



BLOCKCHAIN Y PROTECCIÓN DE DATOS PERSONALES

Yanet Gutiérrez Juárez

Instituto Politécnico Nacional, UPIICSA
ygutierrezj2500@alumno.ipn.mx

Claudia Marina Vicario Solórzano

Instituto Politécnico Nacional, UPIICSA
cvicario@ipn.mx

Abstract

La tecnología blockchain ha estado activa desde 2009, ha evolucionado de soporte para criptomonedas a una infraestructura descentralizada que garantiza seguridad e inmutabilidad. Este ensayo analiza cómo la integración de criptografía y teoría de juegos permite prescindir de intermediarios, transformando sectores como la logística, salud y gobernanza. Se explora especialmente su impacto en la protección de datos personales y la Identidad Digital Soberana, proponiendo arquitecturas híbridas (almacenamiento off-chain y registros on-chain) para armonizar la tecnología con regulaciones legales. Finalmente, se destaca el papel de los Datos (Organizaciones Autónomas Descentralizadas) y la sinergia con la IA frente a la ciberdelincuencia, posicionando a blockchain como el estándar global para la privacidad y transparencia en la sociedad digital actual."

Palabras clave: Blockchain, protección de datos personales, identidad digital soberana, arquitectura híbrida, ciberdelincuencia, contratos inteligentes, descentralización.

La tecnología Blockchain, ha estado activa desde 2009 y se ha consolidado como un sistema descentralizado y distribuido que garantiza la seguridad e inmutabilidad de los datos mediante la combinación de criptografía, teoría de juegos y ciencias de la computación. Sus características fundamentales: inmutabilidad, descentralización y eficiencia eliminan la necesidad de intermediarios y crean un ambiente confiable entre participantes que no necesariamente confían entre sí.

Aunque la aplicación inicial del Blockchain fue en las criptomonedas como Bitcoin, ha evolucionado para transformar sectores como la salud, la logística, la educación y la administración pública a través de contratos inteligentes y la gestión segura de datos.

Un área de impacto crucial es la protección de datos personales, donde Blockchain permite la creación de una identidad digital soberana, usando criptografía, logrando que los usuarios mantengan el control absoluto sobre su información. Para alinear esta tecnología con los marcos legales de privacidad, como el derecho al olvido, se ha adoptado una arquitectura híbrida: los datos sensibles se



almacenan fuera de la cadena (off-chain), mientras que la cadena de bloques registra únicamente las huellas criptográficas (hashes) y los rastros de consentimiento. Este enfoque, que se está convirtiendo en una tendencia global, posiciona a Blockchain como una herramienta estratégica y robusta frente a la ciberdelincuencia, protegiendo la propiedad intelectual a través de Organizaciones Autónomas Descentralizadas (DAOs) y asegurando la integridad de la información en ecosistemas digitales críticos.

En dicho contexto el propósito central de esta contribución es el análisis del blockchain en la protección de datos personales y la construcción de identidades digitales de carácter soberano, desde una perspectiva tecnológica interdisciplinaria, considerado para ello aspectos técnicos, jurídicos y ciberseguridad.

Blockchain

Blockchain no solo ha estado vigente desde principios del año 2009 ha ido tomando un papel importante en los sectores: salud y público, en la gobernanza, así como en la propiedad digital.

Al combinar sus características criptográficas con funciones matemáticas y su estructura descentralizada garantiza la seguridad y la inmutabilidad de los datos (Obregon et al., 2025).

De acuerdo con Sánchez et al., (2023) Blockchain tiene como base la criptografía para mantener la seguridad de las transacciones, teoría de juegos para alcanzar un consenso entre los participantes y ciencias de la computación para llevar todos los conceptos a una aplicación

La tecnología Blockchain o cadena de bloques, es un conjunto de tecnologías que se comporta como un sistema descentralizado y distribuido; en otras palabras permite crear redes entre personas, utilizando sus propios dispositivos, sin depender de una entidad central, por ello se conoce como descentralizada, los dispositivos realizan un mecanismo de consenso para validar transacciones a través de un software que una vez instalado en un dispositivo, descarga toda la cadena de bloques y replica todo el registro en la red lo que garantiza la inmutabilidad de la misma (Llamas Covarrubias, 2021).

La versión moderna de Blockchain fue diseñada en 2008 por una entidad anónima bajo el seudónimo Satoshi Nakamoto. Su primera aplicación práctica ocurrió en 2009 con el lanzamiento de la criptomoneda Bitcoin, además resolvió el problema del “doble gasto” ya que evitó que los datos digitales se replicaran de forma ilegal con el mismo activo (Guaña-Moya et al., 2022).

Con el tiempo evolucionó a Blockchain 2.0 y permitió su aplicación a los contratos inteligentes, convirtiéndose en una herramienta de confianza que ayudan a la determinación real y aproximada de la población de un territorio considerando la implementación de políticas estatales financieras y públicas (Ohlagaray, 2022).

Blockchain opera mediante un ciclo de validación constante Llamas Covarrubias, (2021), describe esta validación a través de una transacción que sucede al iniciarse un movimiento de datos o activos que se agrupan en un bloque, para que el bloque se agregue a la cadena, los nodos deben alcanzar un acuerdo mediante un algoritmo de consenso, después el nuevo bloque se sella con una marca de tiempo y se une al bloque previo formando una estructura cronológica ininterrumpida, cada usuario posee una llave



pública que funciona como el identificador en la red y una llave privada o contraseña secreta lo que garantiza que solo el propietario pueda acceder o autorizar movimientos sobre sus activos, esto último hace referencia a la criptografía asimétrica.

Por otro lado Santos et al.(2023) nos comparte los usos de Blockchain ya que no solo se utiliza en las criptomonedas, actualmente su aplicación está presente en la educación verificando diplomas, la salud gestionando historiales médicos seguros, la logística para tener una trazabilidad de los suministros y la gestión pública en sistemas de votación y transparencia administrativa.

Características del Blockchain

Blockchain ofrece técnicas avanzadas para la seguridad y el control en la gestión de la información personal sin embargo a su vez genera desafíos en la legislación de la privacidad.

El impacto es la creación de un sistema descentralizado lo que permite establecer un consenso confiable y seguro sobre las transacciones compartidas aun cuando los participantes no confían entre sí (Santos et al., 2023), al no ser obligatoria la necesidad de tener intermediarios o una autoridad central de control reduce el índice de desconfianza entre entidades (Guaña-Moya et al., 2022).

Las características principales de la tecnología Blockchain son:

Inmutabilidad: Es la principal fortaleza del Blockchain ya que garantiza que la información, una vez registrada no pueda ser eliminada ni modificada. Según Guaña-Moya et al.,(2022) cada bloque está enlazado mediante un hash criptográfico lo que hace que cualquier modificación sea técnicamente imposible.

Descentralización y Resiliencia: Blockchain “elimina los puntos únicos de falla”(García-Munguía et al., 2022) porque al usar una arquitectura distribuida refuerza la seguridad haciendo teóricamente imposible que un atacante altere los datos ya que forzosamente se vería en la necesidad de controlar la mayoría de los nodos haciendo esta característica valiosa al proteger a los sistemas de ataques centralizados que impactan comúnmente a bancos y al gobierno.

Eficiencia: La seguridad del Blockchain es sin intermediarios ,no depende de una entidad humana, si no de algoritmos matemáticos (Luján et al., 2025) que son resultados de la combinación de firmas digitales y hashes protegiendo incluso los dispositivos del internet de las cosas (IoT) reduciendo la vulnerabilidad intrínseca.

Gracias a estas características, Blockchain se posiciona como una tecnología que empezó a romper paradigmas y además tiene un alto potencial para transformar sectores como los pagos, la ciberseguridad y la salud.

Blockchain y la protección de datos

Proteger los datos personales resulta fundamental para hacer universal el derecho a la identidad Blockchain utiliza un sistema de criptografía asimétrica basado en llaves públicas y privadas por tanto el usuario es el único dueño de su llave privada, la cual es necesaria para descifrar la información o autorizar transacciones, lo que da confidencialidad y el control total sobre quién accede a sus datos (Beck et al., 2023).

De este modo, la tecnología se constituye como un registro inalterable de autorizaciones y movimientos que, al apoyarse en una arquitectura distribuida y contratos inteligentes, neutraliza las amenazas externas,



pues cualquier vulneración del sistema exigiría el control simultáneo de la mayor parte de los nodos de la red (Hancoo Quispe et al., 2022). En este entorno, el usuario mantiene el control soberano de sus datos a través de carteras digitales que permiten la identificación irrefutable sin revelar información innecesaria, superando así los riesgos del anonimato y la centralización (Martínez Boada & Santamaría Ramos, 2024).

Recordemos que Blockchain actúa como una "bitácora inmutable" que registra eventos críticos como el consentimiento del usuario, accesos y actualizaciones de datos. Al ser una red descentralizada, hace que el hackeo sea casi imposible, ya que requeriría comprometer la mayoría de los nodos de la red (Pezzo & Elizabeth, 2025). Esta soberanía digital permite que administraciones públicas desarrollen modelos de identidad digital soberana, donde el ciudadano gestiona su información sin depender de bases de datos gubernamentales centralizadas vulnerables (Flores, 2024).

Sin embargo, Blockchain debe cumplir con los marcos legales y por ello es necesario adoptar una arquitectura híbrida es decir mientras que los datos personales sensibles se almacenan de forma externa (off-chain) para permitir el ejercicio del derecho al olvido, el Blockchain registra únicamente la huella digital criptográfica (hash) y el rastro de consentimiento (Montaño-Rivera et al., 2025). Complementariamente, el uso de cadenas privadas y funciones de autodestrucción de datos permite resolver los vacíos normativos sobre la responsabilidad del tratamiento en redes descentralizadas (Finck, 2018).

Esta estructura híbrida que combina hashes con almacenamiento externo no representa un iniciativa aislada; tal como indican Antoniucci et al. (2024), es ya una tendencia global en la que regiones como la Unión Europea y

diversos países de América Latina procuran conciliar la innovación tecnológica con una sólida protección de datos. Investigaciones recientes sobre tendencias globales en seguridad informática confirman que la privacidad y la integridad de los datos son las variables de mayor relevancia en el desarrollo de la tecnología Blockchain, consolidando el uso de firmas digitales y protocolos de autenticación avanzada como herramientas esenciales para la protección de la información en entornos descentralizados (Rueda-Castañeda et al., 2024)

Así, la adopción de Blockchain deja de ser una mera solución técnica y puede transformarse en un estándar internacional de seguridad de la información, en el que la automatización de las normas de privacidad a través de contratos inteligentes asegura que la confianza repose no en instituciones, sino en algoritmos verificables, auditables y altamente resilientes.

Autores e Instituciones de Afiliación

Los nombres de los autores deben centrarse con respecto al título, utilizando un tipo Times New Roman de 12 puntos; cuando se trate de varios autores deben mostrarse en un formato de una columna, con sus instituciones de afiliación en itálicas y centradas debajo del nombre correspondiente; de ser posible debe incluirse el correo electrónico. Posteriormente se coloca un espacio de dos líneas en 12 puntos.

Desafíos ante la ciberdelincuencia

Es importante considerar implementar Blockchain como una medida robusta frente a la ciberdelincuencia dado que estos ataques afectan la continuidad operativa reflejando pérdidas millonarias (Mecias et al., 2024), en este contexto Blockchain representa una



herramienta pedagógica para fortalecer los archivos institucionales y promover una mentalidad anticipada para reducir la exposición a riesgos comunes (García-Rojas et al., 2023).

El surgimiento de organizaciones autónomas descentralizadas (DAOs) introduce un modelo innovador de gobernanza que salvaguarda la propiedad intelectual en espacios virtuales trascendiendo barreras jurisdiccionales tradicionales (Galvis Torres, 2025) facilitando el uso de llaves y activos digitales lo que se empieza a usar en la protección de derechos de autor y marcas contra falsificaciones (Sánchez et al., 2023).

No obstante, esta tecnología demanda una ética de privacidad proactiva, reconociendo que la huella digital es un rastro omnipresente y una obligación colectiva entre gobiernos y ciudadanos para mitigar riesgos como la vigilancia masiva o el robo de identidad (Sánchez et al., 2023)

Finalmente, Big Data y Blockchain propicia un ecosistema seguro para sectores críticos como la salud digital, donde el manejo anónimo y el almacenamiento distribuido garantizan la legalidad en el intercambio de información sensible (Pérez Campillo, 2019).

Su aplicación en el arbitraje asegura, además, que la confidencialidad y la transparencia coexistan mediante la ejecución automatizada y ética de acuerdos (Pérez-Pacheco & Lee, 2025) Así, el sistema asegura la validez jurídica y técnica ante los retos de una sociedad digitalizada, global y responsable.

Conclusión

La tecnología Blockchain se ha consolidado desde 2009, se ha convertido en una infraestructura descentralizada que rediseña la seguridad digital mediante sus características de inmutabilidad, resiliencia distribuida y eficiencia algorítmica. Además, desplaza la confianza desde las instituciones centralizadas hacia algoritmos auditables, esta tecnología no solo resolvió desafíos históricos como el "doble gasto", sino que introduce el concepto de identidad digital soberana donde el usuario recupera el control absoluto sobre su información personal, permitiendo que sectores como la salud, la logística y la gobernanza pública operen bajo un esquema de transparencia y ética digital sin precedentes.

Para cumplir con el marco legal vigente, ha adoptado arquitecturas híbridas se presenta como la solución definitiva para conciliar la inmutabilidad técnica con el derecho al olvido.

Blockchain no es solo una herramienta que rompe paradigmas tradicionales, sino que es una herramienta para la construcción de una sociedad global donde la privacidad y la integridad de los datos sean derechos universales, protegidos por una infraestructura tecnológica robusta y responsable.

Referencias

- Antoniucci, A., Sierra Alemán, M. R., Báez, J., & Crisafulli, M. (2024). Blockchain y la



- seguridad de la información en América y Europa. *Informática y Derecho: Revista Iberoamericana de Derecho Informático (segunda época)*, 15, 137–153. <https://dialnet.unirioja.es/servlet/articulo?codigo=9870498>
- Beck, C., Manzoni Boff, M., & Covatti Piaia, T. (2023). Blockchain-id: A construção de uma identidade digital baseada na tecnologia blockchain para garantir a universalização do direito à identidade. *Revista Brasileira de Direito*, 18(3), 4792. <https://doi.org/10.18256/2238-0604.2022.v18i3.4792>
- Finck, M. (2018). Blockchains: Regulating the Unknown. *German Law Journal*, 19(4), 665–692. <https://doi.org/10.1017/S2071832200022847>
- Flores, C. V. (2024). Blockchain e identidad. Oportunidades de implementación para la Ley de Ciudadanía Digital de la Ciudad de México. *Estudios en Derecho a la Información*, 155–177. <https://doi.org/10.22201/ijj.25940082e.2024.18.18888>
- Galvis Torres, K. V. (2025). *Organizaciones autónomas descentralizadas (Daos) blockchain y protección de la propiedad intelectual en el metaverso*. <https://hdl.handle.net/20.500.12494/58754>
- García-Munguía, M., Molina-Ruiz, H. D., Moreno-Gutiérrez, S. S., & Alvarado-Reséndiz, J. L. (2022). Blockchain y la ciberseguridad. *TEPEXI Boletín Científico de la Escuela Superior Tepeji del Río*, 9(18), 15–20. <https://doi.org/10.29057/estr.v9i18.8695>
- García-Rojas, J., Vargas-Vega, T. de J., Rodríguez-Aguilar, R., & Landeros-Valenzuela, K. (2023). *Tecnología educativa de blockchain para prevenir ciberataques en ITSOEH | 593 Digital Publisher CEIT*. https://www.593dp.com/index.php/593_Digital_Publisher/article/view/1702
- Guaña-Moya, J., Roa, H. N., Marcillo, F., Ayavaca-Vallejo, L., Chiluisa-Chiluisa, M., & Moya-Carrera, B. (2022).



- Tecnología Blockchain, qué es y cómo funciona.* *Innovation and Software*, 6(1), 103–114.
<https://doi.org/10.48168/innosoft.s23.a19>
- Hancoo Quispe, J. K., Borda Colque, J. P., Ticona Salluca, H., Torres-Cruz, F., Mamani Luque, O. M., Supo Gutierrez, J. A., Aleman Gonzales, L. L., & Laura Murillo, R. P. (2022). ADOPCIÓN DE ESTRATEGIAS DE CIBERSEGURIDAD PARA LA BLOCKCHAIN. En *Fake News: Objetividade e subjetividade na era da pós-verdade* (1a ed., pp. 10–26). Editora Científica Digital.
<https://doi.org/10.37885/230312490>
- Llamas Covarrubias, J. Z. (2021). Transparencia y protección de datos personales en la cadena de bloques (blockchain). *Estudios en derecho a la información*, 11 (Enero-junio 2021), 27–63.
<https://dialnet.unirioja.es/servlet/articulo?codigo=7751091>
- Luján, J. A. Y., Rengifo, M. A. L., & Santos, A. C. M. de los. (2025). Criptografía y Blockchain en el Internet de las Cosas: Protección de Datos a través de Tecnologías Descentralizadas. *Innovation and Software*, 6(1), 103–114.
<https://doi.org/10.48168/innosoft.s23.a19>
- Martínez Boada, J., & Santamaría Ramos, F. J. (2024). Blockchain: La nueva era de la identificación digital en internet. *Teoría & Derecho. Revista de pensamiento jurídico*, 37, 258–283.
<https://doi.org/10.36151/TD.2024.114>
- Mecias, C. J. B., Cabello, Y. K. J., Mueses, L. M. S., & Paredes, A. G. R. (2024). La ciberdelincuencia y la protección de datos personales. *Sinergia Académica*, 7(Especial 5), 594–612.
<https://doi.org/10.51736/sjq7b043>
- Montaño-Rivera, C. J., Andrade-Paredes, R. O., & Cuenca--Tapia, J. P. (2025). Aplicación Blockchain para cumplir la Ley de Protección de Datos Personales en Ecuador. *MQRInvestigar*, 9(1), e67–e67.
<https://doi.org/10.56048/MQR20225.9.1.2025.e67>
- Obregon, J. M. H., Haro, M. L. G., & Santos, A. M. de L. (2025). Identificando Tecnologías Blockchain para la Protección de Información Sensible en



- Redes Sociales: Una Revisión
Sistemática. *Innovation and Software*,
6(1), 6–23.
<https://doi.org/10.48168/innosoft.s23.a197>
- Ohlagaray, R. M. (2022). Diseño de
procedimientos de gestión de conflictos
sustentados en las tecnologías de
blockchain. *IUS ET VERITAS*, 64, 228–
249.
<https://doi.org/10.18800/iusetveritas.202201.013>
- Pérez-Pacheco, Y., & Lee, D. B. (2025). Impacto
de las tecnologías emergentes en la
confidencialidad y transparencia del
arbitraje internacional. *Jurídica Ibero.
Revista Semestral del Departamento de
Derecho de la Universidad
Iberoamericana*, 19, 77–96.
<https://doi.org/10.48102/ji.19.314>
- Pezzo, O. D., & Elizabeth, P. (2025). *Análisis de
protección de datos personales con
sistemas de Big Data y Blockchain*
[masterThesis, Quito: Universidad de las
Américas, 2025].
- <http://dspace.udla.edu.ec/handle/33000/17651>
- Rueda-Castañeda, J. E., Gallego-Gómez, N.,
Estanling-Cárdenas, E., Tello, J. S., &
García-Pineda, V. (2024). Identificación
de variables relacionadas a la seguridad
informática a partir de tendencias
investigativas de la tecnología
Blockchain. *Revista Politécnica*, 20(40),
09–29.
<https://doi.org/10.33571/rpolitec.v20n40a1>
- Sánchez, P. A. V., Obando, J. G., & Echeverry, A.
M. L. (2023). Elementos de Seguridad
para Gestión Documental con
Blockchain. *Entre Ciencia e Ingeniería*,
17(34), 36–42.
<https://doi.org/10.31908/19098367.2667>
- Santos, L. C. V. de los, Alarcón, R. B., Martínez,
Á. Z., & Aguiñaga, M. A. V. (2023).
Blockchain: Una tecnología que
revolucionará la seguridad y la
transparencia en la era digital. *UCE
Ciencia. Revista de postgrado*, 11(3).
<https://uceciencia.edu.do/index.php/OJS/article/view/341>



Notas de los autores

Los autores del presente artículo Yanet Gutiérrez Juárez <https://orcid.org/0009-0003-6272-184X> y Claudia Marina Vicario Solórzano <https://orcid.org/0000-0003-0144-3607>, agradecen y dan crédito al Instituto Politécnico Nacional (IPN) por el apoyo brindado a través de

la Maestría de Informática de la UPIICSA para la realización de la contribución y a la Secretaría de Investigación y Posgrado (SIP) del IPN el apoyo financiero recibido a través del proyecto 20254760. .