Blockchain-Based Evidence in Courts: Standards, Reliability, and Admissibility Challenges

1. Michael Harris*: Department of Criminal Law and Criminology, Harvard University, Cambridge, USA
*Correspondence: e-mail: michael.harris@law.harvard.edu

Abstract

The rapid expansion of blockchain technology across commercial, administrative, and digital ecosystems has introduced a new category of evidence into judicial processes, compelling courts to evaluate records generated through decentralized, cryptographic systems. This narrative review examines the evidentiary implications of blockchain by analyzing its technical foundations, legal admissibility standards, and the practical and doctrinal challenges that arise when decentralized ledger records enter the courtroom. The review outlines how blockchain architecture, hashing, timestamping, and distributed consensus mechanisms influence traditional evidentiary concepts such as authenticity, reliability, verifiability, and chain of custody. It further evaluates how courts interpret blockchain records under doctrines governing scientific validity, hearsay exceptions, relevance, and digital signature legislation, highlighting the varied approaches taken in jurisdictions including the United States, European Union, China, Singapore, and the United Arab Emirates. Despite blockchain's potential to enhance evidentiary integrity, the analysis reveals significant obstacles, including risks of flawed or fraudulent data input, challenges in validating permissioned blockchain systems, cross-border inconsistencies, lack of standardized forensic protocols, expert dependency, and tensions between immutability and data protection rights. Interpretive difficulties also emerge when courts must assess meaning, context, or intent behind automated ledger entries or smart contract execution logs. By integrating technological, doctrinal, and policy perspectives, the review demonstrates that blockchain evidence offers both powerful advantages and substantial limitations. The article concludes that judicial systems must cultivate technological literacy, refine evidentiary standards, and develop regulatory frameworks that reconcile blockchain's capabilities with established principles of legal proof. Such evolution is essential for ensuring that blockchain-based evidence is incorporated into judicial reasoning in ways that uphold fairness, accuracy, and procedural integrity.

Keywords: Blockchain evidence; admissibility; digital signatures; smart contracts; chain of custody; evidentiary reliability; decentralized systems; forensic analysis; legal standards; immutability

Received: date: 10 May 2023
Revised: date: 11 June 2023
Accepted: date: 24 June 2023
Published: date: 01 July 2023

Citation: Harris, M. (2023). Blockchain-Based Evidence in Courts: Standards, Reliability, and Admissibility Challenges. *Legal Studies in Digital Age*, 2(3), 49-63.

1. Introduction

The rapid expansion of blockchain technology into commercial, governmental, and interpersonal transactions has introduced a new category of digital artefacts into courtrooms, compelling judges and litigators to confront evidentiary forms that differ fundamentally from traditional documents. Courts increasingly encounter blockchain-generated or blockchain-stored materials because actors across sectors rely on distributed ledgers to authenticate transactions, execute smart contractual relationships, verify digital identities, and record asset transfers in immutable formats. The earliest wave of judicial references to blockchain arose from commercial disputes and cryptocurrency crimes, yet the technological ecosystem has since broadened, making

blockchain evidence relevant not only to financial litigation but also to administrative law, intellectual property disputes, supply-chain verification, and decentralized identity systems. As digital relations intensify, litigants submit hash values, ledger transaction histories, timestamps, and smart contract outputs as supporting documentation, relying on their cryptographic properties to demonstrate authenticity. This transition obliges judicial systems to reinterpret evidentiary standards within a technological environment where verification processes depend not on human witnesses but on algorithmic consensus mechanisms, as illustrated in emerging discussions about decentralized identity infrastructures (Rodionov, 2024). Courts therefore occupy a pivotal frontier where the formal rigor of evidentiary law encounters the technical logic of distributed computing.

The motivation for a scientific narrative review arises from persistent uncertainties about how blockchain-based evidence fits within prevailing frameworks of admissibility, authenticity, and reliability. Even though blockchain ledgers are promoted as immutable and tamper-resistant, courts must still validate whether the submitted record truly corresponds to the ledger in question, whether the ledger itself is trustworthy, and whether the underlying data were accurate at the moment of entry. The legal presumption that blockchain automatically ensures reliability has been challenged by scholars who emphasize the risk of flawed or deliberately false input at the point of data entry, as the immutability of a ledger does not guarantee accuracy of the information written to it. The distinction between immutability and truth becomes especially critical in fields such as dispute resolution, where the interpretation of a smart contract requires contextual understanding of intent, consent, and performance, as highlighted in legal analyses of blockchain-enabled adjudication (Ortolani, 2019). Courts must therefore balance the technology's promise of cryptographic certainty against its practical vulnerabilities, including jurisdictional conflicts, interoperability challenges, and inconsistent forensic capacities across legal systems.

The growth of blockchain use in commercial transactions, public administration, and legal technology further intensifies these evidentiary dilemmas. Governmental and corporate sectors increasingly integrate blockchain into identity management, financial bookkeeping, and audit trails, creating digital footprints that later surface in litigation. Research on decentralized identity systems identifies the tension between technical capability and regulatory legitimacy, showing how cryptographic authentication mechanisms introduce new verification pathways for courts but also require judges to comprehend complex digital signatures and consensus processes (Rodionov, 2024). In accounting and auditing, blockchain-based records are promoted as tools for enhancing transparency, yet their admissibility in court still hinges on legal standards rather than technological novelty, a point underscored in studies of blockchain adoption within financial oversight frameworks (Al-saedi & Almaliki, 2023). Similarly, blockchain's integration into capital markets, including regulatory processes in jurisdictions that explore blockchain-enabled trading mechanisms, raises significant questions about the status of ledger entries as legal proof in disputes involving transactions or market manipulation, a trend observed in analyses of blockchain's role in emerging financial structures (Mahdi & Shafiei, 2022). As these domains expand, courts face mounting pressure to recognize ledger entries, smart contract triggers, and blockchain-stored metadata as formal judicial evidence.

Smart contracts constitute one of the most legally consequential aspects of blockchain evidence. These self-executing agreements, encoded with predefined conditions, generate computational outputs that may serve as proof of contractual performance or breach. Courts evaluating such evidence must determine whether the automated execution aligns with substantive legal requirements, particularly in jurisdictions where contract law imposes conditions that extend beyond algorithmic logic. Legal scholars examining the implications of smart contracts emphasize that blockchain-based automation does not eliminate the need for judicial interpretation of intent, fairness, and contractual capacity, especially within legal systems grounded in human-centered doctrines of autonomy and consent (Singh & Shilpa, 2021). The complexity is amplified in cross-border disputes, where parties may rely on smart contracts executed across decentralized networks spanning multiple jurisdictions. As illustrated in analyses of digital transformation in contract law, blockchain's capacity to alter the mechanics of agreement, performance, and evidence challenges courts to rethink foundational principles while ensuring continuity with established norms (Yazdani, 2021). This expanding body of commentary demonstrates why judicial systems must refine evidentiary standards to accommodate algorithmic contractual outputs without undermining doctrinal coherence.

Alongside commercial implications, the rise of blockchain in criminal investigations presents a parallel set of evidentiary challenges. Law enforcement increasingly traces cryptocurrency transactions, analyzes ledger histories, and identifies wallet interactions to establish links between suspects and criminal activity. As cybercrime becomes more sophisticated, courts must

evaluate evidence derived from ledger analytics, forensic tracing tools, and algorithmic detection systems. The difficulty of establishing personal jurisdiction in decentralized environments illustrates how traditional legal frameworks struggle to adapt to borderless digital infrastructures, prompting scholars to scrutinize the evidentiary foundations needed for prosecuting blockchain-enabled conduct (Watters, 2023). Reports on law enforcement needs related to cryptocurrency investigations further reveal the operational complexities of collecting, interpreting, and verifying ledger-based data in environments where pseudonymity and distributed storage challenge conventional investigative models. These developments illustrate why courts increasingly encounter blockchain evidence not only as a technical object but also as a legal puzzle demanding methodological adaptation.

The evidentiary challenges extend to civil and administrative arenas, where blockchain is used to document public service delivery, property records, and administrative compliance. Studies on digital transformation in public sector service delivery imply that blockchain has the potential to enhance transparency, yet they inadvertently highlight the evidentiary complexities that arise when administrative decisions rely on automated digital inputs (Golabchi et al., 2024). If disputes emerge regarding the validity of algorithmically generated records, courts must adjudicate not only the factual content of those records but also the legitimacy of their generation process. Similarly, legal analyses of blockchain's role in shaping future legal practice note that courts require new evaluative competencies to assess algorithmically derived evidence within the broader landscape of AI-driven legal innovation (Pasupuleti, 2024). These factors underscore a broader transition toward technologically integrated adjudication environments where evidentiary law must evolve to accommodate emerging forms of machine-generated proof.

Another critical dimension arises from blockchain's integration into automated decision-making environments, particularly within digital-first judicial systems. The experience of jurisdictions adopting blockchain for online adjudication demonstrates how courts can incorporate distributed ledger entries directly into their decision-making processes. Reports discussing the adoption of AI and blockchain in Chinese Internet Courts illustrate that algorithm-driven evidence, when combined with immutable ledger records, influences how judges evaluate authenticity and continuity of digital transactions (Alexandre, 2019). Such examples highlight how blockchain-based documents may serve not merely as evidence submitted by litigants but as procedural tools embedded within the judicial apparatus itself. As more courts experiment with digital transformation, blockchain evidence becomes intertwined with new forms of legal infrastructure, thereby expanding the evidentiary frontier into system-level procedural innovation.

Against this backdrop, verification difficulties constitute a core motivation for the present review. Courts must determine the correctness of the cryptographic hash, verify the timestamp accuracy, confirm the identity of the ledger participants, and ascertain whether the specific ledger version presented to the court genuinely reflects the authoritative state of the distributed network. These steps require technical expertise and may necessitate expert testimony, raising concerns about disparities between technologically advanced and resource-limited jurisdictions. Chain-of-custody considerations also pose significant challenges. Even though blockchain provides a permanent record once data are entered, the court must still evaluate who had control over the private keys, how the information was captured, and whether intermediaries affected its integrity before submission. Research on accountability structures in blockchain-based auditing demonstrates that organizational control over data input significantly influences evidentiary reliability, even when the ledger itself is technically tamper-resistant (Al-saedi & Almaliki, 2023).

The compatibility of blockchain evidence with traditional evidentiary doctrines further motivates systematic academic investigation. Some jurisdictions rely heavily on human testimony and document authentication requirements that presuppose centralized recordkeeping. Others incorporate flexible standards that may better accommodate distributed digital records. Legal scholarship indicates that blockchain-enabled dispute resolution mechanisms encourage courts to reconsider foundational assumptions about authorship, document origin, and the meaning of "original" evidence within a cryptographic environment (Ortolani, 2019). Similarly, commentary on transformations in contract law suggests that digital ledger entries complicate evidentiary standards governing intent and performance because they externalize human decision-making into algorithmic systems (Yazdani, 2021). The present review addresses these concerns by synthesizing cross-disciplinary insights to clarify how courts can integrate blockchain evidence into established jurisprudential frameworks without compromising procedural fairness or doctrinal stability.

The scope of this narrative review encompasses legal scholarship, judicial opinions, statutory materials, forensic methodologies, and technological analyses that directly address the evidentiary implications of blockchain. The descriptive analysis method allows for synthesizing diverse sources without imposing quantitative restrictions, enabling a nuanced account of how blockchain's technical properties intersect with legal standards. The literature selection focuses on peer-reviewed publications, policy documents, and authoritative reports that examine blockchain's role in evidence generation, authentication, and admissibility. Particular emphasis is given to works analyzing dispute resolution, criminal investigations, digital identity systems, and contractual frameworks, reflecting the domains where blockchain evidence most prominently appears. By reviewing academic commentary, practical case studies, and regulatory developments, this narrative approach identifies conceptual trends, recurring challenges, and emerging solutions within the evolving ecosystem of blockchain-based judicial evidence.

The review also incorporates comparative observations across jurisdictions, recognizing that blockchain adoption varies widely. Some countries experiment with blockchain-enabled courts and administrative systems, while others remain cautious due to regulatory uncertainty. Analyses of international practice reveal significant divergences in how legal systems interpret the reliability and authenticity of blockchain records, underscoring the need for structured comparative insights (Pasupuleti, 2024). These differences influence admissibility standards, burdens of proof, and requirements for expert testimony, making comparative synthesis essential for identifying global patterns and jurisdiction-specific gaps.

This article therefore aims to articulate a comprehensive conceptual and analytical foundation for understanding blockchain as an emerging evidentiary category within judicial systems. The review examines how blockchain-generated evidence challenges existing legal doctrines, identifies the technological and procedural factors that shape judicial evaluation of ledger-based records, and highlights the areas where evidentiary standards require adaptation. The objective of this study is to clarify the standards, reliability considerations, and admissibility challenges associated with blockchain-based evidence and to propose key questions that guide future judicial and scholarly analysis.

2. Technical Foundations and Evidentiary Characteristics of Blockchain Records

Blockchain technology introduces a distinctive evidentiary paradigm because the structure of a distributed ledger differs fundamentally from traditional data storage architectures. At its core, a blockchain consists of sequential data blocks, each containing a batch of transactions linked cryptographically to the previous block through a hash function. This structural design creates a chain that is mathematically resistant to alteration, because any modification to a prior block would change its hash value and disrupt the integrity of every subsequent block. Legal scholars examining blockchain's influence on dispute resolution emphasize that this architecture creates a technical presumption of integrity that courts must evaluate with precision when determining whether a ledger entry constitutes reliable evidence (Ortolani, 2019). The immutability often attributed to blockchain derives not from absolute impossibility of tampering, but from the prohibitive computational cost of rewriting a decentralized ledger distributed across numerous nodes. This reliance on collective verification rather than centralized authority reshapes the concept of evidentiary authenticity by shifting the focus from institutional control to algorithmic consensus.

Hashing serves as the primary mechanism for ensuring data integrity within blockchain systems. A hash function transforms input data into a fixed-length alphanumeric output such that any alteration to the input—even a single character—produces a radically different hash value. Courts assessing blockchain evidence may therefore rely on hash matches to confirm that a submitted document, image, or transaction corresponds exactly to its stored version on the ledger. Research in financial and auditing domains illustrates how hashing enables organizations to track transaction histories with unprecedented precision, allowing auditors to verify records without directly accessing the underlying data (Al-saedi & Almaliki, 2023). From an evidentiary perspective, hashing provides a mathematical basis for establishing that a digital item has remained unaltered since its initial recording. Legal analyses of blockchain in contract and administrative law similarly observe that hash-based verification introduces a unique technical standard of authenticity that differs from traditional document authentication procedures, which typically rely on witness testimony or institutional certification (Yazdani, 2021). This transition from human-centered validation to algorithmic assurance requires courts to develop new interpretive methods for determining when a hash signature is sufficient to satisfy evidentiary requirements.

The distributed nature of blockchain is crucial to its evidentiary value. Instead of storing data on a single centralized server, a blockchain replicates the entire ledger across a network of independent nodes. Each node maintains a copy of the ledger and participates in a consensus mechanism to validate new transactions. This decentralization increases resilience against data loss and tampering, making it significantly harder for malicious actors to alter records without detection. Scholars studying decentralized identity systems highlight how distributed consensus strengthens trust in digital identities and related records by eliminating the need for centralized verification authorities (Rodionov, 2024). For courts evaluating blockchain-based identity evidence—such as digital signatures, identity credentials, or authentication logs—this distributed validation process enhances credibility because no single entity can unilaterally manipulate the record. However, the same decentralization complicates evidentiary procedures, as courts must determine whether the ledger version presented reflects the authoritative state of the decentralized network. These concerns are especially significant in criminal investigations involving decentralized platforms, where law enforcement must reconcile technical verification with legal standards for establishing chain of custody.

Timestamping also plays an essential role in the evidentiary characteristics of blockchain. Every transaction recorded on a blockchain receives a timestamp, which is validated during the consensus process. This timestamp provides a chronological anchor that can prove when an event occurred, making blockchain particularly valuable in disputes involving priority of rights, contractual deadlines, or sequence of actions. The legal relevance of timestamps is evident in judicial analyses of blockchain-enabled automated agreements, where timestamped records may demonstrate whether a contractual condition was satisfied before triggering a smart contract execution (Singh & Shilpa, 2021). Timestamps validated across a distributed network carry greater evidentiary weight than those generated by centralized systems because they cannot be altered without compromising consensus across nodes. Discussions in technology-driven court systems, such as those employing blockchain to support online adjudication, indicate that timestamp accuracy contributes significantly to judicial confidence in digital records, especially in procedural contexts where the timing of submissions determines enforceability (Alexandre, 2019).

Smart contracts represent one of the most legally consequential technical components of blockchain systems. These self-executing scripts embed contractual terms directly into code and automatically perform designated functions when predefined conditions are met. Smart contracts generate transactional evidence in the form of logs, triggers, and state changes written to the ledger, creating a digital trail that courts may analyze when determining contractual compliance or breach. Legal scholars examining the interaction between automated execution and traditional contract doctrine emphasize that smart contract records raise complex evidentiary questions because their outputs must be interpreted within broader legal frameworks governing intent, fairness, and enforceability (Yazdani, 2021). Moreover, studies of blockchain's impact on dispute resolution highlight that smart contract evidence may integrate seamlessly into automated adjudication systems, yet courts must still evaluate whether the coded logic reflects the substantive legal obligations of the contracting parties (Ortolani, 2019). This duality—algorithmic execution paired with doctrinal interpretation—requires courts to understand not only the technical operations of smart contracts but also their evidentiary implications.

The differences between public, private, and permissioned blockchains significantly influence the reliability of blockchain-based evidence. Public blockchains, such as those used for cryptocurrency transactions, rely on open participation and decentralized consensus mechanisms, making them highly resistant to censorship or manipulation. Their transparency allows anyone to verify transactions independently, which enhances evidentiary reproducibility and auditability. However, their anonymity and global distribution create challenges for jurisdiction and attribution, issues extensively analyzed in research addressing personal jurisdiction in decentralized environments (Watters, 2023). In contrast, private blockchains restrict participation to specific entities and often rely on centralized or semi-centralized governance structures. While this may increase control and efficiency, it reduces decentralization and thereby narrows the evidentiary trust derived from distributed consensus. Permissioned blockchains combine elements of both systems by allowing only authorized participants to validate transactions. These hybrid systems are common in financial auditing, supply chain management, and governmental applications, where organizations require transparency among participants without exposing data to the public. Studies exploring blockchain in accounting and auditing emphasize that permissioned systems can enhance reliability and auditability when properly governed, yet their centralized control means courts must scrutinize the integrity of the participating actors (Al-saedi & Almaliki, 2023).

Blockchain data creation and validation follow specific technical steps that shape their evidentiary characteristics. When a user initiates a transaction—such as transferring a digital asset, updating a record, or executing a smart contract—the transaction

is broadcast to the network and placed into a pool of pending entries. Nodes participating in the consensus mechanism validate the transaction by verifying digital signatures and ensuring it adheres to protocol rules. Once validated, the transaction is included in a block, which is then appended to the chain through cryptographic linkage. This process generates a verifiable chain-of-events that forensic experts can analyze using specialized tools. Reports on law enforcement needs in cryptocurrency investigations illustrate that forensic specialists frequently reconstruct transaction flows by examining how data traversed the ledger at different timestamps, enabling courts to infer relationships between actors or events. These forensic methods rely on blockchain's inherent transparency and traceability, yet they also require expert interpretation due to the technical complexity of ledger analytics.

Digital identity structures are deeply intertwined with blockchain's evidentiary potential. Blockchain-based identity systems may store credentials, authentication data, and verification logs in distributed formats, allowing individuals or organizations to control their identity information without relying on centralized authorities. Scholars analyzing decentralized identity frameworks explain that these systems enhance security and reduce the risk of identity fraud by distributing validation responsibilities among numerous nodes rather than a single entity (Rodionov, 2024). For courts, such identity systems introduce new forms of digital signatures and authentication logs that can serve as evidence of an individual's participation in a transaction. However, they also complicate attribution because identities may be pseudonymous or linked to cryptographic keys rather than personal identifiers. Legal analyses of blockchain in practice underscore that linking an action to a specific individual requires not only validation of the digital signature but also contextual evidence demonstrating possession and use of the corresponding private key (Singh & Shilpa, 2021).

The auditability of blockchain records arises from the full visibility of the ledger and the deterministic nature of consensus rules. Every node retains a copy of the ledger, enabling independent verification of transaction histories. Scholars in public-sector digital transformation note that this auditability strengthens institutional accountability by providing an immutable record of administrative actions, an attribute with clear evidentiary implications when courts examine disputed governmental decisions (Golabchi et al., 2024). In private-sector environments, blockchain-based audit trails support regulatory compliance and financial oversight, providing detailed logs that courts may reference when evaluating disputes over accounting records (Al-saedi & Almaliki, 2023). Yet transparency can create privacy concerns, especially when sensitive personal or commercial information remains visible across nodes. Courts must therefore balance auditability with privacy obligations, particularly in cases involving cross-border data protection frameworks.

The reproducibility of blockchain evidence is a direct consequence of its decentralized architecture. Because multiple nodes store identical copies of the ledger, any party with access to the chain can independently reproduce the transaction history and verify its consistency. This stands in contrast to traditional electronic evidence, where reproduction often depends on a central administrator responsible for maintaining authenticity. Legal scholars discussing blockchain adoption in future legal practice argue that reproducibility enhances the robustness of digital evidence by eliminating reliance on a single custodian (Pasupuleti, 2024). However, reproducibility alone does not guarantee evidentiary sufficiency, as courts must still examine whether the reproduced ledger accurately reflects the authoritative network state at the time of data extraction.

While blockchain's technical properties collectively strengthen the evidentiary foundations of digital records, they do not eliminate the need for rigorous forensic evaluation. Experts interacting with blockchain data frequently use analytic software to trace transactions, identify data anomalies, or verify smart contract states. In criminal, administrative, and commercial investigations, forensic analysts must present their interpretations in ways courts can understand, bridging the gap between complex cryptographic processes and legal standards of proof. Studies on blockchain-enabled law enforcement emphasize that accurate forensic interpretation is essential because courts cannot rely solely on the technological assurances of immutability without contextual understanding of how the ledger operates and under what conditions data were generated.

Together, these technical foundations demonstrate why blockchain evidence holds a unique place within modern adjudication. Blockchain's architecture, consensus mechanisms, cryptographic assurances, and automated functionalities create records that differ from traditional digital documents in authenticity, traceability, and verifiability. These distinctions necessitate evolving evidentiary standards that enable courts to properly assess the reliability, integrity, and interpretive context of blockchain-based materials.

3. Legal Standards for Blockchain Evidence: Authenticity, Reliability, and Chain of Custody

The legal standards governing the admissibility of blockchain-based evidence emerge from a complex interplay between traditional evidentiary doctrines and the novel characteristics of distributed ledger technology. Courts historically evaluate digital records through a framework that prioritizes authenticity, reliability, and proper chain of custody, yet blockchain challenges these categories because its cryptographic operations differ significantly from the mechanisms used to authenticate conventional documents. The doctrine of authenticity requires that proponents of evidence demonstrate that a record is what they claim it to be. In the context of blockchain, authenticity depends not only on the provenance of the data but also on the technical accuracy of the ledger itself. Scholars examining blockchain's role in dispute resolution observe that courts must consider whether a specific block or ledger entry accurately reflects the authoritative state of the chain on a given date, especially when the distributed nature of the ledger complicates verification processes (Ortolani, 2019). Authenticity also requires confirming that a digital signature or hash value corresponds to the presented data, a concept that draws on research demonstrating how blockchain's cryptographic functions help preserve the integrity of financial and auditing records (Al-saedi & Almaliki, 2023). These emerging standards suggest that while blockchain offers strong technical assurances, courts must still evaluate human-controlled aspects of data entry and key management to satisfy authenticity doctrines.

The requirement of relevance and materiality remains unchanged in principle, but blockchain records present unique challenges for establishing the contextual significance of data. For example, a transaction recorded on a blockchain may demonstrate that a digital asset changed hands, yet relevance depends on whether that transfer bears on the facts at issue. In some disputes, courts must determine whether a smart contract execution or a timestamped ledger entry truly supports the legal claim being advanced. Commentary exploring the transformation of contract law in blockchain environments highlights how blockchain entries often require interpretation to determine whether they reflect genuine contractual intent or merely automated system responses (Yazdani, 2021). Likewise, analyses of blockchain-based identity frameworks demonstrate how courts may struggle to interpret the legal meaning of digital identity credentials or authentication logs in disputes involving identity fraud, administrative processes, or access rights (Rodionov, 2024). As blockchain applications expand across sectors, courts must learn to differentiate between the technical occurrence of an event recorded on a ledger and its legal materiality within the dispute.

Reliability—particularly under scientific validity standards such as Daubert in the United States or similar principles in other jurisdictions—constitutes one of the most significant challenges in admitting blockchain evidence. Under the Daubert standard, courts evaluate whether a technical method is testable, peer reviewed, associated with a known error rate, and accepted within the relevant scientific community. These criteria require judges to assess whether blockchain's consensus algorithms, cryptographic signatures, and validation methods meet the threshold for scientific reliability. Scholars studying the intersection of AI, blockchain, and legal practice note that while cryptographic hashing and consensus protocols are widely accepted in computer science, courts must still evaluate whether the implementation of these technologies in a specific case was reliable and whether the data were properly captured before recording (Pasupuleti, 2024). Moreover, forensic analyses in blockchain-related criminal investigations reveal that ledger analytics may involve probabilistic interpretations rather than absolute certainty, raising questions about whether such analyses satisfy scientific validity standards, particularly when reconstructing transaction histories or attributing actions to specific individuals. These challenges highlight the need for expert testimony capable of explaining blockchain's technical underpinnings in terms accessible to legal decision-makers.

Judicial evaluation of blockchain evidence routinely intersects with hearsay doctrine and the exceptions governing digital records. Traditional hearsay rules prohibit the admission of out-of-court statements offered for their truth unless they fall within recognized exceptions. Blockchain records complicate this analysis because they may not originate from human statements but from automated processes. In many jurisdictions, computer-generated records do not constitute hearsay if they are produced without human intervention, an argument that may apply to blockchain transactions when they are executed automatically through consensus mechanisms or smart contracts. Legal analyses of smart contract operations point out that automated blockchain activity challenges courts to determine whether the recorded entries reflect declarative statements or merely mechanical outputs (Singh & Shilpa, 2021). This distinction is significant because many jurisdictions allow machine-generated data to bypass hearsay restrictions when they result from routine, reliable processes. However, courts must still

evaluate whether the system producing the data was functioning correctly, a requirement that introduces questions about consensus failures, chain forks, or vulnerabilities in smart contract code.

Digital signature laws and electronic transactions legislation also shape the admissibility of blockchain evidence. Many jurisdictions have enacted statutes recognizing electronic signatures as legally valid so long as they demonstrate intent and maintain a reliable association between the signer and the record. Blockchain-based signatures, which rely on public–private key cryptography, often exceed the security assurances of traditional digital signatures. Comparative analyses of electronic transaction frameworks reveal that while public–private key authentication aligns well with statutory requirements for secure digital signatures, courts must still confirm that the private key was under the exclusive control of the purported signer (Singh & Shilpa, 2021). Blockchain's ability to embed digital signatures directly into ledger transactions creates opportunities for stronger evidentiary authentication, yet this advantage is contingent on accurate identification of key holders. Legal scholarship examining decentralized identity systems underscores that linkage between a cryptographic key and a specific individual may require corroborating evidence beyond the blockchain itself (Rodionov, 2024). These complexities highlight that while blockchain strengthens signature integrity, it does not eliminate evidentiary burdens associated with identity attribution.

Jurisdictional comparisons demonstrate varying levels of judicial comfort with blockchain evidence. In the United States, courts have begun considering blockchain entries in cases involving cryptocurrency transactions, intellectual property verification, and commercial disputes, applying existing evidentiary frameworks to determine admissibility. While U.S. courts have not yet established comprehensive standards for blockchain evidence, analyses of digital jurisdiction issues indicate that judges are increasingly attentive to the decentralized nature of the underlying networks, especially when evaluating evidence related to transnational activities or anonymous actors (Watters, 2023). In the European Union, the eIDAS Regulation provides a robust legal framework for electronic signatures and trust services, which may facilitate recognition of blockchain data when it aligns with these established standards. Some EU member states have explicitly recognized blockchain timestamps and signatures as legally valid forms of authentication, though courts continue to assess reliability on a case-by-case basis.

In China, specialized Internet Courts have integrated blockchain into their judicial infrastructure, using it to authenticate evidence related to online transactions, copyright claims, and digital communications. Reports discussing the role of AI and blockchain in these courts reveal that judges and court staff increasingly rely on automated verification systems that check hash values and ledger entries against trusted blockchain repositories (Alexandre, 2019). These innovations demonstrate a proactive approach to integrating blockchain into evidentiary procedure, potentially reducing the need for extensive expert testimony. Singapore has also demonstrated openness to blockchain evidence, supported by strong electronic transaction laws and a judiciary familiar with technological innovation. The UAE follows similar trends, incorporating blockchain into governmental and legal processes to enhance administrative transparency and facilitate digital litigation, though courts continue to rely on established evidentiary principles when reviewing blockchain entries.

Judicial decisions that touch on blockchain or similar digital records provide valuable insight into emerging evidentiary principles. In disputes involving cryptocurrency exchanges, courts have accepted blockchain transaction histories as circumstantial evidence when supported by expert testimony explaining how ledger analysis reveals wallet ownership patterns or transaction flows. Studies describing law enforcement's reliance on blockchain analytics to track illicit activity demonstrate that courts increasingly accept forensic blockchain evidence when accompanied by credible methodological explanation. In commercial cases involving smart contracts, courts have evaluated whether coded terms represent enforceable agreements and whether execution logs can prove breach or compliance. Commentary examining the implications of blockchain for contract law notes that these judicial analyses often hinge on whether the smart contract accurately reflects the parties' intentions, highlighting that technological evidence must be interpreted within substantive legal doctrines (Yazdani, 2021).

Chain of custody remains one of the most critical issues for blockchain admissibility. Traditional chain-of-custody rules require documenting each stage of evidence handling to demonstrate that no unauthorized alteration occurred. Blockchain's immutability appears at first glance to simplify this requirement, because once a transaction is written to the ledger, it cannot be altered without disrupting the chain. However, immutability applies only after data entry and does not address how the information was collected, who controlled the private keys, or whether intermediate devices were compromised. Research in auditing and financial blockchain applications highlights that organizations can shape the integrity of blockchain records through internal controls and data entry procedures, meaning courts must assess not only the ledger's technical immutability

but also the trustworthiness of those who entered the data (Al-saedi & Almaliki, 2023). Likewise, criminal investigations relying on blockchain analytics must ensure that forensic extraction methods are documented thoroughly to establish continuity between the data on the ledger and the evidence presented in court. Reports on law enforcement challenges underscore that even when blockchain itself is tamper-resistant, evidentiary continuity can be compromised during data retrieval or interpretation.

Despite these challenges, blockchain offers opportunities to strengthen evidentiary chain-of-custody frameworks. Courts evaluating timestamped blockchain entries may treat ledger inclusion as proof that a digital object existed at a particular moment, enhancing temporal continuity in chain-of-custody documentation. Scholars studying public-sector digital transformation argue that blockchain's transparency and auditability provide mechanisms for tracking administrative actions, potentially extending to evidence handling procedures (Golabchi et al., 2024). In private-sector contexts, blockchain-based audit trails have been proposed as tools for enhancing the traceability of evidence storage, creating immutable logs of access events and modifications. Legal analyses of emerging technologies suggest that blockchain-enabled evidentiary systems may provide more reliable continuity than traditional document management systems, but only when implemented within robust procedural frameworks that align technological capabilities with legal requirements (Pasupuleti, 2024).

Across jurisdictions, courts exhibit a cautious willingness to incorporate blockchain evidence when it is presented with proper foundation and supported by expert testimony. Judges increasingly recognize blockchain's potential to enhance evidentiary reliability, yet they also emphasize that technological trust must not replace legal scrutiny. The emerging practice demonstrates that blockchain evidence is most persuasive when it supplements, rather than supplants, traditional proof methods. As legal actors become more familiar with the technical and conceptual foundations of blockchain, evidentiary doctrine will likely evolve to reflect the unique strengths and limitations of distributed ledger technology while maintaining the essential safeguards that underpin procedural fairness.

4. Admissibility Challenges: Practical, Doctrinal, and Theoretical Barriers

One of the most persistent admissibility challenges arises from the difficulty of validating records stored on private or permissioned blockchains, particularly when the entity controlling the network has a vested interest in the outcome of litigation. Unlike public blockchains, where decentralized consensus mechanisms provide a distributed trust framework, permissioned systems allow a limited group of participants to write, validate, or modify entries. This creates structural vulnerabilities because courts cannot automatically assume that a ledger governed by a closed consortium maintains the same level of independence or resistance to manipulation as a public chain. Scholars examining blockchain-enabled auditing point out that organizational control over internal blockchains may allow actors to shape or curate data inputs in ways that undermine evidentiary neutrality (Al-saedi & Almaliki, 2023). This concern aligns with legal analyses of blockchain in dispute resolution, which emphasize that judicial reliance on ledger immutability must be tempered by scrutiny of the governance structures behind the chain (Ortolani, 2019). The difficulty is compounded when litigants present blockchain entries as inherently trustworthy without acknowledging that a permissioned network may reflect curated or selectively validated data rather than an immutable record maintained through open consensus. As a result, courts must examine the underlying governance model, participant roles, and access controls before determining whether a private blockchain can satisfy evidentiary standards of authenticity and reliability.

The problem of flawed or fraudulent data entry—often referred to as the "garbage in–garbage out" dilemma—further complicates judicial evaluations of blockchain evidence. Blockchain immutability prevents modification of data after entry, but it offers no inherent protection against inaccurate, manipulated, or intentionally falsified information submitted at the outset. This dynamic is frequently observed in financial and administrative applications where human operators or automated systems generate inputs that later acquire the appearance of irrefutable truth due to the blockchain's cryptographic permanence. Research on blockchain use in capital markets underscores the risk that incorrect or improperly vetted transaction data may become entrenched within immutable ledgers, potentially misleading courts that treat blockchain records as inherently trustworthy (Mahdi & Shafiei, 2022). Likewise, discussions of digital identity frameworks reveal that inaccurate identity credentials or improperly verified identity claims can be permanently embedded in decentralized identity systems (Rodionov, 2024). These examples illustrate that blockchain immutability may ironically strengthen the evidentiary status of fraudulent or

erroneous data unless courts maintain rigorous scrutiny of the circumstances surrounding data creation. The doctrinal implication is that immutability supports evidentiary integrity only when paired with robust safeguards at the point of input—something many blockchain systems currently lack.

Cross-border evidentiary conflicts and interoperability limitations present another major barrier to blockchain admissibility. Blockchain transactions frequently occur across jurisdictions, especially in digital commerce, decentralized finance, and international contracting. Courts must determine which legal system governs the evidentiary interpretation of a ledger entry, whether foreign privacy or cybersecurity laws restrict access to blockchain data, and whether the chain's technical standards align with domestic rules governing digital records. Studies examining blockchain's role in international legal practice highlight the complexity of determining jurisdiction when evidence originates from decentralized networks or involves pseudonymous actors dispersed across multiple countries (Watters, 2023). These concerns parallel discussions in legal scholarship on blockchain-mediated dispute resolution, which indicate that traditional territorial frameworks struggle to accommodate networks that operate independently of geographic boundaries (Ortolani, 2019). Interoperability challenges add a further layer of complexity, as courts may encounter difficulties interpreting data derived from chains using different consensus mechanisms, data formats, or governance models. When litigants present blockchain-based evidence from foreign or incompatible systems, courts must rely on experts capable of explaining how those systems function and whether their validation processes meet the evidentiary standards of the forum jurisdiction.

The absence of standardized forensic procedures for blockchain analysis exacerbates these challenges. Although forensic investigators increasingly employ blockchain analytics tools to trace transactions or verify ledger entries, methods vary widely and often depend on proprietary software. Reports on the evidentiary needs of law enforcement emphasize that blockchain investigations require specialized analytic competencies, yet there is little uniformity in how such analyses are conducted or presented. This lack of standardization raises questions about reliability, reproducibility, and error rates—criteria central to scientific validity assessments under the Daubert or Frye standards. Legal practitioners analyzing the future of AI and blockchain integration observe that forensic blockchain interpretation often relies on highly technical inferences rather than direct observation, making courts dependent on expert testimony to explain analytic methods (Pasupuleti, 2024). Without standardized protocols, courts may encounter conflicting expert opinions regarding the accuracy of transaction tracing, the identification of wallet owners, or the interpretation of smart contract execution logs. This inconsistency risks undermining judicial confidence in blockchain evidence and invites challenges based on methodological uncertainty.

Expert dependency represents a further doctrinal and practical barrier. Because blockchain technology remains unfamiliar to many judges and litigators, courts often rely on expert witnesses to interpret technical details, explain consensus mechanisms, or reconstruct ledger events. However, access to qualified experts is uneven across jurisdictions, and litigants with greater financial resources may be better positioned to present persuasive blockchain analyses. Scholars examining digital transformation in public-sector processes note that while blockchain's technical capabilities can enhance transparency, they also create asymmetries between technologically sophisticated actors and those lacking similar resources (Golabchi et al., 2024). Expert dependency thereby risks entrenching procedural inequalities, particularly in cases involving small businesses, individuals, or public agencies without dedicated technical support. Legal commentators studying blockchain-related disputes emphasize that courts must develop internal capacity to evaluate foundational blockchain concepts so that judges can critically assess expert testimony rather than deferring entirely to technical interpretations (Yazdani, 2021). Theoretical analyses further suggest that without broader judicial literacy in decentralized systems, evidentiary doctrine may drift toward overreliance on expert authority, thereby undermining the epistemic balance required in adversarial proceedings.

A more complex theoretical tension arises from the conflict between blockchain immutability and legal rights associated with data protection and privacy, including the right to erasure recognized in many jurisdictions. Immutability is a defining characteristic of blockchain: once data are recorded, they cannot be deleted without network consensus, and in many systems, deletion is technically impossible. This feature clashes directly with data protection regulations that grant individuals the right to request deletion or correction of personal information. Comparative legal analyses highlight that while blockchain enhances auditability and reduces the risk of unauthorized alteration, it also embeds personal data in ways that complicate compliance with regulatory requirements (Pasupuleti, 2024). Decentralized identity frameworks underscore similar concerns, as identities stored on blockchains may remain traceable indefinitely even after the underlying relationship or consent has lapsed

(Rodionov, 2024). Courts reviewing blockchain-based evidence must therefore balance the probative value of immutable records against the potential violation of statutory privacy rights. In some cases, blockchain data may be inadmissible if its collection or retention violates domestic or international privacy law, regardless of its evidentiary usefulness.

Interpretive challenges also play a significant role in the admissibility of blockchain evidence, particularly when courts must determine the meaning, context, or intent behind ledger entries. Blockchain records capture transactions, timestamps, and coded events, but they do not inherently explain the subjective motivations or contextual circumstances of the parties involved. For example, a smart contract may execute automatically based on predefined triggers, but judicial interpretation is still required to determine whether the coded execution reflects contractual intent or whether external factors should influence enforcement. Legal commentators examining transformations in contract doctrine argue that smart contract outputs cannot be understood purely as mechanical facts; they must be contextualized within broader legal principles governing intent, fairness, and the relationship between the parties (Yazdani, 2021). Similarly, scholars studying blockchain-enabled digital courts note that while automated evidence verification may enhance procedural efficiency, it does not eliminate the need for human interpretation of the narrative and factual context surrounding blockchain entries (Alexandre, 2019). These interpretive gaps challenge courts to reconcile algorithmic processes with legal reasoning grounded in human agency and normative judgment.

The divergence in judicial comfort with blockchain evidence across jurisdictions further illustrates the theoretical instability of current admissibility standards. In technologically advanced legal systems, such as those in China's Internet Courts, blockchain evidence is routinely integrated into litigation processes, with judges relying on automated verification tools to authenticate digital records (Alexandre, 2019). By contrast, courts in jurisdictions with limited technological infrastructure may remain skeptical of blockchain records due to unfamiliarity or concerns about reliability. Studies analyzing global trends in digital legal transformation emphasize that judicial acceptance often correlates with broader institutional investment in technological capacity and digital governance frameworks (Pasupuleti, 2024). Cross-border disputes amplify these disparities, as courts may differ in their willingness to recognize foreign blockchain records or rely on forensic methods developed in other jurisdictions. This unevenness creates doctrinal fragmentation, making it difficult to establish coherent global standards for blockchain admissibility.

Another barrier emerges from the difficulty of attributing blockchain activity to specific individuals or entities. Because blockchain systems often operate pseudonymously, linking a transaction to a legally identifiable actor requires additional evidence beyond the ledger itself. Reports on law enforcement investigations into illicit cryptocurrency use reveal that attribution frequently depends on correlating blockchain analytics with off-chain information such as IP addresses, exchange records, or device metadata. Without such corroboration, courts may find blockchain evidence insufficient to satisfy burdens of proof related to identity or intent. Legal scholars examining smart contract disputes similarly caution that blockchain records may document execution events but offer limited insight into whether the parties meaningfully consented to the coded terms or understood the implications of automated enforcement (Singh & Shilpa, 2021). These attribution challenges underscore the theoretical limits of relying exclusively on blockchain evidence in contexts where legal responsibility hinges on demonstrating agency and knowledge.

Finally, the absence of uniform international standards governing blockchain evidence contributes to doctrinal instability. While some jurisdictions adopt progressive approaches integrating blockchain into statutory frameworks for electronic signatures and evidentiary authentication, others continue to treat blockchain as a novel technology requiring heightened scrutiny. Comparative analyses of electronic transaction laws indicate that blockchain aligns well with existing frameworks in many regions, yet the degree of legal recognition varies widely (Singh & Shilpa, 2021). This variability complicates cross-border litigation and arbitration, where parties may disagree about the admissibility or weight of blockchain-based records. Scholars exploring blockchain's potential to transform dispute resolution systems note that these inconsistencies hinder the development of interoperable legal norms and undermine blockchain's promise as a trustworthy evidentiary infrastructure (Ortolani, 2019).

Together, these practical, doctrinal, and theoretical challenges illustrate why courts continue to struggle with the admissibility of blockchain evidence. While blockchain offers unprecedented opportunities for ensuring authenticity, transparency, and auditability, these strengths do not resolve the deeper legal and interpretive issues associated with

decentralized systems. Judicial adaptation will require not only technical literacy but also doctrinal evolution that reconciles traditional evidentiary principles with autonomous digital technologies.

5. Conclusion

Blockchain technology has introduced a transformative evidentiary paradigm that challenges foundational assumptions about how courts authenticate, interpret, and evaluate digital records. As judicial systems increasingly encounter blockchain-generated materials—ranging from smart contract execution logs to distributed identity credentials and cryptocurrency transaction histories—traditional evidentiary doctrines are strained in ways that demand conceptual and procedural adaptation. The conclusion of this narrative review synthesizes the technological, doctrinal, and practical insights presented in earlier sections to clarify the emerging contours of blockchain admissibility and to articulate the broader implications for legal practice and judicial reasoning.

At its core, blockchain redefines the nature of recordkeeping by creating a decentralized, tamper-resistant ledger that does not rely on centralized authorities. This technical architecture provides unprecedented opportunities for enhancing evidentiary integrity, as the cryptographic hashing and distributed consensus mechanisms that underpin blockchain systems offer inherent safeguards against post hoc manipulation. These properties strengthen judicial confidence in the stability and traceability of digital records, particularly in contexts involving financial transactions, automated agreements, and identity verification. Yet immutability alone does not guarantee evidentiary sufficiency. Courts must still examine the origins of data, the trustworthiness of the systems that generated it, and the broader context in which blockchain entries were created. This distinction between post-entry integrity and pre-entry reliability continues to shape the evidentiary landscape.

The review reveals that authenticity—historically grounded in human testimony and institutional recordkeeping—must be reconceptualized when applied to blockchain. Judges must become comfortable with evaluating cryptographic signatures, ledger replication, and consensus algorithms as substitutes for more familiar forms of verification. Because blockchain systems operate automatically and often without human intervention, the task of establishing authenticity shifts from verifying the identity and intention of a document's creator to verifying the correct functioning of a technological system. This evolution does not diminish the importance of authenticity but reorients its evidentiary criteria toward technical validation and expert interpretation.

Reliability remains a central pillar of admissibility, yet blockchain complicates traditional reliability assessments by introducing complex interactions between human decision-making, software design, and cryptographic processes. Courts must discern whether blockchain data accurately reflects real-world events or merely captures the outputs of flawed or manipulated inputs. In automated environments—such as smart contract execution—reliability depends not only on the ledger's integrity but also on the correctness of the code governing contractual conditions. Similarly, forensic analyses of blockchain activity require careful evaluation of analytic tools and methodologies, underscoring the need for courts to develop stronger standards governing expert testimony and technical scrutiny.

Chain of custody, long viewed as a procedural safeguard ensuring the continuity and integrity of physical and digital evidence, acquires new dimensions in blockchain contexts. The permanence and transparency of blockchain entries offer inherent advantages, yet chain of custody cannot be presumed simply because the ledger is immutable. Courts must consider who controlled the private keys, how the data were captured, and whether intermediate handling compromised the evidentiary value of the blockchain record. As blockchain becomes more integrated into public administration, financial auditing, and automated decision-making systems, chain-of-custody analysis will require new frameworks that account for decentralized data environments.

Across jurisdictions, the review highlights significant differences in judicial comfort with blockchain evidence. Some legal systems have embraced blockchain as a formal evidentiary tool, integrating it into electronic litigation platforms and developing procedural guidelines to support its use. Others remain cautious, treating blockchain as a novel technology that requires heightened scrutiny and expert support. These disparities complicate cross-border litigation, where evidentiary standards must accommodate varying levels of technological familiarity and differing statutory frameworks governing electronic records. Interoperability issues further widen these gaps, underscoring the need for harmonized international standards that can guide courts in assessing blockchain-based evidence.

The review also emphasizes the importance of interpretive judgment in integrating blockchain evidence into legal reasoning. While blockchain can verify that a given event occurred, it cannot convey the meaning, intention, or context underlying that event. Smart contracts illustrate this tension vividly: they execute automatically upon meeting coded conditions, yet courts must still interpret the contractual significance of their outputs. Similarly, blockchain entries documenting transactions or identity verifications must be examined in light of human motivations, regulatory conditions, and broader factual circumstances. Legal interpretation, therefore, remains indispensable even as blockchain automates aspects of record generation and verification.

Despite the significant challenges outlined throughout the review—ranging from flawed data entry to expert dependency, privacy conflicts, and doctrinal fragmentation—blockchain holds substantial promise as an evidentiary resource. Its transparency, auditability, and resistance to post-entry alteration can reinforce judicial objectives of accuracy, fairness, and procedural integrity. Realizing this potential, however, requires coordinated efforts across legal, technological, and regulatory domains. Courts must cultivate greater technological literacy to evaluate blockchain evidence confidently. Legislatures should consider updating electronic transactions laws, privacy frameworks, and evidentiary statutes to clarify how blockchain records fit within modern jurisprudence. Legal practitioners must develop strategies for presenting blockchain evidence in ways that align with doctrinal expectations while supporting judges through clear and comprehensible explanations.

Ultimately, blockchain invites a broader reflection on the nature of legal proof in the digital age. It challenges courts to rethink how evidence is generated, stored, authenticated, and interpreted, while reminding legal actors that technological certainty does not replace legal reasoning. The future of blockchain admissibility will depend not merely on technological advancements but on the capacity of legal systems to integrate those advancements thoughtfully, balancing innovation with enduring principles of fairness, due process, and evidentiary rigor.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Al-saedi, M. O., & Almaliki, O. J. (2023). The impact of applying blockchain technology in accounting and auditing. *World Bulletin of Management and Law*, *22*, 136-142.

Alexandre, A. (2019). Chinese Internet Court Employs AI and Blockchain to Render Judgement.

Golabchi, H., Kiaee, M., & Kameli, M. J. (2024). Designing a Superior Service Delivery Model in Education to Enhance Public Satisfaction [Research Article]. *Iranian Journal of Educational Sociology*, *7*(1), 189-197. https://doi.org/10.61838/kman.ijes.7.1.18

Mahdi, M., & Shafiei, G. (2022). New Capital Market in the Light of Sixth Development Plan Law (Functionality of blockchain technology in the capital market). *Journal of Securities Exchange*, *14*(56), 197-224. https://www.sid.ir/paper/955559/fa

Ortolani, P. (2019). The impact of blockchain technologies and smart contracts on dispute resolution: Arbitration and court litigation at the crossroads. *Uniform Law Review*, *24*(2), 430-448. https://doi.org/10.1093/ulr/unz017

Pasupuleti, M. K. (2024). AI and Blockchain in Law: Shaping the Future of Legal Practice. 307-325. https://doi.org/10.62311/nesx/46649

Rodionov, A. (2024). The Potential of Blockchain Technology for Creating Decentralized Identity Systems: Technical Capabilities and Legal Regulation. *Irshad J. Law and Policy*, *2*(4), 19-30. https://doi.org/10.59022/ijlp.170

Singh, J., & Shilpa. (2021). Smart contracts and blockchain: legal issues and implications for Indian contract law. *International Review of Law, Computers & Technology*, *36*, 313-314. https://doi.org/https://doi.org/10.1080/13600869.2021.1999312

Watters, C. (2023). When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment. *Laws*, *12*(2), 33. https://doi.org/10.3390/laws12020033
Yazdani, F. (2021). Blockchain and Transformations in Contract Law. *Journal of Modern Law*, *11*(32), 67-80.