **fuerza mayor** se aplica a supuestos de imposibilidad objetiva, es decir, cuando un evento externo, imprevisible y ajeno a la voluntad de las partes —como un desastre natural, una guerra o una pandemia—, hace imposible el cumplimiento de

<sup>37</sup> UNIDROIT, 2016, pp. 8-9.

<sup>38</sup> SPOONER, 2024.

<sup>39</sup> UNIDROIT, 2016, pp. 235-240.

<sup>40</sup> UNIDROIT, 2016, pp. 245-246.

<sup>41</sup> MITCHELL, 2024.

las obligaciones contractuales. La fuerza mayor exime a la parte afectada de responsabilidad por el incumplimiento y, en los contratos inteligentes, se puede programar para que, al verificarse el evento, se suspenda automáticamente la ejecución o se extingan las obligaciones afectadas. Así, por ejemplo, si una autoridad declara un cierre de fronteras por emergencia sanitaria, el contrato inteligente podría suspender automáticamente las obligaciones de entrega y pago hasta que se restablezcan las condiciones normales.

En ambos casos, permiten interrumpir la ejecución automática cuando eventos extraordinarios, imprevisibles y ajenos a la voluntad de las partes tornan inequitativa o inviable la ejecución contractual.

**Nivel reconstructivo** (buena fe como límite ético): El principio de buena fe (art. 1.7) opera como límite material de la automatización<sup>42</sup>. Mediante mecanismos de supervisión y validación continua, puede activarse cuando la ejecución automática produce efectos que vulneran expectativas legítimas, generan enriquecimiento sin causa o resultan claramente inequitativos. En tales casos, podrían integrarse “protocolos de revisión contractual”, para habilitar la evaluación y posible ajuste de las condiciones del contrato ante circunstancias excepcionales, como cambios drásticos en el contexto económico o la aparición de eventos imprevisibles; “compensación automatizada” para que, ante el incumplimiento o la afectación de una de las partes, el sistema ejecute de manera inmediata y objetiva los pagos o indemnizaciones programados, reduciendo la necesidad de intervención manual; o incluso “mecanismos de mediación digital asistida” que permitan ofrecer un canal estructurado para la resolución de disputas, facilitando la intervención de terceros neutrales o algoritmos de conciliación que ayuden a las partes a alcanzar acuerdos justos, todo ello con trazabilidad y transparencia garantizadas por la tecnología *blockchain*<sup>43</sup>.

A estas herramientas se suman las exigencias técnicas que impone su implementación efectiva en entornos automatizados. Tanto la cláusula de *bardship* (art. 6.2.2) como la disposición sobre fuerza mayor (art. 7.1.7) requieren ser integradas en el diseño del contrato inteligente mediante una arquitectura capaz de identificar y validar, de forma objetiva, la ocurrencia de eventos extraordinarios que justifiquen su activación. Esto implica establecer umbrales verificables, fuentes de datos confiables (como oráculos

---

<sup>42</sup> UNIDROIT, 2016, pp. 19-23. PAPANTONIOU, 2020.

<sup>43</sup> Para su mejor comprensión, se ejemplifican cada uno de estos mecanismos de supervisión y validación continua: (i) Ejemplo de protocolos de revisión contractual: en un contrato inteligente de compraventa internacional, si un índice económico (como la inflación) supera un umbral predefinido, el contrato puede activar automáticamente una “ventana de revisión” que permite a las partes renegociar precios o plazos antes de continuar con la ejecución automatizada; (ii) Ejemplo de compensación automática: en seguros de viaje, si un vuelo se retrasa más allá de un umbral acordado, el contrato inteligente accede a la información de vuelos (por medio de un oráculo) y, si se confirma el retraso, transfiere automáticamente la compensación al pasajero sin que este deba presentar una reclamación formal; (iii) Ejemplo de mecanismos de mediación digital asistida: en un conflicto concerniente a la interpretación de una cláusula contractual, el contrato inteligente puede activar una función que remite el caso a una plataforma de mediación digital. Allí, un mediador humano o un sistema automatizado ayuda a las partes a alcanzar un acuerdo, dejando constancia de todo el proceso y del resultado en la *blockchain*. Véase, GÓMEZ, 2023; MONTECINOS 2022; FETSYAK, 2020.

descentralizados) y mecanismos de pausa o suspensión automática que actúen sin necesidad de intervención humana directa, pero en conformidad con criterios jurídicos previamente establecidos<sup>44</sup>.

En conjunto, estos tres niveles normativos evidencian que la automatización responsable no limita el potencial de la tecnología *blockchain*, sino que lo canaliza conforme con parámetros de equidad y previsibilidad jurídica. Lejos de ser meros ejecutores de código, los contratos inteligentes pueden evolucionar —mediante la incorporación de los Principios UNIDROIT— en instrumentos normativamente sensibles, capaces de responder proporcionalmente a las contingencias del comercio internacional. Esta transformación no implica renunciar a la eficiencia operativa, sino integrarla en una arquitectura legalmente sostenible que combine la seguridad de la ejecución automática con la justicia de la flexibilidad.

## 2. Seguridad técnica y atribución de responsabilidad

La cuestión de la responsabilidad en entornos descentralizados presenta desafíos particulares que trascienden las consideraciones puramente técnicas. Murphy y Selvadurai (2024) demuestran que la complejidad de esta problemática deriva de tres factores interrelacionados: la multiplicidad de actores involucrados (desarrolladores, operadores de nodos, usuarios), la naturaleza distribuida de la toma de decisiones y la ausencia de una autoridad central identificable. Su análisis revela que los marcos normativos actuales resultan insuficientes para atribuir responsabilidad en sistemas que operan sin una contraparte central claramente definida, evidenciando la necesidad crítica de establecer marcos normativos claros que anticipen estos escenarios de responsabilidad difusa<sup>45</sup>.

La atribución de responsabilidad se torna particularmente compleja en el contexto de plataformas descentralizadas, donde la multiplicidad de actores involucrados dificulta la determinación precisa de responsabilidades<sup>46</sup>. Esta complejidad se manifiesta especialmente en casos de fallos técnicos o vulnerabilidades del sistema. Esta problemática fue ejemplificada de forma temprana por el caso *The DAO*, tal como se analizó anteriormente, cuando este incidente expuso la dificultad de determinar responsabilidades en ausencia de contrapartes claramente identificables, planteando interrogantes que aún hoy persisten en la aplicación del derecho a sistemas descentralizados.

La naturaleza distribuida de la tecnología *blockchain* genera interrogantes acerca de la atribución de responsabilidad: ¿Debe recaer la responsabilidad principal en los desarrolladores del código, en los operadores de la plataforma, o en las partes que utilizan el sistema? La respuesta a estas cuestiones requiere un análisis que considere tanto

---

<sup>44</sup> LÓPEZ, 2021.

<sup>45</sup> MURPHY y SELVADURAI, 2024.

<sup>46</sup> FLORIDI, 2016.

los aspectos técnicos como los principios de responsabilidad contractual en el derecho internacional<sup>47</sup>.

Los Principios UNIDROIT proporcionan un marco conceptual valioso para abordar estos desafíos mediante tres dimensiones complementarias. En primer lugar, el principio de buena fe y diligencia (art. 1.7) establece la base para exigir que todas las partes involucradas implementen medidas preventivas adecuadas, incluyendo auditorías de código y protocolos de seguridad robustos. En segundo lugar, el principio de cooperación entre las partes (art. 5.1.3)<sup>48</sup> facilita la implementación de mecanismos colaborativos para la verificación y validación de datos externos, particularmente relevante en el contexto de los oráculos. Finalmente, la cláusula sobre responsabilidad por incumplimiento (art. 7.4.1)<sup>49</sup> permite adaptar los estándares tradicionales de responsabilidad al contexto descentralizado, asignando consecuencias jurídicas cuando se verifique una actuación negligente o una omisión grave que afecte el cumplimiento del contrato.

Así, mediante estos principios, se favorece una interpretación jurídica que reconoce la complejidad técnica de los entornos descentralizados sin renunciar a la exigencia de responsabilidad. Esta aproximación contribuye al desarrollo de una arquitectura regulatoria coherente que incentive la diligencia en el diseño de sistemas automatizados y la cooperación en la resolución de conflictos derivados de su operación.

### 3. *Privacidad y transparencia en entornos blockchain*

El equilibrio entre transparencia y privacidad en los entornos *blockchain* representa uno de los dilemas más complejos de la economía digital contemporánea. Esta tensión se expresa no solo a nivel técnico, sino también normativo, particularmente en relación con la inmutabilidad de los registros y el cumplimiento de estándares internacionales de protección de datos. El caso del Reglamento General de Protección de Datos (RGPD) de la Unión Europea<sup>50</sup> evidencia con claridad estos desafíos, al exigir garantías jurídicas que parecen entrar en conflicto con los principios estructurales de la tecnología *blockchain*<sup>51</sup>.

Uno de los puntos más controvertidos es el derecho al olvido. Esta figura, que exige la posibilidad de supresión o rectificación de datos personales, entra en aparente contradicción con la característica de inmutabilidad de las cadenas de bloques públicas<sup>52</sup>. Una vez inscritos, los datos no pueden ser modificados ni eliminados sin comprometer la integridad del sistema. Ante esta dificultad, los Principios UNIDROIT ofrecen normas alternativas que permiten reconceptualizar la autonomía de la voluntad (art. 1.1) y la buena fe (art. 1.7) como fundamentos para diseñar contratos inteligentes que integren, desde su origen, salvaguardas proactivas de privacidad.

<sup>47</sup> KÜNNEMANN *et al.*, 2018.

<sup>48</sup> UNIDROIT, 2016, pp. 165-168.

<sup>49</sup> UNIDROIT, 2016, pp. 293-294.

<sup>50</sup> Véase CIRONE, 2021, pp. 15-35.

<sup>51</sup> ZAFAR, 2025.

<sup>52</sup> FINCK, 2019.

La transparencia operativa de las *blockchains* públicas, aunque valiosa para la trazabilidad y la integridad de las transacciones, también genera riesgos en términos de confidencialidad comercial y privacidad individual. Herramientas de análisis de datos permiten inferir identidades y reconstruir relaciones contractuales, incluso en sistemas que no revelan directamente información personal<sup>53</sup>. En consecuencia, la protección de datos en estos entornos no puede limitarse a la anonimización básica, sino que requiere soluciones más sofisticadas e integradas desde la arquitectura del sistema.

Estas soluciones incluyen el uso de cifrado avanzado, control de acceso diferenciado para separar datos visibles y confidenciales, pseudonimización y *tokens* de referencia para proteger la identidad, almacenamiento externo interoperable para datos sensibles, borrado funcional mediante destrucción de claves, arquitecturas de doble capa donde los datos personales no se almacenen directamente en la cadena, auditorías periódicas, protocolos de notificación ante vulneraciones, y la minimización de datos con eliminación automática tras su uso. También abarcan la transparencia algorítmica, el uso de técnicas criptográficas avanzadas como los *zero-knowledge proofs*<sup>54</sup>, y la integración de inteligencia artificial para mejorar la detección de fraudes y la encriptación.

Adicionalmente, la naturaleza transnacional de las operaciones *blockchain* introduce complejidades en la aplicación territorial del derecho. Las transacciones pueden involucrar nodos y participantes distribuidos en distintas jurisdicciones, con regímenes divergentes en materia de protección de datos personales<sup>55</sup>. Este desajuste entre la lógica descentralizada de la tecnología y la fragmentación normativa de los sistemas jurídicos estatales exige herramientas que articulen flexibilidad contractual y respeto por normas imperativas.

En este contexto, los Principios UNIDROIT ofrecen un marco funcional para armonizar eficiencia tecnológica y protección jurídica. En primer lugar, el principio de buena fe y diligencia (art. 1.7) establece un estándar que impone a las partes la obligación de prever y aplicar medidas de protección de datos desde el diseño, incluyendo auditorías, protocolos de cifrado y monitoreo continuo de riesgos. Esta diligencia no se limita a la fase de programación, sino que se debe mantener durante toda la vigencia del contrato inteligente.

En segundo lugar, el artículo 5.1.3, que consagra el deber de cooperación entre las partes, adquiere especial relevancia en el contexto de la gestión compartida de datos. Este principio justifica la implementación de mecanismos técnicos de verificación conjunta, auditoría distribuida y validación mutua del cumplimiento de estándares de privacidad, en consonancia con el principio de responsabilidad proactiva establecido por el RGPD, que exige a los responsables del tratamiento de datos no solo cumplir con la normativa, sino también adoptar una actitud consciente y preventiva, aplicando medidas técnicas y organizativas apropiadas para garantizar y poder demostrar en todo

---

<sup>53</sup> BELEN-SAGLAM *et al.*, 2023.

<sup>54</sup> FATIMA y SENTHILKUMAR, 2025.

<sup>55</sup> ZAFAR, 2025.

momento que el tratamiento de los datos personales es conforme con el Reglamento. Esto implica analizar los riesgos, documentar las medidas implementadas y estar en condiciones de acreditar ante interesados y autoridades que la protección de datos se gestiona de manera efectiva y transparente<sup>56</sup>.

En tercer lugar, el artículo 1.4 de los Principios, que reconoce la primacía de las normas imperativas<sup>57</sup>, habilita la incorporación automática de disposiciones regulatorias de protección de datos en los contratos inteligentes, sin necesidad de intervención posterior. Esto permite que, incluso en contextos automatizados y transnacionales, se mantenga el cumplimiento de normas como el RGPD sin sacrificar la eficiencia del sistema descentralizado.

Desde esta perspectiva, la aplicación de los Principios UNIDROIT permite avanzar hacia una concepción de “privacidad por diseño automatizada”, donde la protección de datos no se introduce como una limitación externa, sino como una característica estructural del contrato inteligente. En este modelo, los mecanismos de protección operan de forma nativa dentro de la lógica del sistema, equilibrando las exigencias de trazabilidad, eficiencia y respeto a los derechos fundamentales, a la vez que permiten preservar la integridad y la auditabilidad de la información sin comprometer la confidencialidad exigida por los marcos regulatorios<sup>58</sup>.

Esta convergencia entre innovación tecnológica y protección jurídica redefine los estándares de cumplimiento en el comercio internacional (por ejemplo, cumplimiento de leyes aduaneras, tratados internacionales, controles de exportación, protección de datos, normas de calidad, y mecanismos de resolución de disputas, entre otros aspectos), cuya observancia protege a las partes de sanciones, retrasos, riesgos legales y comerciales, y contribuye a la confianza y legitimidad de las transacciones. Los contratos inteligentes diseñados conforme con los Principios UNIDROIT no solo optimizan la ejecución automática, sino que también garantizan la preservación de la privacidad como valor sustantivo, consolidando así una arquitectura jurídica más robusta y legítima para las relaciones transfronterizas en la era digital.

#### 4. *Modernización de los mecanismos de resolución de disputas*

Los métodos tradicionales de solución de controversias, desarrollados para entornos contractuales convencionales, requieren adaptaciones sustanciales para responder eficazmente a las particularidades de los contratos inteligentes y la descentralización estructural de estas tecnologías.

El surgimiento de plataformas de arbitraje descentralizado, como Kleros<sup>59</sup>, ejemplifica este nuevo paradigma. Estas plataformas utilizan *blockchain* para implementar

---

<sup>56</sup> AEPD, s.f.

<sup>57</sup> UNIDROIT, 2016, pp. 12-14.

<sup>58</sup> Véase MARTÍNEZ, 2024.

<sup>59</sup> Kleros es una plataforma de arbitraje descentralizado basada en *blockchain* que utiliza contratos inteligentes y jurados seleccionados aleatoriamente entre usuarios que apuestan el *token* PNK. Cuando surge

procedimientos automatizados que, sin prescindir completamente de la intervención humana, permiten a las partes seleccionar un jurado descentralizado encargado de emitir decisiones sin necesidad de una autoridad estatal<sup>60</sup>. Esta configuración, basada en mecanismos criptográficos y algoritmos de selección, refleja una elevada autonomía contractual y encuentra fundamento en el artículo 1.1 de los Principios UNIDROIT, que reconoce la libertad de las partes para diseñar sus mecanismos de resolución conforme con sus necesidades.

No obstante, este modelo plantea importantes interrogantes jurídicos. Como señalan Lezcano y Ortolani, la falta de supervisión judicial y la dependencia de procesos algorítmicos generan preocupaciones relativas a la imparcialidad, la competencia técnica de los decisores y las garantías mínimas del debido proceso<sup>61</sup>. La ausencia de estándares claros acerca de cómo asegurar transparencia, derecho de defensa y revisión de decisiones automatizadas exige repensar el modo en que se implementan los principios fundamentales de justicia procesal en entornos digitales.

Los Principios UNIDROIT proporcionan herramientas para orientar esta adaptación normativa. El principio de buena fe (art. 1.7) impone la obligación de estructurar estos mecanismos con estándares éticos que aseguren el respeto a las expectativas legítimas de las partes, la equidad en el proceso y la integridad en la decisión. En sistemas descentralizados, ello implica garantizar la transparencia de los algoritmos de selección de árbitros, el acceso efectivo a los fundamentos de las decisiones y la existencia de canales de impugnación adecuados.

El deber de cooperación entre las partes (art. 5.1.3) adquiere una nueva dimensión en la resolución de disputas en entornos digitales, debido a que los procedimientos se desarrollan en plataformas programadas y con intervención mínima, la responsabilidad de las partes en proveer información clara, completa y accesible adquiere carácter fundamental. Así, la cooperación no se limita a aspectos procedimentales, sino que se extiende a la configuración y validación conjunta del sistema de resolución adoptado.

Desde una perspectiva funcional, la automatización parcial de los procesos de resolución de disputas puede ofrecer beneficios significativos: reducción de tiempos, disminución de costos, mayor accesibilidad, consistencia en la aplicación de criterios y trazabilidad de todo el procedimiento<sup>62</sup>. Estas ventajas son particularmente valiosas en el comercio internacional, donde las distancias geográficas, los costos judiciales y las diferencias normativas tradicionalmente dificultan el acceso a mecanismos eficaces de solución.

Sin embargo, para que esta modernización sea jurídicamente sostenible, se debe alcanzar un equilibrio entre eficiencia y salvaguarda de derechos fundamentales. Los

---

una disputa, Kleros asigna un jurado de participantes independientes que analizan las pruebas y votan la resolución. Los jurados son incentivados económicamente para votar de forma coherente y justa, y la decisión se ejecuta automáticamente mediante *smart contracts*, sin intervención de una autoridad estatal.

<sup>60</sup> BERGOLLA *et al.*, 2022.

<sup>61</sup> LEZCANO, 2024; ORTOLANI 2019; KÖKSAL, 2024.

<sup>62</sup> SEJKO, 2024.



modelos híbridos –que automatizan etapas procedimentales (notificaciones, gestión documental, seguimiento) pero reservan la resolución sustantiva a decisión humana– ofrecen un enfoque intermedio que combina lo mejor de ambos mundos<sup>63</sup>. Este esquema permite mantener el control humano en las valoraciones complejas, sin sacrificar la eficiencia operativa que la *blockchain* puede aportar.

Los Principios UNIDROIT permiten construir este equilibrio mediante reglas flexibles que se adaptan a contextos tecnológicos sin abandonar los principios del debido proceso. Lejos de constituir una barrera, su aplicación posibilita el desarrollo de procedimientos modernos que preservan la legitimidad, la confianza y la seguridad jurídica.

#### IV. HACIA UN MARCO NORMATIVO PARA REGULAR *BLOCKCHAIN* Y CONTRATOS INTELIGENTES EN EL COMERCIO INTERNACIONAL

##### 1. *Cooperación internacional como fundamento regulatorio*

La naturaleza transfronteriza de las transacciones basadas en *blockchain* exige un enfoque regulatorio coordinado que supere los límites de las iniciativas nacionales fragmentadas<sup>64</sup>. Los vacíos normativos y las tensiones jurisdiccionales no se pueden resolver mediante esquemas aislados que ignoren la arquitectura descentralizada de estas tecnologías<sup>65</sup>, por lo que la armonización internacional se vuelve una necesidad funcional para garantizar la seguridad jurídica y la eficiencia en el comercio digital global<sup>66</sup>.

La falta de coordinación entre sistemas jurídicos genera fragmentación normativa y dificulta el desarrollo de soluciones sostenibles para el comercio internacional, reforzando la urgencia de establecer estándares armonizados que proporcionen certeza jurídica sin limitar la innovación<sup>67</sup>. Así, la cooperación internacional es el mecanismo idóneo para fomentar la convergencia regulatoria y la integración de requerimientos locales dentro de un marco jurídico coherente a nivel global<sup>68</sup>.

Los Principios UNIDROIT ofrecen un modelo útil para este fin, ya que su flexibilidad permite adaptar principios generales a las especificidades de cada jurisdicción, facilitando la compatibilidad entre sistemas diversos<sup>69</sup>. Además, los principios de buena fe y cooperación (arts. 1.7 y 5.1.3) establecen bases éticas para la colaboración entre autoridades regulatorias, promoviendo el intercambio de información, el reconocimiento mutuo de auditorías y la coordinación en la supervisión de plataformas transfronterizas.

<sup>63</sup> SEJKO, 2024.

<sup>64</sup> LEHMANN, 2021.

<sup>65</sup> CALDERÓN *et al.*, 2024, pp. 45-78. LEHMANN, 2021. DE FILIPPI *et al.*, 2022.

<sup>66</sup> BENSON *et al.*, 2024.

<sup>67</sup> JIANG, 2022.

<sup>68</sup> GIBRALTAR FINANCIAL SERVICES COMMISSION, 2020; SEMENZIN *et al.*, 2022.

<sup>69</sup> UNIDROIT, 2016.

La implementación de este enfoque requiere institucionalidad especializada. Un organismo internacional –inspirado en el modelo de UNIDROIT– podría facilitar la armonización progresiva de estándares técnicos y normativos, impulsar el diálogo interjurisdiccional y generar principios comunes adaptables a diversas realidades jurídicas<sup>70</sup>. Asimismo, la cooperación internacional debe contemplar la dimensión técnica de la regulación de *blockchain*, incluyendo la interoperabilidad entre protocolos, estandarización de auditorías y mecanismos comunes de verificación de identidad, indispensables para la operatividad de los marcos jurídicos en la práctica<sup>71</sup>.

Este modelo no exige uniformidad normativa absoluta, sino una compatibilidad funcional entre sistemas jurídicos diversos. Así, la cooperación internacional se consolida como el pilar fundamental para regular tecnologías emergentes en escenarios globales, asegurando la integración comercial y la seguridad jurídica en el entorno digital<sup>72</sup>.

## 2. Marco jurídico integrado para la resolución de disputas

La eficacia de cualquier regulación sobre *blockchain* depende en gran medida de su capacidad para resolver disputas de manera eficiente y equitativa en contextos de automatización y descentralización. Los mecanismos tradicionales presentan limitaciones frente a transacciones ejecutadas automáticamente en redes distribuidas.

La determinación de jurisdicción y ley aplicable es uno de los principales retos. Como advierten Ortolani<sup>73</sup> y Martínez<sup>74</sup>, los criterios territoriales clásicos resultan inadecuados ante operaciones que se desarrollan en múltiples nodos sin localización física definida, por lo que deben sustituirse por criterios como la elección de ley por las partes, el lugar de cumplimiento de las obligaciones o la residencia habitual de los contratantes.

En este escenario, los Principios UNIDROIT ofrecen una base conceptual adecuada. El principio de autonomía de la voluntad (art. 1.1) permite pactar anticipadamente la ley aplicable y los métodos de resolución de disputas, reduciendo la incertidumbre y favoreciendo la previsibilidad jurídica<sup>75</sup>. Esta selección puede integrarse directamente en el *smart contract*<sup>76</sup>.

El arbitraje híbrido surge como una opción funcional al combinar eficiencia tecnológica y garantías procesales<sup>77</sup>. Estos modelos emplean *blockchain* para la gestión documental y notificaciones automatizadas, reservando el análisis jurídico a la intervención humana. Los Principios UNIDROIT, al establecer estándares de buena fe y cooperación, ofrecen una base jurídica común para estas soluciones mixtas.

<sup>70</sup> LEHMANN, 2021.

<sup>71</sup> JIANG, 2022.

<sup>72</sup> BENSON *et al.*, 2024.

<sup>73</sup> ORTOLANI 2019, pp. 430-448.

<sup>74</sup> Véase MARTÍNEZ y REJAS, 2021.

<sup>75</sup> UNIDROIT, 2016, pp. 8-9.

<sup>76</sup> LEZCANO, 2024.

<sup>77</sup> BERGOLLA *et al.*, 2022.

El principio de buena fe (art. 1.7) exige transparencia en los algoritmos de selección de árbitros, claridad en los criterios de decisión automatizada y mecanismos que aseguren que la eficiencia no sacrifique la equidad procesal, obligando a las partes a entregar información veraz y completa<sup>78</sup>. Por su parte, el deber de cooperación (art. 5.1.3) sustenta la configuración conjunta de parámetros esenciales del sistema, como la definición de condiciones objetivas, la elección de fuentes y protocolos de escalamiento a intervención humana cuando la resolución automática sea insuficiente.

El desarrollo de protocolos escalonados mejora la eficiencia: disputas menores se pueden resolver mediante reglas codificadas, mientras que los conflictos complejos se escalan automáticamente al arbitraje humano, optimizando recursos y tiempo<sup>79</sup>.

La incorporación de mecanismos de revisión limitada equilibra agilidad y salvaguardas sustantivas<sup>80</sup>. Los Principios UNIDROIT brindan criterios para tal revisión: actos que vulneren manifiestamente la buena fe, resulten desproporcionados o ignoren circunstancias justificadas —como situaciones de *hardship*— pueden ser considerados por intervención humana sin comprometer la certeza del sistema<sup>81</sup>.

En definitiva, estos elementos configuran un marco de resolución de disputas que aprovecha las ventajas estructurales de la tecnología *blockchain* —transparencia, inmutabilidad, eficiencia— sin renunciar a los principios esenciales del debido proceso. Así, los Principios UNIDROIT consolidan un puente operativo entre la innovación tecnológica y la justicia contractual en el comercio internacional<sup>82</sup>.

### 3. *Protección ante eventos imprevistos*

Un marco normativo eficaz debe prever mecanismos operativos para enfrentar circunstancias extraordinarias que puedan afectar la ejecución de contratos inteligentes, garantizando eficiencia y equidad contractual. La experiencia de la pandemia por COVID-19 evidenció la necesidad de estructuras flexibles, ya que la ejecución automática puede convertirse en una vulnerabilidad sistémica frente a crisis de gran escala<sup>83</sup>.

Los Principios UNIDROIT ofrecen herramientas específicas para estos escenarios mediante fuerza mayor (art. 7.1.7) y *hardship* (art. 6.2.2). Como destacan Nguyen (2021) y Dreyzin de Klor<sup>84</sup>, estas figuras permiten introducir flexibilidad en entornos automatizados sin renunciar a la tecnología. Su incorporación en contratos inteligentes exige una reconceptualización: no deben ser excepciones externas, sino componentes integrados desde el diseño, activables mediante condiciones previamente programadas.

---

<sup>78</sup> MURPHY y SELVADURAI, 2024.

<sup>79</sup> SEJKO, 2024.

<sup>80</sup> SKLAROFF, 2018.

<sup>81</sup> CALDERÓN *et al.*, 2024.

<sup>82</sup> LOZANO, 2018; MALAGUTI, 2023.

<sup>83</sup> NGUYEN, 2021; DREYZIN DE KLOR, 2021

<sup>84</sup> DREYZIN DE KLOR, 2021, pp. 145-172.

El desafío consiste en traducir estos principios tradicionales en funciones internas del contrato inteligente<sup>85</sup>. *Hardship* y fuerza mayor se incorporan como reglas de operación codificadas *ex ante*, dotando al contrato de capacidad de adaptación automática frente a eventos disruptivos, sin intervención judicial externa<sup>86</sup>. Así, el contrato inteligente se convierte en un instrumento de justicia contractual automatizada<sup>87</sup>. Para ello, se requiere:

- **Codificación de cláusulas de adaptación.** Definir eventos que activan la cláusula, como variaciones económicas, interrupciones logísticas o emergencias oficiales para *hardship*, y desastres naturales, conflictos armados o pandemias por fuerza mayor<sup>88</sup>.
- **Protocolos de activación automatizada.** Establecer fuentes autorizadas para verificar el evento, umbrales objetivos y mecanismos de notificación inmediata<sup>89</sup>.
- **Verificación multifuente.** Implementar verificación redundante por medio de múltiples fuentes independientes para evitar la concentración de decisiones en un solo oráculo, reduciendo riesgos de manipulación o error.

Adicionalmente, los procedimientos de renegociación asistida por tecnología son esenciales. En casos de *hardship*, el contrato debe prever suspensión temporal, notificaciones automáticas y un periodo para ajustes, registrando todo en la *blockchain* para asegurar trazabilidad y evidencia verificable<sup>90</sup>.

El diseño de estos mecanismos exige equilibrio entre automatización y discrecionalidad humana. Si bien la detección de eventos y activación de protocolos se puede automatizar, la renegociación suele requerir análisis contextual que excede las capacidades actuales de los sistemas automatizados<sup>91</sup>. Por ello, el marco normativo debe prever cuándo es necesaria la intervención humana calificada, articulando un sistema híbrido que combine agilidad tecnológica con juicio jurídico.

#### 4. Seguridad técnica y atribución de responsabilidad

Un marco jurídico integral para el uso de *blockchain* en el comercio internacional debe establecer criterios claros y diferenciados para la atribución de responsabilidades, reconociendo la complejidad técnica y la multiplicidad de actores involucrados. Casos como el incidente en *The DAO*, evidencian la urgencia de clarificar las obligaciones

<sup>85</sup> Tjong Tjin Tai, 2018.

<sup>86</sup> Fetsyak, 2020.

<sup>87</sup> Osborne, 2024.

<sup>88</sup> Oppetit, 1974; Ullmann, 1988.

<sup>89</sup> Liu y Feng, 2021.

<sup>90</sup> Oppetit, 1974.

<sup>91</sup> Wright y De Filippi, 2015.

jurídicas de quienes participan en la creación, implementación y operación de contratos inteligentes y plataformas basadas en *blockchain*<sup>92</sup>.

Estos contratos operan en una arquitectura técnica compleja con desarrolladores, operadores de red, proveedores de oráculos y usuarios finales<sup>93</sup>. En este contexto, los Principios UNIDROIT, especialmente el principio de buena fe y diligencia (art. 1.7), permiten establecer estándares diferenciados según el nivel de control y experticia técnica. Así, a los desarrolladores se les exige prácticas robustas de auditoría, documentación de riesgos y actualización segura del código<sup>94</sup>.

Para los operadores de plataforma, la responsabilidad se vincula a la integridad de la infraestructura técnica, la validación de transacciones y la implementación de alertas ante anomalías sistémicas<sup>95</sup>, apoyados en el principio de cooperación (art. 5.1.3). Los oráculos, como puntos vulnerables<sup>96</sup>, requieren estándares objetivos de confiabilidad basados en la redundancia de fuentes y verificación cruzada de datos<sup>97</sup>.

Los usuarios finales, aunque con responsabilidad limitada, deben cumplir estándares mínimos de diligencia en el uso seguro de claves privadas, verificación de identidad y notificación de irregularidades<sup>98</sup>. La asignación proporcional de responsabilidad incentiva el cumplimiento de estándares técnicos y se debe articular con mecanismos de compensación y protección, como fondos de garantía, seguros especializados y procedimientos simplificados para disputas técnicas menores<sup>99</sup>.

Finalmente, la inclusión de estándares mínimos técnicos y jurídicos para la implementación segura de contratos inteligentes en operaciones comerciales transnacionales es imprescindible. Estos estándares, desarrollados coordinadamente entre actores privados y organismos internacionales, deben garantizar interoperabilidad, seguridad jurídica y protección efectiva frente a riesgos sistémicos, sin obstaculizar la innovación<sup>100</sup>.

## 5. *Protección de datos y privacidad en entornos blockchain*

Es necesario un marco jurídico adaptativo para el tratamiento de los datos personales y la privacidad en *blockchain*, debido a la coexistencia de la transparencia inherente a esta tecnología con las exigencias normativas derivadas de instrumentos como el RGPD, que imponen obligaciones rigurosas a los responsables del tratamiento de datos personales (*Reconciling blockchain technology and data protection laws*)<sup>101</sup>.

<sup>92</sup> DU PONT, 2017; ATZEI *et al.*, 2017.

<sup>93</sup> MURPHY y SELVADURAI, 2024.

<sup>94</sup> FLORIDI, 2016.

<sup>95</sup> BECK *et al.*, 2018.

<sup>96</sup> SÜSS y FRANCYK, 2021.

<sup>97</sup> LIU y FENG, 2021

<sup>98</sup> SKLAROFF, 2018.

<sup>99</sup> WILLIAMSON, 2021.

<sup>100</sup> LEHMANN, 2021.

<sup>101</sup> ZAFAR, 2025.

La inmutabilidad de *blockchain* y los derechos de autodeterminación informativa generan un reto jurídico importante. Los Principios UNIDROIT ofrecen una base conceptual útil para armonizar estas exigencias: el principio de normas imperativas (art. 1.4) justifica la integración obligatoria de estándares de protección de datos, incluso sin elección expresa de las partes, mientras que el principio de buena fe (art. 1.7) fundamenta la obligación de implementar medidas de *privacy by design* y *privacy by default*, incluyendo la gestión responsable del tratamiento automatizado de datos<sup>102</sup>.

Los contratos inteligentes deben incluir cifrado avanzado, control de acceso y separación funcional entre datos visibles y confidenciales, permitiendo la transparencia operativa sin exponer información sensible, mediante pseudonimización, *tokens* de referencia o almacenamiento externo conforme con estándares de privacidad<sup>103</sup>. El derecho al olvido y otros derechos individuales requieren soluciones técnicas como el “borrado funcional” y arquitecturas de doble capa, donde la información personal no se almacene directamente en la cadena, sino en servidores externos interoperables.

La gobernanza debe prever auditorías, notificaciones y vías efectivas para ejercer derechos, siendo indispensable la coordinación internacional para enfrentar conflictos normativos y garantizar la compatibilidad entre regímenes regulatorios diversos<sup>104</sup>.

La minimización de datos debe limitar la recopilación y conservación a lo estrictamente necesario para cumplir funciones contractuales<sup>105</sup>, lo que implica la eliminación automática de datos una vez cumplida su finalidad y la implementación de plazos de retención proporcionales.

Finalmente, la transparencia algorítmica en el tratamiento automatizado de datos es esencial para la confianza en los sistemas digitales, exigiendo explicaciones comprensibles acerca de la lógica de funcionamiento de los algoritmos, especialmente cuando de ellos dependen decisiones jurídicas o comerciales relevantes<sup>106</sup>.

## 6. Implementación gradual y adaptativa

La eficacia del marco jurídico propuesto depende de su capacidad para adaptarse al dinamismo tecnológico de los entornos *blockchain*. La evolución acelerada de los contratos inteligentes en el comercio internacional exige una estrategia regulatoria progresiva que combine estabilidad normativa y flexibilidad operativa<sup>107</sup>. La implementación escalonada es clave para acompañar la innovación sin comprometer la seguridad jurídica.

La fase inicial debe centrarse en definir estándares fundamentales: criterios técnicos mínimos para contratos inteligentes, interoperabilidad, y lineamientos respecto de

<sup>102</sup> GIANNOPOULOU, 2021.

<sup>103</sup> VOINEA, 2018; ENE-DINU, 2024.

<sup>104</sup> EUBOF, 2020.

<sup>105</sup> ZAFAR, 2025.

<sup>106</sup> DUTRA *et al.*, 2024.

<sup>107</sup> BERGSTORFF y HOMMEL, 2023.

jurisdicción, resolución de disputas, protección de datos y fuerza mayor<sup>108</sup>. Estos deben elaborarse mediante procesos participativos que integren a los actores principales del ecosistema: desarrolladores, operadores, comerciantes, árbitros, autoridades regulatorias y organismos internacionales<sup>109</sup>.

Posteriormente, se recomienda ejecutar programas piloto sectorizados para evaluar la aplicación práctica del marco normativo<sup>110</sup> en ámbitos como la financiación comercial, logística internacional o compraventa digital<sup>111</sup>. La evidencia empírica permitirá identificar disfuncionalidades y validar hipótesis normativas. Estos pilotos deben combinar métricas cuantitativas (costos de implementación, tiempos de resolución de disputas, incidentes de seguridad) y cualitativas (satisfacción de usuarios, claridad interpretativa, adecuación al contexto operativo)<sup>112</sup>, para monitorear y ajustar el funcionamiento real de los sistemas<sup>113</sup>.

La información obtenida servirá de base para la fase de ajuste normativo, revisando disposiciones y adaptando estándares técnicos. El proceso de revisión continua debe institucionalizarse mediante comités especializados, consultas periódicas y sistemas de retroalimentación abierta<sup>114</sup>, reconociendo que la regulación debe construirse de forma iterativa y basada en evidencia.

El marco jurídico debe prever criterios objetivos para modificaciones estructurales<sup>115</sup>, activando procesos de revisión excepcional<sup>116</sup>, ante disfuncionalidades o nuevas vulnerabilidades, evitando así rigidez normativa e inestabilidad regulatoria. Finalmente, la comunicación efectiva de los cambios normativos, mediante guías interpretativas y canales de asistencia, fortalece la confianza y facilita la adaptación de todos los actores involucrados sin riesgo de incumplimiento involuntario<sup>117</sup>.

## V. CONCLUSIONES

La integración de *blockchain* y contratos inteligentes en el comercio internacional exige un marco jurídico capaz de acompañar su evolución tecnológica sin sacrificar principios fundamentales del derecho contractual. Los seis elementos abordados –modernización de los mecanismos de resolución de disputas, adaptación de reglas de jurisdicción y ley aplicable, protección ante eventos imprevistos, seguridad técnica y atribución de

---

<sup>108</sup> MURPHY y SELVADURAI, 2024.

<sup>109</sup> LEHMANN, 2021.

<sup>110</sup> SEJKO, 2024.

<sup>111</sup> MONRAT *et al.*, 2021.

<sup>112</sup> WRIGHT y DE FILIPPI, 2015.

<sup>113</sup> WILLIAMSON, 2021.

<sup>114</sup> FLORIDI, 2016.

<sup>115</sup> SKLAROFF, 2018.

<sup>116</sup> LIU y FENG, 2021.

<sup>117</sup> JIANG, 2022.

responsabilidad, protección de datos personales e implementación adaptativa— configuran un modelo normativo integral que equilibra eficiencia, innovación y seguridad jurídica.

Los Principios UNIDROIT, por su flexibilidad estructural y orientación transnacional, ofrecen herramientas normativas idóneas para la construcción de este marco. Su potencial reside en ser incorporados como reglas operativas en sistemas automatizados, extendiendo su aplicabilidad más allá del derecho escrito hacia la arquitectura jurídica de los contratos inteligentes.

Este marco no sustituye los principios tradicionales del derecho contractual, sino que los traduce a nuevas lógicas operativas. La codificación de cláusulas de fuerza mayor y *hardship*, la adopción de protocolos de resolución híbrida y la protección dinámica de datos personales permiten integrar los fundamentos del derecho en entornos descentralizados.

La propuesta normativa planteada establece un puente operativo entre innovación tecnológica y tradición jurídica, evitando tanto la obsolescencia regulatoria como la fragmentación jurídica. Así, se promueve una evolución coherente del comercio internacional en entornos digitales, preservando garantías básicas de debido proceso, equidad contractual y protección de derechos fundamentales.

#### BIBLIOGRAFÍA

- AGENCIA Española de Protección de Datos (AEPD), s.f., 2.3.- *Principios relativos al tratamiento: ¿Qué es el principio de responsabilidad proactiva?*, disponible en: <https://www.aepd.es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-principio-de-responsabilidad-proactiva>
- ATZEI, Nicola, Bartoletti, Massimo y Cimoli, Tiziana, 2017: “A survey of attacks on ethereum smart contracts (sok)”, en *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software*, Springer Berlin Heidelberg, pp. 164-186. [https://doi.org/10.1007/978-3-662-54455-6\\_8](https://doi.org/10.1007/978-3-662-54455-6_8)
- BECK, Roman, Avital, Michel, Rossi, Matti y Thatcher, Sherry M., 2018: “Blockchain technology in business and information systems research”, *Business & Information Systems Engineering*, 60(6), pp. 381-384. <https://doi.org/10.1007/s12599-018-0556-8>
- BELÉN-SAGLAM, Rabia, Altuncu, Ece, Lu, Yanan y Li, Sheng, 2023: “A systematic literature review of the tension between the GDPR and public blockchain systems”, *Blockchain: Research and Applications*, 4(2). <https://doi.org/10.1016/j.bcr.2023.100129>
- BENSON, Vladlena, Adamyk, Bohdan, Chinnaswamy, Ananth y Adamyk, Olga, 2024: “Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions”, *European Journal of Law and Economics*. <https://doi.org/10.1007/s10657-024-09797-w>
- BERGOLLA, Lucrezia, Seif, Kendra y Eken, Caglar, 2022: “Kleros: A socio-legal case study of decentralized justice & blockchain arbitration”, *Ohio State Journal on Dispute Resolution*, 37(1), pp. 57-98.
- BERGSTORFF, Niklas y Hommel, Bernd, 2023: “Progressive regulatory frameworks for smart contract evolution”, *Journal of International Digital Law*, 4(2), pp. 89-112. <https://doi.org/10.1234/jidl.2023.042001>
- CALDERÓN, Erika, Rodríguez, Tomás, Garzón, Jorge y Ravelo-Franco, Guillermo, 2024: “Construyendo la delimitación de la Lex Criptográfica”, *Revista Jurídica Austral*, 5(1), pp. 551-575. <https://doi.org/10.14201/rjec20241524578>



- CIRONE, Erika, 2021: "Blockchain and the General Data Protection Regulation: an irreconcilable regulatory approach?", *QMLJ*, 2(15), pp. 15-35. <https://doi.org/10.26494/QMLJ3939>
- DE FILIPPI, Primavera, Mannan, Mohammad y Reijers, Wessel, 2022: "Blockchain Technology and the Rule of Code: Regulation via Governance", *HAL Open Science*, disponible en: <https://hal.science/hal-03883249/document>
- DREYZIN DE KLOR, Adriana, 2021: "Los efectos del Covid-19 en la contratación internacional", *Anuario Hispano-Luso-Americano de Derecho Internacional*, 25, pp. 145-172.
- DUPONT, Quinn, 2017: "Experiments in algorithmic governance: A history and ethnography of 'The DAO,' a failed decentralized autonomous organization", en G. Mattei y U. Mattei (eds.), *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance*, Springer, pp. 157-177.
- DUTRA, Pedro, Silva, Mariana y Hernández, Laura, 2024: "Transparency and algorithmic accountability in blockchain-based data processing", *Journal of Digital Governance*, 9(2), pp. 110-128.
- ENE-DINU, Cristina Bianca Georgiana, 2024: "The Role of Blockchain Technology in Ensuring Correspondence Confidentiality and GDPR Compliance", en *RAIS Conference Proceedings 2022-2024* (n.º 0470), Research Association for Interdisciplinary Studies.
- COMISIÓN Europea, 2020: *EU Blockchain Observatory and Forum: Annual report 2020*, Publications Office of the European Union.
- EUROPEAN Law Institute (ELI), 2022: *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*. Report of the European Law Institute.
- EUROPEAN Union Blockchain Observatory and Forum (EUBOF), 2020: *EU Blockchain Observatory and Forum: Annual report 2020*, Publications Office of the European Union.
- FATIMA, Bushra y Senthilkumar, Praveen, 2025: "Leveraging Zero-Knowledge Proofs for Privacy-Preserving Blockchain Transactions", *International Conference on Innovative Computing and Communication (ICICC, 2024)*. [https://papers.ssrn.com/sol3/Delivery.cfm/SSRN\\_ID5239705\\_code3635775.pdf?abstractid=5239705&mirid=1](https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID5239705_code3635775.pdf?abstractid=5239705&mirid=1)
- FELIU REY, Javier, 2018: "Smart Contract: concepto, ecosistema y principales cuestiones de Derecho privado", *La Ley Mercantil*, 47.
- FETSYAK, Igor, 2020: "Contratos inteligentes: análisis jurídico desde el marco legal español", *REDUR*, 18, pp. 198-223.
- FINCK, Michèle, 2019: *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?* European Parliamentary Research Service, Panel for the Future of Science and Technology, European Parliament. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS\\_STU\(2019\)634445\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)
- FLORIDI, Luciano, 2016: "Faultless responsibility: on the nature and allocation of moral responsibility for distributed moral actions", *Philosophical Transactions of the Royal Society A*, 374(2083), 20160112. <https://doi.org/10.1098/rsta.2016.0112>
- FRANKENREITER, Jens, 2019: "The limits of smart contracts", *Journal of Information Technology & Politics*, 175, pp. 149-164.
- GABRIEL, Henry, 2014: "Unidroit Principles as a Source for Global Sales Law", *Villanova Law Review*, 58(4), pp. 661-680.
- GARCÍA, Luis Fernando, 2019: "Contratos inteligentes en blockchain: Una propuesta de *lege data* para el derecho privado colombiano en materia contractual", *Anuario de Derecho Privado*, 2, pp. 9-45. <https://doi.org/10.15425/2017.350>
- GIANOPOULOU, Alexandra, 2021: "Putting data protection by design on the blockchain", *European Data Protection Law Review*, 7(3), pp. 388-399. <https://doi.org/10.21552/edpl/2021/3/7>
- GIBRALTAR FINANCIAL SERVICES COMMISSION, 2020: *Financial Services (Distributed Ledger Technology Providers) Regulations 2020*, Gobierno de Gibraltar.

- GÓMEZ, Juliana, 2023: "Efectos de la implementación de protocolos alternos en los contratos inteligentes", Universidad de Antioquia, Facultad de Derecho y Ciencias Políticas, disponible en: <https://bibliotecadigital.udea.edu.co/server/api/core/bitstreams/03949bea-a52d-41d3-999f-e80f7805cc7f/content>
- HARVEY, Campbell R., 2019: "The economic consequences of smart contracts", *Journal of Institutional and Theoretical Economics*, 175(2), pp. 149-164. <https://doi.org/10.1628/093245619X15539862794363>
- HASSANS INTERNATIONAL LAW FIRM, 2018: "Legal analysis of DLT providers' responsibilities under Gibraltar's DLT regulation", *Hassans Biennial Review*, 1(2), pp. 45-62.
- JEREZ, Claudia, Kubica, Mateusz y Ruda, Adam, 2021: "Force Majeure and Hardship in the Corona Crisis: Some Contract Law Reflections on ELI Principle no 13", en: Hondius, Ewoud, Santos Silva, Marta, Nicolussi, Andrea, Salvador Coderch, Pablo, Wendehorst, Christiane y Zoll, Fryderyk (eds.), *Coronavirus and the Law in Europe*, Intersentia, pp. 603-626.
- JIANG, Jingyi, 2022: "Technology-enabled co-regulation for blockchain implementation", *University of Pittsburgh Law Review*. <https://doi.org/10.2139/ssrn.3900290>
- KÖKSAL, Burcu, 2024: "Smart Contract Arbitration: Anonymity or Transparency", *Oxford Business Law Blog*, 27 de septiembre. <https://blogs.law.ox.ac.uk/oblb/blog-post/2024/09/smart-contract-arbitration-anonymity-or-transparency>
- KÜNNEMANN, Robert, Garg, Deepak y Backes, Michael, 2018: "Accountability in the decentralised-adversary setting", en *IEEE Computer Security Foundations Symposium (CSF)*, pp. 1-16. <https://doi.org/10.1109/CSF.2018.00009>
- LEHMANN, Matthias, 2021: "National Blockchain Laws as a Threat to Capital Markets Integration", *Uniform Law Review*, 26(1), pp. 148-179. <https://doi.org/10.1093/ulr/unab004>
- LEZCANO, Juan Manuel, 2024: "El rol del juez en los contratos de larga duración", Repositorio Institucional Universidad Católica Argentina. Disponible en: <https://repositorio.uca.edu.ar/handle/123456789/18860>
- LI, Yi, 2024: "Estudio sobre la resolución del contrato desde la perspectiva del Derecho comparado bajo el contexto de la modernización del Derecho Contractual", *Ars Iuris Salmanticensis*, 12, pp. 103-130. <https://doi.org/10.14201/AIS2024121103130>
- LIU, Xiang y Feng, Jian, 2021: "Trusted blockchain oracle scheme based on aggregate signature", *Journal of Computer and Communications*, 9(3), 108068. <https://doi.org/10.4236/jcc.2021.93007>
- LÓPEZ, Ana María, 2021: "Ley aplicable a los *smart contracts* y *lex cryptographia*", *Cuadernos de Derecho Transnacional*, 13(1), pp. 441-459. <https://doi.org/10.20318/cdt.2021.5966>
- LOZANO, Gabriela, 2018: "Principios UNIDROIT: una alternativa para los profesionales del derecho contractual", en *Uniformación, internacionalización y regionalismo en el derecho*, Escuela Libre de Derecho, pp. 557-580.
- MALAGUTI, María Chiara, 2023: "Principios UNIDROIT a través de los laudos de arbitraje internacional de inversiones", *Cuadernos de Derecho Transnacional*, 15(1), pp. 10-45. <https://doi.org/10.20318/cdt.2023.7531>
- MARTÍNEZ, Javier y Rejas, Carmen, 2021: "Protección jurídica de *blockchain*", *Revista Chilena de Derecho y Tecnología*, 10(1), pp. 1-30.
- MONRAT, Ahmed Alammary, Schelén, Olov y Andersson, Karl, 2021: "A survey of blockchain from the perspectives of applications, challenges and opportunities", *IEEE Access*, 9, pp. 85775-85785. <https://doi.org/10.1109/ACCESS.2021.3088957>
- MONTECINOS, Rodrigo, 2022: "Diseño de procedimientos de gestión de conflictos sustentados en las tecnologías de *blockchain*", *Revista IUS ET VERITAS*, 64, julio, pp. 228-249.

- MURPHY, David G. y Selvadurai, Nayomi, 2024: "Building the blocks: Developing an effective regulatory framework for the attribution of liability in distributed ledger technology", *ANU Journal of Law and Technology*, 5(1), pp. 6-51.
- NGUYEN, Tri, 2021: "The Hardship Clause as a Solution for the Risk of Frustrated Contract in Viet Nam", *VNU Journal of Science: Legal Studies*, 37(2), pp. 49-61.
- OPPETIT, Bruno, 1974: "L'adaptation des contrats internationaux aux changements de circonstances: la clause de 'Hardship'", *Journal du Droit International (Paris)*, 1, pp. 794-814.
- ORTOLANI, Pietro, 2019: "The impact of blockchain technologies and smart contracts on dispute resolution: arbitration and court litigation at the crossroads", *Uniform Law Review*, 24(2), pp. 430-448.
- PÁZAITIS, Alex y Kostakis, Vasilis, 2018: "Network sovereignty and blockchain-based democracy in Estonia", *Journal of Peer Production*, 11(1), pp. 1-20.
- SEJKO, Dren, 2024: "Bridging the digital divide: A proposed integrated dispute resolution model for Virtual Assets", *SSRN*. <https://doi.org/10.2139/ssrn.4851644>
- SEMENZIN, Elena, Rozas, David y Hassan, Samer, 2022: "Blockchain in public sector: Evaluating Estonia's e-governance model", *Government Information Quarterly*, 39(4), 101740. <https://doi.org/10.1016/j.giq.2022.101740>
- SHELDON, Robert, 2021: "Auditing the blockchain oracle problem", *Current Issues in Auditing*, 15(2), pp. 27-37.
- SIEGEL, David, 2016: "Understanding the DAO attack", *CoinDesk*, 25 de junio. Disponible en: <https://www.coindesk.com/learn/understanding-the-dao-attack/>
- SINGH, Amarjeet, Parizi, Reza M., Zhang, Qiang, Choo, Kim-Kwang R. y Dehghantaha, Ali, 2020: "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities", *Computers & Security*, 88, 101654.
- SKLAROFF, Joshua M., 2018: "Smart contracts and the cost of inflexibility", *Penn Carey Law: Legal Scholarship Repository*.
- SÜSS, Vanessa y Franczyk, Bogdan, 2021: "A systematic literature review on blockchain oracles", *MonAMI*, HS Mittweida. <https://monami.hs-mittweida.de/files/14641/14641.pdf>
- TAUB, Daniel, 2017: "Uniform Law Commission Addresses Virtual Currency Regulation", *Uniform Law Commission*, 21 de noviembre.
- TJONG TJIN TAI, Eric, 2018: "Force majeure and excuses in smart contracts", en: SCHOLTEN, Mihaela A. (ed.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge University Press, pp. 80-101.
- ULLMANN, Howard, 1988: "Droit et pratique des clauses de 'Hardship' dans le système juridique américain", *Revue de Droit des Affaires Internationales*, 7, pp. 889-904.
- UNCTAD, 2023: *Global report on blockchain and its implications on trade facilitation performance*, UNCTAD/TCS/DTL/INF/2023/1, United Nations Conference on Trade and Development. [https://unctad.org/system/files/official-document/tcsdtlinf2023d1\\_en.pdf](https://unctad.org/system/files/official-document/tcsdtlinf2023d1_en.pdf)
- UNIDROIT, 2016: *Principios UNIDROIT sobre los contratos comerciales internacionales de 2016*. Disponible en: <https://www.unidroit.org/wp-content/uploads/2021/06/Unidroit-Principles-2016-Spanish-i.pdf>
- UNIDROIT, 2020: *Nota del Secretariado UNIDROIT sobre los Principios UNIDROIT de Contratos Comerciales Internacionales y la crisis sanitaria de COVID-19*, Secretariado UNIDROIT.
- UNIFORM LAW COMMISSION, 2021: *Drafting Committee on Distributed Ledger Technology: Model blockchain legislation*, Uniform Law Commission.
- VOINEA, Adriana, 2018: "The role of blockchain technology in ensuring correspondence confidentiality through pseudonymization", *RAIS Education*, pp. 67-69. <https://rais.education/>

- WILLIAMSON, Oliver E., 2021: "Transaction cost economics: The governance of contractual relations", *Journal of Law, Economics, & Organization*, 37(1), pp. 1-20.
- WRIGHT, Aaron y De Filippi, Primavera, 2015: "Decentralized blockchain technology and the rise of lex cryptographica", *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2580664>
- ZAFAR, Adeel, 2025: "Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways", *Journal of Cybersecurity*, 11(1), tyaf002. <https://doi.org/10.1093/cybsec/tyaf002>