INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

Volume 1 | Issue 1 [2023] | Page 74-86

DIGITAL EVIDENCE IN INDIAN COURTS: ENSURING AUTHENTICITY AND ADMISSIBILITY IN A VIRTUAL WORLD

-Shreyash Gupta[1]

ABSTRACT

The judiciary has wrestled with the challenge of authenticating electronic evidence since the advent of digitization, leading to a surge in problems within legal systems. Ensuring the authenticity, originality, and admissibility of digital evidence has become imperative. This research paper delves into the impact of emerging technologies, particularly blockchain, on digital evidence's authenticity and verifiability. The study examines key attributes of blockchain technology, including its cryptographic security, transparency, and irrefutable nature. Additionally, the paper discusses the implications and challenges faced by Indian courts. The analysis also focuses on block blockchain's role in guaranteeing the authenticity and originality of electronic evidence. Furthermore, the paper briefly scrutinizes several case studies and relevant examples, aiming to illuminate the advantages and disadvantages of adopting such technology within the Indian legal system.

KEYWORDS

Blockchain, Digital Evidence, Emerging Technologies, Authenticity, Admissibility, Indian Legal System and Digitization.

1. INTROD[2]UCTION

[1] Shreyash Gupta is a 3rd year student at Bhimrao Ambedkar University, Lucknow.

In the modern age, marked by the proliferation of computers and digitalization, one of humanity's most revolutionary achievements has unfolded. Yet, within this rapid transformation, a distinctive set of challenges has emerged, particularly in the realm of cyber security and the prevalence of cybercrimes. The accessibility and far-reaching scope of cyber space have engendered a wealth of content and information, coexisting with an escalating potential for misuse and tampering. Consequently, the authenticity of electronic evidence has ignited ongoing debates, driven by its inherent susceptibility to manipulation. This discourse extends to hold significant ramifications for investigation agencies and the pivotal matter of evidence admissibility within the judicial context.

Against this backdrop, the emergence of disruptive technologies, such as blockchain, has begun to redefine paradigms across global sectors. Beyond its foundational role in digital currencies like bitcoin, blockchain's applications have expanded to encompass diverse fields, spanning data management, supply chain logistics, financial services, and the intricate fabric of the legal domain itself. Notably, 2 the revolutionary capability of blockchain to secure and validate transaction records has ignited transformational shifts, permeating even the nuanced arena of electronic evidence management.

Within this era of rapid technological evolution, the ability of the legal system to keep pace is frequently challenged. The role of digital evidence in court proceedings serves as a prime illustration. While conventional evidence relies on validation through witnesses and tangible objects, electronic records present distinctive complexities. These records, while convenient, are encoded, encrypted, and vulnerable to alterations that compromise their authenticity. Deciphering these records and tracing alterations to specific individuals introduce intricate issues, entwined with privacy concerns and the upholding of evidentiary integrity.

Despite these intricacies, the allure of digital evidence remains potent due to its convenience, heightened security, and cost-effectiveness. The reliance on electronic evidence in both civil and criminal cases underscores its indispensable role. In a landscape where the rapid progress of technology frequently outpaces societal development, navigating the intricate terrain of digital evidence's authenticity and admissibility in the virtual realm assumes critical importance. This research delves into the intricate realm of digital evidence, examining its authentication, admissibility, and evolving significance within the judicial domain and aims to dissect the

challenges, implications, and opportunities that come to the fore as India's legal system grapples with the evolving nuances of digital evidence.

2. RESEARCH QUESTION

How does the use of emerging technologies, such as blockchain, impact the authenticity and admissibility of digital evidence in the Indian legal system?

3. RESEARCH OBJECTIVE

• Understand the foundational principles of blockchain technology and its applications beyond cryptocurrencies.

• Examine the technical aspects of block blockchain's secure and decentralized structure, emphasizing its role in ensuring the integrity and reliability of transaction records.

• Analyze the complexities associated with integrating digital evidence within the Indian legal system, including challenges related to technical knowledge gaps, evidence reliability, admissibility, privacy concerns, and storage complexities.

• Explore how blockchain technologies' unique features, such as the 'hash' function and 'time stamping,' contribute to establishing the authenticity and irrefutability of digital evidence.

• Investigate the alignment of blockchain technology with existing legal provisions and evolving perspectives of the judiciary regarding digital evidence admissibility.

• Provide insights through case studies and examples within the Indian legal context that illustrate the practical implications of using blockchain technology to enhance the credibility and acceptance of electronic evidence in court proceedings.

• Contribute to the broader understanding of how emerging technologies, particularly block chain, impact the authenticity and admissibility of digital evidence, informing legal practices and policy decisions in the realm of technology and the judiciary.

4. UNDERSTANDING BLOCKCHAIN TECHNOLOGY

Blockchain technology operates as a cybernetic framework designed to store diverse transactional records, referred to as "blocks." These blocks are also shared across multiple computers, forming an unbroken sequence of interconnected structures, thus the term "chain." While renowned for its critical role in crypto currency systems, ensuring secure and decentralized transaction records, the utility of blockchain extends beyond the realm of crypto currencies. Its application can establish data immutability across various industries, safeguarding against unauthorized alteration. Since altering a block is virtually impossible, only trusted entities or algorithms can input data, eliminating the necessity for intermediaries like auditors, which often result in added costs and potential errors.

Following Bit coin's introduction in 2009, blockchain's utility has expanded exponentially, manifested through the creation of diverse cryptocurrencies, non-fungible tokens (NFTs), decentralized finance (DeFi) platforms, and smart contracts. Analogous to a database or spreadsheet such as Google Sheets, a blockchain serves as an information repository. Nevertheless, its differentiating factor lies in the organization and accessibility of data. A conventional database relies on scripts for tasks like data entry, retrieval, and storage, akin to those performed in a blockchain. However, a blockchain uniquely distributes data, storing multiple copies across numerous machines, requiring consensus for validity.

Transaction details are aggregated within a block, similar to a cell in a spreadsheet. Once capacity is reached, encryption algorithms generate a hexadecimal hash, an encrypted representation of the information. This hash becomes part of the subsequent block's header and is encrypted along with other data, forming a sequential chain of interlinked blocks. The resulting structure ensures that the enclosed data remains unalterable, providing a secure foundation for various applications across industries.

5. DIGITAL EVIDENCE CHALLENGES IN INDIAN COURTS

In an era marked by the rapid proliferation of technology, the integration of digital evidence within the framework of legal proceedings has become increasingly pivotal. The advent of electronic communication mediums, encompassing emails, text messages, computer files, and the sprawling realm of social media updates, has ushered in a new dimension of evidence

presentation in courtrooms. As the significance of digital evidence escalates in our technologically driven world, its introduction and utilization within the Indian judicial system unfurls a tapestry of challenges and complexities.

5.1 TECHNICAL KNOWLEDGE GAP

A prominent hurdle lies in the limited technical proficiency among lawyers and judges. Many remain more comfortable with conventional methods, lacking familiarity with electronic devices. The technical intricacies involved in obtaining, preserving, and presenting digital evidence remain foreign to numerous legal professionals in India. This unfamiliarity can lead to misinterpretations and inaccuracies, influencing the ultimate outcomes of cases.

5.2 RELIABILITY CONCERNS

Digital evidence is more susceptible to manipulation compared to physical evidence. Ensuring its authenticity and integrity is paramount. Regrettably, Indian courts lack established protocols for validating digital evidence, raising questions about its trustworthiness.

5.3 ADMISSIBILITY CHALLENGES

While the Indian Evidence Act [2] governs the admissibility of evidence, it does not explicitly address digital evidence. This results in ambiguity regarding whether digital evidence can be presented in court.

5.4 PRIVACY IMPLICATIONS

Dealing with digital evidence also raises privacy concerns. The collection of personal information from digital sources can raise valid privacy issues. It's imperative to adhere to privacy laws and regulations during the collection and use of digital evidence. 1 The Indian Evidence Act, 1872, Act No. 1 of 1872, India Code (1872).

5.5 STORAGE AND PRESERVATION COMPLEXITIES

There are many difficulties in properly preserving and storing digital evidence. Data loss or corruption can result from poor storage practices. It is crucial to create reliable methods for the effective preservation of digital evidence.

ROLE OF BLOCKCHAIN IN ENSURING AUTHENTICITY

By utilizing the transformational potential of blockchain technology, the role of blockchain in ensuring authenticity with respect to digital evidence proposes a novel method of managing digital evidence. This innovation has the potential to change how cybercrime investigations and judicial cases are handled in the future.

The suggested system's incorporation of blockchain technology to handle the difficulties of managing digital evidence is its main novelty. Digital evidence may be authenticated and secured using block chain, which is recognized for being decentralized, transparent, and tamper-proof. This increases the evidence's dependability and legal admissibility. Here is a more thorough investigation of the application and its revolutionary effects:

6.1 DECENTRALIZED AND TAMPER-PROOF

Blockchain functions without a central authority thanks to a decentralized network of computers known as nodes. Each piece of digital proof is time-stamped, encrypted, and kept in a block. These blocks are connected in a chronological order after being added to the blockchain, forming an unchangeable chain. This immutability makes it very hard to change or remove any information without agreement from the whole network, ensuring that digital evidence is always impenetrable.

6.2 CHAIN OF CUSTODY

Keeping a trustworthy chain of custody in place is one of the most important parts of evidence integrity. The transparency and traceability of blockchain make it the ideal technology for assuring the reliability of the chain of custody. Every contact with the evidence is documented as a blockchain transaction, giving a traceable record of who accessed it when and for what reason.

6.3 TRANSPARENCY AND AUDITABILITY

Every member of the network may observe and confirm the history of the evidence thanks to block chain's transparency. Every stakeholder, including investigators, attorneys, judges, and juries, benefits from this transparency. The blockchain's suitability also makes it feasible to follow alterations, additions, and verifications made to the evidence over the course of its lifetime

6.4 SMART CONTRACTS

The suggested approach has much more revolutionary potential when smart contracts are used. Self-executing contracts with set terms are known as smart contracts. Smart contracts can automate procedures like evidence filing, verification, and sharing in the context of digital evidence. This simplifies the evidence management procedure while lowering the possibility of manipulation and human mistake.

6.5 CROSS-VERIFICATION AND COLLABORATION

Blockchain's distributed nature allows multiple parties, such as law enforcement agencies, legal experts, forensic investigators, and experts, to collaborate and cross-verify evidence securely. Each participant's contribution is recorded and time-stamped, ensuring a transparent and accountable collaboration process.

6.6 ADMISSIBILITY IN COURT

The integration of blockchain technology bolsters the admissibility of digital evidence in court. With a verifiable and tamper-proof digital chain of custody, the authenticity and integrity of evidence are inherently established, making it more compelling and credible during legal proceedings. The incorporation of blockchain revolutionizes digital evidence management. Its tamper-proof integrity, transparency, and collaboration potential redefine legal proceedings, ensuring evidence credibility and efficiency, propelling the legal sphere into a new era of technological trustworthiness.

IMPACT ON ADMISSIBILITY

Blockchain technology carries profound implications for evidence admissibility within India's legal framework. With each user's computer housing multiple information blocks, the need for a centralized authority, such as a bank, is eliminated. Key functions like 'hash' and 'time stamping' further fortify its uniqueness. The 'hash' function validates file integrity by producing a distinct result in case of tampering, while 'time stamping' chronicles transaction details, establishing an unalterable repository of events. This unique combination positions blockchain as an irreversible and incorruptible source of information, making it highly valuable as evidence.

Beyond its initial association with cryptocurrencies, notably Bitcoin, blockchain's utility extends across various sectors in India, including banking, intellectual property, and evidence law. The watershed moment arrived in 2018 when the Supreme Court of China recognized blockchain-based evidence as admissible in court proceedings. This breakthrough was witnessed in the intellectual 7 property dispute between Byte Dance's Douyin (TikTok) and Baidu, where blockchain was employed to substantiate copyright claims. [3]

This development contrasts with previous practices in both China and India. The procedure to admit electronic evidence in China necessitated notarization and corroboration, akin to India's current stance. However, the distinctive feature of blockchain technology, ensuring a secure chain of custody due to its traceable and tamper-resistant nature, circumvents the need for corroboration, aligning with the best evidence rule. This aligns with Section 65B [44] of the Indian Evidence Act[4], 1872, which holds significance for the enforcement and jurisdiction of transactions conducted through blockchain networks. Since records reside on blockchain networks, Section 65B [45] [5]governs their admissibility as electronic evidence, enabling the use of computer-generated records as evidence without requiring additional proof, subject to defined limitations.

The judiciary's evolving perspective is evident in cases like ***Shafhi Mohammad v. The State of Himachal Pradesh[6]***, reflecting a more open stance towards embracing blockchain evidence. The fundamental question surfaces: Should blockchain be categorized like conventional electronic evidence within the Indian legal framework? Here, the block blockchain's intrinsic tamper resistance, demonstrated in cases like *U.S. v. Lizarraga-Tirado**[7]***, sets it apart. Thus, the Indian Evidence Act should differentiate blockchain due to its unique attributes. Additionally,

the government's adoption of blockchain bolsters its credibility and underlines its applicability within India.

CASE STUDIES AND EXAMPLES

The law concerning the admissibility of digital evidence in India has witnessed developments through landmark cases***State (NCT of Delhi) v. Navjot Sandhu[8]***, which established a significant precedent. It determined that even in the absence of a Section 65B8 certificate, secondary digital evidence could be admissible if it adhered to the provisions of sections 639 and 6510 of the Evidence Act. This ground-breaking Ruling allowed oral testimony from prosecution witnesses to satisfy, thereby relaxing the standards for electronic evidence.

Anvar P.V. v. P.K. Basheer and Others[9], The Supreme Court declared Sections 65A12 and 65B13 as the exclusive provisions governing electronic records' admissibility, replacing Sections 63 and 65. The requirement for a Section 65B (4)14 certificate for secondary electronic evidence, like data on CDs, DVDs, and Pen Drives, was emphasized. Expert opinions under Section 45A15 could no longer bypass this condition. Challenges emerged from improperly obtained evidence and the potential manipulation of certificate-based authentication. The issued certificate, though, didn't guarantee secure content or source authenticity, raising concerns about known control over the computer.

Tomaso Bruno and Anr. v. State of Uttar Pradesh [10]emphasized the significance of incorporating modern technology and scientific methods in investigations, particularly underlining the value of electronic evidence in establishing facts. This highlighted the role that scientific and electronic evidence can play in assisting investigative agencies.

In the case of ***Shreya Singhal v. Union of India[11]***, the Supreme Court declared Section 66A of the IT Act18 as illegal, asserting that the internet's wider reach doesn't curtail the freedom of expression. ***Suvarna Musale v. Rahul Musale*** recognized electronic methods for recording evidence, allowing video conferencing due to practical constraints faced by the petitioner-wife working abroad with a child.

Digital evidence's significance was particularly evident in the Rajasthan WhatsApp Lynching Case19 and the Nirbhaya Gang Rape Case. In the former, the court collaborated with forensic

experts to verify the authenticity of WhatsApp messages, showcasing the need for specialized digital forensic expertise. In the latter, CCTV footage, mobile phone records, and location data played a pivotal role in establishing movements. The court addressed authenticity concerns through expert testimonies and data integrity verification using hash values.

The **Zoom-Bombing Case** highlighted challenges posed by virtual hearings, with disruptive elements exploiting software vulnerabilities. Courts responded by issuing secure virtual hearing guidelines, underscoring the importance of unaltered digital records.

The ***Anvar P.V. vs. P.K. Basheer*** [12]judgment clarified the criteria, emphasizing certification and evidence integrity. Collectively, these cases outline a framework for handling digital evidence, striking a balance between technological advancements and legal standards

9. SUGGESTIONS

9.1 IMPROVE DIGITAL FORENSIC CAPABILITIES

Improve the knowledge and tools that law enforcement authorities in India have access to in order to efficiently gather, examine, and store digital evidence. This can entail funding cutting-edge forensic equipment and technology and offering detectives specialized training.

9.2 STRENGTHEN LEGAL FRAMEWORK

To make sure they are complete and current, review and amend existing laws pertaining to digital evidence, such as the Information Technology Act[13]. Clear instructions on the gathering and storage of such evidence should also be included, as well as procedures for the admission of digital evidence in court.

9.3 ESTABLISH A CENTRALIZED DATABASE

To securely store and retrieve all digital evidence gathered by law enforcement organizations, establish a single repository or database. This would make information exchange across organizations more effective and cut down on effort duplication.

9.4 COLLABORATION WITH TECHNOLOGY COMPANIES

To provide tools and methods for efficient collecting and analysis of digital evidence, and form relationships with Indian technology businesses. This can entail collaborating on research initiatives, exchanging best practices, or even creating special teams inside these businesses to help law enforcement organizations.

9.5 PUBLIC AWARENESS CAMPAIGNS

Educate the general public about the importance of preserving digital evidence and reporting cybercrimes promptly. This could be done through awareness campaigns, workshops, or online resources that provide guidance on how individuals can protect their own digital footprints while also assisting law enforcement efforts.

9.6 INTERNATIONAL COOPERATION

Strengthen collaboration with international counterparts in areas such as information sharing, capacity building, and joint investigations involving cross-border cybercrimes. This would help address challenges posed by global nature of cybercrimes and facilitate smoother exchange of digital evidence between countries.

9.7 ENCOURAGE RESEARCH AND DEVELOPMENT

Promote research initiatives focused on developing innovative techniques for handling emerging forms of digital evidence, such as those related to artificial intelligence, blockchain technology, or Internet of Things (IoT) devices. Encouraging academia-industry partnerships in this field can lead to advancements that benefit both law enforcement and the overall digital ecosystem in India.

10. CONCLUSION

In conclusion, the secure, immutable, and time-stamped nature of blockchain records holds promise as admissible evidence in court proceedings. While certain jurisdictions, like China, explicitly accept block chain evidence in Internet courts, broader acceptance as legally binding

evidence faces legal barriers and practical challenges. The potential for wider blockchain evidence admissibility involves revisiting rules governing electronic signatures and electronic evidence within the judicial framework. The evolving landscape of Digital Forensics stands in stark contrast to the handling of Physical Evidence in traditional court settings. Within this context, Blockchain Technology emerges as a viable solution to address the complexities of managing digital evidence. Its flexibility allows for the integration of critical attributes such as authority, authenticity, integrity, transparency, auditability, and security into the evidence management process. This confers a distinct advantage over conventional methods, facilitating meticulous maintenance and tracking of the forensic and scientific chain of custody. Blockchain application holds the potential to minimize conflicts by nurturing elevated trust through their transparent and tamper-resistant characteristics. This transformative potential extends to the Forensic Network and Community, instilling genuine assurance of precision and dependability. Consequently, blockchain's integration serves as a pragmatic remedy to avert human errors that could otherwise compromise the admissibility of digital evidence within the legal framework. By deploying blockchain to safeguard the chain of custody for digital evidence, the risk of compromised integrity is considerably curtailed, thereby reinforcing the credibility of such evidence within the legal domain.

REFERENCES

[1] Student, BBALLB (3rd Year), Bhimrao Ambedkar University, Lucknow

[2] The Indian Evidence Act, 1872, Act No. 1 of 1872, India Code (1872).

[3] Yingzhi Yang, Blockchain data accepted as evidence in a legal complaint filed by short video app Douyin, South China Morning Post (Sept. 13, 2018)

[4] The Indian Evidence Act, 1872, §65B[44]

[5] The Indian Evidence Act, 1872, §65B[45]

[6] Shafhi Mohammad v. State of H.P., (2018) 2 SCC 801

[7] United States v. Lizarraga-Tirado, 789 F.3d 1107 (2015)

[8] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600

[9] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473

[10] Record Of Proceedings SUPREME COURT, (Mar. 21, 2015)

[11] Shreya Singhal v. Union of India, (2015) 5 SCC 1

[12] Ibid

[13] Information Technology Act, 2000, India Code (2000).