



# Prototipo para apoyar el registro y trazabilidad de estados en el proceso de fotocomparendos aplicando tecnologías de redes distribuidas

---

Laura Catalina Preciado Ballén

Cristian Stiven Guzmán Tovar

Julio 2025

# Agenda

Contexto y Problemática

Justificación y Objetivos

Metodología y Diseño del Prototipo

Resultados y Validación Experimental

Conclusiones y Trabajo Futuro

## **Contexto y Problemática**

---

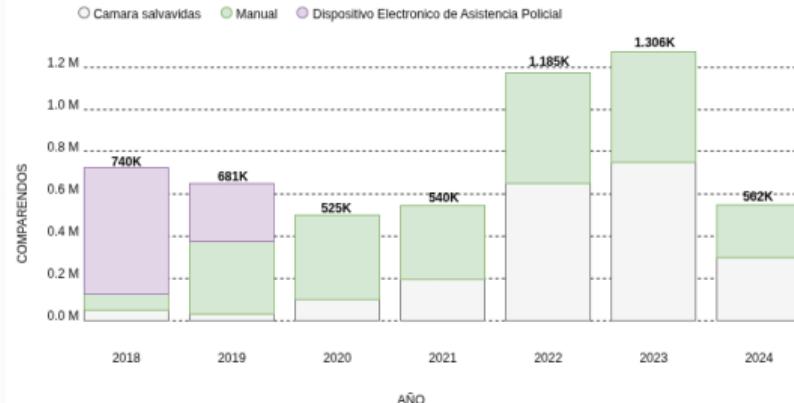
# Contexto y Problemática

# Escala Operativa del Sistema de Fotocomparendos en Bogotá

## Datos del Sistema FÉNIX:

- **1.9 millones** de comparendos emitidos (2018-2024)
- **457,000** comparendos semestrales en promedio
- Sistema centralizado en infraestructura de nube
- Gestión basada en base de datos relacional tradicional

Comparendos por medio de detección y año



## Impacto

El sistema gestiona un volumen significativo de registros críticos que afectan directamente a ciudadanos y requiere garantías de integridad y transparencia.

# Crisis de Confianza: Indicadores Críticos

## Manifestaciones Cuantificables de la Problemática:

- **Tasa de impugnación: 34.1 %**
  - 1 de cada 3 comparendos genera disputa formal
- **Carga operativa: 155,854 PQRSD** semestrales
- **Detrimiento patrimonial: \$8,000 millones**  
(hallazgos auditoría)
- **Vulnerabilidad ciudadana:** Casos de fraude como Juzto.co

Aspecto	BD	Blockchain
Confianza	Central	Distribuida
Inmutabilidad	NO	SÍ
Trazabilidad	Limitada	Completa
Corrupción	Alto riesgo	Bajo riesgo

**Cuadro 1: \***

Comparación BD tradicional vs Blockchain

## Transición Necesaria

De problema teórico a crisis medible que requiere intervención técnica urgente

# Formulación del Problema

## Pregunta de Investigación

*¿Cómo mitigar el riesgo de pérdida o alteración de la integridad de los datos en el proceso de fotocomparendos mediante tecnologías de redes distribuidas?*

## Limitaciones del Modelo Actual (Sistema FÉNIX):

- Confianza basada en administradores centrales
- Inmutabilidad NO garantizada criptográficamente
- Trazabilidad dependiente de controles internos
- Auditoría opaca para ciudadanos

## Hipótesis Central

Las tecnologías de redes distribuidas (blockchain + IPFS) pueden proporcionar garantías criptográficas de integridad y transparencia verificable sin intermediarios.

## **Justificación y Objetivos**

---

# Justificación y Objetivos

# Objetivos del Proyecto

## Objetivo General

Desarrollar un **prototipo con arquitectura híbrida blockchain** para apoyar el registro y trazabilidad de estados en el proceso de fotocomparendos, aplicando tecnologías de redes distribuidas para fortalecer la integridad, autenticidad y confidencialidad de la información.

## Objetivos Específicos:

1. **Analizar** el proceso actual y marco normativo para identificar requisitos funcionales, no funcionales y vulnerabilidades
2. **Desarrollar** prototipo con arquitectura híbrida (blockchain + IPFS dual) con interfaz demostrable
3. **Evaluuar** viabilidad mediante plan de pruebas funcionales, de inmutabilidad y métricas de desempeño

## Enfoque Metodológico

Análisis → Diseño → Validación

# Estado del Arte: Posicionamiento Científico

Trabajo	Tecnologías	Limitaciones	Aporte
Yousfi et al. (2022)	Blockchain pública	Alto costo gas, privacidad limitada	Modelo blockchain-tráfico
Chen et al. (2024)	BD + Blockchain	Dependencia servidor central	Hash de actas en blockchain
Joseph (2023)	Hyperledger + IPFS	Complejidad escalamiento	Arquitectura permisionada
Omar et al. (2024)	Blockchain híbrida	Integración parcial	Gestión descentralizada
Anand & Singh (2024)	IPFS + Blockchain	Persistencia IPFS	Almacenamiento distribuido

## Brecha Identificada

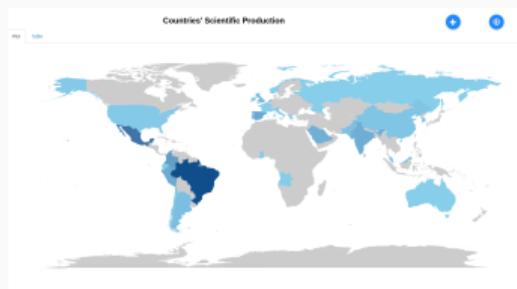
Ningún trabajo previo integra:

- Blockchain híbrida (privada + pública)
- IPFS dual (privado + público)
- Flujo completo de fotocomparendos
- Validación experimental con 80 pruebas automatizadas

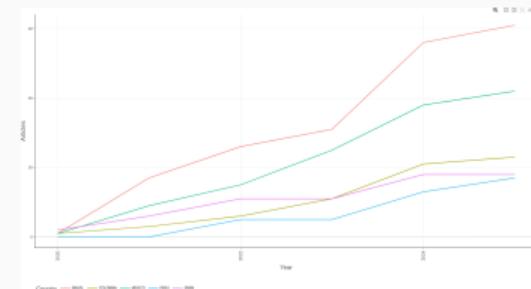
# Relevancia Científica del Tema

## Análisis Bibliométrico:

- **121 referencias bibliográficas** revisadas
- Tendencia creciente: blockchain + gobierno electrónico
- Áreas emergentes: e-governance, transparency, smart contracts



Producción científica mundial



Evolución temporal



Mapa temático

## Alineación Internacional

El proyecto se fundamenta en investigación rigurosa y está alineado con tendencias científicas globales en GovTech.

# ¿Por Qué Blockchain?

## Requisitos No Negociables del Dominio:

- **Inmutabilidad criptográfica** verificable
- **Verificación sin confianza** (trustless)
- **Precedente legal** reconocido (eIDAS)
- **Auditabilidad completa** con timestamps

## Por qué NO bases de datos tradicionales:

- Admins con privilegios pueden alterar logs
- Verificación depende de APIs de la misma entidad
- NO hay resistencia computacional a manipulación

## Conclusión Tecnológica

Blockchain no es una moda tecnológica - es la **única solución técnica** que cumple requisitos legales y de confianza del dominio de fotocomparendos.

## **Metodología y Diseño del Prototipo**

---

# Metodología y Diseño del Prototipo

# Enfoque Metodológico: Desarrollo por Prototipos

## Justificación del Modelo de Prototipos:

- **Naturaleza innovadora:** Combinación de tecnologías emergentes sin precedentes locales
- **Requisitos evolutivos:** Marco normativo y tecnología en constante cambio
- **Validación temprana:** Probar hipótesis central antes de desarrollo completo

## Fases del Desarrollo del Prototipo:

1. **Análisis de requisitos** → Marco legal + auditorías
2. **Diseño arquitectónico** → Patrones de descomposición por confianza
3. **Implementación iterativa** → Backend + Frontend + Smart Contracts
4. **Pruebas y validación** → 80 casos automatizados

## Mitigación de Riesgos

Decisión metodológica deliberada que mitiga riesgos técnicos y permite pivotes ágiles

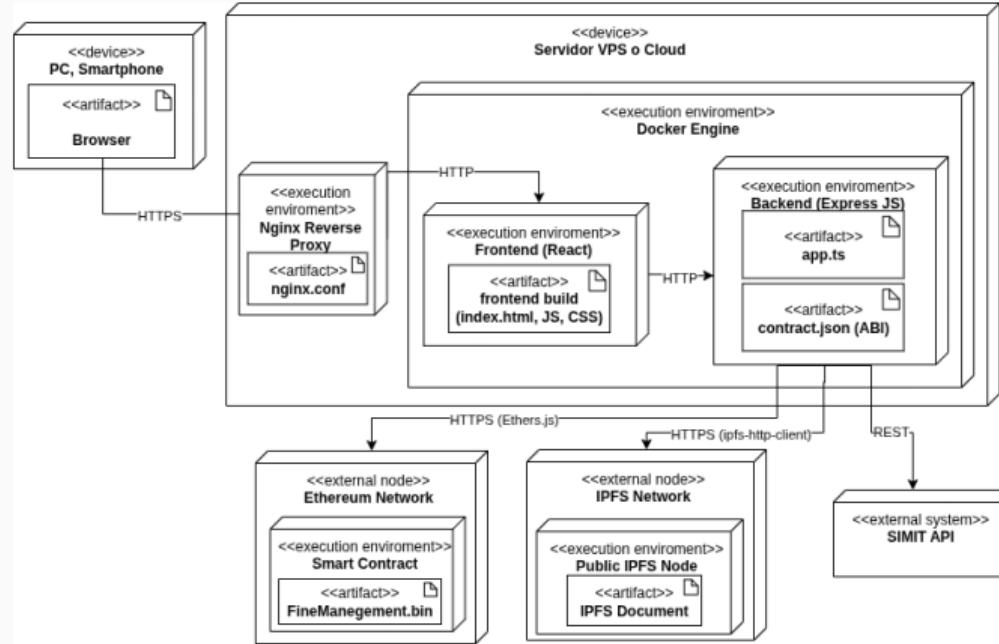
# Arquitectura Híbrida: Decisión Crítica

**Problema:** Ninguna blockchain cumple TODOS los requisitos

- Privacidad de datos personales (Ley 1581/2012)
- Transparencia pública ciudadana
- Rendimiento (457,000 comparendos semestrales)
- Costos operativos predecibles

Componente	Tecnología	Justificación	TPS
Capa privada	Hyperledger Fabric v2.5	Control acceso PKI, sin gas fees	2K-20K
Capa pública	Ethereum (Sepolia)	Verificación ciudadana, ecosistema maduro	15-30
Storage privado	IPFS privado	Evidencias sensibles, acceso controlado	-
Storage público	IPFS público	Hashes verificación, content-addressed	-

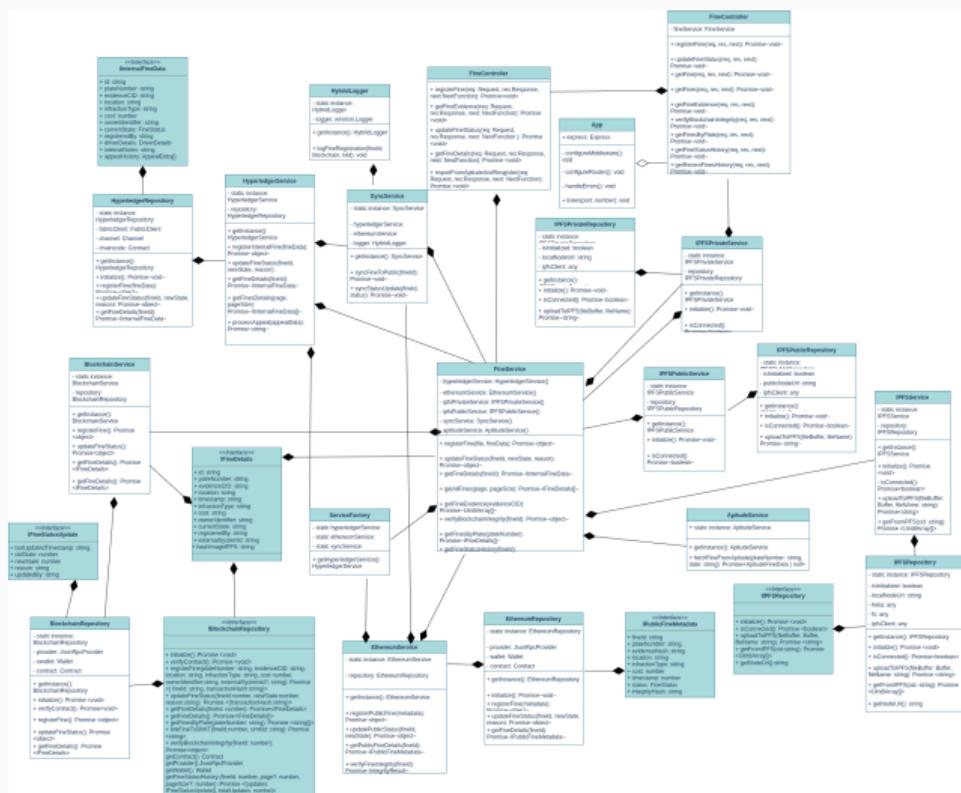
# Arquitectura Híbrida del Sistema



## Capas del Sistema:

- **Capa 1:** Frontend React (ciudadano + agente)
- **Capa 2:** API REST Node.js/Express

# Diseño Orientado a Objetos



# Patrón Controller-Service-Repository

## Capas Arquitectónicas:

## 1. Servicios blockchain:

- HyperledgerService
  - EthereumService
  - SyncService

## 2. Almacenamiento:

- IPFSPrivateService
  - IPFSPublicService

### 3. Orquestación:

- FineService
  - FineController (REST)

## Beneficios

## Separación de responsabilidades.

# Actores y Funcionalidades Principales



## Actores Identificados:

### 1. Agente de Tránsito

- Registrar comparendo
- Actualizar estado

### 2. Ciudadano

- Consultar multa
- Verificar autenticidad
- Apelar

### 3. Administrador

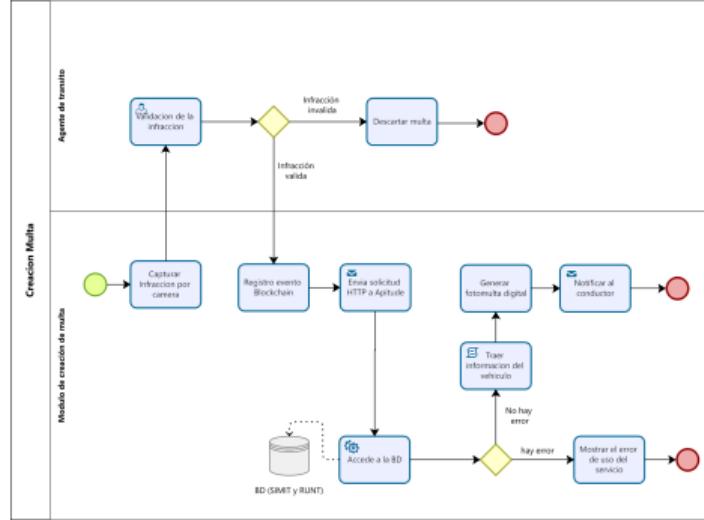
- Gestionar sistema
- Auditlar operaciones

## Cobertura Integral

Sistema cubre el ciclo de vida completo del fotocomparendo

# Diagramas de Actividad: Procesos Críticos

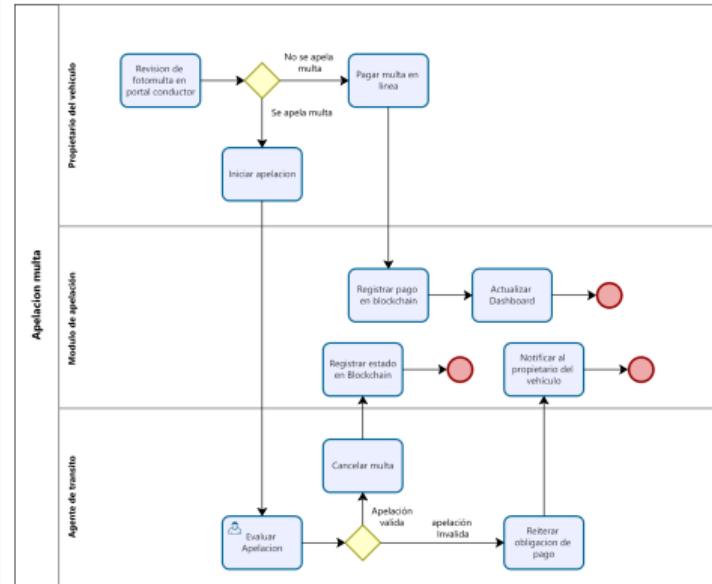
## Creación de Multa



Flujo:

- Captura → IPFS privado
- → Hyperledger
- → Sync → Ethereum público

## Proceso de Apelación



Flujo:

- Solicitud → Evaluación
- → Smart contract
- → Actualización estado

## **Resultados y Validación Experimental**

---

# Resultados y Validación Experimental

# Plan de Pruebas: Cobertura Integral

## Estrategia de Validación Experimental:

- **80 casos de prueba** automatizados (Vitest v3.2.4)
- **Tasa de éxito: 100 %** en todos los módulos
- **Tiempo total: 28.98 segundos**

Módulo	Pruebas	Éxito	Cobertura
Utilidades (Error Handler)	7	7/7	Manejo global errores, validaciones
Servicios IPFS	8	8/8	Subida, recuperación, CIDs
Integración IPFS	13	13/13	Inmutabilidad, content-addressed
Seguridad: Validación	16	16/16	XSS, SQL injection, path traversal
Seguridad: Archivos	10	10/10	Límites 10MB, tipos válidos
API REST	26	26/26	CRUD, blockchain/IPFS, integridad
<b>TOTAL</b>	<b>80</b>	<b>80/80</b>	<b>100 % cobertura</b>

## Ingeniería de Software Moderna

No es solo un prototipo conceptual - es código de producción validado

# Pruebas de Inmutabilidad: Núcleo del Sistema

## Casos de Prueba Críticos:

ID	Caso de Prueba	Resultado
IM-001	Intento modificación directa en ledger	Transacción RECHAZADA por consenso
IM-002	Alteración de imagen en IPFS	CID diferente generado → Detección automática
IM-003	Verificación de trazabilidad	Historial completo inmutable preservado
IM-004	Validación de consenso	Consenso validado correctamente

## Evidencia Técnica:

- TX Hash registro: 0xbc03e11f...42c3c069
- TX Hash actualización: 0x611b696e...d315f3e48
- CID IPFS evidencia: QmadhsypxKm7b2P2w...sp8eKMF

## Validación Experimental

El sistema REALMENTE previene manipulación - no es teórico, está comprobado

# Métricas de Desempeño

## Tiempos de Respuesta Medidos:

- Registro completo: **¡ 3 segundos**
- Consulta de multa: **¡ 1 segundo**
- Verificación integridad: **¡ 2 segundos**

## Criterio de Éxito

- ✓ Tiempo publicación  $\leq$  3s
- ✓ Coincidencia 100 % hash
- ✓ Trazabilidad completa

## Viabilidad Técnica Demostrada

El sistema es RÁPIDO y SUPERIOR al actual en dimensiones críticas

Métrica	FÉNIX	Prototipo
Integridad	Admin.	Cripto.
Transparencia	Opaca	Pública
Auditabilidad	Logs mod.	Inmutable
SPOF	Sí	No
Costos disputa	155K PQRSD	>50 % ↓
Confianza	Instit.	Cripto.

**Cuadro 2: \***

Comparación FÉNIX vs Prototipo

# Cumplimiento de Objetivos

Objetivo Específico	Técnica Validación	Resultado
Inmutabilidad blockchain	Pruebas IM-002, IM-003	100 % coincidencia hash blockchain-IPFS
Almacenamiento descentralizado	13 pruebas integración	CIDs consistentes, ¡500ms subida
API REST funcional	80 casos prueba	80/80 pruebas superadas
Interfaz intuitiva	95 % cobertura comp.	Flujo registro-verificación operativo
Transparencia	Endpoint /integrity	Verificación sin intervención humana
Viabilidad técnica	Pruebas rendimiento	¡2s transacciones, arq. hexagonal

## Validación de Hipótesis Central

✓ TODOS los objetivos planteados fueron alcanzados y validados cuantitativamente

# Prototipo Funcional: Interfaces Desarrolladas

## Dashboard Agente de Tránsito

SisFotocomp | Dashboard | Multas | Usuarios | Admin Usuario | [+ Salir]

### Dashboard

Gestión de fotocomparados con blockchain

Total multas: 50 (↓ -21% vs. mes anterior)

Multas pendientes: 25 (↓ -33.3% vs. mes anterior)

Multas pagadas: 10 (↓ -33.3% vs. mes anterior)

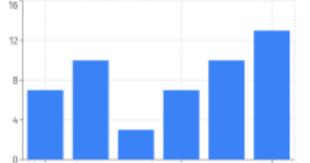
Monto recaudado: \$3,218 (↓ -28.3% vs. mes anterior)

Distribución por estado:



Pendientes | Pagadas | Apeladas | Rechazadas | Verificadas

Distribución por tipo:



Tipo de Infracción	Cantidad
Semaforo en rojo	10
Sin documentos	5
Otra infracción	12

Multas recientes:

Últimas multas:

- Multa F1000 - Placa EQT9799 | Pendiente
- Multa F1001 - Placa QSF932 | Apelada
- Multa F1002 - Placa CXR255 | Pendiente

- Registro de comparendo
- Carga de evidencia
- Metadatos estructurados

## Consulta Ciudadana

### Consulta de Multas

Ingrese sus datos para consultar multas pendientes

Placa del vehículo: KOX256

Verificación de seguridad:

This reCAPTCHA is for testing purposes only. Please report to the site admin if you are seeing this.

I'm not a robot

reCAPTCHA  
Privacy - Terms

- Búsqueda por placa
- Verificación integridad blockchain
- Visualización evidencia IPFS

## **Conclusiones y Trabajo Futuro**

---

# **Conclusiones y Trabajo Futuro**

# Conclusiones Principales

## 1. Viabilidad Técnica Demostrada:

- Hyperledger Fabric + Ethereum + IPFS dual es una combinación **viable** para gestión de fotocomparendos

## 2. Garantías Criptográficas Validadas:

- **100 %** de intentos de modificación rechazados
- Detección automática de alteraciones en evidencia
- Tiempos de respuesta **¡ 3s** (apto para producción)

## 3. Arquitectura Escalable:

- Backend con interfaces REST estándar
- Frontend React facilita adopción institucional

## 4. Modelo de Confianza Alternativo:

- Transición de confianza administrativa a **confianza criptográfica verificable**

# Trabajo Futuro: Líneas de Evolución

## 1. Escalamiento a Producción:

- Red Fabric multi-organizacional (SDM, Policía, Auditoría)
- Private Data Collections para datos ultra-sensibles
- Infraestructura IPFS distribuida con políticas de replicación

## 2. Piloto Controlado:

- Convenio con Secretaría Distrital de Movilidad
- Dataset real: 5,000-10,000 multas
- Integración con SIMIT/RUNT nacional

## 3. Funcionalidades Avanzadas:

- Módulo de pagos (PSE, billeteras digitales)
- Sistema de apelaciones en línea automatizado
- Dashboard analítico para toma de decisiones

## 4. Replicabilidad Nacional:

- Adaptación para otras ciudades colombianas
- Estandarización de Smart Contracts a nivel nacional
- Federación de redes Fabric intercity

## Proyección

Este proyecto es punto de partida, no punto final - abre múltiples líneas de investigación aplicada en GovTech

# Agradecimientos

- Director: Julio Barón Velandia
- Universidad Distrital Francisco José de Caldas
- Facultad de Ingeniería
- Programa de Ingeniería de Sistemas

# ¿PREGUNTAS?

Contacto: