The Double Edge of Absolute Trust: The Ethical Paradox of Blockchain

El Doble Filo de la Confianza Absoluta: La Paradoja Ética de Blockchain

Diginomics.
2025; 4:150
DOI: 10.56294/digi2025150
ISSN: 3072-8428

José Martin Leonardo Marquez Vaamonde[1]

[1]Universidad Nacional Experimental de las Telecomunicaciones y la Informática, Decanato de Estudios De Tecnologías Emergentes, Caracas, Venezuela.

Citar como: Marquez Vaamonde JML. The Double Edge of Absolute Trust: The Ethical Paradox of Blockchain. Diginomics. 2025; 4:150. https://doi.org/10.56294/digi2025150

Autor para la correspondencia: José Martin Leonardo Marquez Vaamonde

ABSTRACT

Introduction: the study examined blockchain technology as a pillar of Web3, highlighting its principles of immutability, transparency, and decentralization. It analyzed the paradox that these same virtues could become disadvantages when it was necessary to correct errors, delete data, or deal with malicious uses, generating legal and ethical tensions.

Development: cases and studies were reviewed that showed how immutability guaranteed integrity and resistance to censorship but was incompatible with rights such as the "right to be forgotten" under the GDPR. Situations were also documented in which decentralization empowered both legitimate actors and criminals, eliminating consumer protection mechanisms.

Faced with these dilemmas, solutions such as off-chain storage, updatable smart contracts, decentralized identity, and zero-knowledge proofs were evaluated. The proposal for double validation was highlighted, which incorporated a layer of smart contract verification to authenticate the origin and legitimacy of information before it was recorded. The validation of sensitive content by the people involved was also proposed as a strategy to prevent defamation, misinformation, or the dissemination of illegal material.

Conclusion: the paper concluded that the potential of blockchain lay in its integration within an ethical, legal, and social framework. The implementation of mandatory verification and validation mechanisms strengthened accountability and individual protection, transforming blockchain into a tool that is not only secure and transparent, but also fair and socially responsible.

Keywords: Blockchain**;** Immutability; Decentralization; Technological Ethics; Validation.

RESUMEN

Introducción: el estudio examinó la tecnología blockchain como pilar de la Web3, resaltando sus principios de inmutabilidad, transparencia y descentralización. Se analizó la paradoja de que estas mismas virtudes podían transformarse en desventajas cuando era necesario corregir errores, eliminar datos o enfrentar usos maliciosos, generando tensiones legales y éticas.

Desarrollo: se revisaron casos y estudios que evidenciaron cómo la inmutabilidad garantizaba integridad y resistencia a la censura, pero resultaba incompatible con derechos como el "derecho al olvido" del GDPR. También se documentaron situaciones en las que la descentralización empoderó tanto a actores legítimos como a criminales, eliminando mecanismos de protección al consumidor. Frente a estos dilemas, se evaluaron soluciones como almacenamiento off-chain, contratos inteligentes actualizables, identidad descentralizada y pruebas de conocimiento cero. Se destacó la propuesta de una doble validación, que incorporaba una capa de verificación contractual inteligente para autenticar el origen y la legitimidad de la información antes de su registro. Asimismo, se planteó la validación de contenido sensible por parte de las personas implicadas, como estrategia para prevenir difamación, desinformación o la difusión de material ilícito.

Conclusión: el trabajo concluyó que el potencial de blockchain residía en su integración dentro de un marco ético, legal y social. La implementación de mecanismos de verificación y validación obligatoria fortaleció la responsabilidad y la protección del individuo, transformando la blockchain en una herramienta no solo segura y transparente, sino también justa y socialmente responsable.

Palabras clave: Blockchain; Inmutabilidad; Descentralización; Ética Tecnológica; Validación.

Enviado: 02-06-2024 **Revisado:** 10-09-2024 **Aceptado:** 21-12-2024 **Publicado:** 01-01-2025

INTRODUCCIÓN

La promesa y la paradoja de una nueva arquitectura digital

En el corazón de la revolución digital del siglo XXI, la tecnología *blockchain* ha emergido como uno de los pilares fundamentales de la Web3, presentándose como una solución disruptiva para restaurar la confianza en un ecosistema digital cada vez más fragmentado, centralizado y vulnerable.[1,2] Su arquitectura se basa en tres principios fundamentales: inmutabilidad, transparencia y descentralización, que prometen un nuevo paradigma donde la confianza no depende de instituciones intermediarias, sino de la criptografía y el consenso distribuido.[3]

Sin embargo, como señalan De Filippi y Wright[4], esta arquitectura, aunque matemáticamente robusta, entra en conflicto con las complejidades del entorno social, legal y ético en el que opera. Es aquí donde se manifiesta la tesis central de este ensayo: la confianza generada por la inmutabilidad y transparencia de la cadena de bloques se convierte en una desventaja cuando se requiere corregir errores o eliminar datos, y el empoderamiento derivado de la descentralización puede ser aprovechado tanto por actores legítimos como maliciosos. Esta dualidad no es un fallo técnico, sino una paradoja inherente que plantea dilemas éticos profundos sobre el diseño, la gobernanza y la responsabilidad en los sistemas tecnológicos.

El paradigma de la confianza permanente: Inmutabilidad vs. falibilidad humana

La inmutabilidad es considerada la piedra angular de la confianza en *blockchain*. Una vez que una transacción es validada y agregada a la cadena, no puede ser alterada sin invalidar toda la cadena posterior.[5] Esta característica garantiza integridad y resistencia a la censura, lo que la hace ideal para aplicaciones en finanzas, cadenas de suministro y registros de propiedad.[6]

No obstante, como advierte Werbach[7], esta rigidez choca frontalmente con la falibilidad humana. Errores simples —como una transacción mal dirigida o un registro con datos incorrectos— quedan grabados permanentemente, sin posibilidad de corrección. En un sistema tradicional, existen mecanismos de reversión y arbitraje; en una *blockchain* pública, el principio de "código es ley" (*code is law*) elimina tales recursos.

Este dilema se agrava cuando se consideran los derechos fundamentales de protección de datos. El derecho al olvido, establecido en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, exige que los individuos puedan solicitar la eliminación de sus datos personales. Sin embargo, la inmutabilidad de *blockchain* es incompatible con esta exigencia legal. Como señalan Finck y Pallas[8], "una tecnología que no puede olvidar no puede cumplir con un derecho que exige olvidar". Esta colisión entre tecnología y derecho representa un desafío estructural para la adopción legal de *blockchain* en contextos sensibles.

Peor aún, la inmutabilidad puede convertirse en una herramienta de opresión cuando se utilizan cadenas para registrar información difamatoria, secreta o ilegal. Un caso emblemático es el de la publicación de contenido de "porno venganza" en transacciones públicas, donde la víctima queda marcada permanentemente en un registro global e inmutable.[9] En este sentido, la confianza absoluta se transforma en una prisión digital, evidenciando que la seguridad técnica no implica justicia social.

El empoderamiento desatado: El doble filo de la descentralización

La descentralización es la promesa ideológica más poderosa de *blockchain*. Al eliminar intermediarios, se redistribuye el poder desde instituciones centralizadas hacia los usuarios individuales.[4,10] Este principio ha dado lugar a innovaciones como las Finanzas Descentralizadas (DeFi) y las Organizaciones Autónomas Descentralizadas (DAOs), donde las comunidades toman decisiones mediante votaciones codificadas y contratos inteligentes.[11,12]

Sin embargo, como advierte Sandvig[13], la ausencia de autoridad central no elimina el poder; lo redistribuye, a menudo hacia actores que lo utilizan de forma opaca o maliciosa. El anonimato relativo (más precisamente, el seudonimato) facilita actividades ilícitas como el lavado de dinero, el financiamiento del terrorismo y el comercio en mercados oscuros como *Silk Road*.[14] El caso de Tornado Cash, un mezclador de criptomonedas sancionado por el Departamento del Tesoro de EE. UU. en 2022 por facilitar el lavado de fondos de hackers norcoreanos, ilustra cómo herramientas técnicamente neutrales pueden ser instrumentalizadas para el crimen.[15]

Además, la descentralización elimina los mecanismos de protección al consumidor. En el sistema financiero tradicional, los bancos y reguladores ofrecen garantías contra fraudes y errores. En DeFi, la máxima "código es ley" implica que no hay remedio ante errores o estafas. Si un usuario pierde su clave privada o es víctima de un ataque de *phishing*, sus activos se pierden irremediablemente.[16] Esta ausencia de recurso crea un entorno de alto riesgo que excluye a los usuarios no expertos, contradiciendo la promesa de inclusión financiera.

Como argumenta Zittrain[17], la libertad tecnológica sin responsabilidad institucional puede derivar en anarquía funcional, donde los más técnicos o ricos dominan a los demás. La descentralización, en este sentido, no garantiza equidad, sino una nueva forma de desigualdad basada en el conocimiento y el acceso.

DESARROLLO

En busca del equilibrio: Soluciones tentativas y el camino hacia un diseño ético

Frente a estas tensiones, la comunidad tecnológica y los reguladores buscan un equilibrio entre los ideales de *blockchain* y las exigencias del mundo real. A continuación, se presentan soluciones emergentes, analizadas desde una perspectiva crítica.

A. Abordando la inmutabilidad: Flexibilidad sin traicionar la integridad

1. Bifurcaciones (forks) y gobernanza colectiva: Tras el hackeo de *The DAO* en 2016, la comunidad de Ethereum decidió realizar una bifurcación dura para revertir las transacciones afectadas.[18] Aunque efectiva, esta acción generó una división (Ethereum vs. Ethereum Classic) y demostró que la inmutabilidad puede ser socavada por decisiones sociales. Como señala Swanson[19], "la cadena es inmutable hasta que no lo es", lo que revela una paradoja política en el corazón de la tecnología.
2. Almacenamiento off-chain: Una estrategia común es almacenar datos sensibles fuera de la cadena y solo registrar su *hash* criptográfico en la *blockchain*.[9] Esto permite cumplir con el GDPR, pero reintroduce

puntos centralizados de fallo. Como advierte Benet[20] con IPFS, estos sistemas híbridos requieren una arquitectura cuidadosa para no comprometer la seguridad.

3. Contratos inteligentes actualizables: Permitir actualizaciones bajo condiciones predefinidas ofrece flexibilidad, pero introduce vulnerabilidades. Como demostró el hackeo de Parity Wallet en 2017, una "puerta trasera" bien intencionada puede ser explotada.[21]

B. Domesticando la descentralización: Privacidad, regulación y reputación

1. Regulación (KYC/AML): Gobiernos imponen obligaciones de "Conozca a su Cliente" a exchanges, lo que mejora el cumplimiento, pero contradice el ideal de privacidad.[22] Como señala Lessig[23], el código es una forma de regulación; ahora, el Estado regula el código.

2. Pruebas de conocimiento cero (ZKPs): Tecnologías como zk-SNARKs permiten verificar transacciones sin revelar datos.[24] Esto abre la posibilidad de cumplir con AML sin sacrificar la privacidad, aunque su complejidad limita su adopción masiva.

3. Identidad descentralizada (DID): Los sistemas DID permiten a los usuarios controlar su identidad digital.[25] Combinados con reputación basada en grafos sociales, podrían distinguir actores confiables de maliciosos,[26] aunque el riesgo de sesgos y manipulación persiste.

Blockchain y la Reinvención de la Confianza: Un Camino Hacia un Ecosistema Maduro

El futuro de *blockchain* no reside en la defensa dogmática de sus principios absolutistas —inmutabilidad total, descentralización anárquica—, sino en su capacidad para evolucionar hacia un diseño responsable y adaptable. Como argumenta Floridi[27], la ética de la información debe guiar el desarrollo tecnológico para que sirva al bien común.

La tecnología debe reconocer que la humanidad no es perfecta, y que los sistemas que la sirven deben incluir mecanismos de corrección, recurso y perdón. El verdadero potencial de *blockchain* no se realizará cuando sea completamente inmutable o descentralizado, sino cuando sea lo suficientemente robusto para ser seguro y lo suficientemente sabio para ser humano.

La tecnología blockchain ha sido aclamada como una fuerza transformadora, prometiendo descentralización, inmutabilidad y transparencia. Sin embargo, su camino hacia una adopción masiva y responsable está lleno de desafíos que van más allá de lo técnico. Para que blockchain cumpla su promesa original de ser una herramienta de justicia y empoderamiento, es imperativo que trascendamos la visión utópica y nos enfoquemos en construir un ecosistema maduro que integre la tecnología con principios éticos, legales y sociales.

Este camino hacia la madurez exige un diálogo interdisciplinario. Los ingenieros que construyen los protocolos deben colaborar estrechamente con juristas que establecen los marcos regulatorios, con éticos que guían las decisiones sobre la privacidad y la equidad, y con ciudadanos que son los usuarios finales y los guardianes de la confianza. Solo a través de esta conversación multifacética podemos garantizar que blockchain no se convierta en una caja negra opaca, sino en una herramienta de empoderamiento responsable.

La Doble Validación como Eje de un Sistema Confiable

Una de las propuestas más prometedoras para universalizar la blockchain y mitigar sus riesgos inherentes es la implementación de un sistema de doble validación. Actualmente, la inmutabilidad de los datos y la transparencia son pilares del diseño de blockchain, pero el origen y la veracidad de la información que se registra pueden ser problemáticos. La propuesta de crear una capa de validación contractual inteligente sobre la blockchain es fundamental para abordar esta debilidad.

Esta capa actuaría como un filtro inteligente, verificando la validez y el contexto de la información antes de que se inscribe en la cadena de bloques. La doble validación se aplicaría a las transacciones de la siguiente manera:

- El Iniciador: El proceso comienza cuando un usuario solicita una transacción. Esta persona debe validar su identidad de forma digital, actuando como el punto de inicio de una cadena de confianza.
- El Emisor: La solicitud llega al emisor, quien también debe validar la transacción con su propia identificación digital. Esta segunda validación es crucial para confirmar que ambas partes están de acuerdo con los términos de la transacción.
- La Red Blockchain: Una vez que el emisor ha validado la transacción, esta se difunde en la red. La blockchain, a través de su mecanismo de consenso, valida que la transacción cumple con las reglas del protocolo (por ejemplo, que no hay doble gasto). Solo después de esta triple validación (solicitante, emisor y red), la transacción se registra de forma inmutable.

Este mecanismo de doble validación no solo mantiene la inmutabilidad de la blockchain, sino que también introduce una capa de responsabilidad en el origen de los datos. En lugar de simplemente registrar lo que se le envía, la blockchain se vuelve un participante activo en la verificación de la legitimidad de la información.

Regulación Inteligente de Contenido y la Lucha contra la Desinformación

La inmutabilidad de blockchain es una espada de doble filo. Si bien protege los datos de ser alterados, también puede ser utilizada para perpetuar contenido dañino, como la difamación, la desinformación o incluso la distribución de material ilícito. Para enfrentar este desafío, la blockchain inteligente propuesta no solo validaría las transacciones, sino que también requeriría la validación del contenido por parte de las personas directamente involucradas.

Consideremos un escenario en el que se intenta registrar información que podría ser difamatoria, secreta o ilegal. La blockchain inteligente detendría el proceso y solicitaría la autorización de la persona involucrada de la siguiente manera:

- Material Escrito: Si el contenido es un texto que identifica a una persona (por nombre, identificador digital o cualquier otro dato sensible), la blockchain solicitaría a esa persona una validación con su identificación digital. Esto garantiza que la persona ha dado su consentimiento para que su información se registre y se mantenga en la blockchain, mitigando el riesgo de difamación o robo de identidad.
- Material Audiovisual o Identificatorio: En el caso de fotografías, videos, audios o incluso

descripciones de tatuajes o marcas corporales, el sistema de validación sería similar. El propietario de la imagen, el audio o las características identificatorias tendría que dar su autorización digital antes de que el material pueda ser registrado. Este mecanismo es particularmente relevante para combatir el llamado "porno venganza" y proteger la privacidad y la dignidad de las personas.

Este enfoque no solo reduce al mínimo el registro de contenido dañino, sino que también introduce un mecanismo de rendición de cuentas en la cadena de bloques. Si se registra contenido sin la autorización requerida, la transacción puede ser revertida o, al menos, marcada y penalizada dentro del ecosistema. Esto transforma a la blockchain de una simple base de datos inmutable a un sistema de registros inteligentes y éticos que prioriza la protección del individuo.

CONCLUSIÓN

El verdadero potencial de blockchain no reside en su tecnología, sino en cómo la integramos en un marco social, legal y ético. Un ecosistema maduro no se limita a la descentralización, sino que abarca la responsabilidad, la verificación y la protección del individuo. Al implementar capas de validación inteligentes y obligatorias, podemos transformar la blockchain en una herramienta poderosa para construir una sociedad más justa, transparente y empoderada, donde la confianza no sea una premisa, sino una característica verificable en cada paso.

FINANCIACIÓN

Ninguna.

CONFLICTO DE INTERESES

Los autores declaran que no existe conflicto de intereses.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: José Martin Leonardo Marquez Vaamonde.

Curación de datos: José Martin Leonardo Marquez Vaamonde.

Análisis formal: José Martin Leonardo Marquez Vaamonde.

Investigación: José Martin Leonardo Marquez Vaamonde.

Metodología: José Martin Leonardo Marquez Vaamonde.

Administración del proyecto: José Martin Leonardo Marquez Vaamonde.

Recursos: José Martin Leonardo Marquez Vaamonde.

Software: José Martin Leonardo Marquez Vaamonde.

Supervisión: José Martin Leonardo Marquez Vaamonde.

Validación: José Martin Leonardo Marquez Vaamonde.

Visualización: José Martin Leonardo Marquez Vaamonde.

Redacción – borrador original: José Martin Leonardo Marquez Vaamonde.

Redacción – revisión y edición: José Martin Leonardo Marquez Vaamonde.

REFERENCIAS

1. Bernal Aragón AJ. Impacto de la tecnología blockchain en la auditoría financiera en Colombia. Actas Iberoam Cienc Soc. 2024;2(1):9–26. https://doi.org/10.69821/AICIS.v2i1.18
2. Tapscott D, Tapscott A. Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Nueva York: Penguin; 2016.
3. Suescum Coelho C, Suescum Coelho CE. Sostenibilidad empresarial: descifrando el código para el nuevo estándar en la toma de decisiones. Actas Iberoam Cienc Soc. 2025;3(1):120–36. https://doi.org/10.69821/AICIS.v3i1.84
4. De Filippi P, Wright A. Blockchain and the law: The rule of code. Cambridge: Harvard University Press; 2018.
5. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. Disponible en: https://bitcoin.org/bitcoin.pdf
6. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE Access. 2016;4:2292–303. https://doi.org/10.1109/ACCESS.2016.2566339
7. Werbach K. The blockchain and the new architecture of trust. Cambridge: MIT Press; 2018.
8. Finck M, Pallas F. Data protection and blockchain: A clash of paradigms? Comput Law Secur Rev. 2019;35(3):277–88. https://doi.org/10.1016/j.clsr.2019.03.001
9. Zyskind G, Nathan O, Pentland A. Decentralizing privacy: Using blockchain to protect personal data. IEEE Secur Privacy Workshops. 2015:180–4. https://doi.org/10.1109/SPW.2015.27
10. Millán Tinoco V, Hernández Vargas AD, Aldazaba Jácome G. Indicadores logísticos como medidas de rendimiento para evaluar el desempeño en una cadena de trabajo. Rev Multidiscip Voces Am Carib. 2024;1(2):328–49. https://doi.org/10.69821/REMUVAC.v1i2.97
11. Buterin V. A next-generation smart contract and decentralized application platform. Ethereum White Paper. 2014.
12. Fotă AE, Expósito-Langa M, Tomás-Miquel JV, Maldonado-Gómez G. Dinámicas de innovación en el clúster vitivinícola de Alicante. El rol de la competencia relacional. Rev Multidiscip Voces Am Carib. 2024;1(1):180–99. https://doi.org/10.69821/REMUVAC.v1i1.31
13. Sandvig C. Anonymity, surveillance, and the case for privacy. Daedalus. 2013;142(1):29–39. https://doi.org/10.1162/DAED_a_00187
14. Foley S, Karlsen JR, Putniņš TJ. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Econ J. 2019;129(618):573–604. https://doi.org/10.1111/ecoj.12553
15. U.S. Department of the Treasury. Treasury sanctions cryptocurrency mixer Tornado Cash. 2022. Disponible en: https://home.treasury.gov
16. Cong LW, He Z, Li J. Decentralized finance: On blockchain- and smart contract-based financial markets. Rev Financ Stud. 2021;34(7):3152–90. https://doi.org/10.1093/rfs/hhab027
17. Zittrain J. The future of the Internet and how to stop it. New Haven: Yale University Press; 2008.
18. Voshmgir S. Token economy: How the Web3 reinvents the internet. Viena: Token Kitchen; 2020.
19. Swanson E. The economic fundamentals of Bitcoin. 2015. Disponible en: https://unenumerated.blogspot.com/
20. Benet J. IPFS – Content addressed, versioned, P2P file system. arXiv preprint. 2014. arXiv:1407.3561.
21. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts. Int Conf Principles of Security and Trust. 2017:164–86. https://doi.org/10.1007/978-3-662-54455-6_8
22. Finck M. Blockchain regulation and governance in Europe. Cambridge: Cambridge University Press; 2019.
23. Lessig L. Code and other laws of cyberspace. Nueva York: Basic Books; 1999.
24. Ben-Sasson E, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. Zerocash: Decentralized anonymous payments from Bitcoin. IEEE Symp

Secur Privacy. 2014:459–74. https://doi.org/10.1109/SP.2014.36
25. W3C. Decentralized Identifiers (DIDs) v1.0. 2022. Disponible en: https://www.w3.org/TR/did-core/
26. Back A, Cascaval M, Dorri A. Decentralized reputation management. IEEE P2P Proc. 2014:1–8.
27. Floridi L. The logic of information. Oxford: Oxford University Press; 2019.