Respuestas, 30 (2) May - August 2025 2025, pp. 42-69, ISSN 0122-820X - E ISSN: 2422-5053

Respuestas
UFPS

Artículo Original https://doi.org/10.22463/0122820X.5145

Blockchain and software engineering: trends in requirements, databases, development, and system architecture

Blockchain e ingeniería del software: tendencias en requerimientos, bases de datos, desarrollo y arquitectura de sistemas

Nallig Leal-Narváez[1], Danilo Torres-Pimiento[2], Esmeide Leal-Narváez[3], Fabián Ramos-Torres[4], Andrea Baquero-Tobías[5] and Carlos Gabriel Díaz-Sáenz[6*]

[1] *PhD en Ingeniería de Sistemas y Computación, nallig.leal65@uac.edu.co, https://orcid.org/0000-0002-4913-8540, Universidad Autónoma del Caribe, Barranquilla, Colombia*

[2] *MSc en Ingeniería, danilo.torres@uac.edu.co, https://orcid.org/0000-0002-6795-6061, Universidad Autónoma del Caribe, Barranquilla, Colombia*

[3] *PhD en Ingeniería, esmeide.leal@uac.edu.co, https://orcid.org/0000-0003-2468-370X, Universidad Autónoma del Caribe, Barranquilla, Colombia*

[4] *MSc en Software Libre, fabian.ramos@uac.edu.co, https://orcid.org/0000-0003-1678-7533, Universidad Autónoma del Caribe, Barranquilla, Colombia*

[5] *PhD en Gestión de la Tecnología y la Innovación, investigadorprincipal.blockchain@uac.edu.co, https://orcid.org/0000-0002-5317-9142, Universidad Autónoma del Caribe, Barranquilla, Colombia*

[6*] *PhD en Dirección de Proyectos, carlos.diaz18@uac.edu.co, https://orcid.org/0009-0009-7778-3799, Universidad Autónoma del Caribe, Barranquilla, Colombia*

Cómo citar: N. Leal-Narváez, D. E. Torres-Pimiento, E. Leal-Narváez, F. Ramos-Torres, A. Baquero-Tobías, y C. G. Díaz-Sáenz, “Blockchain e ingeniería del software: tendencias en requerimientos, bases de datos, desarrollo y arquitectura de sistemas”, *Respuestas,* vol. 30, n.º 2, pp. 42-69, may 2025. https://doi.org/10.22463/0122820X.5145

Received on January 29, 2025 - Approved on April 20, 2025 - Published on May 1, 2025.

ABSTRACT

Keywords:

Blockchain, Decentralized Applications, Software Engineering

Blockchain technology has advanced well beyond its origins in cryptocurrencies and now underpins applications and platforms interacting with decentralized networks. This is especially evident in NFT marketplaces, digital asset management, and decentralized applications (DApps), where blockchain ensures secure and transparent transactions. As adoption expands, integrating blockchain-derived data into software systems presents challenges in areas such as system design, database integration, and development practices. This paper presents a comprehensive review of blockchain’s impact on software requirements, database architectures, development strategies, and system design—domains often overlooked in mainstream blockchain research. By examining current trends, key challenges, and best practices, the study offers practical insights into how blockchain connects with software engineering and contributes to the development of modern digital solutions.

RESUMEN

Palabras clave:

Blockchain, Aplicaciones descentralizadas, Ingeniería del software

La tecnología blockchain ha evolucionado más allá de sus orígenes en las criptomonedas, y actualmente sustenta aplicaciones y plataformas que interactúan con redes descentralizadas. Esto es particularmente evidente en mercados de NFT, gestión de activos digitales y aplicaciones descentralizadas (DApps), donde blockchain garantiza transacciones seguras y transparentes. A medida que su adopción se amplía, la incorporación de datos generados por blockchain en sistemas de software plantea desafíos importantes en diseño de sistemas, integración de bases de datos y prácticas de desarrollo. Este artículo ofrece una revisión integral del impacto de blockchain en los requisitos de software, arquitecturas de bases de datos, estrategias de desarrollo y principios de diseño de sistemas, áreas frecuentemente subestimadas en la investigación convencional sobre blockchain. Al analizar tendencias actuales, desafíos clave y buenas prácticas, el estudio proporciona conocimientos prácticos sobre cómo blockchain se vincula con la ingeniería de software y contribuye al desarrollo de soluciones digitales modernas.

***Corresponding author.**
E-mail Address: *nleal@uac.edu.co (Nallig Eduardo Leal-Narváez)*

Introducción

From the very beginning, blockchain technology has evolved to become an indispensable technology for developing applications and platforms that interact with decentralized networks. Blockchain technology ensures secure and transparent transactions in various areas, such as digital asset management, decentralized applications (DApps), and non-fungible token markets. This progress is particularly noteworthy. While the adoption of blockchain increases, the need to store, process, and integrate data generated from blockchains poses important challenges in terms of software engineering methodology, database management, and system architecture.

There is an emerging body of literature focused on integrating blockchain technology into a software engineering paradigm. Dzhalila et al. [1], for example, conducted a systematic literature review focusing on software engineering challenges and identified various blockchain applications, analyzing existing problems and proposing potential solutions. As noted in their findings, software development projects can benefit from requirements engineering processes that apply blockchain methodology due to improvements in data reliability.

Paik et al. [2] examined the problem of integrating blockchain as an information store in large-scale software systems from a data management perspective. Their analysis showed that, although blockchain improves data quality due to its inherent transparency and immutability, new data management issues arise that must be addressed in the design of such systems.

Nathan et al. [3] designed and developed a blockchain-assisted relational database called the Blockchain Relational Database (BRDB), which is essentially a distributed, replicated relational database. This work utilized the powerful capabilities of relational databases, coupled with years of optimization work on them, to create a system that maintains consistency across nodes using a distributed consensus approach.

From an architectural perspective, Wohrer and Zdun [4] investigated the problem of blockchain integration into software solutions. Their emphasis is that there is a need for higher-level design in systems integration that solves the unique problems presented by blockchain.

However, there remains a lack of detailed studies analyzing the influence of blockchain technology on software requirements, databases, system architecture, and development methods. The purpose of this article is to provide such a review by highlighting the neglected aspects of software engineering in blockchain technology. By exploring new challenges and trends, this research aims to build a holistic perspective on the impact of blockchain technology on modern software development.

The structure of the article is as follows: next section presents the theoretical foundations of blockchain technology. Following sections explores how blockchain affects the definition and analysis of software requirements, discuss database structures and management in blockchain-based applications, examines architectural models and design patterns for blockchain integration, covers software development practices and methodologies for blockchain applications, and highlights future challenges and opportunities in this field. Finally, the conclusions and general considerations are presented.

Theoretical foundations

Smart contracts and blockchains become increasingly identified as revolutionary aspects in law and business. Smart contracts aren't completely "intelligent" yet enable the enforcement of agreements in an automated blockchain setting [5]. Both advantages and challenges come with smart contracts, such as contract enforceability, the roles of intermediaries, and regulatory challenges [6]. In Latin America, the governance of Decentralized Autonomous Organizations (DAOs) through smart contracts faces legal barriers, such as jurisdiction and privacy issues, necessitating flexible regulations and international standards [7].

Blockchain technology has been touted for its potential to reduce the risk of contractual failure through the automated enforcement of legal contracts and the careful following of contractual terms in line with its value proposition [8]. However, its adoption requires careful consideration of the legal implications of technology and its impact on conventional legal professions [6].

As an early-stage framework, blockchain technology has far-ranging implications in many fields [9]. Blockchain integrity is maintained through an alliance of disseminated nodes and cryptographic methods, ensuring information immutability and traceability [10]. In such contexts, tokens play an imperative role, being grouped based on properties and value [11]. Tokenization has given birth to innovations including Initial Coin Offerings (ICOs) and Decentralized Autonomous Organizations (DAOs), hence providing unprecedented opportunities in finance and company governance [12]. Furthermore, blockchain technology holds high potential in the defense sector, especially in the area of supply chain management as well as in cybersecurity [9]. However, the major hindrance in the development of technology is the existing regulatory ambiguity [12]. Despite this hindrance, blockchain technology continues its relentless march, displaying commendable diversification in its uses in different disciplines, hence confirming its feasibility and suitability for mass application [11].

Here, blockchain denotes an innovative and revolutionary technology that manifests versatility in many fields, such as public administration [13-14]. Its design provides an immutable, public, distributed database, thus enabling trust by through transparency [14]. Also, blockchains may be categorized in terms of access, privileges, and layers of development [15].

While several governments are exploring possible uses of blockchain technology, its uptake is still hampered, possibly owing to the immature development of the technology as well as inadequate scalability levels [16]. Oracles and smart contracts play an important role in furthering the development of technology, to this end [15]. The European Union has strongly promoted blockchain integration into public administration, particularly asset registration [13]. However, end-to-end integration requires changes to regulation, and to date, government acts that were successfully implemented as planned remain few in number [13-16].

Blockchain, which started to be created for use by Bitcoin, has also been extended to other platforms including Ethereum, Hyperledger, and Corda [17]. Hyperledger Fabric is an enterprise permissioned blockchain that offers private transactions and better performance compared to public chains [18]. In parallel, IOTA brings about an innovative consensus protocol [19].

In terms of security, Hyperledger Fabric as well as Bitcoin both possess strong properties, while that of Ethereum can be termed as moderate. Due to their higher integrity and higher level of security features, Hyperledger Fabric and Bitcoin are preferred where strong security is required [20]. Additionally, blockchain platforms vary in terms of transaction flow complexity, where Hyperledger Fabric has higher complexity owing to its vast components [21]. Performance comparison underlines that private blockchain channels like Hyperledger Fabric support higher stability, lesser latency, and lower fees associated with transactions in comparison to public blockchain channels [18].

Since its introduction, blockchain technology has undergone significant development, well beyond its original application in cryptocurrency. Recent studies highlight its possible application within supply chain administration in terms of ensuring transparency, traceability, and integrity [22]. Its reach is wide, sparking debate about legal and governance framework, where European minors' rights and interests were of particular interest [23].

Due to its decentralized character, as well as its features of data integrity, anonymity, and security, blockchain has attracted much interest from financial corporations and other industries [24]. In accounting, it helps to minimize fraud risks, reduce errors, and increase efficiency as well as transparency.

Current research trends include network security, information management, digital storage, edge computing, commerce, and the Internet of Things [25]. As technology continues to evolve, it presents both opportunities and challenges across different sectors, necessitating ongoing studies and adaptations.

Current State of Requirement Aspects Associated to Blockchain Related Applications

Requirements engineering is considered the cornerstone phase of the software development lifecycle due to its impact on subsequent phases. Success in this stage largely ensures the fulfillment of the needs of the stakeholders involved in the project.

Requirements engineering is the process of discovering, analyzing, documenting, and validating the services and constraints of a system, defined in cooperation with users and other stakeholders [26]. Its main objective is to identify, document, and manage requirements throughout the system's lifecycle, ensuring that they are complete, consistent, and traceable, in addition to specifying the system's functionality [27].

It is also important to clarify the difference between a requirement and a specification: the former refers to what the product or system must/should do, while the latter describes how it works and how it is built. Requirements are classified into functional and non-functional requirements. Functional requirements define the services that the system must provide, the system's reactions to particular inputs, and how it behaves in certain situations. Non-functional requirements state constraints on the services or functions the system offers, such as time limitations, compliance with specific standards, or software quality needs [26].

To carry out engineering requirements, various industry standards based on ISO/IEC/IEEE norms exist, including:

- ISO/IEC/IEEE 24765:2010 – Defines a standard vocabulary for systems and software engineering [28].

- ISO/IEC/IEEE 24766:2010 – Specifies the requirements for requirements engineering tools [29].
- ISO/IEC/IEEE 29148:2011 – Describes the processes for requirements engineering [30].

As a complement to these standards, additional supporting frameworks can be used, such as BABOK (Business Analysis Body of Knowledge), ISO/IEC 25012:2008, CMMI (Capability Maturity Model Integration), and PMBOK (Project Management Body of Knowledge).

NFT platforms, NFT utility models, and smart contracts

In order to determine the minimum functionalities required for developing NFT marketplaces, various web applications in the market that offer NFT publishing, selling, and purchasing services were reviewed. Among these applications, the following stand out [31][32][33]:

- OpenSea: The largest and most comprehensive NFT marketplace internationally, with a high transaction volume across multiple blockchains. It offers a wide selection of NFTs in digital art, virtual real estate, and digital collectibles. It features a unique "free gas" function that significantly reduces transaction fees, although its suboptimal customer support is its biggest drawback.
- Rarible: A decentralized NFT marketplace that allows users to create custom NFT stores, conduct transactions across multiple blockchains, and earn RARI tokens to contribute to the platform's development. However, it faces challenges in ensuring scalability.
- Foundation: A platform exclusively for invited artists, ensuring high-value artwork. It features a well-designed auction system and a percentage of earnings from secondary sales for artists, though it has high commission fees on sales.
- SuperRare: A marketplace for exclusive digital art collections, offering royalties on secondary sales and attracting high-profile collectors willing to invest. Its exclusive approach makes it less accessible to the public.

Additionally, Table 1 presents a comparison of several existing NFT marketplaces, based on the following aspects:

- Supported Blockchains: Indicates the blockchain networks on which the platform operates.
- Transaction Fees: The percentage that the platform charges for each completed sale.
- Accepted Payment Methods: Currencies or payment methods used for transactions.
- Market Type: Specifies whether the marketplace is open (accessible to any user) or curated (restricted to selected artists and collections)
- Creator Royalties: The percentage that creators receive from secondary sales of their works.

- Launch Date: The month and year the platform was released to the public.
- Main Focus: The specific market in which the platform specializes or stands out.

Table 1. NFT Marketplaces Comparison.

Platform	Supported Blockchains	Transaction Fees	Accepted Payment Methods	Market Type	Creator Royalties	Launch Date	Main Focus
OpenSea	Ethereum, Polygon, Klaytn	2.5% per sale	ETH, WETH, DAI, USDC	Open	Up to 10%	December 2017	General NFT marketplace
Rarible	Ethereum, Flow, Tezos	2.5% for buyers and sellers	ETH, XTZ, FLOW	Open	Up to 10%	November 2019	Community-driven NFT marketplace
Foundation	Ethereum	5% per sale	ETH	Curated	10% on resales	February 2021	Digital art and collectibles
SuperRare	Ethereum	3% for buyers, 15% for artists on primary sales	ETH	Curated	10% on resales	April 2018	Exclusive digital art
Nifty Gateway	Ethereum	5% + 30¢ per sale	ETH, credit card	Curated	Up to 10%	March 2018	Digital art and collectibles from renowned artists
Mintable	Ethereum, Immutable X	2.5% for regular items, 5% for mintable items	ETH, credit card	Open	Customizable	2018	Easy create, buy, and sell NFTs
NBA Top Shot	Flow	5% per transaction	Credit card, Dapper-compatible cryptocurrencies	Curated	Not specified	October 2020	NBA highlights in digital collectible format
Blur	Ethereum	No fees	ETH	Open	Customizable	October 2022	Platform for professional NFT traders
Magic Eden	Solana, Ethereum	2% per transaction	SOL, ETH	Open	Up to 2%	September 2021	Leading NFT marketplace on Solana, expanding to Ethereum

Digital art marketplaces in NFT format, such as OpenSea, Rarible, and SuperRare, allow any artwork to be showcased for sale. The only thing digital artists need to do is "mint" their art as NFTs. The minting process creates an NFT with its first entry into a digital ledger on the blockchain, thus ensuring the value of a digital artwork [34].

In this NFT buying and selling process, Smart Contracts are incorporated—a computerized transaction protocol that executes the terms of a contract, automating the conditions of an agreement between participants and fostering trust and transparency in a decentralized system [35]. The operation of a Smart Contract transaction protocol is structured in different steps, including agreement, coding, deployment, execution, verification, and completion of the transaction [36].

Smart contracts must be deployed on blockchain platforms, with the most influential being Ethereum, Hyperledger Fabric, Corda, Stellar, Polkadot, and Solana. Additionally, they can be classified into four categories [43]:

- Smart Legal Contracts.
- Decentralized Applications (DApps).

- Decentralized Autonomous Organizations (DAO).
- Smart Contracting Devices.

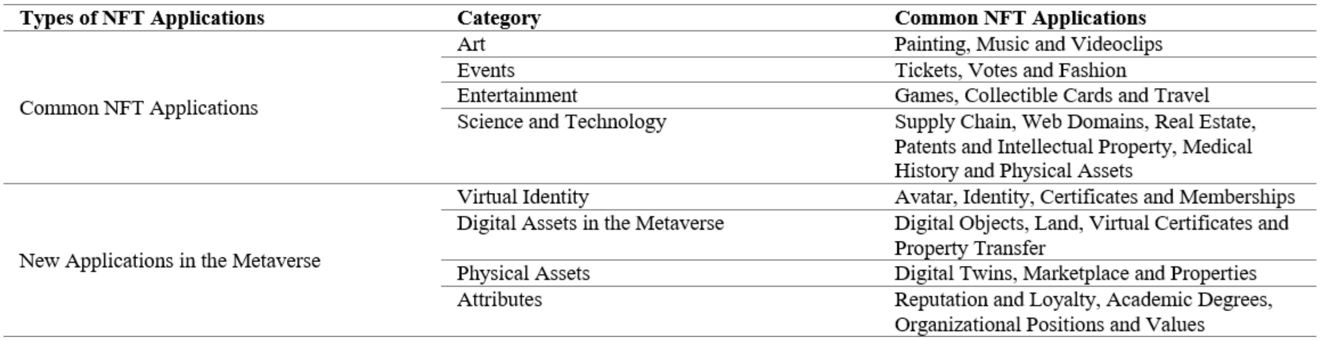
Considering the possibility of buying and selling NFT products through these platforms, there are various NFT utility models, which are digital assets designed for a specific purpose or function within a particular ecosystem, providing benefits to their owners.

Unlike traditional NFTs, primarily used for collectibles or digital art, utility NFTs have a practical application within a specific platform or application. Among the most common utility models, we find [35]:

- Memberships and Tickets: Allowing access to real or virtual events such as sports games, concerts, exhibitions, or serving as membership cards for private clubs with exclusive benefits.
- Physical Products: Acting as certificates of authenticity for a work of art or music.
- Loyalty Rewards: Earned through purchases or interactions with a specific brand, redeemable for discounts or exclusive offers.
- Governance and Voting Rights: Collecting cast votes by identifying each user linked to an NFT as a voter, enabling participation in key decisions or proposals within an organization.
- Airdrops: Tokens distributed to holders of another token as a reward or incentive.
- Allowlist: Used to represent access to exclusive content or events, such as the right to participate in a limited-edition product release.
- Gamification: Offering holders challenges, rewards, or special features within digital games.
- Discounts and Promotional Codes: Serving as a visual representation of coupons or discounts.
- Exclusive Content: Indicating special material such as VIP access, early access, or behind-the-scenes interactions with an artist or creator.

Table 2 presents a grouping of these utility models framed into two main categories: common NFT applications and applications in the metaverse [17].

Table 2. NFT Platform Categories.



Types of NFT Applications	Category	Common NFT Applications
Common NFT Applications	Art	Painting, Music and Videoclips
	Events	Tickets, Votes and Fashion
	Entertainment	Games, Collectible Cards and Travel
	Science and Technology	Supply Chain, Web Domains, Real Estate, Patents and Intellectual Property, Medical History and Physical Assets
New Applications in the Metaverse	Virtual Identity	Avatar, Identity, Certificates and Memberships
	Digital Assets in the Metaverse	Digital Objects, Land, Virtual Certificates and Property Transfer
	Physical Assets	Digital Twins, Marketplace and Properties
	Attributes	Reputation and Loyalty, Academic Degrees, Organizational Positions and Values

Key Aspects of Requirements Engineering for NFT Platforms and Smart Contracts

Based on a review of the most popular NFT marketplaces, the following basic functionalities offered to users were identified [37]:

- Wallet integration.
- Integration and/or communication with a blockchain platform to enable transparent and secure transactions.
- Implementation of smart contracts.
- Visual interfaces that comply with UX/UIX standards.
- Filtering and searching for tools for NFTs.
- Secure purchasing and payment systems.
- Legal and compliance considerations.

Additionally, these applications should strive to meet the following key aspects [43]:

- Readability
- System Performance
- Code Validation
- Interoperability
- Dynamic Control Flow
- Information and Technological Infrastructure Security
- System Scalability
- User Experience
- Cross-Platform Compatibility
- System Availability and Reliability Aligned with Contingency and Business Continuity Plans

Requirements Engineering Methodology

To carry out the requirements engineering phase for the development of an NFT marketplace, a methodology is proposed consisting of six (6) basic activities:

- Requirements elicitation: The process of gathering information about customer needs and system constraints using data collection, collaboration, and analysis techniques [38].

- Requirements analysis: Classification of system requirements, establishing priorities and performing a feasibility analysis for each of them.

- Requirements specification: Structured documentation of system requirements, including user stories/use cases and UML diagrams.

- Validation and verification: Requirements validation ensures that the defined requirements accurately describe the system that stakeholders need [26]. Verification focuses on reviewing that the documented requirements are complete, traceable, and technically correct according to the defined standard [27]. This phase includes the following tasks:
    - Review with stakeholders to verify the completeness, clarity, and understanding of requirements.
    - Creation of prototypes that reflect the elaborated requirements.
    - Definition of acceptance criteria: Specifies the minimum requirements that a user story must be considered functional [39].
    - Change management: Control of modifications made to requirements and specifications due to various factors. Version control of documents is essential for traceability.
    - Final acceptance: Approval of requirements by project stakeholders.

These activities were defined based on various requirements engineering methodologies, including [40]:

- DoRCU Methodology
- XRE Methodology
- AMMETH Methodology
- Borja Methodology
- Páez Methodology

The final product of this phase is the Requirements Specification Document, which must include the following information [41]:

- Identification of stakeholders.
- Business processes and operational rules.
- Functional and non-functional requirements.
- Use case documentation.
- User interface definitions.

- System interface definitions.
- Hardware interface definitions.
- Software interface definitions.
- Communication interface definitions.
- Data requirements definitions.

Functional and Non-Functional Requirements for the Development of the Web Platform and Mobile Application.

The functional and non-functional requirements in the Requirements Specification Document for NFT marketplace and Smart Contract development projects must address the following core functionalities:

Functional Requirements

- User Management: User registration, login with multi-factor authentication (MFA) and profile management.
- NFT Management: NFT creation, uploading digital artwork, NFT configuration and linking NFTs with Smart Contracts.
- NFT Commercialization: Buying and selling NFTs, NFT auctions, blockchain wallet integration and cryptocurrency transactions.
- Smart Contract Management: Smart contract creation, monitoring and tracking contract statuses and digital rights management.
- Digital Artwork Communication Management: Ratings and comments on digital artwork, artist following, publications and notifications.
- Reports and Statistics: Metrics dashboard and report generation.

Non-Functional Requirements

- Platform Security: Implementation of data encryption, audit logs, and secure code development for risk mitigation.
- Performance: Optimization of response times for web and mobile requests, support for approximately 1,000 concurrent users, and high-performance transaction handling.
- Scalability: Expandable platform for new functionalities.
- Usability: Intuitive and user-friendly interface, responsive web and mobile platform.
- Compatibility: Integration with various blockchain platforms and cross-browser functionality.
- Availability: 24/7 platform accessibility and 24/7 technical support.

- Maintenance: Software change management, version control for web and mobile platforms, error log monitoring, and service agreements with providers for maintenance and support.
- Legal Aspects: Data handling compliance with national and international regulations, copyright policies, and usage rights for digital artwork.

Current State of Database Aspects Associated to Blockchain Related Applications

Data storage in the blockchain ecosystem plays a fundamental role in ensuring accessibility, security, and integrity. The choice of data storage technology impacts the interoperability, scalability, and performance of decentralized applications, particularly those involving NFT transactions and contracts. This section presents the current state of database technology related to supporting or interacting with blockchain applications, including both centralized and decentralized solutions, as well as considering distributed storage systems, security mechanisms, and scalability.

Blockchain applications, from the perspective of architecture and data management approach, can be classified as centralized or decentralized. These approaches are presented below.

- Centralized Databases
  Conventional SQL databases, such as PostgreSQL and MySQL, offer structured storage that supports ACID-compliant transactions. NoSQL solutions, such as MongoDB and Firebase, facilitate the flexible management of unstructured data, as well as its scalability. Although centralized databases rely on high performance and administrative control, their centralized approach and management of data without trust constitute a lacking the main foundations of blockchain technology [44].

- Decentralized Databases:
  In contrast to centralized models, decentralized databases operate on distributed networks where multiple nodes participate in storing and verifying data. Examples include BigchainDB, which provides distributed storage with the ability to modify and audit, and LevelDB and CouchDB in Hyperledger Fabric, which are used to store blockchain transaction states [45]. The InterPlanetary File System (IPFS) and Swarm provide decentralized file storage, ensuring availability and censorship resistance. Decentralized databases improve information integrity, transparency, and error tolerance. However, their implementation can be complex and often requires replication and consensus strategies to ensure secure and efficient data recovery [46].

Decentralized Storage Systems

Decentralized storage systems eliminate intermediaries, enhance security, and improve data availability across blockchain networks. Unlike traditional cloud-based storage, these systems distribute data across multiple nodes, enhancing resilience and privacy. Some of the most widely used decentralized storage solutions include:

- IPFS (InterPlanetary File System): A protocol for distributed file storage that enables content addressing through cryptographic hashes, widely adopted for storing NFT metadata [47].

- Arweave: A blockchain-based permanent storage network that ensures long-term data availability through a one-time payment model, making it ideal for storing historical records and NFT assets [48].
- Filecoin: A decentralized storage network that incentivizes providers to offer storage capacity in exchange for cryptocurrency rewards, ensuring scalability and security [49].
- Storj and Sia: These platforms utilize smart contracts and data fragmentation techniques to distribute encrypted data across nodes, ensuring high availability and reduced operational costs [50].

Blockchain Database Engines

Blockchain-based database engines provide advanced features to optimize transaction security, query efficiency, and data scalability in decentralized applications. Depending on the system architecture, databases may be fully decentralized, hybrid, or designed to interact with specific blockchain networks. Some notable blockchain database engines include:

- BigchainDB: A hybrid database that combines traditional database capabilities with blockchain immutability, allowing efficient querying and decentralized asset management [51].
- Hyperledger Fabric (LevelDB & CouchDB): These are the primary databases used in Hyperledger Fabric networks. LevelDB provides key-value storage for transaction states, while CouchDB facilitates structured JSON document storage, enabling efficient queries in permissioned blockchain networks [52].
- Ethereum Swarm: A decentralized storage protocol designed to work alongside Ethereum, facilitating smart contract storage and DApp data availability through cryptographic incentives [53].
- Tendermint (Cosmos DB): A high-performance consensus protocol that powers Cosmos network interoperability, enabling secure cross-chain data exchange without compromising decentralization and scalability [54].

Security and Scalability Challenges in Blockchain Databases

Security and scalability are among the most pressing concerns in blockchain-based database implementations. As blockchain networks expand, ensuring data integrity, consistency, and high performance is essential for sustainable adoption.

Data Consistency and Replication

Data consistency ensures that all nodes in a distributed network always reflect the same information. In blockchain databases, consistency is achieved through replication models and consensus mechanisms:

- Strong Consistency: Ensures that all nodes always have identical data but may reduce performance.
- Eventual Consistency: Allows temporary data discrepancies, which eventually synchronize across nodes, enhancing scalability.
- Replication Strategies:

- » Consensus-Based Replication: Algorithms like Proof of Work (PoW) and Proof of Stake (PoS) synchronize blockchain data across all nodes [55].
- » Sharding: Divides a database into smaller partitions (shards), reducing node load and improving transaction throughput [56].

Cryptographic Security in NFT Storage

Since NFTs represent unique digital assets, securing their metadata and ownership records is critical. Cryptographic security in blockchain databases involves:

- Hashing and Merkle Trees: Ensures data integrity by verifying changes without requiring full storage replication.
- Data Encryption (AES-256, RSA): Protects NFT metadata and on-chain/off-chain data storage through private keys [53].
- Digital Signatures and Ownership Authentication: Smart contracts leverage public-private key cryptography to verify NFT ownership and prevent fraud [57].

Integrity and Consensus Mechanisms

Blockchain-based databases rely on consensus mechanisms to validate transactions and maintain data immutability:

- Proof of Work (PoW): Provides high security but is computationally intensive.
- Proof of Stake (PoS): Reduces energy consumption and enables efficient transaction validation.
- Zero-Knowledge Proofs (ZKP): Allows verification without revealing underlying data, enhancing privacy in sensitive transactions [55].
- Multi-Party Computation (MPC): Distributes computation across nodes while ensuring data confidentiality.

Security and Scalability Challenges in Blockchain Databases

As blockchain adoption continues to expand, research and development in blockchain-compatible databases focus on scalability, interoperability, and efficiency. Emerging trends include:

- Hybrid Database Solutions: Combining SQL, NoSQL, and decentralized storage for enhanced NFT and DApp management.
- Decentralized Indexing: Utilizing platforms like The Graph to optimize smart contract data retrieval.
- AI-Driven Query Optimization: Integrating machine learning for real-time query efficiency in blockchain databases.

Current State of Software Development Aspects Associated to Blockchain Related Applications

Software development with Blockchain is a rapidly expanding field, driven by the need for decentralized applications that are secure, transparent and efficient. This technology has transformed the management of digital data and transactions, providing security and resistance to manipulation. Since its beginnings with cryptocurrencies like Bitcoin, Blockchain is redefining the design and execution of applications, marking a before and after in software development.

Programming languages used: Solidity, Rust, Go, Python

It would be appropriate to imagine or think of blockchain technology as an unalterable and shared digital ledger. Each new annotation links to the previous one, creating an indelible and transparent sequence. This feature makes it extremely secure, since its validation depends on multiple participants, preventing any unauthorized modification. Therefore, when developing with blockchain, it is vital to select the programming language, because by choosing the right tool for a complex task, it offers various advantages and challenges, which with a good decision will enhance the success of any initiative [58]. Some of them are:

- Solidity: a type of programming language specifically designed to write smart contracts using Blockchain, so that decentralized applications are created, tokens or NFT, secure voting systems that allow managing assets in the blockchain. This allows contracts to be automatically executed when certain conditions are met, without the need for an intermediary.

- Rust: is a type of system programming language that addresses the security of memory, speed and concurrency. At the same time, it works to cement operating systems, game engines, web browsers, among others. "Rust" is very efficient as it allows us to guarantee the security of memory without the need for a garbage collector.

- Go: A simple, efficient and easy-to-use programming language for large-scale software development as used in server programming, command line tools, cloud systems and microservices, Simple operation for distributed systems.

- Python: it is another type of high-level, general-purpose programming language known for its clear, readable and extremely versatile syntax. Used in web development, data analytics, artificial intelligence and machine learning, task automation, software development and more. This type of programming language stands out for its simplicity, for its libraries and frameworks, making it a widely used tool at all levels of software development.

Key tools for blockchain development: Truffle, Hardhat and Hyperledger Fabric SDK.

Blockchain development, a constantly expanding field, demands robust tools for the creation and management of decentralized applications and enterprise networks. Among the most prominent solutions, Truffle and Hardhat are positioned as integral development environments that facilitate the compilation process, a correct deployment of infrastructure and the appropriate testing of smart contracts for their final execution.

Thus, for enterprise-level Blockchain solutions, Hyperledger Fabric SDK offers a set of programmatic tools to interact with Manufactured networks, allowing the integration of applications with decentralized business logic. Therefore, it should be stressed that the choice of the tool will depend on the ecosystem and the specific requirements of the project implemented, which in turn includes even public blockchains and other private networks for their realization

Best practices in software development with blockchain

The use of Blockchain as a means or tool to guarantee adequate development and implementation of software is based on the implementation of actions and/or good practices, some of these good practices include:

- Security: Security is paramount in blockchain software development due to the immutable and transparent nature of transactions. Robust security measures must be implemented to protect smart contracts and user data from potential vulnerabilities and malicious attacks.
- Efficiency: Blockchain applications must be designed to be efficient in terms of resource consumption and processing time. Smart contracts and transactions should be optimized to minimize gas costs and improve overall application performance.
- Scalability: As blockchain applications grow in popularity and transaction volume, scalability becomes a critical factor. Appropriate scalability solutions, such as sharding or payment channels, must be implemented to ensure the application can handle more users and transactions without compromising performance.
- Comprehensive testing: Testing remains a requirement to ensure the reliability and quality of blockchain applications. At a minimum, unit testing, integration testing, and security testing should be performed to mitigate any errors and vulnerabilities before deployment [59].

Software development lifecycle for blockchain applications

The framework for developing software for blockchain applications is similar to the conventional framework, however, it has some modifications tailored to the nature of blockchain technology [60–62]. The following stages form a typical life cycle:

- Requirements Analysis: In relation to users, the objectives, functions, and features of the blockchain application are mapped, along with the technical requirements of the selected blockchain platform.
- Design: The system is divided into modules through the creation of smart contracts, databases, and user interfaces; thus, the application structure is outlined.
- Development: The application's business logic is implemented in appropriate programming languages and development tools, and smart contracts are created.
- Testing: The application is deployed on the blockchain network and made available to users.

1. Maintenance: Updates and bug fixes are made to ensure the correct operation of the application over time.

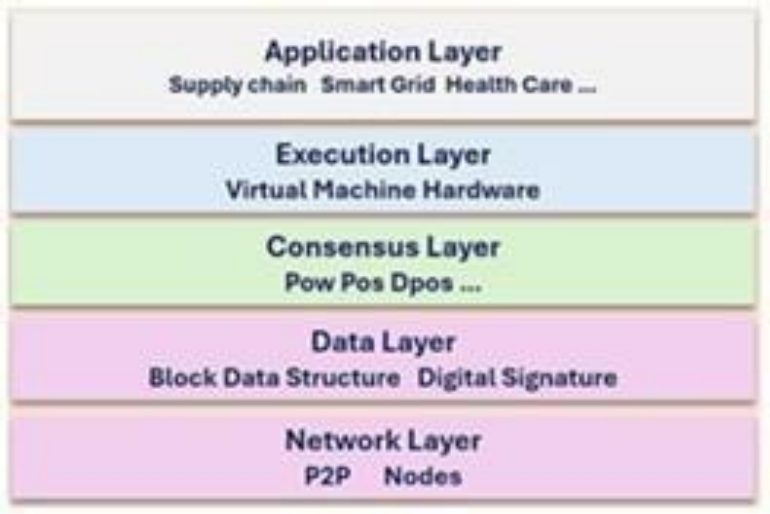


Figure 1. A typical layered blockchain architecture.

Current State of Software Architecture Aspects Associated to Blockchain Related Applications

Blockchain-based software architecture is of great importance in many applications in which it is necessary to take advantage of three key factors such as: decentralization, security, and scalability. Initially, blockchain was designed for the development of cryptocurrencies [66], but over time it evolved to support everything related to smart contracts [63,64], decentralized finance (DeFi) [65], and supply chains, which makes specialized architectural approaches necessary. The introduction of blockchain has had a great impact on software development since it leads to the introduction of new paradigms, such as the non-intervention of intermediaries, ensuring data immutability, and autonomous execution of business logic. New architectural designs must facilitate interoperability between traditional software systems and blockchain-based software systems. To do this, resource management must be optimized while ensuring high performance in distributed environments. Smart contracts require secure and efficient execution frameworks. Finally, blockchain-based software architecture must balance scalability, security, and sustainability to meet the needs of different industries. Figure 1 shows a typical layered blockchain architecture.

Main Architectural Components in Blockchain-Based Applications

Decentralization and Distribution

Software architecture based on blockchain technology is crucial for creating and organizing applications that benefit from decentralization, security, and scalability. Conventional software architectures largely rely on centralized systems, in which a single system is responsible for data management, operations, and user verification through central servers. This centralized methodology entails risks such as system errors, susceptibility to attacks, and potential trust issues due to the potential for control over data and decision-making. In contrast, decentralized architectures based on blockchain eliminate the need for a central device by distributing transaction validation and data storage across a network of nodes. Here, consensus tools such as Proof of Work (PoW) or Proof of Stake (PoS) are crucial, as they facilitate group decision-making and enhance resilience to errors and attacks by eliminating specific areas of vulnerability. Blockchain technology also ensures the immutability and clarity of information, creating a secure and reliable environment without intermediaries.

Consensus and Security

The architecture of blockchain networks and distributed systems is significantly influenced by consensus mechanisms such as PoW, PoS and others [68]. These mechanisms affect aspects such as scalability, security, energy efficiency, and finally decentralization. They also determine how consensus is reached in the decentralized network. These aspects and their impact on architecture are discussed below in Table 3.

Table 3. Consensus Mechanisms in Blockchain.

Consensus Mechanism	Network Architecture	Security and Decentralization	Scalability and Performance	Energy Efficiency and Cost
Proof of Work (PoW)	Requires nodes (miners) to solve cryptographic problems, leading to a distributed network with high processing capacity. Expensive and challenging to scale.	Extremely secure due to the high computational cost of attacks (51% attack). However, mining pools can hinder decentralization.	Less scalable due to complex calculations per block (e.g., ~10 min for Bitcoin), leading to slow transaction speeds and high latency.	Very high energy consumption, prompting the search for more sustainable alternatives.
Proof of Stake (PoS)	Eliminates the need for specialized hardware, using token staking for block validation.	Secure but has a higher risk of centralization, as those with more tokens have more influence. The cost of attacking the network is high.	Improves scalability by removing intensive calculations. Networks like Solana use PoS + PoH to achieve high TPS (~50,000).	Reduces energy consumption by approximately 99% compared to PoW, making it more sustainable and accessible.
Delegated Proof of Stake (DPoS)	Introduces a voting system where token holders elect delegates to validate transactions, increasing efficiency and scalability.	Improves efficiency but is more vulnerable to collusion among delegates, leading to lower decentralization.	More scalable than PoS due to fewer validators, enabling higher transaction throughput.	Energy-efficient, similar to PoS, and suitable for high transaction volumes.
Proof of Authority (PoA)	Uses pre-approved validators, making it highly efficient and secure, especially in private or consortium networks.	Highly secure but extremely centralized, as only a limited group of validators approve transactions.	Very scalable due to its low computational requirements.	Low energy consumption, as no intensive calculations or mining competition are needed.

Scalability and Performance

Scalability and performance are fundamental challenges in blockchain architecture, especially due to the blockchain trilemma, a concept coined by Vitalik Buterin [69] that describes the difficulty of optimally balancing security, decentralization, and scalability. In practice, improving one of these properties often compromises the other two. For example, Bitcoin prioritizes security and decentralization, which limits its scalability (processing only 7-10 transactions per second). On the other hand, more centralized networks like EOS achieve greater scalability but sacrifice decentralization and, in some cases, security. This trilemma is a key barrier to the mass adoption of blockchain, as networks must handle high transaction volumes without compromising their integrity or openness.

To address these challenges, sharding, sidechains, and layer 2 protocols have been suggested. Sharding involves segmenting the network into smaller fragments (shards) that handle transactions in parallel, thereby increasing the overall network capacity (e.g., Ethereum 2.0). Sidechains are autonomous chains tied to the main chain, facilitating faster and more accurate transactions without overloading the network. Finally, there are layer 2 protocols, such as Bitcoin's Lightning Network and Ethereum's Optimistic Rollups, which perform transactions off-chain and then consolidate the results, optimizing performance without compromising security. These tactics seek to boost scalability without compromising security or decentralization, though each has its own drawbacks and technical challenges [70].

Interoperability

In the blockchain space, the ability to interoperate is essential, as it enables interaction and information exchange between various decentralized networks, helps minimize ecosystem fragmentation, and optimizes the effectiveness of decentralized applications (dApps). Other important solutions that have emerged to address these problems include mechanisms such as Polkadot, Cosmos, and blockchain bridges. Polkadot is based on a Relay Chain and parachain structure, where multiple chains operate autonomously but share security and consensus through the parent chain [71]. Cosmos, on the other hand, employs the Hub-and-Zone model, which links independent blockchains through communication protocols such as Inter-Blockchain (IBC), eliminating the need for intermediaries. Blockchain bridges allow the transfer of assets and data between networks with different protocols, such as Ethereum and Binance Smart Chain, using smart contracts or external validators. However, these bridges can be susceptible to attacks and require rigorous security measures [73].

Interoperability has significantly influenced software design, as developers need to adapt to frameworks such as Substrate (Polkadot) and Tendermint (Cosmos). They also need to adhere to protocols such as IBC or XCMP, which ensure cross-chain compatibility [72]. This encourages the development of modular and adaptable applications, allowing them to operate in multi-chain environments, which in turn improves both scalability and user experience. However, this also introduces new challenges, such as securing blockchain bridges and securely validating cross-chain transactions. As interoperability advances, it is anticipated to drive further blockchain adoption by facilitating more connected and effective networks, but it also requires greater attention to security and building decentralized infrastructure.

Smart Contracts and their Architecture

Regarding smart contracts and their architecture, the use of both the Ethereum Virtual Machine (EVM) and WebAssembly (WASM) [74] is crucial for their execution. To support its execution in Ethereum, the EVM is the main environment, which is why it is designed to process smart contracts written in Solidity. This is based on stacks and volatile memory, which guarantees a high level of security and isolation, but has the weakness that its efficiency and flexibility can be limited by its nature. On the other hand, WASM [75] guarantees greater portability and efficiency, this allows smart contracts to run in various environments, not limited to just blockchains. This improves performance and expands compatibility with other languages such as Rust and C++. Used by projects such as Polkadot and Near Protocol, WASM allows faster and more flexible execution of smart contracts, facilitating interoperability between different blockchain platforms.

Solidity and Hyperledger Fabric are frameworks and programming languages that address the needs of different types of smart contract applications. The most popular language on Ethereum for writing smart contracts is Solidity, which is optimized for interaction with the EVM. Solidity's syntax is similar to JavaScript, allowing for easy adoption by developers, but it presents code security vulnerabilities that must be addressed. Hyperledger Fabric is a platform that uses chaincode instead of smart contracts and operates in private and consortium environments. Hyperledger Fabric is not based on a virtual machine, as EVM is; instead, it allows smart contracts to run in Docker containers, enabling scalability and flexibility in enterprise applications that require high privacy controls. These technologies and tools allow for the design of blockchain solutions tailored to the needs of each project, balancing the challenges of security, efficiency, and flexibility according to the requirements of the execution environment.

Architectural Patterns and Best Practices

In blockchain architecture, scalability and modularity are enhanced by the adoption of microservices and hybrid models. Microservices allow applications to be decomposed into smaller, independent components so they can be efficiently managed, updated, and scaled [76]. Microservices are valuable in the context of blockchain because they allow separating critical functions that require distributed consensus (on-chain) from those that can be processed more quickly and cost-effectively off-chain. An example of this is computationally intensive transactions; these can be processed off-chain, with only the final results being recorded on the blockchain to ensure transparency and security. This hybrid approach increases performance while also reducing costs, as demonstrated by the use of Hyperledger Fabric [77], which enables microservices-based deployments. This helps to scale components without disrupting the system. Combining on-chain and off-chain storage improves efficiency, as large or sensitive data can be stored in traditional databases or decentralized systems like IPFS or Arweave, while critical records remain on-chain.

Minimizing risks and improving the reliability of blockchain systems depends largely on the secure design of smart contracts. This requires implementing unit testing and external security audits by experts such as CertiK or OpenZappelin [78]. This ensures that vulnerabilities are addressed before implementation. Implementing access control and security mechanisms contribute to the security of smart contracts. These practices ensure the resilience of contracts against common vulnerabilities, such as reentrancy attacks or improper input validation. Furthermore, hybrid models, which combine both on-chain and off-chain elements, allow applications to balance the speed and scalability of traditional systems with the security and transparency of blockchains. By separating sensitive data and large-volume information from the blockchain, these solutions reduce operational costs while maintaining the fundamental advantages of blockchain immutability and decentralization.

Challenges and Future Directions

Scalability, interoperability, and security are challenges when developing the architecture of blockchain systems. In networks like Bitcoin and Ethereum, which process a limited number of transactions per second compared to decentralized systems, scalability remains a major concern. Solutions such as sharding, sidechains, and Layer 2 protocols are emerging, although challenges remain in terms of implementation complexity and decentralization. Interoperability between different blockchains is another major issue, as networks often operate under different protocols and standards, complicating communication between them. The use of Polkadot, Cosmos, and Interledger seek to address this by creating interoperable blockchain ecosystems. Furthermore, smart contract security is a persistent problem, as vulnerabilities have led to significant financial losses, highlighting the need for better coding practices and rigorous security audits.

In the future, the expansion of Blockchain as a Service (BasS) [67] will help companies implement these types of solutions without the burden of managing a complex infrastructure, reducing costs and accelerating their adoption. Large BigTech companies, with their frameworks such as IBM Blockchain, Amazon Managed Blockchain, and Microsoft Azure Blockchain, make it easier for companies to integrate blockchain. Confidential computing is becoming a key trend, as it allows the processing of sensitive data securely and privately, even in decentralized environments, using technologies such as TEE and zk-SNARKs. Finally, advances in consensus models, such as Proff of Stake (PoS) and Proff of History (PoH), will improve the energy efficiency and scalability of these systems. Also, the use and integration of blockchain technology with AI and machine learning are driving the next generation of developments in decentralized applications, which will contribute to the creation of more scalable, secure, and adaptable applications to business needs.

Challenges and future opportunities

Scalability and efficiency in transaction processing

Recent research emphasizes the role of blockchain technology in increasing efficiency and scalability of transaction processing. Testing trials on Ethereum networks have verified improved performances and latency reductions in accordance with an increase in nodes, as much as ten times as many transactions processed every second on a 16-node network versus one node [79, 80]. In addition, sharding technology has also been seen to greatly increase scalability, as studies have measured up to 70% increases in transaction processing and 50% increases in network efficiency [81].

These advances make blockchain an accessible choice for a wide range of applications, such as environmental monitoring systems. In the field of financial auditing, blockchain offers potential advantages such as process automation, enhanced system integration, and real-time processing, although its implementation still presents challenges [82]. Overall, these studies underscore blockchain's ability to improve efficiency and scalability in transaction processing across different sectors.

Interoperability between blockchain platforms

Blockchain interoperability, defined as the ability of different blockchain networks to communicate and interact, has become a key challenge in the industry. While most blockchains operate independently, researchers are exploring various solutions to enable cross-chain communication [83, 84]. Current research primarily focuses on the interoperability of public blockchains, whereas interoperability in private networks and between public and private systems remains in its early stages [83].

Proposed solutions include notary and hash-locking mechanisms for token transfers [85], as well as gateway-based approaches for permissioned blockchains [86]. These strategies aim to enhance the scalability and connectivity of blockchain networks while addressing critical aspects such as privacy and identity management in permissioned systems. With the advancement in the field, scholars continue to develop more efficient solutions for blockchain communication, leading to an impressive increase in interoperability approaches in recent years [84].

Regulation and legal aspects

Blockchain technology faces significant legal and regulatory challenges across jurisdictions. Key issues include the legal status of cryptocurrencies, concerns over data protection, and the validity of smart contracts [87, 88]. In Colombia, the impact of blockchain on privacy rights and personal data protection has been analyzed, highlighting the need to adapt traditional legal frameworks to this disruptive technology [89]. Its decentralized nature poses regulatory difficulties, particularly regarding asset ownership and registration [90].

Globally, regulatory approaches have evolved from an initially hostile stance to more prudent and market-friendly strategies, emphasizing the regulation of virtual currencies, the supervision of Initial Coin Offerings (ICOs), and the legal recognition of blockchain and smart contracts [88]. With the increasing use of blockchain in the private sector, understanding its legal implications and associated risks is becoming increasingly essential for stakeholders [89].

Business adoption and new applications

Recent research highlights the growing adoption and diverse applications of blockchain technology across various commercial sectors. Studies indicate a significant increase in scientific publications on blockchain over the past five years, with applications extending to medicine, insurance, banking, and transactional services [91]. Empirical evidence suggests that companies are investing in blockchain to optimize processes and services, although priorities vary depending on the industry and the organization's size [92, 93].

In the field of marketing, blockchain is being used to address trust issues, strengthen data security and privacy, and respond to evolving consumer expectations [94]. Despite its potential, blockchain adoption still faces challenges, and further research is needed to understand its long-term impact on organizational transformation and business models [92 – 94].

Conclusions

Blockchain has established itself as a disruptive technology with the potential to transform multiple sectors, although it still faces technical and regulatory challenges. Its integration with software engineering, database optimization, and scalable architecture design will be key to its widespread adoption [95]. As research progresses, blockchain is expected to continue evolving, enhancing transparency, security, and efficiency in data and transaction management.

In the legal and business domains, smart contracts enable the automation of contractual processes, reducing intermediaries and increasing efficiency. However, regulatory barriers persist, particularly in Latin America, concerning jurisdiction, privacy, and legal validity. At a global level, the European Union is promoting its integration into public administration, although governmental adoption remains limited due to techno-logical immaturity and the need for regulatory reforms [96].

Blockchain significantly impacts software development by strengthening security and transparency across various industries, especially in the financial sector [97]. It also transforms cybersecurity through decentralized services and innovative business models. In academia, blockchain facilitates the certification and traceability of educational credentials, potentially revolutionizing transaction management in this field [98]. Its continuous evolution will require adjustments in development strategies and technological adoption.

Future studies should be centered on technical optimalization and scalability to argument efficiency while not compromising decentralization. Database optimization of blockchain systems will drastically enhance efficiency, as well as reduce computational expenses. In addition, combining blockchain technology and artificial intelligence can strengthen security and streamline data management processes, thus opening up possibilities in various industries.

In the financial institutions, blockchain is transforming conventional systems by expanding into decentralized finance (DeFi) and digital identification systems, ensuring higher levels of user privacy and security in them. In supply chain management, its use ensures that industries like food and healthcare benefit from heightened levels of transparency and traceability. In cybersecurity, it enables decentralized protective measures that require novel privacy approaches to create equilibrium among transparency and user data protection. Additionally, its vulnerability to quantum attacks is becoming increasingly relevant, which highlights the need to analyze blockchain security in the context of quantum computing.

Its future ultimately depends on further development of the technical, regulatory, and commercial fields. Solving current issues will increase its effectiveness and hasten its application in various industries.

Author contributions: All authors contributed equally to the conception, design, research, and writing of this article. Each author participated in the literature review, analysis, and discussion of the findings. All authors re-viewed and approved the final version of the manuscript.

Acknowledgments: This article is part of the research project titled "Implementation of a Web and Mobile Platform to Strengthen the Commercialization of Artistic Production through the Use of NFTs and Smart Contracts under Blockchain Technology in the Department of Atlántico - BPIN: 2022000100083". This project is funded by resources from Colombia's General System of Royalties (SGR). The authors express their gratitude to the Ministerio de Ciencia, Tecnología e Innovación de Colombia - Minciencias for supporting the development of this research project.

Conflicts of interest: The authors declare that they have no conflict of interest regarding the publication of this article.

References

[1] D. Dzhalila et al., "A systematic literature review on blockchain technology in software engineering," *Jurnal ELTIKOM*, vol. 7, no. 1, pp. 38–49, Jun. 2023. https://doi.org/10.31961/eltikom.v7i1.725

[2] H.-Y. Paik et al., "Analysis of data management in blockchain-based systems: From architecture to governance," *IEEE Access*, vol. 7, pp. 186091–186107, 2019. https://doi.org/10.1109/ACCESS.2019.2961404

[3] S. Nathan et al., "Blockchain meets database: Design and implementation of a blockchain relational database," *Proc. VLDB Endow.*, vol. 12, no. 11, pp. 1539–1552, Jul. 2019. https://doi.org/10.14778/3342263.3342632

[4] M. Wohrer and U. Zdun, "Architecture design of blockchain-based applications," *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, pp. 1–10, Mar. 2021. https://doi.org/10.1109/BRAINS52497.2021.9569813

[5] J. A. Padilla Sánchez, "Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos," *Revista de Derecho Privado*, no. 39, pp. 175–201, Jun. 2020. https://doi.org/10.18601/01234366.n39.08.

[6] J. Simón Marco, "Blockchain, criptomonedas, contrato inteligente y otras figuras: ¿Nuevos retos para los juristas?," *CEFLegal. Revista práctica de derecho*, no. 10, pp. 41–70, Oct. 2018. https://doi.org/10.51302/ceflegal.2018.10025

[7] C. Torres-Bernal and M. N. Varela-Vielma, "Retos de los contratos inteligentes en la gobernanza de las organizaciones autónomas descentralizadas en LATAM," *Revista Politécnica*, vol. 20, no. 39, pp. 171–182, Mar. 2024. https://doi.org/10.33571/rpolitec.v20n39a12

[8] J. Caballero Martínez, "La tecnología Blockchain y su carácter integrador dentro del negocio jurídico," *Revista La Propiedad Inmaterial*, no. 35, pp. 5–41, Jun. 2023. https://doi.org/10.18601/16571959.n35.01.

[9] R. J. Palomo Zurdo, "Blockchain: la descentralización del poder y su aplicación en la defensa," *bie3: Boletín IEEE*, no. 10, 2018.

[10] M. Allende López, "Cómo desarrollar confianza en entornos complejos para generar valor de impacto social," *Banco Interamericano de Desarrollo*, 2018. http://dx.doi.org/10.18235/0001139

[11] M. Riba, "Token," *Revista Blockchain e Inteligencia Artificial*, no. 2, Jul. 2021. https://doi.org/10.22529/rbia.2021(2)08

[12] M. N. Pacheco Jiménez, "De la tecnología blockchain a la economía del token," *Derecho PUCP*, no. 83, pp. 61–87, 2019. https://doi.org/10.18800/derechopucp.201902.003

[13] M. Vega Maza, "El auge de blockchain y sus posibilidades reales de aplicación en los registros de las administraciones públicas," *IDP Revista de Internet Derecho y Política*, no. 28, pp. 109–126, Feb. 2019. https://doi.org/10.7238/idp.v0i28.3154

[14] C. Dolader Retamal et al., "La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas," *Economía Industrial*, vol. 405, pp. 33–40, 2017.

[15] R. Enríquez Espinoza, "Blockchain, de mineros a oráculos," *Journal Boliviano de Ciencias*, vol. 18, no. 53, pp. 64–84, Dec. 2022. https://doi.org/10.52428/20758944.v18i53.381

[16] F. Serale et al., "Blockchain en la administración pública: ¿Mucho ruido y pocos bloques?," *Inter-American Development Bank*, 2019.

[17] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," *2018 IEEE Int. Conf. Innov. Res. Dev. (ICIRD)*, May 2018. https://doi.org/10.1109/ICIRD.2018.8376323

[18] P. M. Abhishek et al., "Performance evaluation of Ethereum and Hyperledger Fabric blockchain platforms," *2022 13th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Oct. 2022. https://doi.org/10.18280/isi.280227

[19] M. H. Tabatabaei et al., "Understanding blockchain: Definitions, architecture, design, and system comparison," *Comput. Sci. Rev.*, vol. 50, Nov. 2023. https://doi.org/10.1016/j.cosrev.2023.100575

[20] A. Maariz et al., "Blockchain technology: Revolutionizing data integrity and security in digital environments," *Int. Trans. Educ. Technol. (ITEE)*, vol. 2, no. 2, May 2024. https://doi.org/10.33050/itee.v2i2.435

[21] F. J. Moreno-Arboleda et al., "Comparación de dos Plataformas de Blockchain: Bitcoin y Hyperledger Fabric," *Ingeniería y competitividad*, vol. 24, no. 1, Oct. 2021. https://doi.org/10.25100/iyc.v24i1.11027

[22] P. Alzate and D. Giraldo, "Tendencias de investigación del blockchain en la cadena de suministro: transparencia, trazabilidad y seguridad," *Revista Universidad y Empresa*, vol. 25, no. 44, May 2023. https://doi.org/10.12804/revistas.urosario.edu.co/empresa/a.12451

[23] B. A. Segovia, "La defensa del interés del menor ante la irrupción de las tecnologías blockchain," *Actualidad Jurídica Iberoamericana*, no. 13, pp. 1024–1045, 2020.

[24] J. E. Ferreira et al., "Estudo de Mapeamento Sistemático sobre as Tendências e Desafios do Blockchain," *Gestão.Org*, vol. 15, Special Issue, pp. 108–117, Dec. 2017. https://doi.org/10.21714/1679-18272017v15Ed.p108-117

[25] E. Abad-Segura et al., "Blockchain technology for secure accounting management: Research trends analysis," *Mathematics*, vol. 9, no. 14, p. 1631, Jul. 2021. https://doi.org/10.3390/math9141631

[26] I. Sommerville, *Software Engineering*, 9th ed. Boston, MA, USA: Addison-Wesley, 2011.

[27] K. Pohl, *Requirements Engineering: Fundamentals, Principles, and Techniques*, 1st ed. Berlin, Germany: Springer, 2010. https://doi.org/10.1007/978-3-642-12578-2

[28] ISO/IEC/IEEE 24765:2010, *Systems and software engineering — Vocabulary*, Dec. 2010.

[29] ISO/IEC TR 24766, *Information technology — Systems and software engineering - Guide for requirements engineering tool capabilities*, Dec. 2009.

[30] ISO/IEC/IEEE 29148:2011, *Systems and software engineering — Life cycle processes - Requirements engineering*, Nov. 2011.

[31] Omprakash,Thara, Dash and Singh "A Review on NFT Marketplace," 2023-. https://doi.org/10.55248/gengpi.4.1223.123444

[32] R. Leaño Balon and I. Fabaan Hanbal, "An NFT Marketplace for Graphic Artists in Bicol Region," *Proc. Eng. Technol. Innov.*, pp. 35–54, 2024. https://doi.org/10.46604/peti.2024.13379

[33] Bautista, Betsi & Lozano, Luis & Santos, Alberto. " NFTs in the electronic market and its impact on digital art," 2022. https://doi.org/10.17268/sciendo.2022.026

[34] D. Weijers and H. Turton, "Environmentally smart contracts for artists using non-fungible

tokens," *2021 IEEE Int. Symp. Technol. Soc. (ISTAS)*, pp. 1–4, 2021. https://doi.org/10.1109/ISTAS52410.2021.9629203

[35] Q. Razi et al., "Non-fungible tokens (NFTs)—Survey of current applications, evolution, and future directions," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 2765–2791, 2024.

[36] Arakcheev, Artem., "Contract Smarter: Advancing Law with Technologies (Presentation)," 2024. https://doi.org/10.13140/RG.2.2.20954.96966.

[37] Y. Mhatre et al., "Challenges of implementing an NFT marketplace," *Int. Res. J. Eng. Technol. (IRJET)*, vol. 9, no. 5, pp. 323–327, 2022. https://doi.org/10.22214/ijraset.2023.49046

[38] K. E. Wiegers and J. Beatty, *Software Requirements*, 3rd ed. Redmond, WA, USA: Microsoft Press, 2013.

[39] Herranz, Raúl & Mamoghli, Noel & Yazyi, Sergio & Vera, José & González, Edgar & Matulis, Daniel & Ratón, Victor & Salas, Miguel & Arauzo, Salvador & Farias, Felipe, "Scrum Distribuido,".2011

[40] A. Llanque et al., "Metodologías Centradas en el Usuario para la Ingeniería de Requisitos," *ReCIBE*, vol. 11, no. 1, pp. C2–14, 2022.

[41] NICSI, "NICSI-PBD-SRS Template 830-1998 -13082019-V1.0," 2019.

[42] S. Banaeian Far et al., "A review of non-fungible tokens," 2022. https://doi.org/10.1109/IOTM.001.2200244

[43] R. Singh et al., "A systematic literature review on blockchain-based smart contracts," *Distrib. Ledger Technol.*, Nov. 2024. https://doi.org/10.1145/370474

[44] C. Mohan, "State of public and private blockchains: Myths and reality," *Proc. 2019 Int. Conf. Manag. Data*, 2019. https://doi.org/10.1145/3299869.3314116

[45] M. Raikwar et al., "Trends in development of databases and blockchain," *2020 7th Int. Conf. Softw. Defin. Syst. (SDS)*, pp. 177–182, 2020. https://doi.org/10.1109/SDS49854.2020.9143893

[46] B. Ravishankar et al., " Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments," *2020 Int. Conf. Mainstreaming Blockchain Implement. (ICOMBI)*, pp. 1–4, 2020. https://doi.org/10.23919/ICOMBI48604.2020.9203500

[47] S. Nathan et al., "Blockchain meets database: Design and implementation," *Proc. VLDB Endow.*, vol. 12, no. 11, pp. 1539–1552, Jul. 2019. https://doi.org/10.14778/3342263.3342632

[48] L. Balduf et al., "Dude, where's my NFT: Distributed infrastructures," *DICG '22*, pp. 1–6, 2022. https://doi.org/10.1145/3565383.3566106

[49] Davoudi, Mansour & Ghavipour, Mina & Sargolzaei-Javan, Morteza & Dinparast, Saber. (2023). Decentralized Storage Cryptocurrencies: An Innovative Network-Based Model for Identifying Effective Entities and Forecasting Future Price Trends. https://doi.org/10.21203/rs.3.rs-3127291/v1.

[50] Nanayakkara, Samudaya & Rodrigo, M.N.N. & Perera, Srinath & Weerasuriya, Thilini & Hijazi, Amer, "A Methodology for Selection of a Blockchain Platform to Develop an Enterprise System," 2021. https://doi.org/10.1016/j.jii.2021.100215

[51] F. Casino et al., "A systematic literature review of blockchain-based applications," *Telemat. Inform.*, vol. 36, pp. 55–81, 2019. https://doi.org/10.1016/j.tele.2018.11.006

[52] Yang, Qinglin & Huang, Huawei & Lin, Kaixin & Wu, Jiajing. "An Introduction to Web3 and Metaverse,"2023. https://doi.org/10.1007/978-981-99-3648-9.

[53] Z. Zheng et al., "An overview of blockchain technology," *2017 IEEE Int. Congr. Big Data*, pp. 557–564, 2017. https://doi.org/10.1109/BigDataCongress.2017.85

[54] W. Stallings, *Cryptography and Network Security*, 7th ed. Pearson, 2017.

[55] E. Ben Sasson et al., "Zerocash: Decentralized anonymous payments from bitcoin," *2014 IEEE Symp. Secur. Privacy*, pp. 459–474, 2014. https://doi.org/10.1109/SP.2014.36

[56] M. C. L. Jieyi Long, "Non-fungible token (NFT) based digital rights management," *US Patent US11075891B1*, 2021.

[57] H. T. Bao Tran, "Non-fungible token (NFT)," *US Patent US20210256070A1*, 2021. https://doi.org/10.3390/fintech1040023

[58] M. Fahmideh et al., "Engineering blockchain based software systems," *ACM Comput. Surv. (CSUR)*, vol. 54, no. 3, pp. 1–35, 2021. https://doi.org/10.1145/3530813

[59] P. Jagwani et al., "Blockchain technology and software engineering practices," *Int. J. Syst. Assurance Eng. Manag.*, vol. 14, no. 1, pp. 1–17, 2023.

[60] López Jiménez, D., "Blockchain: aspectos tecnológicos, empresariales y legales," 2020. https://doi.org/10.32870/Pk.a10n18.421

[61] V. Buterin, "Ethereum: A next-generation cryptocurrency and decentralized application platform,". First version 53 (2014).

[62] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, vol. 2018-January, Apr. 2018, doi: 10.1145/3190508.3190538

[63] L. Ante, "Smart contracts on the blockchain – A bibliometric analysis and review," *Telemat. Inform.*, vol. 57, 2021. https://doi.org/10.1016/j.tele.2020.101519

[64] M. Abdelhamid and G. Hassan, "ICSIE '19: Proceedings of the 8th International Conference on Software and Information Engineering," pp. 91–95, Apr. 2019. https://doi.org/10.1145/3328833.3328865

[65] A. Alamsyah and N. Salsabila, "Exploring the mechanisms of decentralized finance (DeFi) using blockchain technology," *3rd Int. Conf. Creative Commun. Innov. Technol. (ICCIT)*, Aug. 2024.

https://doi.org/10.1109/ICCIT62134.2024.10701148

[66] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. https://doi.org/10.2139/ssrn.3440802

[67] Bhuvana R and Sreeramana Aithal, " Blockchain based Service: A Case Study on IBM Blockchain Services & Hyperledger Fabric," 2020. [Online]. https://doi.org/10.47992/IJCSBE.2581.6942.0064

[68] G. Tripathi et al., "A comprehensive review of blockchain technology," *Decis. Anal. J.*, vol. 9, Oct. 2023.

[69] V. Buterin, "A next-generation smart contract and decentralized application platform," *Ethereum Whitepaper*, 2017. https://doi.org/10.1007/978-981-15-3376-1_5

[70] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," in *Handbook of Research on Blockchain Technology*, Academic Press, 2020, pp. 373–406. https://doi.org/10.1016/b978-0-12-819816-2.00015-0

[71] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *Polkadot White Paper*, 2017.

[72] S. S. Mohammed Abdul et al., "CrossDeFi: A novel cross-chain communication protocol," *Future Internet*, vol. 16, no. 9, p. 314, 2024.

[73] E. Buchman, " Unlocking the Potential of Interconnected Blockchains: A Comprehensive Study of Cosmos Blockchain Interoperability," 2024. https://doi.org/10.1109/ACCESS.2024.3497298

[74] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Yellowpaper*, 2014.

[75] B. Sletten, *WebAssembly: The Definitive Guide*, O'Reilly Media, Inc., Dec. 2021.

[76] N. Dragoni et al., "Microservices: Yesterday, today, and tomorrow," in *Present and Ulterior Software Engineering*, Springer, Cham, 2017. https://doi.org/10.1007/978-3-319-67425-4_12

[77] Hyperledger Fabric, "Hyperledger Fabric documentation," 2023.

[78] OpenZeppelin, "Smart contract security best practices," 2023.

[79] C. de P. Bianchini et al., "Avaliação de desempenho de transações da rede blockchain Ethereum," *Cuadernos de Educación y Desarrollo*, vol. 16, no. 11, 2024. https://doi.org/10.55905/cuadv16n11-116

[80] D. B. de Oliveira et al., "Avaliação de desempenho de transações em protocolos blockchain," *Simpósio em Sistemas Computacionais de Alto Desempenho*, 2022. https://doi.org/10.55905/cuadv16n11-116

[81] S. Toxanov et al., "Analysis of the impact of sharding on the scalability and efficiency of blockchain technologies," *Sci. J. Astana IT Univ.*, pp. 66–74, 2024. https://doi.org/10.1145/3532640.3532642

[82] J. J. Barreno Arreaga et al., "Análisis del uso de blockchain en auditoría financiera," *Revista Social Fronteriza*, vol. 4, no. 5, 2024. https://doi.org/10.59814/resofro.2024.4(5)500

[83] G. Llambias et al., "Blockchain interoperability: A feature-based classification framework," *CLEI Electron. J.*, vol. 25, no. 3, 2023. https://doi.org/10.19153/cleiej.25.3.4

[84] I. A. Qasse et al., "Inter blockchain communication," *ArabWIC 6th Annu. Int. Conf. Res. Track*, 2019. https://doi.org/10.1145/3333165.3333167

[85] R. D. Mendonça et al., "Mecanismos de Interoperabilidade em Blockchains," *Workshop em Blockchain*, pp. 15–28, 2024. https://doi.org/10.5753/wblockchain.2024.2332

[86] B. Bradach et al., "A gateway-based interoperability solution for permissioned blockchains," *2022 XVLIII Latin American Computer Conference (CLEI)*, 2022. https://doi.org/10.19153/cleiej.26.2.5

[87] I. Lianos et al., *Regulating Blockchain: Techno-Social and Legal Challenges*, Oxford University Press, 2019. https://doi.org/10.1093/oso/9780198842187.003.0001

[88] S. Blemus, "Law and blockchain," *SSRN Electron. J.*, 2018. http://dx.doi.org/10.2139/ssrn.3080639

[89] L. Mendoza Munar and A. A. Riascos Diaz, "Aspectos jurídicos de la tecnología blockchain," *Law, State and Telecommunications Review*, vol. 13, no. 1, 2021. https://doi.org/10.26512/lstr.v13i1.29262

[90] A. Legerén-Molina, "Retos jurídicos que plantea la tecnología de la cadena de bloques," *Revista de Derecho Civil*, vol. 6, no. 1, pp. 177–237, 2019.

[91] C. E. Remolina-Medina, "Análisis Bibliométrico de Blockchain," *Revista científica anfibios*, vol. 6, no. 2, pp. 56–69, 2023. https://doi.org/10.37979/afb.2023v6n2.137

[92] O. Lage et al., "Real business applications and investments in blockchain technology," *Electronics*, vol. 11, no. 3, 2022. https://doi.org/10.3390/electronics11030438

[93] O. Lage et al., "The value and applications of blockchain technology in business," *Blockchain and Applications*, Springer, 2021, pp. 149–160. https://doi.org/10.1007/978-3-030-86162-9_15

[94] P. Huijbregts Jaén, "Aplicaciones de la tecnología blockchain en marketing," *Revista de Marketing y Publicidad*, 2021. https://doi.org/10.51302/marketing.2021.706

[95] M. A. Burgos Rojas et al., "El impacto del Blockchain en la cadena de suministros," *INGENIERÍA INVESTIGA*, vol. 4, 2022. https://doi.org/10.47796/ing.v4i0.708

[96] S. Almeida et al., "An approach to develop software that uses blockchain," *Advances in Intelligent Systems and Computing*, Springer, 2018, pp. 346–355. https://doi.org/10.1007/978-3-319-91186-1_36

[97] O. Lage Serrano and M. Saiz Santos, "Blockchain and the decentralisation of the cyber-security industry," *DYNA*, vol. 96, no. 3, p. 239, 2021. https://doi.org/10.6036/10188

[98] A. M. Moreno-Ballesteros, "La blockchain para transmitir, trazar y certificar valor," *Revista Docencia Universitaria*, 2021. https://doi.org/10.18273/revd.vesp1-2021030