International Journal of Innovation in Indic Studies

ISSN: ISSN: 2583-5149 | Vol-4, Issue-1 | July 2026

Digital Forensics and Blockchain-Based Evidence in Criminal Trials

Khushi Mogha

B.B.A. LL.B. and LL.M. (Corporate Law).

Abstract

It highlights a research gap: while the technology to trace and preserve blockchain evidence has matured quickly, the legal rules for admitting such evidence, especially the certification requirements under Indian law and the hearsay debate under the American Federal Rules of Evidence, have not kept pace. Using a doctrinal and analytical method, the study examines recent judgments, including the Bitcoin Fog and Sterlingov prosecution in the United States and the evolving Section 63 framework under India's Bharatiya Sakshya Adhiniyam, 2023. The discussion is supported by simple charts showing the growth of blockchain-related evidentiary disputes and a comparison between traditional and blockchain-based chain of custody. The paper finds that blockchain can strengthen the integrity of digital evidence, but it cannot replace the human and procedural safeguards, such as expert testimony, certification, and cross-examination, that criminal law demands. It ends with practical recommendations for lawmakers, judges, and forensic examiners, and calls for clearer, technology-neutral rules that let genuine blockchain evidence in in front of courts without lowering the standard of proof beyond reasonable doubt.

Keywords: Digital Forensics; Blockchain Evidence; Chain of Custody; Admissibility; Criminal Trials; Electronic Evidence

1. Introduction

Crime today rarely happens without leaving some kind of digital trace. A phone's location history, a WhatsApp message, a CCTV recording, or a cryptocurrency transfer can often tell investigators more about what happened than a traditional eyewitness. Digital forensics is the branch of forensic science that deals with recovering, preserving, and presenting this kind of electronic material so that it can be used safely in a court of law. Over the last decade, a new layer has been added to this picture: blockchain technology. Originally built to support Bitcoin, blockchain is a shared, tamper-resistant ledger that records transactions in a way that is very hard to alter quietly. Because of this property, investigators and technology companies have started using blockchain both as a tool to trace criminal activity, particularly cryptocurrency crime, and as a method to protect the integrity of other digital evidence, such as CCTV footage or forensic images, by recording their digital fingerprints on a public or private ledger.

This shift raises a simple but important question: can evidence that is created, stored, or verified through blockchain be trusted and admitted in a criminal trial the same way a signed document or a fingerprint report would be? Criminal trials carry serious consequences, including loss of liberty, so the rules of evidence are strict about how material is collected, preserved, and proved. Blockchain's promise of tamper-resistance is attractive, but it does not automatically satisfy the legal tests of relevance, authenticity, and reliability that most legal systems demand.

This paper studies the intersection of digital forensics and blockchain-based evidence specifically inside criminal trials. It looks at how the law in the United States and India, two systems that have both dealt with high-profile digital and cryptocurrency cases, has responded to blockchain evidence. The paper is written in plain language so that it is useful to law students, practising lawyers, forensic examiners, and policymakers, not only to specialist technologists.

The importance of this topic goes beyond academic curiosity. Police forces around the world are already using blockchain analytics to freeze and trace stolen cryptocurrency, and some courts are being asked, sometimes for the first time, to decide whether a printout of a blockchain transaction or an expert's tracing report can be trusted the same way a bank statement or a call detail record would be. If courts get this wrong in either direction, by trusting unreliable technology too easily

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

or by rejecting genuinely reliable evidence out of unfamiliarity, real harm follows: either innocent people may be wrongly convicted on shaky technical evidence, or guilty people may escape justice because a court refused to look at proof that was, in fact, sound. Getting the legal treatment of blockchain evidence right is therefore not a side issue for technology lawyers alone; it sits at the heart of a fair and effective criminal justice system in the digital age.

2. Historical Development

Digital forensics as a discipline began in the 1980s and 1990s, when law enforcement agencies started recovering data from floppy disks and early personal computers involved in fraud and hacking cases. The field grew quickly after the year 2000, driven by the spread of the internet, mobile phones, and email, which meant that almost every crime, even purely physical ones, left behind some digital footprint. Many countries responded by amending their evidence laws to deal with this new kind of proof. India, for example, added Section 65B to the Indian Evidence Act, 1872 through the Information Technology Act, 2000, to allow computer-generated records to be admitted as evidence, subject to a certificate confirming how the record was produced.

Blockchain entered the picture much later. The technology was first described in the 2008 Bitcoin white paper as a way to let strangers transact online without needing a bank or other trusted middleman. For the first several years, blockchain was mostly discussed in the context of financial regulation and cryptocurrency crime, such as the Silk Road darknet marketplace case in the United States, which first showed investigators that blockchain transactions, although pseudonymous, could actually be traced back to real people using specialised analytics software.

From around 2017 onwards, two separate but related developments took shape. First, law enforcement agencies and private companies built blockchain analytics tools, such as Chainalysis Reactor and TRM Labs, to help trace illicit cryptocurrency flows and connect wallet addresses to real identities. These tools have since been used and tested in major prosecutions, including the Bitcoin Fog money-laundering case decided in the United States District Court for the District of Columbia. Second, legal scholars and some governments began exploring blockchain not just as a subject of investigation but as a tool for protecting evidence itself, for example by hashing digital

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

files such as CCTV footage or forensic disk images and recording the hash value on a blockchain so that any later tampering can be detected. China's Supreme People's Court has been especially active here, issuing guidance in 2018 and again in 2022 that encourages the use of blockchain in its internet courts and judicial case management systems.

In India, the transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024, is the most recent milestone. The new law widened the definition of an electronic record to cover data stored on communication devices and networks, and it retained a certification requirement, now placed in Section 63, that closely follows the older Section 65B. Indian courts, most importantly the Supreme Court in Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal (2020), have gone back and forth on how strictly this certificate requirement should be enforced, and that debate continues to affect how blockchain-based records would be treated if produced in an Indian criminal trial today.

3. Key Terms and Definitions

A few terms recur throughout this paper and are explained here in simple language before the discussion goes further.

- Digital forensics: The scientific process of identifying, collecting, preserving, and analysing data stored on computers, phones, or networks so that it can be presented as evidence.
- Chain of custody: The documented history of who handled a piece of evidence, when, and how, from the moment it was collected until it is produced in court. Any gap in this chain can be used to challenge the evidence.
- Blockchain: A distributed, shared record book (ledger) maintained by many computers at once, where new entries are added in blocks that are cryptographically linked to earlier blocks, making silent alteration very difficult.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

- Hash value: A short, fixed-length string of characters generated from a file or piece of data using a mathematical function. Even a tiny change in the original file produces a completely different hash, so hashes are used to prove that a file has not been altered.
- Blockchain analytics: Software, such as Chainalysis Reactor, that studies patterns of transactions on a public blockchain to group addresses together and link them to real-world individuals or organisations.
- Admissibility: The legal question of whether a court will allow a particular piece of evidence to be considered at all, based on rules such as relevance, authenticity, and reliability.
- Hearsay: An out-of-court statement offered to prove the truth of what it asserts. Many legal systems restrict hearsay evidence unless it fits within a recognised exception, and this debate is important for blockchain records.
- Section 63, Bharatiya Sakshya Adhiniyam, 2023 (India): The current Indian provision governing the admissibility of electronic records, requiring a certificate to accompany such evidence, similar to the earlier Section 65B of the Indian Evidence Act.

4. Literature Review

Recent academic writing on this subject can be grouped into three broad streams. The first stream studies how blockchain analytics is treated as expert evidence in criminal trials, mainly in the United States. Commentary on the Sterlingov prosecution, connected to the Bitcoin Fog mixing service, explains how the trial court applied the Daubert standard under Federal Rule of Evidence 702 to decide that testimony based on Chainalysis Reactor software was reliable enough to go before the jury, even though the defence argued that the software had not been peer reviewed and had no known error rate. Commentators note that this software evidence was not the only proof in the case; it worked alongside more traditional evidence such as online forum posts and IP address analysis, which suggests that blockchain analytics is best understood as one part of a wider evidentiary picture rather than a stand-alone silver bullet.

The second stream of literature looks at whether blockchain records themselves count as hearsay and how they fit within existing rules of evidence in the United States. Scholars are divided. One view is that blockchain records do not fit comfortably into existing hearsay exceptions and that evidence rules should be specifically amended to deal with them. A competing view argues that the cryptographic security and consensus-based verification built into blockchain already reduce the traditional concerns that hearsay rules are designed to address, so new rules may not be strictly necessary, only clearer guidance. This literature also tracks how individual American states such as Vermont, Arizona, Ohio, and Illinois have passed laws that give blockchain records a presumption of authenticity, while noting that the lack of a uniform federal approach creates inconsistent practice across the country.

The third stream is centred on India and on comparative and international criminal law. Indian legal writing in 2025 and 2026 consistently points to the same structural problem: the certification requirement under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which was designed for records generated on a single computer controlled by one identifiable person, does not fit well with a blockchain, where data is spread across many independent nodes with no single custodian. Writers have suggested reforms such as a government-run digital evidence registry, wider recognition of hash values as sufficient proof of authenticity, and specially trained expert witnesses to explain distributed ledger technology to judges. Recent commentary also flags a practical bottleneck: very few government-notified digital evidence examiners exist under Section 79A of the Information Technology Act, and courts, including the Madras High Court, have directly asked the government to notify more such experts. Comparable work in international criminal law and post-conflict prosecutions looks at how blockchain-based chain-of-custody systems could help preserve evidence, such as open-source material documenting war crimes, that is collected outside formal state institutions, while cautioning that blockchain guarantees only that a record has not been altered after it was entered, not that the original content was truthful or was captured correctly in the first place.

Taken together, this body of work shows a field that is moving quickly on the technical and investigative side, with real prosecutions already relying on blockchain analytics, but moving

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

much more slowly on the legal and procedural side, where basic questions about certification, hearsay, and expert qualification remain unsettled in most jurisdictions, including India.

A smaller but growing fourth stream looks at judicial infrastructure rather than individual cases. Writers studying China's internet courts describe how the Supreme People's Court has pushed for blockchain to be built directly into court case-management systems, allowing judges to check the integrity of filed documents automatically rather than relying on a party's certificate. Similar proposals for a purpose-built, multi-stakeholder blockchain architecture for judicial case management, in which separate ledgers serve the judiciary, the prosecution, and the defence and are coordinated through a shared meta-ledger, show that some engineers and scholars are now thinking about blockchain as a piece of court infrastructure, not just as a source of contested evidence. This infrastructure-focused literature is still largely separate from the case-law-focused literature on admissibility, and this paper treats the connection between the two as part of the research gap described in the next section.

5. Research Gaps

Based on the review above, this paper identifies four specific gaps that existing research has not fully addressed.

- Certification mismatch: Indian evidence law still assumes a single, identifiable custodian of an electronic device, which does not match how a decentralized blockchain actually works, and there is limited concrete guidance on how a Section 63 certificate should be completed for blockchain-anchored evidence.
- Reliability testing beyond one jurisdiction: Much of the detailed judicial reasoning on the reliability of blockchain analytics software comes from a small number of American federal court decisions; there is far less published judicial reasoning from India, the United Kingdom, or other common law jurisdictions on the same question.
- Distinguishing tracing tools from custody tools: Existing literature often discusses blockchain analytics, used to trace criminals, and blockchain-based evidence preservation,

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

used to protect the integrity of other evidence, as if they were the same issue, even though they raise different legal questions and need to be examined separately.

- Human and institutional capacity: There is limited research on whether police, forensic labs, and trial judges in developing countries currently have the training and the notified expert examiners needed to handle blockchain evidence competently, as opposed to research that focuses only on what the law should say in theory.

6. Objectives

- To trace the historical development of digital forensics and blockchain-based evidence and to explain the key technical and legal terms involved.
- To review recent literature, statutes, and case law from the United States and India on the admissibility of blockchain and digital forensic evidence in criminal trials.
- To identify the main legal and practical gaps that prevent the smooth use of blockchain evidence in criminal proceedings.
- To analyse how courts have actually applied existing evidentiary standards, such as the Daubert test and Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, to blockchain-related evidence.
- To offer practical, implementable recommendations for lawmakers, judges, and forensic practitioners.

7. Scope and Limitations

This paper focuses on the use of digital forensic and blockchain-based evidence specifically inside criminal trials. It draws mainly on the legal systems of the United States and India, using illustrative material from China and the European Union where relevant, because these jurisdictions currently generate the largest volume of published case law and academic commentary on this subject. The paper deals with two related but distinct uses of blockchain: first,

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

as an investigative tool used to trace cryptocurrency transactions, and second, as a method to preserve the integrity of other digital evidence through hashing and timestamping.

The paper does not attempt an exhaustive country-by-country survey of every jurisdiction's evidence law, nor does it provide a deep technical tutorial on how blockchain consensus algorithms work internally; only the level of technical detail needed to understand the legal discussion is included. The charts presented later in the paper are conceptual and illustrative, built to visualise trends and relationships described in secondary literature, and should not be read as official government or court statistics. Because blockchain-related case law is still developing quickly, the analysis reflects the position as understood up to mid-2026, and readers should check for more recent judgments before relying on this paper for practical legal advice.

8. Materials and Methods

This is a doctrinal and analytical legal study rather than an empirical one. The material used includes primary legal sources, such as the Indian Evidence Act, 1872, the Bharatiya Sakshya Adhiniyam, 2023, the United States Federal Rules of Evidence, and reported judgments including Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal (2020) and the Sterlingov prosecution connected to the Bitcoin Fog case in the United States District Court for the District of Columbia (2024). Secondary material includes recent peer-reviewed articles, law firm client alerts, and specialist legal commentary published between 2024 and 2026, gathered through targeted searches of legal databases and journal repositories.

The method follows four steps. First, relevant statutes and judgments were identified and read in full or in extract to understand the legal test being applied. Second, secondary academic and professional commentary was reviewed to understand how scholars and practitioners interpret these developments. Third, the material was organised thematically into the sections of this paper, comparing the American approach, built around the Daubert reliability test and the hearsay debate, with the Indian approach, built around the Section 63 certification requirement. Fourth, two simple illustrative charts and one workflow diagram were prepared using Python's matplotlib library to

visually summarise the trends and comparisons discussed in the text, based on patterns described in the literature rather than on any single official dataset.

9. Results and Discussion

The material reviewed for this paper shows a consistent pattern: blockchain evidence is becoming more common in criminal proceedings, but courts are handling it using existing evidentiary tools rather than creating entirely new ones. Figure 1 below presents an illustrative trend, based on patterns reported in recent legal commentary, showing how disputes over blockchain-specific evidence have grown at a faster relative rate than general digital evidence disputes since blockchain analytics tools became mainstream around 2017.

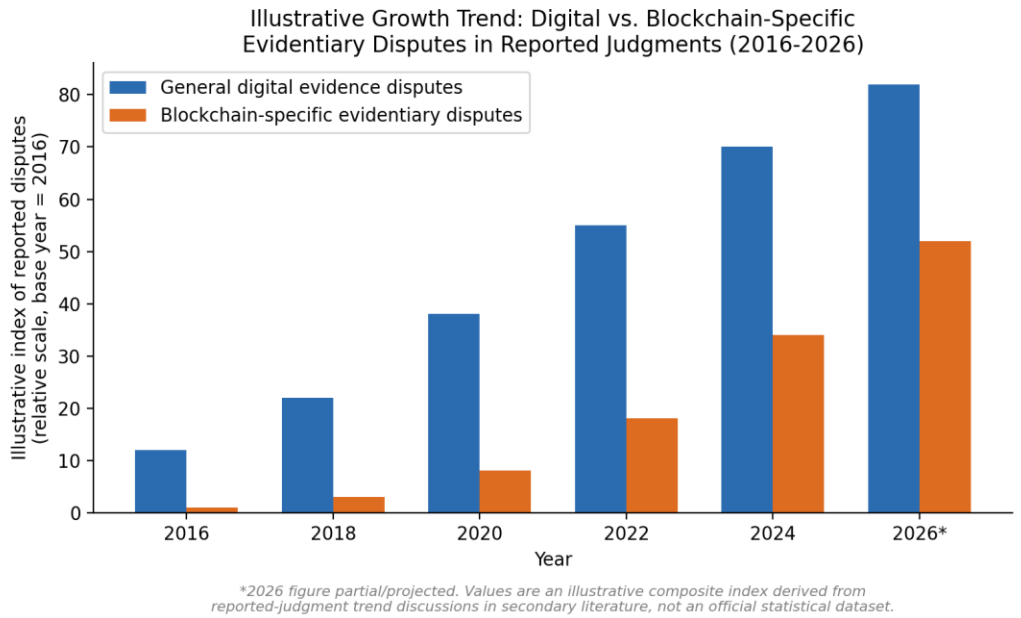

Figure 1: Illustrative growth trend of general digital evidence disputes compared with blockchain-specific evidentiary disputes in reported judgments, 2016-2026. Values represent a composite illustrative index, not an official count.

The clearest example of how courts are applying existing rules to blockchain evidence is the Sterlingov prosecution in the United States. Before the trial began, the court had to decide whether an expert could testify using Chainalysis Reactor, a proprietary tool that traces Bitcoin transactions

by grouping addresses that appear to belong to the same entity. Applying the four Daubert factors, namely whether the method has been tested, subjected to peer review, has a known error rate, and is accepted in the relevant field, the court allowed the testimony, while also noting that this software evidence was supported by other, more conventional evidence such as materials found with the defendant and online forum activity. This shows an important pattern: American courts are not treating blockchain analytics as automatically reliable, but they are also not shutting it out; they are asking the same reliability questions they would ask of any other scientific or technical evidence.

A second, related pattern concerns the debate on whether blockchain records amount to hearsay. Some commentators argue that because blockchain entries are made and verified by a network of independent computers rather than by a single person making an out-of-court assertion, they may not fit the traditional definition of hearsay at all. Others are more cautious and argue that new, specific rules are still needed. A small number of American states, including Vermont, Arizona, Ohio, and Illinois, have passed laws that give blockchain records a degree of legal recognition, but this has created uneven practice, since most states and the federal system have no such specific rule.

Turning to India, the picture is different but related. Figure 2 compares traditional, paper-based chain-of-custody practices with a blockchain-based approach across six practical attributes that matter in a criminal trial.

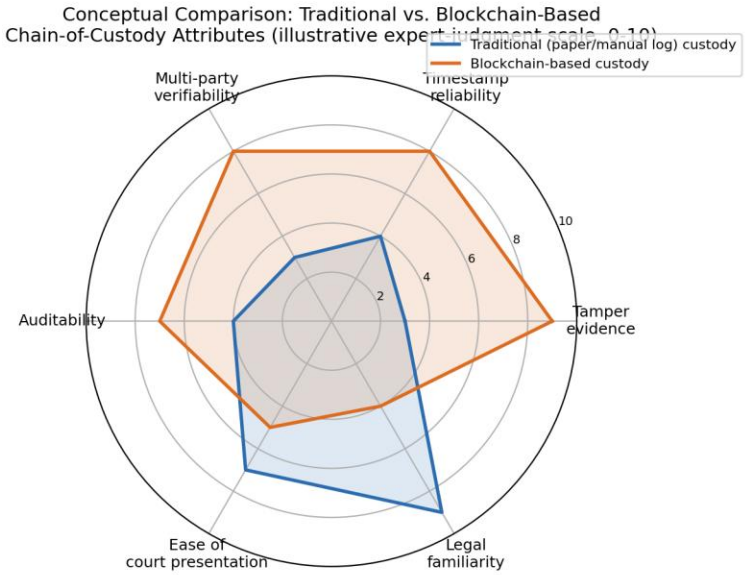

Figure 2: Conceptual comparison of traditional versus blockchain-based chain-of-custody attributes, on an illustrative 0-10 expert-judgment scale derived from themes discussed in the literature.

As Figure 2 suggests, blockchain-based custody scores well on tamper evidence, timestamp reliability, and multi-party verifiability, since altering a blockchain record after the fact requires overturning many independently held copies at once. However, it scores lower on ease of court presentation and legal familiarity, mainly because judges, lawyers, and even forensic examiners in most Indian courts are still more comfortable with paper certificates and conventional hash-based hard-disk imaging than with distributed ledger concepts. This gap matters because Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, like the Section 65B it replaced, was written with a single, identifiable computer and a single responsible official in mind, whereas a public blockchain has no single custodian who can sign such a certificate in the traditional sense. The Supreme Court's decision in Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal (2020) reaffirmed that this certificate is mandatory unless the original device itself is produced in court, a rule that

becomes difficult to apply cleanly when the underlying record is spread across a decentralised network rather than sitting on one identifiable machine.

Figure 3 draws together the practical workflow that this paper's review suggests is emerging in practice, showing how a piece of digital evidence typically moves from seizure through hashing, ledger entry, forensic analysis, and finally into the courtroom, where it must still satisfy conventional legal tests of chain of custody and admissibility.

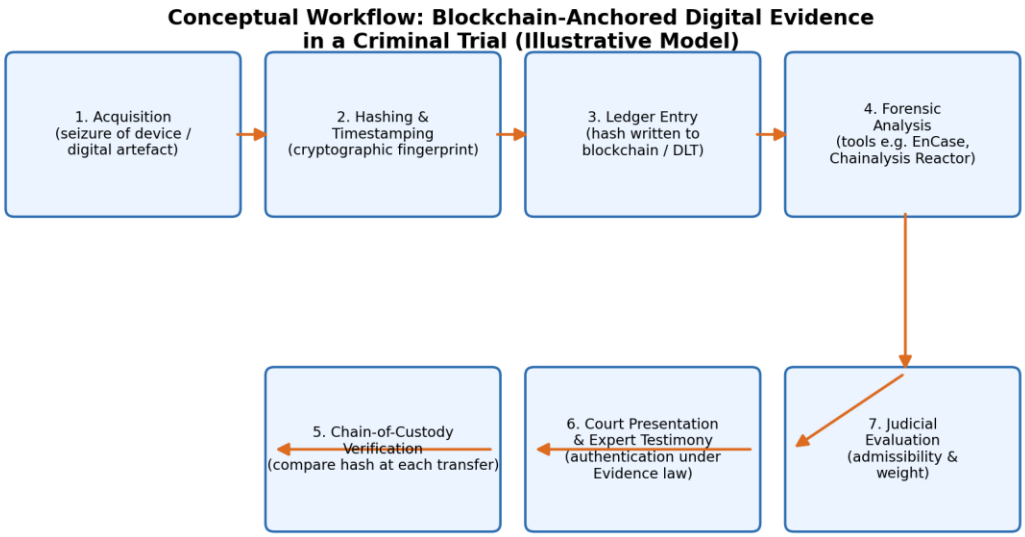

Figure 3: Conceptual workflow showing how blockchain-anchored digital evidence typically moves from seizure to judicial evaluation in a criminal trial.

This workflow highlights a point that runs through both the American and the Indian material: blockchain is best understood as reinforcing, rather than replacing, the traditional steps of evidence handling. It can strengthen step two (hashing and timestamping) and step three (ledger entry) by making later tampering easier to detect, but steps one, four, five, six, and seven, namely lawful seizure, competent forensic analysis, verified custody, skilled courtroom presentation, and independent judicial evaluation, still depend entirely on trained people and sound procedure, not on the technology itself. India's shortage of government-notified digital evidence examiners under

Section 79A of the Information Technology Act, a gap that the Madras High Court has specifically flagged, illustrates this limitation clearly: even excellent blockchain technology cannot compensate for a shortage of qualified experts able to explain it convincingly to a trial court.

It is also worth noting what blockchain evidence cannot do. A hash value recorded on a ledger proves only that a specific file has not changed since the hash was taken; it says nothing about whether the camera that recorded a video was working correctly, whether the person who took the first hash captured the right file, or whether the file was genuine in the first place. This distinction, between integrity after capture and truthfulness of the original content, is emphasised repeatedly in the international criminal law literature reviewed for this paper, particularly in discussions of open-source evidence used in post-conflict prosecutions, where material is often collected by non-government actors before it ever reaches a court. The same caution applies with equal force inside an ordinary domestic criminal trial: a prosecutor who proves that a video file's hash has not changed since it was seized still has to independently prove where the video came from, who recorded it, and that it has not been edited before that first hash was taken.

10. Findings

- Blockchain analytics tools, such as Chainalysis Reactor, are increasingly accepted as reliable expert evidence in American courts when tested against the Daubert standard, but they are rarely, if ever, treated as the sole basis for a conviction.
- There is no single, settled answer to whether blockchain records count as hearsay under American evidence law; the position currently depends on the specific type of record and, in some states, on specific legislation.
- India's certification requirement under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, remains structurally difficult to apply to decentralised blockchain records, since it was designed around a single identifiable custodian.
- Blockchain strengthens the technical integrity of evidence, particularly against silent tampering, but does not by itself establish that the original content was true, accurate, or properly captured.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

- A shortage of trained experts and notified digital evidence examiners, especially in India, is a practical bottleneck that is at least as significant as any gap in the written law.
- Courts across jurisdictions are, in practice, adapting existing evidentiary frameworks, such as Daubert and Section 63/65B certification, to blockchain evidence rather than waiting for entirely new legislation, which suggests that targeted reform, not wholesale rewriting of evidence law, is the more realistic path forward.

11. Recommendations

- Lawmakers in India should consider amending Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, to recognise a properly generated and independently verifiable hash value as sufficient proof of authenticity for blockchain-anchored records, reducing over-reliance on a single-custodian certificate.
- Governments should notify more digital evidence examiners under Section 79A of the Information Technology Act, so that every district, not just major cities, has access to a qualified expert who can explain blockchain evidence to a trial court.
- Judicial academies in India and similar training bodies elsewhere should run regular, practical training programmes for judges and public prosecutors on how blockchain technology works and how to question expert witnesses about it.
- Where possible, courts should treat blockchain analytics as one part of a larger body of evidence, consistent with the approach seen in the Sterlingov prosecution, rather than allowing a conviction to rest on blockchain tracing alone.
- Legislators in the United States could look at the more detailed state-level rules from Vermont, Arizona, Ohio, and Illinois as a starting point for a clearer, more uniform federal approach to blockchain record authentication.
- A neutral, government-backed digital evidence registry, as suggested in recent Indian legal commentary, could help standardise how blockchain and other electronic evidence certificates are issued and checked, reducing inconsistent practice across courts.

ISSN: 2583-5149 | Vol-4, issue-1| July 2026 | License (CC BY 4.0)

12. Conclusion

Blockchain technology offers a genuinely useful tool for both tracing criminal activity and protecting the integrity of digital evidence, and courts in the United States have already shown that existing rules of evidence, such as the Daubert reliability test, are flexible enough to accommodate it. At the same time, this paper's review shows that the legal and institutional side of the story has not caught up with the technology, particularly in India, where the certification requirement under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, was written for a world of single computers and identifiable custodians, not decentralised ledgers. Blockchain cannot replace the basic safeguards of criminal procedure, including lawful seizure, a documented chain of custody, competent expert testimony, and a fair opportunity for the defence to challenge the evidence. What blockchain can do is make some of these safeguards easier to prove and harder to fake, provided that lawmakers, judges, and forensic professionals are given clear rules and proper training to use it well. With targeted, technology-neutral reforms of the kind recommended in this paper, digital forensics and blockchain-based evidence can be brought fully and fairly into the criminal trial process, without lowering the standard of proof that protects every accused person's right to a fair trial.

References

Katten Muchin Rosenman LLP. (2025). Crypto in the courts: Five cases reshaping digital asset regulation in 2025. Katten Client Advisory.

Lenahan-Pfahlert, K. A. (2024). Blockchain analysis and related expert testimony admissible in criminal trial. Money Laundering Watch, Ballard Spahr LLP.

Chainalysis. (2024). Bitcoin Fog case confirms Chainalysis analytics is reliable and admissible in court. Chainalysis Inc. Blog.

Frontiers in Blockchain. (2024). Blockchain in the courtroom: Exploring its evidentiary significance and procedural implications in U.S. judicial processes. Frontiers in Blockchain, 7.

Frontiers in Blockchain. (2026). The evidentiary value of blockchain in civil litigation: Comparative insights and future directions. Frontiers in Blockchain.

The Legal Quorum. (2025). Blockchain and evidence law: Admissibility of blockchain records in courts. The Legal Quorum, Legal Commentary Series.

NALSAR Tech Law Forum. (2026). Securing digital evidence in India: A case for integrating blockchain-based smart contracts. Tech Law Forum @ NALSAR.

Key Cases Referred

- Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal, (2020) 3 SCC 216 (Supreme Court of India).
- Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 (Supreme Court of India).
- Anvar P.V. v. P.K. Basheer, AIR 2015 SC 180 (Supreme Court of India).
- United States v. Sterlingov, U.S. District Court for the District of Columbia (Bitcoin Fog prosecution), Daubert ruling and conviction, 2024.
- Upasana Sajeev v. State, Madras High Court (on notified digital evidence examiners under Section 79A, IT Act).