HOW DO EMERGING TECHNOLOGIES, LIKE BLOCKCHAIN, IMPACT THE AUTHENTICITY AND ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIAN COURTS?

Aman Puri, SVKM's Pravin Gandhi College of Law

1. ABSTRACT

The emergence of emerging technologies such as blockchain has brought about significant changes in different aspects of society, including the legal environment This paper examines the impact of emerging technologies, particularly blockchain, on the authenticity and recognition of digital evidence in India in the courts of law. The paper begins by providing an overview of traditional methods of evidence collection and admission, focusing on challenges faced in the digital age, such as cases of misuse of digital evidence on, truth and acceptability.

The paper then explores the concept of blockchain technology, explaining its main characteristics and how it can meet these challenges by providing a secure, decentralized, and immutable method for digital storage and verification in the evidence. It covers aspects of blockchain technology, including immutability, cryptographic hashing, and distributed ledger technology, which ensure the authenticity and authenticity of digital evidence.

Furthermore, the paper examines the legal framework surrounding the admissibility of digital evidence in Indian courts, including the Indian Evidence Act, 1872, and related case It examines how blockchain technology fits with these legal requirements and affects utility and potential challenges in adopting blockchain technology in the Indian regulatory framework. The study also includes a comparative analysis of how other countries have implemented blockchain technology in their legal systems to accommodate digital evidence. This study provides insights into the best practices and possible pitfalls that could inform the adoption of blockchain technology in India.

Overall, this paper aims to explore how emerging technologies, particularly blockchain, can enhance the authenticity and admissibility of digital evidence in Indian courts, ultimately contributing to the judicial system being effective and reliable.

2. INTRODUCTION:

In today's rapidly evolving digital landscape, it is no surprise that society is moving towards a digitalized future. Increased productivity and competitiveness requirements make digitalization inevitable. It offers opportunities to improve operational efficiency and enhance decision-making processes. By leveraging digital technologies such as blockchain, artificial intelligence, cloud computing and data analytics, organizations can streamline operations, personalize customer experiences, and drive innovation.

Yet, within this rapid transformation, a distinctive set of challenges has emerged, particularly in the realm of cybersecurity and the prevalence of cybercrimes. The ease of access and extensive reach of the internet have led to an abundance of data and material, but there is also a growing risk of exploitation and manipulation.

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. The exposure of digitalization has not only affected our daily lives but also affected the legal aspects and legal philosophies.

The reliance on electronic evidence in both civil and criminal cases underscore its indispensable role. In this research we delve into the importance as well as the challenges of digital evidence in courts, and finally, should the ongoing cases be allowed to be streamed on various digital platforms which would allow transparency and accountability of the Indian Courts?

3. UNDERSTANDING THE BLOCKCHAIN TECHNOLOGY

The term "Blockchain" might be confusing for some people, so let's understand what Blockchain exactly is. Blockchain is a digital database of transactions that is stored on many computers called nodes, which are linked by a network. It is a distributed ledger that helps record the transactions taking place among multiple users over the internet.

Blockchain's decentralized nature not only creates redundancy but maintains the fidelity of the data. For instance, if an attempt is made to modify a record in one instance of the database, the other nodes in the network would collectively prevent such alteration. This distributed

consensus mechanism ensures that no single node can unilaterally change the information stored within the blockchain.

We can transparently view every single transaction by either having a personal node or using Blockchain explorers (that allow anyone to see transactions occurring live) due to Blockchain's decentralized nature.

In recent years, there have been several instances of cryptocurrency transactions being compromised, leading to significant losses. Even though the hackers may have been anonymous, but their wallet addresses were not – the transactions are easily traceable because their wallet addresses are published on the Blockchain.

In India, the regulatory framework for blockchain technology and its applications is currently absent. Despite the slow pace of growth, technological advancements in the legal sector have significantly enhanced efficiency, reduced errors, and improved the understanding of judicial procedures. The digitization of the legal industry, spurred by the unprecedented pandemic, marked a significant shift from traditional paper filings to virtual court hearings. This transformation was made possible by the Supreme Court's e-committee, led by Hon'ble Justice DY Chandrachud, which implemented a contingency plan to ensure the continued operation of courts during the pandemic.

4. BLOCKCHAIN'S RESPONSE TO AUTHENTICITY AND ADMISSIBILITY CHALLENGES

The admissibility of evidence in India's court system would be significantly impacted by the development of blockchain technology. The decentralized nature of blockchain, where several information blocks are stored on each user's computer, eliminates the need for middlemen, in contrast to traditional systems that rely on centralized authorities like banks. Its dependability is further increased by important features like "hash" and "timestamping." While 'timestamping' captures transaction information to provide an immutable record of events, the 'hash' function guarantees file integrity by producing a unique code that changes if the file is altered. This special mix increases blockchain's potential as legal evidence by making it an invaluable and impenetrable source of data.

4.1 IMMUTABLE NATURE

Blockchain tackles its challenges in several ways, and its immutable nature is one of its key features. When digital evidence is stored and collected in Blockchain, it creates a block connected to all the other subsequent blocks, creating a chain of custody in chronological order.

The data stored in the blocks is almost impossible to alter and tamper with, because to do so, one will have to change and alter all the other subsequent blocks connected to it, which is computationally infeasible.

Therefore, by leveraging blockchain's immutability, digital evidence can be securely stored and reliably authenticated, enhancing its admissibility in legal proceedings.

4.2 CHAIN OF CUSTODY

As we talked about earlier, when digital evidence is stored on the Blockchain, it establishes a block, connecting to a chronological chain and because they are immutable, the evidence cannot be altered or deleted.

When there is a transfer or change of custody of digital evidence, it is recorded as a separate transaction on the Blockchain, ensuring security of the evidence. Furthermore, Blockchain’s transparency ensures that the parties involved in a particular case can access and verify the chain of custody. The use of cryptographic techniques and measures ensures secure access, and only authorized personnel can access the chain of custody.

Overall, blockchain technology offers a robust solution for maintaining the chain of custody for digital evidence, enhancing its integrity and admissibility in legal proceedings.

4.3 DIGITAL SIGNATURES

Blockchain technology has emerged as a promising solution for ensuring the authenticity and admissibility of digital evidence. By using its core features like unchangeability, transparency, and secure encryption, blockchain can create a secure record of the chain of custody for digital evidence.

Each piece of evidence added to the blockchain is time-stamped, establishing a verifiable record of when it existed. Digital signatures can also be used to confirm the origin and integrity of digital evidence, making it tamper-resistant. This technology not only improves the reliability of digital evidence but also simplifies the process of verifying its authenticity in legal proceedings.

As blockchain technology continues to evolve, its potential to revolutionize how digital evidence is handled and verified in the legal system is becoming increasingly clear.

4.4 SMART CONTRACTING TECHNOLOGY

"Smart contracts are lines of code on Blockchain technology that execute themselves after meeting the predetermined conditions", as outlined by one of India's most desirable employers. What distinguishes these devices as 'smart' is their capability to adhere to regulatory standards while carrying out predefined commands.

Blockchain technology uses smart contracts, self-executing agreements with coded terms, to ensure digital evidence's authenticity. These contracts record each transfer, creating a transparent, tamper-proof chain of custody. They can require specific actions or conditions, like multiple digital signatures, for authentication. Smart contracts can also include cryptographic hashes of the evidence, detecting any tampering instantly. By automating legal and procedural compliance, smart contracts enhance trust and transparency. All parties can verify the authenticity and integrity of digital evidence without relying on a central authority. These automated processes, encoded into contracts, establish a tamper proof record and transparency, enhancing digital evidence's authenticity.

5. CHALLENGES OF DIGITAL EVIDENCE IN INDIAN COURTS

The challenges of digital evidence in Indian courts stem from various factors, including technological complexities, legal admissibility, authenticity, and the need for specialized expertise.

5.1 RELIABILITY CONCERNS

The reliability of the computer program generating electronic evidence can be contested in a court of law. Both parties and the court have the right to question the trustworthiness of the

program producing electronic data used as evidence.

One of the most common challenges of authenticity of electronic evidence is that the parties may bring up in a trial the claim of tampering of electronic evidence. Given that the evidence is stored in electronic form, parties can allege that the electronic evidence has been altered or manipulated since its collection. Tampering with electronic evidence is a major challenge due to its vulnerability to manipulation when proper precautions are not followed.

5.2 AVAILABILITY OF INTERNET

The internet's accessibility presents several hazards pertaining to the validity and integrity of the evidence, which makes it difficult for electronic evidence to be admitted. Electronic evidence is vulnerable to unauthorized parties' interception, alteration, or manipulation when it is transferred via the internet.

For example, there is a chance that hackers or other bad actors could access and alter electronic evidence kept on a server connected to the internet. In a similar vein, there's a chance that electronic evidence sent online could be intercepted and changed in transit.

It is crucial to take the proper safety measures when gathering, storing, and sending electronic evidence to address these issues. This can entail utilizing encryption.

5.3 TECHNOLOGICAL GAP

One major obstacle is the low level of technical expertise among judges and attorneys. Many people still find that using traditional ways is more pleasant than using electronic equipment.

For many legal practitioners in India, the technical nuances of obtaining, maintaining, and presenting digital evidence are still foreign. This unfamiliarity may cause misunderstandings and errors, which could affect how cases turn out in the end.

The technological gap in Indian courts refers to the disparity between advancing digital technologies and the infrastructure, resources, and expertise available to handle digital evidence. This gap poses challenges in managing, authenticating, and admitting digital evidence. Courts lack standardized protocols for handling digital evidence, leading to inconsistencies. There is also a shortage of technical expertise to analyze digital evidence, and

keeping up with evolving technologies is difficult. Addressing this gap requires investment in technology infrastructure, training, and standardized protocols for handling digital evidence.

6. CASE STUDIES

"Tomaso Bruno and Anr. vs. State of Uttar Pradesh" The court stressed how crucial it is that the inquiry process considers scientific methods and information technology advancements. It emphasized the use of electronic evidence to establish facts and pointed out that investigating agencies might gain a great deal by using scientific and electronic evidence.

"**Anwar P.V. vs. P.K Basheer and Others"** Sections 63 and 65 of the Indian Evidence Act, 1872 have been superseded by the Supreme Court's decision that only Sections 65A and 65B control the admissibility of electronic records. It underlined that secondary electronic evidence, including information on CDs, DVDs, and pen drives, requires a Section 65B certificate. This implies that these criteria cannot be met by expert opinions under Section 45A. Nevertheless, problems include evidence that has been unlawfully obtained and the possibility of certificate-based authentication being manipulated. It's crucial to remember that, even while the given certificate attests to the source's legitimacy, it doesn't provide safe content or known control over the machine, which raises questions regarding the legitimacy of the source.

"**State vs. Mohd. Afzal and Ors."** In this case, it was decided that section 65B of the Indian Evidence Act, 1872 specifies "computer generated electronic records." Additionally, it was decided that electronic evidence is acceptable. If someone contests the veracity of computer evidence or an electronic record on the grounds of system abuse, malfunction, or interpolation, they must establish their case beyond reasonable doubt.

"Ram Singh and Ors. vs. Col Ram Singh" It will be wrong to deny the law of evidence advantages to be gained by new techniques and new devices," the ruling in this instance stated, if it can be demonstrated that the recording is accurate. It is generally advisable to exercise caution when evaluating such evidence and consider all relevant facts in each case. The court ruled that electronic evidence was acceptable if it was accompanied by measures to ensure its legitimacy.

7. SOLUTIONS FOR THE STEP AHEAD

7.1 STRENGTHEN LEGAL FRAMEWORK

The legal framework that governs the collection, preservation, and presentation of digital evidence is what makes it admissible in courts. Evidence needs to be authenticated, pertinent, and have a record of its chain of custody. There are some exceptions to the rule that hearsay is not admissible. Unless copies are approved, originals are required per the best evidence criterion. Admissibility is also impacted by privacy laws. It may be necessary to obtain expert witness on complex technological matters. This framework guarantees the validity of digital evidence and its appropriate consideration in court.

7.2 ENSURING TRANSPARENCY AND ACCOUNTABILITY

For digital evidence to be considered credible in court, accountability and transparency are essential. Clear documentation of the procedures used to gather, store, and evaluate the evidence is necessary for transparency. This contains information on the people and tools that were utilized. Accountability makes sure that individuals who handle evidence adhere to procedures and are held accountable for any errors or improper behavior. These guidelines uphold the credibility of digital evidence and the public's faith in the justice system.

7.3 PUBLIC AWARENESS CAMPAIGNS

Campaigns for public awareness can inform people about the function and significance of digital evidence in the legal system. These efforts make clear the procedures for gathering, utilizing, and admitting digital evidence in court. They debunk rumors and false beliefs, assisting people in realizing their obligations and rights with reference to digital data. These initiatives use a variety of platforms, including seminars and social media, to promote increased confidence and trust in the legal system.

7.4 ETHICAL GUIDELINES

Ethical guidelines for digital evidence ensure the integrity, authenticity, and privacy rights of individuals. They require documenting the chain of custody, using reliable methods, obtaining consent, and ensuring transparency and accountability. These guidelines maintain public trust

and confidence in the legal system and ensure the admissibility and reliability of digital evidence in court.

8. SUMMARY

As we conclude, digital evidence is admissible, but they are not free from the challenges that question their authenticity in Indian Courts. To sum up, the way digital evidence is handled in Indian courts may completely change as a result of the introduction of cutting-edge technology like blockchain. The decentralized and impenetrable characteristics of blockchain technology have the potential to greatly augment the legitimacy and admissibility of digital evidence. Blockchain can assist in resolving the issues with authenticity, integrity, and admissibility that currently plague the Indian judicial system by offering a transparent and safe way to store and validate digital data.

But the incorporation of blockchain technology into the legal system will necessitate giving serious thought to several aspects, such as technological infrastructure, legislative frameworks, and the requirement for specialized knowledge. The compatibility of blockchain technologies with current legal procedures and systems may also provide difficulties.

All things considered, despite certain obstacles, utilizing blockchain technology for digital evidence in Indian courts has a lot of potential advantages. It might result in more dependable and effective legal procedures, which would eventually improve India's access to justice system and rule of law.

10. CONCLUSION

In conclusion, blockchain technology stands out as a promising solution for enhancing the authenticity and admissibility of digital evidence in legal proceedings. Despite facing some challenges, such as reliability concerns and technological gap among individuals, the benefits it offers outweigh these obstacles.

Furthermore, blockchain can streamline the process of presenting evidence in court, reducing the time and resources required for legal proceedings. By providing a secure and accessible platform for storing and sharing evidence, blockchain can improve the efficiency and reliability of the legal system.

Overall, the potential benefits of blockchain technology for ensuring the authenticity and admissibility of digital evidence make it a valuable tool for the legal field. With further development and adoption, blockchain has the potential to revolutionize the way digital evidence is handled in legal proceedings, improving trust, efficiency, and reliability.