frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 12 April 2024
DOI 10.3389/fbloc.2024.1306058

OPEN ACCESS

EDITED BY
Jannice Käll,
Lund University, Sweden

REVIEWED BY
Aaron M. Lane,
RMIT University, Australia
Gianluigi M. Riva,
Bocconi University, Italy
Katrin Becker,
University of Luxembourg, Luxembourg
Sudeep Jadey,
National Institute of Engineering, Mysore, India

*CORRESPONDENCE
Ying Cheng Wu,
wyc9@uw.edu

RECEIVED 03 October 2023
ACCEPTED 03 April 2024
PUBLISHED 12 April 2024

CITATION
Wang X, Wu YC and Ma Z (2024), Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes.
Front. Blockchain 7:1306058.
doi: 10.3389/fbloc.2024.1306058

Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in U.S. judicial processes

Xukang Wang[1], Ying Cheng Wu[2]* and Zhe Ma[3]

[1]Sage IT Consulting Group, Shanghai, China, [2]School of Law, University of Washington, Seattle, United States, [3]Ming Hsieh Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA, United States

This paper explores the evidentiary significance of blockchain records and the procedural implications of integrating this technology into the U.S. judicial system, as several states have undertaken legislative measures to facilitate the admissibility of blockchain evidence. We employ a comprehensive methodological approach, including legislative analysis, comparative case law analysis, technical examination of blockchain mechanics, and stakeholder engagement. Our study suggests that blockchain evidence may be categorized as hearsay exceptions or non-hearsay, depending on the specific characteristics of the records. The paper proposes a specialized consensus mechanism for standardizing blockchain evidence authentication and outlines strategies to enhance the technology's trustworthiness. It also highlights the importance of expert testimony in clarifying blockchain's technical aspects for legal contexts. This study contributes to understanding blockchain's integration into judicial systems, emphasizing the need for a comprehensive approach to its admissibility and reliability as evidence. It bridges the gap between technology and law, offering a blueprint for standardizing legal approaches to blockchain and urging ethical and transparent technology use.

KEYWORDS

blockchain, blockchain evidence, U.S. law, technology and law, judicial procedure

1 Introduction

Emerging technology governance pivots on striking a balance between fostering innovative development and mitigating security risks. Post the advent of the Internet, blockchain has emerged as one of the most promising technologies in the information technology era. While blockchain technology has indeed provided societal benefits, such as enhancing transparency in supply chains and enabling secure and immutable records for financial transactions, its applications have also raised concerns. For instance, the use of blockchain in cryptocurrencies has been linked to challenges such as energy consumption and facilitating illicit activities due to its anonymity features (Nakamoto, 2008). Furthermore, while blockchain can democratize data access and integrity, it has also been critiqued for potentially enabling a new form of digital divide and for the environmental impact of mining processes (Hileman and Rauchs, 2017). The 'Collingridge Dilemma' underscores the complexity of regulating emerging technologies like blockchain. It highlights a critical timing issue: intervene too early, and we risk

stifling innovation; act too late, and we face potentially irreversible societal consequences (Collingridge, 1980).

This paper focuses specifically on the use of blockchain technology as evidence within the United States legal system, primarily addressing the admissibility and procedural implications of blockchain evidence in federal criminal trials, while also acknowledging the potential relevance to civil cases. The U.S. legal system, based on common law principles, differs significantly from civil law systems found in the European Union and China, which rely heavily on codified procedural laws for admitting evidence in trials (Merryman and Pérez-Perdomo, 2019).

1.1 Overview of the U.S. legal system and evidence procedures

The United States legal system is a common law system, where legal principles are derived from judicial decisions and precedents, in addition to statutory laws (Burnham, 2016). In the context of federal criminal trials, the Federal Rules of Evidence (FRE) play a crucial role in determining the admissibility of evidence (USC, 2022). In criminal proceedings, the prosecution bears the burden of proving the defendant's guilt beyond a reasonable doubt, a high standard designed to minimize the risk of wrongful convictions and protect the defendant's presumption of innocence (Supreme Justia, 1970).

The admissibility of evidence in federal criminal trials is determined by several factors, including relevance (FRE 401), authenticity (FRE 901), and the balance between probative value and unfair prejudice (FRE 403) (LII, 2022). Electronic evidence, such as digital records and data, is subject to the same admissibility standards as traditional physical evidence (United States District Court District of Maryland, 2007).

1.2 Comparison with civil law systems

In contrast to the U.S. common law system, civil law systems, such as those found in the European Union and China, place a greater emphasis on codified procedural laws for admitting evidence in trials (Zweigert and Kötz, 1998). In civil law jurisdictions, the admissibility of evidence is often determined by strict adherence to procedural rules and regulations, with judges playing a more active role in fact-finding and evidence gathering (Glendon et al., 2016).

The differences between common law and civil law systems have implications for the admissibility and treatment of blockchain evidence. While the U.S. legal system may have more flexibility in adapting to new forms of digital evidence through judicial interpretation and precedent, civil law systems may require more explicit statutory recognition of blockchain evidence to ensure its admissibility (Zou, 2019).

1.3 Blockchain technology: an overview

Blockchain is a decentralized, distributed ledger technology that records transactions across a network of computers (Narayanan et al., 2016). Each block in the chain contains a cryptographic hash of the previous block, a timestamp, and transaction data, forming an immutable and tamper-evident record (Yaga et al., 2018) Currently, there's a broad recognition of blockchain technology's evidentiary value, largely attributed to its technical reliability. Several jurisdictions have come to accept blockchain records in litigation, acknowledging the enhanced likelihood of courts admitting such evidence under conditions similar to other forms of electronic data. Indeed, the immutability and decentralized verification mechanisms inherent in blockchain design have led some judges to display a favorable disposition toward admitting blockchain evidence (Polydor, 2020).

However, the trustworthiness of blockchain technology is not universally accepted, and some scholarship has outlined many criticisms around the reliability of the architecture of this technology, both on the technical aspects and the legal ones (Riva, 2020). For instance, the reliability of timestamp data in blockchain systems may depend on the specific consensus mechanism used and the potential for collusion or influence by a majority of nodes (Natoli et al., 2019).

It is important to recognize that blockchain is not a monolithic technology, and its characteristics and applications can vary significantly across different implementations (Buterin, 2015). Public blockchains, such as the Bitcoin blockchain, operate on a permissionless basis and rely on a decentralized network of nodes to validate transactions (Antonopoulos, 2017). In contrast, private or permissioned blockchains, also known as "sidechains," are developed and controlled by centralized entities and may have different levels of decentralization and trust assumptions (Hyperledger, 2023).

1.4 Fundamental elements of blockchain and their legal implications

Blockchain technology presents a dichotomic nature in terms of its legal effects and evidentiary value. On one hand, it can provide a high degree of certainty regarding the form of a legal action, such as a transaction, due to its immutable and tamper-evident record-keeping (Wang and Zha, 2021). On the other hand, the content of the transaction itself may not be inherently trustworthy, as blockchain cannot guarantee the accuracy or legitimacy of the information entered into the system (Wüst and Gervais, 2018).

The role of metadata in blockchain evidence is another crucial aspect to consider. Metadata, such as timestamps and transaction IDs, can provide valuable contextual information about the records stored on the blockchain (Benet, 2014). However, the legal implications of metadata may vary depending on the specific use case and the type of evidence being considered (Savelyev, 2018).

When addressing the scope of blockchain evidence, it is important to clarify whether the focus is solely on blockchain transactions or if it extends to other types of content that can be stored on a blockchain-based ledger, such as non-fungible tokens (NFTs) (Lee, 2021). The legal considerations surrounding NFTs, including their creation, ownership, and transfer, may differ from those of traditional blockchain transactions (Guadamuz-Gonzalez, 2021).

1.5 Standards of proof and evaluation criteria in U.S. criminal trials

In U.S. criminal trials, the prosecution must prove the defendant's guilt beyond a reasonable doubt, which is a high

standard of proof designed to minimize the risk of wrongful convictions (Supreme Justia, 1970). The concept of "beyond a reasonable doubt" is not precisely defined but generally requires that the evidence presented by the prosecution is so convincing that there is no reasonable doubt about the defendant's guilt (Supreme Justia, 1994).

The admissibility and evaluation of evidence in criminal trials are governed by the Federal Rules of Evidence, which establish standards for relevance, authenticity, and the balancing of probative value against unfair prejudice. The assessment of evidence also involves considerations of logical probability, the defendant's ability to present counterproof, and the preservation of the right to a fair trial (Tuzet, 2020).

The evaluation criteria for evidence in criminal trials may include factors such as the reliability of the evidence, the credibility of witnesses, and the strength of the logical inferences that can be drawn from the evidence (Damaska, 2019). The minimum threshold for consideration of evidence is generally determined by its relevance to the case, while the threshold for conviction is established by the "beyond a reasonable doubt" standard (Mnookin, 2013).

1.6 Blockchain evidence in the context of U.S. criminal trials

The use of blockchain evidence in U.S. criminal trials presents both opportunities and challenges. On one hand, the inherent immutability and transparency of blockchain records may enhance the reliability and integrity of digital evidence (Kumar and Tripathi, 2019). On the other hand, the technical complexity of blockchain systems and the potential for misinterpretation or misuse of blockchain data may raise concerns about the fairness and accuracy of trials involving such evidence (Kshetri and Voas, 2018).

When considering blockchain evidence in criminal trials, it is important to treat blockchain as a means of storing and transmitting data rather than as a legal phenomenon in itself (Nascimento et al., 2018). The evidentiary value and legal implications of blockchain records may vary depending on factors such as the specific blockchain architecture, the content of the transactions, the context of the case, and the methods used to collect and present the evidence (Xu, 2016).

To ensure the fair and accurate use of blockchain evidence in criminal trials, courts and legal practitioners must develop a comprehensive understanding of the technology and its potential limitations (Wright and De Filippi, 2015). This may involve the use of expert witnesses to explain the technical aspects of blockchain systems and to provide guidance on the interpretation and evaluation of blockchain evidence (Savelyev, 2017).

Furthermore, the development of clear legal standards and guidelines for the admissibility and evaluation of blockchain evidence in criminal trials is essential to promote consistency and fairness across cases (Regner et al., 2018). Such standards should take into account the unique characteristics of blockchain technology while also preserving the fundamental principles of due process and the right to a fair trial (Wirth and Kolain, 2018).

2 Methodology

This paper employs a comprehensive methodological approach, drawing from a diverse set of resources and strategies to elucidate the complex interplay between blockchain technology and the legal framework of evidence.

2.1 Legislative analysis

The study begins with a review of current legislative amendments, particularly the 2017 revision of the Federal Rules of Evidence (FRE) which introduced electronic data self-certification. This analysis sets the groundwork by delineating the legal context for the use of blockchain as evidence.

The paper also scrutinizes state-level legislations, such as those passed in California, Arizona, Delaware, Illinois, Vermont, and Ohio, to identify patterns, innovations, and challenges in integrating blockchain within legal proceedings at a regional level.

2.2 Comparative analysis

The paper undertakes a comparative examination of case law, most notably United States v. Lizarraga-Tirado (UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, 2015) and United States v. Costanzo (UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, 2020), to identify key issues and precedents related to the admissibility and authentication of digital evidence in criminal trials.

2.3 Technical examination

Recognizing that blockchain's evidentiary significance lies in its technological uniqueness, the paper delves deep into the mechanics of blockchain. By exploring how transactions are initiated, processed, and added to the chain, the research contextualizes its findings within the realm of technical feasibility and integrity.

The paper underscores the critical role of domain experts in elucidating blockchain technology's operations and ensuring its accurate representation in legal proceedings. Specifically, there is a paramount need for legal scholars who are proficient in blockchain technology. Such expertise is crucial for interpreting blockchain's implications within the legal framework, guiding the development of legislation, and informing judicial decisions. By emphasizing the importance of legal scholars with blockchain proficiency, we acknowledge the interdisciplinary approach required to fully integrate this technology into the judicial system.

2.4 Stakeholder engagement

Engaging with legal practitioners, technologists, and academics, we gather insights on the practical implications of blockchain in judicial processes. This engagement aims to bridge theoretical research with practical applicability.

3 Evidence effect analysis of blockchain evidence: does blockchain evidence fall into the category of hearsay?

3.1 Tolerance and acceptance of the traditional evidence theory system on blockchain evidence

Traditional evidence law has historically focused on non-algorithmic evidence, creating a framework to assess its probative value and admissibility. However, through a modern perspective, it becomes evident that these traditional rules often fall short when applied to algorithmic evidence, particularly in matters of authenticity. The reliability of algorithmic evidence is fundamentally dependent on the credibility of its source, requiring assessments to pivot towards technological and scientific criteria, rather than relying on human perception, memory, or the tangible qualities of items. This shift necessitates a thorough evaluation of the technology's foundational integrity, the accuracy of its inputs, and the consistency of its operational mechanisms.

Taking blockchain-stored electronic data as an instance, the method for validating its authenticity has evolved from conventional notarization to a process known as 'technical self-authentication.' Technical self-authentication refers to the process by which data integrity and authenticity are verified through the technology itself, rather than external verification methods. In the context of blockchain, this is achieved through cryptographic signatures and consensus mechanisms that ensure each piece of data or transaction recorded on the blockchain is immutable and traceable to its origin without requiring traditional forms of validation. This method emphasizes the shift towards reliance on the intrinsic security features of the technology, marking a significant departure from traditional evidentiary standards. This evolution necessitates a recalibration in how we evaluate and cross-examine such electronic data. Factors such as the data generation mechanism, storage process, and the overall credibility of blockchain technology become pivotal when courts assess the authenticity of on-chain information.

Blockchain evidence and traditional electronic digital data share similarities in their digital format, authentication methods, and integrity assurance, affecting their admissibility in court. Both require verification to ensure authenticity and have not been altered, leveraging mechanisms like cryptographic signatures for blockchain and digital signatures for traditional data. The integrity of both data types is paramount, with blockchain offering an immutable record through decentralized ledger technology, enhancing credibility. In legal contexts, demonstrating the reliability and relevance of both blockchain evidence and traditional electronic data is crucial for their acceptance. An example includes verifying digital contracts, where courts assess cryptographic signatures and timestamps for blockchain-based contracts, akin to digital signatures and metadata for traditional electronic contracts, emphasizing the need for transparency and data integrity in both cases.

While blockchain evidence exhibits similarities to other forms of electronic data, given its digital nature, its introduction to judicial proceedings was initially treated as a unique subset of electronic evidence, subject to traditional evaluation methods (Wu and Zheng, 2020). Historically, the introduction of blockchain as a form of evidence in courtrooms marked a significant shift, particularly noticeable in the United States around the mid-2010s. States like Vermont and Arizona were pioneers in this regard. Vermont's legislature acknowledged blockchain data in legal contexts as early as 2016, aiming to facilitate the use of blockchain technology for maintaining records and electronic transactions. Arizona followed suit by amending its Electronic Transactions Act to include blockchain signatures and records, further legitimizing blockchain evidence in legal proceedings. Around the same time, China also saw advancements in legal frameworks concerning blockchain evidence. In 2018, the Internet Court in Hangzhou recognized blockchain as a method for securing evidence in legal disputes, marking a significant acknowledgment of blockchain's utility in judicial processes.

However, blockchain's intrinsic technology, creation process, and foundational principles challenge the efficacy of these conventional review rules. In digital transactions, users' activities are typically documented and stored in centralized databases. The data generated during these transactions mirrors the transactional facts (Pappas, 2022). If disputes emerge, this centralized data, once lawfully collected, serves as electronic evidence for legal proceedings, providing the foundation for judicial decisions. However, a salient vulnerability of this centralized storage model is the susceptibility to data manipulation, which can erode the probative value of the evidence. Blockchain technology aims to mitigate vulnerabilities in electronic evidence management, such as tampering, by leveraging its decentralized and immutable ledger. This technological shift inherently strengthens the integrity of evidence, potentially enhancing its credibility. However, the extent of this enhancement depends on the blockchain's design, its operational security, and the legal framework's ability to assess such evidence accurately. Thus, while blockchain presents a promising solution to improve electronic evidence's reliability, its effectiveness is contingent upon judicious implementation and evaluation within judicial processes (Kosba et al., 2016).

Hearsay evidence refers to statements made outside of court proceedings and is typically tendered as evidence to validate the veracity of the facts proclaimed. Conventional wisdom posits that hearsay evidence, due to its perceived unreliability, should be excluded. However, certain statements with strong evidentiary value have increasingly been accepted as exceptions to the hearsay rule (Zech, 2016). Blockchain records are considered 'out-of-court statements' because they serve as evidence of transactions or events that occurred outside the courtroom, which are introduced to establish the truth of the information they contain. This classification stems from the nature of blockchain as a decentralized ledger technology that records and verifies transactions without the need for centralized authentication. When such records are used in court to substantiate the authenticity of documented transactions, they function as statements made outside of court, similar to traditional documentary evidence or witness testimonies. Unless they align with exceptions, such as those found in Section 803 of the Federal Rules of Evidence (FRE), they might be dismissed as inadmissible hearsay (Richter and Slowinski, 2018). Blockchain evidence is often introduced to establish the truth of the transactions it records, thus functioning as an 'out-of-court

statement.' Given this role, it naturally falls under the scrutiny of the hearsay rule, which generally excludes statements made outside the courtroom from being used to prove the truth of the matter asserted, due to concerns over their reliability.

The primary criteria for verifying the authenticity of documents for hearsay evidence revolve around the ability to establish the reliability and integrity of the evidence. In the context of blockchain, this involves demonstrating that the records are immutable and accurately reflect the transactions they represent. However, blockchain technology's inherent features—such as cryptographic security, immutability, and consensus mechanisms—challenge traditional concerns associated with hearsay evidence by providing a transparent and verifiable record of transactions. Therefore, while blockchain evidence is initially approached through the hearsay framework, its technological attributes invite a reevaluation of how such evidence is viewed in terms of reliability and admissibility. This reevaluation suggests that blockchain evidence may not fit neatly within traditional hearsay exceptions but instead may warrant the development of new legal standards or exceptions tailored to its unique characteristics (Kraft, 2017).

3.2 Criteria for judging whether blockchain evidence is hearsay: the relationship between computer program generation and human intervention

In United States v. Lizarraga-Tirado, the Ninth Circuit Court of Appeals grappled with the admissibility of digital evidence derived from Google Maps in an immigration case. The crux of the matter hinged on a Google Earth satellite image (Exhibit 1) and a computer-generated GPS "pushpin" (Exhibit 2), which the federal prosecutor introduced to validate that the defendant, an undocumented alien charged with illegal entry, was indeed apprehended within U.S. territory. Contradicting this, the defendant contended that he was detained on the Mexican side of the border. Given that the defense's argument fundamentally revolved around the exact location of the arrest, the Google Earth exhibits carried significant evidentiary weight. To support the prosecutor's argument, testimony from border patrol agents was introduced, detailing their use of handheld GPS devices to verify the defendant's location immediately before and at the moment of arrest. This evidence was pivotal in substantiating the charge of illegal entry by demonstrating conclusively that the defendant was apprehended within U.S. borders, as opposed to his claim of being on the Mexican side. To elucidate the origin of the Google Earth images and associated pushpins for the jury, the prosecutor demonstrated the automated generation of these markers on specific coordinates.

Judge Kozinski's assessment of the hearsay implications of the "Exhibit 1: Google Earth satellite images" was straightforward. He posited that these images, akin to photographs, merely depict factual representations of a particular place and moment. As a result, these digital representations were not considered hearsay under legal standards. This distinction was pivotal for the Ninth Circuit Court of Appeals, which led to the dismissal of the hearsay objection raised against the Google Earth images. The court's rationale was grounded in the understanding that such images, akin to photographs, offer direct, factual depictions of locations without the need for interpretative statements from an out-of-court source. The challenge arose with the "Exhibit 2: Pushpins". Given their automated generation, the defense argued that their authenticity and accuracy could not be cross-examined. Addressing this, Judge Kozinski referenced Federal Rule of Evidence 201(b), elucidating that any computer, upon searching a Google Earth coordinates, would generate analogous images and pushpins. Given that the markers were generated autonomously by the software without any human intervention, the Ninth Circuit concluded that they do not constitute hearsay. This decision highlights the distinction between evidence created through human testimonial processes and that generated by computer algorithms, underscoring the court's recognition of the reliability and objectivity of automated data production.

In reinforcing its analysis, the court referenced the precedent set by United States v. Lamons (United States Court of Appeals and Eleventh Circuit, 2008), which established that computer-generated records are generally not considered hearsay. This precedent underlines the legal distinction between testimonial evidence, which is subject to hearsay rules, and data produced by computers, which is recognized for its objective generation process, free from human bias or error. Hearsay applicability is predominantly tethered to human-derived out-of-court statements. Automated computer statements, devoid of human mediation, are thereby exempted from this classification (Knight, 2019).

Blockchain records, with their timestamps marking specific moments, are analogous to Google Earth images, serving as factual representations of distinct times and places. This similarity suggests that the autonomous generation of blockchain records might not inherently constitute hearsay, similar to how Google Earth's satellite images are treated. Yet, blockchain's distinction lies in the human agency required to initiate its transactions, setting it apart from the purely automated generation of Google Earth pushpins. This involvement of human action introduces complexities into the hearsay analysis of blockchain evidence, suggesting that the precedents set by cases like Lizarraga-Tirado may not directly apply. Consequently, a tailored evaluation recognizing blockchain's unique blend of automated integrity and human initiation is essential for accurately addressing its implications under hearsay law.

3.3 Hearsay evaluation of blockchain evidence: judgment of whether blockchain evidence is hearsay or its exceptions

The crux of the issue with blockchain evidence in relation to the precedent set in United States v. Lizarraga-Tirado lies in the nuances of computer-generated evidence and the role human intervention plays in its creation. A critical aspect requiring thorough examination is the role of human intervention at the inception of blockchain records. This initial human input raises the question of whether such records could be considered hearsay within legal proceedings. Understanding the extent to which human actions influence the creation and integrity of blockchain entries is essential for determining their admissibility as evidence (Singh and Chatterjee, 2019).

While computer-generated evidence devoid of human intervention is generally not classified as hearsay, blockchain presents a unique

quandary. The core argument revolves around the requirement for proper authentication of blockchain evidence. Notwithstanding any objections raised at trial, such evidence must inherently satisfy thresholds of reliability and accuracy. The prevailing legal sentiment in the U.S. posits that automatically computer-generated evidence is not hearsay. Extending this logic, blockchain records created through automated processes should, in theory, be exempt from hearsay classifications, mirroring the treatment of other computer-generated records. This exemption is predicated on the lack of human intervention in the record's creation, which aligns with the rationale for excluding certain types of electronic evidence from hearsay constraints. However, in instances where blockchain evidence is considered hearsay, the blockchain system itself might then be viewed as the declarant (Ching, 2016).

The point of contention arises from the human element in initiating transactions on the blockchain. It is axiomatic that a purely digital system, devoid of human input, can't make a "statement." Thus, if the supposed declarant is the computer or network, hearsay does not factor in. However, reframing the perspective to consider the human initiation of a transaction complicates matters. From this perspective, it is not the blockchain technology that acts as the declarant but rather the individual who inputs data into the system. The blockchain essentially functions as a digital ledger, storing information provided by users. Each time data is recorded on the blockchain, it constitutes a 'statement' by the user, thereby meeting one of the key criteria for hearsay (Lemieux, 2016). This interpretation emphasizes the role of human agency in creating the content of blockchain records, distinguishing these inputs from the technology's role as a passive container for the data. Understanding this distinction is crucial for legal analyses concerning the admissibility of blockchain-based evidence under the hearsay rule, pointing towards the need for legal standards that can accurately reflect the intricacies of digital information exchange. Moreover, since blockchain records are created outside the courtroom milieu, their use in validating the veracity of the stated material in legal proceedings does earmark them as hearsay. This perspective is consonant with the derivative theory of blockchain-recorded evidence.

While blockchain's immutability ensures that records cannot be altered once stored, it does not inherently validate the veracity of data at the point of entry (Sklaroff, 2017). This 'garbage in, garbage out' issue highlights a critical vulnerability; even though blockchain technology can secure data against post-entry tampering, it cannot guarantee the initial integrity of that data. To mitigate this concern, it is essential to implement rigorous verification processes at the point of data entry into the blockchain. This might include the cryptographic signing of data by trusted parties, the use of secure and verified data collection methods, or integrating blockchain with systems that have robust data validation mechanisms. Only through such comprehensive measures can the potential of blockchain as a reliable repository for evidentiary purposes be fully realized, addressing the valid concerns raised about pre-entry data falsification.

The exploration of hearsay in the context of blockchain evidence is crucial because it challenges traditional legal frameworks and necessitates a reevaluation of evidence admissibility standards. Blockchain technology, by its nature, blurs the lines between direct evidence and hearsay due to its digital, decentralized, and immutable record-keeping. The consideration of hearsay is essential as it directly impacts the legal process, including the authentication of evidence and the protection of defendants' rights. In judicial proceedings, the integrity and reliability of evidence are paramount. Blockchain's unique characteristics—such as the cryptographic sealing of data, the decentralized consensus for transaction validation, and the ledger's immutability—offer new dimensions for assessing evidence. These features compel a nuanced analysis beyond conventional hearsay rules, which were not designed with such technological advancements in mind. Thus, exploring hearsay classification helps illuminate the broader implications of integrating blockchain into the legal domain, ensuring that its use aligns with the principles of justice and fairness.

While blockchain evidence poses challenges in its classification concerning hearsay, not all blockchain records inherently qualify as such. Two primary reasons underpin this distinction:

Firstly, Intrinsic Human Element in Machine-Generated Data: In its truest essence, no statement is entirely machine-generated. Even the most sophisticated AI systems bear traces of human intervention. Machines, inclusive of their software and algorithms, are human-designed. If we were to apply rigorous standards to discern hearsay, then precedents like United States v. Lamons and United States v. Lizarraga-Tirado—which rule that machine-generated evidence is not hearsay—would lose their jurisprudential significance (Ferguson, 2016).

Secondly, Blockchain as an Incapable Declarant: In the case of United States v. Lizarraga-Tirado, the court considered Google Earth's satellite images and computer-generated pushpins not as hearsay because they were produced autonomously by a computer program without human intervention. This decision underscores a critical aspect of digital evidence: when data is generated and recorded autonomously by technology, it may not be subject to the same hearsay limitations as statements made by humans. Applying this logic to blockchain evidence, it is essential to distinguish the nature of the data generation and recording process. Blockchain technology operates through consensus algorithms that autonomously validate and record transactions across a distributed network. This process ensures the integrity and immutability of the data without direct human interference in the data's validation or recording phase, similar to how Google Earth's pushpins are generated. However, the initiation of blockchain transactions involves human action, distinguishing it from the purely automated process seen in Google Earth's satellite imagery. This human involvement could suggest a closer examination under hearsay rules, as the original input into the blockchain may reflect a human statement or intent. To reconcile this apparent contradiction, we must consider the role of blockchain as a secure and immutable ledger for recording data, similar to digital storage media like USB sticks or CDs. However, blockchain's unique value lies in its additional layers of security and immutability, which are not inherent to traditional storage devices. The technology itself, like the Google Earth software, does not create statements but rather securely records data input by humans. The subsequent automated process of data validation and recording by the blockchain may place it outside the traditional bounds of hearsay, akin to the rationale applied to Google Earth's pushpins. Thus, while the human element in initiating blockchain transactions introduces complexities, the overarching principle that data produced and recorded by technology may not constitute hearsay can still apply. This perspective requires a nuanced understanding of

blockchain's operational mechanics and its implications for hearsay can still apply.

Acknowledging this, it is clear that blockchain does not serve as a declarant in the legal sense. Instead, it acts as a technologically advanced medium for preserving evidence, where the integrity of the data is maintained from the moment of its entry. This characteristic positions blockchain as a tool in evidence management, offering assurances against manipulation that are unparalleled by conventional means of digital storage. Therefore, the examination of blockchain in judicial contexts should focus on its strengths as a repository for evidence, while recognizing the need for complementary measures to verify the authenticity of the data before its blockchain registration.

Even if the incipient transaction had human initiation, the subsequent processes, being immutable, reinforce the non-hearsay nature of such blockchain records (Lyons et al., 2018).

Building on this, American jurisprudential thought has conceptualized a fresh exception to traditional hearsay rules tailored for the digital age—the "e-hearsay exception." The admissibility of blockchain evidence vis-à-vis hearsay can be bifurcated by referencing this exception:

1. Blockchain Storage Records Under Derivation Theory: These constitute hearsay exceptions. While they encapsulate human declarations, the blockchain is not the declarant. As such, these records need to be evaluated against the hearsay rule and authenticated before serving as evidential proof.
2. Blockchain Transaction Records Under Automated Generation Ontology: These are not hearsay. Spawned autonomously by the blockchain, they bypass the hearsay rule's scrutiny.

In conclusion, the applicability of hearsay regulations to blockchain records hinges on whether these records meet specific hearsay exceptions. Records that are autonomously generated by the blockchain, without direct human input to the content of the data itself, do not fall within the traditional scope of hearsay since their creation and validation are purely technological processes. The integrity and authenticity of such records are assured through cryptographic authentication, making hearsay considerations irrelevant to them. Instead, the focus shifts to authentication standards, which evaluate the technical processes ensuring the data's immutability and the blockchain's operational security. This approach underscores the distinction between blockchain records as evidence and the conventional understanding of hearsay, emphasizing the importance of technical verification over hearsay analysis for autonomously generated records.

3.4 Can blockchain evidence invoke the judgment standard established in the United States v. Lizarraga-Tirado case?

From the preceding discussion, it is evident that blockchain evidence might be categorized either as hearsay exceptions or as non-hearsay. Given this variability, the logical query that arises is the applicability of the judgment criterion delineated in United States v. Lizarraga-Tirado. This article contends that the automatic generation characteristic of Google Earth is not an entirely fitting comparison for blockchain evidence. The human element in the initiation phase of blockchain transactions, and the potential biases therein, differentiate it from Google Earth's inherently automated tagging and recording (Snider, 2022).

Yet, two considerations emerge: 1. Inherently Hearsay, but Admissible: Blockchain evidence, under most conditions, qualifies as hearsay. However, this classification does not preclude its admissibility. 2. Objective Factual Depiction: Irrespective of human input during its inception, blockchain evidence chronicles objective realities. Its essence is not just the automated process of record generation but encompasses the record's induction into the blockchain system. Emphasizing its reliability, immutability, and authenticity, blockchain evidence bears semblance to Google Earth's depiction of specific instances and automatically generated markers. As such, the Lizarraga-Tirado case, which offers jurisprudential guidance for machine or computer-system-generated evidence, holds analogous value for blockchain evidence. Although blockchain and Google Earth serve different functions, the underlying principle of providing an objective and verifiable record makes the extrapolation of Lizarraga-Tirado's framework to blockchain evidence a viable consideration. This approach underscores the need for judicial systems to adapt and reconsider traditional hearsay rules in the face of evolving technology.

Once the non-hearsay nature of computer-generated data is clarified, concerns about potential subsequent alterations arise. While blockchain, theoretically, is resistant to post-initiation modifications—both external and internal—ensuring the originality and integrity of such evidence is pivotal (Levi and Lipton, 2018). Here, blockchain holds an edge over other computer programs like Google Earth, given its inherent robustness in authenticity and reliability. The GPS coordinates deliberation in United States v. Lizarraga-Tirado can offer insights into blockchain evidence's admissibility (Raskin, 2017).

As blockchain technology permeates more sectors in the future, resolving its evidentiary admissibility can catalyze its broader application, advancing the protection of parties' legitimate rights. Especially in cases of financial malfeasance where blockchain might be employed for money laundering, blockchain evidence can harness its intrinsic strengths.

4 Legislative changes of blockchain evidence

As technological advancements reshape our digital environment, the principles and regulations of evidence law must evolve accordingly. From a legislative standpoint, delineating clear criteria for the validity and regulation of blockchain evidence is paramount to ensuring its consistent admissibility in legal proceedings.

4.1 The federal Rules of Evidence regulates self-verification of blockchain records

In December 2017, the United States revised the Federal Rules of Evidence (FRE). Specifically, Article 902 was augmented with

provisions 902(13) and 902(14) to address the self-certification of electronic data, including potential blockchain evidence. This amendment aimed to streamline the ways parties handle electronically stored information (ESI), facilitating the self-certification of specific digital evidence, and thereby reducing the reliance on, and associated costs of, expert testimony. These provisions underscore a robust foundation for admitting blockchain evidence. The essence of these provisions lies in their recognition of electronic records' reliability when generated and maintained by a process that ensures accuracy. For blockchain, this means that records, which are cryptographically secured and consensus-driven, might fit within the ambit of these rules, given their design for inherent data integrity and immutability.

However, the application of these provisions to blockchain technology warrants careful consideration. While blockchain's decentralized verification and record-keeping mechanisms enhance the security and authenticity of stored data, equating this process with the self-certification criteria requires a comprehensive understanding of blockchain's operational dynamics. It is critical to distinguish between the automated integrity of blockchain records and the traditional electronic records contemplated by the Federal Rules.

Thus, while the Federal Rules of Evidence provide a foundation for the admissibility of blockchain evidence, they do not automatically apply. A detailed examination of the blockchain's functionality and its compliance with the Federal Rules' criteria for self-verification is necessary. This analysis ensures that blockchain evidence is not only admitted based on its technological features but also scrutinized to meet established legal standards for evidence reliability and authenticity.

4.2 Adjustments to blockchain evidence rules in state legislation

To address the admissibility challenges blockchain evidence faces amid technological advancements, several U.S. states have undertaken legislative amendments (Fenwick and Vermeulen, 2019). For instance, in February 2015, California introduced a bill proposing the use of blockchain for information storage (California Assembly Bill 1,326). Despite significant media attention, the bill failed to secure Senate approval.

Between February and March 2017, the Arizona Legislature passed the amended Arizona Electronic Transaction Act (Arizona, 2017). Article 5 of this Act recognizes blockchain records and electronic signatures, ensuring that smart contracts embedded within are not denied legal effect, validity, or enforceability.

In the same timeframe, Delaware updated the Delaware General Corporation Law. Section 224 of this legislation allows businesses to utilize distributed electronic networks, like blockchain, for maintaining corporate records, positing these networks as viable tools for corporate record-keeping and stock ledgers (Delaware, 2017). By 2018, Ohio had enacted legislation mirroring Arizona's provisions.

Illinois went a step further with the Blockchain Technology Act, which sanctions the use of blockchain technology in transactions. Furthermore, records generated via blockchain are deemed admissible as evidence in legal proceedings (Illinois General Assembly, 2020).

Vermont's Blockchain Enabling Act, passed in June 2016, introduced provisions recognizing the legitimacy of blockchain records. These records are admissible in court without needing external validation (Vermont General Assembly, 2016). Such records, once registered electronically on a blockchain and backed by a sworn statement from a qualified individual, are assumed truthful under oath. This positioned Vermont as the first state to set self-certification norms for blockchain evidence, thereby reinforcing the evidentiary significance of blockchain records. However, the bill has notable constraints:

Firstly, it transfers the evidentiary burden. Though the legislation attempts to dilute the self-certification presumption for blockchain evidence, it mandates that the bill's provisions are inapplicable when there's a perceived lack of trustworthiness in the information's source, preparation method, or circumstances. This indirectly shifts the burden of disproving blockchain evidence's reliability onto its challengers.

Besides, the legislation fails to distinguish between public and private blockchains, applying a universal standard. This broad application potentially paves the way for unreliable blockchain evidence to gain acceptance, undermining the very purpose of such rigorous standards (Wong et al., 2021). By 'broad application,' we refer to a scenario where the inherent features of blockchain are assumed to automatically confer reliability on all data recorded on a blockchain, regardless of its source or the accuracy of the data at the time of entry. This assumption could lead to a situation where evidence that has not been thoroughly vetted for accuracy or relevance is accepted simply because it is stored on a blockchain. Such a scenario undermines the purpose of establishing rigorous standards for evidence admissibility, which is to ensure that only reliable, relevant, and probative evidence is presented in court. The critical point here is that while blockchain technology provides a robust framework for data integrity post-entry, it does not inherently validate the veracity or relevance of the data before it is recorded. Therefore, a discerning approach is necessary to evaluate blockchain evidence, distinguishing between the technological advantages of blockchain for data security and the separate issue of data accuracy and reliability.

While Vermont's bill is undoubtedly a progressive stride towards codifying evidence standards for blockchain records, addressing its inherent limitations is crucial for holistic and effective legislation.

4.3 Improvement of blockchain evidence authenticity rules

Upon examining the legislative practices of the aforementioned states, one can discern a distinct advantage in their rules concerning the authenticity of blockchain evidence: substantive utility, which refers to the practical effectiveness and applicability of blockchain evidence within the legal framework, as established by the legislative practices in certain states. These jurisdictions have recognized and codified the value of blockchain technology in authenticating and preserving digital records, granting it legal standing. The 'substantive utility' thus denotes the tangible benefits these legal

provisions offer for using blockchain evidence in judicial processes. This can be attributed to three prevailing consensuses.

Scope of Rule Construction: The primary emphasis is on the authenticity of data once it has been recorded on the blockchain. Any records or data prior to its blockchain registration are not encompassed within these rule constructions.

Legal Authenticity Over Technical Infallibility: Blockchain evidence across various U.S. states is governed by principles such as the "presumption of business records exception." This implies that the judiciary does not seek an absolute, technical unforgeability in blockchain evidence. Instead, the emphasis is on achieving a "truth that conforms to the legal standards within a specific case." (Farzaneh et al., 2020).

Adoption of Lateral Validation Mechanisms: The authenticity of evidence can be evaluated from two perspectives: one that outlines comprehensive validation elements or standards from the outset, and another that prescribes methods to ascertain the veracity of the evidence. Given that many judicial officers currently lack the expertise to directly validate the authenticity of blockchain evidence, constructing a lateral or secondary validation mechanism emerges as a more pragmatic approach.

4.4 Role of expert witnesses to strengthen the probative value of blockchain evidence

The inherent reliability of blockchain as a technology does not automatically extend to the trustworthiness of the evidence recorded on it. Recognizing this, the role of expert witness testimonies becomes not to conflate the two but to clarify them separately. Expert witnesses can elucidate the technical underpinnings of blockchain technology—its encryption, consensus mechanisms, and immutability—to demonstrate its capability as a secure and reliable medium for storing data (Shafeeq et al., 2022). Simultaneously, they can assess the specific context in which data was entered into the blockchain, evaluating the procedures followed to ensure its accuracy and integrity at the point of entry. This approach provides a balanced method for assessing blockchain evidence's admissibility, distinguishing between the technology's reliability and the validity of individual records. It underscores the necessity for a detailed technical analysis of both the blockchain system in question and the specific evidence derived from it, ensuring that the court understands the distinction between the general security features of blockchain and the veracity of the particular piece of evidence.

For instance, as stipulated under Vermont's Rules of Evidence 902, blockchain records achieve self-authentication and consequent admissibility when complemented by a sworn statement from an individual possessing expertise in blockchain technology. It is important to note that such expert testimony primarily furnishes formal validation of the blockchain records' reliability. The onus of establishing the substantive veracity of its content remains with the concerned parties.

Those well-versed in blockchain technology can readily access and interpret blockchain records, demystifying its underlying concepts and operations for stakeholders in litigation. In cases involving digital tokens, regardless of the jurisdictional trial system in place, parties presenting blockchain evidence often seek professionals to elucidate the rudimentary mechanics of digital tokens and blockchain. Such explanations facilitate a more nuanced understanding of blockchain evidence and its evidentiary potential. In blockchain-centric financial crime scenarios, prosecutors equipped with direct evidence can further bolster their cases by enlisting specialists to clarify blockchain terminologies and the modus operandi of related financial crimes to the judiciary.

A case in point is the United States v. Costanzo, a money laundering case entailing the conversion of peer-to-peer digital tokens linked with drug trafficking proceeds. Here, the prosecution incorporated a law enforcement witness's expert testimony on Bitcoin and blockchain functionalities. This officer, instrumental in the investigation, possessed extensive experience in digital token-related cases and had undergone comprehensive blockchain analysis training. His deposition shed light on blockchain operational principles, covert transactions with the defendant, and methods employed in translating drug sale proceeds into digital tokens (McKinney et al., 2018).

While law enforcement witnesses play pivotal roles in numerous cases, it is crucial to consider neutrality. Defendants often view law enforcement testimonies with skepticism, leaning towards impartial third parties for professional depositions. Especially in intricate domains like blockchain, where the onus is on experts to distill complex technological matters for layperson juries or judges, the choice of witness becomes paramount. In blockchain-linked financial crime litigation, the strategy of opting for law enforcement witnesses is prevalent. Yet, some defendants, wary of potential biases, gravitate towards neutral, specialized professionals for more balanced insights.

4.5 Challenges of integrating blockchain into legal proceedings at the regional level

The challenges of integrating blockchain into legal proceedings at the regional level are manifold and can be categorized into legislative, technical, and practical domains.

Legislative Heterogeneity: Our study identifies a variety of state-level legislations, such as those in California, Arizona, Delaware, Illinois, Vermont, and Ohio, showcasing the diverse approaches to blockchain regulation. This diversity creates a fragmented legal landscape where the admissibility and treatment of blockchain evidence can vary significantly from one jurisdiction to another. The lack of standardized regulations complicates the integration of blockchain into legal proceedings.

Technical Complexity: Blockchain's technological intricacies pose a significant challenge. The evidentiary significance of blockchain is derived from its unique technological attributes, such as immutability, decentralization, and the consensus mechanism. However, the understanding of these technical aspects among legal professionals is often limited.

Expert Testimony Requirement: The paper emphasizes the importance of expert testimonies in establishing the authenticity of blockchain evidence. The reliance on experts to explain blockchain technology's operations to a non-technical audience (judges and jurors) introduces challenges related to the availability, cost, and variability of expert opinions. This can

affect the consistency and predictability of how blockchain evidence is treated across different cases and jurisdictions.

Practical Implementation Issues: Integrating blockchain into legal proceedings involves more than theoretical legal acceptance. It requires practical mechanisms for verifying the authenticity of blockchain records and understanding their relevance and reliability as evidence. The paper suggests potential feedback mechanisms, such as the establishment of an information technology review committee, to bridge the gap between theoretical legal frameworks and practical implementation. However, setting up such mechanisms involves logistical, financial, and institutional challenges.

To address these challenges, this paper recommends a comprehensive framework that combines both technological and legal perspectives. This framework aims to ensure the consistent integration of blockchain evidence within judicial processes, preserving procedural justice while harmonizing blockchain technology with established principles of justice. It involves legislative efforts to standardize the treatment of blockchain evidence, education initiatives to improve the legal community's understanding of blockchain technology, and practical guidelines for the authentication and evaluation of blockchain evidence in court.

5 Summary

Undoubtedly, the expansive network of independent validators buttresses the credibility and veracity of blockchain evidence. Scholarly explorations into blockchain evidence chiefly concentrate on the trustworthiness of factual assertions, emphasizing the unblemished nature of blockchain records and the absence of human interference during their formulation. When these records remain impervious to external influences and transparently verify pertinent facts, their reliability, precision, and authenticity stand validated. Nonetheless, courts encounter a dilemma during adjudications. Although the blockchain framework can vouch for the fidelity of autonomously generated outcomes, it cannot ascertain the accuracy of the foundational information fed into the blockchain. Imperfections or lapses at the initial stages might lead to the incorporation of fallacious data into the blockchain. Despite receiving erroneous data, the blockchain, acting on its predefined code, would process it as legitimate and archive it accordingly.

Thus, to bolster the authenticity validation of blockchain evidence concerning admissibility, legislators, blockchain industry standard associations, and other relevant bodies should ardently endeavor to establish a robust blockchain evidence consensus mechanism, with the Hash algorithm as its cornerstone, and devise associated operational guidelines. The proposal for a robust blockchain evidence consensus mechanism seeks to standardize the validation of blockchain records for legal admissibility. This initiative requires collaboration between legislators, industry standards bodies, and the legal community to integrate the cryptographic strength of hash algorithms into a universally accepted framework. Such a mechanism aims to ensure the integrity and reliability of blockchain evidence, providing a clear, cryptographic verification process that courts can trust. Operational guidelines would accompany the consensus mechanism, outlining the procedures for authenticating blockchain records. These guidelines would detail how to apply hash algorithms and assess the security of the blockchain network, offering a consistent approach for evaluating evidence across different legal systems. By fostering a standardized method for blockchain evidence verification, this mechanism promises to simplify the admissibility process, enhance the credibility of blockchain as a source of evidence, and align technological innovation with judicial standards. Addressing core concerns such as code standardization and consensus algorithms at the infrastructural level of blockchain can dramatically alleviate the evidentiary burden on litigants in authenticating blockchain records, subsequently diminishing the judiciary's resource allocation in scrutinizing blockchain evidence.

However, it is essential to recognize that blockchain technology is not a monolithic concept, and its characteristics and applications can vary significantly across different implementations. Public blockchains, such as the Bitcoin blockchain, operate on a permissionless basis and rely on a decentralized network of nodes to validate transactions. In contrast, private or permissioned blockchains, also known as "sidechains," are developed and controlled by centralized entities and may have different levels of decentralization and trust assumptions. These distinctions have important implications for the reliability and admissibility of blockchain evidence, as the specific architecture and governance model of a blockchain system can impact the integrity and trustworthiness of the data stored on it.

Moreover, the legal considerations surrounding blockchain evidence may extend beyond traditional blockchain transactions to encompass other types of content stored on blockchain-based ledgers, such as non-fungible tokens (NFTs). NFTs are unique digital assets that represent ownership or rights to specific pieces of content, such as artwork, collectibles, or real-world assets. The generation and transfer of NFTs within a blockchain-based system raise additional challenges for their use as evidence in legal proceedings, as the legal status and enforceability of NFTs may vary depending on the jurisdiction and the specific nature of the NFT in question.

Certainly, blockchain innovations are redefining the conventional pattern of judicial equity. The critical challenge lies in adapting judicial due process to meet the demands of emerging technologies and ensuring a fair allocation of rights and responsibilities within this updated legal framework. This involves rethinking traditional legal processes to incorporate the unique characteristics and implications of innovations such as blockchain, thereby maintaining justice and equity in a rapidly evolving digital world. What's the assurance of rights for the stakeholders? Currently, an actionable and pragmatic approach entails broadening the evaluative standards of due process from both an external assessment viewpoint and its intrinsic ethos. This can pave the way for refining associated procedures and evidentiary rules in the realm of automated judicial determinations via technological due process. Ensuring blockchain technology aligns with justice principles requires a comprehensive approach: from embracing core legal ideologies to adapting detailed regulatory frameworks, thereby avoiding mismatches. A crucial step towards this integration is establishing transparency about the technology's origins. For instance, blockchain providers should make their system's source code publicly accessible. Public blockchains operate on an open-source model where transparency and accessibility are paramount. The public accessibility of their source code is a key feature that allows

for scrutiny, trust, and security through collective verification by the community. In contrast, private blockchains, managed by specific entities or consortia, may not always follow the same principle of open access to their source code due to proprietary concerns, security, and controlled access needs. While transparency in the source code can enhance trust and security in both types of blockchains, the approach to accessibility may vary based on the blockchain's intended use case, governance model, and the need to protect sensitive information.

Then, the sanctity and trustworthiness of technology should be enhanced. Incorporating blockchain technology into judicial systems not only involves technological implementation but also requires a consensus on its ethical use and governance. To ensure blockchain applications align with societal values and legal standards, it is crucial to engage the public and stakeholders in their development and oversight. Ethical guidelines and governance frameworks must be established to dictate the technology's use, prioritizing privacy, equity, and accountability.

Besides, when employing blockchain technology, judicial authorities should transparently notify all concerned parties, even bestowing upon them the rights of refutation and objection. In essence, actualizing the procedural justice of blockchain necessitates rigorous exploration to systematically align technological and legal dimensions, ensuring the seamless interplay between blockchain technology and judicial principles without causing discord or inconsistency.

In conclusion, this paper makes significant contributions to understanding blockchain's integration into judicial systems, emphasizing the need for a comprehensive approach to its admissibility and reliability as evidence. It proposes a specialized consensus mechanism to standardize blockchain evidence authentication, enhancing legal processes. Furthermore, it outlines strategies to bolster the technology's trustworthiness, including security, transparency, ethical governance, and stakeholder engagement, crucial for public trust and legal alignment. The importance of expert testimony in clarifying blockchain's technical aspects for legal contexts is also underlined, advocating for neutrality to prevent biases.

This research stands out for bridging the gap between technology and law, offering a blueprint for standardizing legal approaches to blockchain and urging ethical and transparent technology use. Its educational value and groundwork for future policy-making highlight the urgency of legal systems adapting to technological advancements, ensuring blockchain's integration serves justice and fairness effectively. This contribution is pivotal in guiding legal professionals, technologists, and policymakers through the complexities of blockchain technology, marking a significant step towards modernizing judicial processes with cutting-edge technologies. By treating blockchain as a means rather than a phenomenon and considering the specific architecture, content, context, and procedural integrity of blockchain evidence, this paper provides a comprehensive perspective on the evidentiary implications of this transformative technology.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

XW: Writing–original draft, Methodology, Formal Analysis. YW: Writing–review and editing, Writing–original draft, Supervision, Methodology, Formal Analysis, Conceptualization. ZM: Writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

Author XW was employed by Sage IT Consulting Group.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Antonopoulos, A. M. (2017). *Mastering Bitcoin: programming the open blockchain*. Sebastopol, California, United States: O'Reilly Media, Inc.

Arizona (2017). Arizona house bill 2417. Available at: https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf.

Benet, J. (2014). IPFS - content addressed, versioned, P2P file system. Available at: http://arxiv.org/abs/1407.3561 (Accessed: April 19, 2023).

Burnham, W. (2016). *Introduction to the law and legal system of the United States*. St. Paul, MN, USA: West Academic Publishing.

Buterin, V. (2015). On public and private blockchains. Available at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (Accessed April 19, 2023).

Ching, J. (2016). Is blockchain evidence inadmissible hearsay? Available at: https://www.law.com/sites/almstaff/2016/01/07/is-blockchain-evidence-inadmissible-hearsay/ (Accessed April 19, 2023).

Collingridge, D. (1980). *The social control of technology*. New York: St. Martin's Press.

Damaska, M. (2019). *Evaluation of evidence: pre-modern and modern approaches*. Cambridge, United Kingdom: Cambridge University Press.

Delaware (2017). Delaware general corporation law, section 224. Available at: https://delcode.delaware.gov/title8/c001/sc07/index.html.

Farzaneh, A., Koosha, S., Boochanpour, M., and Srivastava, G. (2020). "On search friction of route discovery in offchain networks," in 2020 IEEE International Conference

on Blockchain (Blockchain), Rhodes, Greece, November. 2020, 255–262. doi:10.1109/Blockchain50366.2020.00039

Fenwick, J., and Vermeulen, K. (2019). A primer on blockchain, smart contracts & crypto-assets from a legal perspective. *SSRN Electron. J.*, doi:10.2139/ssrn.3488542

Ferguson, A. G. (2016). The Internet of things and the fourth amendment of effects. *Calif. Law Rev.* 104 (4), 805–880. doi:10.15779/Z38BG31

Glendon, M. A., Carozza, P. G., and Picker, C. B. (2016). *Comparative legal traditions in a nutshell*. St. Paul, MN: West Academic Publishing.

Guadamuz-Gonzalez, M. (2021). The treachery of images: non-fungible tokens and copyright. *J. Intellect. Prop. Law Pract.* 16 (12), 1367–1378. doi:10.1093/jiplp/jpab102

Hileman, G., and Rauchs, M. (2017). 2017 global blockchain benchmarking study. *SSRN Electron. J.*, doi:10.2139/ssrn.3040224

Hyperledger, H. (2023). Introduction — hyperledger-fabricdocs master documentation. Available at: https://hyperledger-fabric.readthedocs.io/en/release-2.2/ (Accessed April 19, 2023).

Illinois General Assembly (2020). Illinois blockchain technology act. Available at: https://www.ilga.gov/legislation/ilcs/.

Knight, E. (2019). Blockchain jenga: the challenges of blockchain discovery and admissibility under the federal rules. *Hofstra Law Rev.* 48 (2), 519–553.

Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C. (2016). "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, May 2016, 839–858. doi:10.1109/SP.2016.55

Kraft, T. J. (2017). Big data analytics, rising crime, and forth amendment protections. *J. Law, Technol. Policy* 259.

Kshetri, N., and Voas, J. (2018). Blockchain in developing countries. *IT Prof.* 20 (2), 11–14. doi:10.1109/MITP.2018.021921645

Kumar, R., and Tripathi, R. (2019). "Traceability of counterfeit medicine supply chain through Blockchain," in 2019 11th International Conference on Communication Systems and Networks (COMSNETS), Bengaluru, India, January. 2019, 568–570. doi:10.1109/COMSNETS.2019.8711418

Lee, J. (2021). Non-fungible tokens and copyright law. *SSRN Electron. J.*, doi:10.2139/ssrn.3905452

Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Rec. Manag. J.* 26 (2), 110–139. doi:10.1108/RMJ-12-2015-0042

Levi, S. D., and Lipton, A. B. (2018). An introduction to smart contracts and their potential and inherent limitations. Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ (Accessed April 19, 2023).

LII (2022). Federal rules of evidence, rules 401, 403, 901. Available at: https://www.law.cornell.edu/rules/fre.

Lyons, T., Courcelas, L., and Timsit, K. (2018). Blockchain and the GDPR. Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (Accessed: April 19, 2023).

McKinney, S., Landy, R., and Wilka, R. (2018). Smart contracts, blockchain, and the next frontier of transactional law. *Wash. J. Law, Technol. Arts* 13 (3), 313–347. doi:10.2139/ssrn.3103612

Merryman, J. H., and Pérez-Perdomo, R. (2019). *The civil law tradition: an introduction to the legal systems of europe and Latin America*. Redwood City, California, United States: Stanford University Press.

Mnookin, J. L. (2013). Atomism, holism, and the judicial assessment of evidence. Available at: https://www.uclalawreview.org/atomism-holism-and-the-judicial-assessment-of-evidence/ (Accessed: April 19, 2023).

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton, New Jersey, United States: Princeton University Press.

Nascimento, S., Pólvora, A., and Sousa Lourenço, J. (2018). *Blockchain4EU: blockchain for industrial transformations*. EUR 29215 EN. Luxembourg: European Commission. doi:10.2760/204920

Natoli, C., Yu, J., Gramoli, V., and Esteves-Verissimo, P. (2019). Deconstructing blockchains: a comprehensive survey on consensus, membership and structure. Available at: http://arxiv.org/abs/1908.08316 (Accessed: April 19, 2023).

Pappas, J. M. (2022). Blockchain evidence: hearsay, authentication, and the best evidence rule. *SSRN Electron. J.*, doi:10.2139/ssrn.4066534

Polydor, S. (2020). Blockchain evidence in court proceedings in China--A comparative study of admissible evidence in the digital age (as of June 4, 2019). *Stanf. J. Blockchain Law Policy* 3, 96. doi:10.2139/ssrn.3418485

Raskin, M. (2017). The law and legality of smart contracts. Available at: https://georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017/ (Accessed April 19, 2023).

Regner, A., Schweizer, L., and Urbach, N. (2018). "Blockchain and GDPR: application scenarios and compliance requirements," in Proceedings of the 1st ERCIM Blockchain Workshop 2018, Amsterdam, Netherlands, May 2018, 20–31.

Richter, H., and Slowinski, P. R. (2018). The data sharing economy: on the emergence of new intermediaries. *IIC - Int. Rev. Intellect. Prop. Compet. Law* 50, 4–29. doi:10.1007/s40319-018-00777-7

Riva, G. M. (2020). What happens in blockchain stays in blockchain. A legal solution to conflicts between digital ledgers and privacy rights. *Front. Blockchain* 3. doi:10.3389/fbloc.2020.00036

Savelyev, A. (2017). Contract law 2.0: «Smart» contracts as the beginning of the end of classic contract law. *Inf. Commun. Technol. Law* 26 (2), 116–134. doi:10.1080/13600834.2017.1301036

Savelyev, A. (2018). Copyright in the blockchain era: promises and challenges. *Comput. Law Secur. Rev.* 34 (3), 550–561. doi:10.1016/j.clsr.2017.11.008

Shafeeq, A., Latiff, A., Iskandar, F., Arshad, R., Zhang, M., and Zhang, K. (2022). Blockchain for public sector services: cases from the UAE and Estonia. *Sustainability* 14 (7), 4067. doi:10.3390/su14074067

Singh, A., and Chatterjee, D. (2019). "Evaluating time varying connectivities and system throughput in opportunistic networks for smart grid applications," in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, April. 2019, 589–594. doi:10.1109/WF-IoT.2019.8767305

Sklaroff, J. M. (2017). Smart contracts and the cost of inflexibility. *Univ. Pa. Law Rev.* 166, 263–303.

Snider, S. R. (2022). Blockchain and the law of evidence: authentication of blockchain-based legal records. *SSRN Electron. J.*, doi:10.2139/ssrn.4033172

Supreme Justia (1970). In re Winship, 397 U.S. 358, in re Winship. Available at: https://supreme.justia.com/cases/federal/us/397/358/.

Supreme Justia (1994). Victor v. Nebraska, 511 U.S. 1. Available at: https://supreme.justia.com/cases/federal/us/511/1/.

Tuzet, G. (2020). Assessment criteria or standards of proof? An effort in clarification. *Artif. Intell. Law* 28 (1), 91–109. doi:10.1007/s10506-018-9233-1

United States Court of Appeals, Eleventh Circuit (2008). United States v. Lamons, 532 F.3d 1251 (11th Cir. 2008). Available at: https://casetext.com/case/us-v-lamons.

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT (2015). United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. 2015). Available at: https://casetext.com/case/united-states-v-lizarraga-tirado.

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT (2020). United States v. Costanzo, 956 F.3d 1088 (9th Cir. 2020). Available at: https://casetext.com/case/united-states-v-costanzo-24.

United States District Court District of Maryland. Lorraine v. Markel American insurance Co., 241 F.R.D. 534 (D. Md. 2007), 2007, Baltimore: United States District Court District of Maryland.

USC (2022). Federal rules of evidence, 28 U.S.C. Available at: https://www.uscourts.gov/sites/default/files/federal_rules_of_evidence_december_1_2022_0.pdf.

Vermont General Assembly (2016). Vermont blockchain enabling act, H.868. Available at: https://legislature.vermont.gov/bill/status/2016/H.868.

Wang, X., and Zha, Q. (2021). Consensus mechanism and algorithm based on blockchain technology: a survey. *IEEE Access* 9, 43920–43949. doi:10.1109/ACCESS.2021.3066787

Wirth, C., and Kolain, M. 2018, "Privacy by BlockChain design: a blockchain-enabled GDPR-compliant approach for handling personal data," in Proceedings of 1st ERCIM Blockchain Workshop 2018, Amsterdam, Netherlands, May 2018.

Wong, M. C. (2021). "Blockchain and alternative dispute resolution: opportunities and challenges," in *Handbook of blockchain law: a guide to understanding and resolving the legal challenges of blockchain technology*. Editors P. Hacker, I. Lianos, G. Dimitropoulos, and S. Eich (Cham: Springer International Publishing), 333–345.

Wright, A., and De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electron. J.*, doi:10.2139/ssrn.2580664

Wu, H., and Zheng, G. (2020). Electronic evidence in the blockchain era: new rules on authenticity and integrity. *Comput. Law Secur. Rev.* 36, 105401. doi:10.1016/j.clsr.2020.105401

Wüst, K., and Gervais, A. (2018). "Do you need a blockchain?," in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, June, 2018, 45–54. doi:10.1109/CVCBT.2018.00011

Xu, J. J. (2016). Are blockchains immune to all malicious attacks? *Financ. Innov.* 2 (1), 25. doi:10.1186/s40854-016-0046-5

Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018). *Blockchain technology overview*. Gaithersburg, Maryland, United States: National Institute of Standards and Technology, NISTIR. doi:10.6028/NIST.IR.8202

Zech, H. (2016). A legal framework for a data economy in the European digital single market rights to use data. *11 J. Intellect. Prop. Law Pract.* 460, 470. doi:10.1093/jiplp/jpw049

Zou, M. (2019). The application of blockchain technology in the field of evidence: a comparative study of China, us, and europe. *SSRN Electron. J.*, doi:10.2139/ssrn.3447404

Zweigert, K., and Kötz, H. (1998). *An introduction to comparative law*. Oxford, United Kingdom: Oxford University Press.