LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

EXPLORING THE POTENTIAL AND USE CASES OF BLOCKCHAIN TECHNOLOGY IN COLOMBIAN EVIDENTIARY LAW: CHALLENGES AND OPPORTUNITIES.

Andres Felipe Adarme Niño[1]

[1]Universidad Libre de Colombia, Bogota
https://orcid.org/0009-0000-1412-044X

andresf-adarmen@unilibre.edu.co[1]

Abstract
Blockchain technology has been presented as a revolutionary tool with enormous potential to change justice systems, especially when it comes to the right to evidence. Their capacity to guarantee integrity, completeness, authenticity, and traceability of data creates new possibilities for enhancing trust and efficacy in judicial processes. This paper examines the primary applications of blockchain technology within the Colombian evidence system, which are classified into three approaches: The use of blockchain in legal proceedings encompasses two primary applications: (i) the substantiation of factual claims, and (ii) the preservation of evidence through the implementation of unalterable records and timestamps that are subject to verification. Beyond its role within the judicial context, blockchain has a significant function in the realm of document creation and validation. This application extends to domains such as intellectual property and notarial law. Employing a qualitative approach and a document analysis grounded in legal, technological, and comparative literature, the benefits, limitations, and technical and legal challenges related to its adoption are examined. The findings indicate that blockchain has the potential to function as an effective instrument for enhancing legal certainty, transparency, and the validity of evidence in Colombia, provided that it is employed in conjunction with regulatory modifications, institutional training, and technical standards that are interoperable and designed to facilitate its integration into the prevailing judicial system.

Keywords: Blockchain, Evidentiary Law, use cases, evidence, authenticity, Means of proof, Intellectual Property, Insurtech, Notarial Law.

1. Introduction

In the past decade, distributed ledger technology, more commonly referred to as blockchain, has evolved from its initial application in cryptocurrencies to permeate a diverse array of technological, economic, and legal domains. The system's primary feature is a decentralized, permanent, verifiable registry that can track data blocks. This feature is noteworthy as an innovative solution to the challenges posed by conventional systems in the domains of evidence, conservation, and validation. As De Filippi and Hassan (2018) have noted, blockchain can be regarded as a "regulatory technology" that transforms the relationship between code, trust, and legality. In this paradigm shift, the traditional "code is law" model gives way to a new model in which "law is code."

In this context, the evidentiary process is undergoing a necessary change. The proliferation of digital evidence, the internationalization of transactions, and the increase in complex crimes (e.g., cyber, financial, and cross-border) have exposed the limitations of conventional models for preserving, authenticating, and safeguarding evidence. This has led to a growing demand for enhanced transparency and efficiency in the judicial system. It is imperative to recognize the significance of three fundamental elements in ensuring the validity and efficacy of evidence. These elements encompass integrity, control of the chain of custody, verification of origin, and the guarantee that data have not been denied. Additionally, the possibility of auditing and certifying evidence is crucial.

In Colombia, the field of evidentiary law faces particular challenges that condition the application of justice in an increasingly digital environment. Among the aforementioned

challenges are: The following factors must be considered when assessing the reliability of digital evidence:

- The susceptibility of digital evidence to alterations, destruction, or manipulation
- The lack of clear and uniform criteria for the preservation of electronic evidence
- The limited interoperability between institutional platforms of different types (forensic, judicial, technological)
- The lack of a solid institutional culture on the digitization and validation of means of evidence
- The normative difference between traditional regulations and the requirements of technological testing in hybrid contexts This combination of factors limits not only legal certainty, but also the confidence of the State and citizens in evidentiary processes. Consequently, this has a direct impact on the effectiveness of the judicial system.

The subject matter of this article can be understood as the presence of a lack of regulation, technical and institutional, that hinders the full implementation of blockchain as a method of proof or form of preservation of evidence in the Colombian sphere. Specifically, at least three manifestations of this lack stand out: The following factors have been identified as contributing to the challenges associated with the acceptance of blockchain-based records as valid evidence in court:

The absence of a clear and general consensus on the acceptability of blockchain-based records as valid evidence in court.

The lack of interoperable standards and approved technological protocols that ensure that the blockchain systems used meet the criteria of integrity, traceability, and transparency.

The lack of training and awareness of judicial officials, experts, and technical entities regarding the use, evidentiary value, and risks associated with distributed ledger technologies. This situation contributes to weaknesses in the chain of custody, gaps in the validation of digital evidence, and ultimately less trust in the digital justice system.

A comprehensive review of the extant literature on the subject suggests that blockchain technology has the potential to contribute to the resolution of the aforementioned problems. For instance, Bonomi, Casini, and Ciccotelli (2018) developed the B-CoC (Blockchain-based Chain of Custody) prototype for digital evidence management, which employs blockchain technology to dematerialize the custody process by ensuring audited integrity and the tracking of owners in forensic investigations. In a similar vein, Brotsis et al. (2019) proposed a blockchain-powered solution for evidence preservation in IoT environments, establishing an immutable record of metadata with smart contracts that interact with investigative entities. In South Asia, Shahaab, Hewage, and Khan (2021) developed a conceptual model ("EvidenceChain") that enables citizens to upload digital evidence anonymously to a distributed repository, thereby circumventing the potential for corrupt individuals to destroy or manipulate information. These studies provide an empirical basis for considering the application of blockchain in evidentiary contexts. However, they also highlight that technology is not a definitive solution; its implementation necessitates regulatory adjustments, clear protocols, and an appropriate institutional transition.

However, the integration of blockchain technology into the testing system engenders structural tensions that necessitate both academic and practical scrutiny. On the one hand, the immutability of the blockchain registry gives rise to inquiries regarding the right to privacy, the protection of personal data, and the principle of proportionality in the preservation of digital evidence (Belen-Saglam, Altuncu, Lu, & Li, 2022). Conversely, the decentralization of the registry prompts inquiries into the conventional models of custody and control of evidence by the State. This could potentially conflict with the

preservation, access, and auditing obligations of justice agencies. Furthermore, the certification, validation, and auditing of blockchain platforms persist in exhibiting a discrepancy between their technical level, characterized by cryptography, consensus mechanisms, and nodes, and their legal level, encompassing admissibility, chain of custody, and expertise. This finding indicates that, while technology offers substantial theoretical capabilities, its practical value is contingent on the institutional framework that envelops it.

In the context of Colombia, despite the implementation of digitalization projects in the judicial field, such as digital signatures, electronic files, and pilot tests of electronic registration, there is still regulatory dispersion and uneven application that restricts the effectiveness of the digital evidence ecosystem. The objective of this analysis is to explore the most pertinent applications of blockchain technology in the domain of Colombian evidentiary law. These applications include its use as a medium for presenting evidence in legal proceedings, as a mechanism for safeguarding evidence, and as a tool for extrajudicial validation of documents. The analysis seeks to identify the advantages of blockchain technology, the technical and legal obstacles that may impede its implementation, and the possibilities for policy and institutional coordination in this regard. This type of analysis serves not only to detail the current state, but also to develop a practical route for its integration into the Colombian testing system.

In terms of methodology, this research employs a qualitative approach that is predicated on the analysis of documents, with consideration given to legal, technological, and comparative literature. A comprehensive perspective is presented on the relationship between blockchain technology and the current legal framework of evidence in Colombia. This perspective is derived from a synthesis of doctrinal research, articles from academic publications, technical reports, and implementation experiences. The objective of this examination is to propose a series of recommendations. These recommendations are intended to facilitate the design of adapted regulations, technical certification protocols, interoperability between institutions, and the development of specific skills. The development of these skills is intended to support the management, evaluation, and presentation of digital evidence based on blockchain.

The significance of this study lies in its contribution to both the academic field and its practical application. By integrating novel technological advancements with the framework of evidentiary law in Colombia, a pathway to fortify legal certainty, enhance transparency in judicial proceedings, optimize digital evidence management, and, in essence, nurture a more dependable and contemporary justice system is paved. The examination of case studies concerning the employment of technology and the barriers encountered by institutions will furnish insights to policymakers, legal practitioners, legal technology experts, and members of academia. This will, in turn, stimulate an interdisciplinary discourse, a pivotal element in the advancement of digital justice.

2. Theoretical framework

1. Evolution of Blockchain Technology

The genesis of blockchain technology can be traced back to the proposal put forth by Satoshi Nakamoto in 2008. This seminal contribution involved the conceptualization of a decentralized digital currency system, underpinned by cryptography and a distributed consensus model. While the inaugural implementation of blockchain technology was Bitcoin, its potential to transcend the financial sector was swiftly recognized (Antonopoulos, 2017; Gupta, 2018). At its core, blockchain is described as a database that is distributed and overseen by various nodes within a network. These nodes validate

transactions using cryptographic algorithms and consensus methods. This design eliminates the need for a central agent, ensuring the permanence and integrity of records (Swan, 2015).

Since the 2010s, prominent scholars such as Tapscott and Tapscott (2016) and De Filippi and Wright (2018) have contributed to the expansion of the understanding of blockchain. These scholars have characterized it as an "institutional digital infrastructure" with the potential to transform forms of trust, governance, and verification in social and legal contexts. Its evolution can be categorized into three generations: the initial one, which pertains to the registration of transactions; the second, which is marked by the incorporation of smart contracts (Buterin, 2014); and the third, which ushers in decentralized applications and hybrid models of digital governance (Pérez, 2021).

The advancement of distributed ledger technologies (DLT) has enabled the proliferation of their applications in domains such as health, logistics, public administration, and the legal sector (World Economic Forum, 2020). In the domain of law, the surge in interest in blockchain is attributable to its capacity to guarantee the authenticity and traceability of evidentiary data (Risius & Spohrer, 2017). The capacity to inscribe data in a manner that is both indelible and resistant to modification offers a technical solution to the challenges posed by fraud, tampering, and the loss of evidence.

2. Technical and legal principles: immutability, transparency and traceability

The blockchain is predicated on three fundamental technical principles that bear significant legal ramifications: immutability, transparency, and traceability. Immutability is a property that signifies the inability of stored records to undergo modification without inducing alterations to the entire chain. This is due to the incorporation of a cryptographic code (hash) from the preceding block within each block. This mechanism offers a level of certainty that exceeds that of conventional centralized systems (Rodeck & Curry, 2022).

Transparency is a characteristic of most blockchains due to their public or auditable nature, which allows for the verification of information without the intervention of third parties, thereby reinforcing institutional trust (Tapscott and Tapscott, 2016). Finally, traceability ensures that the complete sequence of transactions or events can be reconstructed, which is essential in judicial scenarios, where continuity and chain of custody are decisive for the probative value of evidence (Bonomi, Casini, & Ciccotelli, 2018).

From a legal vantage point, these principles are congruent with the stipulations of authenticity, integrity, and availability as outlined by international regulations concerning electronic evidence. In Colombia, Law 527 of 1999 stipulates that data messages are admissible as documents, contingent upon their ability to meet criteria pertaining to integrity and reliability. In accordance with this definition, records created using blockchain can be regarded as valid documentary evidence (Peñaranda Rodríguez, 2019). However, as Belen-Saglam et al. (2022) have noted, the tension between technical inalterability and data protection rights (e.g., the right to be forgotten) poses significant regulatory challenges. The incapacity to modify or delete records has the potential to be in conflict with privacy regulations. Consequently, there has been an examination of hybrid approaches, such as the storage of on-chain metadata and content externally, as methods to achieve a balance between security and confidentiality (Deloitte, 2021).

3. Evidence in the digital age

The advent of digital technologies has precipitated significant transformations in the realm of evidence, thereby warranting a reevaluation of its nature and function. Gómez (2020) asserts that the evolution of judicial processes towards digital formats necessitates a reconceptualization of the notion of a document, along with its authenticity and evidentiary value. In Colombia, the General Code of Procedure (Law 1564 of 2012) acknowledges the validity of data messages and establishes their presumption of authenticity, thereby establishing an appropriate regulatory context for the acceptance of digital evidence.

However, in practice, there remain technological and institutional mismatches. Judges, lawyers, and experts lack the requisite training in information technologies. Moreover, the infrastructure of the judicial system does not yet ensure interoperability between document management systems, electronic files, and evidence repositories (Castellanos, 2020). This issue is further compounded by the absence of consistent jurisprudential criteria to evaluate electronic evidence, particularly in cases where the integrity of digital records is contested.

The prevailing theoretical perspective highlights the necessity of perceiving the digitization of evidentiary law not merely as a technological endeavor, but rather as a reevaluation of the value of evidence from an epistemological standpoint (Vargas Osorno, 2021). The credibility of a document is no longer contingent solely on its physical format; rather, it is determined by the reliability of the technological system that ensures its preservation and traceability (Sun & Wu, 2023). In this particular context, the implementation of distributed technologies, such as blockchain, appears to be a rational extension of the fundamental principles of public trust and document authenticity.

4. Connection between Blockchain and evidentiary law

The relationship between blockchain technology and evidentiary law can be examined through three primary lenses:

The employment of documentation serves as a means of recording and authenticating evidence at a specific point in time.

(ii) as a judicial mechanism to preserve evidence, thereby guaranteeing the inalterability and traceability of records.

As posited by Lu (2020) and Sumner (2025), the practice functions as an extralegal instrument for the authentication and preconstitution of documents.

From a theoretical standpoint, these applications are predicated on the doctrine of the data message and on the functional equivalence between physical and digital media. Peñaranda Rodríguez (2019) posits that blockchain records satisfy the integrity and authenticity criteria stipulated by Law 527 of 1999, thereby conferring upon them the status of electronic documents. However, Vargas Osorno (2021) cautions that its evaluation necessitates technical expertise, wherein the cryptographic elements are translated into a language comprehensible to the judge. This underscores the importance of specialized training.

Comparative law offers illuminating examples. In the Asian country of China, Internet Courts have adopted blockchain technologies to manage digital evidence, thereby granting online records a presumption of veracity (Lu, 2020). In Italy and in Washington State in the United States, legislation recognizes the legal validity of temporary stamps generated using decentralized ledger technology. These situations demonstrate that blockchain does not supplant traditional principles of proof; rather, it fortifies them through automated verification methods (Sun and Wu, 2023).

5. Theoretical contributions and gaps in the literature of Colombia

The relationship between blockchain technology and evidentiary law can be examined through three primary lenses:

The employment of documentation serves as a means of recording and authenticating evidence at a specific point in time.

(ii) as a judicial mechanism to preserve evidence, thereby guaranteeing the inalterability and traceability of records.

As posited by Lu (2020) and Sumner (2025), the practice functions as an extralegal instrument for the authentication and preconstitution of documents.

From a theoretical standpoint, these applications are predicated on the doctrine of the data message and on the functional equivalence between physical and digital media. Peñaranda Rodríguez (2019) posits that blockchain records satisfy the integrity and authenticity criteria stipulated by Law 527 of 1999, thereby conferring upon them the status of electronic documents. However, Vargas Osorno (2021) cautions that its evaluation necessitates technical expertise, wherein the cryptographic elements are translated into a language comprehensible to the judge. This underscores the importance of specialized training.

Comparative law offers illuminating examples. In the Asian country of China, Internet Courts have adopted blockchain technologies to manage digital evidence, thereby granting online records a presumption of veracity (Lu, 2020). In Italy and in Washington State in the United States, legislation recognizes the legal validity of temporary stamps generated using decentralized ledger technology. These situations demonstrate that blockchain does not supplant traditional principles of proof; rather, it fortifies them through automated verification methods (Sun and Wu, 2023).

3. Methodology

The present study was conducted using a qualitative approach, grounded in a meticulous analysis of pertinent documents. This method was employed to meticulously examine the potential, constraints, and challenges associated with the integration of blockchain technology within the domain of evidentiary law in Colombia. The selection of this approach is substantiated by the exploratory and theoretical nature of the topic in question. This nature demands an interpretative understanding of legal and technological phenomena based on secondary academic, normative, and doctrinal sources.

3.1 Research approach and design

According to Hernández Sampieri, Fernández Collado, and Baptista (2018), the qualitative approach is appropriate when the objective is to understand complex situations within their natural context, interpreting meanings and interactions. In this case, it was decided to use a design that is not experimental, cross-sectional, and descriptive, since no variables were altered. However, the phenomenon of blockchain was studied in its current state of development, both theoretical and practical, in relation to evidentiary law.

The study was meticulously organized through a systematic and critical review of various academic sources, institutional reports, and policy papers dealing with the connection between distributed ledger technologies (DLT) and digital evidence. This approach facilitated the identification of the prevailing conceptual frameworks, application models,

and theoretical debates on the international level. Furthermore, it enabled the analysis of the potential adaptation of these frameworks and models to the context of Colombia.

3.2 Types and sources of information

The research was based on secondary sources obtained from scientific and technical literature, which were selected according to criteria of relevance, timeliness, and academic rigor. A review of articles published in recognized databases, including Scopus, Web of Science, SpringerLink, Taylor and Francis, and Google Scholar, was conducted. Additionally, technical reports produced by international organizations, such as the World Economic Forum, Deloitte, EY, and IBM, as well as official regulatory documents generated by the Congress of the Republic of Colombia and the Ministry of Information and Communications Technologies (MinTIC), were also reviewed.

Specifically, significant doctrinal research by authors such as De Filippi and Wright (2018), Tapscott and Tapscott (2016), Bonomi, Casini, and Ciccotelli (2018), Vargas Osorno (2021), and Peñaranda Rodríguez (2019) was examined, providing a robust conceptual foundation concerning the relationship between blockchain and digital evidence. The triangulation of sources was instrumental in facilitating the articulation of technological, legal, and comparative perspectives. This approach ensured a comprehensive vision of the object of study.

3.3 Analysis process

The documentary analysis was carried out in three successive phases:

Identification and selection of documents: inclusion criteria were established that prioritized peer-reviewed academic publications, reports from institutions, and current regulations. Unverifiable sources or sources that did not meet scientific standards were discarded.

Coding and thematic classification: the content was organized according to the previously defined axes of analysis:

- Blockchain as a means of proof in legal proceedings.
- Blockchain as a judicial mechanism for the preservation of evidence.
- Blockchain as an out-of-court tool for document authentication.

This classification facilitated the systematization of the information and the establishment of conceptual relationships between the literature analyzed.

A critical analysis and interpretation was conducted by comparing the global findings with Colombian legislation (Law 527 of 1999, Law 1564 of 2012, and Law 1581 of 2012). The analysis identified similarities, conflicts, and regulatory gaps. The study also examined the influence of technical, legal, and operational factors on the incorporation of blockchain within the testing system at the national level.

The analysis employed legal hermeneutics as an interpretative method, thereby facilitating a comparison of the principles of evidentiary law (i.e., authenticity, integrity, veracity, and burden of proof) with the fundamental properties of blockchain technology (i.e., immutability, transparency, and traceability). This perspective fosters an interdisciplinary dialogue between the legal sphere and technological innovation, aligning

with the qualitative interpretative methodology proposed by Flick (2018) and Creswell (2014).

3.4 Validity, reliability and methodological rigor

In order to ensure the internal validity and reliability of the study, various strategies of source triangulation and cross-review of information were implemented. A variety of academic, normative, and technical approaches were considered, with the objective of avoiding interpretative biases or over-reliance on a single type of source. Furthermore, the phases of the analysis were systematically documented, ensuring the traceability of the arguments and conclusions. This approach adhered to the standards of rigor established by Lincoln and Guba (1985) for qualitative research.

The ethical principles that govern documentary research were taken into account, including respect for intellectual property, verification of sources, and clarity in the citation. The selection of references was made on the basis of their theoretical relevance and their applicability in the domain of digital evidentiary law.

3.5 Scope and limitations of the study

The present study adopts an exploratory-descriptive approach, as its objective is to elucidate the conceptual and practical underpinnings of blockchain implementation in the context of evidentiary law. This undertaking does not entail the quantification of variables. The primary contribution of this study is the establishment of an interpretative framework that promises to facilitate future empirical and comparative research endeavors.

A notable limitation of the analysis is its exclusive reliance on documentary sources, excluding empirical validation through interviews or case studies in judicial entities. However, this restriction is counterbalanced by the exhaustive and meticulous bibliographic review, which encompasses both international theoretical frameworks and local regulations.

It is anticipated that the results of this study will serve as a valuable academic and technical resource in the development of public policies aimed at the digital transformation of justice in Colombia. The integration of blockchain technology into evidentiary processes has the potential to represent a significant advancement in the pursuit of a more transparent, effective, and secure justice administration.

4. Results

4.1 Conceptualization of Blockchain technology.

In order to conceptualize blockchain in the simplest way possible, and for academic and explanatory purposes, it is pertinent to make an analogy or simile with a ledger, such as those used to record each transaction. However, this book possesses a distinctive characteristic that sets it apart from others: it does not belong to a single individual or entity, but rather, it is a book that is collectively owned and accessed by thousands, even millions, of people and computers worldwide, concurrently.

In the context of the blockchain, the addition of a new page to the book is analogous to the insertion of a new block. This new block is characterized by the inclusion of specific information, such as a transaction involving a cryptocurrency, the details of a sale, the clauses of a contract that has been signed, or the registration of ownership of an asset. The link between each page and the preceding one is considered indissoluble and permanent. This process establishes an uninterrupted sequence of records. Once a page

has been inscribed and validated in this great book, it is virtually impossible to alter or delete it. This depiction, though a simplification, provides a concise representation of the fundamental principles underlying blockchain technology.

In its most rigorous definition, blockchain is described as a distributed and decentralized database (Di Pierro, 2017). To elucidate this concept, one may conceptualize the disparity between the storage of a singular vital file on a single individual's computer and the dissemination of that identical file across myriad computers worldwide. Each computer possesses an exact replica of the aforementioned ledger.

This distributed approach endows blockchain with noteworthy authenticity and resilience. In the event of a failure or unavailability of one of the aforementioned computers, the network would remain operational due to the replication of information in multiple other locations.

Nevertheless, the fundamental innovation of blockchain lies beyond its decentralized nature. The most impressive aspect of this technology is derived from the ingenious integration of several existing technologies, with cryptography serving as the fundamental element of this integration. Each "block" of information, which contains a group of transactions, is "sealed" with a kind of secret code or digital signature called a "Hash" and then inextricably linked to the previous block. This phenomenon is known as the "blockchain."

It is evident that each page of the aforementioned book possesses its own content, as well as a distinctive and personal imprint. The creation of this imprint necessitates the adherence to specific criteria, and its successful execution is contingent upon the foundation established by the preceding page. Any attempt to modify a detail, regardless of its apparent insignificance, will result in the emblem's fracturing, rendering the subsequent sliding emblem devoid of value. It would be a remarkable occurrence, akin to extracting a page from a meticulously crafted book and discovering that the pages surrounding it have been systematically peeled away, irreparably divulging the intervention (Rodeck & Curry, 2022). This encrypted architecture is the foundation for modern security and immutability, which, prior to the advent of blockchains, were regarded as impractical ideals.

It is imperative to acknowledge that the potential of blockchain technology extends well beyond the realm of cryptocurrencies and digital assets. While Bitcoin and Ethereum are the most prominent examples of its implementation, the immense capacity of this technology enables its integration into various domains, including logistics, health services, public administration, and notably, the protection of intellectual property.

In 2014, Vitalik Buterin's proposal to incorporate smart contracts into Ethereum represented a significant advancement for blockchain technology. Buterin (2014) asserts that this advancement transformed blockchain from a rudimentary transaction record system to a sophisticated system capable of automating and verifying processes without the need for intermediaries. Consequently, this paradigm shift has engendered an environment conducive to the development of novel concepts that challenge established norms. Supply chains exemplify this phenomenon, as they facilitate the creation of an immutable record that documents each phase in the trajectory of a product. This level of openness was previously thought to be impossible (IBM, 2024; World Economic Forum, 2020).

The blockchain technology has the capacity to assist in verifying the provenance and precision of digital files stored within the network. This indicates the authenticity of the information provided (Binance Academy, 2023). Consequently, this protocol significantly increases the probability of accurate certification of documents. Individuals

have greater agency over their personal information, facilitating the monitoring of their digital identities. This development implies that individuals will no longer be as dependent on centralized databases, which have been shown to compromise security (Deloitte, 2021).

In the domain of insurance, Insurtech solutions leveraging smart contracts facilitate the automated disbursement of compensation upon the fulfillment of predetermined criteria. Moreover, this expedites processes and mitigates the risk of fraud (EY, 2021). Finally, the benefits of blockchain extend to the realm of intellectual property. The technology facilitates the registration of works by artists and creators on the network, thereby establishing a clear record of their authorship. Additionally, it simplifies the management of related rights (WIPO, 2021).

In light of the aforementioned points, it is evident that the potential of blockchain technology is most evident in the realm of legal practice, encompassing a broad spectrum of real-world applications. The subject has been demonstrated to possess a considerable degree of additional value, particularly within the domain of testing. The creation of records that are impervious to modification, readily locatable, and subject to verification by any individual without the necessity of intermediaries constitutes a notable benefit.

4.2 The Blockchain as a means of proof or as an object of proof within a Judicial process.

The central objective of this study is to examine the potential of blockchain technology to transform the legal landscape of evidence in Colombia. This challenge is situated at the intersection of cutting-edge technological development and the regulatory framework that has historically defined our society. At this juncture, it is imperative that we proceed with the development of the second half of our initial premise, which is, specifically, to discern how the decentralized architecture of the blockchain is articulated and, at certain times, responds to the rules that govern the strength and admissibility of evidence in the country. This section is dedicated to this inquiry, and it will do so based on a methodical examination of the capacity of said system to become a means of evidence within the current regulatory framework.

In any judicial proceeding, evidence constitutes the central axis of the debate and the basis on which the competent authority builds its decision. In order to form a conviction, a judge requires evidence that is both robust and transparent in terms of the facts presented. Consequently, respect for the rules and principles that govern evidentiary activity is indisputably an indispensable requirement for the proper exercise of legal knowledge.

In the specific case of Colombian evidentiary law, the weight of documentary truth becomes even more evident when trying to combine blockchain with our procedural scheme. In the contemporary context, the digital landscape has evolved from a mere add-on to a foundational substrate that will determine the resolution of both established and emerging uncertainties.

Prior to exploring the potential applications and benefits of blockchain technology in evidentiary contexts, it is imperative to pose a fundamental question: Can this technological innovation be considered a valid form of evidence within the legal system? In order to address any potential concerns, it is imperative that a thorough examination of the provisions outlined in the General Code of Procedure (CGP) and Law 527 of 1999 be conducted. These legal instruments govern the access to and employment of data messages within the national context.

Article 165 of the General Code of Procedure presents a catalogue of the means of proof available for judicial proceedings. These include the statement of a party involved in the

legal action, a confession, an affidavit of affirmation, testimony from third parties, an expert opinion, a judicial inspection, documentary evidence, indications, reports, and others deemed useful by the presiding judge in formulating a decision. While the statement does not preclude creative interpretation, its expansiveness necessitates a reading that eschews literality in favor of openness to technological advancements in society and the potential incorporation of these advancements into the process.

To comprehend the efficacy of blockchain technology as a form of evidence, it is pertinent to cite the research conducted by Daniel Peñaranda Rodríguez, which was published in 2019 in the Department of Computer Law at the Universidad Externado de Colombia. Peñaranda's analysis of blockchain technology as digital evidence focuses on the rules concerning data messages and their subsequent articulation in Law 527 of 1999, as established by the General Code of Procedure.

The regulations governing civil procedure, in accordance with Article 243 of the General Code of Procedure, strictly recognize data messages as a type of document within the broad spectrum of documentary evidence. Furthermore, paragraph a) of Article 2 of Law 527 provides the following operational definition: a data message is any information that, by electronic, optical, or analogous means, has been generated, sent, received, stored, or made available to a recipient.

This expansive definition engenders a substantial legal opportunity to consider blockchain as a legitimate data message within our evidentiary framework. It should be noted that this will remain contingent upon adherence to the stipulated conditions of integrity and authenticity as outlined by the pertinent regulations.

It is evident that, from a fundamental operational perspective or from a legal standpoint, blockchain technology is indisputably regarded as a data message. The underlying technology of blockchain functions as a distributed ledger within a peer-to-peer network, integrating data, operations, and transactions in a uniform and decentralized manner. Additionally, and this is of the utmost importance, blockchain employs protocols to reach a consensus that the stored information is immutable and the data is authentic. For each set of actions delineated in subsection a) of Article 2 of Law 527 that defines a data message in the acts of generating, sending, receiving, storing, and communicating, there is a functional counterpart in the dynamics of technology. The inherent properties of blockchain, as well as its adequacy to the distinctive notes of the means of proof referred to in the Law, dispel any doubt that it can be considered a data message (Peñaranda Rodríguez, 2019).

In this manner, and through a thorough examination of regional legislation, it can be unequivocally substantiated that blockchain fulfills the function of documentary evidence in the form of a data message, having satisfied the legal criteria for such consideration (Peñaranda Rodríguez, 2019). This development signifies a substantial enhancement in the adaptability of our evidentiary system to technological advancements.

Subsequent to ascertaining the capacity of the blockchain to function as valid proof, it is imperative to ensure that its authenticity remains unassailable. This point is critical because the digital essence of the blockchain, being composed of data messages, leaves it exposed to the risks of duplication and, even more worrisome, modification.

In response to this approach, the General Code of Procedure provides a presumption of authenticity from the outset. Article 244 explicitly states that "documents in the form of data messages are presumed to be authentic." This assertion establishes a preliminary threshold of confidence in electronic evidence, thereby ensuring that, for the purposes of assessment, the digital document is accorded a favorable presumption of genuineness and its suitability for the evidentiary activity. Furthermore, Article 247 of the aforementioned

statute reinforces this presumption by stipulating that documents presented in the same format in which they were generated, sent, or received, or in an alternative format that accurately reproduces their content, shall be considered as data messages. The regulatory framework pertaining to blockchain technology has been determined to confer upon it a status that facilitates its incorporation as documentary evidence in judicial proceedings. This determination is primarily based on the characteristics inherent to this technology, which have been demonstrated to fully comply with the requirements stipulated in Article 247. The immutability characteristic of blockchain ensures the integrity, fidelity, and authenticity of the data, evidence, or transactions presented in a process in which it is implemented as a guarantor of authenticity. (Peñaranda Rodríguez, 2019). At this juncture, the application of blockchain technology offers a substantial contribution to the field, exemplifying its capacity to transform Colombian evidentiary law. The aforementioned points become evident after an analysis of the provisions of Article 257 of Law 527 of 1999. It is established as a fundamental requirement for the evidentiary evaluation by the authorities that for a document to be valued as a data message, it must be presented in the original format in which it was generated, sent, or received. Alternatively, it must be presented in a format that reproduces its content with absolute accuracy, and one that guarantees the authenticity and immutability of the original format. One of the most interesting main applications of this technology is that it would represent a way of guaranteeing the fidelity and authenticity of means of proof that are extremely volatile and mutable. Such means of proof are contained in web pages or applications where they can be easily modified. In these cases, it is sometimes not possible to preserve the original format in which the document was published or sent.

In such a scenario, blockchain emerges as the optimal solution for ensuring precise adherence to the specified criteria. The system's decentralized design and cryptographically secure structure facilitate the recording and preservation of information in its entirety, ensuring its integrity and immutability. This protocol is designed to ensure the authenticity of the data message, thereby validating its use as legal evidence in court proceedings. It must be noted, however, that this does not imply that blockchain technology is the sole solution to this challenge. The innovative nature of this technology lies in its ability to augment the authenticity and probative value of documents recorded and verified within the network.

These details are of particular relevance given that, during hearings, both judges and administrative bodies lack effective systems to verify the authenticity of submitted documents, as well as methods to ensure that documents have been submitted precisely as intended. This is especially problematic in cases where document content may be subject to change, such as in the case of social media and websites.

This dearth of evidence is further compounded by persistent issues within an evolving digital justice system, including the proliferation of forged, tampered, or modified documents. It is important to note that this phenomenon was exacerbated in situations similar to the one created by the COVD-19 pandemic (Tique Álvarez, 2020). In circumstances analogous to this one, the implementation of a system such as blockchain, which is capable of ensuring the integrity of documents, has the potential to significantly enhance the judge's confidence in the validity of the data or documents presented. This approach would undoubtedly preclude individuals from relying exclusively on assumptions, thereby enhancing the robustness of the evidence evaluation process.

It is imperative to acknowledge that the mere registration of content on the blockchain does not inherently ensure its legality or authenticity in a comprehensive sense. Furthermore, it does not ensure the capacity or identity of the parties involved in legal

business transactions. The primary function of these entities is to ensure the integrity and immutability of data or transactions following their recording. Consequently, the implementation of blockchain technology does not impact the legal existence or validity of businesses registered with it. These issues fall into the category of substantive law, and if there is a dispute about them, a judge must examine them on the merits, something that this tool is not capable of doing.

Timestamping is the component of the blockchain that facilitates the verification of the authenticity of records. Conversely, the blockchain system offers irrefutable evidence that the data or transactions stored on the blockchain have remained constant since a designated point in time. This process of time-stamping renders the data both authentic and verifiable, while also ensuring its integrity and immutability. Consequently, the data's utility as evidence is significantly enhanced. In the context of blockchain technology, this sealing is achieved through a hash, defined as a unique alphanumeric sequence that serves to identify the content of a block with unambiguity. Furthermore, upon integration of this hash into the subsequent block in the chain, a continuous and unbreakable link is established between all the registered blocks.

However, upon thorough examination of the regulatory framework and the prevailing doctrinal consensus regarding the validity of blockchain as a form of evidence, it becomes evident that blockchain possesses unquestionable legitimacy within the context of a judicial process. Its integration as a medium of documentary evidence, manifesting as a data message, is a clear and indisputable assertion of its credibility and efficacy. However, it must be acknowledged that the intricacies and technical characteristics inherent in blockchain technology, a paradigm of cutting-edge innovation, present considerable challenges to the assessment of such evidence by judicial entities. This issue is explored in the scholarly work "Blockchain and its importance in evidentiary law" by Teresa Genoveva Vargas Osorno, which examines the application of blockchain technology in the context of evidentiary law. In this regard, Vargas Osorno states that in the event that the probative value of a document supported by this technology is questioned, it will be necessary to present expert evidence that demonstrates its authenticity, unless the judge has knowledge of the operation of this technology and its associated protocols. The latter scenario is, in my estimation, remote and improbable in practice, due to the dearth of knowledge among judges and judicial operators regarding this particular technology. It should be noted, however, that under certain circumstances, a judge could verify a stamping in select blockchain explorers that are available online. Nevertheless, the probability of this occurring in practice is low due to technical limitations and the complexity of the judicial system in Colombia. It is important to note that the notion of blockchain's full validity and probative value is not a recent development. Comparative law provides pertinent examples of successful implementations, such as those observed in Italy and the state of Washington. In these jurisdictions, the legal validity of records generated by Distributed Ledger Technologies (DLT) and their time stamps, among other characteristics, has been formally acknowledged. (Vargas Osorno, 2021)

Conversely, Vargas Osorno asserts that Article 244 of the General Code of Procedure establishes the presumption of data message authenticity. However, in instances where an electronic document exhibits technical intricacies that impede its comprehension through natural language, the involvement of a technical expert becomes imperative for the certification of its authenticity, chronology, and provenance. In this regard, the Constitutional Court has observed that data messages are comparable to traditional documents in terms of their probative value and legal validity, as outlined in the General

Code of Procedure. This assertion underscores the significance of recognizing that data messages, regardless of their format (i.e., whether stored on digital media or presented in their original form), should be regarded as valid evidence and subject to the same procedural safeguards as other forms of evidence. The responsibility of the judge is to evaluate the reliability of the techniques employed to ensure the integrity, traceability, and conservation of these messages. This evaluation must include ensuring their inalterability and identifying the parties involved. Ultimately, the credibility and evidentiary capacity of the content will be determined by the technology utilized. In this domain of application and within the judge's purview, the efficacy of blockchain technology is likely to be most evident. (Vargas Osorno, 2021).

Blockchain as a judicial mechanism to preserve evidence

In the preceding section, an exploration was conducted into the validity of blockchain technology as a form of evidence within a judicial context. It was demonstrated that the blockchain, with its inherent capacity to generate immutable and transparent records, is emerging as a valid form of evidence before the Colombian legal system. This development signifies a substantial potential for authentication of evidence that extends beyond the scope of judicial processes involving transactions of information or assets contained within the blockchain. Furthermore, it was elucidated that the blockchain's capacity to provide authenticity and attestation can be expanded to encompass other forms of evidence. The objective of this research endeavor is to address a critical question with particular relevance for judicial proceedings: How can blockchain technology serve as a reliable instrument for safeguarding evidence within a judicial procedure? It is imperative to consider not only the nature of the evidence that is introduced, but also the mechanisms in place to ensure its veracity throughout its life cycle. Consequently, the present study will focus on this aspect, exploring how the blockchain architecture responds to the need for a device that, within the context of Colombian law, guarantees the integrity of evidence while the procedure is underway.

A comparison of digital data with paper documents reveals a number of notable differences. Their ease of access and rapid circulation are widely acknowledged as significant advantages. However, the potential for altering, amending, or eradicating this information with minimal traceability has engendered persistent uncertainties within the context of the legal proceedings, which remain unresolved. Digital documents, electronic messages, online conversations, and audio recordings can be altered with relative ease and in a matter of seconds, which poses a significant challenge. In order to employ this evidence, it is incumbent upon the party to provide a new set of elements that demonstrate the content remains intact and that the additional burden becomes a puzzle for the judge, who seeks, in his work, to obtain a full and indisputable certainty about what is in dispute. It is imperative to confront the disconcerting inquiry that preoccupies our collective consciousness: How can we ensure the integrity of a digital file from its inception to its presentation as evidence? Conventional methods depend on extensive chains of custody, time certificates, and expert review, a set that is both laborious and vulnerable to human error. In this context, blockchain technology has the potential to transform the task of managing digital assets. The document's decentralized structure, in conjunction with the capacity for each modification to be registered with a unique temporary stamp that is resistant to alteration, facilitates the verification of document integrity with minimal human intervention and without necessitating trust in a third party.

The properties of blockchain that render it an attractive medium for the preservation of evidence have been previously delineated. These properties include the immutability of

data once recorded, the application of timestamps to each entry, and the distribution of records across multiple locations, thereby eliminating reliance on a single server or entity. To illustrate this point, let us posit the existence of an archive that is to be preserved as irrefutable evidence. The migration of the file to the blockchain entails the generation of a hash value and the subsequent annotation of that value on the chain. This process generates a unique cryptographic impression of the document at the precise moment it was registered. This hash function serves as an ultra-definition photograph of the content. The fundamental operation of the algorithm is such that the introduction of a single distinct letter results in the generation of an entirely new hash, thereby ensuring its immediate detection. The fundamental principle asserts that any modification, regardless of its extent, results in the destruction of the cryptographic print.

This hash is also sealed with an unalterable timestamp within a block in the chain. This system functions by ensuring that each piece of evidence is meticulously recorded with a date and time that is both impossible to erase or tamper with. These records are then sealed within a digital safe deposit box, which is connected to millions of other safe deposit boxes around the world. The distributed nature of the blockchain ensures that this "lockbox" cannot be compromised by a single entity, as the ledger is replicated across the network. In the event that an attempt were made to modify a record, the thousands of copies of the chain would render the attempt immediately apparent, thereby ensuring the integrity of the evidence over time. The capacity for permanent and verifiable preservation of data is a primary factor contributing to the remarkable value of blockchain technology within the judicial sector.

The notion of blockchain technology has evolved from a theoretical concept to a tangible reality, with practical applications in various legal systems across the globe. China and other countries have initiated pilot projects that have transitioned from a testing phase to regular employment in various judicial institutions. This transformation has led to the Chinese judicial system becoming an open laboratory for digitalization. The text provides not only operational figures but also lines of design and governance that are part of the international academic conversation.

Lu's (2020) study, which explores the incorporation of blockchain technology into the daily operations of Chinese courts, offers a pioneering analysis on the subject. His professional endeavors concentrate on the domains of identity verification, evidence custody procedures, and sentence enforcement. The report meticulously documents the advantages and difficulties it faces, providing a comprehensive analysis grounded in empirical data.

In order to enhance the procedural efficiency and reliability of evidentiary data, the nation has initiated the implementation of this tool for the management and certification of electronic evidence. In an effort to address these challenges, judicial entities have developed blockchain platforms that enable legal professionals to collectively upload and hash digital files, thereby creating an immutable history that can be reviewed at any time by the presiding judge. By addressing concerns regarding the legitimacy and chain of custody of electronic evidence with exactitude, this mechanism ensures its integrity and facilitates its evaluation in court.

A thorough examination of the emergence and evolution of Internet courts in China can be found in Lu's (2020) study. According to their analysis, the development of these cases prompted the early adoption of regulations that give blockchain technology a presumption of authenticity and consider it admissible evidence. Concurrently, a procedural plan was formulated that delineated the manner in which this evidence would be presented and evaluated during the trial. These assessments underscore the pivotal role that internet

courts have played in seamlessly integrating technological innovation into the legal system, transcending the conventional scope of dispute resolution.

In a similar vein, Lu (2020) has examined key developments in the Chinese regulatory advancement that used blockchain as a testing tool. The text delves into the historical development of blockchain judicial platforms, offering insights into their inception and subsequent implementation. The author notes that the Hangzhou Internet Court announced the opening of the first such structure in the country on September 18, 2018. The vessel was designated HZ JBCP.

The initiative's primary focus was on the resolution of disputes pertaining to digital copyrights, financial contracts, and Internet service contracts. Concurrently, two normative documents were promulgated to establish the detailed review criteria: the Specifications of the Electronic Evidence Platform of the Hangzhou Internet Court and the Rules for the Judicial Review of Electronic Evidence in Civil Disputes of the Hangzhou Internet Court (Lu, T. 2020).

In a similar vein, Lu T. (2020) has noted that the HZ JBCP is a consortium blockchain that exhibits notable distinctions from public and private blockchains. The HZ JBCP integrates the court, notary's office, judicial expert witness center, and certification authority ("CA") as nodes within the consortium blockchain and has the potential to expand to connect with more consortia of state bodies and social organizations. In order to comprehend the implementation of the Judicial Blockchain of Chinese Internet Courts, it is imperative to define the term "consortium blockchain." This distinction is particularly salient in the context of a potential judicial implementation of blockchain technology. Unlike a private blockchain, in which a single entity controls the network, or a public blockchain, in which anyone can join without permission, a consortium chain is operated and validated by a pre-selected group of entities. This approach offers enhanced privacy and speed relative to public networks, given the limited and known number of participants. However, it also maintains a higher degree of decentralization compared to a private blockchain, as it does not rely on a single authority (Patnaik, 2023). This hybrid model enables collaboration among multiple organizations that require secure and transparent data sharing without compromising their autonomy or subjecting their information to the public domain or the control of a single entity, as is the case with the Judicial Blockchain of the Chinese Internet Courts.

According to Lu, T. (2020), Judge Wang Jiangqiao of the Hangzhou Internet Court asserts that a primary objective of the establishment of the HZ JBCP was to "solve the credibility and usability problems of electronic evidence from the outset." That is to say, the initiative aimed to incorporate all the necessary steps for the generation, transmission, preservation, and final submission of electronic evidence on the blockchain judicial platform. The entire process was to be recorded in a reliable environment and under the supervision of all nodes. (Lu, T., 2020).

A more thorough examination of the establishment of judicial blockchain in China's internet courts is provided by Yan Sun and Yuchen Wu's (2023) research. The study focuses on the application and examination of electronic evidence preserved on blockchain within Chinese copyright judicial practice. The work under consideration is particularly illustrative in nature because it goes beyond showing how blockchain technology applies to the registration of works and protecting intellectual property. It also analyzes how judges in China examine and accept such evidence. Sun and Wu (2023) emphasize that Chinese courts have acknowledged the probative value of digital evidence that has been affected by a blockchain seal, contingent upon the substantiation that the registration procedure on the network validates the integrity and inalterability of the data

from the moment of its capture. This suggests that the court's assessment encompasses not only the existence of the record on the blockchain, but also the reliability of the process by which the evidence was initially "put on-chain."

The cases originating from China demonstrate that blockchain has transitioned from being merely an expectation to its practical implementation as a tool for the custody and validation of electronic evidence in judicial processes. These measures delineate a discernible course toward the enhancement of the reliability of evidence within a progressively digitalized milieu.

The experience of China in the realm of electronic evidence has the potential to provide a roadmap for the modernization of Colombian evidentiary law. By incorporating digital evidence with invariant hashes and time stamps, the blockchain effectively addresses the national mandate to provide evidence that, prior to being assessed, already radiates sufficient authenticity for the judge to grant it credibility. The probative value of a blockchain registration that certifies the integrity of digital data is indisputable, provided that the blockchain's immutable record can be trusted. In the event that the blockchain's integrity is compromised, the reliability of the certification is significantly diminished.

The repercussions for the judicial system's efficiency are evident. By storing evidence within a blockchain network, the expenses and time required to carry out expert opinions aimed at confirming the authenticity of the data could be minimized. This would guide the procedural debate towards the interpretation and relevance of the content, rather than the material fidelity of the content. Nevertheless, the obstacles are substantial. The integration of blockchain technology into the Colombian legal system is contingent upon the development of a robust understanding of its technical intricacies among judges, prosecutors, and other stakeholders within the legal apparatus. Concurrently, it may be imperative for the legal framework to evolve to elucidate the employment, integration, and assessment of technology within the judicial process.

Thirdly, the employment of blockchain as an extraneous judicial apparatus for the antecedent authentication of documents and evidence is posited.

The third part of the study examines how blockchain technology can emerge as an ideal out-of-court mechanism to configure reliable evidence and to authenticate legal documents from its origin. The present study will analyze its potential to strengthen legal certainty in the pre-dispute stage. This will be achieved by implementing innovative methods of registration and verification of authenticity of legal acts and documents. This inquiry will allow for the exploration of the synergy between blockchain and digital signatures. It will also address the potential incorporation of blockchain technology into the domain of notarial and registry law. Furthermore, it will evaluate the impact that this technological framework can have on the redefinition of traditional legal concepts, such as trust, public faith, and authenticity, within private legal relationships.

Within the legal framework, the notion of pre-constitution of evidence signifies the collection and preservation of evidence prior to the initiation of legal action or judicial proceedings. The primary objective of this process is to ascertain the veracity and reality of a fact or document at a given moment in time. In the event that a future lawsuit becomes a possibility, this evidence can be employed to assist in resolving the legal argument.

In the context of this research, it is imperative to distinguish between extrajudicial pre-constitution of evidence and extra-procedural or anticipated evidence. The former is defined by Article 183 of the General Code of Procedure and other provisions of the procedural statute, including Article 189, which stipulates that the practice of judicial inspection of persons may be requested as advance evidence.

Places, things, or documents that are to be the subject of a process. The extrajudicial pre-constitution referred to in this research work focuses on the mechanisms, platforms, and/or protocols of blockchain of a private nature that use "blockchain-based timestamps" or blockchain-based time stamps. The purpose of these mechanisms, platforms, and/or protocols is to guarantee the authenticity of data, files, documents, information, images, videos, and websites, among others.

An illustration of a private mechanism that implements blockchain-based time stamps is the ScoreDetect Web platform. According to Sumner (2025), this platform implements blockchain-based timestamps, which serve as a robust mechanism to verify the authenticity and originality of digital content. By recording a cryptographic hash of the content on the blockchain at a specific time, timestamps create tamper-proof proof that the content existed in that exact form at that time. This innovation enables content creators to readily substantiate the creation of a particular digital asset on a specific date and the absence of subsequent alterations. The immutable ledger of the blockchain ensures the preservation of an accurate and verifiable record of the origins of any digital file, including social media posts, images, videos, or documents. (Sumner, 2025).

The advantages of this system are evident in its ability to provide authenticity to documents, publications on web pages, or any type of digital file. As demonstrated above, the timestamp is linked to the content's hash, thereby establishing a cryptographic record of its existence in that precise format at a specific point in time. This approach has been shown to serve as an effective deterrent against plagiarism and misuse (Sumner, 2025). This notion of trust in a decentralized environment is precisely the foundation of the aforementioned concept. In the contemporary era, the certification of content origin or ownership is no longer contingent upon a centralized authority. The blockchain network, through its operation based on distributed consensus, enables each participant to verify authenticity (Sumner, 2025). Consequently, trust is no longer dependent on an intermediary and is instead founded on the strength of cryptography.

This initiative is not merely a matter of safeguarding artistic works; it is also about empowering creators to exercise complete control over their creations. By embedding the "fingerprints" of their creations in a distributed and immutable record, the authors demonstrate, in a straightforward and compelling manner, the genesis of the idea as their own, thereby refuting any claims of external origin. Consequently, the blockchain-based timestamps are facilitating the emergence of a web in which transparency is no longer a desideratum and the protection of intellectual property is democratized and reinforced, encompassing both the industry leaders and the most unassuming amateur who shares his inaugural drawing.

However, beyond its capacity to record transactions in a decentralized manner, blockchain technology has identified the digital signature as one of its most promising fields of application. The integration of these two tools has been shown to enhance the security of electronic documents significantly by ensuring the authenticity of the signatory and the integrity of the content from the moment the document is signed. The integration of blockchain technology as a support for digital signatures has been shown to enhance legal security, thereby achieving a level of solidity that was previously unattainable. When an individual executes a signature on a document by means of a blockchain-based technology solution, a cryptographic signature is generated that irrevocably links the signer's identity to the content of the document. In the event of subsequent alterations, the signature is rendered invalid. However, if the hash corresponding to the already signed document is also registered in the blockchain, an

additional layer of security and verification is added, which substantially increases the reliability of the electronic instrument.

In this context, the digital signature serves a dual purpose: it allows the signatory to be unequivocally identified and it ensures that the documentary content remains unaltered from the moment the signature was made. Consequently, the digital signature serves to strengthen confidence in the authenticity and integrity of the document in electronic environments. The blockchain, in turn, offers the guarantee that the signed document existed in an unaltered state at a precise time and that the record is public and irremovable (Marr, 2020). Consequently, a document authentication mechanism is achieved that operates at a higher level. Should future controversies emerge concerning the authenticity or date of a document, a comparison of its hash on the blockchain with the digital signature provides a degree of certainty that exceeds any available alternative. The blockchain record functions as an impartial and enduring "digital witness," thereby confirming the existence of the document at any given time and its integrity since its creation (Pérez, 2021). This assertion serves not only as evidence of its provenance but also as a testament to its enduring and unchanging nature.

Finally, the potential use cases that demonstrate full compatibility with blockchain technology are explored. It is evident that the potential of this technology is most evident in the context of notarial and registry law. This is particularly true with regard to the extrajudicial mechanisms of pre-constitution evidence and document authentication. Both fields are predicated on such fundamental pillars as public faith, legal certainty, and documentary certainty, principles that blockchain can undoubtedly substantially reinforce. The notary, in essence, functions as a notary public, serving to authenticate documents, confer legal certainty on agreements, and establish an indisputable date for the validity of acts and contracts. The blockchain technology does not negate the public's faith in the impartiality and authenticity of notaries, nor does it supplant the irreplaceable verification of parties' involvement, faculties, and consent that notaries provide. However, it has the potential to enhance and modernize notarial services, particularly within the digital realm. In instances where private documents do not necessitate mandatory notarial intervention, such as in certain policies, confidentiality agreements, or fruits of intellectual creation, the registration of their hash on the Blockchain provides a time stamp that is impervious to alteration and can be verified by any individual from any geographical location. Consequently, the ability to substantiate the existence of a file at a specific point in time is crucial. This serves as a compelling evidence, for instance, in the context of substantiating the prior existence of a right or safeguarding the ownership of a creation (Binance Academy, 2023). Conversely, the hash of public deeds, wills, or powers of attorney that have been formed by electronic means can be emphasized on a blockchain, resulting in an immutable and distributed backup of their integrity. This mechanism not only facilitates the verification of the authenticity of copies that are presented subsequently, but also incorporates a valuable guarantee against their possible loss or intentional manipulation. Conversely, public registers, irrespective of their categorization as property, commercial, or civil, serve as foundational pillars of legal certainty. These registers ensure the publicity and enforceability of the rights recorded, thereby fostering confidence in the legal system. In their current configuration, they can be understood as extensive accounting records that methodically compile both the owners and the charges that affect the assets. In this context, blockchain technology, conceptualized as a distributed ledger that is impervious to alterations, portends a possible scenario of profound transformation for these traditional systems (World Economic Forum, 2018). Undoubtedly, one of the applications that has generated the most

discussion is the digitization of the real estate registry. In a model of this nature, operations such as the transfer of a property, the constitution of a mortgage, or the creation of an easement could materialize through direct registration in the blockchain. The implementation of such a method has the potential to significantly reduce fraudulent activities, expedite transaction processes by eliminating the need for intermediaries, and substantially shorten verification times. Additionally, it would facilitate the establishment of a transparent and irreversible registry of holders (Deloitte, 2019).

5. Conclusions

The integration of blockchain technology in the domain of evidentiary law in Colombia signifies a substantial advancement towards a digital justice that is more transparent, effective, and secure. This is due to the fact that it provides technological assistance that has the potential to markedly alter the manner in which digital evidence is generated, administered, and assessed in legal proceedings. The blockchain's capacity to guarantee the immutability, integrity, authenticity, and traceability of data positions it as an optimal instrument for fortifying the fundamental tenets of the evidentiary function, including truthfulness, integrity, and the preservation of evidence. This development has the potential to enhance the reliability of documentary and electronic evidence under Colombian law, thereby fostering a greater sense of confidence in the legal system. The present study demonstrates that blockchain technology is in accordance with the provisions of Law 527 of 1999 and the General Code of Procedure (Law 1564 of 2012). These legal frameworks assign legal value to data messages and deem them to be authentic if they comply with integrity and conservation conditions. However, despite the compatibility of the rules, the practical application of this technology faces structural challenges due to the lack of adequate technological infrastructure in the judicial system, the absence of standardized technical protocols, the limited training of legal operators in the use of new technologies, and the tensions between the immutability of records and the right to protection of personal data established in Law 1581 of 2012. Consequently, the transformative capacity of blockchain technology will only be actualized through a strategic and incremental implementation that integrates regulatory reforms, institutional investment, technical training, and collaboration among the state, academia, and the private sector. A review of international examples reveals that the integration of blockchain technology into judicial systems is indeed feasible. For instance, the Internet courts in China and the European regulatory developments on identity and digital proof demonstrate the viability of blockchain within the judicial system. However, it is essential to note that this integration is predicated on the presence of several key elements. Firstly, there must be clear regulatory frameworks in place to govern the use of blockchain within the judicial system. Secondly, public audit mechanisms must be implemented to ensure transparency and accountability. Finally, technological governance frameworks must be established to ensure a balance between efficiency and fundamental rights. When these conditions are met, the integration of blockchain into the judicial system can be a successful endeavor. In this context, blockchain should not be regarded as a substitute for traditional legal institutions; rather, it should be regarded as a complementary tool that expands the capabilities of the judicial system to certify, preserve, and validate digital evidence. This, in turn, reinforces public trust, transparency, and legal certainty. Moreover, its capacity extends beyond the procedural field, encompassing the certification of notarial documents, the defense of intellectual property, the management of public records, and the validation of smart contracts. In these areas, it has the potential to contribute to the reduction of corruption, fraud, and administrative costs.

Consequently, a future emerges in which blockchain is firmly established as a pivotal element in the modernization of the judicial system, fostering citizen trust and engendering a more inclusive, traceable, and responsible justice system. However, such a transformation necessitates a profound cultural and institutional metamorphosis, predicated on an interdisciplinary comprehension of the technical and ethical ramifications of the digitization of evidence. Consequently, it is imperative that academia, legislators, and judicial entities collaborate on a unified agenda. This agenda should aspire to establish national standards for the validation of blockchain-based evidence, develop manuals of good expert practices, and establish a technical body specializing in digital evidence and technological law. In summary, blockchain technology does not supplant the conventional tenets of evidentiary law; rather, it reinvigorates them by integrating them into a cryptographic verification and distributed trust environment. This development positions Colombia to adopt a digital justice paradigm that aligns with the demands of the fourth industrial revolution and meets international standards of transparency and technological governance. The responsible and strategic adoption of this approach has the potential to establish a new evidentiary structure. This structure would be based on data security, information traceability, and institutional credibility. As a result, it would facilitate more reliable, accessible, and sustainable justice from a technological point of view.

Bibliographic references

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies.* O'Reilly Media.

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2022). A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems. *arXiv preprint arXiv:2210.04541*.

Binance Academy. (2023). *What is blockchain technology?* https://academy.binance.com/en/articles/what-is-blockchain-technology

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. *arXiv preprint arXiv:1807.10359*.

Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, E., Bellini, E., & Pavue, C. (2019). Blockchain Solutions for Forensic Evidence Preservation in IoT Environments. *arXiv preprint arXiv:1903.10770.*

Brunner, R. (2020, February 13). *How blockchain technology will impact our legal system.* Lexology. https://www.lexology.com/library/detail.aspx?g=7bc262b3-21df-47c8-9cdd-620367745c32

Buterin, V. (2014). *Ethereum white paper: A next-generation smart contract and decentralized application platform.* https://ethereum.org/en/whitepaper/

Castellanos, N. (2020, September 16). *Two months of digital justice in Colombia.* Legal Matters. https://www.asuntoslegales.com.co/consultorio/dos-meses-de-justicia-digital-en-colombia-3060788

Congress of the Republic of Colombia. (1999). *Law 527 of 1999.* Official Gazette, (43,673).

Congress of the Republic of Colombia. (2012). *Law 1564 of 2012.* Official Gazette, (48,489).

Congress of the Republic of Colombia. (2012). *Law 1581 of 2012.* Official Gazette, (48,587).

Consensys.net. (n.d.). *Blockchain in the legal industry.* https://consensys.net/blockchain-use-cases/law/
Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.
De Filippi, P., & Hassan, S. (2018). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. *First Monday, 21*(12).
De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code.* Harvard University Press.
Deloitte. (2019). *Blockchain in real estate: The next chapter.* https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-blockchain-in-real-estate.pdf
Deloitte. (2021). *Blockchain for Digital Identity.* https://www2.deloitte.com
HEY. (2021). *Blockchain in insurance: An opportunity for innovation.* https://www.ey.com/en_ca/financial-services/blockchain-in-insurance-an-opportunity-for-innovation
Flick, U. (2018). *An Introduction to Qualitative Research* (6th ed.). SAGE Publications.
García, A. (2018, October 17). *What is blockchain, what is it for, and why is it important in cryptocurrency?* ADSLZone. https://www.adslzone.net/reportajes/blockchain-que-es
Gómez, A. (2020). Digital evidence in Colombian judicial processes. *Law and Technology Journal*, 15(2), 45-67.
Gupta, M. (2018). *Blockchain for Dummies.* John Wiley & Sons.
Hernández Sampieri, R., Fernández Collado, C., & Baptista, P. (2018). *Research Methodology* (6th ed.). McGraw-Hill Education.
IBM. (2024). *Blockchain for supply chain.* https://www.ibm.com/blockchain/solutions/supply-chain
Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry.* SAGE Publications.
Lu, T. (2020). The Implementation of Blockchain Technologies in Chinese Courts. *Stanford Journal of Blockchain Law & Policy,* 4, 102.
Marr, B. (2020). *Blockchain: The definitive guide for business and finance.* Wiley.
Ministry of Information and Communications Technologies. (2012). *Decree 2364 of 2012.* Official Gazette, (48,566).
Ministry of Information and Communications Technologies. (2020, December 1). *Blockchain reference guide for adoption and implementation.* https://gobiernodigital.mintic.gov.co
Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org
Patnaik, M. (2023, December 29). *What is consortium blockchain? A comprehensive guide.* AlmaBetter. https://www.almabetter.com/bytes/articles/consortium-blockchain
Peñaranda Rodríguez, D. (2019). *Blockchain as digital evidence.* Universidad Externado de Colombia. https://derinformatico.uexternado.edu.co/blockchain-como-evidencia-digital
Pérez, H. (2021, February 20). *The third-generation blockchains that could replace Ethereum.* DiarioBitcoin. https://www.diariobitcoin.com
Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (Do Not) Know, Where We Go from Here. *Business & Information Systems Engineering,* 59(6), 385-409.
Rodeck, D., & Curry, A. (2022). *Blockchain explained.* Investopedia.

Rodriguez, N. (2020, January 28). *Blockchain for Beginners: Getting Started Guide.* 101 Blockchains. https://101blockchains.com/es/blockchain-para-principiantes/
Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security Services Using Blockchains: A State of the Art Survey. *arXiv preprint arXiv:1810.08735.*
Schwab, K. (2016). *The Fourth Industrial Revolution.* El Tiempo.
Sumner, M. (2025, May 6). *Advantages of blockchain-based timestamps for content security.* ScoreDetect. https://www.scoredetect.com/blog/posts/advantages-of-blockchain-based-timestamps-for-content-security
Sun, Y., & Wu, Y. (2023). Research on the Application and Examination of Electronic Evidence Preserved on the Blockchain in Chinese Copyright Judicial Practice. *Frontiers in Psychology*, 14.
Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* O'Reilly Media.
Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Penguin.
Tique Álvarez, M. (2020, May 30). *The authenticity of evidence in times of COVID-19.* Legal Matters. https://www.asuntoslegales.com.co/consultorio/la-autenticidad-de-la-evidencia-en-tiempos-de-covid-19-3012054
Vargas Osorno, T. (2021). *The blockchain and its importance in evidentiary law.* [Undergraduate thesis, Universidad Externado de Colombia].
WIPO (World Intellectual Property Organization). (2021). *Blockchain and intellectual property: What's not to like?* WIPO Magazine. https://www.wipo.int/wipo_magazine/en/2021/01/article_0006.html
World Economic Forum. (2018). *Blockchain for land registries: Unleashing the potential.* https://www.weforum.org/agenda/2018/01/blockchain-for-land-registries-unleashing-the-potential/
World Economic Forum. (2020). *Blockchain for supply chains: A path to trust and transparency.* https://www.weforum.org/whitepapers/blockchain-for-supply-chains-a-path-to-trust-and-transparency/