

Prototipo de sistema descentralizado para la gestión y verificación de evidencias digitales en fotocomparendos aplicando Blockchain e IPFS

Laura Catalina Preciado Ballen

Cristian Stiven Guzman Tovar

Proyecto de Monografía para Optar por el Título de
Ingeniero(a) de Sistemas



Universidad Distrital Francisco José De Caldas

Facultad de Ingeniería

Colombia, Bogotá D.C.

Julio de 2025

Índice

Introducción	1
Formulación del problema	1
Objetivos	5
Impacto o Alcance Esperado	6
Justificación	10
Marco Teórico	13
El Paradigma de la Confianza Descentralizada	13
Fundamentos de los Sistemas Distribuidos y Redes Descentralizadas	13
Tecnologías para la Gestión Descentralizada de Evidencia	14
Blockchain: Un Registro Distribuido, Inmutable y Transparente	14
IPFS: Almacenamiento Verificable mediante Direccionamiento por Contenido	16
Arquitectura de la Solución: Sinergia Blockchain-IPFS con el Patrón Off-Chain . .	16
Fundamentos Criptográficos Aplicados	17
Estado del Arte	18
Blockchain para Registros Gubernamentales y Gestión de Sanciones	18
Integración de Blockchain e IPFS para Datos Voluminosos y Verificables	19
Gestión de Evidencia Digital y Cadena de Custodia con DLT	20
Implementaciones reales de Blockchain en Gobiernos	22
Registro de propiedad en Suecia	22
Integridad de registros clínicos en Estonia	22
Síntesis y relevancia para el proyecto	22
Funcionamiento de los Fotocomparendos en Bogotá: Mecanismos, Regulación e Im-	
pacto	23
Aplicaciones Específicas en Gestión de Tráfico e Infracciones	25

Avances Significativos	26
Limitaciones Identificadas	28
Novedad y Relevancia del Prototipo	29
La relevancia del prototipo se justifica por su potencial para:	29
Análisis de tendencia internacional	30
Alcance	35
Enfoque y delimitación geográfica	35
Componentes del prototipo	35
Fuera del alcance	36
Entregables	36
Criterios de éxito	36
Limitaciones del Prototipo	36
Entorno de Validación	37
Integración y Comparación con Sistemas Existentes	37
Aspectos Técnicos y de Escalabilidad	38
Seguridad y Robustez	38
Metodología	39
Metodología de investigación	39
Metodología de desarrollo de software: Enfoque por Prototipos	39
Introducción a los artefactos técnicos del diseño	40
Diseño del Prototipo	41
Definición de Requisitos:	41
Diagrama de casos de uso del sistema de gestión de infracciones de tránsito . . .	43
Diagrama de Despliegue	43
Diagrama de clases	44

Diagrama de actividades	45
Interfaz de Usuario	45
Costos del Proyecto	55
Plan de Pruebas	56
Introducción y Propósito	56
Alcance de las Pruebas	56
Fuera de Alcance	56
Entorno de Pruebas (Simulación Controlada)	57
Tipos de Pruebas y Casos de Prueba Detallados	59
Pruebas de Inmutabilidad	59
Pruebas de Rendimiento Básico	60
Casos de Prueba de Inmutabilidad y Verificabilidad	62
Estrategia de pruebas del frontend	62
Herramientas y Tecnologías	63
Pruebas Unitarias	63
Pruebas de Integración	63
Resultados de las Pruebas de Inmutabilidad y Verificabilidad del Prototipo	64
Pruebas de Inmutabilidad en Blockchain	64
Verificación de Integridad con IPFS	64
Verificabilidad Transparente del Registro	64
Casos de Prueba Funcionales	65
Casos de Prueba Funcionales	65
Casos de Prueba de Inmutabilidad	66
Pruebas de Rendimiento Básico	66
Conclusiones	68

Índice de figuras

Figura 1. Estadísticas de comparendos emitidos en Bogotá entre enero de 2018 y agosto de 2024	2
Figura 2. Distribución global de la producción científica sobre blockchain y gestión de infracciones	31
Figura 3. Evolución anual de publicaciones en los países líderes del tema (Brasil, México, Colombia, España y Perú)	32
Figura 4. Nube de palabras de los términos más recurrentes en la literatura sobre blockchain e infracciones	33
Figura 5. Mapa temático de los principales temas de investigación en el área	34
Figura 6. Diagrama de casos de uso del sistema de gestión de infracciones de tránsito	44
Figura 7. Diagrama de despliegue de la arquitectura del sistema	45
Figura 8. Diagrama de clases del sistema de gestión de multas	46
Figura 9. Diagrama de actividades para el proceso de apelación de multa	47
Figura 10. Diagrama de actividades para el proceso de creación de multa	48
Figura 11. Pantalla de login del sistema	49
Figura 12. Pantalla de recuperación de contraseña	50
Figura 13. Dashboard del agente de tránsito	51
Figura 14. Pantalla de consulta del estado de multa	52
Figura 15. Pantalla de consulta de detalle de multa	53
Figura 16. Pantalla de consulta de multas para propietarios de vehículos	54

Índice de tablas

Tabla 1. Comparación entre bases de datos tradicionales y blockchain para gestión de registros gubernamentales	4
Tabla 2. Comparación entre un modelo centralizado y un modelo descentralizado .	11
Tabla 3. Análisis Comparativo del Estado del Arte en Gestión de Infracciones con Blockchain	27
Tabla 2. Casos de prueba funcionales para validar operaciones básicas del sistema	58
Tabla 3. Casos de prueba de inmutabilidad para validar resistencia a modificaciones	59
Tabla 4. Resultados de pruebas de inmutabilidad del sistema	60
Tabla 5. Resultados de pruebas funcionales del sistema	65
Tabla 6. Resumen de casos de prueba de inmutabilidad ejecutados	66
Tabla 7. Tiempos promedio de operaciones en el entorno de prueba	67

Introducción

En Colombia, la gestión de fotocomparendos ha sido objeto de controversia debido a fallas en la transparencia y posibles manipulaciones en el proceso de registro y validación de infracciones. La falta de un sistema confiable ha generado desconfianza entre los ciudadanos, lo que evidencia la necesidad de una solución que garantice la integridad, inmutabilidad y verificabilidad de la información.

La tecnología Blockchain ha demostrado ser una alternativa eficaz para el almacenamiento seguro y descentralizado de datos, asegurando que una vez registrados, estos no puedan ser alterados sin dejar rastro. A través de contratos inteligentes, es posible automatizar la validación y el procesamiento de fotocomparendos, reduciendo la intervención humana y minimizando el riesgo de corrupción o errores administrativos.

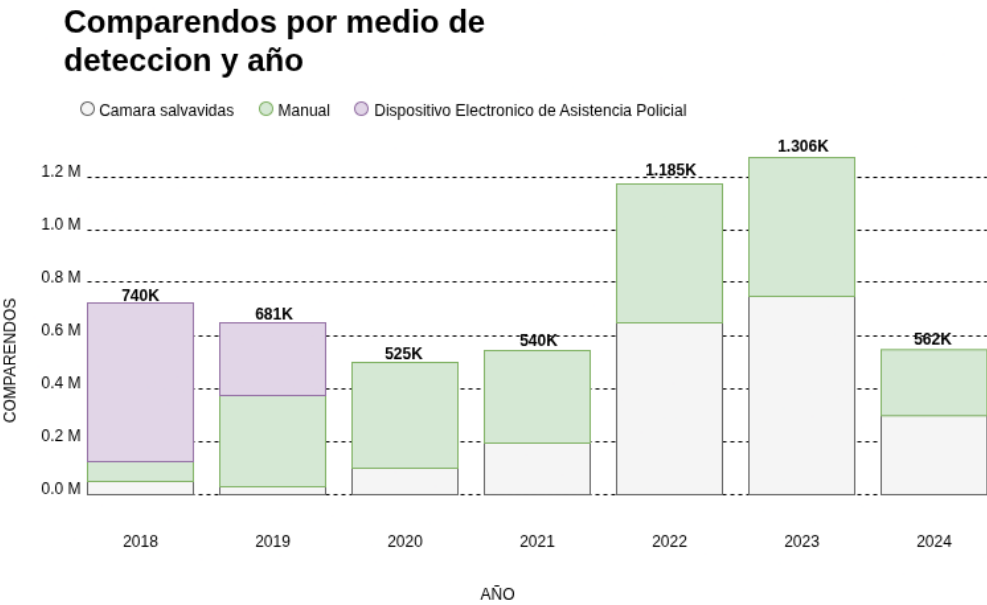
Este trabajo propone el diseño e implementación de un prototipo basado en Blockchain para la gestión de fotocomparendos en Bogotá, con el objetivo de garantizar la transparencia del proceso. Se utilizarán contratos inteligentes para registrar cada infracción, permitiendo que cualquier actor autorizado pueda verificar su autenticidad sin necesidad de intermediarios. Mediante pruebas y simulaciones, se evaluará la viabilidad del sistema, demostrando cómo esta tecnología puede fortalecer la confianza en los procesos de control de tránsito y mejorar la eficiencia en la gestión de sanciones.

Formulación del problema

La gestión de comparendos en Bogotá es un proceso de gran escala. Según datos del Observatorio de Movilidad, entre enero de 2018 y agosto de 2024 se emitieron más de 1.9 millones de comparendos a través de cámaras salvavidas, evidenciando la importancia sistémica de este proceso para la regulación del tránsito en la ciudad, como se presenta en la Figura 1 se observa los diferentes métodos utilizados para crear los comparendos. Esta operación se apoya en el sistema FÉNIX, una aplicación con infraestructura en la nube, cuya arquitectura de datos y control de acceso opera bajo un paradigma centralizado. En el sistema actual, la validez e inmutabilidad de los registros de infracciones se

Figura 1

Estadísticas de comparendos emitidos en Bogotá entre enero de 2018 y agosto de 2024



Nota. Elaboración propia basado en datos del Observatorio de Movilidad.

fundamenta en los procedimientos administrativos y en la gestión de los funcionarios responsables del sistema (Consejo de Estado, 2018). Los cambios en la información solo pueden ser detectados por las entidades autorizadas, lo que implica que el control sobre los registros depende directamente de la correcta aplicación de las políticas internas y del seguimiento realizado por dichas entidades (Consejo de Estado, 2019). La evidencia generada se conserva bajo un modelo centralizado, en el cual la confianza en la integridad de los datos se sostiene en mecanismos administrativos y controles internos, más que en garantías técnicas accesibles públicamente (Departamento Administrativo de la Función Pública, 2021). La potestad sancionatoria y el debido procedimiento administrativo aseguran la validez de los actos administrativos y la correcta motivación en la imposición

de sanciones (Corte Constitucional, 2022; Gamero Casado y Fernández Ramos, s.f.).

De acuerdo con la Auditoría de Cumplimiento de la Contraloría de Bogotá (2024), en el proceso de desarrollo del sistema FÉNIX se identificaron dificultades relacionadas con la supervisión contractual, lo que derivó en retrasos, duplicidad de sistemas y un presunto detrimento patrimonial estimado en más de \$8.000 millones de pesos. Estos hallazgos reflejan que, desde su implementación, la plataforma ha enfrentado retos significativos en materia de gobernanza y gestión, los cuales han tenido impacto en la eficiencia administrativa y en la sostenibilidad financiera del proyecto.

Estas debilidades se manifiestan en la operación técnica actual. A nivel operativo, el riesgo de integridad se materializa en una fricción a gran escala con la ciudadanía. Un análisis correlacional de fuentes oficiales para el primer semestre de 2025 revela la magnitud de esta fricción: frente a 457.000 comparendos impuestos [Observatorio de Movilidad, 2025], se gestionaron 155.854 PQRSD [Informe de Gestión PQRSD, 2025]. De estos datos se deduce una Tasa de Impugnación general del 34.1 %, un indicador cuantitativo que sugiere que al menos uno de cada tres actos administrativos del sistema genera una disputa formal, reflejando una carga administrativa insostenible y un déficit de confianza.

La desconfianza generada por estas opacidades y dificultades procesales crea un vacío que es explotado por terceros, afectando directamente al ciudadano. Reportajes de prensa documentan cómo la ausencia de canales oficiales percibidos como confiables ha fomentado la aparición de redes de fraude, como el caso de Juzto.co, donde miles de ciudadanos fueron estafados con promesas de impugnaciones garantizadas, resultando en trámites inconclusos y mayores deudas (Semana, 2023).

La identificación de estas limitaciones permite estructurar el problema en torno a variables que reflejan tanto el modelo de confianza actual como sus impactos técnicos, operativos y financieros. La Tabla 1 sintetiza estas variables y los indicadores asociados, mostrando cómo el paradigma centralizado de gestión condiciona la integridad de los datos, la eficiencia administrativa, la confianza ciudadana y la sostenibilidad del sistema.

Tabla 1*Comparación entre bases de bd y blockchain para gestión de registros gubernamentales*

Característica	Base de Datos Convencional	Blockchain
Modelo de confianza	Se basa en un administrador central (entidad de TI)	Confianza distribuida entre múltiples nodos
Inmutabilidad	Registros pueden ser modificados o eliminados por administradores	Los registros son inmutables por diseño
Trazabilidad / Auditoría	Depende de la implementación y control interno	Historial completo e inalterable disponible
Riesgo de corrupción interna	Alto, si hay privilegios indebidos o colusión	Bajo, no se puede alterar sin consenso de la red
Seguridad criptográfica	Opcional, no siempre integrada nativamente	Integrada (firmas digitales, hashes, cifrado)
Disponibilidad / tolerancia a fallos	Riesgo de puntos únicos de falla	Alta disponibilidad por replicación descentralizada
Velocidad de operación	Alta velocidad en lectura/escritura	Menor velocidad, prioriza integridad y consenso

Nota. Elaboración propia.

En síntesis, el problema se formula como un Riesgo de Integridad de Datos inherente al paradigma de confianza centralizada del sistema de fotocomparendos. Este riesgo se encuentra documentado por debilidades fundacionales en la gobernanza del proyecto y se manifiesta en consecuencias medibles: (i) una Tasa de Impugnación del 34.1 %; (ii) una carga operativa superior a 155 mil PQRSD semestrales; (iii) un presunto detrimento patrimonial por más de \$8.000 millones; y (iv) la vulnerabilidad de la ciudadanía a esquemas fraudulentos derivados de la falta de transparencia institucional.

Ante este panorama, surge la necesidad de explorar arquitecturas que permitan sustituir la confianza administrativa por garantías criptográficas. La pregunta central que guía este trabajo es:

¿Cómo mitigar el Riesgo de Integridad de Datos en el proceso de fotocomparendos en Bogotá?

Objetivos

Objetivo General. Desarrollar un prototipo para apoyar el registro y trazabilidad de estados en el proceso de fotocomparendos en Bogotá, aplicando tecnologías de redes distribuidas, con el fin de fortalecer la integridad, la autenticidad de la información, y reducir los riesgos asociados a su confidencialidad.

Objetivos específicos.

- Analizar el proceso actual de registro de fotocomparendos en Bogotá, a partir del marco jurídico y regulatorio que lo rige y de los informes de auditoría emitidos por la secretaria distrital de movilidad sobre la gestión de comparendos, para identificar requisitos funcionales, no funcionales y vulnerabilidades que el prototipo debe proporcionar.
- Desarrollar un prototipo con arquitectura híbrida fundamentada en la técnica de descomposición por confianza, integrando tecnologías de almacenamiento distribuido y contenido cifrado, asegurando que cada transacción incorpore los metadatos del

comparendo y disponiendo de una interfaz básica para demostrar que es posible un aplicativo transparente y confiable.

- Evaluar la viabilidad del prototipo desarrollado, mediante la ejecución de un plan de pruebas funcionales y evaluación de métricas de desempeño en un entorno de pruebas, para validar las condiciones de inmutabilidad, trazabilidad y seguridad.

Impacto o Alcance Esperado

Alcance. Enfoque y delimitación geográfica: Este trabajo se circunscribe al proceso de trazabilidad de estados de multas de tránsito automatizadas (fotomultas) emitidas por la Secretaría Distrital de Movilidad de Bogotá. Se excluyen de manera explícita los siguientes aspectos:

- Multas impuestas de forma presencial por agentes de tránsito.
- Procesos sancionatorios de otras ciudades o entidades territoriales.
- Funcionalidades de recaudo y pasarelas de pago (solo se registra el estado del pago, no se procesa el pago en sí).

Componentes del prototipo: El prototipo aborda los siguientes módulos funcionales:

- **Registro inmutable de la infracción:** Captura de metadatos (placa, fecha, hora, ubicación y tipo de infracción) y publicación del identificador de la evidencia en la blockchain (Hyperledger Fabric).
- **Almacenamiento descentralizado de evidencias:** Carga de la imagen o video de la fotomulta en IPFS y obtención de su hash.
- **Verificación pública:** Servicio de consulta que permite contrastar el hash guardado en la cadena con el archivo almacenado en IPFS.

- **Gestión del ciclo de vida de la multa:** Estados: Generada → Notificada → En apelación → Pagada → Cerrada. Cada transición queda registrada mediante eventos de contrato inteligente.
- **Interfaz mínima:** Panel Web para: (i) agentes que registran la infracción y (ii) ciudadanos que consultan la autenticidad y el estado de su fotomulta.

Fuera del alcance:

- Integración completa con sistemas legados del RUNT o SIMIT; se simula mediante datos de prueba.
- Implementación de un modelo económico (tarifas de gas, costos operativos reales).
- Implementación de algoritmos de detección automática de infracciones (visión por computador). Se parte de que la cámara ya detectó la infracción y generó la evidencia.
- Despliegue en un entorno de producción o capacidad más de 10 usuarios.

Entregables:

- Contrato inteligente en Solidity (o «chaincode» en Go, según la red seleccionada) con pruebas unitarias.
- Script de despliegue de red Hyperledger Fabric e instalación de IPFS local.
- Aplicación Web de demostración (frontend ligero) conectada a los servicios anteriores.
- Manual técnico que documenta la arquitectura y el flujo de datos.
- Informe de resultados de las pruebas funcionales y de rendimiento básico.

Criterios de éxito:

- Tiempo medio de publicación de una infracción ≤ 3 s en entorno de laboratorio.

- Coincidencia 100 % entre el hash almacenado en la cadena y la evidencia recuperada desde IPFS.
- Trazabilidad completa del historial de estados para al menos 50 multas de prueba.
- Ausencia de fallos críticos en pruebas de carga con 10 transacciones concurrentes.

Limitaciones del Prototipo. Es fundamental reconocer que, como prototipo desarrollado en un contexto académico, el presente estudio presenta ciertas limitaciones que definen el alcance de sus conclusiones y delinean claras oportunidades para futuras investigaciones. Las principales limitaciones son:

Entorno de Validación:

- **Validación en Entorno de Laboratorio:** El prototipo fue diseñado, desplegado y evaluado en un entorno de simulación controlado. No se sometió a pruebas en una infraestructura productiva real con la carga de transacciones y el volumen de usuarios que gestiona actualmente la Secretaría de Movilidad.
- **Uso de Datos Simulados:** Debido a estrictas normativas de privacidad y protección de datos personales que impiden el acceso a información real de ciudadanos y vehículos, todas las pruebas se realizaron con datos sintéticos.
- **Suposiciones sobre la Calidad de la Evidencia:** El sistema asume que las evidencias fotográficas (imágenes de fotocomparendos) son capturadas con una calidad suficiente para su procesamiento.

Integración y Comparación con Sistemas Existentes:

- **Integración Simulada con Sistemas Externos:** La interacción con plataformas gubernamentales clave como el RUNT y el SIMIT fue simulada a través de APIs de prueba (mocks).

- **Ausencia de Benchmarking Directo con el Sistema Actual (Fénix):** La falta de acceso al código fuente y a la arquitectura interna del sistema Fénix impidió realizar una comparación cuantitativa y directa.

Aspectos Técnicos y de Escalabilidad:

- **Proyección de Costos como Escenario de Referencia:** Los costos de infraestructura y desarrollo estimados corresponden a un escenario de referencia.
- **Estrategia de Persistencia en IPFS:** Para que la evidencia digital permanezca disponible a largo plazo en IPFS, es necesario que al menos un nodo la mantenga "pineada".

Seguridad y Robustez:

- **Ausencia de Pruebas de Seguridad Ofensivas:** El alcance del proyecto no incluyó la realización de auditorías de seguridad formales sobre los contratos inteligentes ni pruebas de penetración sobre la aplicación web.

Justificación

La gestión actual de los fotocomparendos en Bogotá, centralizada en el sistema Fénix, presenta graves limitaciones de seguridad y transparencia que han erosionado la confianza pública en el proceso sancionatorio. Esta se manifiesta en un riesgo sistémico de corrupción, un fenómeno documentado tanto a nivel internacional, como el escándalo de «ticket-fixing» en Nueva York, como a nivel nacional, donde existen redes ilícitas que manipulan y eliminan comparendos en el sistema (**barbaro2011ticketfixing; blogAletta; procuraduriaBucaramanga**).

La raíz de este problema reside en la arquitectura centralizada de las bases de datos tradicionales, que permite a personal interno modificar registros sin dejar un rastro auditable, comprometiendo la integridad de todo el proceso. Esta debilidad se ve agravada por las deficiencias en ciberseguridad identificadas en el *Informe Final de Auditoría AC-SDM-090 de 2023*, que señala controles de acceso insuficientes y falta de monitoreo en los sistemas de la Secretaría de Movilidad (**auditoriaSDM**). Estas falencias no solo incrementan el riesgo de ataques, sino que debilitan la capacidad institucional para defender la legitimidad de las sanciones impuestas. Estas diferencias estructurales entre el modelo centralizado actual y la alternativa descentralizada se resumen en la Tabla 1, evidenciando las ventajas de Blockchain en términos de seguridad, integridad y gobernanza de datos. Con el fin de evidenciar las diferencias estructurales entre el modelo convencional y el prototipo propuesto, en la Tabla 2 se presenta una comparación detallada de sus características:

Frente a este escenario, la tecnología Blockchain, en conjunto con IPFS, ofrece un cambio de paradigma hacia un modelo más seguro y transparente. Como se observa en la comparación, a diferencia de un sistema centralizado donde la confianza recae en una única entidad falible, una solución Blockchain distribuye los datos en una red criptográficamente enlazada. Esto garantiza que cada registro, una vez validado, sea inmutable y verificable por todas las partes autorizadas, haciendo que cualquier intento de alteración sea

Tabla 2

Comparación entre un modelo centralizado y un modelo descentralizado

Característica	Modelo Centralizado	Modelo Descentralizado	Relevancia Contextual
Modelo de Confianza	Basado en la confianza en los administradores del sistema y en la robustez de los controles internos definidos.	Basado en un consenso criptográfico distribuido, donde la confianza reside en el protocolo y no en un intermediario.	Este modelo de confianza depende de la correcta asignación de roles. La auditoría observó que el proceso de implementación se llevó a cabo con la ausencia de un profesional responsable de Seguridad de Información"(página 20-25), lo que subraya la criticidad de los factores de gobernanza en este paradigma.
Integridad de Datos	La integridad se asegura mediante controles de acceso y logs de auditoría internos gestionados por la entidad.	La integridad es una propiedad intrínseca de la estructura de datos; los registros son inmutables por diseño.	La efectividad de los controles internos es fundamental. La auditoría documentó un desafío en esta área, s

computacionalmente inviable y fácilmente detectable. Se elimina así la dependencia de intermediarios y se crea una fuente única y confiable de verdad.

En síntesis, la adopción de este prototipo se justifica por su capacidad para:

- **Mitigar la corrupción**, al garantizar la integridad de los datos y eliminar la posibilidad de manipulación unilateral.
- **Fortalecer la seguridad de la información**, mediante una arquitectura distribuida y tolerante a fallos.
- **Aumentar la confianza ciudadana**, al ofrecer mecanismos transparentes y auditables para la validación de infracciones.
- **Optimizar los procesos administrativos**, automatizando registros, auditorías y la verificación de evidencias.

Esta propuesta no solo responde a desafíos técnicos y éticos urgentes en Bogotá, sino que también se alinea con las tendencias globales en gobernanza digital (*GovTech*), sentando un precedente innovador para la gestión de sanciones públicas con mayor fiabilidad y transparencia.

Marco Teórico

El marco conceptual y tecnologico que sustenta la propuesta del prototipo, presentan las teorías y modelos clave que justifican la selección de Blockchain e IPFS como componentes centrales, evidencian los principios inherentes de integridad, transparencia, resiliencia y auditabilidad en la gestión de evidencia digital crítica como los fotocomparendos.

El Paradigma de la Confianza Descentralizada

Los sistemas de información tradicionales suelen depender de intermediarios centralizados o autoridades certificadoras para validar transacciones y garantizar la fiabilidad de los registros. La teoría de los modelos de confianza descentralizada, en cambio, analiza cómo establecer y mantener la confianza en entornos distribuidos donde tales autoridades centrales están ausentes (**swan2015blockchain**).

La relevancia de este modelo es fundamental para justificar el uso de la tecnología Blockchain en la gestión de fotocomparendos, ya que su propósito es precisamente reemplazar la necesidad de depositar confianza exclusiva en una única entidad para la custodia, validación e integridad de los registros. Blockchain habilita un cambio de paradigma: en lugar de confiar en un actor central, la confianza se distribuye y se deposita en la robustez del protocolo criptográfico subyacente (**nakamoto2008bitcoin**), en la transparencia de las reglas del sistema y en el consenso mayoritario de los participantes de la red (**antonopoulos2023mastering**). Este enfoque reduce drásticamente los puntos únicos de fallo y los vectores de corrupción asociados a la dependencia de intermediarios centralizados, quienes podrían ser comprometidos, cometer errores o actuar de manera malintencionada.

Fundamentos de los Sistemas Distribuidos y Redes Descentralizadas

El paradigma de la confianza descentralizada se sustenta en la teoría de los sistemas distribuidos, donde múltiples entidades autónomas, denominadas nodos, colaboran a través de una red para alcanzar un objetivo común, compartiendo tanto la carga computacional como el almacenamiento de datos (**vanSteen2017**). Estos sistemas se fundamentan en

principios como la distribución de recursos, la comunicación inter-nodo y mecanismos de coordinación que prescinden de intermediarios centrales (**coulouris2011**).

La relevancia de esta teoría para el presente proyecto es primordial, ya que tanto Blockchain como el InterPlanetary File System (IPFS) son implementaciones nativas de sistemas distribuidos. Su adopción conjunta promueve inherentemente:

- **Resiliencia:** Al eliminar puntos únicos de fallo (Single Points of Failure - SPOF).
- **Alta Disponibilidad:** Al permitir el acceso a datos y servicios desde múltiples nodos.
- **Resistencia a la Censura:** Dado que ninguna entidad individual posee control absoluto sobre la red o los datos almacenados (**antonopoulos2023mastering**).

Una característica esencial de estos sistemas es su arquitectura de red **Peer-to-Peer (P2P)**, donde los participantes se conectan y comparten recursos directamente entre sí, sin necesidad de un servidor central. En una red P2P, cada nodo puede actuar simultáneamente como cliente y servidor, lo que posibilita que el registro distribuido (ledger) se mantenga sincronizado y que los archivos puedan ser recuperados desde múltiples fuentes, garantizando la integridad de la información sin depender de una autoridad central.

Tecnologías para la Gestión Descentralizada de Evidencia

Para materializar un sistema de gestión de fotocomparendos descentralizado, se requiere la sinergia de dos tipos de tecnologías: una para el registro inmutable de transacciones y otra para el almacenamiento verificable de la evidencia.

Blockchain: Un Registro Distribuido, Inmutable y Transparente

Blockchain es un tipo específico de Tecnología de Ledger Distribuido (DLT), un sistema de registro digital caracterizado por ser distribuido, sincronizado y asegurado criptográficamente entre múltiples participantes (**narayanan2016bitcoin**). Su estructura fundamental se compone de **transacciones** —operaciones firmadas digitalmente que

modifican el estado del ledger de forma permanente (**antonopoulos2023mastering**)—agrupadas en bloques. Cada bloque contiene un hash criptográfico que lo vincula al anterior, formando una cadena cronológica e inmutable.

La **inmutabilidad** y la **transparencia** son los beneficios centrales que esta tecnología aporta (**swan2015blockchain**; **antonopoulos2023mastering**). La primera se logra mediante la estructura encadenada y los mecanismos de consenso distribuido (ej., Proof-of-Work (**nakamoto2008bitcoin**) o Proof-of-Stake (**king2012ppcoin**)), que hacen que la modificación de un bloque pasado sea computacionalmente prohibitiva. La segunda se habilita por la naturaleza replicada del ledger, permitiendo que actores autorizados puedan consultar y verificar la información de forma independiente. Dentro de este ecosistema, los **Smart Contracts** (Contratos Inteligentes) actúan como programas autoejecutables cuyo código define e impone automáticamente los términos de un proceso, permitiendo automatizar la gestión del ciclo de vida del comparendo (**szabo1997smart**; **wood2014ethereum**; **buterin2014next**).

Modelos Arquitectónicos y Elección para el Prototipo.. La tecnología Blockchain no es monolítica; existen diferentes arquitecturas:

- **Públicas (Permissionless):** Abiertas a cualquier participante, priorizan la descentralización radical (ej. Bitcoin, Ethereum) (**nakamoto2008bitcoin**).
- **Privadas:** Controladas por una única entidad, ofrecen alta eficiencia pero son centralizadas.
- **De Consorcio/Permisionadas (Permissioned):** Operadas por un grupo selecto de participantes autorizados. Ofrecen un equilibrio entre descentralización, rendimiento y confidencialidad, siendo la opción ideal para contextos gubernamentales y empresariales (**vukolic2015quest**; **cachin2018architecture**).

Para este prototipo, se opta por una **implementación permisionada** (simulada con Hyperledger Fabric), permitiendo que solo entidades autorizadas operen nodos y registren

transacciones, con un mecanismo de consenso eficiente (ej. Raft) adecuado para un sistema de gestión de registros.

IPFS: Almacenamiento Verificable mediante Direccionamiento por Contenido

Los ledgers de Blockchain no están optimizados para almacenar grandes volúmenes de datos (blobs), como las imágenes de los fotocomparendos (xu2019taxonomy). Para resolver esto, se utiliza un sistema de almacenamiento descentralizado. La elección de IPFS sobre alternativas centralizadas como AWS S3 es crucial para la integridad del sistema. Mientras que en un sistema centralizado el propietario puede modificar o eliminar unilateralmente un archivo (vogels2008eventually), IPFS opera bajo el paradigma del **direccionamiento por contenido (Content Addressing)** (benet2014ipfs; voigt2017gdpr).

En este modelo, la identidad única de un archivo, su Content Identifier (CID), es un **hash criptográfico** derivado directamente de su contenido. Esto establece un vínculo intrínseco e inmutable: si el contenido del archivo cambia, incluso mínimamente, su CID también cambiará. IPFS es un protocolo y red P2P que utiliza este principio: divide los archivos en bloques, calcula sus hashes y permite su recuperación a través de su CID, utilizando mecanismos como DHT para localizar los nodos que los poseen (maymounkov2002kademlia; benet2014ipfs).

Arquitectura de la Solución: Sinergia Blockchain-IPFS con el Patrón Off-Chain

La integración de ambas tecnologías se materializa mediante el patrón de almacenamiento **off-chain**. El flujo de trabajo es el siguiente:

1. La imagen probatoria del comparendo se carga a un nodo IPFS, obteniendo su CID único.
2. Se crea una transacción en la Blockchain (on-chain) que contiene este CID junto con los metadatos esenciales del comparendo (fecha, hora, lugar, placa).
3. Esta transacción se valida y registra de forma inmutable en el ledger.

Este enfoque crea un enlace criptográfico inalterable entre el registro oficial (en Blockchain) y la evidencia visual original (en IPFS). Cualquier intento de manipulación de la imagen almacenada en IPFS resultaría en un CID diferente, rompiendo explícitamente la cadena de custodia digital y haciendo que la alteración sea detectable de forma inmediata y algorítmica. La combinación de Blockchain e IPFS no solo sigue los principios de descentralización (**vanSteen2017**), sino que refuerza activamente los objetivos de inmutabilidad verificable y transparencia del sistema.

Fundamentos Criptográficos Aplicados

La criptografía proporciona los pilares matemáticos que garantizan la seguridad, integridad y autenticidad en todo el ecosistema del prototipo (**katz2020introduction**).

- **Funciones Hash Criptográficas:** Son algoritmos que transforman datos en una huella digital de tamaño fijo. Sus propiedades (unidireccionalidad, resistencia a colisiones, efecto avalancha) son vitales (**schneier2007applied; menezes1996handbook**). En este proyecto, se utilizan para: generar el CID en IPFS, asegurar la integridad de la cadena de bloques y crear identificadores únicos para las transacciones (**benet2014ipfs; nakamoto2008bitcoin**).
- **Criptografía Asimétrica y Firmas Digitales:** Basada en pares de claves (pública y privada), habilita las firmas digitales (**diffie2022new; rivest1978method**). Cuando un usuario autorizado registra un comparendo, utiliza su clave privada para firmar la transacción. Cualquier participante puede usar la clave pública correspondiente para verificar la firma, garantizando así la **autenticidad** y el **no repudio** de la acción (**katz2020introduction**).

Estado del Arte

Blockchain para Registros Gubernamentales y Gestión de Sanciones

La aplicación de la tecnología Blockchain y DLT (Distributed Ledger Technology) en la administración pública ha sido un área de creciente interés, impulsada por las promesas teóricas de Inmutabilidad, Transparencia y Auditoría mejorada, fundamentales para la Confianza Descentralizada. La investigación sugiere que Blockchain puede transformar la gestión de registros oficiales, como licencias, títulos de propiedad y, potencialmente, multas o sanciones como los fotocomparendos.

Análisis de Aplicación. La capacidad de crear un registro de Transacciones criptográficamente asegurado y distribuido permite generar una pista de auditoría fiable y resistente a la manipulación. Cada registro de sanción, incluyendo sus Metadatos (fecha, hora, ubicación, tipo de infracción) y el Hash de la evidencia asociada, puede ser anclado a la cadena, proporcionando una fuente única de verdad verificable por las partes autorizadas. Esto se alinea con los principios de Sistemas Distribuidos aplicados a la gobernanza.

Blockchains Públicas vs. Permissionadas. En el contexto gubernamental, la literatura y los estudios piloto tienden a favorecer las blockchains permissionadas (o de consorcio). Si bien las blockchains públicas ofrecen máxima transparencia, las permissionadas permiten a las entidades gubernamentales controlar quién puede participar en la red (validar transacciones, acceder a datos), gestionar mejor la privacidad (crucial para datos ciudadanos) y, a menudo, ofrecer mayor rendimiento y escalabilidad. La elección impacta directamente en el modelo de Confianza Descentralizada implementado.

Madurez y Barreras. Aunque existen numerosos estudios y proyectos piloto (ej., registros de tierras en Suecia o Georgia, identidad digital en Estonia), las implementaciones a gran escala para la gestión integral de sanciones administrativas aún son limitadas. La madurez es variable. Las barreras reconocidas incluyen la complejidad técnica, la necesidad de marcos legales y regulatorios adaptados, la interoperabilidad con sistemas heredados, los costos iniciales de implementación y la adopción tanto por parte de las instituciones como

de los ciudadanos. La Percepción Pública de la Tecnología Blockchain también juega un rol significativo.

Integración de Blockchain e IPFS para Datos Voluminosos y Verificables

El almacenamiento directo de datos voluminosos (como imágenes o vídeos de alta resolución) en una Blockchain es ineficiente y costoso. La literatura técnica y diversos prototipos exploran la integración de Blockchain con sistemas de Almacenamiento Direccional por Contenido como IPFS (InterPlanetary File System) para abordar este desafío.

Estado Actual. El enfoque predominante consiste en almacenar el dato voluminoso (la imagen del fotocomparendo) en IPFS, obteniendo un Hash único basado en su contenido. Este Hash IPFS, junto con otros Metadatos relevantes, se almacena en una Transacción Blockchain. Este modelo aprovecha la eficiencia de IPFS para el almacenamiento distribuido y la fortaleza de Blockchain para el registro inmutable y verificable del puntero (el Hash) y los metadatos asociados.

Ventajas y Desafíos. Las ventajas logradas incluyen la verificabilidad (cualquier cambio en el archivo IPFS cambiaría su hash, invalidando el enlace en la Blockchain), la resiliencia potencial (si múltiples nodos almacenan el archivo) y el direccionamiento por contenido inherente a IPFS. Sin embargo, persisten desafíos persistentes significativos:

Persistencia de Datos (Pinning). Los datos en IPFS solo persisten mientras algún nodo los esté "pineando"(almacenando activamente). Garantizar la persistencia a largo plazo de la evidencia requiere mecanismos o servicios de pinning fiables, que pueden tener costos asociados.

Disponibilidad. La recuperación del archivo depende de que los nodos que lo almacenan estén en línea y accesibles.

Costos a Largo Plazo. El almacenamiento distribuido no es necesariamente gratuito, especialmente si se requieren garantías de disponibilidad y persistencia.

Gestión de la Privacidad. Los datos en IPFS son típicamente accesibles públicamente si se conoce el hash. Para evidencia sensible, se requerirían capas adicionales de encriptación antes de la subida a IPFS, añadiendo complejidad.

Gestión de Evidencia Digital y Cadena de Custodia con DLT

La integridad y la cadena de custodia de la evidencia digital son cruciales en procesos sancionatorios. Blockchain/DLT ofrece mecanismos basados en Criptografía Aplicada para fortalecer estos aspectos.

Fortalecimiento de la Integridad y Trazabilidad. Al registrar el Hash de la evidencia digital (imagen del fotocomparendo) en una Transacción Blockchain, se crea un sello de tiempo (timestamping) inmutable y verificable. Cualquier intento posterior de modificar la evidencia original resultaría en un hash diferente, lo que permitiría detectar fácilmente la manipulación. La secuencia de transacciones en la Blockchain proporciona una trazabilidad auditable del ciclo de vida de la evidencia (captura, registro).

Comparación y Valor Añadido. En comparación con los sistemas tradicionales (bases de datos centralizadas, logs de servidor), que pueden ser susceptibles a alteraciones internas o fallos únicos, la DLT aporta un valor añadido significativo al distribuir la confianza y hacer que la manipulación sea computacionalmente inviable (principio de Inmutabilidad). Esto refuerza la Confianza Descentralizada en la validez de la evidencia presentada, reduciendo potenciales disputas.

Estándares Emergentes. En el ámbito de la tecnología blockchain, observamos la consolidación de estándares emergentes en diversas áreas, que representan un consenso práctico y técnico en ausencia de normas formales universalmente ratificadas.

Un área clave es la Seguridad de Smart Contracts. Para construir confianza y fiabilidad en las aplicaciones descentralizadas (dApps) y mitigar vulnerabilidades, se están adoptando ampliamente prácticas que funcionan como estándares de facto:

- **Auditorías y Listas de Chequeo:** Metodologías promovidas por firmas especializadas como ConsenSys Diligence, Trail of Bits y OpenZeppelin se han vuelto

habituales.

- **Patrones de Diseño Seguro:** Se aplican convenciones como Checks-Effects-Interactions y el uso de proxies actualizables (UUPS, Transparent Proxy), aunque estos patrones continúan evolucionando.
- **Estándares de Reporte de Vulnerabilidades:** Propuestas como las EIPs (Ethereum Improvement Proposals) relacionadas con la seguridad ayudan a estandarizar la comunicación de fallos.

Otra área fundamental donde emergen estándares es la Gestión de Evidencia Digital y Cadena de Custodia mediante Blockchain/DLT. Aunque todavía no existe una norma global única (como un estándar ISO específico para esta aplicación), sí se está formando un fuerte consenso técnico sobre los principios tecnológicos clave para asegurar la integridad y fiabilidad:

- **Hashing Criptográfico:** El uso de funciones hash para generar una huella digital única e infalsificable de la evidencia (como el CID en IPFS) es la práctica estándar para garantizar la integridad y detectar manipulaciones (**benet2014ipfs**).
- **Timestamping Inmutable:** Registrar el hash de la evidencia y sus metadatos en una transacción blockchain proporciona una marca de tiempo segura e inalterable, estableciendo una prueba fehaciente del momento del registro (**nakamoto2008bitcoin**).
- **Registro en Ledger Distribuido (DLT):** Utilizar la DLT como el libro contable distribuido para estos registros es el mecanismo reconocido para lograr inmutabilidad, transparencia controlada y auditabilidad (**swan2015blockchain**), superando las limitaciones de las bases de datos centralizadas.

Implementaciones reales de Blockchain en Gobiernos

Registro de propiedad en Suecia

La autoridad catastral sueca *Lantmäteriet* realizó entre 2016 y 2017 un piloto con una cadena permissionada y contratos inteligentes para registrar transacciones inmobiliarias. El proyecto buscó reducir la manipulación documental y agilizar los trámites que involucran a bancos, agentes inmobiliarios y entidades estatales. Los resultados mostraron que el tiempo de compraventa podría reducirse de 4–7 meses a tan solo unos días, con un ahorro estimado de ~100 millones de euros anuales gracias a la eliminación de procesos en papel y la automatización parcial ([lantmateriet2017](#); [lantmateriet__cointelegraph2017](#); [lantmateriet__cointelegraph2__2017](#)).

Durante la segunda fase se incorporaron contratos inteligentes que ejecutaban automáticamente pasos como la firma digital de documentos y el registro de hipotecas cuando se cumplían condiciones predefinidas, demostrando la viabilidad técnica y la interoperabilidad entre actores.

Integridad de registros clínicos en Estonia

Desde 2016 la autoridad nacional de salud de Estonia, en colaboración con Guardtime, emplea la infraestructura KSI (*Keyless Signature Infrastructure*) para asegurar la integridad de los expedientes médicos de más de un millón de ciudadanos. En lugar de almacenar datos sensibles en la cadena, el sistema registra huellas *hash* de cada operación sobre la historia clínica, posibilitando auditorías en tiempo real y la detección inmediata de accesos o modificaciones no autorizadas ([guardtime2016](#); [reddit__estonia__blockchain](#)). Esta aproximación cumple los requisitos de privacidad y refuerza la confianza pública en el manejo de datos sanitarios.

Síntesis y relevancia para el proyecto

Estos casos evidencian que:

- La tecnología blockchain coordina procesos complejos con múltiples partes

interesadas, garantizando un registro único y verificable (ejemplo de Suecia).

- Permite verificar de forma irrefutable la integridad de datos sensibles sin exponer su contenido, manteniendo el cumplimiento normativo (ejemplo de Estonia).

Las lecciones aprendidas refuerzan la pertinencia de aplicar una arquitectura basada en Blockchain e IPFS para gestionar evidencias de fotocomparendos en Bogotá, buscando niveles de transparencia, inmutabilidad y confianza comparables.

Funcionamiento de los Fotocomparendos en Bogotá: Mecanismos, Regulación e Impacto

El sistema de fotocomparendos en Bogotá (FENIX) representa un modelo tecnológico y regulatorio diseñado para mejorar la seguridad vial mediante la detección automatizada de infracciones de tránsito (**mintransporte2023**). Basado en cámaras de fotodetección ubicadas en zonas autorizadas por el Ministerio de Transporte, este sistema combina vigilancia electrónica, validación humana y marcos legales específicos para sancionar conductas de riesgo (**supertransporte2021**). Desde su implementación, ha logrado reducir siniestros en puntos críticos, aunque enfrenta desafíos técnicos y jurídicos. A continuación, se detalla su operación, criterios de aplicación y marco legal que lo regula (**mintransporte2023**).

Marco Legal y Regulatorio. La implementación de fotocomparendos en Bogotá se sustenta en la Ley 1843 de 2017 (**ley1843**) y su reglamentación mediante resoluciones como la Resolución 20203040011245 (**resolucion11245**). Estos instrumentos establecen cuatro criterios para instalar cámaras:

1. **Siniestralidad:** Ubicación en zonas con alto índice de accidentes.
2. **Prevención:** Disuasión de conductas peligrosas.
3. **Movilidad:** Optimización del flujo vehicular.
4. **Historial de infracciones:** Enfoque en corredores con recurrentes violaciones.

Adicionalmente, las autoridades deben garantizar la visibilidad de los dispositivos, señalizando su presencia al menos 500 metros antes de su ubicación (**ley1843**), y cumplir con planes de seguridad vial alineados con políticas distritales. La Secretaría Distrital de Movilidad (SDM) ha enfrentado cuestionamientos legales, como los señalados por la Personería en 2018 (**sdm__camaras2023**).

Proceso Operativo de los Fotocomparendos .

Detección y Captura de Infracciones . Las cámaras de fotodetección en Bogotá se clasifican en dos tipos (**supertransporte2021; mintransporte2023**):

- **Automáticas:** Monitorean velocidades, semáforos en rojo y restricciones como pico y placa.
- **Semiautomáticas:** Vigilan bloqueos de calzadas, paradas prohibidas y recolección irregular de pasajeros.

Estos dispositivos, instalados en corredores de alta accidentalidad como la Avenida NQS o la Calle 100, capturan imágenes o videos que incluyen matrícula, fecha, hora y ubicación GPS¹⁴. Por ejemplo, en 2025, un conductor que exceda el límite de 50 km/h en la Avenida Boyacá será registrado por cámaras previamente señalizadas.

Validación y Notificación . Una vez detectada una presunta infracción, las pruebas se envían a un centro de análisis de la SDM, donde agentes de tránsito verifican:

- Legibilidad de la matrícula.
- Contexto de la violación (ejemplo: si un semáforo en rojo fue respetado).
- Datos del vehículo en el RUNT (Registro Único Nacional de Tránsito).

Tras validar la infracción, se genera un comparendo electrónico notificado al propietario del vehículo mediante correo certificado o plataformas digitales. El plazo máximo para emitir la sanción es de 10 días hábiles desde la detección, seguido de 3 días para su notificación. Si

el domicilio registrado está desactualizado, el infractor podría no recibir la notificación, lo que no exime el pago (**ley1843**).

Tecnología y Transparencia . El sistema combina:

- **Cámaras de última generación:** Equipadas con sensores de velocidad Lidar y visión nocturna.
- **Plataforma de análisis IA:** Algoritmos que descartan falsos positivos (ejemplo: ambulancias en emergencia).
- **Integración con RUNT:** Verificación instantánea de documentos como SOAT o tarjeta de operación.

Los datos se almacenan en servidores con cifrado AES-256, accesibles solo para funcionarios autorizados mediante autenticación biométrica.

Problemas Operativos .

- **Notificaciones fallidas:** Errores en direcciones del RUNT causan sanciones no recibidas, acumulando intereses moratorios.
- **Latencia en validaciones:** En horas pico, el volumen de infracciones puede retrasar procesamientos hasta 72 horas.

Cuestionamientos Legales . En 2018, la Personería de Bogotá identificó que el 15 % de las cámaras operaban sin autorización ministerial durante un periodo de transición legal. La SDM rectificó esta situación en 2019, regularizando todos los dispositivos bajo la Resolución 20203040011245 de 2020 (**secretaria__movilidad2023**).

Aplicaciones Específicas en Gestión de Tráfico e Infracciones

Al revisar las Aplicaciones de Blockchain en la Gestión de Tráfico, Infracciones y Fotocomparendos, como se observa en la Tabla 3, se observa que, si bien hay discusiones teóricas (**yousfi2022its**), propuestas conceptuales (**chen2024blockchain**) y hasta una

joven PYME española, las implementaciones prácticas que integren el flujo completo descrito en el prototipo (captura -> IPFS -> Blockchain -> Verificación -> Pago Automatizado con Billetera Digital) son escasas y se encuentran en fase de propuesta o son parciales (**omar2024srtm**; **choquevilca2024blockchain**).

Análisis de Existencia. La literatura existente se centra más en componentes aislados (**yousfi2022its**), uso de blockchain para registros vehiculares (**mani2023smart**), seguros (**dutta2023solution**), o gestión genérica de multas (**omar2024srtm**), pero raramente combinando el almacenamiento de evidencia en IPFS con la automatización del pago vía billetera digital específicamente para fotocomparendos.

Arquitecturas y Resultados. Dada la escasez de implementaciones completas reportadas (**AnandSingh_ProjectReport_Year**; **juit2024traffic**), es difícil generalizar sobre arquitecturas dominantes o resultados concretos para este caso de uso tan específico. Los estudios existentes a menudo se limitan a explorar la viabilidad teórica o a implementar módulos parciales (**choquevilca2024blockchain**).

Lecciones Aprendidas:. La principal lección aprendida de áreas adyacentes es la importancia de abordar no solo los desafíos técnicos (Zheng et al., 2018) sino también los regulatorios, de gobernanza y de adopción (Tan et al., 2022). La ausencia de soluciones integrales reportadas para el flujo completo de gestión de fotocomparendos representa una brecha significativa en la aplicación práctica de estas tecnologías combinadas.

El análisis del estado del arte revela avances significativos, pero también limitaciones claras:

Avances Significativos

La tecnología Blockchain ha demostrado su potencial para crear registros gubernamentales más inmutables, transparentes y auditables. (Balcerzak et al., 2022; Meroni et al., 2023)

La integración Blockchain + IPFS es una solución técnicamente viable y reconocida para gestionar datos voluminosos referenciados desde una cadena de bloques, mejorando la verificabilidad (Adel et al., 2023; Mishra et al., 2024).

DLT ofrece mejoras sustanciales para la integridad y trazabilidad de la evidencia digital

Tabla 3

Análisis Comparativo del Estado del Arte en Gestión de Infracciones con Blockchain

Trabajo/Proyecto	Ámbito	Tecnologías	Limitaciones Identificadas	Aporte Relevante para el Prototipo
Yousfi et al. (2022)	Gestión de tráfico urbano	Blockchain pública, Smart Contracts	Alto costo de transacciones (gas), privacidad limitada para datos personales	Modelo conceptual de integración blockchain-tráfico, solución a la transparencia y trazabilidad
Chen et al. (2024)	Sistema de multas electrónicas	Base de datos centralizada + Blockchain	Falta de inmutabilidad completa, dependencia del servidor central	Propuesta de registrar hash de actas en blockchain para mayor integridad y transparencia
Joseph (2023)	Registros vehiculares gubernamentales	Hyperledger Fabric, IPFS	Complejidad para escalar, gestión de identidades	Arquitectura permitida para manejo seguro de datos sensibles
Dutta et al. (2023)	Seguros automotrices	Ethereum, Smart Contracts	Latencia en transacciones, costos operativos	Automatización de procesos mediante contratos inteligentes
Omar et al. (2024)	Gestión de infracciones de tránsito	Blockchain híbrida, base de datos	Integración parcial, falta de flujo completo	Aproximación hacia una gestión descentralizada

(Thanasas et al., 2025).

Existen mecanismos (billeteras digitales, smart contracts, stablecoins) para habilitar pagos digitales automatizados en ecosistemas blockchain (**antonopoulos2023mastering**).

Limitaciones Identificadas

Madurez e Integración:. Muchas aplicaciones gubernamentales de Blockchain son pilotos aislados (Zheng et al., 2018; Li et al., 2021). Falta integración entre sistemas y con procesos completos.

Desafíos Técnicos: . La persistencia y gestión a largo plazo de datos en IPFS (pinning), la escalabilidad de algunas blockchains y la seguridad/fiabilidad de los oráculos para Smart Contracts siguen siendo áreas de desarrollo activo (Zheng et al., 2018).

Adopción y Regulación:. La adopción de billeteras digitales para pagos gubernamentales, el uso de criptoactivos/stablecoins y la claridad legal sobre smart contracts en el sector público son obstáculos importantes (Tan et al., 2022).

Política de Reserva de Información:. Bogotá mantiene una política de reserva de información que restringe la divulgación completa de los datos almacenados en su base de datos. Esta política limita el acceso y la difusión de ciertos datos, lo que puede afectar la transparencia y la capacidad de realizar un análisis exhaustivo (**choquevilca2024blockchain**).

Actualización de Datos:. La actualización de los datos almacenados en la base de datos es un proceso que requiere tiempo. Dada la naturaleza progresiva de este proceso, que depende de la cantidad de datos que se agregan diariamente, la actualización completa de los datos con el sistema que se desarrollará puede llevar un tiempo considerable (**choquevilca2024blockchain**).

Aplicación Específica:. Existe una notable ausencia de soluciones documentadas que implementen el flujo completo e integrado (captura de imagen -> subida a IPFS -> registro en Blockchain -> verificación vía app -> pago automático desde billetera digital) específicamente para la gestión de fotocomparendos. (**yousfi2022its**;

chen2024blockchain)

Verificación Participativa:. Los sistemas actuales raramente permiten que el ciudadano verifique independientemente la autenticidad e integridad de la evidencia presentada contra ellos, limitando los beneficios de transparencia inherentes a blockchain.

Adopción en Bogotá:. La literatura muestra una escasez notable de implementaciones o estudios piloto en contextos latinoamericanos, donde factores como confianza institucional, infraestructura tecnológica y marcos regulatorios presentan desafíos particulares.

(choquevilca2024blockchain; rezabala2025blockchain)

Novedad y Relevancia del Prototipo

La(s) brecha(s) específica(s) que este prototipo busca abordar es precisamente la falta de una solución integrada y de extremo a extremo para la gestión de fotocomparendos utilizando la sinergia de Blockchain, IPFS y pagos automatizados, como se evidencia en la revisión de la literatura existente (**yousfi2022its; AnandSingh_ProjectReport_Year**)

La novedad principal radica en la integración holística de todo el flujo propuesto. Mientras que los componentes individuales han sido explorados por separado (Adel et al., 2023; Mishra et al., 2024) o en otros contextos (Mani Joseph P, 2023; Dutta et al., 2023), este prototipo propone conectarlos en una secuencia lógica y automatizada para este caso de uso particular.

Aborda la brecha de aplicación específica, llevando los conceptos teóricos (**swan2015blockchain; antonopoulos2023mastering**) y las soluciones parciales existentes (**choquevilca2024blockchain**) a un dominio concreto (fotocomparendos en Bogotá) con un proceso completo.

La relevancia del prototipo se justifica por su potencial para:

Mejorar la transparencia y confianza en el proceso de fotocomparendos, evidencia verificable e inmutable (Meroni et al., 2023; Thanasas et al., 2025).

Aumentar la eficiencia operativa mediante la automatización del registro, verificación y pago.

Reducir disputas y costos asociados a la gestión manual y a la falta de confianza en la evidencia.

Explorar un modelo innovador de pago automatizado condicional basado en la verificación en Blockchain.

Análisis de tendencia internacional

Producción Científica por Países (Mapa y Gráfico de Líneas) . Descripción

General: Esta gráfica se compone de dos partes. La primera es un mapa mundial que utiliza una escala de color para representar la cantidad de producción científica por país. Las tonalidades más oscuras generalmente indican una mayor producción. La segunda parte es un gráfico de líneas que muestra la evolución de la producción científica (en artículos) a lo largo de los años para un conjunto específico de países.

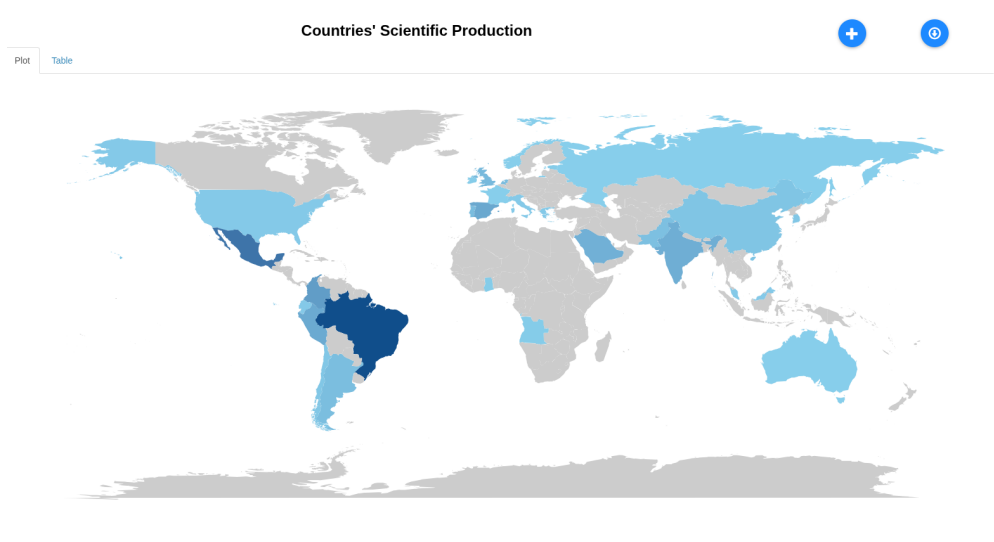
Mapa Mundial:. El mapa muestra la distribución global de la producción científica en el área de estudio. Se observa una concentración significativa de publicaciones en países como Brasil, lo que sugiere un interés y actividad investigadora importante en Latinoamérica. Otros países con una producción notable incluyen México y España. Es importante notar que algunas regiones muestran una menor actividad, lo que podría indicar diferencias en el enfoque de investigación, financiamiento o acceso a recursos.

Nube de Palabras. La Figura 4 muestra los términos más frecuentes en la literatura analizada. Destacan conceptos como *blockchain*, *challenges*, *management* y *secure*, lo que refleja el énfasis de la comunidad académica en los retos de seguridad y gestión al aplicar tecnologías DLT en contextos gubernamentales.

Mapa Temático. El mapa temático representa la distribución de los principales temas de investigación en el área, organizados según su grado de desarrollo (densidad) y relevancia (centralidad). En el cuadrante superior derecho se ubican los "temas motores", como *challenges*, *framework*, *model*", que son altamente desarrollados y centrales en la literatura. En el cuadrante inferior derecho, los "temas básicos" como *management*, *secure*, *networks*, *internet*, *architecture*, *things*"son fundamentales pero menos desarrollados. El cuadrante

Figura 2

Distribución global de la producción científica sobre blockchain y gestión de infracciones



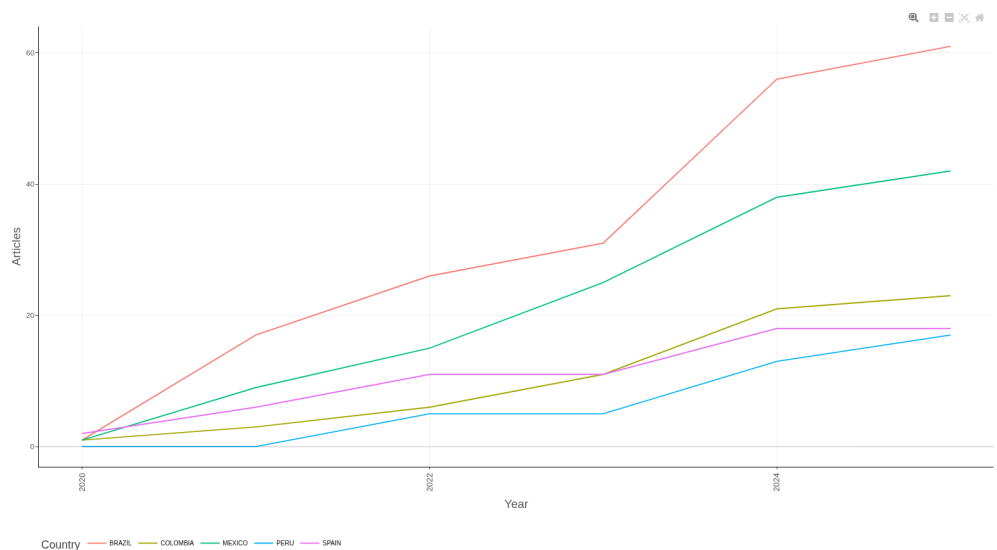
Nota. Elaboración propia con datos bibliométricos.

superior izquierdo agrupa "temas nicho" como "system, encryption, iot", "design, impact, traceability", que presentan alta especialización pero menor centralidad.

Finalmente, en el cuadrante inferior izquierdo se encuentran los "temas emergentes o en declive", como "blockchain", "optimization, technology", que muestran baja densidad y centralidad, indicando áreas de reciente aparición o menor desarrollo. Esta visualización permite identificar las tendencias, vacíos y oportunidades de investigación en el campo.

Figura 3

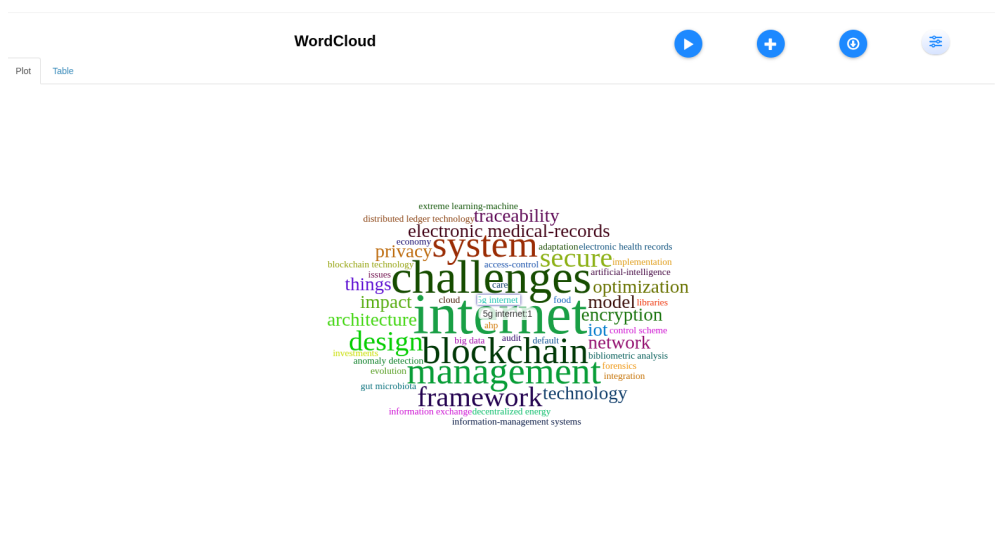
Evolución anual de publicaciones en los países líderes del tema (Brasil, México, Colombia, España y Perú)



Nota. Elaboración propia con datos bibliométricos.

Figura 4

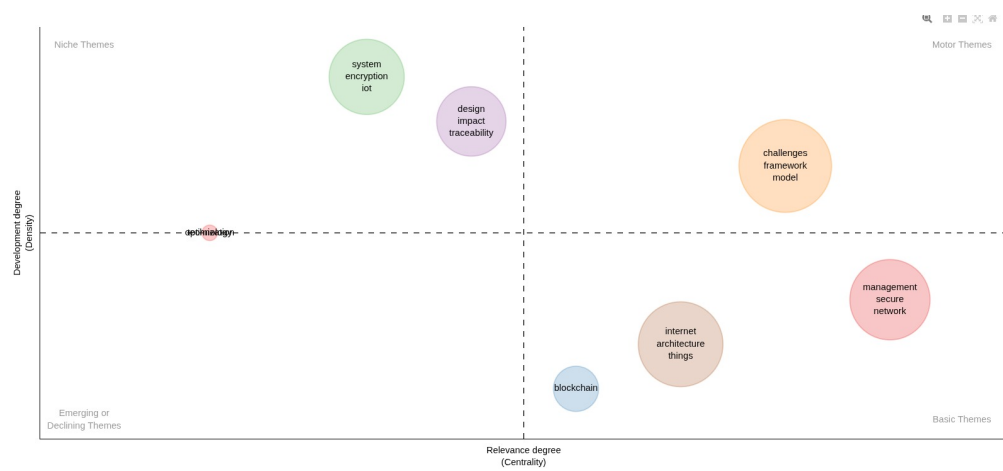
Nube de palabras de los términos más recurrentes en la literatura sobre blockchain e infracciones



Nota. Elaboración propia con datos bibliométricos.

Figura 5

Mapa temático de los principales temas de investigación en el área



Nota. Elaboración propia con datos bibliométricos.

Alcance

Enfoque y delimitación geográfica

Este trabajo se circunscribe al proceso de generación, gestión y verificación de **multas de tránsito automatizadas (fotomultas)** emitidas por la Secretaría Distrital de Movilidad de Bogotá. Se excluyen deliberadamente:

- Multas impuestas de forma presencial por agentes de tránsito.
- Procesos sancionatorios de otras ciudades o entidades territoriales.
- Funcionalidades de recaudo y pasarelas de pago (solo se registra el estado del pago, no se procesa el pago en sí).

Componentes del prototipo

El prototipo aborda los siguientes módulos funcionales:

1. **Registro inmutable de la infracción** Captura de metadatos (placa, fecha, hora, ubicación y tipo de infracción) y publicación del identificador de la evidencia en la *blockchain* (Hyperledger Fabric).
2. **Almacenamiento descentralizado de evidencias** Carga de la imagen o video de la fotomulta en IPFS y obtención de su *hash*.
3. **Verificación pública** Servicio de consulta que permite contrastar el hash guardado en la cadena con el archivo almacenado en IPFS.
4. **Gestión del ciclo de vida de la multa** Estados: Generada → Notificada → En apelación → Pagada → Cerrada. Cada transición queda registrada mediante eventos de contrato inteligente.
5. **Interfaz mínima** Panel Web para: (i) agentes que registran la infracción y (ii) ciudadanos que consultan la autenticidad y el estado de su fotomulta.

Fuera del alcance

- Integración completa con sistemas legados del RUNT o SIMIT; se simula mediante datos de prueba.
- Implementación de un modelo económico (tarifas de gas, costos operativos reales).
- Implementación de algoritmos de detección automática de infracciones (visión por computador). Se parte de que la cámara ya detectó la infracción y generó la evidencia.

Entregables

- Contrato inteligente en Solidity (o «chaincode» en Go, según la red seleccionada) con pruebas unitarias.
- Script de despliegue de red Hyperledger Fabric e instalación de IPFS local.
- Aplicación Web de demostración (*frontend* ligero) conectada a los servicios anteriores.
- Manual técnico que documenta la arquitectura y el flujo de datos.
- Informe de resultados de las pruebas funcionales y de rendimiento básico.

Criterios de éxito

1. Tiempo medio de publicación de una infracción ≤ 3 s en entorno de laboratorio.
2. Coincidencia 100 % entre el hash almacenado en la cadena y la evidencia recuperada desde IPFS.
3. Trazabilidad completa del historial de estados para al menos 50 multas de prueba.
4. Ausencia de fallos críticos en pruebas de carga con 10 transacciones concurrentes.

Limitaciones del Prototipo

Es fundamental reconocer que, como prototipo desarrollado en un contexto académico, el presente estudio presenta ciertas limitaciones que definen el alcance de sus conclusiones y delinean claras oportunidades para futuras investigaciones. Las principales limitaciones son:

1. Entorno de Validación

- **Validación en Entorno de Laboratorio:** El prototipo fue diseñado, desplegado y evaluado en un entorno de simulación controlado. No se sometió a pruebas en una infraestructura productiva real con la carga de transacciones y el volumen de usuarios que gestiona actualmente la Secretaría de Movilidad. Por lo tanto, su rendimiento, estabilidad y escalabilidad bajo condiciones de estrés real aún no han sido cuantificados.
- **Uso de Datos Simulados:** Debido a estrictas normativas de privacidad y protección de datos personales que impiden el acceso a información real de ciudadanos y vehículos, todas las pruebas se realizaron con datos sintéticos. Esto implica que el prototipo no fue expuesto a la variabilidad, inconsistencias y casos atípicos que caracterizan a los datos del mundo real, lo cual podría influir en la lógica de negocio y en el manejo de errores en un entorno de producción.
- **Suposiciones sobre la Calidad de la Evidencia:** El sistema asume que las evidencias fotográficas (imágenes de fotocomparendos) son capturadas con una calidad suficiente para su procesamiento. No se implementaron ni probaron mecanismos para manejar escenarios con imágenes de baja resolución, borrosas o con obstrucciones, que son comunes en la operación real.

2. Integración y Comparación con Sistemas Existentes

- **Integración Simulada con Sistemas Externos:** La interacción con plataformas gubernamentales clave como el RUNT y el SIMIT fue simulada a través de APIs de prueba (mocks). No se abordaron los desafíos técnicos y burocráticos de una integración real, como los protocolos de comunicación, los tiempos de respuesta, la disponibilidad de los servicios y los posibles cuellos de botella.
- **Ausencia de Benchmarking Directo con el Sistema Actual (Fénix):** La

falta de acceso al código fuente y a la arquitectura interna del sistema Fénix impidió realizar una comparación cuantitativa y directa en términos de rendimiento, costos operativos o eficiencia de procesos. El análisis comparativo se basó en las características conceptuales de ambas arquitecturas (centralizada vs. descentralizada).

3. Aspectos Técnicos y de Escalabilidad

- **Proyección de Costos como Escenario de Referencia:** Los costos de infraestructura y desarrollo estimados corresponden a un escenario de referencia. Los costos reales en un despliegue a gran escala podrían variar considerablemente dependiendo de factores como el número de nodos en la red, el volumen de almacenamiento en IPFS, el tráfico de red y la estrategia de persistencia de datos (pinning) que se adopte.
- **Estrategia de Persistencia en IPFS:** Para que la evidencia digital permanezca disponible a largo plazo en IPFS, es necesario que al menos un nodo la mantenga “pineada”. El prototipo no implementa una política de pinning distribuida y resiliente, lo cual sería un requisito crítico para garantizar la cadena de custodia digital en un sistema de producción.

4. Seguridad y Robustez

- **Ausencia de Pruebas de Seguridad Ofensivas:** El alcance del proyecto no incluyó la realización de auditorías de seguridad formales sobre los contratos inteligentes (chaincode) ni pruebas de penetración (pentesting) sobre la aplicación web. Aunque se siguieron buenas prácticas de desarrollo, no se ha verificado formalmente la resistencia del sistema ante ataques maliciosos especializados.

Metodología

La metodología de este proyecto se divide en dos componentes principales: la metodología de investigación y la metodología de desarrollo de software.

Metodología de investigación

La investigación se clasifica de la siguiente manera:

- En función de su aplicación práctica, corresponde a una investigación aplicada, pues se orienta a resolver la falta de seguridad que existe en la gestión de infracciones de tránsito en la ciudad de Bogotá. De acuerdo con (coulouris2011), la investigación aplicada o técnica se centra en ofrecer soluciones concretas o generar innovaciones y mejoras en procesos o productos.
- Por su propósito, el estudio es de tipo descriptivo, ya que pretende identificar y detallar las características más relevantes de la implementación de un servicio web basado en Blockchain, con el objetivo de reforzar la seguridad en la gestión de las infracciones de tránsito en dicha municipalidad. Como señala (vanSteen2017), los estudios descriptivos buscan especificar las propiedades, características y aspectos significativos del fenómeno que se analiza.

Metodología de desarrollo de software: Enfoque por Prototipos

Para el desarrollo de este proyecto, se adoptará la Metodología de Desarrollo por Prototipos. Esta elección se fundamenta en la naturaleza innovadora del proyecto, que combina tecnologías emergentes como Blockchain e IPFS en un dominio específico (gestión de fotocomparendos), donde los requisitos exactos y los desafíos técnicos pueden no ser completamente evidentes desde el inicio. La metodología por prototipos es inherentemente iterativa y se centra en la construcción rápida de versiones funcionales (prototipos) del sistema, permitiendo la validación temprana de conceptos, la recopilación de retroalimentación continua y la adaptación flexible a los descubrimientos realizados durante el desarrollo.

Introducción a los artefactos técnicos del diseño

Con el fin de estructurar de manera clara el desarrollo de la solución propuesta, en esta sección se presentan los principales artefactos utilizados durante la etapa de diseño. Estos elementos permiten representar gráficamente tanto la lógica de funcionamiento como la arquitectura del sistema, sirviendo como guía para la implementación y posterior validación del prototipo.

El conjunto de diagramas que se incluye responde a la necesidad de modelar distintos aspectos del sistema. Por un lado, se usan diagramas de casos de uso para identificar las funcionalidades clave desde la perspectiva del usuario. Por otro, los diagramas de clases permiten definir la estructura del software, mientras que los diagramas de despliegue muestran cómo se distribuyen los componentes en el entorno tecnológico. Además, se incluyen diagramas de flujo que describen el comportamiento del sistema ante eventos específicos, facilitando la comprensión de su dinámica interna.

Cada uno de estos artefactos está alineado con los objetivos del proyecto y fue elaborado considerando tanto las necesidades funcionales como las características propias de las tecnologías involucradas, en particular el uso de Blockchain e IPFS. De esta forma, se busca garantizar coherencia técnica en el diseño y establecer una base sólida para el desarrollo e implementación de la solución.

Diseño del Prototipo

Se hace mención de que, aunque la documentación para elaborar el software está en español, es un estándar escribir código en inglés y, por tanto, para mantener la coherencia, los diagramas mostrados a continuación usarán este idioma para los nombres de las variables, funciones y clases.

Definición de Requisitos:

1. **Datos sobre infracciones de tráfico:** La captura de datos detallados sobre infracciones de tráfico, como la hora de la infracción, las coordenadas GPS, el tipo de infracción, los datos de identificación del vehículo e imágenes o vídeos, garantiza que cada incidente se documenta exhaustivamente. Este registro exhaustivo proporciona transparencia y responsabilidad, ya que los datos son inmutables y a prueba de manipulaciones una vez almacenados en la cadena de bloques. La inclusión de pruebas mediáticas refuerza aún más la credibilidad y verificabilidad de cada infracción, haciendo que los registros sean sólidos a efectos legales y administrativos.
2. **Información sobre el conductor:** Asociar las infracciones de tráfico a conductores concretos utilizando su dirección Ethereum (clave pública), los datos KYC si es necesario, y los números de identificación del conductor permite un seguimiento y una rendición de cuentas precisos. Esta vinculación permite al sistema personalizar el seguimiento y la verificación de las sanciones, garantizando que las sanciones se atribuyan correctamente a las personas adecuadas. El uso de datos KYC garantiza que las identidades de los conductores puedan verificarse de forma fiable, lo que resulta esencial para mantener la integridad y fiabilidad del sistema.
3. **Datos de la sanción:** Registrando los datos de la sanción, incluyendo el tipo de sanción, el importe de la sanción y el estado del pago de la sanción facilita la ejecución automatizada de las sanciones a través de contratos inteligentes. Esta automatización reduce la carga administrativa de y garantiza que las sanciones se

apliquen de forma coherente y transparente. El registro inmutable de las sanciones y su estado de pago en la blockchain garantiza que el proceso sea justo y responsable, proporcionando una pista de auditoría clara para todas las transacciones financieras relacionadas con las infracciones de tráfico.

4. **Eventos de contratos inteligentes:** El registro de eventos de contratos inteligentes, como el registro de nuevas infracciones de tráfico o la ejecución de sanciones, con datos relevantes y marcas de tiempo, garantiza que todas las acciones significativas se documenten de forma transparente. Este registro de eventos mejora la trazabilidad y la rendición de cuentas, proporcionando un registro cronológico de las actividades importantes del sistema. Esta transparencia es crucial para las auditorías y revisiones, ya que ayuda a generar confianza en las operaciones del sistema.
5. **Datos de las transacciones de la cadena de bloques:** El seguimiento de los datos de las transacciones de la cadena de bloques, incluido el hash de la transacción, las direcciones del remitente/receptor y las tarifas del gas, proporciona un registro detallado de todas las interacciones dentro del sistema. Estos datos permiten supervisar y auditar las transacciones, garantizando la transparencia y la trazabilidad. Además, hacer un seguimiento de las tarifas de gas ayuda a gestionar y optimizar los costes asociados a la ejecución de transacciones en la blockchain, que es importante para mantener la rentabilidad del sistema.
6. **Dispositivos de datos IoT:** La integración de datos de dispositivos IoT, como sensores o cámaras, junto con marcas de tiempo e identificación del dispositivo, puede mejorar las pruebas recopiladas para infracciones de tráfico. Estos datos en tiempo real proporcionan contexto adicional y pruebas corroborativas, haciendo que los registros de infracciones sean más sólidos y fiables. El uso de dispositivos IoT también puede automatizar la detección y el registro de infracciones, aumentando la eficiencia y la precisión del sistema.

7. **Opiniones de los usuarios:** La recopilación de opiniones de los usuarios, incluidos el tipo de opinión, los comentarios y las valoraciones de los usuarios, ayuda a los administradores del sistema a comprender las experiencias y percepciones de los usuarios. Esta información es valiosa para identificar áreas de mejora en y mejorar la usabilidad y funcionalidad del sistema. Involucrar a los usuarios de esta manera puede conducir a un diseño del sistema más centrado en el usuario, mejorando la satisfacción y la eficacia general.
8. **Datos de cumplimiento:** El registro de los datos de cumplimiento, incluido el estado de cumplimiento y los detalles normativos, garantiza que el sistema se adhiere a las leyes y normativas de tráfico locales. Este seguimiento es vital para demostrar el cumplimiento de la normativa y evitar problemas legales. El mantenimiento de registros de cumplimiento detallados también facilita las auditorías reglamentarias en, proporcionando pruebas transparentes de que el sistema funciona dentro de las normas legales, lo que es esencial para generar confianza y credibilidad entre las partes interesadas.

Diagrama de casos de uso del sistema de gestión de infracciones de tránsito

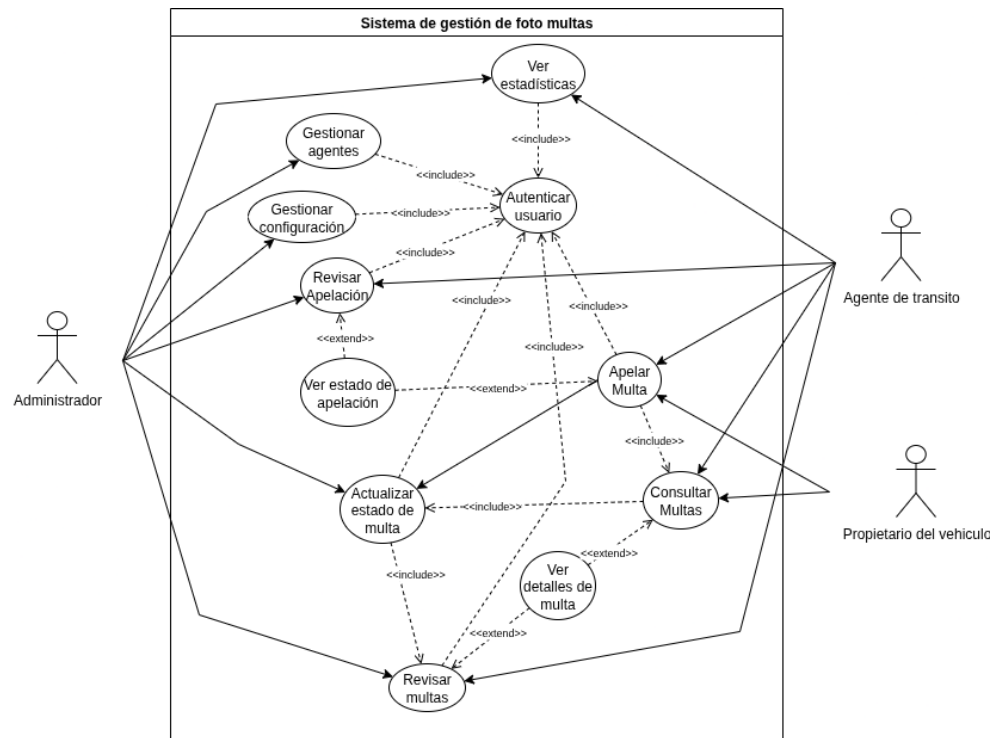
Diagrama de Despliegue

En la Figura 7 se puede observar el diagrama de despliegue propuesto, donde cada nodo cuenta con la misma información, ya que esta se encontrará sincronizada. Asimismo, se conecta mediante servicios web a la base de datos de Apitude como herramienta de terceros para acceder a la información existente en el Registro Único Nacional de Tránsito (RUNT), de donde se obtendrán los datos de conductores, vehículos y el registro de infractores en Bogotá, así como el estado de las multas.

Hay que mencionar que existen dos soluciones para traer la información necesaria de estas entidades: la primera es una API llamada Apitude, de un tercero que provee la información del RUNT y del SIMIT; la segunda consiste en utilizar los datos que estas entidades

Figura 6

Diagrama de casos de uso del sistema de gestión de infracciones de tránsito



Nota. Elaboración propia.

públicas ya poseen en bases de datos tradicionales.

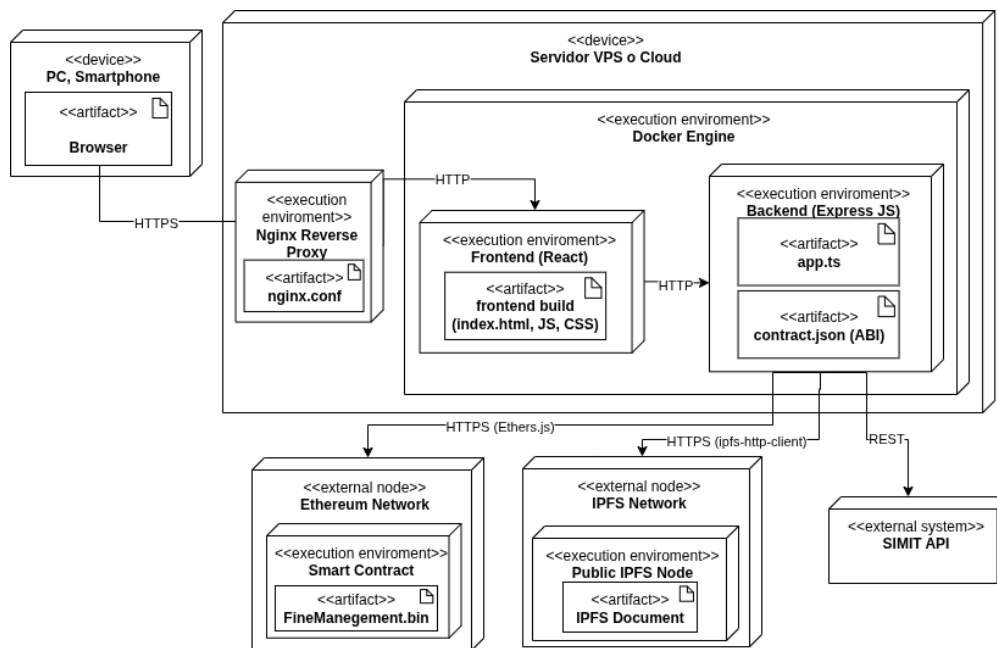
Diagrama de clases

Hay que considerar que se manejarán dos capas de lógica: la primera enfocada en registrar los cambios en los estados de las multas a través de blockchain y la segunda capa encargada de la administración general de las multas (manipular los datos que no son visibles al público). En la Figura 8 se hace un esquema de la primera capa lógica que se encarga de la administración general de las multas y los datos que maneja

En la Figura 9 se hace mención en la segunda capa lógica la cual son los cambios generados

Figura 7

Diagrama de despliegue de la arquitectura del sistema



Nota. Elaboración propia.

en el registro de multas que registramos en la blockchain, que se traducen en los contratos realizados en solidity.

Diagrama de actividades

Interfaz de Usuario

Compartidas. En la Figura 11 se aprecia la pantalla de inicio de sesión, punto de entrada para todos los usuarios autorizados del sistema.

La Figura 12 muestra el formulario para recuperar la contraseña, reforzando la experiencia de autoservicio y seguridad de la plataforma.

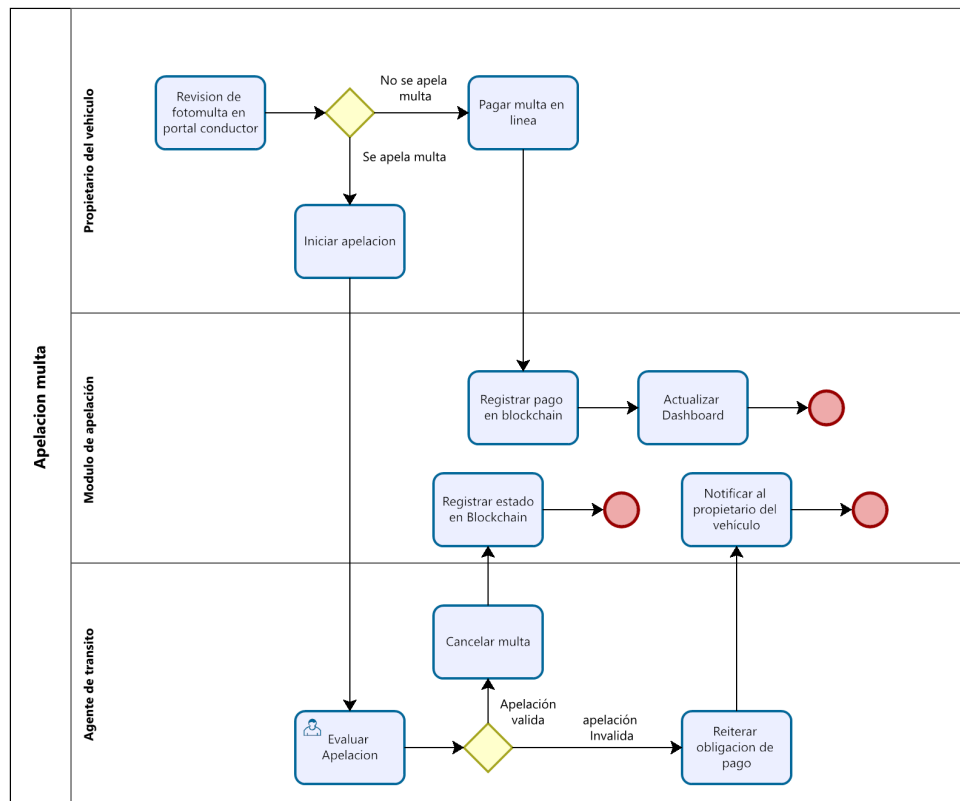
Vista Agente. En la Figura 13 se presenta el tablero principal que resume las métricas de gestión de multas para el agente de tránsito. La Figura 14 ilustra la consulta rápida del

Diagrama de clases del sistema de gestión de multas



Figura 9

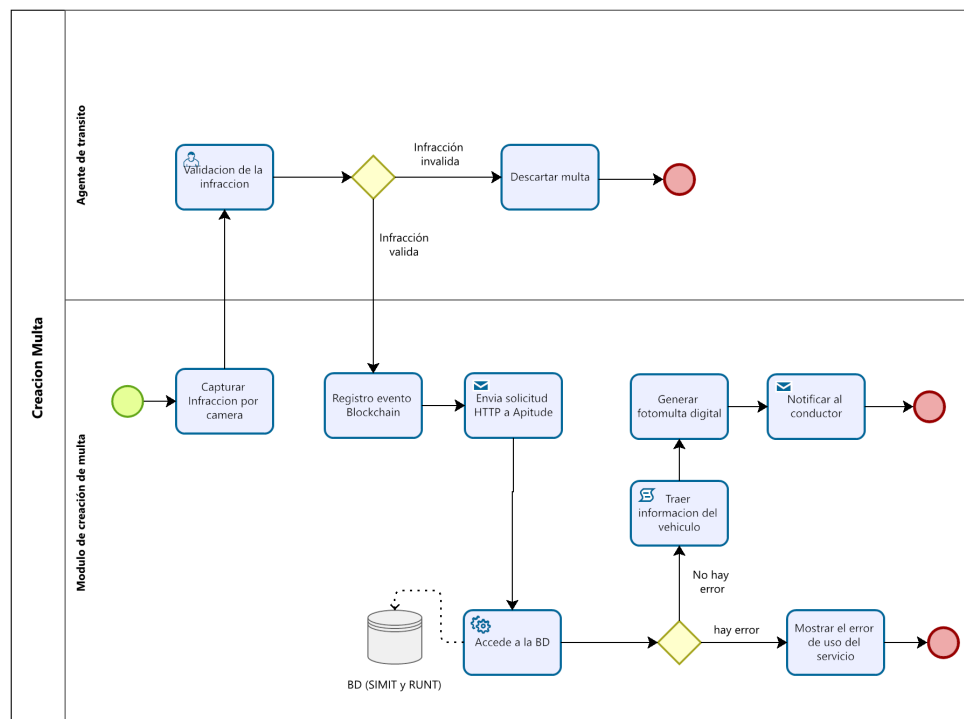
Diagrama de actividades para el proceso de apelación de multa



Nota. Elaboración propia.

Figura 10

Diagrama de actividades para el proceso de creación de multa

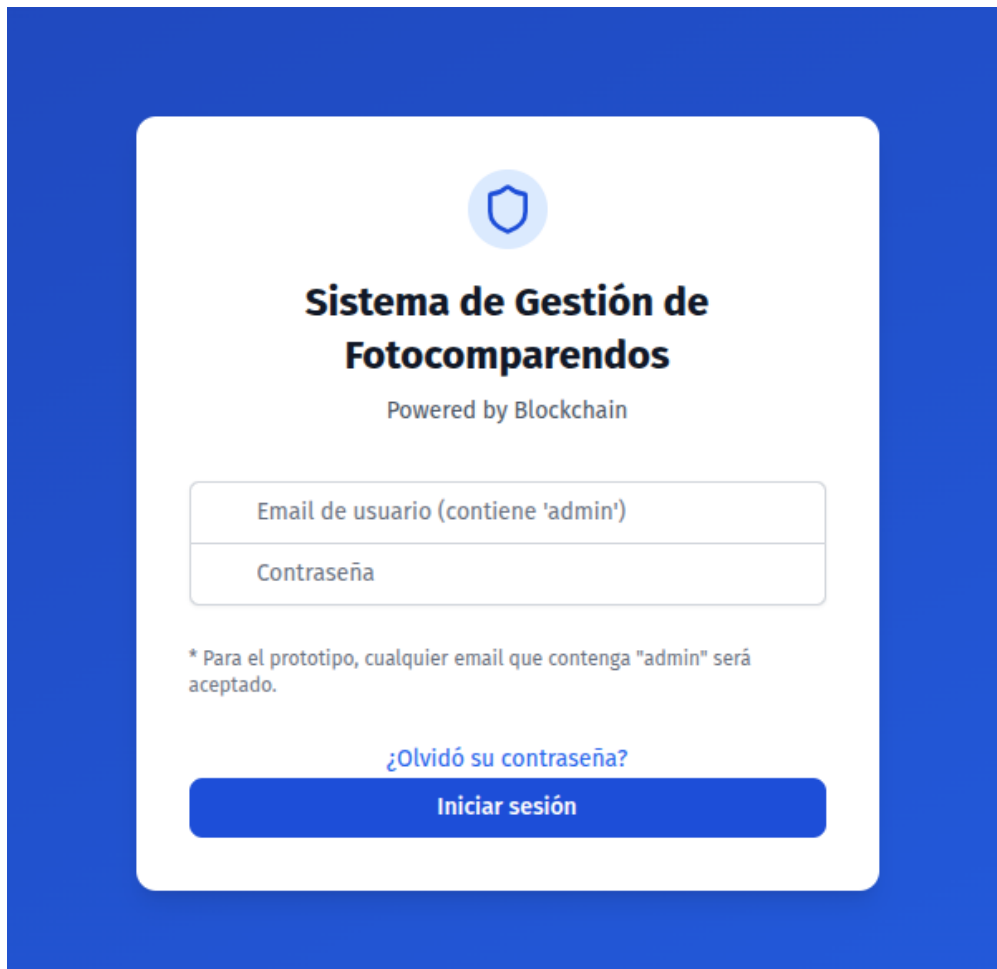



Powered by
brazo
Modeler

Nota. Elaboración propia.

Figura 11

Pantalla de login del sistema





**Sistema de Gestión de
Fotocomparendos**

Powered by Blockchain

Email de usuario (contiene 'admin')

Contraseña

* Para el prototipo, cualquier email que contenga "admin" será aceptado.

[¿Olvidó su contraseña?](#)

Iniciar sesión

Nota. Elaboración propia.

Figura 12

Pantalla de recuperación de contraseña

La imagen muestra una interfaz de usuario para la recuperación de contraseña. El título principal es "Recuperar contraseña" en un color azul oscuro. Debajo del título, hay un texto que dice "Ingrese su correo electrónico y le enviaremos las instrucciones". Hay un campo de entrada de texto con el placeholder "Correo electrónico" y el ejemplo "usuario@ejemplo.com". Debajo del campo de entrada, hay un botón azul con el texto "Enviar instrucciones" y un ícono de correo electrónico. En la parte inferior, hay un enlace azul que dice "Volver al inicio de sesión".

Recuperar contraseña

Ingrese su correo electrónico y le enviaremos las instrucciones

Correo electrónico

usuario@ejemplo.com

✉ Enviar instrucciones

[Volver al inicio de sesión](#)

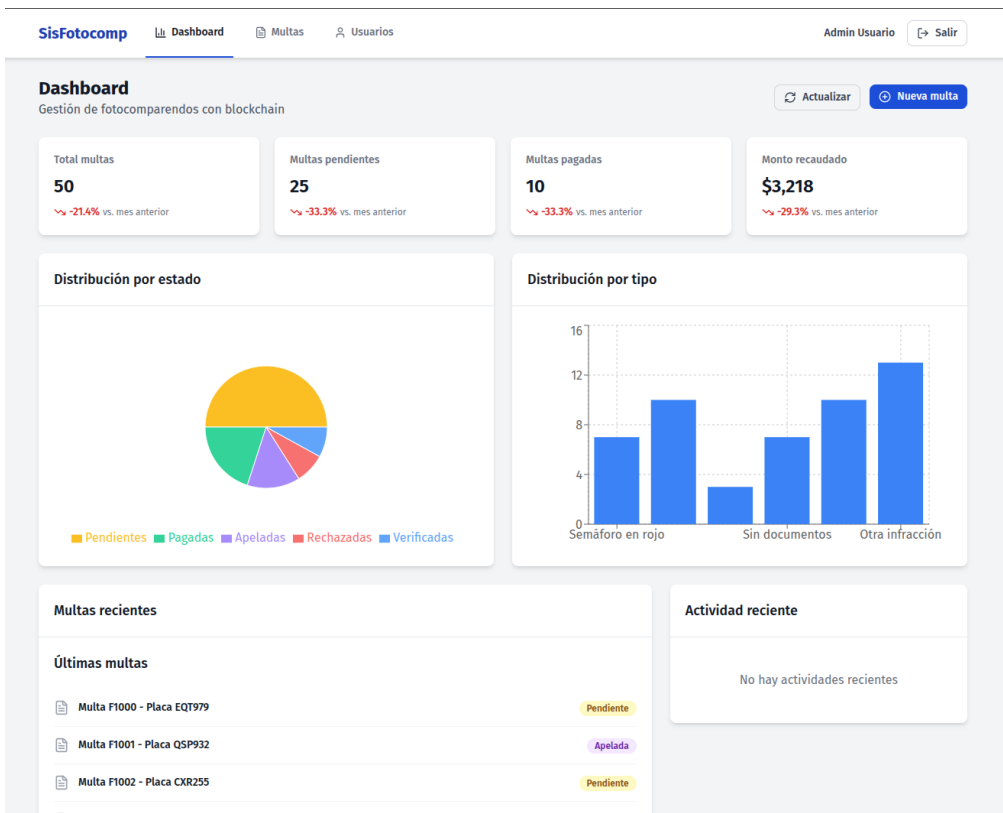
Nota. Elaboración propia.

estado de una multa, facilitando el seguimiento por parte del agente. En la Figura 15 se muestra el detalle completo de una multa específica, incluida la evidencia asociada.

Vista Propietario de Vehículo. Por último, la Figura 16 exhibe la vista que permite al propietario del vehículo revisar todas sus multas pendientes o en proceso.

Figura 13

Dashboard del agente de tránsito



Nota. Elaboración propia.

Figura 14

Pantalla de consulta del estado de multa

SisFotocomDashboardMultasUsuariosAdmin UsuarioSalir

Gestión de multasAdministra todas las infracciones registradas en el sistemaRegistrar nueva multa

Buscar por ID o placa...

Filtros

ID	PLACA	FECHA	TIPO	MONTO	ESTADO	
F1041	KMJ917	11 de jun de 2025, 08:27 a. m.	Estacionamiento ilegal	\$ 132.279	Pendiente	Ver detalles
F1034	ABS169	11 de jun de 2025, 08:27 a. m.	Sin documentos	\$ 170.850	Pendiente	Ver detalles
F1036	SGS466	11 de jun de 2025, 08:27 a. m.	Exceso de velocidad	\$ 172.674	Cancelada	Ver detalles
F1005	VBC893	10 de jun de 2025, 08:27 a. m.	Exceso de velocidad	\$ 210.525	Pendiente	Ver detalles
F1027	ZNN678	9 de jun de 2025, 08:27 a. m.	Conducción bajo influencia	\$ 226.487	Pagada	Ver detalles
F1006	WGD43	9 de jun de 2025, 08:27 a. m.	Sin documentos	\$ 570.843	Apelada	Ver detalles
F1028	ZFZ70	8 de jun de 2025, 08:27 a. m.	Exceso de velocidad	\$ 488.494	Pendiente	Ver detalles
F1008	DCT918	8 de jun de 2025, 08:27 a. m.	Conducción bajo influencia	\$ 511.266	Apelación Resuelta	Ver detalles
F1014	BKB947	7 de jun de 2025, 08:27 a. m.	Conducción bajo influencia	\$ 390.672	Pendiente	Ver detalles
F1047	KKJ664	6 de jun de 2025, 08:27 a. m.	Otra infracción	\$ 241.755	Apelación Resuelta	Ver detalles

Nota. Elaboración propia.

Figura 15

Pantalla de consulta de detalle de multa

SisFotocomDashboardMultasUsuariosAdmin UsuarioSalir

Gestión de multasAdministra todas las infracciones registradas en el sistemaRegistrar nueva multa

Buscar por ID o placa...

Filtros

ID	PLACA	FECHA	TIPO	MONTO	ESTADO	
F1041	KMJ917	11 de jun de 2025, 08:27 a. m.	Estacionamiento ilegal	\$ 132.279	Pendiente	Ver detalles
F1034	ABS169	11 de jun de 2025, 08:27 a. m.	Sin documentos	\$ 170.850	Pendiente	Ver detalles
F1036	SGS466	11 de jun de 2025, 08:27 a. m.	Exceso de velocidad	\$ 172.674	Cancelada	Ver detalles
F1005	VBC893	10 de jun de 2025, 08:27 a. m.	Exceso de velocidad	\$ 210.525	Pendiente	Ver detalles
F1027	ZNN678	9 de jun de 2025, 08:27 a. m.	Conducción bajo influencia	\$ 226.487	Pagada	Ver detalles
F1006	WGD43	9 de jun de 2025, 08:27 a. m.	Sin documentos	\$ 570.843	Apelada	Ver detalles
F1028	ZFZ70	8 de jun de 2025, 08:27 a. m.	Exceso de velocidad	\$ 488.494	Pendiente	Ver detalles
F1008	DCT918	8 de jun de 2025, 08:27 a. m.	Conducción bajo influencia	\$ 511.266	Apelación Resuelta	Ver detalles
F1014	BKB947	7 de jun de 2025, 08:27 a. m.	Conducción bajo influencia	\$ 390.672	Pendiente	Ver detalles
F1047	KKJ664	6 de jun de 2025, 08:27 a. m.	Otra infracción	\$ 241.755	Apelación Resuelta	Ver detalles

Nota. Elaboración propia.

Figura 16

Pantalla de consulta de multas para propietarios de vehículos

Consulta de Multas

Ingrese sus datos para consultar multas pendientes

Tipo de documento
Cédula de Ciudadanía ▼

Número de documento
Ingrese su número de documento

Placa del vehículo (opcional)
ABC123

Verificación CAPTCHA
N z u a L 4
Reload Captcha
Ingrese el código

Consultar

Nota. Elaboración propia.

Plan de Pruebas

Introducción y Propósito

El propósito de este plan es guiar la evaluación de la efectividad y viabilidad del prototipo desarrollado para la gestión de fotocomparendos utilizando Hyperledger Fabric e IPFS. Se busca validar que el prototipo cumple con los requisitos clave de inmutabilidad, transparencia, seguridad, y medir su rendimiento básico, comparándolo con las limitaciones identificadas en el sistema tradicional de Bogotá.

Alcance de las Pruebas

- Proceso completo de registro de un fotocomparendo: captura simulada, carga de evidencia a IPFS, registro de metadatos y hash IPFS en el ledger.
- Consulta y verificación de fotocomparendos registrados.
- Verificación de la inmutabilidad de los registros en el ledger y de la evidencia en IPFS.
- Consistencia de los datos entre la UI, el ledger y IPFS.
- Rendimiento básico de operaciones clave (registro, consulta).
- Actualización del estado de la multa (ej. "Pagada", "Apelada").

Fuera de Alcance

- Pruebas de estrés o carga exhaustivas.
- Pruebas de penetración de seguridad avanzadas.
- Integración completa con sistemas externos reales (RUNT, SIMIT) más allá de APIs simuladas o de prueba.
- Pruebas de usabilidad exhaustivas con usuarios finales.
- Funcionalidad de pago automatizado con billetera digital.

Entorno de Pruebas (Simulación Controlada)**Hardware:.**

- Servidor(es) para nodos Hyperledger Fabric (pueden ser VMs o contenedores Docker).
- Servidor(es) para nodo(s) IPFS (pueden ser VMs o contenedores Docker).
- Máquina para ejecutar la aplicación backend (Node.js/Express según).
- Máquinas cliente para acceder a la interfaz web (simulando Agente de Movilidad y Ciudadano).

Software:.

- Hyperledger Fabric (versión específica).
- IPFS (Kubo/Helia, versión específica).
- Base de datos (si la aplicación backend la usa adicionalmente).
- Aplicación backend (Node.js, Express, etc.).
- Aplicación frontend (navegador web).
- Herramientas de monitoreo y logging.

Datos de Prueba:.

- Conjunto de imágenes de evidencia (JPG, PNG) de diferentes tamaños.
- Datos de fotocomparendos ficticios (placas, fechas, ubicaciones, tipos de infracción).
- Datos de usuarios simulados (Agentes de Movilidad, Administradores, Ciudadanos).

Tabla 2*Casos de prueba funcionales para validar operaciones básicas del sistema*

ID	Caso de Prueba	Precondiciones	Acciones	Resultado Esperado
FP-001	Registro de fotocomparendo	Usuario autenticado, imagen disponible	1. Cargar imagen a IPFS 2. Registrar metadatos en Blockchain	CID generado, transacción exitosa
FP-002	Consulta de comparendo	Comparendo registrado previamente	1. Ingresar ID de comparendo 2. Consultar en Blockchain	Datos completos mostrados
FP-003	Verificación de evidencia	CID válido en Blockchain	1. Extraer CID de transacción 2. Recuperar imagen de IPFS	Imagen original recuperada
FP-004	Actualización de estado	Comparendo en estado "Pendiente"	1. Cambiar estado a "Pagado" 2. Registrar cambio en Blockchain	Estado actualizado inmutablemente
FP-005	Validación de integridad	Comparendo con evidencia asociada	1. Calcular hash de imagen actual 2. Comparar con CID registrado	Integridad verificada

Tipos de Pruebas y Casos de Prueba Detallados

En la Tabla 4 se enumeran los casos de prueba funcionales definidos para verificar el comportamiento básico del sistema, desde el registro de un fotocomparendo hasta la validación de su integridad y actualización de estado. Cada caso detalla las precondiciones, las acciones a ejecutar y el resultado esperado, sirviendo como guía para las pruebas manuales y automatizadas.

Pruebas de Inmutabilidad

Tabla 3

Casos de prueba de inmutabilidad para validar resistencia a modificaciones

ID	Caso de Prueba	Objetivo
IM-001	Intento de modificación directa en ledger	Verificar resistencia a cambios no autorizados
IM-002	Alteración de imagen en IPFS	Validar detección de modificaciones en evidencia
IM-003	Verificación de trazabilidad	Comprobar integridad del historial transaccional
IM-004	Validación de consenso	Evaluar mecanismos de protección distribuida

Nota. Elaboración propia.

Tabla 4*Resultados de pruebas de inmutabilidad del sistema*

Caso de Prueba	Descripción	Resultado Esperado	Resultado Real
IM-001	Modificación directa en ledger	Transacción rechazada	Rechazada correctamente
IM-002	Cambio de imagen en IPFS	CID diferente generado	CID distinto detectado
IM-003	Verificación de trazabilidad	Historial inmutable	Historial preservado
IM-004	Validación de consenso	Consenso mantenido	Consenso validado

Nota. Elaboración propia.

La Tabla 5 detalla los escenarios diseñados para poner a prueba la inmutabilidad del sistema ante intentos de modificación no autorizada, mientras que la Tabla 6 resume los resultados obtenidos en dichas pruebas, evidenciando la correcta detección y rechazo de cambios indebidos.

Pruebas de Rendimiento Básico

Se midió el tiempo requerido para ejecutar operaciones clave en condiciones simuladas de uso real:

Operación	Tiempo Pro- medio (s)
Registro completo (Blockchain + IPFS)	1.60
Consulta de evidencia desde IPFS	0.80
Validación de integri- dad	0.90

Cuadro 2

Tiempos promedio de operaciones en el entorno de prueba

Casos de Prueba de Inmutabilidad y Verificabilidad

Caso de Prueba	Objetivo	Resultado Esperado	Resultado Real
Registro de comparendo con CID válido	Verificar registro inicial	Registro exitoso e inmutable	Registro correcto
Intento de modificación de metadatos post-registro	Comprobar resistencia a cambios internos	Transacción rechazada o inconsistente detectada	Inconsistencia detectada
Carga de imagen modificada (pixel cambiado)	Validar detección de alteraciones en imagen	CID diferente, evidencia no válida	CID distinto generado
Consulta ciudadana por endpoint <code>/integrity</code>	Evaluar mecanismo de verificación independiente	Imagen original y metadatos coinciden	Evidencia verificada

Cuadro 3

Casos de prueba de inmutabilidad y verificabilidad del sistema

Estrategia de pruebas del frontend

Introducción. El frontend de la aplicación de gestión de multas implementa una estrategia integral de pruebas que abarca tanto pruebas unitarias como de integración, utilizando las mejores prácticas de testing en React con TypeScript. Esta estrategia garantiza la calidad del código, facilita el mantenimiento y reduce la introducción de errores durante el desarrollo.

Herramientas y Tecnologías

- **Jest**: Framework principal de testing con soporte para TypeScript.
- **React Testing Library**: Biblioteca para testing de componentes React con enfoque en comportamiento del usuario.
- **@testing-library/jest-dom**: Matchers adicionales para Jest.
- **@testing-library/user-event**: Simulación de eventos de usuario.
- **jsdom**: Entorno DOM para pruebas en Node.js.

Pruebas Unitarias

Pruebas de Integración

Resultados de las Pruebas de Inmutabilidad y Verificabilidad del Prototipo

Con el fin de validar los principios fundamentales sobre los que se sustenta el presente prototipo —particularmente la **inmutabilidad, integridad de evidencia y verificabilidad independiente**— se diseñó y ejecutó un plan de pruebas en entorno simulado controlado, alineado con los objetivos del proyecto y los estándares técnicos de la literatura especializada. Las pruebas se enfocaron en evaluar el comportamiento del sistema frente a intentos de modificación, errores de integridad y recuperación de evidencia a través de mecanismos descentralizados.

Pruebas de Inmutabilidad en Blockchain

Se registraron comparendos en la red *Hyperledger Fabric*, incluyendo el hash IPFS (CID) de la evidencia fotográfica y los metadatos del evento. Luego, se intentó simular una alteración directa sobre el estado del ledger.

Resultado: El sistema rechazó cualquier intento de modificación, manteniendo el hash original y evidenciando que la estructura de bloques y el mecanismo de consenso impiden alteraciones sin detección. Esto confirma que el sistema ofrece **inmutabilidad verificable** en los registros sancionatorios.

Verificación de Integridad con IPFS

Se almacenaron imágenes en IPFS y se compararon los CIDs obtenidos con nuevos hashes locales generados al momento de la consulta.

Resultado: Se comprobó que el CID siempre coincide con el contenido original. Cualquier cambio, incluso mínimo, genera un CID diferente, por lo que el sistema detecta automáticamente cualquier intento de manipulación. Esto demuestra que la evidencia permanece **íntegra y detectable ante alteraciones**.

Verificabilidad Transparente del Registro

Se implementó un mecanismo de consulta pública (`/api/fines/:fineId/integrity`) que permite a cualquier parte autorizada extraer el CID desde la Blockchain y verificar que la

evidencia recuperada desde IPFS corresponde al evento sancionado.

Resultado: La verificación se ejecuta sin intervención humana, desde fuentes independientes, replicando los principios de **transparencia, auditabilidad y confianza descentralizada**.

Casos de Prueba Funcionales

Casos de Prueba Funcionales

Tabla 5

Resultados de pruebas funcionales del sistema

ID	Caso de Prueba	Resultado	Estado
FP-001	Registro de fotocomparendo	Registro exitoso con CID	Exitoso
FP-002	Consulta de comparendo	Datos recuperados correctamente	Exitoso
FP-003	Verificación de evidencia	Imagen recuperada desde IPFS	Exitoso
FP-004	Actualización de estado	Estado actualizado en Blockchain	Exitoso
FP-005	Validación de integridad	Integridad verificada	Exitoso

Nota. Elaboración propia.

Casos de Prueba de Inmutabilidad**Tabla 6***Resumen de casos de prueba de inmutabilidad ejecutados*

ID	Descripción	Estado
IM-001	Intento de modificar metadatos directamente en el ledger	Ejecutada
IM-002	Alteración de imagen ya registrada en IPFS	Ejecutada
IM-003	Verificación de trazabilidad e integridad del historial	Ejecutada

Nota. Elaboración propia.**Pruebas de Rendimiento Básico**

Se midió el tiempo requerido para ejecutar operaciones clave en condiciones simuladas de uso real:

Los resultados obtenidos en el entorno de prueba respaldan la eficacia del modelo propuesto. Tal como se aprecia en la Tabla 7, todas las pruebas funcionales finalizaron de forma exitosa; de manera análoga, la Tabla 8 corrobora que los mecanismos de integridad impiden alteraciones, y la Tabla 9 demuestra que los tiempos de operación se mantienen dentro de márgenes aceptables para un uso en producción.

Tabla 7*Tiempos promedio de operaciones en el entorno de prueba*

Operación		Tiempo Pro- medio (s)
Registro	completo	1.60
(Blockchain + IPFS)		
Consulta de evidencia		0.80
desde IPFS		
Validación de integri-		0.90
dad		

Nota. Elaboración propia.

Conclusiones

1. El uso combinado de Blockchain permissionada e IPFS garantiza la inmutabilidad y verificabilidad de los registros sancionatorios, cumpliendo con el objetivo general del proyecto. La implementación del prototipo demostró que es posible registrar comparendos de forma segura y auditable, asegurando que tanto los metadatos como las evidencias fotográficas permanezcan protegidas ante manipulaciones, incluso frente a ataques internos o errores administrativos.
2. La evaluación funcional del sistema evidenció que los flujos principales de registro, consulta, verificación y actualización de multas operan correctamente, permitiendo una interacción fluida entre los actores del sistema: agentes de tránsito, ciudadanos y administradores. Esto confirma que los requisitos funcionales identificados en la etapa de análisis fueron cubiertos adecuadamente, y que la arquitectura distribuida no impide la usabilidad del sistema.
3. El modelo desarrollado representa un avance significativo hacia una gestión más transparente y confiable de los fotocomparendos en Bogotá, y sienta las bases para su adopción en contextos reales. Si bien el prototipo fue probado en un entorno simulado, sus resultados técnicos, el cumplimiento de los objetivos específicos y su alineación con las necesidades ciudadanas sugieren que su implementación a gran escala podría fortalecer la confianza institucional y reducir los casos de corrupción y disputa legal asociados a los sistemas actuales.

Limitaciones

- El prototipo fue validado en un entorno de laboratorio; no se evaluó en infraestructura productiva con carga real de usuarios.
- Los costos estimados corresponden a un escenario de referencia y podrían variar considerablemente según la escala de despliegue y la política de pinning en IPFS.

- La integración con sistemas externos (RUNT, SIMIT) se simuló mediante APIs de prueba; no se consideraron incompatibilidades de producción.
- No se realizaron pruebas de seguridad ofensiva (pentesting) ni auditorías formales de los contratos inteligentes.

Trabajos Futuros

- Desplegar un piloto controlado en la infraestructura de la Secretaría Distrital de Movilidad para evaluar rendimiento y experiencia de usuario.
- Implementar un servicio de pinning distribuido y políticas de retención para IPFS que garanticen la disponibilidad de la evidencia a largo plazo.
- Diseñar módulos de pago automatizado con pasarelas gubernamentales y billeteras digitales, incluyendo la integración de tokens estables.
- Realizar auditorías de seguridad especializadas en el chaincode y pruebas de penetración sobre la aplicación web.
- Extender el modelo a otras ciudades de Colombia para evaluar portabilidad normativa y técnica.