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

Director: Julio Barón Velandia

Universidad Distrital Francisco José de Caldas
Facultad de Ingeniería
Programa de Ingeniería de Sistemas

Agenda

Contexto y formulación del problema

Objetivos

Metodología e implementación

Validación y pruebas

Conclusiones y aportes

Trabajo futuro

Contexto y formulación del problema

Contexto: el sistema de fotocomparendos en Bogotá

Escala operativa (Sistema FÉNIX):

- **1.9 millones** de comparendos emitidos entre 2018–2024 (Secretaría Distrital de Movilidad, 2024)
- **457,000** comparendos semestrales en promedio
- Arquitectura centralizada (BD relacional)

Indicadores de la problemática:

- Tasa de impugnación: **34.1 %**
- Carga operativa: **155,854 PQRSD** semestrales

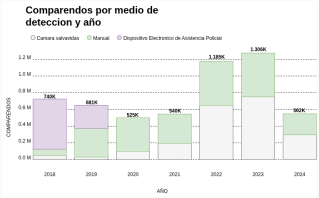

Figura 1: *Comparendos emitidos por semestre*

- Presunto detrimento patrimonial: **$8,000 millones** (Contraloría de Bogotá, 2024)
- Vulnerabilidad ciudadana ante fraudes (Semana, 2023)

Formulación del problema

Pregunta de investigación

¿Cómo mitigar el riesgo de pérdida o alteración de la integridad de los datos asociados a todos los estados en el proceso de fotocomparendos en Bogotá mediante el uso de tecnologías de redes distribuidas que garanticen el registro, la trazabilidad, la autenticidad y la confidencialidad de la información?

Limitaciones del modelo actual (FÉNIX): confianza en administradores centrales, inmutabilidad no garantizada criptográficamente, trazabilidad dependiente de controles internos, auditoría opaca para la ciudadanía.

Hipótesis

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

Objetivos

Objetivo general

Objetivo general

Desarrollar un prototipo software tecnológico que facilite el registro y la trazabilidad de los estados en el proceso de fotocomparendos en Bogotá, mediante la aplicación de tecnologías de redes distribuidas, para el fortalecimiento de la integridad y autenticidad de la información reduciendo los riesgos asociados a su confidencialidad.

Objetivos específicos

1. **Analizar** el proceso actual de registro de fotocomparendos a partir del marco jurídico, regulatorio e informes de auditoría, para identificar vulnerabilidades, requisitos funcionales y no funcionales.

2. **Desarrollar** un prototipo con arquitectura híbrida basado en blockchain permisionado (Hyperledger Fabric) y blockchain público (Ethereum), integrando almacenamiento distribuido mediante IPFS.

3. **Evaluar** la viabilidad técnica y funcional mediante un plan de pruebas que incluya inmutabilidad, trazabilidad, rendimiento y verificación de integridad de documentos.

Metodología e implementación

Enfoque metodológico: desarrollo por prototipos

Justificación del modelo:

- **Naturaleza exploratoria:** integración de tecnologías emergentes sin antecedentes en el contexto local
- **Requisitos evolutivos:** marco normativo y tecnológico en constante actualización
- **Verificación temprana:** contrastar la hipótesis central antes de un desarrollo a escala

Fases del desarrollo:

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

Decisión metodológica

El modelo de prototipos permite mitigar riesgos técnicos y facilitar ajustes iterativos ante cambios normativos o tecnológicos.

Arquitectura híbrida: decisión de diseño

Problema: ninguna plataforma blockchain individual satisface todos los requisitos.

- Privacidad de datos personales (Ley 1581/2012)
- Transparencia pública ciudadana (Ley 1712/2014)
- Rendimiento (457,000 comparendos semestrales)
- Costos operativos predecibles

Cuadro 1: *Componentes de la arquitectura híbrida*

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

Actores y funcionalidades principales

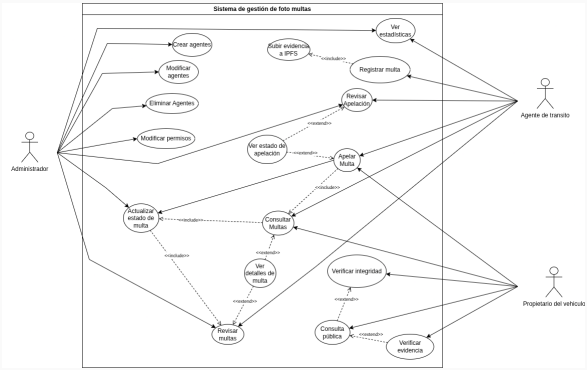

Figura 2: *Diagrama de casos de uso*

Actores identificados:

1. **Agente de tránsito**
   - Registrar comparendo
   - Actualizar estado
2. **Ciudadano**
   - Consultar multa
   - Verificar autenticidad
   - Apelar
3. **Administrador**
   - Gestionar sistema
   - Auditar operaciones

Flujos de proceso: diagramas de actividades

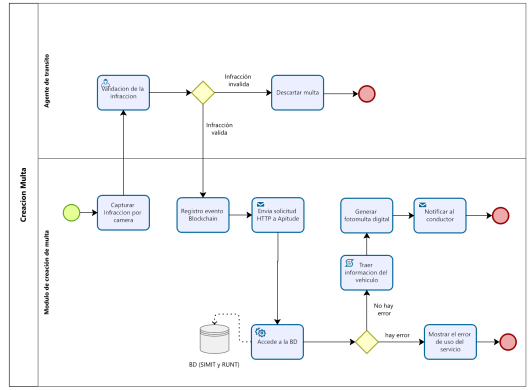

Figura 3: *Registro de multa*

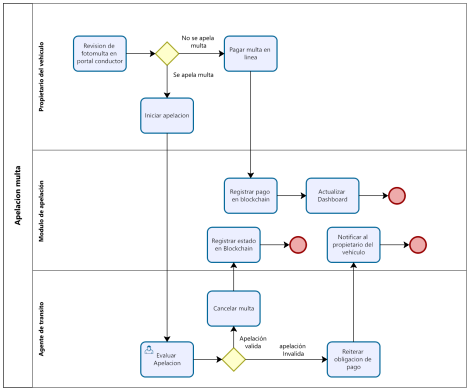

Figura 4: *Proceso de apelación*

Arquitectura del sistema

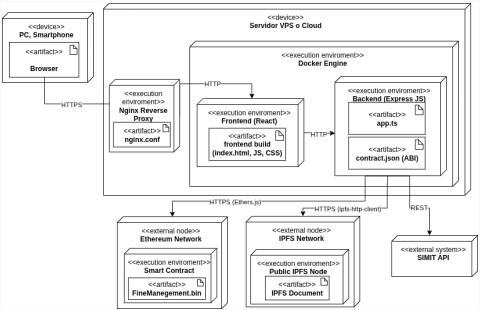

Figura 5: *Diagrama de despliegue del sistema*

Capas: 1. Frontend React — **2.** API REST Node.js/Express — **3.** Hyperledger Fabric — **4.** Ethereum + IPFS público — **5.** IPFS privado

Alcance y delimitaciones del estudio

Delimitaciones metodológicas del prototipo:

- **Datos sintéticos:** la verificación se realizó con datos generados mediante scripts de prueba, dado que no se dispuso de acceso a datos reales del FÉNIX, RUNT ni SIMIT.
- **Cobertura parcial de estados:** se implementaron 5 de los 8 estados del ciclo de vida (PENDING, PAID, APPEALED, RESOLVED_APPEAL, CANCELLED).
- **Volumen controlado:** se emplearon entre 50 y 100 comparendos de prueba, frente a los 457,000 semestrales registrados en producción.
- **Verificación técnica:** los resultados corresponden a una *verificación* en entorno controlado, no a una *validación* operativa institucional.

Nota metodológica

Se distingue entre *verificación* (el sistema cumple las especificaciones de diseño) y *validación* (el sistema opera adecuadamente en condiciones reales). Este trabajo se enmarca en la primera categoría.

Validación y pruebas

Plan de pruebas: cobertura del prototipo

Estrategia: **80 casos de prueba** automatizados (Vitest v3.2.4) — **Tasa de éxito: 100 %** — **Tiempo total: 28.98s**

Cuadro 2: *Resultados del plan de pruebas por módulo*

Módulo	Pruebas	Éxito	Cobertura
Utilidades (Error Handler)	7	7/7	Manejo global de errores
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
Total	**80**	**80/80**	**100 % cobertura funcional**

Pruebas de inmutabilidad

Cuadro 3: *Resultados de pruebas de inmutabilidad*

ID	Caso de prueba	Resultado
IM-001	Modificación directa en ledger	Transacción rechazada por consenso
IM-002	Alteración de imagen en IPFS	CID diferente → Detección automática
IM-003	Verificación de trazabilidad	Historial inmutable preservado
IM-004	Validación de consenso	Consenso validado correctamente

Evidencia técnica: TX Hash registro: `0xbc03e11f...42c3c069` — TX Hash actualización: `0x611b696e...d315f3e48` — CID IPFS: `QmadhsypxKm7b2P2w...sp8eKMF`

Resultado

En el entorno experimental, el prototipo rechazó satisfactoriamente el 100 % de los intentos de modificación no autorizada.

Métricas de desempeño

Tiempos de respuesta medidos:

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

Criterios de éxito

✓ Tiempo de publicación $\leq$ 3s

✓ Coincidencia 100 % hash

✓ Trazabilidad completa en entorno de prueba

Interfaces desarrolladas:

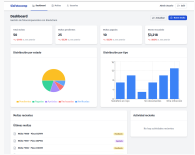

Figura 6: *Dashboard del agente de tránsito*

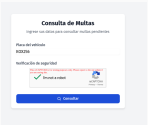

Figura 7: *Consulta y verificación ciudadana*

Conclusiones y aportes

Conclusiones principales

1. Viabilidad técnica demostrada:

- La arquitectura híbrida (Hyperledger Fabric + Ethereum + IPFS dual) demostró ser viable para la gestión de fotocomparendos en el entorno experimental.

2. Garantías criptográficas verificadas:

- 100 % de intentos de modificación no autorizada rechazados satisfactoriamente.
- Detección automática de alteraciones mediante *content-addressing* (CIDs).
- Tiempos de respuesta dentro de los criterios de aceptación ($\leq$ 3s).

3. Modelo de confianza alternativo:

- Transición hacia confianza criptográfica verificable, conciliando privacidad (Ley 1581/2012) y transparencia (Ley 1712/2014).

Respuesta a la pregunta de investigación

Respuesta

La respuesta a la pregunta de investigación es **afirmativa** dentro del alcance experimental definido: las tecnologías de redes distribuidas permiten mitigar el riesgo de alteración de la integridad de los datos en el proceso de fotocomparendos.

Evidencia obtenida:

- Registro y trazabilidad de 5 estados del ciclo de vida con inmutabilidad criptográfica
- Detección automática de alteraciones en documentos y evidencias
- Modelo de confianza verificable sin intermediarios

Oportunidades de extensión:

- Escalamiento a volúmenes operativos reales (457,000 comparendos semestrales)
- Integración con sistemas institucionales (SIMIT, RUNT)
- Incorporación de los estados restantes del proceso
- Estudios de aceptación tecnológica

Evidencia de cumplimiento de objetivos

Cuadro 4: *Cumplimiento de objetivos específicos*

Objetivo	Validación	Resultado
Análisis de vulnerabilidades	Auditoría documental y normativa	Brechas en FÉNIX identificadas; requisitos definidos
Desarrollo prototipo híbrido	Implementación iterativa	Arq. hexagonal: Fabric, Ethereum, IPFS dual, API REST
Evaluación viabilidad técnica	80 pruebas (Vitest v3.2.4)	100 % superadas; $\leq$ 3s; 100 % hash match

Síntesis

Los tres objetivos específicos se cumplieron dentro del alcance experimental definido.

Trabajo futuro

Líneas de evolución

1. Validación operativa:

- Piloto controlado con 5,000–10,000 multas reales
- Integración con SIMIT/RUNT mediante APIs reales
- Estudios de aceptación tecnológica (TAM/UTAUT) con agentes de tránsito y ciudadanos

2. Escalamiento a producción:

- Red Fabric multi-organizacional (SDM, Policía, Contraloría)
- Migración a soluciones Layer 2 (Polygon, Arbitrum)
- Auditoría formal de seguridad (Slither, MythX)

3. Extensión funcional:

- Oráculos certificadores para el estado NOTIFICADA
- Módulo de pagos (PSE, billeteras digitales)
- Sistema de apelaciones en línea automatizado

4. Replicabilidad:

- Adaptación para otras ciudades colombianas
- Estandarización de contratos inteligentes a nivel nacional
- Federación de redes Fabric intercity

Perspectiva

Los resultados obtenidos constituyen una base técnica para futuras investigaciones orientadas a la validación operativa e institucional del sistema propuesto.

Referencias principales

- Antonopoulos, A. M., & Harding, D. A. (2023). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media
- Contraloría General de la República de Colombia. (2024). Informe de Auditoría 170100-0054-24: Auditoría de Cumplimiento a la Secretaría Distrital de Movilidad [Auditoría realizada a la Secretaría Distrital de Movilidad de Bogotá D.C.].
- van Steen, M., & Tanenbaum, A. S. (2017). *Sistemas Distribuidos* (3.ª ed.) [Traducción de Distributed Systems, 3rd edition]. distributed-systems.net. https://www.distributed-systems.net/index.php/books/ds3/
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Agradecimientos

Universidad Distrital Francisco José de Caldas
Facultad de Ingeniería
Programa de Ingeniería de Sistemas

Director

Julio Barón Velandia

Autores

Laura Catalina Preciado Ballén

Cristian Stiven Guzmán Tovar

¿Preguntas?