Blockchain application to comply with the Personal Data Protection Law in Ecuador

Aplicación Blockchain para cumplir la Ley de Protección de Datos Personales en Ecuador

Autores:

Montaño-Rivera ,Carlos Julio
UNIVERSIDAD CATÓLICA DE CUENCA
Ingeniero de Sistemas, Estudiante. Universidad Católica de Cuenca
Cuenca-Ecuador
carlos.montano.92@est.ucacue.edu.ec
https://orcid.org/0009-0000-8935-0362

Andrade-Paredes, Roberto Omar
UNIVERSIDAD CATÓLICA DE CUENCA
Docente de la Unidad Académica de Posgrados
Cuenca-Ecuador
roberto.andrade@ucacue.edu.ec
https://orcid.org/0000-0002-7120-281X

Cuenca -Tapia, Juan Pablo
UNIVERSIDAD CATÓLICA DE CUENCA
Magíster en Sistemas de Información Gerencial
Docente de la Unidad Académica de Tecnologías de la Información y Comunicación (TIC), Unidad Académica de Posgrados
Cuenca-Ecuador
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5982-634X

Fechas de recepción: 23-DIC-2024 aceptación: 23-ENE-2025 publicación: 15-MAR-2025
https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La protección de datos personales en Ecuador enfrenta desafíos significativos debido a la implementación de la Ley Orgánica de Protección de Datos Personales (LOPDP). Este artículo tiene como objetivo proponer una solución basada en la tecnología Blockchain, utilizando la red Avalanche, para garantizar el cumplimiento de los derechos de los titulares, así como la transparencia y la seguridad en la gestión de datos personales. Para lograrlo, se desarrolló un prototipo funcional que integra cifrado avanzado, gestión de consentimiento mediante contratos inteligentes y un diseño modular escalable. La metodología incluyó el despliegue de contratos inteligentes, pruebas de cifrado y evaluaciones de rendimiento en escenarios simulados. Como principal resultado, se comprobó que la solución es efectiva para cumplir con los requerimientos legales de la LOPDP, destacando la seguridad y la trazabilidad en el manejo de datos. En conclusión, esta investigación valida la viabilidad de Blockchain como herramienta para proteger los datos personales y posiciona a Ecuador como un referente en la adopción de tecnologías emergentes en este campo.

Palabras clave: Blockchain; Protección de Datos; Ecuador; Avalanche; Seguridad

Abstract

The protection of personal data in Ecuador faces significant challenges with the implementation of the Organic Law on Personal Data Protection (LOPDP). This article aims to propose a solution based on Blockchain technology, using the Avalanche network, to ensure compliance with data subject rights, as well as transparency and security in data management. A functional prototype was developed, integrating advanced encryption, consent management through smart contracts, and a modular scalable design. The methodology included deploying smart contracts, encryption tests, and performance evaluations in simulated scenarios. The main result showed that the solution effectively meets the legal requirements of the LOPDP, highlighting security and traceability in data handling. In conclusion, this research validates the feasibility of Blockchain as a tool to protect personal data and positions Ecuador as a leader in adopting emerging technologies in this field.

Keywords: Blockchain; Data Protection; Ecuador; Avalanche; Security

Introducción

La protección de datos personales se ha convertido en un tema crítico a nivel global, especialmente con el auge de las tecnologías digitales que han transformado la forma en que se maneja la información personal (Blockchain Council, 2021). En Ecuador, la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) representa un avance significativo en la protección de los derechos de los ciudadanos frente al uso y tratamiento de sus datos (Asamblea Nacional del Ecuador, 2021). Sin embargo, la implementación de esta legislación enfrenta desafíos importantes, como la falta de mecanismos técnicos robustos que garanticen la seguridad, la transparencia y la trazabilidad en la gestión de datos (Avalanche, 2021).

Diversos enfoques tecnológicos buscan resolver estos desafíos. Entre ellos, las soluciones basadas en Blockchain destacan por sus características de descentralización, inmutabilidad y transparencia, las cuales garantizan la trazabilidad y auditabilidad de las transacciones (Nakamoto, 2008). Estudios previos han demostrado la viabilidad de esta tecnología en contextos regulatorios similares, pero persisten brechas relacionadas con los costos de implementación y la adopción técnica (Blockchain Council, 2021). Este estudio no realiza una revisión de literatura completa, pero toma como referencia trabajos relevantes para proponer una solución práctica adaptada al contexto ecuatoriano.

El objetivo principal de esta investigación es diseñar y validar una aplicación tecnológica basada en Blockchain, utilizando la red Avalanche, que permita a las organizaciones cumplir con los requerimientos de la LOPDP. Esta solución incluye la implementación de contratos inteligentes para la gestión de consentimientos, el uso de cifrado avanzado para garantizar la confidencialidad de los datos y la trazabilidad de todas las operaciones realizadas.

En las siguientes secciones se describe el diseño de la arquitectura del sistema, su implementación, los resultados obtenidos y las conclusiones derivadas. Este artículo busca demostrar cómo Blockchain puede posicionarse como una herramienta clave para la protección de datos personales, estableciendo un modelo replicable en otros contextos regulatorios.

Metodología

La investigación desarrollada fue de tipo descriptiva, centrándose en el diseño e implementación de una arquitectura basada en Blockchain para garantizar el cumplimiento de la Ley Orgánica de

Protección de Datos Personales (LOPDP) en Ecuador. Este estudio se apoyó en fuentes primarias y secundarias, incluyendo revisiones de literatura y experimentación con tecnologías relevantes.

Procedimientos Utilizados

Diseño del Sistema: El sistema fue diseñado para ser modular y escalable, utilizando la red Avalanche como base de operaciones. Se implementaron tres capas principales:

Capa de Contrato Inteligente: Diseñada en Solidity para manejar la lógica de almacenamiento y auditoría de datos cifrados.

Capa de Backend: Construida con Python y Flask, conectó el front-end con la Blockchain a través de Web3.py.

Capa de Front-End: Desarrollada en HTML y JavaScript, permitió una interacción fácil para los usuarios finales.

Implementación del Contrato Inteligente:

El contrato MultiCompanyDataStorage.sol fue escrito y compilado utilizando solc. Las pruebas iniciales fueron realizadas en un entorno de prueba de Avalanche antes de su despliegue en la red principal.

Ejemplo de funcionalidad implementada:

La interfaz gráfica desarrollada para el sistema permite realizar operaciones clave, como la generación de tokens CSRF y la creación de empresas en la Blockchain, de manera simple e intuitiva. En la Figura 1, se muestra el diseño del frontend del API Tester, que facilita a los desarrolladores y usuarios finales interactuar con las funcionalidades del sistema.

Figura 1

Frontend del api tester Blockchain.

Nota: La interfaz gráfica permite a los usuarios interactuar de manera sencilla con las funcionalidades del sistema, garantizando la generación segura de tokens CSRF y facilitando la administración de entidades en la Blockchain..

Como se observa en la Figura 1, el sistema incluye módulos interactivos que permiten la generación de tokens CSRF con una duración configurable, necesarios para garantizar la seguridad en las transacciones. Además, la funcionalidad de creación de empresas permite registrar nuevas entidades en la Blockchain mediante un flujo simplificado, mejorando la accesibilidad y eficiencia del sistema.

El contrato inteligente incluye una función llamada *storeData*, que asegura que solo el propietario de los datos pueda almacenarlos. Esta funcionalidad se detalla en la Figura 1.

Figura 2

Función storeData del contrato inteligente.

```
function storeData(bytes32 dataHash, address owner) publ
    require(msg.sender == owner, "Unauthorized access");
    dataStorage[owner].push(dataHash);
}
```

Nota. Función storeData del contrato inteligente, diseñada para garantizar que solo el propietario de los datos pueda añadir información.

En la Figura 2, la función *storeData* emplea el modificador *require* para verificar que la dirección que realiza la transacción coincide con la del propietario.

Esto asegura que no haya accesos no autorizados al sistema, cumpliendo con las disposiciones de seguridad y trazabilidad requeridas por la Ley Orgánica de Protección de Datos Personales (LOPDP).

Integración de Cifrado:

Se utilizó la librería ***pycryptodome*** para garantizar que los datos enviados a la Blockchain estuvieran cifrados. Este proceso asegura la confidencialidad de los datos incluso en un entorno descentralizado.

Proceso de cifrado utilizado:

El sistema utiliza el cifrado AES (Advanced Encryption Standard) para garantizar la seguridad de los datos personales antes de su almacenamiento en la Blockchain. Este proceso de cifrado se implementa mediante la función encrypt_data, presentada en la Figura 3.

Figura 3

Función encrypt_data que implementa cifrado AES.

```
from Crypto.Cipher import AES

def encrypt_data(data, key):
    cipher = AES.new(key, AES.MODE_EAX)
    nonce = cipher.nonce
    ciphertext, tag = cipher.encrypt_and_digest(data.enc
    return ciphertext, nonce
```

Nota. Función encrypt_data que implementa cifrado AES para garantizar la confidencialidad de los datos.

En la Figura 3, la función encrypt_data utiliza el algoritmo AES en modo EAX para encriptar datos. Este proceso incluye la generación de un nonce único, que garantiza la integridad del mensaje cifrado. Este enfoque cumple con los estándares de seguridad exigidos por la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.

Despliegue del Contrato y Configuración del Backend:

El contrato fue desplegado utilizando ***deploy_contract.py***. Este script automatizó el proceso de conexión con la red Avalanche, compilación y despliegue del contrato.

Posteriormente, se configuró el backend para gestionar las interacciones con la Blockchain y realizar validaciones de las transacciones.

Diseño del Front-End:

Se creó una interfaz gráfica utilizando ***data_protect.html***, con formularios interactivos que permiten a los usuarios gestionar consentimientos y consultar datos almacenados.

Pruebas del Sistema:

Pruebas funcionales: Verificación de que todas las funciones del contrato y la API operaran correctamente.

Pruebas de carga: Medición del tiempo promedio de respuesta de las consultas a la Blockchain.

Fuentes de Información:

Primarias: Datos obtenidos mediante pruebas técnicas realizadas en la red Avalanche y los prototipos funcionales desarrollados.

Secundarias: Revisión de literatura académica y documentación oficial de Avalanche y herramientas relacionadas.

Variables Consideradas:

Variable Independiente: La tecnología Blockchain como medio para la protección y gestión de datos personales.

Variables Dependientes: Transparencia, seguridad, y cumplimiento normativo de la LOPDP.

Instrumentos de Investigación

El instrumento principal fue el prototipo funcional desarrollado para validar la propuesta. Este prototipo incluyó:

Contratos inteligentes para gestionar consentimientos y auditorías.

API RESTful para interactuar con la Blockchain.

Una interfaz gráfica amigable para el usuario final.

Consideraciones Éticas

Se cumplieron todas las disposiciones de la LOPDP relacionadas con la gestión de datos personales. Además, el sistema fue diseñado para garantizar que ninguna información personal pudiera ser accedida sin la autorización adecuada.

Referencia al README

Se incluyó un archivo README.md en el repositorio asociado al prototipo. Este archivo proporciona instrucciones detalladas para:

Instalación del proyecto:

Clonar el repositorio utilizando el comando:

```
git clone https://github.com/cjmont/lopd.git
cd lopd
```

Instalar las dependencias:

```
pip install -r requirements.txt
```

Configurar las variables de entorno en un archivo. env:

Para garantizar la configuración adecuada del sistema, se deben definir las variables de entorno en un archivo. env, el cual incluye claves privadas y direcciones necesarias para interactuar con la Blockchain. Este archivo se detalla en la Figura 4.

Figura 4

Variables de entorno en un archivo. env.

```
PRIVATE_KEY=<your_private_key>
CONTRACT_ADDRESS=<your_contract_address>
SECRET_KEY=<your_secret_key>
```

Nota. Configuración de variables de entorno en un archivo: .env para el correcto funcionamiento del sistema.

En la Figura 4 se muestra la estructura básica del archivo. env, donde se especifican la clave privada del usuario (PRIVATE_KEY), la dirección del contrato desplegado (CONTRACT_ADDRESS) y una clave secreta utilizada para la encriptación de datos (SECRET_KEY). Este archivo debe configurarse correctamente para garantizar la conexión segura con la Blockchain y el correcto despliegue de las operaciones.

Ejecución del proyecto:

Iniciar la aplicación Flask:

```
flask run
```

Despliegue con Docker:

Construir y ejecutar el contenedor Docker:

```
docker-compose build
docker-compose up
```

Pruebas:

Utilizar herramientas como Postman para interactuar con los endpoints proporcionados:

Generar tokens CSRF.

Crear empresas.

Añadir y consultar datos cifrados.

Resultados

Los resultados de la investigación se enfocaron en validar la viabilidad técnica y operativa de la solución basada en Blockchain para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador. A continuación, se presentaron los hallazgos más relevantes obtenidos tras el despliegue y las pruebas del sistema propuesto.

Funcionamiento del Prototipo

El prototipo funcional permitió realizar pruebas integrales en la red Avalanche, destacándose las siguientes capacidades:

Creación de empresas: Se validó la capacidad de registrar nuevas empresas en la Blockchain con éxito. Cada registro generó un hash de transacción único y verificable.

Inserción de datos cifrados: Los datos personales fueron encriptados correctamente antes de ser enviados al contrato inteligente, garantizando la confidencialidad de la información.

Consulta de datos almacenados: Los datos almacenados pudieron ser recuperados y descifrados exitosamente, verificando que se mantuvieran íntegros durante todo el proceso.

Pruebas de Rendimiento

Se realizaron pruebas de rendimiento para medir la eficiencia del sistema en escenarios simulados de alta carga. Los resultados clave fueron:

Tiempos de respuesta:

Registro de empresas: 1.8 segundos en promedio.

Inserción de datos: 2.3 segundos en promedio.

Consulta de datos: 1.5 segundos en promedio.

Uso de recursos:

La aplicación utilizó en promedio un 25% de CPU y 512 MB de memoria durante las pruebas de carga.

Cumplimiento Legal

El sistema cumplió con los requisitos establecidos en la LOPDP, incluyendo:

Consentimiento informado: Los contratos inteligentes registraron y auditaron el consentimiento de los usuarios de manera automática.

Protección de datos sensibles: El cifrado de datos personales antes de su almacenamiento aseguró la confidencialidad requerida por la normativa.

Auditoría y trazabilidad: Cada transacción fue registrada con un identificador único, lo que permitió una trazabilidad completa de las operaciones.

4. Viabilidad Operativa

El despliegue del sistema demostó su viabilidad técnica y operativa al integrarse exitosamente con herramientas como Docker y Flask. Además, se logró:

Facilidad de replicación: El uso de un archivo README.md detallado permitió la replicación del sistema sin problemas.

Escalabilidad: La arquitectura modular asegura que el sistema pueda manejar un aumento en el volumen de transacciones sin comprometer el rendimiento.

Tabla 1.

Tiempos promedio de respuesta de las operaciones del sistema durante las pruebas funcionales.

Operación	Tiempo promedio
Registro de empresas.	1.8 segundos.
Inserción de datos.	2.3 segundos.
Consulta de datos.	1.5 segundos.

Nota: Elaboración propia.

En la Tabla 1 se resumen los tiempos promedio de respuesta obtenidos durante las pruebas. Estas cifras reflejan que el sistema cumple con los estándares aceptables para aplicaciones descentralizadas, donde la transparencia y la seguridad suelen priorizarse sobre la velocidad. La operación más rápida fue la consulta de datos, mientras que la inserción de datos mostró un tiempo ligeramente mayor debido al proceso de cifrado y almacenamiento en la *Blockchain*.

Tabla 2.

Uso promedio de recursos del sistema durante las pruebas de carga.

Recurso	Promedio
➢ **CPU.**	➢ 25%.
➢ **Memoria.**	➢ 512 MB.

Nota: Elaboración propia.

En La Tabla 2 detalla el uso promedio de recursos del sistema durante las pruebas de carga. Se observó que el sistema mantuvo un consumo moderado de CPU (25%) y memoria (512 MB), lo que demuestra su eficiencia y capacidad para operar en entornos con recursos limitados.

Limitaciones Observadas:

A pesar de los éxitos obtenidos, se identificaron algunas limitaciones:

Costos iniciales de despliegue: El despliegue en la red principal de Avalanche requirió recursos financieros significativos.

Curva de aprendizaje: La adopción de la tecnología requirió capacitación específica para los desarrolladores involucrados.

En general, los resultados obtenidos confirman la eficacia de la solución propuesta, destacando su capacidad para cumplir con las exigencias legales y operativas de la LOPDP en Ecuador.

Discusión

El análisis de los resultados obtenidos en este estudio confirma la viabilidad técnica y operativa de utilizar la tecnología Blockchain, y específicamente la red Avalanche, para cumplir con los requerimientos de la Ley Orgánica de Protección de Datos Personales (LOPDP).

Interpretación de Resultados:

Los resultados obtenidos evidencian que el sistema propuesto es altamente eficiente en diversas áreas clave. En primer lugar, garantiza la seguridad de los datos personales mediante la implementación del cifrado AES, el cual asegura que la información almacenada en la Blockchain sea inaccesible sin las claves adecuadas. Esto permite cumplir con los requisitos de confidencialidad establecidos en la Ley Orgánica de Protección de Datos Personales (LOPDP). Además, el sistema facilita las auditorías y la trazabilidad de las transacciones, ya que cada operación es registrada de manera inmutable. Este registro inalterable no solo incrementa la transparencia, sino que también posibilita la verificación completa de las operaciones realizadas.

Por otro lado, el sistema cumple con los tiempos de respuesta esperados, registrando un rango promedio de 1.5 a 2.3 segundos. Estos resultados son considerados aceptables en un entorno descentralizado, donde la prioridad radica en la seguridad y la transparencia, incluso por encima de la velocidad.

Comparación con Investigaciones Previas:

Estudios previos han resaltado la utilidad de la tecnología Blockchain para garantizar el cumplimiento normativo en la protección de datos personales. Por ejemplo:

Blockchain Council (2021): Enfatizó la capacidad de Blockchain para cumplir con el Reglamento General de Protección de Datos (GDPR) en Europa mediante sistemas descentralizados y auditables.

Avalanche Documentation: Identificó a Avalanche como una red altamente escalable y eficiente en costos para el desarrollo de soluciones empresariales.

El presente estudio complementa estos hallazgos al validar que las mismas ventajas pueden ser aplicadas en el contexto ecuatoriano con la LOPDP. Además, se destaca el desarrollo de un prototipo funcional que demuestra la aplicabilidad técnica y operativa del sistema propuesto. Este estudio resalta importantes implicaciones prácticas para la adopción de la tecnología Blockchain en Ecuador. Al posicionar a Blockchain como una solución viable para las organizaciones que buscan cumplir con las normativas de protección de datos, se establece una base sólida para su implementación en el ámbito regulatorio. Además, la transparencia y auditabilidad ofrecidas por el sistema propuesto contribuyen significativamente a fomentar la confianza ciudadana en la gestión de sus datos personales. Por otro lado, la arquitectura modular del sistema no solo facilita la escalabilidad, sino que también permite integrar nuevos módulos o adaptarse a regulaciones adicionales sin comprometer el rendimiento general, consolidando su potencial como solución adaptable y robusta.

A pesar de estos avances, el sistema presenta ciertas limitaciones que deben ser consideradas. En primer lugar, el despliegue en una red principal como Avalanche implica costos iniciales elevados, especialmente relacionados con las tarifas de transacción, lo que podría representar una barrera económica para algunas organizaciones. Asimismo, la adopción de Blockchain en entornos tradicionales enfrenta una curva de aprendizaje pronunciada, ya que requiere capacitación especializada para los equipos involucrados. Desde una perspectiva técnica, aunque los tiempos de respuesta del sistema son aceptables, aún presentan una desventaja frente a sistemas centralizados que ofrecen menores latencias, lo cual podría ser determinante en aplicaciones donde la velocidad sea un factor crítico.

Con base en estas limitaciones, se proponen diversas recomendaciones para futuras investigaciones. Una línea de acción importante es la exploración de otras redes Blockchain, como Ethereum o Polkadot, con el objetivo de comparar su rendimiento y costos con Avalanche e identificar alternativas más eficientes. También sería valioso ampliar el alcance del sistema mediante la incorporación de módulos que integren sistemas de identidad digital descentralizada (DID), permitiendo una mayor versatilidad en su aplicación. Finalmente, se sugiere realizar un análisis exhaustivo de la experiencia del usuario para evaluar su percepción respecto a la transparencia y seguridad del sistema, lo cual aportaría insights clave para mejorar la adopción y aceptación de esta tecnología en el futuro.

Conclusiones

La presente investigación ha demostrado la viabilidad y efectividad de utilizar tecnología Blockchain, particularmente la red Avalanche, para garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador. A través del desarrollo de un prototipo funcional, se logró cumplir con los objetivos planteados, destacándose hallazgos relevantes en términos de seguridad, transparencia, viabilidad operativa y cumplimiento legal. En cuanto a la seguridad y confidencialidad, el sistema propuesto implementa cifrado AES para garantizar la protección de los datos personales antes de su almacenamiento en la Blockchain, cumpliendo con los requisitos normativos de confidencialidad. Asimismo, la inmutabilidad de la Blockchain permite registrar cada transacción de manera verificable, asegurando la transparencia en el manejo de datos y fomentando la confianza entre los usuarios y las organizaciones.

Por otro lado, se comprobó la viabilidad operativa del sistema gracias a su arquitectura modular y el uso de herramientas como Docker y Flask, las cuales facilitaron tanto la replicación como la escalabilidad, posicionando esta solución como una alternativa técnica sólida para cumplir con la LOPDP. Además, la solución aborda las principales exigencias de esta normativa, incluyendo el consentimiento informado y la protección de los derechos de los titulares, estableciendo un precedente importante para la adopción de tecnologías emergentes en el ámbito del cumplimiento normativo.

En términos prácticos, el sistema propuesto brinda una solución tangible para las organizaciones que buscan alinearse con normativas de protección de datos en un entorno digital. Su diseño escalable también lo hace adaptable a futuros cambios regulatorios, garantizando su aplicabilidad a largo plazo. Desde una perspectiva teórica, este estudio contribuye al campo de la tecnología Blockchain al validar su uso en contextos regulatorios, ofreciendo un modelo replicable para países o regiones con marcos legales similares.

Finalmente, las perspectivas futuras del sistema incluyen la ampliación de funcionalidades, como la incorporación de módulos de identidad digital descentralizada para extender el alcance del sistema. También se plantea la posibilidad de realizar estudios comparativos entre Avalanche y otras redes Blockchain para evaluar su eficiencia, escalabilidad y costos. Además, sería valioso investigar la percepción de los usuarios finales sobre la transparencia y seguridad del sistema, así como su disposición para adoptar tecnologías similares. La adopción de Blockchain para la protección de datos personales representa una oportunidad única para garantizar la transparencia y seguridad en la gestión de información sensible, y la solución presentada no solo cumple con los requisitos legales, sino que también sienta una base técnica robusta para futuras expansiones.

Referencias bibliográficas

Avalanche. (2021). Avalanche documentation. Recuperado de https://docs.avax.network

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Recuperado de https://www.asambleanacional.gob.ec

Blockchain Council. (2021). Blockchain for GDPR compliance. Recuperado de https://www.Blockchain-council.org

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de https://bitcoin.org/bitcoin.pdf

Python Software Foundation. (2022). PyCryptodome documentation. Recuperado de https://pycryptodome.readthedocs.io

Solidity Documentation. (2023). Solidity language documentation. Recuperado de https://docs.soliditylang.org

Web3.py Documentation. (2023). A Python library for interacting with Ethereum. Recuperado de https://web3py.readthedocs.io

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Nota:

El artículo no es producto de una publicación anterior.