

Descentralización del Centro de Monitoreo Urbano de la Ciudad Autónoma de Buenos Aires mediante Blockchain.

Trabajo Final Integrador.



Alumno: Maximiliano Ceña

Correo electrónico: m.cenaa@hotmail.com

Diplomatura: Diplomatura en Criptoconomía y Derecho – 2025.

Institución: ONG Bitcoin Argentina.

Fecha: 25 de marzo de 2025.-

Índice;

1. Introducción.
 - 1.1. Contexto y Relevancia.
 - 1.2. Planteamiento del Problema.
 - 1.3. Objetivos.
 - 1.4. Metodología.
2. Marco Teórico.
 - 2.1. Perspectiva blockchain.
 - 2.2. Perspectiva Jurídica.
3. Diagnostico del problema.
 - 3.1. Limitaciones operativas del sistema actual.
 - 3.2. Costos y recursos económicos.
 - 3.3. Implicancias jurídicas.
4. Propuesta de Solución.
 - 4.1. Modelo de Descentralización con Blockchain.
 - 4.2. Potencial de integración cámaras privadas.
 - 4.3 Compatibilidad y fortalecimiento jurídico.
 - 4.4. Marco Normativo Propuesto.
5. Conclusión.
6. Bibliografía.

1.1. Contexto y Relevancia.

En la actualidad, el material filmico de cámaras de seguridad constituye una prueba esencial para esclarecer hechos ilícitos en investigaciones judiciales en Argentina.

La Ciudad Autonoma de Buenos Aires, reconoce su importancia y, desde 2008, opera el Centro de Monitoreo Urbano (CMU), que gestiona 15.000 cámaras en tiempo real.

Sin embargo, su gestión centralizada resulta costosa, genera ineficiencias operativas y limita la capacidad de expansión, además de presentar riesgos para la privacidad y seguridad de los datos.

Este trabajo propone un sistema descentralizado basado en blockchain para reducir costos, optimizar el acceso al material filmico mediante contratos inteligentes y ampliar la red de videovigilancia con incentivos para integrar cámaras privadas.

Este enfoque fortalece las normas legales vigentes y se alinea con el uso de tecnologías emergentes que la CABA ya impulsa.

1.2. Planteamiento del Problema.

La gestión centralizada del material filmico en la Ciudad Autónoma de Buenos Aires, depende CMU, operativo desde 2008 con sedes en Chacarita, Avenida 9 de Julio y Puerto Madero, que supervisa 15.000 cámaras públicas instaladas hasta 2022.

Este sistema procesa grabaciones en tiempo real y las archiva para responder a solicitudes judiciales, pero presenta limitaciones estructurales.

En primer lugar, los costos operativos son elevados debido al mantenimiento de servidores robustos, el alto consumo energético de una infraestructura masiva y la necesidad de personal especializado para operar y resolver fallas técnicas, lo que encarece significativamente su funcionamiento.

Además, la concentración de operaciones - monitoreo, almacenamiento y distribución - genera cuellos de botella, retrasando respuestas a operadores judiciales (jueces y fiscales), pese a intentos como la Biblioteca Digital (2020) por agilizar plazos.

Otro problema crítico es la vulnerabilidad de la infraestructura centralizada, que al concentrar los datos en pocos centros aumenta los riesgos de manipulación, pérdida de integridad o ataques informáticos, comprometiendo la cadena de custodia esencial para la validez judicial del material filmico, así como la privacidad de los vecinos, al exponer sus datos a posibles accesos no autorizados o filtraciones.

Finalmente, el sistema centralizado del CMU carece de las oportunidades que ofrece un enfoque descentralizado, como la integración colaborativa de cámaras privadas en lugares públicos.

1.3. Objetivos.

Diseñar un modelo descentralizado basado en blockchain para gestionar de forma segura y eficiente el material filmico, optimizando su acceso al Poder Judicial. Promover la integración colaborativa de cámaras privadas para ampliar la cobertura del sistema. Evaluar los beneficios económicos y operativos de esta descentralización frente al modelo centralizado del CMU. Analizar la compatibilidad con el marco jurídico vigente, buscando fortalecer las normas existentes.

1.4. Metodología.

Se adopta un enfoque interdisciplinario que combina tecnología blockchain — almacenamiento descentralizado (IPFS), contratos inteligentes y soluciones de Capa 2 sobre Ethereum (ZKsync)— con un análisis de normativas vigente sobre la privacidad y seguridad (Ley 25.326, Ley 5.688, Ley 1.845), evaluando su implementación práctica y su fortalecimiento con este sistema.

2.1. Perspectiva Blockchain.

La tecnología blockchain es un sistema descentralizado que registra datos en bloques enlazados criptográficamente, eliminando intermediarios y garantizando seguridad e inmutabilidad.

En la gestión del material filmico ofrece una alternativa innovadora al modelo centralizado del CMU, permitiendo almacenamiento distribuido, trazabilidad transparente y automatización de procesos.

Este enfoque se basa en tres pilares técnicos; primero, el InterPlanetary File System (IPFS), un protocolo de almacenamiento descentralizado que fragmenta y distribuye archivos entre nodos, reduciendo la dependencia de servidores centrales. Segundo, los contratos inteligentes, programas autoejecutables en blockchain que gestiona accesos y establece incentivos de forma transparente y segura. Tercero ZKsync, una red Capa 2 sobre Ethereum que optimiza costos transaccionales y mejora la escalabilidad, con un enfoque robusto de privacidad.

En este contexto, es dable señalar que la CABA, ya ha implementado blockchain en el año 2024 con QuarkiD, un proyecto de identidades digitales descentralizadas, reflejando confianza en estas herramientas y reconociendo su potencial para aplicarlo en áreas del estado.

2.2.Perspectiva Jurídica.

El marco normativo local, busca equilibrar el uso del material filmico para fines judiciales con la protección de derechos fundamentales como la privacidad.

A nivel nacional, la Ley 25.326 de Protección de Datos Personales (2000) regula el tratamiento de datos, incluidas imágenes, exigiendo consentimiento informado salvo por interés público o seguridad, y garantizando resguardo y acceso restringido.

En la Ciudad Autónoma de Buenos Aires, la Ley 5.688 de Seguridad Pública (2016) autoriza el uso de cámaras gubernamentales para prevenir y esclarecer delitos, bajo estrictos protocolos de almacenamiento y acceso, mientras que la Ley 1.845 de Protección de Datos Personales de la CABA (2005) establece principios de finalidad, proporcionalidad y seguridad.

Otras normas relevantes incluyen la Ordenanza 61.852/2009, que regula la instalación de cámaras en espacios públicos y privados con fines de seguridad, y el Decreto 167/2018, que define procedimientos técnicos para la videovigilancia del CMU.

El acceso judicial al material filmico se enmarca en estas normativas específicas y debe respetar las garantías del debido proceso establecidas en el artículo 18 de la Constitución Nacional, así como el derecho a la privacidad reconocido en el artículo 19 nacional y el artículo 11 de la Constitución de la CABA.



3.1. Limitaciones Operativas del Sistema Actual.

El sistema centralizado del CMU, enfrenta limitaciones operativas que comprometen su eficacia como herramienta de apoyo al Poder Judicial.

En primer lugar, la concentración de las funciones - monitorea en tiempo real, almacenamiento de grabaciones y distribución a solicitud de operadores judiciales - genera cuellos de botella que ralentizan los procesos. Las 15.000 cámaras públicas procesan un volumen masivo de datos que, al depender de una infraestructura centralizada, satura los servidores y retrasa el acceso al material filmado afectando la agilidad requerida por investigaciones judiciales. En 2020, se implementó la Biblioteca Digital para reducir los plazos de entrega de grabaciones de 10 días a un objetivo de 24 horas. Sin embargo, esta solución no elimina las demoras estructurales, ya que el flujo centralizado sigue siendo un obstáculo para procesar y cargar las grabaciones de manera inmediata, especialmente en casos urgentes como delitos en flagrancia.

En segundo lugar, las limitaciones del personal humano agravan estas ineficiencias. La falta de automatización obliga a los 422 operadores y técnicos del CMU a manejar manualmente cada solicitud, lo que genera sobrecarga y retrasos.

En tercer lugar, la infraestructura centralizada presenta problemas de escalabilidad que restringe su crecimiento. Incorporar nuevas cámaras es técnicamente complejo y costoso, ya que los servidores actuales no pueden procesar un mayor volumen de datos sin sobrecargarse.

Finalmente, esta centralización expone vulnerabilidades críticas. La dependencia de una infraestructura concentrada aumentó el riesgo de ataques informativos que podrían alterar o eliminar grabaciones, comprometiendo su integridad como prueba judicial.

3.2. Costos y Recursos Económicos.

El sistema centralizado del CMU, demanda una inversión significativa en recursos económicos que refleja tanto su escala operativa como sus limitaciones estructurales. Según datos del Gobierno de la CABA, el CMU gestiona más de 15.000 cámaras públicas, lo que implica un gasto considerable en infraestructura tecnológica y humana. Aunque no se publican desgloses presupuestarios específicos en boletines oficiales recientes, el Presupuesto General de la CABA para 2023 (aprobado por la Ley 6.583, Boletín Oficial N° 6.524, 30/11/2022) asignó al Ministerio de Justicia y Seguridad —bajo cuya órbita opera el CMU— aproximadamente 147.000 millones de pesos, de los cuales una parte sustancial se destina a la videovigilancia y seguridad tecnológica.

Este monto incluye el mantenimiento de servidores robustos, con una sala de almacenamiento de última generación que procesa y archiva grabaciones en

resolución 4K, lo que eleva el consumo energético y los costos asociados a su refrigeración y operación continua.

Además, el CMU requiere una fuerza laboral significativa para funcionar las 24 horas, los 365 días del año. Informes oficiales indican que emplea a 542 personas, de las cuales 422 son operadores distribuidos en tres turnos, junto a coordinadores y personal técnico especializado (Buenos Aires Ciudad, 2021).

Esto genera un gasto anual estimado en sueldos y capacitación que, según parámetros del sector público porteño, podría superar los 2.000 millones de pesos, considerando salarios promedio y beneficios.

Otro costo relevante es la adquisición y renovación de equipos, como el videowall de 15 metros (48 pantallas de 55 pulgadas) y computadoras de alto rendimiento, cuya inversión inicial y mantenimiento periódico representan una carga económica constante. La expansión del sistema, que pasó de 2.000 cámaras en 2009 a más de 15.000 en 2022, evidencia un crecimiento sostenido que exige mayores recursos, incrementando la presión sobre el presupuesto público para sostener y ampliar la infraestructura del CMU.



3.3. Implicancias Jurídicas.

El sistema centralizado del CMU, genera implicancias jurídicas que pueden comprometer su alineación con el marco normativo vigente, exponiendo vulnerabilidades que un modelo descentralizado podría transformar en oportunidades para fortalecer las normas existentes.

La dependencia de una infraestructura concentrada no solo limita la eficiencia

operativa, sino que plantea desafíos legales que afectan la seguridad, la privacidad y la validez del material filmico.

En primer lugar, los riesgos técnicos de la centralización -como ataques informaticos o perdida de datos - conllevan serias implicancias jurídicas. La concentración de grabaciones en pocas sedes facilita su alteración o filtración, lo que podría derivar en violaciones de la Ley 25.326 de Protección de Datos Personales, exponiendo a la CABA a responsabilidades legales por no garantizar la privacidad de los ciudadanos.

En segundo lugar, la gestion centralizada introduce riesgos jurídicos derivados de la intervención humana y la falta de trazabilidad. La ausencia de mecanismos robusto para registrar y controlar los accesos al material filmico facilita errores o manipulación indebidas por parte del personal, lo que podría vulnerar los principios de proporcionalidad y finalidad exigidos por la Ley 5.6888 y la Ley 1.845 de la CABA. Esta falta de transparencia en la cadena de custodia no solo pone en riesgo la legitimidad del material como evidencia, sino que también dificulta la auditoria de su uso, incumpliendo las expectativas de un sistema judicial que requiere certeza y responsabilidad.

4.1. Modelo de Descentralización con Blockchain.

El modelo propuesto para la Ciudad Autónoma de Buenos Aires, consiste en una red descentralizada que reemplaza la gestión centralizada del CMU, integrando las cámaras públicas y privadas mediante blockchain para optimizar la videovigilancia y garantizar un acceso seguro y eficiente al material filmico. Este enfoque busca superar las limitaciones operativas, económicas y jurídicas del sistema actual, alineándose con las necesidades de seguridad y justicia.

Técnicamente, el modelo se basa en tres componentes clave. Primero las grabaciones se almacenan en Interplanetary System (IPFS), un sistema distribuido que fragmenta y guarda los archivos entre múltiples nodos, eliminando la dependencia de servidores centrales vulnerables. Segundo, los metadatos de estos archivos - como fecha, ubicación y hash único- se registran en ZKsync, una solución de Capa 2 sobre Ethereum, seleccionada por su bajo costo transaccional y compatibilidad con iniciativas locales como QuarkID. Tercero, los contratos inteligentes, programas autoejecutables en blockchain, automatizan la gestión de accesos y los incentivos para nodos participantes, asegurando transparencia y eficiencia.

El acceso al material filmico esta restringido solo a actores autorizados, como jueces y fiscales, mediante claves privadas que autentican su identidad y registran cada solicitud en la blockchain. Este sistema exige una justificación alineada con el debido proceso, garantizando que solo se utilice para fines legítimos. La trazabilidad inherente a la blockchain hace responsable a cada usuario, ya que cada acción queda inmutablemente registrada, fortaleciendo la cadena de custodia y la confianza en el

material como evidencia judicial.

En conclusión, este modelo descentralizado optimiza recursos, agiliza procesos y establece una base moderna y escalable para la videovigilancia en la CABA, adaptándose a las demandas actuales de seguridad y justicia con una tecnología innovadora.



4.2. Potencial de Integración cámaras privadas.

El modelo descentralizado basado en blockchain presentado abre la puerta a una nueva función clave: la integración de cámaras privadas para ampliar la cobertura de videovigilancia en la Ciudad Autónoma de Buenos Aires. A diferencia del sistema actual del CMU, que depende exclusivamente de las 15.000 cámaras públicas gestionadas por el gobierno, esta red permite incorporar de manera segura y eficiente las cámaras privadas existentes en comercios edificios, consorcios y hogares, aprovechando su potencial como recurso colaborativo.

Esta integración se habilita gracias a los componentes técnicos del modelo. El almacenamiento distribuido en IPFS asegura que las grabaciones en cámaras privadas puedan subirse a la red sin sobrecargar una infraestructura central, mientras que los contratos inteligentes gestionan la adhesión voluntaria de estos dispositivos, ofreciendo incentivos en token digitales, descuentos fiscales o reconocimiento ciudadano. ZKsync, por su parte, garantiza que estas transacciones sean escalables y de bajo costo, facilitando la participación masiva.

Aunque no hay datos oficiales precisos, estimaciones basadas en la densidad urbana y el registro obligatorio de cámaras privadas bajo la Ley 5.688 (RECAVIP) sugieren que podrían existir entre 50.000 y 100.000 cámaras de este tipo en la CABA, considerando sus 3 millones de habitantes y la proliferación de dispositivos de seguridad en áreas comerciales y residenciales.

Las ventajas de esta función son claras. Incorporar estas cámaras privadas multiplicaría el volumen de material filmico disponible para fines judiciales y de seguridad, cubriendo áreas que las cámaras públicas no registran, sin costo directo para el gobierno.

Además, la red podría extenderse a la ciudadanía, permitiendo a los vecinos subir grabaciones relevantes desde sus teléfonos móviles bajo protocolos seguros que respeten la privacidad, fomentando una colaboración activa con la justicia.

Este enfoque transforma la videovigilancia en un sistema más participativo, potenciando la cantidad de material filmico disponible para esclarecer conductas delictivas.

4.3. Compatibilidad y Fortalecimiento jurídico.

El modelo descentralizado basado en blockchain, se alinea plenamente con el marco normativo vigente en la Ciudad Autónoma de Buenos Aires, al tiempo que potencia sus exigencias legales para una videovigilancia más segura y confiable.

La combinación de almacenamiento distribuido, contratos inteligentes y soluciones Capa 2 no solo cumple con las leyes de proyección de datos y seguridad pública, sino que transforma limitaciones del sistema actual en oportunidades para reforzar la privacidad, la integridad de las pruebas y la transparencia, aspectos críticos para el Poder Judicial y la ciudadanía.

Esta compatibilidad se evidencia en varios niveles. El almacenamiento encriptado en IPFS, distribuye las grabaciones entre nodos, reduciendo riesgos de accesos no autorizados y cumplimiento con la Ley 25.326 de Protección de Datos Personales (2000), que exige resguardo y uso restringido de datos sensibles, como imágenes y videos. ZKsync, con su uso zero- knowledge proofs, añade una capa adicional de privacidad al ocultar detalles sensibles sin comprometer la verificación, fortaleciendo los principios de proporcionalidad y seguridad de la Ley 1.845 de la CABA (2005) y los artículos 19 (nacional) y 11 (CABA) sobre derechos a la intimidad. Los contratos inteligentes, por su parte, automatizan el acceso al material filmico, restringiendo a actores autorizados y registran cada solicitud en la blockchain. Esto asegura la trazabilidad exigida por la Ley 5.688, superando las falencias de trazabilidad del CMU actual y garantizando una cadena de custodia inmutable, alineada con el debido proceso del artículo 18 de la Constitución Nacional. Por otro lado, la integración colaborativa de cámaras privadas propuesto, se ajusta a la

Ordenanza 61.852/2009 y la Ley 5.688, que regulan su uso en espacios públicos bajo consentimiento informado y fines de seguridad, mientras que los incentivos destinados por contratos inteligentes aseguran que esta participación sea voluntaria y transparente, sin vulnerar derechos.

En conclusión, el modelo descentralizado no solo es viable dentro del marco legal existente, sino que lo enriquece al limitar accesos a fines legítimos, reducir riesgos de abuso y transparentar procesos que el sistema centralizado no puede garantizar. La inmutabilidad de blockchain asegura la integridad del material filmico como prueba judicial, mientras que la descentralización mitiga vulnerabilidades legales como filtraciones o manipulaciones.

Este fortalecimiento sienta las bases para ajustes normativos específicos, detallados a continuación, que maximicen el potencial de esta tecnología en la CABA, consolidando un sistema de videovigilancia mas robusto y confiable.

4.4. Marco Normativo Propuesto.

Como se estableció en el anterior punto, el modelo descentralizado basado en blockchain es compatible con el marco normativo vigente y lo fortalece al mejorar la privacidad, la trazabilidad y la integridad del material filmico. Sin embargo, para maximizar estos beneficios y garantizar su implementación efectiva en la Ciudad Autónoma de Buenos Aires, se requiere un marco normativo complementario que adapte las leyes existentes a las capacidades de esta tecnología. Las siguientes propuestas no buscan crear un sistema legal desde cero, sino potenciar las normas actuales para consolidar un modelo de videovigilancia más seguro, transparente y colaborativo.

En primer lugar, para aprovechar la integración de cámaras privadas y su compatibilidad con la Ley 5.688 de Seguridad Pública (2016), se propone modificar esta ley incorporando un capítulo específico que regule su adhesión voluntaria. Este capítulo actualizaría el Registro de Cámaras de Videovigilancia Privada (RECAVIP), estableciendo requisitos técnicos mínimos (resolución, conectividad) y un protocolo de consentimiento informado alineado con la Ley 25.326 de Protección de Datos Personales (2000). Este protocolo también habilitaría la participación ciudadana con grabaciones desde dispositivos móviles, exigiendo autorización expresa para fines judiciales y un proceso de anonimización de datos sensibles antes de su carga a IPFS, fortaleciendo así la privacidad ya garantizada por el modelo.

En segundo lugar, para institucionalizar la trazabilidad y seguridad demostradas en el punto 4.3, se sugiere un decreto complementario al Decreto 167/2018, que regula los procedimientos técnicos del CMU. Este decreto establecería blockchain como estándar de almacenamiento y acceso, definiendo las claves privadas como método exclusivo de autenticación para operadores judiciales. Cada solicitud, registrada en ZKsync con un propósito legítimo, cumpliría con los principios de

finalidad y proporcionalidad de la Ley 1.845 de la CABA (2005), mientras que la validación de grabaciones en IPFS mediante un hash verificado en blockchain reforzaría su integridad como prueba judicial, en línea con el artículo 18 de la Constitución Nacional.

Finalmente, para consolidar la colaboración público-privada y su transparencia, se propone una resolución del Ministerio de Justicia y Seguridad que regule el sistema de incentivos. Este sistema, basado en tokens digitales emitidos vía contratos inteligentes y canjeables por beneficios fiscales, estaría sujeto a auditorías públicas para evitar abusos, potenciando la confianza ciudadana y el cumplimiento normativo. Estas adaptaciones aprovechan las fortalezas jurídicas del modelo descentralizado, transformando las limitaciones del CMU en un sistema de videovigilancia más eficiente y alineado con el compromiso de la CABA por la innovación tecnológica en el ámbito judicial.

5. Conclusión.

Este trabajo demuestra que la gestión centralizada del material filmico del Centro de Monitoreo Urbano de la Ciudad Autónoma de Buenos Aires enfrenta limitaciones operativas, económicas y jurídicas que comprometen su eficacia como herramienta de apoyo a la seguridad y la justicia.

La dependencia de una infraestructura costosa y vulnerable restringe su potencial y expone riesgos que un modelo descentralizado basado en blockchain puede superar.

La propuesta presentada, que utiliza tecnología como IPFS y ZKsync, resguarda de forma segura el material filmico, optimizando el acceso instantáneo para actores autorizados, reduce costos operativos al eliminar servidores centralizados y permite ampliar la red de videovigilancia mediante la integración colaborativa de cámaras privadas.

Esta transición no solo responde a las necesidades inmediatas planteadas, sino que traza un camino hacia un sistema de seguridad más eficiente, participativo y tecnológicamente avanzando para la CABA.

6. Bibliografía.

Normas Jurídicas;

- *Constitución Nacional Argentina, Artículos 18 y 19.*
- *Constitución de la Ciudad Autónoma de Buenos Aires, Artículo 11.*
- *Ley Nacional N° 25.326 de Protección de Datos Personales, sancionada el 4 de octubre de 2000, publicada en el Boletín Oficial N° 29.512, 2 de noviembre de 2000.*
- *Ley de la Ciudad Autónoma de Buenos Aires N° 1.845 de Protección de Datos Personales, sancionada el 27 de octubre de 2005, publicada en el Boletín Oficial de*



CABA

N° 2.305, 15 de noviembre de 2005.

- Ley de la Ciudad Autónoma de Buenos Aires N° 5.688 de Seguridad Pública, sancionada el 1 de diciembre de 2016, publicada en el Boletín Oficial de la CABA N° 5.023, 14 de diciembre de 2016.

- Ordenanza N° 61.852/2009 de la Ciudad Autónoma de Buenos Aires, sancionada el 3 de diciembre de 2009, publicada en el Boletín Oficial de la CABA N° 3.308, 15 de diciembre de 2009.

- Decreto N° 167/2018 del Gobierno de la Ciudad Autónoma de Buenos Aires, publicado en el Boletín Oficial de la CABA N° 5.349, 23 de abril de 2018.

- Ley de la Ciudad Autónoma de Buenos Aires N° 6.583, Presupuesto General 2023, sancionada el 24 de noviembre de 2022, publicada en el Boletín Oficial de la CABA N° 6.524, 30 de noviembre de 2022.

-

Referencias Tecnológicas y Fuentes;

- Gobierno de la Ciudad Autónoma de Buenos Aires. (2021). "Centro de Monitoreo Urbano". Cita; buenosaires.gob.ar/seguridad/centro-de-monitoreo-urbano.

- Gobierno de la Ciudad Autónoma de Buenos Aires. (2024). "QuarkID: Identidad Digital Descentralizada". Informacion de; buenosaires.gob.ar/innovacion/quarkid.

- Ethereum Foundation. (s.f.). "ZKsync: A Layer 2 Scaling Solution". Cita; zksync.io.

- InterPlanetary File System (IPFS). (s.f.). "IPFS Documentation". Cita; ipfs.io/docs.

- Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". Cita; bitcoin.org/bitcoin.pdf (como base teórica de blockchain).