

# Superficial Scrutiny: An Empirical Exploration on Blockchain Evidence from Chinese Courts

Zelin Su

Department of Criminal Investigation, Beijing Police College, Beijing, China

Ph.D. in law, assistant professor in Beijing Police College, visiting scholar in Northwestern University, Email: [suzelin@bjpc.edu.cn](mailto:suzelin@bjpc.edu.cn)

Haoyang Zhao

Department of Economics, Duke University, Durham, North Carolina.

Ph.D. candidate in Duke University, Email: [luke.zhao@duke.edu](mailto:luke.zhao@duke.edu)

Abstract: In judicial practice, blockchain evidence is frequently regarded as self-authenticating by virtue of its decentralized storage architecture and cryptographic safeguards. Nevertheless, these very characteristics may also lead judges to adopt a superficial standard of review, thereby both relaxing the admissibility threshold for blockchain evidence and attenuating its probative value within the broader fact-finding process. Based on empirical analysis of 2,741 judgments, we find that there are two distinct paths behind the seemingly high admissibility rate of blockchain evidence: a logic-driven path of substantive scrutiny and a cue-driven path of superficial scrutiny. Deeper analysis reveals that “notarization or forensic examination” and “explicit objections” both significantly increase the likelihood of substantive scrutiny, indicating that judges tend to construct chains of fact through multiple, interrelated pieces of information. While such external verification can indeed promote substantive scrutiny, the primary responsibility must rest with judges rather than litigants. Accordingly, future reforms should aim to reduce over-reliance on peripheral cues and, by strengthening courtroom communication, enhancing the effectiveness of cross-examination, and refining evidentiary rules, foster a shift toward substantive scrutiny of blockchain evidence.

Keywords: Blockchain evidence; superficial scrutiny; logistic regression analysis; cognitive psychology.

## 1. Introduction

The court's duty to give reasons is regarded as a "function of due process, and therefore of justice,"<sup>1</sup> which also constitutes the very purpose of a judgment. In this sense, substantive scrutiny, as opposed to superficial scrutiny, demands that *justice not only be done, but also be seen to be done*—which is to say, the judicial task is twofold: first, to enable the parties to understand why they have won or lost; and second, to provide sufficient detail and analysis to allow an appellate court to determine whether the judgment is sustainable.

Across jurisdictions, the duty to provide reasons in judicial decisions remains a persistent and unresolved challenge. As scholars have noted, although this duty is widely recognized in principle, the threshold for what constitutes adequate reasoning varies significantly across cases and courts, making it difficult to determine when a judgment falls short in practice.<sup>2</sup> Moreover, courts sometimes acquire prior consents from the parties and issue decisions without providing any explanation, which risks undermining transparency, appellate oversight, and public confidence in the judicial system.<sup>3</sup> Superficial scrutiny in judicial decisions has also been a longstanding practical issue in China.<sup>4</sup> After the 2012 revision of the *Criminal Procedure Law of the People's Republic of China*, "How to make court proceedings shift from superficial to substantive" became a focal theoretical topic for Chinese scholars. The court proceedings emphasize adhering to the principle of immediacy, requiring that judgments are grounded in evidence presented directly and orally in court.<sup>5</sup> This lays the foundation

---

<sup>1</sup> *Flannery v. Halifax Estate Agencies Ltd.*, [1999] EWCA Civ 811 (Eng. C.A.), aff'd by [2000] 1 All ER 373

<sup>2</sup> Hock Lai Ho, *The Judicial Duty to Give Reasons*, 20 Leg. Stud. 42 (2000).

<sup>3</sup> Eyal Zamir, *With No Reason: Allowing Courts to Decide Cases Without Explaining Their Decisions*, 43 Civ. Just. Q. 395 (2024).

<sup>4</sup> He Jiahong, Xingshi Tingshen Xuhua de Shizheng Yanjiu [Empirical Studies on Nominalization of Criminal Court Trials], *Faxuejia* [Jurist], no. 6, 2011, at 124–136.

<sup>5</sup> Groenhuijsen, M.S. & Selçuk, H., *The Principle of Immediacy in Dutch Criminal Procedure in the Perspective of European Human Rights Law*, 126 Journal of Entire Criminal Law Science (Zeitschrift für die gesamte Strafrechtswissenschaft) 248 (2014).

for substantive scrutiny—one that is grounded in direct confrontation and in-court reasoning. By contrast, superficial scrutiny manifests as “simplified argumentation,” “clichéd expressions,” and “heavy reliance on third-party institutions for reasoning support.”

Compared to traditional forms of evidence, blockchain evidence,<sup>6</sup> as a type of technical evidence, presents a greater challenge when it comes to substantive scrutiny. An overall trend is the unusually high admissibility rate: After surveying 2,741 cases related to blockchain evidence from the past six years, the plaintiffs’ litigation requests in 2,452 cases were fully or partially supported,<sup>7</sup> accounting for 89.46% of the total. However, a high admissibility rate itself does not necessarily suggest superficial scrutiny. Building on this macro-level trend, a closer examination reveals two notable features that appear repeatedly in these cases. First, blockchain evidence is rarely treated as independently probative. Instead, it is often accompanied by “opinion evidence” in the form of notarial certificates, forensic expert opinions, and similar opinion-based evidence, indicating that judges may rely on these auxiliary sources to establish the credibility of blockchain evidence. Second, cross-examination of blockchain evidence tends to be minimal or perfunctory. In many cases, the adverse party either raises no substantive objection or offers only cursory challenges. More importantly, judges seldom engage with the procedural integrity of how the evidence was obtained or examine its factual relevance to the disputed issues. These two features combined – relying on opinion evidence from third parties and potentially perfunctory objections – raise the question whether the court has paid sufficient effort to examine blockchain evidence. In other words, whether blockchain evidence is

---

<sup>6</sup> Zelin Su, *Evidentiary Value and Evidentiary Status of Blockchain Evidence*, 29 Int’l J. Evid. & Proof 58 (2024).

<sup>7</sup> Full support refers to cases where all claims by the plaintiffs were upheld, while partial support involves cases where only some aspects of the claims were granted. Examples of partial support include instances where the court upheld a fraction of the plaintiff’s monetary claim, such as supporting only 2,000 yuan of a requested 10,000 yuan, or only awarding compensation for property damage without ordering restoration to its original state. Any instance of partial support implies that blockchain evidence was effectively considered and accepted in the decision.

substantively scrutinized.

To answer this question, we adopt an empirical method to establish the relation between the scrutiny paths of blockchain evidence and related factors mentioned above, such as third-party verification and raising objections. More specifically, we first established a theoretical framework that models the driving forces of evidence scrutiny. When facing a piece of evidence, the judge decides the desired effort level to scrutinize the evidence by evaluating the benefits and costs of paying efforts, such as gains or losses in reputation or career prospects. Case-specific features are then modeled as factors that affect the benefits and costs of efforts. The theoretical model then becomes the foundation of the empirical analysis, where we use logistic regression to analyze how case-specific features affects the blockchain evidence scrutiny, with data extracted from judgements using semantic analysis.

Regarding research on blockchain evidence, the current literature mainly focuses on three aspects: demonstrating the value of blockchain evidence, proposing improvements to admissibility rules, and, in a small number of articles, addressing its probative value. First, in terms of evidential value, most scholars hold a positive attitude towards its judicial application. For example, Vivien Chan believes that blockchain technology has been applied in Chinese Internet Courts for tamper-resistant evidence reservation, a process that is more cost-effective.<sup>8</sup> Zheng Ge contends that, in the future, all areas involving records and verification can be completed with the help of blockchain technology.<sup>9</sup> Zhang Yujie considers blockchain evidence to be a comprehensive innovation of the existing evidence law system.<sup>10</sup> In contrast, a small number of scholars do not recognize the judicial value of blockchain

---

<sup>8</sup> Vivien Chan & Anna Mae Koo, *Blockchain Evidence in Internet Courts in China: The Fast Track for Evidence Collection for Online Disputes*, Lexology, July 15, 2020.

<sup>9</sup> Zheng Ge, Qukuailian yu Weilai Fazhi [Blockchain and the Future Rule of Law], *Dongfang Faxue* [Oriental Law], no. 3, 2018, at 75–86.

<sup>10</sup> Zhang Yujie, Qukuailian Jishu de Sifa Shiyong, Tixi Nanti yu Zhengju Fa Gexin [Judicial Application, System Problems and Evidence Law Innovation of Blockchain Technology], *Dongfang Faxue* [Oriental Law], no. 3, 2019, at 99–

evidence. Hong Wu and Guan Zheng argue that, although blockchain technology may fundamentally change the rules of evidence, it also cannot be absolutely tampered with.<sup>11</sup> Second, as for the admissibility of this type of evidence, studies are abundant, but primarily focus on authentication. Some scholars hold a negative view of the self-authentication of blockchain evidence. For example, Wang Congguang argues that the authenticity of blockchain evidence should be confined to the carrier level.<sup>12</sup> Another group of scholars holds a positive view of the self-authentication of blockchain. For example, Shi Guanbin and Chen Quanzhen contend that electronic data certified by blockchain can be regarded as automatically generated.<sup>13</sup> Liu Pinxin believes that, due to the technical features of hash checking, time locking, and node verification, the authenticity of data is ensured once the blockchain evidence is placed on the chain.<sup>14</sup> Third, although there is a small body of literature addressing specific rules to blockchain evidence, it largely lacks discussion on the probative value and the corresponding proof theory. For these specific rules, Deng Yongmin and Xu Xin argue that the verification rules for blockchain evidence should be clarified,<sup>15</sup> while Yang Jiwen maintains that the comprehensive verification mechanism for online and offline evidence should be externally enhanced.<sup>16</sup> Even so, the existing literature fails to provide a systematic analysis of each stage in which blockchain evidence is

---

109.

<sup>11</sup> Hong Wu & Guan Zheng, *Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity*, *Computer Law & Security Review*, 36, 105401, 2020.

<sup>12</sup> Wang Congguang, *Qukuailian Cunzheng yu Yuanjian Guiding [Blockchain-Based Evidence Preservation and the Original Document Rule]*, *Shanghai Faxue Yanjiu Jik kan [Shanghai Law Research Journal Series, Vol. 5 (Total Vol. 53)]*, 2021, at 222–230.

<sup>13</sup> Shi Guanbin & Chen Quanzhen, *Lun Quankuailian Cunzheng Dianzi Shuju de Youshi ji Sifa Shencha Lujing [On the Advantages and Judicial Review Path of Blockchain-Based Electronic Evidence]*, *Xinan Minzu Daxue Xuebao (Renwen Shekexue Ban) [Journal of Southwest Minzu University (Humanities & Social Sciences)]*, no. 1, 2021, at 67–73.

<sup>14</sup> Liu Pinxin, *Lun Quankuailian Zhengju [On Blockchain Evidence]*, *Faxue Yanjiu [Law Studies]*, no. 6, vol. 43, 2021, at 130–148.

<sup>15</sup> Deng Yongmin & Xu Xin, *Quankuailian Zhengju “Keguan Yinzhen” de Helixing Sikao [Rational Reflections on the “Objective Validation” of Blockchain Evidence]*, *Henan Shifan Daxue Xuebao (Zhexue Shehui Kexue Ban) [Journal of Henan Normal University (Philosophy & Social Sciences Edition)]*, no. 3, vol. 49, 2022, at 68–75.

<sup>16</sup> Yang Jiwen, *Quankuailian Zhengju Guize Tixi [Blockchain Evidence Rule System]*, *Suzhou Daxue Xuebao (Zhexue Shehui Kexue Ban) [Journal of Soochow University (Philosophy & Social Sciences Edition)]*, no. 3, 2021, at 86–95.

involved throughout the entire litigation process.

While the above studies focus on theoretical and doctrinal discussions of blockchain evidence, understanding its practical application also requires insights from empirical research on electronic evidence more broadly. The number of such research is rather limited, partly due to the technical difficulty of assembling a qualified database from large numbers of judicial documents. For some examples, Ferreira & Gromova conducted a statistical analysis of 92 cases from the Brazilian Center for Mediation and Arbitration, examining the types of electronic evidence used in arbitration;<sup>17</sup> Bérubé used a trial case to explore in depth the process by which digital traces are transformed into electronic evidence and the challenges involved;<sup>18</sup> Bauge employed surveys and interviews to assess the scope and implementation of peer review in the field of digital forensics.<sup>19</sup> Overall, in the field of electronic evidence, empirical research with quantitative data analysis remains limited.

To our best knowledge, this paper is the first to explore the blockchain evidence scrutiny paths with empirical methods. We argued that the evidence scrutiny decision can be considered as a result of a cost-benefit analysis of the judge, established a clear and relatively general set of rules to categorize evidence scrutiny patterns from the judgements, and showed that third-party authentication and explicit objections have positive effects on substantive scrutiny. These findings suggest that promoting substantive scrutiny requires not only enhancing procedural rules, but also constructing a cognitively oriented model of proof—one that clarifies relevance, enforces admissibility standards, and strengthens probative reasoning through courtroom communication and abductive logic, which are

---

<sup>17</sup> Daniel B. Ferreira & Elizaveta A. Gromova, *Electronic Evidence in Arbitration Proceedings: Empirical Analysis and Recommendations*, 20 Digital Evid. & Elec. Signature L. Rev. 30 (2023)

<sup>18</sup> Maxime Bérubé, Laurie-Anne Beaulieu, Sophie Allard & Vincent Denault, *From Digital Trace to Evidence: Challenges and Insights from a Trial Case Study*, 65 Sci. & Just. 101306, 101309 (2025).

<sup>19</sup> Rune Kenneth Bauge, Elénore Ryser, Nina Sunde & Graeme Horsman, *Evaluating the Scope of Peer Review in Digital Forensics: Insights from Norway and the U.K.*, 65 Sci. & Just. 139, 139 (2025).

abstracted from the common mechanisms underlying the observed positive effects.

The rest of this paper proceeds as follows. Section 2 outlines the technological advantages and potential limitations of blockchain evidence in terms of admissibility and probative value. Section 3 introduces the theoretical foundation for the assumption of superficial scrutiny, and based on observed misunderstandings in judicial practice, proposes two possible scrutiny paths: a logic-driven central path and a clues-relying peripheral path, shaped by factors such as notarization or forensic examination and explicit objections. Section 4 presents the empirical strategy, including the construction of a binary logistic regression model to test the relationship between these factors and the level of substantive scrutiny. Section 5 discusses the results and their implications.

## 2. Advantages and limitations of blockchain evidence

The greatest advantage of blockchain evidence lies in its ability to shift “personal trust” into “technological trust”. This helps minimize the influence of human factors in litigation—an activity heavily reliant on interpersonal communication—thus reducing potential loopholes and “gray areas” in judicial processes and enhancing mutual trust among participants. However, this advantage also gives rise to pitfalls in judicial scrutiny—not only in admissibility criteria, but also in the extent of its relevance to the fact. These issues exemplify what we call superficial scrutiny. In this section, we begin by introducing the technical characteristics of blockchain evidence, and then identify common misconceptions in its judicial application.

### 2.1 The generation principle

In an increasingly digital world, blockchain technology constrains user behavior through its traceability and tamper-resistance, ensuring that each participant operates strictly in accordance with



predefined system rules. It is highly unlikely for a user to circumvent these rules to engage in fraud or malicious manipulation. Therefore, blockchain evidence is often described as self-authenticating, meaning it requires no extrinsic evidence of authenticity in order to be admitted. To ensure this self-authenticating property, three layers of technical safeguards are in place.

First, blockchain is essentially a database, with “distributed storage” as its core distinguishing feature from traditional centralized databases.<sup>20</sup> As long as someone can set up a computer to act as a node in the network, they can become part of the blockchain system<sup>21</sup>. Once the computer becomes a node, it enjoys the same rights and obligations as all other nodes, including reading data and writing data. This multi-node form enables multiple backups and joint maintenance of the database, with all nodes supervising the transactions recorded therein.

Second, based on distributed storage, blockchain introduces a “consensus mechanism” that allows all nodes in the system to agree on a specific version of the database. This mechanism ensures that all participating nodes reach a common understanding of the validity of transactions on blocks. In most cases, a certain percentage (e.g., 50%, 60%, or even higher) of nodes must verify and approve a block before it is officially added to the blockchain. This mechanism ensures data consistency and integrity by synchronizing information across all nodes.

Finally, the blockchain system is manifested as a “block-chain” structure—data is stored in discrete blocks, arranged chronologically via timestamps, and linked together to form a closed-loop chain. During the process of adding or modifying a block to a blockchain, cryptographic technology is used to add timestamps to this operation, which are then protected by digital signatures. A timestamp proves

---

<sup>20</sup> Centralized operation refers to a system in which management and decision-making authority are concentrated in a single core or central point.

<sup>21</sup> “Node” refers to an active point in a network, which can be either a physical computer device or a virtual entity.

that a transaction existed at a specific point in time, effectively addressing the uncertainty timing of evidence collection in legal practice. Since judicial proof is essentially the reconstruction of facts, the ability to preserve temporal information through timestamps aligns well with the demands of litigation. It enables high-fidelity preservation of information and supports accurate reconstruction of case facts, thereby enhancing the credibility of evidence.

## 2.2 Pitfalls in the admissibility of blockchain evidence

Although blockchain evidence possesses aforementioned advantages, it should not be regarded as infallible or exempt from evidentiary scrutiny. However, courts may, due to an overreliance on its perceived strengths, fall into certain pitfalls in determining its admissibility.

### 2.2.1 Overlooking evidence-type differences in authentication

Blockchain evidence should not be simply understood as “evidence that uses blockchain technology”. In a strict sense, blockchain evidence is not an independent form of evidence. Instead, it is a technical method for evidence storage, transmission, and fixation. It represents a blockchainized form of the existing statutory evidence formats. These blockchainized evidence can be further categorized into two types based on their generation method: native evidence generated on-chain and derived evidence generated off-chain.<sup>22</sup>

Native evidence generated on-chain primarily refer to blockchains that were originally set up to store transaction records. Examples include the distributed ledgers of cryptocurrencies like Bitcoin and Ethereum, who introduce anti-tampering measures at the point of data creation, ensuring the utmost authenticity of the data. Derived evidence is generated off-chain, referring to storing existing evidence

---

<sup>22</sup> Zelin Su, *Evidentiary Value and Evidentiary Status of Blockchain Evidence*, 29 Int’l J. Evid. & Proof 58 (2024).

or its hash value on a blockchain platform, which not only includes digital evidence but also the digital forms of other evidence types such as “physical evidence, documentary evidence, statements of victims, testimonies, and expert opinions.”<sup>23</sup> Essentially, the blockchain technology applied to this kind of evidence serves as a method for evidence preservation.

Depending on the type of evidence carrier, authentication generally has two distinct meanings: first, to prove that the evidence presented in court is consistent with what the presenting party claims it to be, and that the physical medium has not been forged or tampered with; second, to prove that the content of the evidence—such as text, charts, audio, or images—accurately reflects the actual facts of the case. For derivative evidence generated off-chain, priority should be given to the first type of authentication—verifying that the evidence presented in court matches what is claimed, originates from a reliable source, was collected through proper procedures, and has been securely stored. For native on-chain evidence, emphasis should be placed on the second type of authentication, which requires ensuring that the recorded audio, images, charts, and other content accurately reflect the facts of the case.

When evaluating blockchain evidence, especially derivative evidence generated off-chain, judges sometimes overlook the fact that blockchain can only ensure “on-chain authenticity.” This is closely related to the manner in which the evidence is submitted. If the blockchain evidence is submitted in the form of “raw data” (such as webpage screenshots or platform records), judges are usually more aware that they must first evaluate that “the evidence was not tampered with before being uploaded to the blockchain”. However, if the blockchain evidence is submitted in the form of a notarial certificate

---

<sup>23</sup> Ma Dehuan, Quankuailian Zhengju Zhenshixing de Shencha Rending [On the Judicial Review of Blockchain Evidence Authenticity], Shangquan Xingshi Bianhu Forum Lunwenji [Shangquan Criminal Defense Forum Proceedings], 2022, at 10–18.

or an expert opinion, the judge’s attention may shift to the legal effect of these “auxiliary forms”, while neglecting to examine whether the original data was free from fabrication before being uploaded.

### 2.2.2 Overlooking risks undermining evidence integrity

According to Federal Rules of Evidence Rule 106, *If a party introduces all or part of a statement, an adverse party may require the introduction, at that time, of any other part—or any other statement—that in fairness ought to be considered at the same time.* This rule is grounded in the concern that taking information out of context may create a misleading impression.

By the same logic, blockchain evidence—even native evidence generated on-chain—faces similar risks. On the one hand, part of the data may be intentionally omitted: the presenting party might submit only those portions of the blockchain record that are favorable to its position. On the other hand, multiple versions aiming to the same fact may be uploaded in advance: the presenting party may have recorded a series of evolving electronic records on the blockchain regarding a particular fact (for example, by pre-uploading several contracts containing inconsistent liquidated damages clauses), and upon the emergence of a dispute, selectively submitted the version most favorable to its claim—reflecting an original malicious intent of multi-version reservation.

### 2.2.3 Outsourced verification dilutes judicial responsibility

As previously mentioned, descriptive statistics on cases involving blockchain evidence show that the vast majority of such evidence was admitted. Among the few cases in which blockchain evidence was not admitted, the typical reason for non-admission is the “potential risk of tampering”, cited in two example cases. Rejecting a claim on the grounds that blockchain “may” have been tampered with requires considerable effort and even courage. These two cases are: a copyright ownership dispute

heard in 2019 by the Beijing Internet Court (hereinafter “Case 1”),<sup>24</sup> and a dispute over the right of communication to the public heard in 2022 by the Intermediate People’s Court of Xinyu City, Jiangxi Province (hereinafter “Case 2”).<sup>25</sup>

These two cases share two common features. First, the plaintiffs in both cases submitted blockchain evidence to prove the defendants’ infringing acts. In each case, the plaintiff had lawfully obtained authorization for the work in question and file a suit because the defendant’s work infringed their intellectual property rights. Second, the defendants’ raised explicit objections in both cases: they argued that the blockchain evidence had not been notarized, and the collection process had not strictly followed the *Operational Guidelines*<sup>26</sup> to complete self-checks on cleanliness, security, and the authenticity, so the possibility of setting up a virtual proxy website could not be ruled out.

To address the defendants’ objections, the judges in two cases adopted different but similar approaches—outsourced verification—to examine the blockchain evidence. In Case 1, the court appointed a technical investigator (similar to an expert assistant but without legal status) to participate in the trial and provide an expert opinion. Referring to the *Operational Guidelines*, the investigator found that three key steps were missed in the preliminary check of the evidence-collection video. The judge ultimately held that the absence of these key steps rendered the blockchain evidence substantially defective and insufficient to be admitted. In Case 2, the judge sent an inquiry letter to the blockchain platform, which replied that the evidence submitted by the plaintiff did not comply with their

---

<sup>24</sup> See judgment (2019) Jing 0491 Min Chu No. 1212. Here, “(2019)” represents the year of the judgment; “Jing” represents the province or province-level municipality where the court is located; “0491” is the court code identifying a specific court within that jurisdiction (typically at the district level); “Min” represents that the case is civil (as opposed to criminal or administrative); “Chu” represents that this is the first trial; and “No. 1212” is the unique case number assigned by the court. In the Chinese legal system, these elements together constitute a unique identifier for a judgment. The citation format for the judgments below follows this structure.

<sup>25</sup> See judgment (2022) Gan 05 Min Chu No. 15

<sup>26</sup> Here, the “Operational Guidelines” refers specifically to the usage guidelines issued for the Trusted Timestamp Blockchain Evidence Preservation Platform.

*Operational Guidelines.* The judge concluded that, because the plaintiff had connected both a data cable and Wi-Fi network during the evidence reserving process—contrary to the operational requirements—there was a possibility that the data could have been replaced through data cable or Wi-Fi hijacking. Accordingly, the evidence submitted by the plaintiff was not admitted.

To summarize, most blockchain evidence is admitted by courts (as noted above), and in the relatively few instances where it is not, the adverse party has raised detailed objections during cross-examination, and the judge, in addressing those objections, relies on outsourced verification. This gives rise to a concern: if the adverse party had not objected, or if the judge's expertise and judicial resources were insufficient to identify technical flaws in the blockchain evidence, might unreliable evidence have been admitted without substantive scrutiny?

If this concern proves valid, the worst impact on the judiciary would be that judges may not have the time and energy to conduct detailed scrutiny in every case, especially during current period of litigation explosion, and thereby increasing the risk of erroneous judgments. In the past, electronic evidence commonly required notarization or forensic examination before being admitted. When blockchain evidence first emerged, it was widely believed that its reliability could be ensured without those procedures, making it a reliable tool for improving litigation efficiency. As things stand, the advantages of blockchain evidence have yet to materialize, and courts still end up relying on outsourced verification.

### 2.3 Dilemmas in proving facts with blockchain evidence

In addition to admissibility, proving facts with blockchain evidence also requires an assessment of its probative value—the extent to which the evidence supports a fact that is relevant to the case. In Chinese

judicial practice, both determinations—admissibility and probative value—are made by the same judge, who is responsible for giving the reasons in the judgment. Therefore, the concept of superficial scrutiny, as discussed in this paper, encompasses both aspects. Given the aforementioned pitfalls in the admissibility stage, corresponding difficulties also arise in the subsequent assessment of probative value.

### 2.3.1 Discussions of evidence attributes displace factual reasoning

In current judicial practice, judges may “substitute discussions of evidence attributes for reasoning about the facts” in the fact-finding process—a tendency that is particularly pronounced in blockchain evidence. To understand this, it is necessary to clarify the distinction between “evidence attributes” and “factual reasoning.”

Evidence attributes constitute the theoretical foundation for constructing evidentiary rules, and only evidence possessing certain attributes may be admitted into judicial proceedings. Thus, evidence attributes not only guide the processes of collection, but also define the basic boundaries of admissibility.<sup>27</sup> In the common law system, relevance serves as the minimum threshold, while reliability functions as a further filter for assessing evidence. More importantly, within the common law litigation, the determination of admissibility is made by the judge, whereas the reasoning process “from evidence to fact” is typically entrusted to the jury.

Compared to that, in China’s evidentiary system, the “three attributes of evidence” — authenticity, legality, and relevance — serve as standards for evaluating evidence prior to fact-finding, and in

---

<sup>27</sup> Zhang Baosheng & Chang Lin, *Zhongguo Zhengju Fazhi Fazhan de Guiji: 1978-2014* [The Trajectory of the Development of Evidence Rule of Law in China: 1978–2014], China University of Political Science and Law Press, 2016, at 282.

essence represent a hybrid adoption of the admissibility and probative value. Authenticity emphasizes the consistency between the evidence and objective facts; legality focuses on the compliance of evidence collection with procedural rules; and relevance is used to assess the degree of connection between the evidence and the fact to be proven in the case.

Unlike in the common law tradition—where relevance is merely a prerequisite for admissibility—China’s conception of “relevance” often carries an element of reasoning. In a judgement, the argument regarding relevance not only encompasses the basic relevance between evidence and fact, but also implicitly includes the reasoning logic of whether the evidence can prove the fact, thereby blurring the line between relevance and probative value.

There are consequences assigning the responsibility of verifying probative value and admissibility to a single judge. As Terence Anderson has pointed out, “The probative force of evidence depends on every link in the chain of reasoning”.<sup>28</sup> In common law litigation, the jury takes the responsibility for evaluating probative value. However, in Chinese practice, this chain of reasoning is often artificially absorbed into admissibility or even bypassed: In the absence of a structural division between fact-finding and the admissibility, Chinese judges are required to independently perform both tasks. This is particularly true when dealing with evidence types that carry strong “technological endorsements,” such as blockchain evidence.

In such cases, courts are prone to equating formal demonstrations of “legality” or “authenticity” with the actual establishment of case facts. In other words, judges often substitute “the authenticity of the timestamp” or that “the hash value has not been tampered with”—for substantive reasoning about

---

<sup>28</sup> Terence Anderson, David Schum & William Twining, *Analysis of Evidence* (2d ed., trans. Baosheng Zhang, China Renmin Univ. Press 2012), at 84.



whether the evidence truly reflects the facts of the case (e.g., whether a particular act of infringement occurred). The boundary between authentication and proof becomes blurred, leading to judgments that lack substantive rationality. This phenomenon represents one of the key issues of judicial misalignment in reasoning that this paper seeks to address.

### 2.3.2 Overestimating the probative scope of blockchain evidence

All types of evidence—including electronic, documentary, and testimonial evidence—have specific probative purposes, that is, they are used to prove particular facts. Take electronic evidence as an example: transaction records can be used to prove an online transaction, the identities of the parties involved, or the specific terms and conditions of the transaction. Communication records such as emails, text messages, and social media messages can prove the content and timing of communications. Internet browsing history and location data can prove a person’s behavior patterns or whereabouts at a specific time. Similarly, the purpose of opinion evidence is to provide expert knowledge or inferring technical issues in a case.

It is common in court hearings to hear statements such as: “The plaintiff has submitted five pieces of evidence, each intended to prove a specific fact in dispute.” This process essentially marks the process from evidence to an element. An element proven by a single piece of evidence focuses on a specific aspect and is usually narrower in scope—such as the time, location, manner, or motive of the alleged offense.

The authenticity guaranteed by blockchain evidence applies only at the carrier level. In this sense, there are certain fixed conclusions about what facts blockchain evidence can prove, and such facts are significantly limited. Tamper-proofing of on-chain data carries different implications depending on

the type of case. In tort cases, the data often reflects the process of the infringing act—i.e., who published which work at what time—thus infringing on the rights to that work. As long as the infringing work ever existed on-chain, the fact to be proven is established. In contract disputes, however, the on-chain data may only reflect a certain version of the contract, whether that contract is the one claimed by the plaintiff remains uncertain. As discussed above, it may have been altered before being uploaded, or multiple versions of the contract may have been uploaded to the blockchain. Therefore, in this context, a single piece of blockchain evidence can only prove the existence of “a certain version” of a document, rather than confirm which version shows the disputed clause.

### 2.3.3 Weak reasoning undermines the evidentiary chain

A lack of judicial reasoning does not necessarily lead to an erroneous judgment, but significantly increases the risk. In cases involving blockchain evidence, the most serious problem caused by insufficient reasoning is incomplete evidentiary chain.

For example, in a loan agreement dispute<sup>29</sup>, the plaintiff uploaded the loan agreement signed with the defendant to *Baoquan.com* (a blockchain platform), thereby forming blockchain evidence to be submitted to the court. The defendant was absent from the trial and did not raise any objections. In the end, the judge held: “Based on the evidence presented at trial, the *WeChat* records, *WeChat* transfer e-vouchers, screen recordings of the chat, and the video records and blockchain preservation certificate from *Baoquan.com* submitted by the plaintiff are of lawful origin and have clear content, therefore admits them as evidence.” However, based solely on the information in the judgment, there are significant doubts in this case. First, both the plaintiff and defendant are natural persons, without

---

<sup>29</sup> See judgment No. (2023) Xiang 0281 Min Chu 1840

having used any automated technical means to submit the evidence. The loan contract signed between them was uploaded to a blockchain platform, making the resulting blockchain evidence a typical example of derivative, off-chain generated evidence, the authenticity of which prior to being uploaded is questionable. Second, the defendant did not appear in court, raised no objections to the blockchain evidence, and did not acknowledge its authenticity. In this context, the blockchain evidence did not in substance enhance the probative value of the loan contract, and its authenticity remains unverifiable. While the judge may reasonably form a decision based on the overall hearing and corroboration with other evidence to support the plaintiff's claims, the lack of these reasoning in the written judgment remains a key factor contributing to the risk of error in similar cases.

### 3. Model selection

As discussed above, while blockchain evidence possesses considerable advantages, pitfalls at both the admissibility and probative value stages often lead to deficient reasoning in judgments. Depending on whether the concerns that lead to pitfalls are properly addressed, there are two distinct pathways of scrutiny—substantive and superficial. In this section, we will examine the psychological underpinnings of this phenomenon, and building on this, develop our theoretical model.

#### 3.1 Theoretical basis

Distinguishing between “substantive” and “superficial” scrutiny is a subjective judgment, which is challenging to identify solely through data. *Persuasion theory*, first proposed by Yale University scholar Carl Hovland, is among the most extensively studied topics in cognitive psychology. With its two pathways, it may precisely explain the differences between what can be considered scrutiny of

“substantive” and “non-substantive”.<sup>30</sup> According to this theory, the two pathways can be described as follows: a logic-driven central pathway and a clues-relying peripheral pathway. By influencing specific factors, it is possible to enhance the persuadee’s cognitive motivations and ability, thereby guiding the original path toward logical processing. To identify these “specific factors” would be the first step towards developing effective approach to enhancing cognitive ability.

In a general sense, judges’ decision-making is a type of cognitive behavior and follows common principles of cognitive psychology. Although the law mandates strict scrutiny of evidence and highlights the risks of wrongful convictions, judicial discretion still results in individual variations. This variability likely leads judges to take different approaches in their decision-making processes. For cases involving new types of evidence such as blockchain, the key in court debate is to “persuade” the judge to believe that “although the evidence is innovative in form, its ‘reliability’ is sufficient to prove the facts,” thereby providing persuasive basis for the judge to admit the evidence.

When this theory is applied to the scrutiny process, sufficient adversarial debate enhances cognitive motivation, thereby increasing the likelihood of a judge engaging in a “detailed, high-quality, logic-driven” substantive path; when cognitive motivation is low, the judge is more likely to follow a superficial path that relies on external factors in deciding whether to admit the evidence. Except for the prior knowledge, which is established before the evidence scrutiny and remains largely unchanged, other factors influencing cognitive ability may vary throughout the scrutiny process. For example, factors such as whether the case is heard by a collegial panel, whether the blockchain evidence has undergone detailed cross-examination, whether the evidence-preserving institution is clearly identified

---

<sup>30</sup> George M. Belknap, *Review of Communication and Persuasion: Psychological Studies of Opinion Change*, by Carl I. Hovland, Irving L. Janis & Harold H. Kelley, 48 Am. Pol. Sci. Rev. 600 (1954).

during the trial, and whether the evidence involves notarization or digital forensic examination may all enhance the judge's cognitive ability. These factors may incline the judge to adopt a logic-driven route in evaluating the blockchain evidence; otherwise, the judge is more likely to rely on other information in making the decision.

In view of this, the following discussion refers to substantive scrutiny as the logic-driven path and superficial scrutiny as the externally driven path. Based on these two paths, we assume that factors which, under common sense, can enhance cognitive motivation or cognitive ability are considered to have a positive impact on the logic-driven path.

### 3.2 Theoretical model

Following from the discussion above, whether a judge would engage in substantive scrutiny of blockchain evidence depends on whether the judge has sufficiently high cognitive motivation. The next question, naturally, is what factors affects the cognitive motivation, and to what extent such factors achieve high enough cognitive motivation that eventually leads to substantive scrutiny. To answer these questions, we model evidence scrutiny problem as a discrete choice problem of judges. Specifically, when facing blockchain evidence to be scrutinized, a judge chooses from the two alternatives: substantive scrutiny (alternative 1 below) and superficial scrutiny (alternative 0 below). If we use  $\gamma$  to denote the judge's choice,  $\gamma=1$  means the judge chooses substantive scrutiny, while  $\gamma=0$  means the judge chooses superficial scrutiny. From economics perspective, each alternative offers the judge a different utility, which depends on the rewards and costs associated with the alternative. Rewards can include monetary awards, brighter career perspectives, and better reputations among peers for making correct decisions regarding evidence, while costs can include effort costs when

carefully scrutinizing evidence, or unsettling conscience and risks of making wrong decisions that jeopardize the judge's future when superficially scrutinizing evidence. The judge evaluates the rewards and costs of choosing an alternative, which forms the utility of the alternative, then choose the alternative that provides higher utility. This utility then can be used to consider cognitive motivation. If substantive scrutiny offers higher utility than superficial scrutiny, the judge should be viewed as highly cognitively motivated and will engage in substantive scrutiny. Conversely, the judge will not be sufficiently motivated and succumb to superficial scrutiny if the utility from superficial scrutiny is higher.

Alternatively, it might be helpful to consider the judge as a firm when facing scrutiny decisions. The scrutiny decision of blockchain evidence is a risky project that is associated with potential rewards (or losses). The judge must decide how much to invest in this project, and the investment is done by paying efforts. A larger investment leads to substantive scrutiny, which increases the potentiality of better rewards but also triggers a higher cost of effort. A lower investment leads to superficial scrutiny, which reduces the potentiality of rewards, increases the potentiality of losses, with a lower cost of effort.<sup>31</sup>

The rewards and costs of a scrutiny path obviously depend on the specific case. A case has many attributes that contribute to the rewards and the costs, which we denote as a vector

$$X=(X_1,X_2,...,X_K).$$

---

<sup>31</sup> In general, one can consider that a judge can choose her/his effort level more than two levels. Still, it should be a reasonable and necessary abstraction to simply the scrutiny into two levels, substantive and superficial. For one thing, the effort levels are not directly observed, and a binary scrutiny path are more easily observed and recognized from legal documents. For another, efforts are (reasonably) assumed to be costly. If a judge would like to shirk, she/he should do the bare minimum to make her/his decision seemingly valid. Even if a judge is hardworking, it is sufficient to spend just enough effort to confirm the validity of the blockchain evidence. Paying some intermediate effort level that is more than necessary for a seemingly valid decision but less than enough for a true verification of the evidence or paying more effort when the evidence is already believed to be valid are not rational.

Here,  $K$  is the number of attributes considered by a judge that are also observed by researchers. Then, we can consider the utility of alternative  $j$ , denoted by  $U_j$ ,  $j=0,1$ , as a function of these attributes. Following the tradition of discrete choice modelling, we assume that the utility function takes the following form

$$U_j(X,V)=X\beta_j+V,$$

where  $\beta_j=(\beta_{j1},\beta_{j2},\dots,\beta_{jK})$  measures how each attribute affects the utility of choosing alternative  $j$ , and  $V$  contains the attributes considered by the judge but not observed by the researchers. From the researchers' perspective,  $V$  is a random variable.

The judge chooses substantive scrutiny if

$$U_1(X,V)\geq U_0(X,V).$$

Since only the order of the utility matters, it is conventional to normalize  $U_0(X,V)=0$  and consider  $U_1(X,V)$  only. For this reason, we can also omit the subscript of  $\beta$ . The conditional probability of a judge choosing substantive scrutiny, conditioned on the observed attributes, is then

$$P(Y=1|X)=P[U_1(X,V)\geq 0|X]=P(V>-X\beta|X).$$

This is a probability that can be observed from the data. In the population level, this means we can first select the observations that shares the same observed attributes, then observe in how many observations the judge took substantive scrutiny. Then, for a given distribution of the unobserved attributes, we can use the observed probability and the attributes to identify the effects of the attributes,  $\beta$ .

In the remaining part of this section, we will introduce the attributes  $x$  that are of interest of this paper and potentially significantly affect the scrutiny choices of judges when facing blockchain evidence by affecting the rewards and the costs of scrutiny. These attributes include: (i) Whether the case has undergone notarization, digital forensic examination, or verification through inquiries from professional institutions (in some cases, referred to as “outsourced verifications” for simplicity); (ii) Whether specific objections on blockchain evidence were raised (in some cases, referred to as “explicit objections” for simplicity).

### 3.2.1 Outsourced verifications

We now consider the second attribute, whether notarization, forensic examination, or third-party verification occurred for blockchain evidence.

In judicial practice, the submission of blockchain evidence is most often accompanied by a notarized certificate issued by an evidence preservation institution. However, the information presented in such a certificate can only provide a brief record, without fully presenting the scientific theory and collection process involved. Therefore, as the application of blockchain evidence evolves, it has become increasingly common in practice to supplement it with notarization or digital forensic examination, and then submit it to the court in the form of opinion evidence. It is generally believed that, compared to merely submitting a blockchain certificate, when a case involves notarization, digital forensic examination, or verification by professional institutions, the resulting evidence tends to be viewed as more reliable and authoritative because such evidence is issued by officially recognized and specialized entities.



In China, notarization is typically carried out by officially recognized notary offices under the supervision of the Ministry of Justice. These offices are authorized to issue evidence preservation certificates, often through designated platforms, that document the existence, content, and timestamp of specific digital materials such as web pages, videos, or screenshots. While such notarizations are presumed to be reliable and are often exempted from further challenge in court, the underlying technical process is usually opaque to the judges and parties, as it merely confirms what was preserved rather than how the blockchain mechanisms work or how the digital evidence was originally created. Also, the personnel responsible for the opinion evidence is usually not available in person in court.

Forensic examinations performed by judicial appraisal institutions or professional firms with expertise in digital forensics. These institutions may extract metadata, verify hash values, and analyze digital signatures, typically issuing expert opinions in the form of forensic reports. Unlike in the U.S., where expert testimony is subject to adversarial cross-examination and stricter evidentiary standards (e.g., Daubert standard), Chinese practice places substantial weight on such institutional opinions, especially when issued by entities listed in the Ministry of Justice's official registry. However, the judge's reliance on these opinions often occurs in a non-adversarial setting, which may obscure the boundary between independent judicial scrutiny and deference to external expertise.

Third-party verifications mentioned above can elevate the utility of the substantive scrutiny by lowering the effort costs. In particular, such third parties usually are more professional and technologically knowledgeable than the judges from non-Internet-specialized courts and in general provide verification reports that contains necessary details of the blockchain evidence that can be time- and energy-consuming for the judges to acquire themselves. The reports from outsourced verifications often already include enough reliable and well-organized information for the judge to engage in

evidence scrutiny. In the case that the opinion evidence is not sufficiently clear, it is also an option for the judge to require following-up information of the evidence from the third parties if needed. Therefore, while the third parties may not directly increase the reward of substantive scrutiny, the lowering cost of scrutiny also increases the utility of substantive scrutiny.

However, third-party verifications can also have negative effects and increase the utility of superficial scrutiny. A judge may consider the research by the third party substitutable to her/his own scrutiny, so that reducing the scrutiny effort is then not easily perceived, and in turn, the judge may then believe that her/his reputation will not be jeopardized even with superficial scrutiny. Moreover, the verifications of the blockchain evidence are conducted by third parties that are not directly related to the judge. On the one hand, if the judge uses substantive scrutiny and disagrees with the third party, the judge needs to pay significant extra effort to dismiss the blockchain evidence and the opinion evidence from the third party. This can be expensive for the judge: not only the judge needs to understand the mechanism of blockchain evidence, which is relatively innovative and has certain technology barrier, but she/he must accept the risk of making a mistake. On the other hand, if the judge makes an incorrect decision by easily adopting the verification results of the third parties, the consequences of the wrong decision can be bear or at least shared by the third-party verification institutions, which lowers the cost of superficial scrutiny.

### 3.2.2 Explicit objections

Cross-examination is a crucial step in courtroom proceedings, which ensures the fairness and transparency of judicial fact-finding. Both parties may comment on each other's evidence, raise objections, or offer counter evidence. Although the Chinese litigation system is not adversarial in a

strict common-law sense, objections from the parties still serve as important cues for the judge's evaluation of evidence.

Clear and well-articulated objections can enhance judicial engagement with blockchain evidence in several ways.<sup>32</sup> On the one hand, under the principle of self-admission, if the opposing party explicitly acknowledges the admissibility of the evidence without raising substantive challenges, such evidence is often presumed to meet the standard of authenticity, legitimacy, and relevance, thereby relieving the judge from conducting further scrutiny. On the other hand, objections help the judge identify weaknesses or irregularities in the evidence, especially when technical issues such as hash consistency, time stamping, or the traceability of on-chain data are involved. For blockchain evidence, which inherently contains technical complexity, targeted objections—such as questioning whether the hash value in court matches the one on the blockchain, or whether the platform used is sufficiently credible—can signal where deeper examination is warranted. Moreover, high-quality objections can stimulate more rigorous courtroom debate, prompting the judge to consider multiple interpretive frames and to reflect more critically on the sufficiency and probative value of the evidence. For instance, an objection questioning whether the notarization process fully captured the state of the digital content prior to blockchain submission can force the court to confront the issue of pre-chain authenticity, which is often overlooked. From the reward and cost perspective, a clear objection lowers the cost of substantive scrutiny by outlining the necessary examinations needed. It also increases the cost of superficial scrutiny: without carefully addressing the concerns in the objection, the party raises the objection has a higher probability to appeal.

---

<sup>32</sup> Latour Lafferty, *Trial Objections: The Way of Advocacy*, 11 Suffolk J. Trial & App. Advoc. 1 (2006).

Such clarity, however, may not always be beneficial. Instead, it can create unintended judicial reliance. Faced with complex technical evidence and time constraints, judges may be inclined to adopt the language and framing offered by the objections, directly incorporating them into the reasoning section of the judgment. This phenomenon has been observed in various rulings where the judge's analysis mirrors the objection language nearly verbatim. Over time, this may contribute to judicial inertia, whereby the objection substitutes for independent scrutiny. Instead of evaluating the probative chain and epistemic reliability of the evidence, the court may rely on the existence—or absence—of objection as a proxy for evidentiary assessment, blurring the line between procedural formality and substantive reasoning. From the reward and cost perspective, this means the cost of superficial scrutiny is lower: a judge can use the objection and better disguise the superficial scrutiny as a substantive one, lowering the risk of being spotted.

### 3.2.3 Other attributes

Apart from the two major attributes discussed above, there are a few other attributes that need to be considered and controlled. These include not only judge-specific characteristics but also case-specific attributes, as the effort required for evidence scrutiny may vary from case to case. Controlling these attributes helps us better measure the effects of outsourced verifications and explicit objections.

First, regarding judge-specific characteristics, two judges can choose different scrutiny paths when facing the same case. One judge may be more risk-averse and psychologically exacerbate the perceived risk of making a wrong decision, leading to substantive scrutiny, while the other judge may suffer from poor health conditions and regard substantive scrutiny as too costly. Some judges may also face greater

peer pressure than others, or is more knowledgeable or a fast learner regarding blockchain evidence.

To partially capture these factors, we control for:

(1) Whether the trial court is an Internet-specialized court, reflecting the educational background and learning ability of the judge.

(2) Whether the case is adjudicated by a collegiate bench (panel), reflecting the level of peer pressure faced by the judge.

(3) Local disposable income per capita, as a proxy for the average level of risk aversion in the judge's region.<sup>33</sup>

Of course, there are not all judge-related attributes that can affect the utilities of two evidence scrutiny path. Other attributes are omitted as they are likely to be secondary to the attributes that shown above, and due to data availability. Still, it should be recognized as a limitation of this research that more judge-specific attributes are not included in the model.<sup>34</sup>

Second, case-specific attributes are also controlled, as the level of scrutiny may depend on the complexity, stakes, or procedural context of a case. Such factors include:

(1) Whether the party submitting the blockchain evidence is a legal person or a natural person, to account for differences in litigation resources and evidentiary strategies.

(2) Whether the judgment was issued before or after August 2021, to capture the potential regulatory impact of the Online Litigation Rules issued by the Supreme People's Court.

---

<sup>33</sup> This is based on the empirical observation that people's risk attitudes often depend on their income levels. For a summary, see Chapter 21 of Handbook of the Economics of Finance by Guiso and Sodini, 2013.

<sup>34</sup> This is partially mitigated by the relatively large size of the sample.

(3) Whether the cause of action is a contract dispute or a tort dispute, to control for differences in the typical evidentiary structure across case types.

(4) The amount in controversy, to reflect the potential stakes involved and their influence on the level of scrutiny applied.

Missing variables in terms of case-specific attributes is less a concern since case attributes, as long as it is meaningful, should be clearly included in the judgement.

#### 4. The Empirical Analysis of Blockchain Evidence Scrutiny

This section builds on the theoretical model from the last section and empirically analyze the effect of outsourced verifications and explicit objections on blockchain evidence scrutiny using logistic regressions. We will start by briefly introducing the logistic regression model, before discussing the data and presenting the empirical results.

##### 4.1 The empirical model

A common statistical model used for discrete choice model is logistic regression. Recall that the object of interest is  $P(V > -X\beta | X)$ , the probability of substantive scrutiny given the observed case attributes. To calculate this with logistic regression, we assume that  $V$  is independent and identically distributed, with the Type-I extreme value distribution. This allows us to write

$$P(Y=1|X) = P(V > -X\beta | X) = \frac{\exp(X\beta)}{1 + \exp(X\beta)}.$$

One reason of employing the logistic regression is its ease of interpretation. It is easy to see from above that

$$\ln \left( \frac{P(Y=1|X)}{P(Y=0|X)} \right) = \ln(\exp(X\beta)) = X\beta,$$

so that  $\theta_j$  is the partial effect of attribute  $j$  regarding the log-likelihood ratio. That is, fixing all other attributes,  $\theta_j$  measures how much the log-likelihood ratio changes when attribute  $j$  changes by 1 unit. Very loosely speaking, a positive  $\theta_j$  means that a larger attribute  $j$  implies the probability of substantive scrutiny is also larger.

The regression model is summarized in Figure 1.

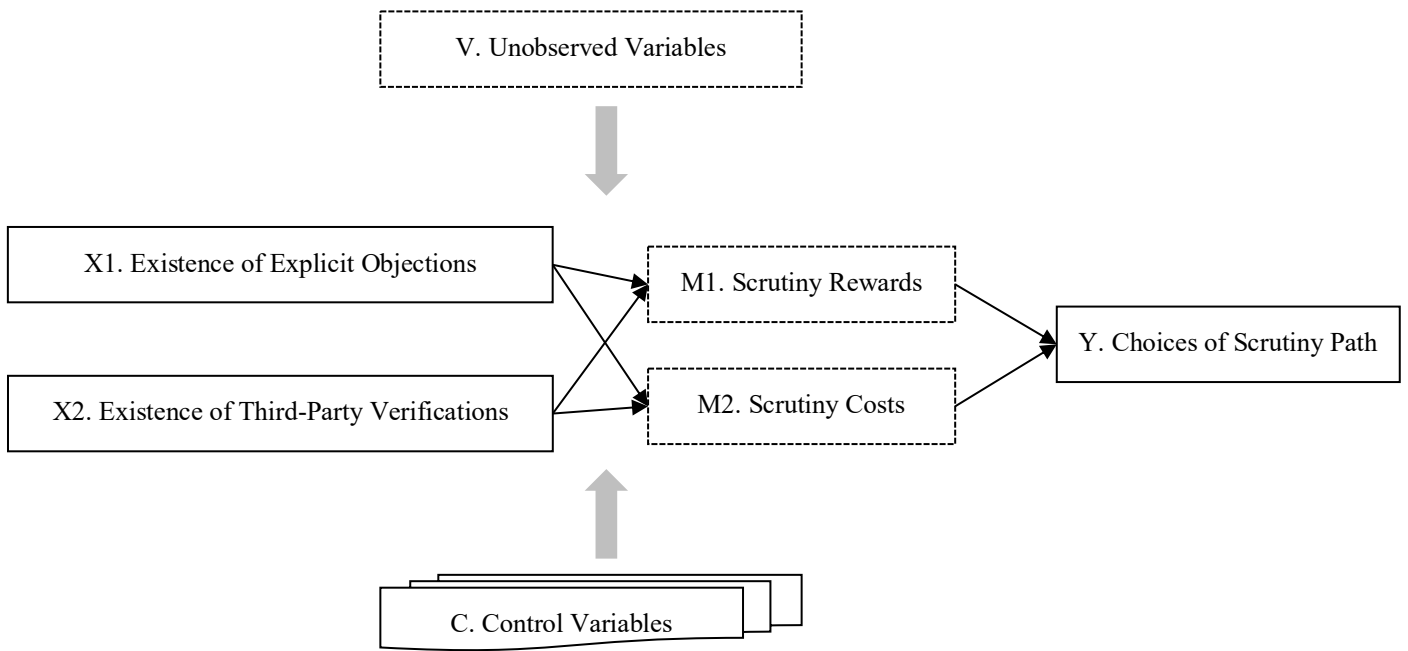


Figure 1. The Statistical Model

We next discuss the reasonability of the regression model. First, we have assumed that in the theoretical model that the choice of the scrutiny path, either substantive or superficial, is based on the trade-offs between scrutiny rewards and costs. The explanatory variables, i.e., X1 and X2 in Figure 1, directly affect intermediate variables M1 and M2, i.e., rewards and costs, and indirectly affect the choices of scrutiny path through the intermediate variables. If we can observe rewards and costs, a better estimation strategy is to estimate the complete causal chain – how M’s affect Y, and how X’s affect

M's. However, this is mostly impossible since M1 and M2 are not observed or easily measured from the observables. In particular, judges consider relevant factors of rewards and costs and synthesize these factors to form reward and cost estimations internally. The decision-making process is psychological and by experience rather than formal. This being said, we believe that regressing Y on X's here is still a valid estimation strategy for the following reasons. Under our theoretical model, the intermediate variables, rewards and costs, are rather general concepts and determine the choices of scrutiny path. The generality of the intermediate variables suggests that all factors affecting the choices of scrutiny path can be summarized as rewards and costs, including the factors that are not observed. In other words, although M's are not observed, U is not a confounding variable since U does not affect Y directly (bypassing M's).

Second, the estimations can still contain spurious associations if U are correlated with X's. This is indeed a valid concern since the unobserved attributes of a case can reasonably related to the observed attributes. To solve this issue, we have included multiple control variables discussed in the last section so that the unobserved variables, conditioned on X's and C, can be considered independent.

## 4.2 Data

One particular challenge is that lawsuit documents of a case is often confidential, meaning that researchers often can only observe limited information from publicly available resources, or mostly, judgements. In this section, we discuss how we extract useful information and define variables using the texts of judgements.

### 4.2.1 Independent variables

We first introduce how treatment variables are defined, which include “outsourced verifications” and



“explicit objections”. For simplicity and clarity of the discussions, the definitions of the seven control variables are placed in the appendix.

Variable 1: Whether the case has undergone notarization, digital forensic examination, or verification through inquiries from professional institutions (outsourced verifications)

This variable was extracted through manual review of judgment texts, supplemented by regular expression-based keyword identification. The focus was placed on sections of judgments describing the form of evidence and its source of collection. Key sections examined include the court’s description of the origin of the evidence and the reasoning for admitting the evidence. The keywords used for identification include, “notarization,” “judicial appraisal,” “appraisal opinion,” “electronic data forensic center,” “technical explanation of electronic evidence,” and “explanation of evidence collection principles.” After initial extraction, key expressions were manually verified to determine whether they were directly related to the blockchain evidence submitted in the corresponding case.

In the sample cases, there is a wide variety of situations involving notarization, digital forensic examination, or verification through inquiries from professional institutions. We offer some examples below.

Common scenarios for notarization of blockchain evidence include cases such as in broadcasting dispute, the plaintiff used the “Notarybao APP” for evidence collection, and the Notary Office of Shaoyang City issued the corresponding “Electronic data storage certificate” for the electronically stored data.<sup>35</sup>

Common scenarios for digital forensic examination of blockchain evidence include cases such as in a

---

<sup>35</sup> See judgment No.(2021) Ji 03 Min Chu 44.

trademark dispute, the plaintiff applied for evidence preservation, and Beiqianmai Forensic Center in Zhejiang completed the evidence preservation in the defendant's business premises. They provided electronic data collection and blockchain certification.<sup>36</sup> Similar forensic institutions include Beijing Network Industry Association Electronic Data Forensic Center,<sup>37</sup> Fujian Zhongzheng Forensic Center,<sup>38</sup> and Shanghai Chenxing Electronic Data Forensic Center,<sup>39</sup> among others.

Common scenarios for verification through inquiries from professional institutions include cases such as in a copyright dispute, the plaintiff submitted a “The explanations of the technology principle of electronic evidence” issued by Truth Network Company, stating that Truth Technology's product services are provided through cloud computing, and all computations, evidence collection processes, and evidence storage are conducted on the Truth Preservation Cloud. Relying on the financial-level security protection of the Truth Preservation Cloud, it undergoes digital forensic examination by the Ministry of Public Security and security equipment forensic expertise to ensure the reliability of the computation and storage processes.

The above situations are all conducive to enhancing the cognitive motivation and cognitive abilities of judges, so similar situations are designated as 1, while others are designated as 0.

Variable 2: Whether the adverse party raise specific objections to blockchain evidence

This variable was extracted by reviewing relevant sections of the judgment, including the cross-examination opinions, deliberation opinions, and court’s reasoning. Sentences that evaluate or comment on the content of the evidence were identified. Keyword filtering and manual comparison

---

<sup>36</sup> See judgment No.(2022) Su 1291 Min Chu 1391.

<sup>37</sup> See judgment No.(2019) Jing 0108 Min Chu 35902.

<sup>38</sup> See judgment No.(2021) Yue 0192 Min Chu 3358.

<sup>39</sup> See judgment No.(2021) Hu 0104 Min Chu 14413.

were used, with keywords such as “objection,” “disagreement,” “challenge,” “not notarized,” “lacks probative value,” “cannot support the claim,” “emulator,” and “lack of objectivity.” Particular attention was paid to determining whether the objection is targeted at the blockchain evidence itself, the technical methods used in its collection, or the facts that the evidence aimed to prove.

In the sample cases, the objections present the following situations: (i) The opposing party is absent; (ii) The opposing party is present but does not express objections; (iii) objections are expressed but are entirely unrelated to blockchain evidence, or even admit the facts to be proven by blockchain evidence directly; (iv) Not specifically challenging blockchain evidence, but the objections deny the truth of the facts intended to be proven by the blockchain evidence; (v) Clear objections regarding blockchain evidence are expressed.

Specifically, a typical scenario for item (iii) is when the opposing party claims that as a small and micro-enterprise, they cannot afford the high compensation demands put forth by the party presenting evidence;<sup>40</sup> A typical scenario for item (iv) is when the opposing party asserts that they did not commit any tort acts,<sup>41</sup> and there is no lending relationship between the opposing party and the party presenting evidence.<sup>42</sup>

A typical scenario for item (v) is when the opposing party believes that the entire evidence collection process was not notarized, and this lack of notarization cannot guarantee the objectivity and neutrality of the evidence collection process and its results. Additionally, the emulator software used during the evidence collection process is not the actual mobile device itself, which raises the possibility of cheating. It cannot ensure that the data obtained through this emulator is representative of the data of

---

<sup>40</sup> See judgment No.(2020) Zhe 0106 Min Chu 4289.

<sup>41</sup> See judgment No.(2022) Gan 05 Min Chu 15.

<sup>42</sup> See judgment No.(2020) Liao 0212 Min Chu 2158.

the relevant application.<sup>43</sup>

In light of this, situations represented by items (i), (ii), and (iii) are designated as 0, while situations represented by items (iv) and (v) are designated as 1.

#### 4.2.2 Dependent variable

As discussed earlier, although the admissibility and scrutiny of blockchain evidence can be theoretically considered as a continuous variable, in China's judicial practice, judges often produce binary outcomes that manifest either as a logic-driven central path (substantive scrutiny) or a formalistic peripheral path (superficial scrutiny). Therefore, the dependent variable is binary, with 1 for substantive scrutiny, and 0 for superficial.

The specific measurement of whether blockchain evidence has undergone substantive scrutiny or merely superficial scrutiny should be based on the previously established criteria. In line with the Chinese evidentiary framework of "authenticity, legality, and relevance," substantive scrutiny in this research is defined as the presence of reasoning that addresses both reliability (covering the authenticity and legality dimensions) and relevance.

First of all, it needs to be clarified that the most typical form of substantive scrutiny involves a three-tier review based on "platform qualifications—reliability of the evidence collection process - integrity of the evidence collection results." For example, in the case of the dispute involving the tort of the online dissemination rights by Chinese Online Digital Publishing Group Co., Ltd., the court successively examined the "qualification of the evidence preservation platform, the reliability of

---

<sup>43</sup> See judgment No.(2018) Jing 0101 Min Chu 4402.

electronic data generation and storage, and the integrity of maintaining electronic data .”<sup>44</sup> However, in many judgments, the judges do not necessarily focus on discussing blockchain evidence extensively, so they may not cover all three aspects in their arguments. Nevertheless, it can still be observed that consideration has been given to the aforementioned scrutiny criteria.

Second, relevance is identified through explicit reasoning linking blockchain evidence to the facts of the case. In this research, relevance is considered present if the judgment, within the same paragraph or adjacent sentences, mentions blockchain-related terms (“blockchain”, “electronic data”, “evidence preservation”) along with expressions indicating evidentiary connection or probative value, such as “relevance,” “probative value,” “corroboration,” “supporting the claim,” “reflecting the facts,” or “basis for finding facts.” Typical expressions include “can corroborate the case facts,” “has probative value and can support the plaintiff’s claim,” or “the preservation material reflects the facts of the case.”

Given this, judgments are coded as 1 (substantive scrutiny) if they provide reasoning that meets both of the following criteria: (i) Reliability: covering all three sub-elements (platform qualification, process reliability, data integrity and anti-tampering); and (ii) Relevance: as defined by the linguistic markers above.

Conversely, 0 (superficial scrutiny) is assigned to judgments that lack substantive reasoning, which includes but is not limited to: (i) no mention of blockchain evidence; (ii) merely citing legal provisions (e.g., the Online Litigation Rules) to affirm the legal validity of blockchain evidence without connecting them to the facts of the case; (iii) only stating that blockchain evidence has been notarized, judicially authenticated, or verified by professional institutions, thereby affirming its validity without

---

<sup>44</sup> See judgment No.(2018) Jing 0101 Min Chu 4624.

further analysis; (iv) concluding that blockchain evidence should be admitted solely because the opposing party raised no objections.

In addition, to ensure that the estimation results are not sensitive to the author-defined dependent variable values, a robustness check is performed under alternative, much loosened definitions of dependent variable values. In this alternative definition,  $Y$  is assigned a value of 0 if the reasoning in the judgment does not mention any discussion concerning blockchain evidence, and 1 for all other cases.

#### 4.3 Descriptive Statistics of variables

A total of 2,741 judicial decisions were initially collected as sample cases. It is observed that there are a few “batch cases”, cases filed by the same plaintiff within very short time periods, presided by the same judge, feature very similar arguments, and reach very similar judgements. To reduce noise and control for repeated patterns resulting from the same litigants and judges, we applied a filtering process to eliminate highly repetitive cases. Specifically, we identified cases with the same plaintiff (or the same defendant) by extracting party information from the judgment documents (e.g., fields such as “Plaintiff: ×××” and “Defendant: ×××”), and identified the presiding judge using fields such as “Presiding Judge” or “Adjudicating Judge.” If multiple cases involved the same plaintiff or defendant and were adjudicated by the same judge, only one case was retained from each such group.

After applying this filtering procedure, 361 unique cases remained. In these 361 cases, a total of 7 categorical independent variables were extracted from the sample data for this research, along with the categorical dependent variable of whether blockchain evidence underwent substantive scrutiny. The number of categories and their respective percentages for these 8 categorical variables are

presented in Table 1.

Table 1: Descriptive statistics for categorical variables

Variable		Frequency	Percentage
X1: Whether the case has undergone notarization, digital forensic examination, or verification through inquiries from professional institutions	Yes	62	17.1%
	No	299	82.8%
X2: Whether there are specific objections on blockchain evidence	Yes	35	9.6%
	No	326	90.3%
C1: Whether the trial court is an “Internet specialized court”	Yes	66	18.2%
	No	295	81.7%
C2: Whether the cause of action is a contract dispute or a tort dispute	Tort	113	31.3%
	Contract	248	68.6%
C3: Whether the presenting party is a legal entity or a natural person	Legal Person	233	64.5%
	Natural Person	128	35.4%
C4: The composition of the judicial panel	Collegiate Bench	163	45.1%
	Single Judge	198	54.8%
C5: Whether the judgment date is before or after August 2021	After	201	55.6%
	Before	160	44.3%
Y: Whether blockchain evidence underwent substantive scrutiny	Y1: Yes	52	14.4%
	Y1: No	309	85.5%
	Y2: Yes	225	62.3%
	Y2: No	136	37.6%

The remaining two control variables, “value of claim” “Per capita disposable income” are continuous variables that can in theory take any positive value (instead of binary 0 and 1). The descriptive statistics for this continuous variable are presented in Table 2.

Table 2: Descriptive statistics for continuous variables

	N	Minimum	Maximum	Mean	Standard Deviation
C6: Value of claim	361	659.300	40000000.000	327232.907	2249804.992
C7: Per capita disposable income	361	23273.000	84834.000	45504.676	16013.251

From the descriptive statistics in Tables 1 and 2, the categorical variables are not extremely imbalanced and shows sufficient variations, meeting the requirements for subsequent regression analysis. As a

usual practice for money-related variables, the natural logarithm of these variables will be used in the following analysis. Also, the ratio distributions reflected by the above variables are generally consistent with the relatively clear situation in China's judicial practice, further validating the effectiveness of the sample data used in this research.

#### 4.4 Results

The results of logistic regression are presented in Table 3.

Table 3: Results of binary logistic regression

Independent Variable	Baseline		Robustness Check	
	B	Exp(B)	B	Exp(B)
X1: Whether the case has undergone notarization, digital forensic examination, or verification	0.989*** (0.358)	2.687	2.932*** (0.618)	18.763
X2: Whether there are specific objections on blockchain evidence	1.300*** (0.417)	3.669	0.995* (0.514)	2.706
C1: Whether the trial court is an "Internet specialized court"	-0.056 (0.506)	0.945	-0.928** (0.377)	0.395
C2: Whether the cause of action is a contract dispute or a tort dispute	0.268 (0.417)	1.308	-0.779** (0.307)	0.459
C3: Whether the presenting party is a legal entity or a natural person	0.927** (0.404)	2.528	-0.013 (0.279)	0.987
C4: The composition of the judicial panel	-0.740* (0.388)	0.477	0.316 (0.294)	1.371
C5: Whether the judgment date is before or after August 2021	-0.567 (0.365)	0.567	0.199 (0.295)	1.22
C6: Value of claim	0.204** (0.101)	1.227	0.133* (0.079)	1.143
C7: Per capita disposable income	-0.566 (0.562)	0.568	-0.294 (0.427)	0.745
Constants	1.379 (5.642)	3.972	2.323 (4.407)	10.209

Standard errors in parentheses

\*  $p < 0.10$ , \*\*  $p < 0.05$ , \*\*\*  $p < 0.01$



We can make the following observations from the results in Table 3. First, outsourced verifications significantly and positively affect the probability of substantive scrutiny. More specifically, the likelihood ratio that judges engage in substantive scrutiny to the judges engage only in superficial scrutiny increases by about 2.687 when outsourced verifications are presented to the court. Second, explicit objections also show a significant positive effect on substantive scrutiny. The quantitative effect is even stronger compared to the outsourced verifications, with an even larger increase in the likelihood ratio when explicit objections are presented.

In the robustness check, the signs of the regression coefficients for the two core independent variables remain consistent with those in the baseline model. This indicates that, under the redefined dependent variable and a more conservative model specification, the influence of the core explanatory variables on the court's choice of scrutiny path remains directionally stable, thereby confirming the robustness of the baseline model.

Specifically, both Variable 1 (whether a third-party verification or response was provided) and Variable 2 (whether explicit objections were raised) exhibit significant positive effects in both models. These results suggest that the presence of third-party verifications and clear objections consistently promote substantive scrutiny. Importantly, this effect remains robust after controlling for seven background factors: the type of court, cause of action, nature of the evidence-submitting party, composition of the adjudicating panel, date of judgment, amount in controversy, and regional per capita disposable income. This underscores the stability and central importance of these two factors in influencing scrutiny outcomes.

These findings are consistent with the logic of the dual-path cognitive model. When facing blockchain

evidence, courts tend to choose between a substantive scrutiny path and a superficial scrutiny path based on whether the evidence is supported by reliable institutional mechanisms or adversarial challenges. Revisiting the theoretical model, we have argued that these two variables can contribute to the probability of substantive scrutiny in either positive or negative way, by contributing both to the costs and rewards of the utility each scrutiny path. The empirical result from Table 3 shows that the direction of total effects of both variables is to positively facilitate substantive scrutiny. When third-party institutions provide verification reports, or when litigants raise explicit objections, courts are more inclined to engage in in-depth scrutiny of the evidence. In contrast, when such institutional or procedural supports are lacking, courts tend to rely on surface-level formalities, thereby opting for a superficial path that minimizes decision-making costs.

To summarize, the empirical result indicates that in the current landscape of blockchain evidence in judicial proceedings, courts place particular emphasis on the presence of third-party verification and the clarity of the cross-examination process from explicit objections. As key institutional foundations supporting deeper evidentiary scrutiny, both factors play a critical role in steering courts toward a more substantive approach to authentication.

## 5. Discussion

It should be reiterated that the purpose of this research is to examine whether cases involving blockchain evidence exhibit superficial scrutiny, and how to promote the transition toward substantive scrutiny. As discussed earlier, undergoing outsourced verifications and raising specific objections have a positive effect on the substantive scrutiny of blockchain evidence. However, this does not mean that the value of this research lies in encouraging these two actions. A “positive effect” does not imply that

such factors are to be regarded as “reasonable expectations.” In fact, the ideal situation is that, regardless of whether blockchain evidence has undergone notarization or forensic examination, and regardless of whether the adverse party is able to raise targeted objections, judges should take the ultimate responsibility of evidence scrutiny, and the scrutiny should be substantive. Judicial improvement should not be based on imposing demands on the parties, but rather on adjusting the rules governing the application of evidence.

In view of this, firstly, we should make it clear that the key to substantive scrutiny lies in inferential reasoning, which should be reflected in detail in the judgment. Such details help a party involved in a case understand the judge’s reasoning and, if the party would like to appeal, better direct their effort and prepare for the appealing process, by using the most basic common sense. Superficial scrutiny of the evidence, however, cannot provide such details. This not only makes the judgement more prone to mistakes and lead to wrongful convictions, but it also renders the appealing process more difficult. Due to the lack of details and sufficient logical reasoning, superficial scrutiny of evidence often produces ad-hoc arguments that are accompanied by inherent uncertainty. The appealing parties in turn can find the judgement provides little guidance regarding the next step, such as how to gather additional evidence or how to develop a more logically and legally sound argument. For this reason, superficial scrutiny should be avoided to the greatest extent possible.

Secondly, the common features of the two factors, outsourced verifications and specific objections, could enlighten how to achieve substantive scrutiny. However, as explained in the persuasion model, both factors fall within a clue-relying peripheral pathway. Simply promoting the two factors may not boost substantive scrutiny. Instead, judges may put too much attention on outsourced verifications or specific objections, deeming them indispensable when scrutinizing blockchain evidence. A better,

more constructive approach is to propose improvements grounded in the deeper logic behind these two measures. To eliminate superficial scrutiny, it is necessary to enhance the judges' reasoning ability, more importantly, to the ability that allows the judges to construct a proof process that lets evidence meet the standards of admissibility and employs proof methods to infer the facts. While the fallibility of judicial activities is an objective reality,<sup>45</sup> and the results of reasoning inherently permit uncertainty, how this proof process is clearly reflected in the judgment must be absolutely certain, as opposed to general, vague reasoning such as “blockchain evidence is authentic—therefore, the fact it reflects is true.” The following section will analyze the relevance, admissibility, and probative value of evidence, clarifying the objectives that need to be achieved at each step and exploring the proof process from blockchain evidence to case facts.

Specifically, in terms of relevance, we will clarify what constitutes an intermediate premise in cases involving blockchain evidence, so as to strengthen it in the subsequent admissibility and probative value stages. In terms of admissibility, the focus is on how approaches similar to notarization and forensic examination can be adopted to enhance judges' ability to make determinations, while avoiding excessive reliance on such measures in every case. In terms of probative value, the focus is on how raising objections can more specifically capture the judge's attention, as well as on other comparable means of ensuring effective communication in court.

## 5.1 Relevance

In this context, relevance should be interpreted as the basic threshold under common law. Relevance is the intrinsic attribute of evidence and marks the beginning of the process by which certain

---

<sup>45</sup> Chen Ke, Lun Sifa de Kecuo Xing [On the Fallibility of the Judiciary], Faxue [Legal Science], no. 12, 2020, at 80–96.

information can enter the trial. The assessment of the relevance of evidence is a dynamic analytical process. In the *Federal Rules of Evidence*, the “any tendency” standard defines relevant evidence as “that which has any tendency to make a fact more or less probable than it would be without the evidence, provided that the fact is of consequence in determining the action (Rule 401).” This means that for evidence to be considered relevant, it does not need to conclusively prove a fact, but merely make it more or less likely to be true. The rule sets a relatively low threshold for determining relevance, emphasizing that evidence must significantly pertain to the case but doesn't need to be overwhelmingly convincing on its own.

*The Federal Rules of Evidence* 401 to 403 establish the basic standards for assessing relevance, but these are not a priori rules that allow inferential facts to be deduced from evidentiary facts. The assessment of specific evidence relevance still depends on the evidence presented by the parties, their claims, and the judge's cognitive abilities in each specific case. To successfully prove case facts from evidence, it is necessary to incorporate the “intermediate premise,” achieving a transition from evidentiary facts to essential elements.<sup>46</sup>

Although it may not be possible to establish a specific set of rules regarding the relevance of blockchain evidence, it is important to achieve a basic understanding: what constitutes the “intermediate premise”<sup>47</sup> in the inferential process of cases involving blockchain evidence. Taking copyright infringement as an example, the plaintiff submits blockchain evidence consisting of a screen recording showing the defendant publishing the infringing article on a website, which constitutes an evidentiary fact. The judge's internal conviction that “the blockchain evidence has not been tampered with”

---

<sup>46</sup> Zhang Baosheng, Shishi Rending jiqi zai Falü Tuili zhong de Zuoyong [Fact-Finding and Its Role in Legal Reasoning], *Zhejiang Shehui Kexue* [Zhejiang Social Sciences], no. 6, 2019, at 25–42, 155–56.

<sup>47</sup> Ronald J. Allen, *The Myth of Conditional Relevancy*, 25 *Loy. L.A. L. Rev.* 871 (1991).

(including before and after it was recorded on the blockchain) belongs to the "intermediate premise". The judge's inference that the defendant did indeed publish the infringing article online is considered an inferential fact. Based on this, the judge further considers that the defendant's actions are classified as copyright infringement, referred to as "an element." In the entire proof process, whether an element can ultimately be derived from blockchain evidence largely depends on the strength of the "intermediate premise." When the "intermediate premise" lacks sufficient strength, parties need to introduce new evidence to reinforce the entire chain of evidence.<sup>48</sup> In other words, the issue of relevance becomes whether a person can believe in the intermediate premise, thereby allowing a reasonable person to make such an inference in times of uncertainty.

In most cases throughout the entire reasoning process, judges can internally conclude that a piece of blockchain evidence is relevant to the fact (making such a conclusion of relevance is not difficult); however, in this process, they often fail to clarify what they internally believe to be the "intermediate premise," which directly leads to cognitive confusion when subsequently applying rules of admissibility and probative force to strengthen the "intermediate premise."

The failure to clarify the "intermediate premise" in cases involving blockchain evidence is partly attributed to the diversity of forms in which blockchain evidence is submitted. Commonly found in infringement and contract cases, blockchain evidence can be submitted as either direct or indirect evidence, such as notarization or expert opinion. When blockchain evidence is submitted as direct evidence, judges often recognize that the intermediate premise is "the blockchain evidence was not tampered with before and after being recorded on the blockchain". When blockchain evidence is

---

<sup>48</sup> Liu Yan, Dianzi Shuju Quankuailian Shanglian Qian Zhenshixing de Shencha Jizhi—Jiyu Tuilun Liantiao he Shencha Fanshi de Fenxi [Pre-Blockchain Authentication Mechanism of Electronic Data: An Analysis Based on Inference Chains and Review Paradigms], *Fazhi Luntan* [Legal Forum], no. 1, 2023, at 54–73.

submitted in the form of notarization or expert opinion, it is considered indirect evidence, requiring further inference to reach an element. In these situations, judges often overlook that the “intermediate premise” should include that the evidence was not tampered with before being recorded on the blockchain. In other words, if an expert opinion about blockchain evidence is considered an evidentiary fact, it must go through a certain "intermediate premise" to infer that the material submitted for appraisal was authentic before it was formed, and thus conclude that the Fact of Consequence (FOC) it reflects, such as an infringement, is also authentic. This is specific to blockchain evidence: In the appraisal process, appraisers typically only perform technical analysis on the samples they have received. This expert opinion can only attest to the authenticity of the evidence at the carrier level, while the authenticity of the content before being recorded on the blockchain still requires the judge to assess based on the specifics of the case. At this point, when deciding about the intermediate premise, judges are highly likely to overlook their internal conviction regarding the authenticity of the pre-blockchain data, even when the technical appraisal process itself does not include an analysis of data authenticity prior to being recorded on the blockchain.

Overall, although there may not be a universal routine, the key step of establishing the relevance of blockchain evidence is to clarify “intermediate premise”, which follows from the “any tendency” standards of the relevance of general evidence. Specific to blockchain evidence, during the relevance scrutiny phase, the most crucial aspect is to clarify that the intermediate premise asserts that the evidence is authentic both before and after being recorded on the blockchain. The entire subsequent proof process is aimed at strengthening this intermediate premise, which serves as the premise for the further discussions on the admissibility and probative value of blockchain evidence.

## 5.2 Admissibility

It is generally believed that the admissibility of evidence refers to the capacity and qualification of certain evidence to be presented and permitted by the court.<sup>49</sup> Admissibility is not an inherent attribute of evidence, but a characteristic imposed upon it to meet specific needs, primarily based on the protection of human rights and the consideration of ascertaining facts. The evidence that can serve as a basis for a decision must not infringe on individual fundamental rights throughout the entire litigation process, and this established that evidence must not have a great potential for falsehood. In this sense, the objective of transitioning from evidentiary facts to an element is to find evidence that conforms to basic human rights protections and does not contain obvious falsehoods, and the requirements of this stage can be determined through the rules of evidence.

Based on these considerations, the following discussion will address the objectives that blockchain evidence admissibility rules should serve, the means by which purposes similar to those of notarization and forensic examination can be achieved, and, more specifically, the portion of knowledge within notarization and forensic examination that judges currently lack. If this specific knowledge gap is filled, judges may no longer need to rely on notarization or forensic examination.

### 5.2.1 Clarify distinctions rules to different types of blockchain evidence

For evidence that clearly does not comply with legal standards, such as evidence with uncertain origins, potential tampering, or obvious forgery, it should be excluded during the admissibility stage, following the Authenticity Rule, the Hearsay Rule, and the Best Evidence Rule (Original Document Rule). Based on the classification of blockchain evidence discussed above (native evidence generated on the

---

<sup>49</sup> Yi Yanyou, Zhengju Faxue: Yuanze, Guize, Anli [Evidence Jurisprudence: Principles, Rules, Cases], Law Press China, 2017.



blockchain and derivative evidence generated off the blockchain), during the scrutiny process, the argumentation logic regarding the authentication of blockchain evidence should depend on whether it constitutes hearsay, and whether it is considered an original document.

Regarding the authentication of blockchain evidence, depending on different evidence carriers, there are two types of authentications: one is to prove that the evidence presented in court is consistent with what the presenting party claims, and that the physical carrier it relies on has not been forged or tampered with. Another is to prove that the content of the evidence—text, charts, sounds, images, etc.—accurately records the original facts. For derivative evidence generated off the blockchain, the primary focus should be on the first type of authentication, ensuring that physical and documentary evidence presented in court is consistent with what is claimed. Additionally, it should guarantee that it is collected from a reliable origin, the collection and extraction procedure is conventional or standardized, and it is properly preserved. For native evidence generated on the blockchain, the main focus should be on the second type of authentication, which requires verifying whether the recorded sounds, charts, photos, etc., accurately reflect the facts of the case.

Regarding the hearsay rule, blockchain evidence can be considered in a slightly tricky position and, to some extent, constitutes hearsay: According to the general rules of hearsay, statements or records not directly experienced by a party are considered unreliable. The primary standard in U.S. courts is that computer-generated evidence is not considered hearsay.<sup>50</sup> The logic behind this exception is that hearsay requires a "declarant," and evidence produced through automated processes electronically clearly cannot make a statement. Therefore, for native blockchain evidence generated on-chain, there is no declarant, and thus this evidence is not considered hearsay. For derivative evidence generated

---

<sup>50</sup> Hunichen v. Atonomi LLC, 2020 WL 6875558 (S.D. N.Y. 2020).

off-chain, since the evidence is recorded outside the court, and the user uploading information to the blockchain can be considered the "declarant," that information should be examined under hearsay rules to determine whether it was tampered with before being uploaded to the blockchain. Only blockchain evidence that has not been tampered with should be considered an exception to hearsay.

Regarding the original document rule, one should recognize that blockchain evidence can be original, derivative, or secondary. As previously mentioned, blockchain evidence can be essentially considered as existing evidence converted into a blockchain-based format. Audiovisual materials and electronic data usually appear in electronic form and can be stored on the blockchain. Other forms of evidence such as physical evidence, documentary evidence, and witness testimony, although not in electronic form, can be converted into electronic format before being stored on the blockchain. This means that blockchain evidence can be originals (original evidence), copies (derivative evidence), or even transformations related to the originals and copies (secondary evidence). Therefore, when examining blockchain evidence, it is necessary to first determine its inherent type in order to ascertain its legal status in the case, and to judge whether the inherent type of evidence qualifies as an original and which evidence rules apply.

#### 5.2.2 Improve the expert assistant system to strengthen scrutiny

The prevailing approach to reviewing the reliability of blockchain evidence prior to its being uploaded continues to rely on seeking opinions from specialized technical institutions. This reflects an attempt to shift the judge's psychological burden stemming from uncertainty about case outcomes and the risk of wrongful judgments to such technical institutions. By outsourcing technical review and then directly adopting such opinions into the courtroom, the judiciary embeds external assessments into judicial

proceedings, which reflects an excessive pursuit of determinacy in judgments. Given the inherent limitations of judicial cognition, judge should instead focus on encouraging and assisting parties in enhancing their objecting capabilities. Strengthening procedural safeguards with this perspective may offer a more fundamental path toward reinforcing the viability of “intermediate claims”.

The expert assistant system is a mechanism primarily aimed at enhancing the parties’ ability to argue their case, with the auxiliary goal of supporting judges’ cognitive ability. It helps to compensate for the parties’ lack of specialized knowledge and prevents cross-examination of technically complex evidence—such as expert opinions or blockchain evidence—from becoming a mere formality. This, in turn, minimizes the risk of incorrect expert opinions entering the trial process and influencing the judgment.

Through expert assistants’ in-court explanations or challenges regarding the reliability and integrity of blockchain evidence, they can serve dual purposes: first, to supplement and reinforce the probative value of one’s own evidence; second, to question and weaken the probative value of the adverse party’s evidence, thereby disrupting the chain of proof. Without the assistance of expert assistants, even if there are flaws in an expert opinion of blockchain evidence, such issues are difficult to uncover during trial—despite the presence of the expert for examination by the parties or the judge.

However, in current judicial practice, the application of the expert assistant system is primarily initiated by judges *ex officio*. As noted in the aforementioned cases, the courts sought to ascertain the facts by either “appointing a technical investigator to participate in the trial” or “issuing an inquiry to the blockchain evidence preservation service provider. Both instances can be regarded as the courts initiating the expert assistant mechanism *ex officio*. As the previous analysis suggests, this judge-led

model of activation is not conducive to fostering adversarial confrontation between differing expert opinions. It may hinder the fact-finding process and lead to an overreliance on third-party opinions.

Specifically, the following measures should be adopted. First, if the adverse party requests the expert assistant to appear in court and the expert assistant refuses, the expert opinion cannot be used as a basis for the final judgment. Expert assistants often only submit written opinions. However, the information contained in such written statements is typically quite limited. Even if they contain false representations or flawed reasoning, these flaws are often well-concealed in form, making them difficult to detect through written review alone. Second, specific qualifications for serving as an expert assistant should be clearly defined. Those who understand how blockchain operates may include individuals involved in on-chain operations, such as miners, node participants, or evidence preservation platform personnel. When a party applies to having such an individual testify, they should also submit supporting evidence to prove that the person possesses the relevant expertise or has actual experience in blockchain operations, thereby ensuring the credibility of their testimony. Finally, objections to the views of expert assistants should be permitted in character evidence. Character-related challenges relevant to their technical credibility—such as their professional standing, published works, or past opinions—should be admissible.

Taken together, although these requirements may increase the evidentiary burden on the presenting party, fully protecting the opposing party's right to challenge will enhance the credibility of blockchain evidence.

### 5.2.3 Establish a remedial rule for defective evidence

Many exclusion rules are the products of compromises between various social values and the pursuit of truth; if certain evidence has sufficient justifiable grounds to warrant a concession to the pursuit of truth, such evidence should be excluded. The Exclusionary Rule, rooted in the Fourth Amendment's prohibition against unlawful searches and seizures, was established by the U.S. Supreme Court in *Weeks v. United States* (1914) and *Mapp v. Ohio* (1961). Unlike the absolute exclusionary rule, however, evidence that does not amount to a flagrant violation of statutory procedures but is nevertheless collected through flawed or improper methods should be addressed differently. In such cases, it is necessary to rely on the inherent characteristics of data to regulate key aspects that are easily overlooked during the collection process, thereby rationalizing and refining the specific rules governing blockchain evidence.

Blockchain evidence must adhere to a set of procedural rules during its generation and collection process to ensure its reliability. If it is not collected in accordance with the prescribed procedures, it may constitute defective evidence. The primary cause of such defects lies in the inability to guarantee the “cleanliness” of the preservation process—for example, the absence of a proxy connection during data capture, the failure to display complete system configuration information, or the inability to verify the authenticity of the accessed website.

To ensure the cleanliness of the preservation process, specific technical standards should be established in two areas: the systems of the preservation platforms and the procedures used in the evidence preservation process.

With respect to the systems of preservation platforms, in order to ensure the reliability and integrity of blockchain evidence, the following functions should be supported:

First, write-protection. To achieve write protection for blockchain evidence storage devices, storage media that do not permit any data writing operations should be used, or technical measures should be implemented to prevent data from being written. Second, full replication. In particular, the term “full” means that the storage device must be capable not only of duplicating existing data, but also of copying deleted data, hidden data, and all data stored in every area of the storage medium, including unused space. Third, identity verification. The system must be able to compute and compare the hash values of the source and target media to verify their identity, or, alternatively, perform binary comparison to achieve the same purpose without computing hash values.

As for the specific standards governing evidence preservation procedures, reference can be made to the industry standard SF/T 0076-2020: *Technical Specifications for Electronic Data Preservation*, issued by the Ministry of Justice. First, in terms of electronic data storage, each piece of stored electronic data must be assigned a unique preservation identifier. The preserved electronic data record should include elements such as an integrity check value, a trusted time stamp, user signature information, and log information. Reviewing these elements enables an assessment of the technical compliance of the data storage system used by the preservation platform; Second, in terms of electronic data transmission, the specifications mandate that the preservation platform must conduct trusted authentication of users before transmission. The cryptographic technologies used during transmission must comply with the standards certified and approved by the national cryptography regulatory authority. After transmission, integrity verification technologies must be employed to ensure that the electronic data has not been altered. These provisions help ensure the security and compliance of data transmission during preservation; Third, regarding electronic data verification, the preservation platform support multiple methods of verification, including verification of original preserved content

and non-original content. The platform must also be capable of producing reliable verification results, such as a preservation identifier, integrity check value, and trusted time stamp.

### 5.3 Probative value

The assessment of the reliability of blockchain evidence runs through the entire proof process. Relevancy includes a basic assessment of reliability, while admissibility excludes evidence that is significantly unreliable. The following will explore, in addition to relying on admissibility standards functioning as the first and basic screening device, is there other possible channels that can further enhance the reliability of blockchain evidence? Unlike the reliability of a single piece of evidence, the probative value concerns not only a specific piece of evidence itself but also its interrelation with other evidence in the case. In this sense, to enhance the probative value of evidence, it involves not only improving the reliability of the evidence itself but also coherently identifying its relationship with other evidence. In light of this, the purpose of discussing proof method is not to illustrate that blockchain evidence is unique in this respect compared to other types of evidence (in fact, proof method do not vary with the type of evidence), but rather, it is to propose possible proof method, which help assess the reliability of blockchain evidence in conjunction with the entire chain of evidence.

#### 5.3.1 Acknowledge the uncertainty of the premises in the proof method

Evidentiary reasoning seeks to penetrate beyond the surface of discourse and identify the facts that truly occurred from ambiguous narratives. However, a judge cannot decline to make a decision even when the facts remain unclear,<sup>51</sup> which is the reason why modes of proof need to be discussed in evidence law. In this sense, the optimal mode of proof we seek is as follows: when faced with an

---

<sup>51</sup> In criminal cases, even an acquittal rendered due to unclear facts—under the presumption of innocence—is still a form of judicial decision.

erroneous decision, the party—who knows the truth better, or perhaps is the only one who knows it—should be able to easily recognize the error in the judgment based on common sense, thus finding direction to supplement evidence and pursue remedial procedures (appeal or petition for retrial).

In contrast, the previously discussed superficial scrutiny creates an excessively burdensome and hardly attainable remedial process for the party, which should be avoided as much as possible. While we can certainly promote the two significant factors — outsourced verifications and specific objections — toward substantive scrutiny in specific cases, simply promoting such factors can also mask the fact that it is the deeper, more fundamental features that contains probative values from outsourced verifications and specific objections that fuel the substantive scrutiny. Moreover, simply promoting the two factors may risk misleading the judges and the parties involved in a case, let them believe that substantive scrutiny cannot be absolutely achieved without these factors. Therefore, it is necessary to examine the deep commonality of these two factors.

It should be observed that that these two factors all create clues beyond the evidence itself, and their impact on substantive scrutiny relies on the one-way reinforcement of evidence, leading judges to form an internal conviction about the facts in advance. Specifically, judges may directly trust evidence generated by a platform based on the qualification; when faced with notarization or forensic examination, judges rely on the authoritative certification to deem the data trustworthy; and after discussing (or rejecting) objections, judges further establish the reliability of the evidence through the psychological comfort gained from eliminating doubts. This psychological conviction is not derived from independent trust of the evidence, rather through external associative factors. This mode fails to provide a solid framework that truly encourages skepticism and independent verification. While it may



facilitate substantive scrutiny, the scrutiny under such process are often partial, unstable, and highly dependent on specific conditions.

To move beyond this dilemma, it's necessary to acknowledge the Certainty Trap within the mode of proof. Judicial personnel usually experience anxiety due to the inherent unpredictability of case outcomes. Nevertheless, adopting the current proof mode merely "attempts" to alleviate such anxiety rather than to achieve certainty in decision-making. In fact, neither technological advancement nor the refinement of evidentiary rules can eliminate the subjectivity and ambiguity within judicial process. Evidence scrutiny is essentially a type of interpersonal communication. For instance, judges can form convictions based on twitching at the corners of the mouth, hesitant pauses, and flushed complexions. This has also led to the development of new disciplines such as forensic psychology and courtroom linguistics to help assess the reliability of evidence. Even though similar disciplines cannot eliminate the uncertainty of judicial conclusions, such uncertainty must be allowed within a certain range. Established rules cannot accommodate the endless variety of social phenomena, and completely disregarding human subjective judgment would infinitely magnify the flaws of legislation.

The advancement of technology offers greater possibilities for the standardization of proof mode. However, blockchain evidence, or more broadly, digital evidence, can neither eliminate the uncertainty from evidence scrutiny nor remove the need of case-specific considerations in proof modes. For this reason, to address the superficial scrutiny of blockchain evidence, instead of defining a standardized or even rigid proof mode or evidence scrutiny procedure, one should take a step back: The core of addressing superficial scrutiny lies in reflecting on the shortcomings of the current proof method and clearly defining the courts' primary responsibility. Any effort toward institutionalizing evidentiary rules must fully consider and remain compatible with courtroom structures, procedures, and subjective

human judgments, rather than attempting to entirely replace courts' scrutiny through technology or third-party opinions. Thus, courts should avoid using "multiple corroborations" merely as a tool to circumvent subjective judgment. Instead, detailed rules for electronic and opinion evidence should be refined within the existing legal framework based on "reasonable conviction" and "procedural safeguards". This will guide courts to resume substantive scrutiny, decrease reliance on peripheral factors and litigant behaviors, and ultimately achieve an integration of novel evidence forms with traditional judicial reasoning.

### 5.3.2 Adopt a focused approach in cross-examination.

The process of proof is abductive reasoning, all attempts to enhance the "intermediate premise" and thereby increase the reliability of blockchain evidence should focus on improving the cognitive abilities of litigation participants. It is not advisable to establish a standardized, formalized pattern in hopes of definitively judging the authenticity of blockchain evidence. Rawls once mentioned that the "expected outcome of a trial is that if the defendant has committed the crime charged, he should be declared guilty. The trial procedure is designed to explore and ascertain the truth in this regard."<sup>52</sup> The inherent mechanism lies in allowing both the prosecution and defense to equally and unrestrictedly present their viewpoints and permitting either party the right to rebut the other, thereby revealing the true facts. This is a primary condition for a judge to make a fair judgment.

---

<sup>52</sup> Rawls argues that the meaning of imperfect procedural justice is that "even if the law is scrupulously followed and the process is conducted in a fair and proper manner, it is still possible to reach the wrong result. An innocent person may be convicted, and a guilty person may go free. In such cases, we witness a kind of miscarriage of justice in which injustice does not stem from human fault but from a fortuitous combination of circumstances that frustrates the purpose of legal norms." John Rawls, *A Theory of Justice* (Huaihong He, Baogang He & Shenbai Liao trans., China Social Sciences Press 1988), at 81.

Different litigation participants play different roles in a case and present different narratives. The adverse party must construct its own narrative and interpretation around the evidence presented at trial, using skillful yet sincere strategies of cross-examination to dispel the “technological ghost” created by the high barriers of blockchain technology,<sup>53</sup> thereby enabling the adjudicator to form an inner conviction regarding the facts. This process is inseparable from language and symbols. In a sense, the adverse party is like a painter: “A painter must carefully mix paint to achieve the ideal tone when creating a work of art. Similarly, to obtain a favorable judgment, one must choose words and language with the same precision as an artist selects color”.<sup>54</sup> Only through the careful construction of objection structure can the adverse party influence the adjudicator’s inner conviction.

In specific cases, impeaching the authenticity, legality, and relevance of blockchain evidence one by one, and presenting a comprehensive opinion in court is a common approach from adverse party, this often raises many doubts about the evidence, making the litigation proceedings quite “actively”. However, while such an approach seems to cover all doubts, it actually leads to an unclear direction in negating the reliability of the evidence, as the impeach points raised against blockchain evidence are too scattered. Given the limited time in court, judges are generally unable to follow a checklist-style opinion, even when some arguments may be reasonable and point to actual doubts. Judges’ primary objective is to ascertain the truth, and only after forming inner conviction about facts do they retrospectively consider which of the points raised by the adverse party aligns with that conviction. This logic precisely resonates with the abductive reasoning discussed above. Accordingly, effective

---

<sup>53</sup> Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Lin Shaowei trans., Shanghai People’s Publ’g House 2019), at 26.

<sup>54</sup> Meizhen Liao, *Fating Yuyan Jiqiao [Courtroom Language Techniques]* (3d ed., Law Press 2009), at 192.

cross-examination does not lie in raising numerous fragmented objections, but in presenting focused rebuttals that directly challenge the alleged facts rather than showing off technical tricks of law.

For these criteria, the effort in impeaching should not be uniform, it should adopt a focused approach that prioritizes key aspects. Previous discussion indicates that impeaching blockchain evidence regarding relevance (probative value) is most likely to reveal doubts and is also the most persuasive; impeaching regarding the authenticity is secondary in effectiveness. Impeaching legality equality may lag behind in practice, because the concept of “flawed evidence” is widely applied, and judges tend to be somewhat tolerant of such evidence (which is not to suggest that this phenomenon is justice). Focusing solely on the authenticity and legality of blockchain evidence significantly reduces the likelihood that such arguments will be adopted by the court.

It should also be noted that, relevance is not an isolated standard for the admissibility of blockchain evidence; rather, it often overlaps with authenticity and legality. To effectively challenge the relevance of blockchain evidence, one must grasp the role that the evidence plays within the entire chain of proof. It is especially important to note that the scope of blockchain’s authenticity guarantee is temporally limited—it only applies after the data has been uploaded to the blockchain. Since pre-upload data lies outside the control of blockchain technology, the truthfulness of such data is no different from that of traditional evidence.

## 6. Conclusion

In cyberspace, code is law;<sup>55</sup> in judicial practice, however, rules can rarely be fully expressed or enforced through automated, code-based mechanisms. As noted earlier, whether judges conduct

---

<sup>55</sup> Lawrence Lessig, *Code and Other Laws of Cyberspace* 45 (Basic Books 1999).

substantive scrutiny and give reasons for it in their judgments depends on a balance between costs and benefits. Both outsourced verity and explicit objection can alter this balance, thereby influencing the extent to substantive scrutiny.

First, we set out the technological advantages and potential limitations of blockchain evidence, in terms of admissibility and probative value. Second, based on these practical manifestations, we hypothesize that judges may follow two possible paths in scrutiny—the logic-driven central path and the clues-relying peripheral path—and that “notarization or forensic examination” and “explicit objections” may influence the choice between these two paths. Third, in light of this, we constructed a binary logistic regression model, taking judicial scrutiny as the dependent variable, the two aforementioned factors as independent variables, and other case-specific characteristics that can affect the costs and benefits to judges during adjudication as mediating variables. The regression results indicate that these two factors indeed have a positive impact on substantive scrutiny. Finally, drawing on the above empirical results, we argue that although enhancing “notarization or forensic examination” and “explicit objections” can promote substantive scrutiny, from the perspective of judicial improvement, expectations for substantive scrutiny should not rest solely on the parties’ initiative to seek outsourced verification or to vigorously pursue evidentiary challenges, which are responsibilities that ought to be borne by the judge. Instead, attention should be directed to the common underlying goal of improving judges’ cognitive capacity and fostering thorough courtroom communication, and, on this basis, targeted reform proposals for blockchain evidence can be advanced from the three dimensions of relevance, admissibility, and probative value.

Specifically, at the level of relevance, the proposition that the evidence was “authentic both before and after being placed on the blockchain” should be clarified as an intermediate premise during proof. At

the level of admissibility, evidence that is substantially weak in authenticity should be excluded. By applying such admissibility rules, it should be possible to achieve purposes similar to those of outsourced verification (notarization and forensic examination) and, more precisely, to enable judges to address the gap in knowledge within notarization and forensic examination that they currently lack. This entails clarifying differentiated rules for different types of blockchain evidence, improving the expert assistant system to strengthen judicial scrutiny, and establishing a remedial rule for defective evidence.

At the level of probative value, similar to the effect of clear objections during trial, comparable outcomes should be achieved through courtroom communication. Such communication enhances the parties' understanding of blockchain evidence and therefore strengthens judges' ability to articulate reasoning about it. In particular, this requires acknowledging the uncertainty of the premises in proof methods. Because the process of proof is essentially abductive reasoning, all efforts to reinforce the intermediate premise—and thus increase the reliability of blockchain evidence—should concentrate on improving the cognitive abilities of litigation participants. This entails constructing an “ideal speech situation” between the parties and the judge. When impeach the three aspects of authenticity, legality, and probative value (the extent of relevance to the case), the adverse party should focus on what is most significant, target the key issues, and prioritize the cross-examination of probative value.

Overall, it is crucial to specify the above tasks at each stage and to give reasons for them in the judgment. Further, absence of systematized proof processes—of much at all that resembles “rules”—gives rise to identical concerns about whim and caprice, which animate the concern over the law's inability to specify its commands clearly in advance.<sup>56</sup> Our study is intended, in the final outlook, to

---

<sup>56</sup> Ronald J. Allen, *Artificial Intelligence and the Evidentiary Process: The Challenges of Formalism and Computation*, 9

argue that if litigants and judges generally lack sufficient cognitive capacity when confronted with technological advancements, then the current model of proof—particularly when it involves scientific evidence—should, at the very least, be the one that provides both litigants and judges with adequate cognitive motivation and is committed to approaching the truth, and strives to exhaust all possible means to uncover additional evidence. Only the abductive reasoning (which is also the sole method by which judges form their inner conviction in practice) ensures that during the evidence discovery phase, the chain of evidence remains in a state flexible enough to accommodate new findings. Any emerging evidence can be seamlessly integrated into one side’s narrative to enhance their initially proposed “explanatory version”. However, should any evidence contradict this “explanatory version”, the party must face the consequences of their claims being scrutinized and potentially deemed false.

It should be noted that, although this study reveals significant impacts of various variables on scrutiny paths, certain limitations in the model design remain. Some factors influencing scrutiny judgments, such as judges’ individual learning abilities, technological literacy, and acceptance of new evidence, are difficult to directly observe or quantify from judicial documents. Also, incorporating socio-economic characteristics—such as judges’ age, educational background, and academic research experience in law—as control variables in future studies could potentially enhance the explanatory power of the model. Nevertheless, China’s current judge selection and training system provides a certain degree of assurance regarding judges’ qualifications, such as standardized legal education backgrounds, the requirement of undergraduate or higher degrees, and rigorous national judicial examinations, which helps mitigate systematic errors arising from individual differences and provide structural support for the validity of the current model.

---

Artif. Intell. Law 99 (2001).

## Appendix

To provide transparency and replicability, this appendix details the definitions and coding rules of the seven control variables included in the analysis. Dichotomous coding was applied (1 if the condition is satisfied, 0 otherwise), except for amount in controversy and local disposable income per capita, which were treated as continuous variables.

### Control Variable 1: Whether the trial court is an “Internet specialized court”

China has nearly 3000 grassroots administrative units, and the cases selected in the sample predominantly occur in the jurisdictional courts located within these grassroots administrative regions. Among these grassroots courts, the Beijing Internet Court, Hangzhou Internet Court, and Guangzhou Internet Court were established after 2017 and have essentially emerged in response to the emergence of blockchain evidence. In the variable setup, the cases handled by these three Internet courts are designated as 1, while cases handled by other courts are designated as 0.

### Control Variable 2: Whether the cause of action is a contract dispute or a tort dispute

In this study, the cause of action is coded as a binary variable. Contract disputes, such as financial loan contract disputes, lease contract disputes, and civil lending disputes, are coded as 0. By contrast, tort disputes, including cases involving the online dissemination right of works, copyright ownership and infringement, internet tort liability, screening right of works, and trademark infringement, are coded as 1.

### Control Variable 3: Whether the presenting party is a legal entity or a natural person



In the sample cases, for the sake of convenience in statistical analysis, cases where the party presenting evidence is the defendant have been excluded. Therefore, when the party presenting evidence is a legal entity, meaning the plaintiff is a legal entity, this situation is designated as 1. Considering that this classification is essentially aimed at distinguishing the ability of the party presenting evidence concerning blockchain evidence, cases involving non-legal entities not recognized as legal persons under the law, such as the 19th Asian Games Organizing Committee, the Zhongyi Food Processing Factory in Bo'ai County, and the China Audio-Visual Copyright Collective Management Association, are also designated as 1, while all other cases are designated as 0.

#### Control Variable 4: The composition of the judicial panel

In the sample cases, there are several types of trial organization forms, including: a single judge handling the case, a single substitute judge handling the case, a collegial panel consisting of one chief judge and two associate judges, and a collegial panel consisting of one chief judge and two lay assessors. According to the aforementioned theoretical assumption, the primary reason for distinguishing between single and collegial trials is based on the differences between individual decision-making and group decision-making. Therefore, situations involving collegial panels (including one chief judge and two associate judges, as well as one chief judge and two lay assessors) are designated as 1, while single trials (including cases handled by a single judge and a single substitute judge) are designated as 0.

#### Control Variable 5: Whether the judgment date is before or after August 2021

The judgment dates of the sample cases in this research fall between June 2018 and November 2023. Considering that the "Online Litigation Rules of the People's Court" were officially introduced in

August 2021, which stipulated rules for the scrutiny of blockchain evidence, cases with judgment dates after August 2021 are designated as 1, while those before that date are designated as 0.

#### Control Variable 6: Value of claim

Because the litigation claims made by the parties can encompass both substantive rights and procedural rights, quantifying the interests in such claims is a problem that this research aims to address. In cases where the party's claim involves a monetary payment, the object of action in this research is the specific monetary amount associated with the claim, and this amount is log-transformed for regression analysis. In cases where the claim involves the transfer of physical assets or the confirmation of property rights, the equivalent monetary value of the physical assets is used (and similarly log-transformed). If the claim involves rights such as procedural rights or other interests that cannot be directly translated into an equivalent monetary amount, it is treated as missing data.

#### Control Variable 7: Per capita disposable income

Per capita disposable income of the region where the court is located is included as a continuous control variable, measured in RMB and log-transformed for regression analysis. This variable serves as a proxy for regional risk attitudes, based on the basic sense that individuals' willingness to take risks often correlates with their income levels.