Desafíos legales en la implementación de Contratos inteligentes en compañías del sector financiero en Colombia.

María Fernanda Cuestas Diaz

Leidy Paola Hilarión Bonilla

Tutor:
Erick Rincón Cárdenas

Título a obtener: Magister en Derecho Corporativo

Facultad de Jurisprudencia

Maestría en Derecho Corporativo

Universidad del Rosario

2025

Desafíos legales en la implementación de Contratos inteligentes en compañías del sector financiero en Colombia.

María Fernanda Cuestas Diaz y Leidy Paola Hilarión Bonilla.

Abstract

This article analyzes the duality involved in the implementation of smart contracts in the Colombian financial sector. On one hand, this technology emerges as a transformative force capable of automating the execution of agreements, reducing costs, minimizing operational errors, and strengthening the transparency and traceability of transactions. Its feasibility is not merely theoretical, as demonstrated by the regulatory *Sandbox* of the Colombian Financial Superintendence, where pilot projects have shown significant improvements in process efficiency and agility. Likewise, the Colombian legal framework provides initial support, as Law 527 of 1999 recognizes the validity of electronic contracting and, by extension, smart contracts as atypical yet legally valid instruments.

Nevertheless, this development faces substantial legal and operational risks. The immutability of blockchain creates tensions with rights such as the right to be forgotten, while decentralization dilutes the figure of the data controller, making oversight and the exercise of rights more difficult. Additional challenges include risks derived from automation, limitations in fulfilling the duty of information toward financial consumers, and issues related to data integrity, cybersecurity, and anti-money laundering compliance.

The article concludes that the adoption of smart contracts in the financial sector requires a specific regulatory framework and the collaboration of regulators, technologists, and legal experts to ensure responsible innovation, legal certainty, and effective user protection

Keywords: Smart Contracts; Electronic Contracting in Colombia; Blockchain; Legal Risks; Financial Sector; Coding.

Resumen

El presente artículo analiza la dualidad que presenta la implementación de contratos inteligentes (*smart contracts*) en el sector financiero colombiano. Por un lado, esta tecnología se proyecta como un motor de transformación capaz de automatizar la ejecución de acuerdos, reducir costos, minimizar errores operativos y fortalecer la transparencia y trazabilidad de las transacciones. Su viabilidad no es meramente teórica, como lo demuestra el *Sandbox* regulatorio de la Superintendencia Financiera de Colombia, donde proyectos piloto evidencian mejoras significativas en eficiencia y agilidad de procesos. Asimismo, el marco jurídico colombiano ofrece un sustento inicial, al reconocer la Ley 527 de 1999 la validez de la contratación electrónica y, por extensión, de los contratos inteligentes como figuras atípicas pero válidas.

No obstante, este desarrollo enfrenta riesgos legales y operativos sustanciales. La inmutabilidad de *blockchain* plantea tensiones con derechos como el olvido, mientras que la descentralización diluye la figura del responsable del tratamiento de datos, dificultando la supervisión y el ejercicio de derechos. A ello se suman los riesgos derivados de la automatización, las limitaciones en el deber de información al

consumidor financiero, y los desafíos de integridad de datos, ciberseguridad y prevención del lavado de activos.
El artículo concluye que la adopción de *smart contracts* en el sector financiero requiere un marco regulatorio específico y la colaboración entre reguladores, tecnólogos y juristas para garantizar innovación responsable, seguridad jurídica y protección efectiva de los usuarios.
Palabras Clave: Smart Contracts; Contratación electrónica en Colombia; Blockchain; Riesgos legales; Sector financiero; Codificación.

Índice

1. Introducción

En las últimas décadas, los diversos avances tecnológicos han transformado profundamente las dinámicas sociales, económicas y jurídicas a nivel global. La creciente digitalización de las interacciones humanas, sumada al auge de tecnologías disruptivas, han propiciado nuevas formas de comunicación, intercambio y contratación. En este contexto, el derecho se enfrenta al reto de adaptarse a una realidad en permanente evolución, donde las herramientas digitales no solo median las relaciones jurídicas, sino que también asumen la ejecución autónoma de las obligaciones pactadas.

Entre los fenómenos más relevantes de la evolución tecnológica se destaca el surgimiento de los contratos inteligentes (*smart contracts*), que nacen como una aplicación concreta de la tecnología *Blockchain* o cadena de bloques (en adelante "*Blockchain*"), inicialmente concebida en el ámbito financiero con la creación de criptomonedas como *Bitcoin,* pero cuyo potencial de transformación trasciende dicho sector.

La tecnología *Blockchain* se define como una estructura digital que permite el registro descentralizado, inmutable, seguro y transparente de transacciones e información. A diferencia de las bases de datos tradicionales, *Blockchain* prescinde de una autoridad central para validar las operaciones, distribuyendo la información entre múltiples nodos que verifican colectivamente cada bloque de datos, lo que otorga elevados niveles de confiabilidad e integridad.

Sobre esta arquitectura se edifican los contratos inteligentes, entendidos como instrumentos digitales que automatizan la ejecución de obligaciones contractuales mediante la incorporación de cláusulas codificadas que se ejecutan de manera automática al verificarse determinadas condiciones. Esta lógica de programación basada en el esquema "*si ocurre X, entonces ejecutar Y*" optimiza la eficiencia, reduce los costos operativos y minimiza los errores derivados de la intervención humana, configurándose como una innovación particularmente relevante en entornos comerciales altamente digitalizados.

La consolidación de *Blockchain* como tecnología transversal a diversos sectores ha propiciado la irrupción de los contratos inteligentes como una nueva modalidad de contratación, lo cual plantea desafíos sustanciales para los sistemas jurídicos tradicionales, especialmente en ordenamientos como el colombiano, donde el contrato ha sido históricamente concebido como un acuerdo de voluntades celebrado entre personas naturales o jurídicas.

La introducción de mecanismos de ejecución automatizada y descentralizada cuestiona nociones jurídicas fundamentales como el consentimiento, la forma, la ejecución y la responsabilidad contractual, generando interrogantes acerca de la necesidad de adaptar el marco normativo vigente para evitar vacíos jurídicos y salvaguardar la seguridad jurídica.

Particularmente en el sector financiero colombiano, caracterizado por su alta regulación y estrictas exigencias de cumplimiento, la implementación de contratos inteligentes supone enfrentar retos adicionales. La principal problemática jurídica radica en determinar si estos instrumentos pueden integrarse de manera armónica al régimen contractual actual, basado en los principios tradicionales del derecho privado, o si, por su carácter atípico y su soporte en tecnologías emergentes, requieren la creación de un marco regulatorio específico.

Esta dificultad se agrava ante la tendencia del legislador colombiano a asumir una postura reactiva frente a la innovación tecnológica, generando vacíos regulatorios, riesgos de inseguridad jurídica y barreras a la implementación efectiva de dichas tecnologías.

En este sentido, el objetivo general del presente artículo de reflexión consiste en analizar los principales desafíos legales que enfrenta el sector financiero en Colombia en la implementación de contratos inteligentes, identificando los riesgos jurídicos y contractuales asociados, con el fin de proponer recomendaciones orientadas a su integración segura y eficaz dentro del marco jurídico vigente.

Para el logro de este objetivo general, se plantean los siguientes objetivos específicos: (i) identificar las principales características técnicas y jurídicas de los contratos inteligentes aplicables al sector financiero; (ii) analizar el marco normativo colombiano en materia de contratación electrónica y tecnologías disruptivas; (iii) evaluar los riesgos legales derivados de la implementación de contratos inteligentes en compañías del sector financiero colombiano; y (iv) formular propuestas estratégicas que permitan mitigar dichos riesgos y promover una adopción segura de la tecnología.

La justificación de este trabajo se sustenta en la necesidad de adaptar el derecho colombiano a los nuevos paradigmas tecnológicos que configuran las relaciones jurídicas contemporáneas. La ausencia de regulación específica sobre contratos inteligentes, unida a la complejidad inherente de las tecnologías emergentes, plantea desafíos significativos en términos de validez contractual, manifestación del consentimiento, ejecución automatizada y protección de los derechos de las partes.

Este estudio pretende aportar al debate doctrinal y práctico mediante un análisis sistemático y crítico, orientado a proporcionar insumos que fortalezcan la seguridad jurídica en la implementación de contratos inteligentes, fomentan la confianza en el uso de tecnologías disruptivas y contribuyan al desarrollo de un entorno normativo más dinámico, proactivo y adecuado a las exigencias de la transformación digital.

2. Marco Teórico.

2.1.Fundamentos técnicos: *Blockchain*, Codificación y Automatización.

La tecnología *Blockchain*, constituye la base en la que se fundamenta el desarrollo y ejecución de los contratos inteligentes. Se trata de un sistema de registro distribuido y

descentralizado que permite almacenar información de forma inmutable, segura y transparente. Cada bloque contiene un conjunto de transacciones o datos que, una vez verificados mediante un mecanismo de consenso como Proof of Work (en adelante "PoW") o Proof of Stake (en adelante "PoS")[1], son agregados a la cadena de forma cronológica y permanente.

A diferencia de los sistemas tradicionales centralizados, donde una entidad controla y valida la información, en *Blockchain* la verificación se realiza colectivamente por los nodos de la red. Esto garantiza un alto nivel de resistencia frente a fraudes, manipulaciones o ataques maliciosos. Además, cada bloque está vinculado criptográficamente con el anterior, lo cual refuerza la integridad del sistema.

Uno de los elementos más relevantes de esta tecnología es su inmutabilidad: una vez que la información es registrada, no puede ser modificada sin alterar toda la cadena, lo cual requeriría la aprobación de la mayoría de los nodos. Esta característica hace que la *Blockchain* sea una infraestructura confiable para almacenar contratos inteligentes, ya que asegura que los términos codificados se ejecuten exactamente como fueron programados.

Existen tres tipos principales de *Blockchain*:

- Públicas: como *Bitcoin* o *Ethereum,* abiertas a cualquier usuario para participar como nodo validador.
- Privadas: gestionadas por una entidad específica.
- Permisionadas: que combinan elementos de las públicas y privadas, permitiendo el control de acceso sin perder completamente la descentralización.

Ethereum es hoy la plataforma más usada para crear contratos inteligentes, porque cuenta con su propia máquina virtual (EVM) y un lenguaje de programación llamado Solidity. En esta red, los contratos inteligentes funcionan como programas informáticos (*scripts*) que se guardan en la *Blockchain* y se ejecutan automáticamente cuando se cumplen las condiciones que fueron definidas de antemano, sin que nadie tenga que intervenir para activarlos.

La tecnología *Blockchain* no solo sustenta el funcionamiento de las criptomonedas, sino que también permite el desarrollo de aplicaciones complementarias como la emisión de activos digitales o *tokens*, la trazabilidad en cadenas de suministro, los sistemas de votación electrónica, las finanzas descentralizadas (*DeFi*) y la gestión de la identidad digital soberana, entre otras.

En este contexto, los contratos inteligentes surgen como una de sus aplicaciones más relevantes. Su implementación exige la traducción de los términos legales a lógica computacional, lo que plantea retos significativos, pues el lenguaje de programación carece de la flexibilidad interpretativa propia del lenguaje jurídico. Además, la automatización de obligaciones y derechos conlleva que ciertos efectos se ejecuten de

[1] PoW o PoS: son el "filtro de seguridad" que garantiza que lo que pasa dentro de un contrato inteligente (ejemplo: un pago automático) se registre sin alteraciones, de manera descentralizada e inmutable.

manera automática, lo cual puede generar dificultades en la práctica cuando surgen situaciones no previstas en el contrato.

De acuerdo con el Ministerio de Tecnologías de la Información y Comunicaciones (2021), la *Blockchain* constituye una infraestructura estratégica para el gobierno digital y la innovación contractual, dado que permite la trazabilidad de bienes, la verificación de identidad y la administración de contratos automatizados, aspectos que fortalecen la seguridad, la transparencia y la eficiencia en las relaciones jurídicas y comerciales.

2.2.Concepto de contratación electrónica en Colombia

En Colombia, la contratación electrónica se encuentra regulada por la Ley 527 de 1999, norma que reconoce la validez jurídica y probatoria de los mensajes de datos, y establece el marco para el comercio electrónico y las firmas digitales. De acuerdo con el artículo 5º de la citada ley, se ha establecido lo siguiente: "*Reconocimiento jurídico de los mensajes de datos. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos*".

Asimismo, el artículo 6º de la misma ley, aclara que, cuando una norma exija que cierta información conste por escrito, esa exigencia puede satisfacerse mediante un mensaje de datos, otorgando así equivalencia funcional entre los documentos físicos y electrónicos. De esta forma, el consentimiento contractual puede manifestarse válidamente por medios electrónicos, sin necesidad de la presencia física de las partes.

El Decreto 2364 de 2012, por su parte, regula el uso de las firmas electrónicas y digitales, diferenciándose entre ambas en cuanto a su nivel de sofisticación y requisitos técnicos. Según esta normativa, la firma electrónica permite identificar al firmante y vincularlo con el contenido del mensaje de datos, siempre que se utilice de manera confiable y conforme a las exigencias legales.

Estos fundamentos normativos permiten inferir que los contratos inteligentes, en tanto manifestaciones de voluntad expresadas mediante lenguaje computacional ejecutado automáticamente, pueden entenderse como una forma de contratación electrónica, siempre que cumplan con los requisitos esenciales del contrato: (i) consentimiento; (ii) objeto; y (iii) causa lícita. Esta postura ha sido respaldada por autores como Cárdenas Rincón (2022), quien argumenta que la manifestación de voluntad puede darse a través de medios electrónicos, siempre que el entorno digital garantice la autenticidad, integridad y trazabilidad de dicha manifestación.

Adicionalmente, la Sentencia C-662 de 2000 de la Corte Constitucional reafirmó la Ley 527 de 1999, al reconocer que la regulación del comercio electrónico y la contratación por medios digitales se ajusta a los principios de libertad contractual y autonomía de la voluntad, siempre que se respete el orden público y las garantías legales.

En este contexto, el contrato inteligente puede cumplir con las exigencias de la contratación electrónica, en tanto constituye un mensaje de datos susceptible de generar obligaciones jurídicas válidas y exigibles.

Por tanto, los contratos inteligentes, como manifestaciones de voluntad expresadas mediante código ejecutable, podrían encuadrarse dentro de la contratación electrónica reconocida en el ordenamiento jurídico colombiano.

2.3. Definición y características de los Contratos Inteligentes o *Smart Contracts.*

Como hemos anotado, la ley en materia de tecnología ha sido más reactiva que anticiparse a los cambios y retos, lo que genera una brecha frente al ritmo acelerado con el que la innovación se desarrolla en la sociedad. Por ello el concepto de *Smart Contracts* (en adelante "SC") no es la excepción a la regla, situación que se acentúa al vincularlos c*on la tecnología Blockchain*, cuyo propósito central, como se ha abordado líneas arriba, radica en eliminar la intermediación y favorecer esquemas de comunicación directa P2P *(peer-to-peer)* entre los consumidores en la realización de operaciones.

El origen de los SC se remonta a la década de 1990, cuando se publicaron algunos estudios de programadores y académicos, explorando su potencial para automatizar decisiones mediante algoritmos matemáticos. En este contexto, Nick Szabo los definió como estructuras de código y datos almacenados en una dirección de la cadena de bloques. En términos simples, un contrato inteligente es un programa creado por un desarrollador para ejecutarse en la *Blockchain*.

Por su parte, Puyol Montero, definió los SC como protocolos informáticos que facilitan, verifican y hacen cumplir la negociación de un contrato sin tener necesidad de una cláusula contractual, y Tur Faúndez los define como aquellos contratos celebrados a través de una plataforma web accesible para las partes, cuya forma se compone de la interfaz de usuario de la aplicación y de uno o varios programas autoejecutables alojados en la cadena de bloques, los cuales tienen la capacidad de interactuar tanto entre sí como con dicha interfaz.

En conclusión, dentro de la contratación electrónica pueden distinguirse dos modalidades: aquellos contratos que requieren la intervención humana para su ejecución, como ocurre en las transferencias electrónicas, y los denominados SC, caracterizados por ser programas autónomos que no necesitan de un tercero para operar. Su funcionamiento automático les otorga un rasgo de inmutabilidad, ya que el código no puede ser alterado una vez desplegado.

La doctrina ha resaltado que una de sus principales ventajas radica en el aumento de la trazabilidad y de la seguridad frente a los contratos tradicionales, así como en la reducción de costos y tiempos asociados a las transacciones. Todo ello es posible gracias a la tecnología de registros distribuidos (*DLT*), que facilita la interacción directa entre consumidores digitales en un entorno en el que resulta difícil cuestionar la validez de las operaciones realizadas.

De acuerdo con lo anterior, las principales características de de los SC son:

1) Automatización: la ejecución de derechos y obligaciones se produce de forma inmediata y automática cuando se cumplen las condiciones previstas en el código.

2) Inmutabilidad: una vez desplegado en la red *Blockchain*, el contrato no puede ser modificado unilateralmente; cualquier alteración requiere consenso de las partes y validación por la red.
3) Transparencia: el código fuente del contrato es accesible para las partes, quienes pueden verificar de antemano sus términos y condiciones.
4) Seguridad: el uso de criptografía y el registro distribuido minimizan los riesgos de manipulación o fraude.
5) Desintermediación: eliminan la necesidad de terceros confiables para ejecutar o validar el contrato, reduciendo costos y tiempos.
6) Ejecución condicionada: su lógica "*if–then*" (si ocurre X, entonces se ejecuta Y) asegura que las transacciones se realicen únicamente cuando se cumplan las condiciones programadas.

En coherencia con lo expuesto, las aplicaciones de los SC son múltiples y abarcan diversos sectores de la economía. A modo de ejemplo, se encuentran podemos verlo en: contratos de compraventa de vehículo automotor, contratos de compraventa de inmueble (vivienda urbana, establecimiento de comercio), contratos de seguro, contratos de mutuo de dinero, contratos de arrendamiento de vivienda urbana, contratos de garantías mobiliarias, la emisión de títulos académicos por parte de universidades, determinados servicios notariales como testamentos o registros civiles de nacimiento, la venta de tiquetes aéreos y, de manera destacada, su utilización en el sector financiero, como el contrato de leasing financiero, contrato de factoring, entre otros.

En el sector financiero, un contrato inteligente puede ejemplificarse con una simple transferencia de recursos entre cuentas. No obstante, sus aplicaciones pueden llegar a ser mucho más complejas. Ejemplo de ello es el de los contratos *swap*, que corresponden a instrumentos derivados mediante los cuales dos partes (denominadas usuarios finales) acuerdan realizar pagos recíprocos en fechas predeterminadas, en la misma o en diferentes monedas.

Los montos a transferir se fijan de manera cierta o con base en parámetros objetivos, y dado que se trata de contratos de carácter aleatorio, el resultado final es incierto. En este contexto, los SC permiten automatizar la totalidad del proceso, posibilitando la gestión del riesgo en tiempo real. Así, cuando la operación se realiza en el mercado mostrador (*over the counter*), la ejecución puede llevarse a cabo de manera autónoma, sin que ninguna de las partes deba intervenir directamente.

De acuerdo con Tur Faúndez, un contrato inteligente también puede programarse para realizar funciones específicas como:

a. Cobrar automáticamente de la cuenta de un deudor y transferir los fondos a la propia cuenta o a la de un acreedor, con o sin intereses.
b. Retener fondos en su propia cuenta hasta que se cumplan determinadas condiciones.
c. Recibir información de eventos externos (hechos contables u operativos) y actuar en consecuencia.

d. Ordenar la activación o desactivación de mecanismos electrónicos conectados al programa (encender o apagar dispositivos, bloquear o desbloquear accesos, entre otros).
e. Suspender su propia ejecución si así se establece en el código.
f. Autodestruirse, es decir, eliminarse permanentemente de la cadena de bloques, de manera que no pueda volver a ser utilizados.

A partir de lo expuesto, puede afirmarse que, las relaciones contractuales pueden materializarse en un código informático o en un protocolo capaz de ejecutar funciones específicas e, incluso, de extinguirse automáticamente una vez cumplido su propósito. Para que ello sea posible, resulta necesario que un desarrollador traduzca en un algoritmo los acuerdos alcanzados por las partes.

Este proceso supone una etapa previa de negociación, en la cual deben definirse cuestiones esenciales como el objeto, las obligaciones de cada parte, la normativa aplicable, la jurisdicción competente y, en términos generales, los elementos característicos de cualquier contrato vinculante. La diferencia sustancial radica en que la ejecución no se realiza de forma tradicional, sino a través del propio programa, que activa de manera automática las disposiciones pactadas.

También encontramos otra clase de contratos, en los que no media ninguna negociación entre las partes. En este tipo de acuerdos, el usuario simplemente revisa las condiciones preestablecidas y decide si adherirse o no a ellas. Un caso ilustrativo se presenta en el ámbito de los seguros de viaje: a un pasajero se le ofrece cobertura automática frente a retrasos de vuelo.

Si el itinerario se cumple normalmente, la prima pagada representa un beneficio íntegro para el asegurador. Por el contrario, si ocurre la demora prevista en las cláusulas, el sistema ejecuta de inmediato el pago compensatorio en el medio elegido por el pasajero, sin necesidad de trámites adicionales.

Estos ejemplos evidencian que los SC, más allá de replicar acuerdos tradicionales en formato digital, ofrecen la posibilidad de diseñar mecanismos autónomos, seguros y verificables, con aplicaciones que abarcan desde operaciones financieras simples hasta procesos altamente sofisticados en distintos sectores económicos.

2.4. Revisión normativa relevante: Derecho Comparado y aplicación de los SC en Colombia.

Partiendo de la premisa de que los SC constituyen acuerdos entre partes cuya forma de expresión es el código de programación, puede afirmarse que se trata de verdaderos contratos, vinculantes y obligatorios para quienes los celebran.No obstante, autores como Almonacid Sierra y Coronel Ávila (2020) advierten que las características intrínsecas de los SC —como la inmutabilidad de las transacciones, la autoejecución sin intervención humana y las dificultades para corregir errores— introducen riesgos que no encuentran tratamiento adecuado bajo el derecho contractual tradicional, justificando así la necesidad de un régimen jurídico específico.

En Estados Unidos, no existe mayor controversia sobre la validez y obligatoriedad de los SC. Varios estados, como Delaware, Arizona o Vermont, han avanzado en su reconocimiento jurídico, adoptando normas que equiparan los efectos de la tecnología *Blockchain* y las firmas electrónicas a los mecanismos contractuales tradicionales. Estas regulaciones buscan, en términos generales, otorgar seguridad jurídica a las operaciones realizadas mediante *Blockchain*, reconociendo la validez de los datos electrónicos allí registrados y la ejecutabilidad de los SC dentro del comercio electrónico.

En el contexto europeo, los avances legislativos de la Unión Europea reflejan una tendencia hacia el diseño de marcos normativos especializados que aborden los desafíos propios de los SC (Parlamento Europeo, 2023). Asimismo, la normativa española ha aportado consideraciones de gran relevancia en materia de comercio electrónico.

Tal como expone Illezcas Ortíz, de la legislación vigente se desprenden cinco principios rectores: (i) la equiparación jurídica entre los actos electrónicos y los realizados de forma manuscrita; (ii) la neutralidad tecnológica de las disposiciones regulatorias; (iii) la preservación de las reglas tradicionales sobre obligaciones y contratos; (iv) la exigencia de actuar conforme a la buena fe; y (v) la libertad de pactar. Desde esta perspectiva, el regulador español reconoce que los principios de neutralidad tecnológica y de inalterabilidad contractual resultan plenamente aplicables a los SC, en la medida en que la automatización de su ejecución no elimina la existencia del consentimiento entre las partes.

La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) establece el marco aplicable a las operaciones en línea, incluyendo aspectos como el lugar de perfeccionamiento del contrato. En particular, el artículo 29 de la citada Ley dispone que, cuando participe un consumidor, se entenderá celebrado en el lugar de su residencia habitual.

Sin perjuicio de lo anterior, y pese a estos avances, la autonomía de la voluntad continúa siendo el eje problemático en diversas jurisdicciones. En especial, cuando un contrato inteligente contiene errores en su codificación, el conflicto debe resolverse conforme a las normas de responsabilidad contractual, recordando que detrás de cada algoritmo existe siempre un programador humano, y por tanto, un margen de error.

Teniendo en cuenta lo expuesto, puede sostenerse que, más allá de una regulación especial orientada a contextualizar el uso de la tecnología *Blockchain*, los SC no requieren de un marco normativo distinto al que ya emana de la legislación vigente en cada país. En este sentido, la adopción de dichas tecnologías favorece la eficiencia, incrementa la productividad y contribuye a la mitigación de los riesgos operacionales propios de las transacciones realizadas en entornos digitales.

Para el caso de Colombia, la implementación de SC se encuentra en fase de desarrollo, especialmente en el sector financiero y el marco normativo vigente en materia de contratación electrónica, comercio digital y tecnología permite su análisis y aplicación.

Desde la perspectiva jurídica, como ya se ha mencionado, los SC podrían encuadrarse dentro de los contratos electrónicos regulados por la Ley 527 de 1999 y el Decreto 2364 de 2012. Este respaldo normativo ha sido complementado con instrumentos y lineamientos emitidos por la Superintendencia Financiera y la Superintendencia de Sociedades en el marco de la transformación digital del país.

Otros instrumentos relevantes incluyen:

1) Decreto 333 de 2014 (Reglamento del operador de confianza).
2) Ley 1341 de 2009 (Principios de convergencia tecnológica).
3) Normativa de la Superintendencia Financiera de Colombia sobre tecnologías de la información y su aplicación en entidades vigiladas, entre ellas, la Circular Externa 014 de 2022, mediante la cual, se adoptaron de forma.en forma permanente algunas instrucciones transitorias emitidas durante la emergencia sanitaria con ocasión de la pandemia del COVID-19.

En cuanto a usos concretos, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha desarrollado pilotos con *Blockchain* para mejorar la transparencia en procesos de contratación, utilizando SC que liberan pagos automáticamente al verificarse la ejecución de ciertos hitos contractuales. En el ámbito financiero, *startups* y entidades *fintech* han comenzado a integrar SC para préstamos P2P, automatización de pagos y validación de identidad.

El entorno de pruebas regulatorias (*sandbox*) promovido por la Superintendencia Financiera ha permitido el desarrollo de estas tecnologías dentro de un marco supervisado. En paralelo y en línea con la normativa citada, se ha establecido que, las entidades vigiladas están llamadas a fomentar el uso de canales digitales en la prestación de servicios a los consumidores financieros, garantizando en todo momento condiciones adecuadas de seguridad y calidad para la realización de las operaciones.

De igual manera, las entidades pueden incorporar tecnologías emergentes —como la realidad aumentada, el internet de las cosas, *Blockchain*, inteligencia artificial, machine learning, big data o robótica, entre otras— siempre que ello resulte pertinente para mejorar la experiencia de los consumidores financieros y optimizar sus procesos internos. Para tal fin, será indispensable que dichas entidades trabajen en la implementación de una gestión adecuada de los riesgos inherentes a la tecnología adoptada, verificar de manera periódica la eficacia de los controles establecidos y cumplir de forma estricta con la normativa vigente en materia de protección de datos personales y hábeas data.

Por su parte, varios académicos han señalado que, si bien su ejecución automática representa una innovación contractual significativa, persisten retos en cuanto a la interpretación, la imputación de responsabilidades y la resolución de controversias derivadas de estos contratos. Por ello, recomiendan entenderlos como una evolución de la contratación electrónica que debe analizarse dentro del marco de la autonomía privada y los principios contractuales vigentes.

2.5.Retos jurídicos en la implementación de SC en Colombia.

Aunque los SC ofrecen ventajas significativas en términos de automatización, eficiencia y transparencia, su adopción en el contexto colombiano plantea importantes desafíos jurídicos que requieren una evaluación cuidadosa desde la teoría general del contrato.

Los SC presentan desafíos particulares en cuanto a la formación del consentimiento, que se da a través de la aceptación del código informático y no mediante declaraciones tradicionales. Esto genera interrogantes sobre la comprensión real de los términos y la posibilidad de retractación.

La atribución de responsabilidades también resulta compleja, especialmente en contratos con lógica condicional o elementos de inteligencia artificial, y se intensifica en plataformas descentralizadas donde no hay un único operador. Asimismo, la interpretación del contrato y la resolución de controversias dependen del código fuente, lo que puede generar rigidez y dificultades ante eventos imprevistos.

Desde el punto de vista procesal, surge la necesidad de adaptar los mecanismos de prueba y ejecución, dado que el código requiere análisis técnico especializado. Aunque existe regulación aplicable en materia de contratación electrónica, esta no es completamente suficiente para abordar todas las particularidades de los SC, lo que genera cierta incertidumbre. Para que estos contratos cumplan con los requisitos esenciales, resulta fundamental garantizar trazabilidad, autenticidad, consentimiento informado y capacidad de las partes.

En conclusión, su implementación efectiva no solo demanda ajustes normativos, sino también evolución en la interpretación jurídica, formación de operadores y estándares técnicos que permitan integrar esta tecnología dentro del derecho privado de manera segura y confiable.

3. Análisis jurídico de los SC en Colombia.

3.1. Naturaleza jurídica: contratos atípicos y su reconocimiento en derecho colombiano.

En Colombia, los SC deben ser inicialmente abordados bajo la categoría de contratos atípicos, dado que no cuentan con una regulación expresa en la legislación vigente. Esta posibilidad encuentra su fundamento en el principio de autonomía privada, el cual permite a los particulares celebrar acuerdos que respondan a sus intereses, siempre que respeten el orden público, la ley y las buenas costumbres.

Dicho principio se desprende de la estructura general del derecho privado colombiano, reflejado en normas como el artículo 1495 del Código Civil, que define el contrato como una convención orientada a constituir, regular o extinguir obligaciones, sin exigir que las mismas estén previamente tipificadas.

La doctrina colombiana ha profundizado en el análisis del fundamento de los contratos atípicos. En particular, Pardo Mantilla (2015) sostiene que la atipicidad contractual constituye una manifestación legítima de la autonomía privada, entendida como la facultad de los individuos para estructurar acuerdos jurídicos que no necesariamente correspondan a figuras expresamente previstas por el legislador. En tal sentido, los contratos atípicos son válidos en tanto cumplan con los requisitos esenciales de existencia y validez: consentimiento, objeto lícito y causa.

De acuerdo con esta perspectiva, los SC, aunque innovadores y mediados por tecnología *Blockchain*, pueden desplegar efectos jurídicos plenos en el derecho colombiano bajo la categoría de contratos atípicos. Su régimen jurídico se encuentra determinado, en primer lugar, por la voluntad de las partes y, en defecto de regulación específica, por los principios generales del derecho.

La jurisprudencia de la Corte Suprema de Justicia ha ratificado esta interpretación, reconociendo que la ausencia de tipificación legal no invalida un acuerdo que cumpla con los elementos esenciales exigidos para su formación. En consecuencia, los SC, en tanto figuras contractuales innovadoras, pueden ser reconocidos válidamente en el derecho colombiano, evidenciando la capacidad del sistema jurídico para adaptarse a las nuevas formas de contratación surgidas en el marco de la transformación digital.

Así, aunque los SC se consideran atípicos por su innovación y mediación tecnológica, el sistema jurídico colombiano sí les brinda soporte. Las normas generales de los códigos Civil y de Comercio, junto con la legislación sobre contratación electrónica y demás disposiciones, permiten que estos contratos desplieguen efectos jurídicos plenos, siempre que se cumplan los requisitos esenciales.

Esto demuestra que, pese al reciente desarrollo de una regulación específica detallada, el marco normativo existente proporciona herramientas suficientes para su reconocimiento, ejecución y validez, reflejando la capacidad del derecho colombiano de adaptarse a nuevas formas de contratación surgidas en la era digital.

3.2. Aplicación de Elementos del Derecho Contractual: Oferta, Aceptación, Consentimiento, Objeto y Causa.

La integración de los SC al derecho contractual colombiano demanda un examen sobre su compatibilidad con los elementos estructurales de todo contrato: (i) oferta, (ii) aceptación, (iii) consentimiento, (iv) objeto y (v) causa. Estos conceptos, reflejados en el Código Civil y el Código de Comercio, constituyen el núcleo de la validez contractual. En cuanto a la oferta y la aceptación, estas figuras encuentran un correlato funcional en el entorno digital.

El diseño del código que establece las condiciones de ejecución puede interpretarse como una manifestación anticipada de oferta, mientras que la interacción del usuario con la *Blockchain* constituye la aceptación que perfecciona el contrato. Este proceso,

aunque mediado tecnológicamente, no elimina la existencia de un acuerdo de voluntades, sino que reconfigura la manera en que se exterioriza.

El consentimiento, por su parte, plantea una de las mayores tensiones conceptuales. La automatización y la despersonalización del proceso contractual han dado lugar a lo que algunos autores denominan "*consentimiento algorítmico*", expresión que busca dar cuenta de cómo la voluntad se plasma en la programación inicial y se activa con la interacción del usuario. No obstante, este modelo no excluye la posibilidad de vicios del consentimiento, particularmente frente a la opacidad técnica del código o los errores de programación, situaciones que deben resolverse a la luz de los principios tradicionales de responsabilidad contractual.

Respecto del objeto y la causa, los SC permanecen sujetos a las exigencias del ordenamiento colombiano: el objeto debe ser lícito, determinado o determinable (art. 1517 C.C.), y la causa igualmente lícita (art. 1524 C.C.). La automatización de la ejecución no exime del cumplimiento de estas condiciones, de modo que un contrato inteligente cuyo contenido sea ilícito carecerá de efectos jurídicos válidos, independientemente de la neutralidad tecnológica que lo soporte.

En conclusión, los SC no sustituyen los principios clásicos del derecho contractual, sino que los trasladan a un escenario tecnológico distinto. Oferta, aceptación, consentimiento, objeto y causa siguen siendo requisitos ineludibles de validez, aunque su manifestación se canalice a través de la programación informática y la ejecución automática.

En este sentido, la regulación colombiana ya ofrece bases normativas suficientes para reconocer su eficacia, siempre que respeten el orden público y las normas imperativas, lo que demuestra que la novedad tecnológica no desarraiga los fundamentos del derecho contractual, sino que los desafía a dialogar con nuevas formas de expresión de la autonomía privada.

Si bien la regulación vigente ha permitido reconocer y dotar de validez a los SC dentro del marco jurídico colombiano, resulta evidente la ausencia de una norma que los regule de manera específica, como ya ha ocurrido en distintas jurisdicciones comparadas. Esta carencia se hace especialmente notoria en el sector financiero, caracterizado por su alta regulación y su dependencia de la certeza jurídica.

La falta de una anticipación normativa en este ámbito puede traducirse en mayores costos de cumplimiento, un aumento de la litigiosidad y, en consecuencia, una disminución de la competitividad del país en un entorno globalizado. Ante este panorama, se vuelve indispensable que el legislador colombiano adopte esquemas de regulación proactiva y flexible, capaces de acompañar los procesos de transformación digital, garantizando la protección de los derechos de las partes y, al mismo tiempo, fomentando una innovación responsable.

4. Desafíos legales en la implementación de SC en el Sector Financiero.

4.1. Problemáticas relacionadas con el consentimiento algorítmico.

4.1.1. El consentimiento en entornos automatizados.

Como ya se ha abordado a lo largo de este texto, el consentimiento constituye un elemento esencial para la formación de todo contrato. En el contexto de los SC, el consentimiento se expresa a través de interacciones digitales programadas, lo que plantea interrogantes sobre su manifestación válida y consciente.

Cáceres Malagón (2024) introduce el concepto de "*Consentimiento Algorítmico*" para referirse a la aceptación de términos codificados que se ejecutan automáticamente, muchas veces sin una comprensión cabal del contenido por parte de los usuarios. Este fenómeno resulta particularmente problemático en el sector financiero, donde los productos y servicios contratados pueden tener implicaciones patrimoniales significativas. La problemática del consentimiento algorítmico también plantea desafíos en materia de transparencia, información previa y protección del consumidor financiero.

4.1.2. Deber de Información.

En el ámbito financiero, el deber de información hacia el consumidor constituye un principio fundamental. Las entidades deben garantizar que la información proporcionada sea cierta, objetiva, detallada, eficaz, completa, oportuna e idónea respecto de los productos y contratos que se celebren y ejecuten. Esta exigencia tiene una doble fundamentación: por un lado, de carácter jurídico, dado que el marco normativo impone obligaciones específicas de información y transparencia; y por otro, de naturaleza económica, relacionada con las particularidades de las operaciones financieras.

La obligación de informar encuentra su justificación económica en la existencia de una asimetría informativa inherente a las relaciones entre entidades financieras y consumidores. En estas transacciones, la entidad financiera, dispone de un volumen de información técnica y especializada significativamente superior al de su contraparte; el consumidor, lo que genera un desequilibrio natural en la posición de negociación.

Como señala la doctrina especializada en análisis económico del derecho, cualquier negocio jurídico en el que una parte posee información de la que carece su contraparte sitúa a esta última en una posición de desventaja, otorgando al titular de la información una ventaja negociadora injustificada (Posner, 2007).

Adicionalmente, la Corte Constitucional colombiana ha señalado que, en un contexto de información asimétrica, los consumidores tienden a adoptar decisiones de adquisición de bienes y servicios basadas en una relación de confianza, más que en una comprensión detallada de los términos y condiciones ofrecidos.

Esta realidad acentúa la necesidad de evaluar la buena fe objetiva derivada del deber de información, cuyo propósito es equilibrar la relación contractual y proteger la voluntad libre e informada del consumidor.

Surgen entonces cuestionamientos inevitables: ¿De qué sirve entregar información si el consumidor no la lee antes de aceptar? ¿Qué responsabilidad existe si, aún leyendo, no logra comprender lo que firma? ¿Puede una entidad financiera limitarse a entregar información técnica y compleja, sin asegurarse de su verdadero entendimiento? ¿Hasta qué punto es válido considerar que el consumidor ha renunciado a protegerse cuando firma de manera apresurada o sin plena conciencia de su decisión?

En el contexto de los SC, este problema se agrava, ya que la naturaleza técnica y automatizada del instrumento dificulta aún más la comprensión por parte de los consumidores. Por tanto, asegurar el cumplimiento del deber de información en los SC resulta crucial para proteger adecuadamente los intereses del consumidor financiero y para garantizar que el consentimiento otorgado sea libre, informado y consciente.

4.1.2.1.Deber de información en el ámbito del consumidor financiero.

En Colombia, el derecho a la información del consumidor es fundamental para decisiones de compra conscientes, especialmente en el comercio electrónico, donde existen riesgos de asimetrías informativas. La Ley 1480 de 2011 establece que la información debe ser clara, veraz, suficiente, oportuna y comprensible, incluyendo aspectos como uso, cantidad, precio y garantías. Los proveedores son responsables si la información es insuficiente o engañosa, mientras que los consumidores tienen la obligación de informarse y evaluar los datos disponibles. Este marco normativo busca equilibrar la relación de consumo, promoviendo transparencia, protección y seguridad jurídica en entornos digitales.

En el ámbito financiero, existe una regulación especial en materia de información al consumidor, contenida en el Estatuto Orgánico del Sistema Financiero. En particular, el numeral 1 del artículo 97 y el numeral 5 del artículo 98 establecen los deberes de las entidades vigiladas en cuanto a la información que deben proporcionar.

De acuerdo con estas disposiciones, las entidades sujetas a vigilancia tienen la obligación de suministrar información con las características mencionadas de tal forma que el consumidor cuente con los elementos adecuados para evaluar los riesgos y consecuencias de sus decisiones.

El alcance de estas normas permite concluir que sólo cuando el consumidor financiero conoce y comprende plenamente el significado jurídico y económico de lo que suscribe —ya sea un contrato o cualquier otro documento— y cuando dicha información está redactada de manera clara, concreta y sencilla, puede decirse que se garantiza su derecho a la información y se promueve un entorno de transparencia en las relaciones de consumo.

La Corte Constitucional, en reiterada jurisprudencia, ha sostenido que el derecho a recibir información cierta, suficiente, clara y oportuna es fundamental para la protección del consumidor. En esa línea, ha advertido que la información entregada no debe ser ambigua, oscura, insuficiente ni excesiva, ya que esto podría afectar negativamente la capacidad del consumidor medio —quien generalmente cuenta con recursos limitados para procesar información compleja— para comprender los términos contractuales al momento de la contratación.

En consecuencia, la Corte ha subrayado que la protección al consumidor no es meramente retórica, sino que constituye un eje esencial del ordenamiento jurídico, exigiendo que la información sea comprensible, objetiva y accesible, con el fin de que el consumidor pueda conocer sus deberes, ejercer oportunamente sus derechos y tomar decisiones fundamentadas sobre los productos o servicios financieros.

Por ello, el Alto Tribunal ha considerado que la restricción injustificada al acceso a la información configura una práctica abusiva, especialmente cuando proviene de quien ostenta una posición dominante. Esta asimetría —caracterizada por la diferencia económica, técnica y profesional entre las entidades financieras y los consumidores— exige un estándar más elevado de transparencia, a fin de equilibrar la relación jurídica y evitar que el desconocimiento del consumidor se traduzca en una desprotección efectiva de sus derechos.

4.1.2.2. El requisito de información y su tensión con el lenguaje de programación

De acuerdo con lo expuesto sobre el deber de información en el ámbito del consumidor financiero, el código de un SC no satisface los requisitos de información que exigen las normas de protección al consumidor financiero, principalmente porque su lenguaje no es accesible para un usuario promedio. Aunque uno de los atributos del código, como Solidity, es su claridad frente a la ambigüedad y subjetividad del lenguaje legal tradicional, esta "precisión" sólo resulta comprensible para quienes poseen conocimientos técnicos especializados.

Interpretar correctamente un SC requiere habilidades de programación que no pueden presumirse en una persona común, lo que genera una brecha significativa entre la intención de automatización y la comprensión del consumidor. Por esta razón, el código de un SC, por sí solo, no garantiza que se cumplan los estándares de información exigidos para productos financieros, ni asegura que el consumidor pueda tomar decisiones plenamente informadas.

Esto evidencia la necesidad de complementar los SC con mecanismos de divulgación, explicación o interfaces accesibles que permitan traducir los términos técnicos a un lenguaje comprensible y garantizar la protección efectiva de los derechos del consumidor.

Ante esta dificultad, es previsible que las empresas recurran a herramientas de visualización que mejoren la experiencia del usuario, ya que facilitan la comprensión de los contratos y reducen los costos asociados a posibles disputas. No obstante, debe diferenciarse entre el código del SC —un lenguaje de programación diseñado para ser interpretado por máquinas— y su visualización, que traduce dichas instrucciones a un formato comprensible para las personas. Aunque estas herramientas contribuyen a hacer más claros los documentos y a prevenir conflictos, también pueden originar discrepancias entre lo que percibe el consumidor y lo que realmente ejecuta el código. Para superar esta limitación se han desarrollado los *Ricardian Contracts*, que integran tres elementos: el código, encargado de automatizar las acciones; la prosa legal, destinada a regular derechos y obligaciones; y los parámetros —como precios, fechas o cantidades— que articulan ambos planos. Este modelo ofrece la posibilidad de innovar en el diseño contractual sin perder rigor técnico.

En el contexto colombiano, donde el código de un SC por sí mismo no satisface los requisitos de información exigidos al consumidor financiero por su carácter técnico y poco accesible, las interfaces visuales resultan útiles pero insuficientes. En este escenario, los *Ricardian Contracts* se perfilan como una alternativa más adecuada, al garantizar información clara, suficiente y comprensible, manteniendo al mismo tiempo la precisión de la programación. Más que imponer su adopción por vía normativa, lo recomendable es fomentar buenas prácticas que promuevan la innovación tecnológica dentro del marco legal vigente.

4.2. Riesgos derivados de la automatización: ejecuciones automáticas e imprevistos.

La automatización de la ejecución contractual, facilitada por tecnologías como *Blockchain* y los denominados SC, representa un avance significativo en términos de eficiencia, celeridad y desintermediación. No obstante, este modelo también implica riesgos jurídicos sustanciales, especialmente cuando la ejecución automática se produce sin espacio para la intervención humana o la adaptación frente a eventos imprevistos.

La característica de *inmutabilidad* que define a los SC puede derivar en situaciones contractuales rígidas, donde las partes no tienen la posibilidad de modificar o suspender la ejecución aun cuando surjan circunstancias sobrevinientes o errores en la programación del código.

Uno de los principales problemas radica en que los SC presuponen la perfección del código, lo cual es difícil de garantizar. La existencia de errores de programación (*bugs*) o una codificación que no represente fielmente la voluntad de las partes puede dar lugar a ejecuciones automáticas erróneas, con consecuencias irreversibles debido a la imposibilidad de detener o revertir el proceso una vez activado.

A diferencia de los contratos tradicionales, donde el incumplimiento puede evaluarse desde la perspectiva de la buena fe o la razonabilidad, la lógica binaria de los SC no

admite interpretaciones flexibles ni mecanismos de adaptación a la realidad contractual cambiante.

Además, la automatización contractual elimina deliberadamente la opción del incumplimiento eficiente, figura reconocida en el derecho contractual contemporáneo, según la cual una de las partes puede decidir no cumplir voluntariamente con sus obligaciones si ello le resulta más beneficioso, siempre y cuando indemnice adecuadamente a la otra parte. Esta posibilidad desaparece en los SC, dado que el sistema ejecuta automáticamente la obligación sin considerar criterios de costo-beneficio o de conveniencia económica

Otro aspecto crítico es la incapacidad de los SC para incorporar cláusulas abiertas, estándares de comportamiento o condiciones que requieran interpretación, como el cumplimiento de buena fe o el uso de medios razonables. En efecto, la ejecución automática requiere que las condiciones estén programadas con precisión ex ante, lo que reduce la posibilidad de adaptar la relación contractual a contextos dinámicos. Esta rigidez representa una amenaza en contratos de larga duración o sujetos a variaciones de mercado, donde la flexibilidad es una herramienta esencial para preservar el equilibrio y la funcionalidad del acuerdo.

Por último, la desconexión entre el código y la realidad puede ocasionar conflictos cuando la información que activa la ejecución automática proviene de eventos externos no verificables directamente por la *Blockchain*. En estos casos, la figura del *oráculo* —entidades o sistemas que transmiten datos del mundo real a la cadena de bloques— se vuelve indispensable, aunque introduce nuevos riesgos asociados a la confiabilidad, imparcialidad y disponibilidad de dicha fuente de información.

En conclusión, si bien la automatización representa un hito en la evolución de las relaciones contractuales, también impone desafíos regulatorios y técnicos que deben ser abordados con cautela. La reducción de la ambigüedad y la eliminación del juicio humano en la ejecución contractual pueden generar más problemas que soluciones, especialmente en contextos complejos o jurídicamente sensibles.

5. Análisis de casos.

5.1.Breve descripción de iniciativas y proyectos en Colombia.

En Colombia, la adopción de SC se ha dado principalmente en fases exploratorias, bajo modelos piloto o pruebas de concepto, especialmente en el sector financiero y asegurador. Esto responde a la necesidad de minimizar riesgos regulatorios, operativos y jurídicos, en línea con los principios de gestión prudencial que rigen estos sectores.

Uno de los entornos más relevantes ha sido el *sandbox regulatorio* de la Superintendencia Financiera de Colombia (2020), diseñado para permitir la experimentación tecnológica en condiciones supervisadas. Allí, entidades vigiladas y *startups* han probado soluciones que integran *Blockchain* y SC, con énfasis en

mecanismos de pago automatizados, validación de identidad digital y gestión de garantías.

En el ámbito *fintech*, se destacan proyectos enfocados en microcréditos y seguros paramétricos. *Startups* colombianas han utilizado SC que liberan desembolsos o indemnizaciones al verificarse condiciones como fenómenos climáticos adversos, integrando oráculos de datos. No obstante, la dependencia de fuentes externas confiables ha evidenciado limitaciones para asegurar la veracidad, oportunidad y legalidad de la información que alimenta el contrato.

5.1.1. *Sandbox* regulatorio Superintendencia Financiera de Colombia (SFC).

El Espacio Controlado de Prueba (ECP), conocido como *laArenera*, constituye la iniciativa de la Superintendencia Financiera de Colombia (SFC) para promover la innovación tecnológica en el sector financiero bajo un entorno supervisado y temporal. Su objetivo es permitir la experimentación de modelos de negocio basados en tecnologías emergentes —como *distributed ledger technology (DLT)*, *Blockchain* o SC— que en condiciones normales se enfrentarían a restricciones normativas, todo ello sin modificar de manera inmediata o definitiva el marco regulatorio vigente.

Este mecanismo se configura, por tanto, como una herramienta de aprendizaje regulatorio, en la medida en que permite evaluar riesgos, beneficios y limitaciones de los proyectos, al tiempo que garantiza la protección del consumidor y la estabilidad del sistema financiero.

Desde el punto de vista normativo, el ECP fue formalizado mediante el Decreto 1234 de 2020, incorporado al Decreto 2555 de 2010, que definió su naturaleza, objetivos y el esquema de dispensas regulatorias temporales para facilitar la prueba de innovaciones. Posteriormente, la SFC complementó este marco con la Circular Externa 016 de 2021 y el Manual del ECP, en los que se detallan los requisitos de acceso, etapas, métricas de evaluación y controles que rigen la participación en estos pilotos.

Cabe subrayar que dichas dispensas tienen un alcance limitado: no se extienden a regímenes de protección de datos personales (Ley 1581 de 2012), *habeas data* financiero (Ley 1266 de 2008), normativa cambiaria y tributaria, ni a la regulación monetaria del Banco de la República, los cuales deben cumplirse de manera estricta incluso en el contexto experimental.

En cuanto a su funcionamiento, el proceso de vinculación al *sandbox* comprende cuatro fases principales. En primer lugar, la postulación y evaluación ex ante, en la cual el proponente debe demostrar la novedad del modelo, su potencial de beneficio para el consumidor o el mercado, la adecuada gestión de riesgos tecnológicos, operativos, de ciberseguridad y de prevención de lavado de activos y financiación del terrorismo (LA/FT), así como la justificación de por qué su desarrollo requiere de un entorno controlado.

En segundo lugar, una vez aprobado el ingreso, la SFC expide una autorización con condiciones específicas, que delimita el alcance, duración, número de usuarios, volúmenes de operación, salvaguardas y obligaciones de reporte, además de los indicadores de éxito que permitirán evaluar el piloto. La tercera fase corresponde a la ejecución en condiciones de producción controlada, caracterizada por un monitoreo intensivo por parte de la autoridad, la aplicación de mecanismos de protección al consumidor y la previsión de distintas rutas de salida, que pueden consistir en el escalamiento del modelo, su cierre ordenado o la incorporación de ajustes regulatorios.

Finalmente, la cuarta fase está orientada a la generación de lecciones regulatorias, en tanto los resultados de la prueba alimentan el diseño de guías de supervisión, ajustes normativos o buenas prácticas que fortalezcan la interacción entre innovación y regulación.

5.1.1.1. Exposición de caso en el *Sandbox*: Emisión de bonos en *Blockchain* mediante SC en el ECP.

Uno de los hitos más relevantes del Espacio Controlado de Prueba (ECP) en Colombia fue la emisión y liquidación de un bono utilizando tecnología *Blockchain* y SC, en un proyecto conjunto con la participación del Grupo BID, Banco Davivienda como emisor, BID Invest como suscriptor, y con el Banco de la República como veedor, es decir, operó un nodo dentro de la red—y tuvo acceso a todo el ciclo de vida del instrumento: emisión, negociación, pagos, inscripción y cancelación, todo lo anterior, bajo la supervisión de la SFC.

Este proyecto, se trató de la primera experiencia regional en la que se probó, de manera integral, la emisión, colocación, negociación y liquidación de un instrumento de deuda en un entorno basado en tokenización y en automatismos de *settlement*[2] a través de SC. Este piloto experimentó con tecnología *Blockchain* en un contexto regulado, controlado por autoridades financieras y estudió cómo estas tecnologías pueden generar eficiencias operativas, menores costos, mayor transparencia y trazabilidad en los mercados de capitales colombianos.

En este sentido, el objetivo principal de esta prueba, fue validar, de extremo a extremo, la infraestructura tecnológica que soporta este tipo de operaciones, así como las eficiencias y desafíos asociados a su implementación. Toda la emisión, registro y liquidación del bono, por un monto de COP 110 millones, se llevó a cabo sobre la red *Blockchain* LACChain.

El piloto concluyó en 2022, cuando la SFC informó que el proceso se ejecutó exitosamente mediante el uso de SC, un token no fungible (NFT) y algoritmos diseñados para la operación. Los resultados confirmaron la existencia de ganancias operativas significativas, mayor trazabilidad en la cadena de negociación y la reducción

[2] Es el proceso final para completar una transacción mediante la transferencia de activos o fondos, asegurando que el comprador reciba lo acordado y el vendedor el pago.

de tiempos en los procesos post-negociación, lo cual ofrece insumos valiosos para una eventual modernización de la regulación en materia de infraestructura de mercado.

Desde el punto de vista jurídico, este caso evidencia la capacidad de los SC para automatizar obligaciones propias de los instrumentos financieros, tales como el pago de cupones, la ejecución de eventos corporativos o la liquidación de transacciones, garantizando simultáneamente trazabilidad, transparencia y control bajo la vigilancia del supervisor.

La prueba permitió, además, identificar y gestionar riesgos, validar mecanismos de protección y documentar los requisitos necesarios para su eventual escalabilidad normativa, confirmando el potencial de estas tecnologías para transformar la forma en que opera el mercado de valores colombiano.

5.1.2. Banco de la República y R3 Corda en Colombia.

La compañía especializada en tecnología de Registros Distribuidos (DLT), R3 realizó una alianza con el Banco de la República Colombia, para el desarrollo de la plataforma Blockchain Corda, enfocados en su uso para el intercambio de valores. La compañía establece la necesidad de esta alianza con el ente público, confirmando el potencial de la tecnología *Blockchain* para servicios financieros en Latinoamérica, el cual se basa en un modelo colaborativo de trabajo público-privado es crucial para acelerar la implementación de plataformas empresariales de DLT, como lo es Corda.

Estas experiencias revelan un patrón común: la tecnología es viable y deseable, pero aún se encuentra condicionada por la necesidad de ajustes normativos, criterios de interpretación jurídica claros y mayor estandarización en la interacción entre sistemas digitales y jurídicos.

5.2.Aprendizajes de los casos expuestos.

Estas experiencias dejan ver que los *sandboxes* regulatorios y las alianzas público-privadas no solo permiten validar la viabilidad técnica de los SC en entornos seguros, sino que también funcionan como espacios de construcción de confianza entre los actores del mercado y los reguladores. El piloto del bono en *Blockchain* mostró que es posible automatizar operaciones con altos estándares de trazabilidad, mientras que la iniciativa de R3 con el Banco de la República evidenció que la colaboración institucional es clave para impulsar plataformas de infraestructura financiera basadas en DLT.

El aprendizaje central que se desprende de ambos casos es que la tecnología por sí sola no basta: para que los SC y la tokenización se consoliden en el sector financiero se requieren marcos regulatorios claros, criterios jurídicos armonizados y mecanismos de gobernanza compartida que faciliten la integración entre lo digital y lo legal. En este sentido, los *sandboxes* no deben verse como fines en sí mismos, sino como laboratorios

normativos que anticipan ajustes regulatorios, promueven la innovación responsable y fortalecen la competitividad en un entorno financiero cada vez más globalizado.

6. Riesgos asociados a la implementación de SC.

Aunque la tecnología *Blockchain* ofrece beneficios significativos, su adopción también implica riesgos que deben ser gestionados de manera adecuada, en particular aquellos relacionados con la protección de los usuarios frente a posibles asimetrías de información o fallas en la prestación de servicios. Este escenario evidencia la necesidad de establecer marcos normativos y de gobernanza claros, que regulen la interacción de los distintos actores dentro del ecosistema digital y definan responsabilidades precisas en la cadena de valor. Solo así será posible garantizar un entorno seguro, confiable y alineado con los principios de transparencia y equidad que demanda el sistema financiero.

a) Protección de los Datos

En el sector financiero, la implementación de SC plantea riesgos significativos en materia de protección de datos personales. La inmutabilidad de la *Blockchain*, aunque es una de sus principales fortalezas en términos de seguridad y trazabilidad, puede entrar en tensión con derechos fundamentales como el *habeas data y* el derecho al olvido, al impedir la modificación o eliminación de la información una vez registrada.

De igual forma, la transparencia propia de estos sistemas incrementa la posibilidad de exposición de datos sensibles, facilitando prácticas de perfilamiento o vigilancia no autorizada. A ello se suma la dificultad de garantizar el control efectivo del titular sobre sus datos, pues la autonomía de los SC limita la revocación del consentimiento y la restricción de usos posteriores.

En escenarios transfronterizos, donde la red opera de manera descentralizada, la transferencia internacional de datos personales añade un nivel de complejidad adicional, al no siempre existir equivalencia en las garantías legales. Finalmente, la ausencia de reglas claras sobre la asignación de responsabilidad en caso de incidentes evidencia la necesidad de un marco normativo más robusto, capaz de equilibrar la innovación con la protección efectiva de los derechos de los usuarios.

b) Integridad de los Datos.

Por otro lado, si bien la tecnología *Blockchain* asegura inmutabilidad una vez que la información ha sido registrada, ello no garantiza la veracidad ni la precisión de los datos en el momento de su incorporación. Errores, omisiones o inconsistencias en el ingreso inicial —por ejemplo, en procesos de tokenización de activos, validación de identidades o registros transaccionales— pueden perpetuarse a lo largo de todo el ciclo de vida del contrato inteligente, generando consecuencias jurídicas y financieras de gran impacto.

En este contexto, la ausencia de mecanismos claros de verificación y auditoría previa pone en riesgo no solo la confiabilidad del sistema, sino también la protección de los derechos de los usuarios y la estabilidad del mercado.

c) Tratamiento de los Datos Personales.

La normativa vigente en cada jurisdicción impone obligaciones claras —como ocurre con el Reglamento General de Protección de Datos (RGPD) en la Unión Europea, que distingue entre controladores y procesadores de datos—, pero la arquitectura descentralizada de *Blockchain* dificulta precisar quién asume dichas responsabilidades cuando no existe un proveedor de servicios centralizado.

Por su parte, en Colombia, la Ley 1581 de 2012 está diseñada para un modelo de gobernanza centralizado, donde la figura del "Responsable del Tratamiento" está claramente definida y es la encargada de garantizar el cumplimiento de la ley. Sin embargo, en un entorno descentralizado de SC, no hay una entidad única y central a la que se puedan dirigir los reclamos, lo que crea un vacío de responsabilidad y deja a los titulares de los datos sin un mecanismo efectivo para hacer valer sus derechos.

Surgen entonces cuestionamientos críticos: ¿quién supervisa efectivamente el tratamiento de los datos?, ¿cómo se garantiza el derecho de supresión si la información registrada en la cadena es inmutable? Estas tensiones se acentúan en un entorno financiero, donde los datos de los usuarios son particularmente sensibles y estratégicos.

Por ello, cualquier iniciativa que implique la implementación de SC debe contemplar desde su fase de diseño el cumplimiento normativo aplicable en Colombia —especialmente la Ley 1581 de 2012 y sus decretos reglamentarios—, sin dejar de observar las buenas prácticas internacionales en materia de privacidad y gobernanza de datos. De lo contrario, se corre el riesgo de que la innovación tecnológica entre en conflicto con los derechos fundamentales de los consumidores financieros.

d) La Seguridad Cibernética o Ciberseguridad.

Si bien la tecnología *Blockchain* ofrece ventajas como la resistencia a la manipulación de registros, no está exenta de vulnerabilidades que pueden comprometer tanto la infraestructura como la confianza de los usuarios. Riesgos como fallos en el código de los SC, ataques a las llaves privadas, suplantación de identidad o brechas en la interoperabilidad con otros sistemas financieros tradicionales, representan amenazas críticas que deben ser gestionadas de manera anticipada.

Aunque la tecnología evoluciona con rapidez, los principios de ciberseguridad siguen siendo aplicables: protección de datos, gestión de accesos, monitoreo constante, respuesta a incidentes y planes de recuperación. En este sentido, la experiencia internacional ha demostrado que un enfoque de gestión integral del riesgo —que combine marcos de seguridad reconocidos, auditorías periódicas y simulaciones de vulnerabilidades— resulta indispensable para la adopción segura de soluciones basadas en *Blockchain*.

En el ámbito financiero, donde el impacto de un ataque puede traducirse en pérdidas económicas, sanciones regulatorias y afectación reputacional, estas medidas no son opcionales, sino un requisito esencial para garantizar confianza y sostenibilidad.

A esto se suman otros riesgos de seguridad y confidencialidad. La transparencia de las redes públicas de *Blockchain*, una de sus ventajas, contradice la obligación de confidencialidad de los datos personales. Aunque se pueden usar técnicas de encriptación para ofuscar la información, la permanencia de los datos, incluso encriptados, en la cadena sigue siendo un riesgo potencial. Además, los errores de codificación son una amenaza persistente, ya que la inmutabilidad de la cadena hace que un fallo en el código no pueda ser corregido fácilmente una vez que se ha desplegado el contrato inteligente.

e) Lavado de Activos y Financiación del Terrorismo.

Por otra parte, la tecnología *Blockchain* también puede facilitar la creación de esquemas de ocultamiento o fragmentación de operaciones, dificultando la identificación de beneficiarios finales o el origen ilícito de los fondos.

El carácter transnacional de las redes distribuidas incrementa la complejidad del monitoreo, ya que las operaciones pueden ejecutarse de manera automática, sin intervención humana, y fuera del alcance inmediato de las autoridades de supervisión locales. Esto genera un riesgo de arbitraje regulatorio y de uso indebido de la infraestructura para fines ilícitos.

Por lo tanto, resulta imprescindible complementar la automatización de los SC con mecanismos de debida diligencia digital, herramientas de análisis transaccional y estándares de *compliance* integrados en la programación de los contratos. De igual forma, es fundamental la cooperación entre entidades financieras, supervisores y desarrolladores tecnológicos, de manera que la innovación en servicios financieros no se convierta en un canal inadvertido para actividades de Lavado de Activos y Financiación del Terrorismo (en adelante “LA/FT”).

6.1.Mitigación de los Riesgos Asociados.

A fin de abordar los desafíos y riesgos identificados en el uso de SC en el sector financiero, es fundamental adoptar un enfoque proactivo que combine soluciones técnicas con un marco de gobernanza y regulación claro. Las siguientes recomendaciones buscan equilibrar la innovación con la protección efectiva de los datos personales y la seguridad jurídica.

En primer lugar, para resolver la tensión entre la inmutabilidad de la cadena de bloques y el derecho a la supresión de datos, se deben considerar modelos de arquitectura híbridos. Una de las soluciones más viables es almacenar los datos personales fuera de la cadena de bloques (*off-chain*) en sistemas centralizados que permitan su modificación y eliminación, registrando en la cadena solo una referencia o un *hash* criptográfico de la información.

Esto garantizaría que los datos sensibles no sean permanentes en la cadena, mientras que la integridad del registro se mantiene intacta. Además, se deben emplear técnicas de criptografía y encriptación para asegurar la confidencialidad de la información, incluso si esta se encuentra en una red visible para todos los nodos.

Por otra parte, en cuanto a la falta de claridad en la atribución de responsabilidades en un entorno descentralizado, es crucial establecer un marco de gobernanza explícito, pudiéndose optar por la implementación de *Blockchains* permisionadas o de consorcio.

En estas redes, los participantes son conocidos y auditables, lo que facilita la asignación de roles de "Responsable del Tratamiento" y "Encargado del Tratamiento" definidos por la Ley 1581 de 2012. El marco de gobernanza también debe definir los procedimientos para la resolución de disputas, la corrección de errores de programación y la gestión de incidentes.

Si bien la inmutabilidad de la cadena de bloques garantiza que los datos no se alteren una vez que se han registrado, no previene errores en el momento de su ingreso inicial. Para mitigar este riesgo, se deben implementar rigurosos mecanismos de verificación y auditoría antes de que la información se escriba en la cadena. Los SC deben ser diseñados para interactuar con "oráculos" o fuentes externas de información confiable, lo que permitiría validar la veracidad de los datos antes de que se activen las cláusulas contractuales.

Respecto del riesgo de ciberseguridad, las empresas deben adoptar un enfoque de gestión integral del riesgo que incluya auditorías de código exhaustivas y simulaciones de vulnerabilidad antes del despliegue del contrato. Dado que los errores en el código son una amenaza persistente debido a la inmutabilidad de la cadena, la prevención es la mejor estrategia.

Finalmente, el riesgo de lavado de activos y financiación del terrorismo debe abordarse mediante la integración de mecanismos de cumplimiento normativo directamente en la arquitectura de la red y los SC. Esto incluye la incorporación de herramientas de debida diligencia digital, análisis transaccional y cumplimiento (*compliance*) en la programación de los contratos.

Además, es crucial que los desarrolladores y las entidades financieras colaboren estrechamente para asegurar que la innovación no se convierta en un canal para actividades ilícitas y que se pueda identificar al beneficiario final de las transacciones, lo que se facilita en redes permisionadas donde los participantes son conocidos.

7. Conclusiones.

La implementación de SC y la tecnología *Blockchain* en el sector financiero colombiano se presenta como un catalizador para la modernización, ofreciendo beneficios tangibles que justifican su adopción. El análisis realizado en este artículo ha demostrado que la tecnología no solo es viable, sino que promete una transformación profunda al

automatizar acuerdos, reducir costos y tiempos operativos, y elevar los estándares de transparencia y trazabilidad en el sistema.

La experiencia práctica en el *sandbox* regulatorio de la Superintendencia Financiera de Colombia, con proyectos piloto como la emisión de bonos en *Blockchain*, ha validado este potencial, confirmando ganancias significativas en la eficiencia de los procesos post-negociación. A nivel jurídico, el marco normativo colombiano ya proporciona una base para el reconocimiento de los SC, encuadrándolos como una forma de contratación electrónica atípica, lo que refleja la capacidad del sistema legal para adaptarse a las innovaciones de la era digital.

No obstante, para capitalizar plenamente estos beneficios, es indispensable abordar los desafíos inherentes a la tecnología. La inmutabilidad de la cadena de bloques, si bien asegura la integridad de los registros, entra en una tensión conceptual con derechos fundamentales como el *hábeas data* y el derecho a la supresión de datos. De manera similar, la descentralización de la red, que elimina intermediarios, crea un vacío en la atribución de responsabilidades legales, lo que limita la capacidad de supervisión y la protección de los derechos de los consumidores.

La rigidez de la automatización y la opacidad técnica del código también exponen a riesgos como ejecuciones irreversibles por errores de programación y una asimetría de información que desafía el deber de transparencia y el consentimiento informado de los usuarios.

Para mitigar estos riesgos de manera efectiva, el camino a seguir no es la prohibición, sino la creación de un marco normativo que actúe como un facilitador de la innovación. Se requiere un enfoque híbrido que combine las virtudes de la tecnología con principios de gobernanza sólidos.

La implementación de soluciones técnicas como el almacenamiento de datos sensibles fuera de la cadena (*off-chain*) o el uso de redes permisionadas se perfila como una estrategia para armonizar la privacidad con la eficiencia. Asimismo, la adopción de modelos como los *Ricardian Contracts* se presenta como una vía para conciliar la precisión del código con la claridad de la prosa legal.

En definitiva, el éxito y la escalabilidad de los SC en el sector financiero colombiano dependerán de la colaboración indispensable entre reguladores, perfiles técnicos y juristas. El objetivo es construir un ecosistema digital que, reconociendo el potencial transformador de la tecnología, establezca las reglas claras de juego que mitiguen los riesgos, fortalezcan la confianza del público y garanticen la seguridad jurídica en un entorno cada vez más competitivo y globalizado.

8. Bibiliografia.

i) Almonacid Sierra, Juan Jorge, y Yeisson Coronel Ávila. 2020. “Aplicación de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado.” *Revista de Derecho Privado* 38 (enero-junio): 119-142.

https://doi.org/10.18601/01234366.n38.05.
ii) Cáceres Malagón, Juan Antonio. 2024. "¿Sueñan las máquinas con contratar? Un estudio sobre smart contracts y consentimiento algorítmico." *Revista de Derecho Privado* 46 (enero-junio): 155-185.
iii) Cárdenas Rincón, Andrés. 2022. "Contratos inteligentes en Colombia: una aproximación desde la teoría general del contrato." *Revista de Derecho Privado* 42 (enero-junio): 115-140.
iv) Congreso de Colombia. 1999. Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. 18 de agosto de 1999. *Diario Oficial* 43.654.
v) Congreso de Colombia. 2008. Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. 31 de diciembre de 2008. *Diario Oficial* 47.219.
vi) Congreso de Colombia. 2009. Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. 30 de julio de 2009.
vii) Congreso de Colombia. 2011. Ley 1480 de 2011. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. 12 de octubre de 2011.
viii) Congreso de Colombia. 2012. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012. *Diario Oficial* 48.584.
ix) Corte Constitucional de Colombia. 2000. Sentencia C-662 de 2000. 14 de junio de 2000. M.P. Álvaro Tafur Galvis.
x) Fuentes Blanco, Santiago. 2022. "Smart contracts: entre la automatización y el derecho." *Revista Estudios Socio-Jurídicos* 24, no. 2: 203-225.
xi) Guiza Pinzón, Estefany. 2021. "Aplicabilidad de los smart contracts en el ordenamiento jurídico colombiano y la protección al consumidor financiero." Tesis de maestría, Universidad de los Andes. https://repositorio.uniandes.edu.co/server/api/core/bitstreams/7f974baa-ac5a-4eae-a209-e6e51ca7f95c/content.
xii) Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). 2021. Guía para la implementación de blockchain. Bogotá: MinTIC. https://www.mintic.gov.co.
xiii) Padilla Sánchez, Jorge A. 2020. "Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos. Blockchain and Smart Contracts. Approach to their Legal Problems and Challenges." *Revista de Derecho Privado* 39: 175-201.
xiv) Pardo Mantilla, María Carolina. 2015. "Contratos atípicos: reflexiones sobre su fundamento y régimen jurídico." *Revista de Derecho Privado* 29: 147-172.
xv) Parlamento Europeo. 2023. "El Parlamento Europeo aprueba el reglamento de inteligencia artificial." *Publicación del Parlamento Europeo*, 13 de marzo de 2024. https://www.europarl.europa.eu/news/es/press-room/20240308IPR19015/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial.

xvi) Presidencia de la República de Colombia. 2012. Decreto 2364 de 2012. Por el cual se reglamenta el uso de las firmas electrónicas. 26 de noviembre de 2012. *Diario Oficial* 48.629.
xvii) Presidencia de la República de Colombia. 2020. Decreto 1234 de 2020. Por medio del cual se adiciona el Decreto 2555 de 2010 en lo relacionado con el espacio controlado de prueba para actividades de innovación financiera. 14 de septiembre de 2020.
xviii) Presidencia de la República de Colombia. 2022. Decreto 1297 de 2022. Por medio del cual se modifica el Decreto 2555 de 2010 en lo relacionado con la regulación de las finanzas abiertas en Colombia y se dictan otras disposiciones. 25 de julio de 2022.
xix) Puyol Montero, Javier. 2016. "Los smart contracts, contratos digitales." *Confilegal*, 3 de abril de 2016. https://confilegal.com/20160403-los-smart-contrats-contratos-digitales/.
xx) Szabo, Nick. 1997. Formalizing and Securing Relationships on Public Networks "First Monday"
xxi) Superintendencia Financiera de Colombia. 2020. Entorno de prueba regulatorio – Sandbox financiero. https://www.superfinanciera.gov.co.
xxii) Superintendencia Financiera de Colombia. 2022. Circular Externa 014 de 2022. 16 de junio de 2022.
xxiii) Superintendencia Financiera de Colombia. 2024. Circular Externa 004 de 2024. 7 de febrero de 2024.
xxiv) Tur Faúndez, Carlos. 2018. *Smart contracts. Análisis jurídico*. Madrid: Editorial Reus. España, 2018. P53, 60, 61,63