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.

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

Corresponding Author: 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.

Submitted: 02-06-2024 **Revised:** 10-09-2024 **Accepted:** 21-12-2024 **Published:** 01-01-2025

INTRODUCTION

The promise and paradox of a new digital architecture

At the heart of the 21st-century digital revolution, *blockchain* technology has emerged as one of the fundamental pillars of Web3, presenting itself as a disruptive solution to restore trust in an increasingly fragmented, centralized, and vulnerable digital ecosystem.[1,2] Its architecture is based on three fundamental principles: immutability, transparency, and decentralization, which promise a new paradigm where trust does not depend on intermediary institutions, but on cryptography and distributed consensus.[3]

However, as De Filippi and Wright[4], this architecture, although mathematically robust, conflicts with the complexities of the social, legal, and ethical environment in which it operates. This is where the central thesis of this essay comes into play: the trust generated by the immutability and transparency of the blockchain becomes a disadvantage when errors need to be corrected or data deleted, and both legitimate and malicious actors can exploit the empowerment derived from decentralization. This duality is not a technical flaw, but an inherent paradox that raises profound ethical dilemmas about the design, governance, and accountability of technological systems.

The paradigm of permanent trust: Immutability vs. human fallibility

Immutability is considered the cornerstone of trust in *blockchain*. Once a transaction is validated and added to the chain, it cannot be altered without invalidating the entire chain that follows.[5] This feature guarantees integrity and resistance to censorship, making it ideal for applications in finance, supply chains, and property records.[6]

However, as Werbach[7] warns, this rigidity clashes head-on with human fallibility. Simple errors—such as a misdirected transaction or a record with incorrect data—are permanently recorded, with no possibility of correction. In a traditional system, there are mechanisms for reversal and arbitration; in a public *blockchain*, the principle of "code is *law"* eliminates such resources.

This dilemma is exacerbated when fundamental data protection rights are considered. The right to be forgotten, established in the European Union's General Data Protection Regulation, requires that individuals be able to request the deletion of their data. However, the immutability of *blockchain* is incompatible with this legal requirement. As Finck and Pallas[8] point out, "a technology that cannot forget cannot comply with a right that requires forgetting." This collision between technology and law represents a structural challenge for the legal adoption of *blockchain* in sensitive contexts.

Worse still, immutability can become a tool of oppression when chains are used to record defamatory, secret, or illegal information. A case in point is the publication of "revenge porn" content in public transactions, where the victim is permanently marked in a global and immutable registry.[9] In this sense, absolute trust becomes a digital prison, showing that technical security does not imply social justice.

Empowerment unleashed: The double-edged sword of decentralization.

Decentralization is *blockchain's* most powerful ideological promise. By eliminating intermediaries, power is redistributed from centralized institutions to individual users.[4,10] This principle has given rise to innovations such as Decentralized Finance (DeFi) and Decentralized Autonomous Organizations (DAOs), where communities make decisions through coded voting and smart contracts.[11,12]

However, as Sandvig[13] warns, the absence of central authority does not eliminate power; it redistributes it, often to actors who use it in opaque or malicious ways. Relative anonymity (more precisely, pseudonymity) facilitates illicit activities such as money laundering, terrorist financing, and trade on dark markets such as *Silk Road*.[14] The case of Tornado Cash, a cryptocurrency mixer sanctioned by the US Treasury Department in 2022 for facilitating the laundering of funds from North Korean hackers, illustrates how technically neutral tools can be instrumentalized for crime.[15]

Furthermore, decentralization eliminates consumer protection mechanisms. In the traditional financial system, banks and regulators offer guarantees against fraud and errors. In DeFi, the maxim "code is law" means that there is no remedy for mistakes or fraud. If a user loses their private key or falls victim to a *phishing* attack, their assets are irretrievably lost.[16] This lack of recourse creates a high-risk environment that excludes non-expert users, contradicting the promise of financial inclusion.

As Zittrain[17] argues, technological freedom without institutional responsibility can lead to functional anarchy, where the most technical or wealthy dominate the rest. Decentralization, in this sense, does not guarantee equity, but rather a new form of inequality based on knowledge and access.

DEVELOPMENT

In search of balance: Tentative solutions and the path to ethical design

Faced with these tensions, the tech community and regulators are seeking a balance between the ideals of *blockchain* and the demands of the real world. Emerging solutions are presented below, analyzed from a critical perspective.

A. Addressing immutability: Flexibility without compromising integrity

1. Forks and collective governance: Following the hacking of *The DAO* in 2016, the Ethereum community decided to perform a hard fork to reverse the affected transactions.[18] Although effective, this action created a split (Ethereum vs. Ethereum Classic) and demonstrated that immutability can be undermined by social decisions. As Swanson[19] points out, "the chain is immutable until it isn't," revealing a political paradox at the heart of the technology.
2. Off-chain storage: A common strategy is to store sensitive data off-chain and only record its cryptographic *hash* on the *blockchain*.[9] This allows compliance with the GDPR, but reintroduces centralized points of failure. As Benet[20] warns with IPFS, these hybrid systems require careful architecture to avoid compromising security.
3. Upgradable smart contracts: Allowing upgrades under predefined conditions offers flexibility but introduces vulnerabilities. As demonstrated by the Parity Wallet hack in 2017, a well-intentioned "back door" can be exploited.[21]

B. Taming decentralization: Privacy, regulation, and reputation

1. Regulation (KYC/AML): Governments impose "Know Your Customer" obligations on exchanges, which improves compliance but contradicts the ideal of privacy.[22] As Lessig[23] points out, code is a form of regulation; now, the state regulates code.

2. Zero-knowledge proofs (ZKPs): Technologies such as zk-SNARKs allow transactions to be verified without revealing data.[24] This opens up the possibility of complying with AML without sacrificing privacy, although its complexity limits its mass adoption.

3. Decentralized identity (DID): DID systems allow users to control their digital identity.[25] Combined with social graph-based reputation, they could distinguish trustworthy actors from malicious ones,[26] although the risk of bias and manipulation persists.

Blockchain and the Reinvention of Trust: A Path Toward a Mature Ecosystem

The future of *blockchain* does not lie in the dogmatic defense of its absolutist principles—total immutability, anarchic decentralization—but in its ability to evolve toward a responsible and adaptable design. As Floridi[27] argues, information ethics must guide technological development so that it serves the common good.

Technology must recognize that humanity is not perfect, and that the systems that serve it must include mechanisms for correction, recourse, and forgiveness. The true potential of *blockchain* will not be realized when it is completely immutable or decentralized, but when it is robust enough to be secure and wise enough to be human.

Blockchain technology has been hailed as a transformative force, promising decentralization, immutability, and transparency. However, its path to mass adoption and responsible use is fraught with challenges that go beyond the technical. For blockchain to fulfill its original promise as a tool for justice and empowerment, we must transcend the utopian vision and focus on building a mature ecosystem that integrates the technology with ethical, legal, and social principles.

This path to maturity requires interdisciplinary dialogue. Engineers building the protocols must collaborate closely with lawyers establishing regulatory frameworks, ethicists guiding decisions about privacy and fairness, and citizens who are the end users and guardians of trust. Only through this multifaceted conversation can we ensure that blockchain does not become an opaque black box, but rather a tool for responsible empowerment.

Double Validation as the Cornerstone of a Reliable System

One of the most promising proposals for universalizing blockchain and mitigating its inherent risks is the implementation of a double validation system. Currently, data immutability and transparency are pillars of blockchain design, but the origin and veracity of the information being recorded can be problematic. The proposal to create a smart contract validation layer on top of the blockchain is fundamental to addressing this weakness.

This layer would act as an intelligent filter, verifying the validity and context of the information before it is recorded on the blockchain. Double validation would be applied to transactions as follows:

- The Initiator: The process begins when a user requests a transaction. This person must digitally validate their identity, acting as the starting point of a chain of trust.
- The Issuer: The request reaches the issuer, who must also validate the transaction with their digital ID. This second validation is crucial to confirm that both parties agree to the terms of the transaction.
- The Blockchain Network: Once the issuer has validated the transaction, it is broadcast across the network. The blockchain, through its consensus mechanism, validates that the transaction complies with the rules of the protocol (e.g., that there is no double spending) only after this triple validation (requester, issuer, and network) is the transaction recorded in an immutable manner.

This double validation mechanism not only maintains the immutability of the blockchain but also introduces a layer of accountability at the source of the data. Rather than simply recording what is sent to it, the blockchain becomes an active participant in verifying the legitimacy of the information.

Smart Content Regulation and the Fight Against Misinformation

The immutability of blockchain is a double-edged sword. While it protects data from being altered, it can also be used to perpetuate harmful content, such as defamation, misinformation, or even the distribution of illicit material. To address this challenge, the proposed innovative blockchain would not only validate transactions but also require content validation by the people directly involved.

Consider a scenario in which someone attempts to record information that could be defamatory, secret, or illegal. The innovative blockchain would halt the process and request authorization from the person involved as follows:

- Written Material: If the content is text that identifies a person (by name, digital identifier, or any other sensitive data), the blockchain would request validation from that person using their digital ID. This ensures that the person has given their consent for their information to be recorded and stored on the blockchain, mitigating the risk of defamation or identity theft.
- Audiovisual or Identifying Material: In the case of photographs, videos, audio recordings, or even descriptions of tattoos or body markings, the validation system would be similar. The owner of the image, audio, or identifying characteristics would have to give their digital authorization before the material can be recorded. This mechanism is particularly relevant for combating so-called "revenge porn" and protecting people's privacy and dignity.

This approach not only minimizes the registration of harmful content but also introduces an accountability mechanism into the blockchain. If content is registered without the required authorization, the transaction can be reversed or, at the very least, flagged and penalized within the ecosystem. This transforms the blockchain from a simple immutable database into a system of competent and ethical records that prioritizes the protection of the individual.

CONCLUSION

The true potential of blockchain does not lie in its

technology, but in how we integrate it into a social, legal, and ethical framework. A mature ecosystem is not limited to decentralization, but encompasses accountability, verification, and protection of the individual. By implementing smart and mandatory validation layers, we can transform blockchain into a powerful tool for building a more just, transparent, and empowered society, where trust is not a premise, but a verifiable characteristic at every step.

FINANCING

None.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHOR CONTRIBUTION

Conceptualization: José Martin Leonardo Marquez Vaamonde.

Data curation: José Martin Leonardo Marquez Vaamonde.

Formal analysis: José Martin Leonardo Marquez Vaamonde.

Research: José Martin Leonardo Marquez Vaamonde.

Methodology: José Martin Leonardo Marquez Vaamonde.

Project management: José Martin Leonardo Marquez Vaamonde.

Resources: José Martin Leonardo Marquez Vaamonde.

Software: José Martin Leonardo Marquez Vaamonde.

Supervision: José Martin Leonardo Marquez Vaamonde.

Validation: José Martin Leonardo Marquez Vaamonde.

Visualization: José Martin Leonardo Marquez Vaamonde.

Writing – original draft: José Martin Leonardo Marquez Vaamonde.

Writing – review and editing: José Martin Leonardo Marquez Vaamonde

REFERENCES

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.