FORENSIC ANALYSIS OF BLOCKCHAIN, CRYPTOCURRENCY AND AI-RELATED CRIMES: A COMPARATIVE ANALYSIS OF EMERGING TRENDS IN THE ADMISSIBILITY OF DIGITAL EVIDENCE

Dr. Ramprakash Chaubey, Principal, Gyan Ganga College of Excellence (Law), Jabalpur, M.P.

ABSTRACT

The rise of blockchain, cryptocurrency, and AI has opened new doors for criminals, demanding an update to how we approach forensic investigations and digital evidence. This research compares the admissibility of digital evidence in crimes involving these technologies, specifically in India, the USA, the UK, and the EU. The study examines legal frameworks, court interpretations, and forensic practices for authenticating and presenting digital evidence from blockchain, crypto wallets, and AI systems. While India has advanced with the Bharatiya Sakshya Adhiniyam, 2023, its legal and forensic systems are still evolving compared to other nations. The findings emphasize India's need to invest in specialized training, create specific legal guidelines for new digital evidence, promote diverse authentication methods, strengthen its virtual asset legal framework, and boost international collaboration. By learning from leading foreign jurisdictions, India can improve its capacity to investigate and prosecute crimes involving these advanced digital technologies.

Keywords: Digital Evidence Admissibility, Forensic Analysis, Blockchain Crimes, Cryptocurrency Crimes, AI-Related Crimes, Comparative Law, India.

1- INTRODUCTION

Forensic science is at a crucial juncture, with technological advancements revolutionizing crime investigation but also introducing significant challenges. While innovations like DNA sequencing and digital forensics enhance accuracy, forensic practitioners face hurdles in the pursuit of justice. One major challenge is the overwhelming volume and complexity of data from modern technologies. Sifting through vast digital landscapes, network logs, and encrypted data demands advanced tools, expertise, and significant resources, often exceeding lab capacities and potentially delaying investigations. The constant emergence of new devices and software also means forensic tools can quickly become outdated, requiring substantial continuous investment in equipment, software, and training.[1]

Moreover, ensuring the integrity and authenticity of digital evidence is critical, as digital data is easily manipulated. Forensic experts must use rigorous methodologies to authenticate evidence and prove its reliability in court. Jurisdictional challenges also arise due to the global nature of technology, especially in cybercrimes that cross borders, complicating evidence gathering and admissibility in international cases.[2]

Addressing these issues requires substantial investment in specialized training for forensic professionals. Traditional expertise must now be supplemented with in-depth knowledge of computer science, network security, data analytics, and mobile device forensics. Continuous professional development is essential to equip forensic scientists to tackle the evolving technological landscape of crime effectively.[3]

2- FORENSIC ANALYSIS OF BLOCKCHAIN, CRYPTOCURRENCY AND AI-RELATED CRIMES

The widespread adoption of blockchain, cryptocurrencies, and AI has brought remarkable innovation but also a surge in sophisticated criminal activities. Investigating these crimes demands a multidisciplinary approach, combining traditional forensics with expertise in

[1] Delia Magherescu, “Challenges of the forensic science facing new technologies” 7(1) IUS ET SCIENTIA 59 (2021).

[2] Xavier Chango Llerena, Omar Flor, et.al., “Technology in Forensic Sciences: Innovation and Precision”12(8) Technologies 120 (2024).

[3] Fredesvinda Insa, “The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study” 1 Journal of Digital Forensic Practice 285-289 (2007).

cryptography, distributed ledger technology, and AI.

Blockchain and Cryptocurrency Crimes: While blockchain's transparency can aid investigations, the pseudonymous nature of cryptocurrency addresses and complex transactions pose significant challenges for attribution. Criminals use multiple wallets, mixers, and privacy-focused cryptocurrencies to obscure identities. Investigators need expertise in on-chain analysis, using specialized tools to trace transaction patterns and identify related addresses. The cross-jurisdictional nature of cryptocurrencies complicates investigations due to varying legal frameworks and difficulties in international coordination. The rise of decentralized finance (DeFi) platforms adds further complexity, creating new avenues for illicit activities like scams and flash loan attacks, requiring specialized forensic skills to unravel.

AI-Related Crimes: Artificial intelligence presents unique forensic challenges, acting as both a criminal tool and a target. AI can facilitate crimes such as generating deepfake videos for fraud or disinformation, or powering phishing attacks. Analyzing these requires identifying AI-generated content, tracing its origin, and understanding underlying algorithms, often involving metadata analysis and reverse-engineering AI models.

Conversely, AI systems can be targets of attacks like data poisoning, model theft, or adversarial attacks. Investigations involve analyzing system logs and identifying anomalies in AI behavior, demanding expertise in machine learning, cybersecurity, and data science. The "black box" nature of some AI models, where understanding their decision-making is difficult, is a significant hurdle. Developing explainable AI (XAI) techniques is crucial for forensic investigations to uncover malicious manipulation.

3- EMERGING STRATEGIES IN FORENSIC ANALYSIS

Combating crimes involving blockchain, cryptocurrency, and AI demands a multi-pronged strategy. Specialized training for law enforcement in these technologies is crucial, alongside developing advanced forensic tools through collaboration between forensic scientists, developers, and academics.

Given the borderless nature of these crimes, enhanced interagency and international cooperation and public-private partnerships with blockchain analytics firms, crypto exchanges, and AI research institutions are vital. Furthermore, establishing clear legislative and regulatory frameworks is essential. Finally, standardization and best practices for collecting and analyzing digital evidence related to these technologies are needed to ensure forensic findings are reliable and admissible in court.[4]

4- EMERGING TRENDS IN THE ADMISSIBILITY OF DIGITAL EVIDENCE

The digital revolution has profoundly impacted crime and litigation, making digital evidence—from emails to cloud data—increasingly vital in legal proceedings. Despite its volatility and susceptibility to alteration, courts are increasingly accepting and relying on digital evidence, recognizing its probative value due to the ubiquitous nature of digital footprints in modern life. However, this reliance comes with heightened scrutiny regarding authenticity and integrity.[5] Unlike physical evidence, digital data is easily modified, demanding robust chain of custody documentation for meticulous collection, preservation, and analysis to prevent tampering.

Metadata, or "data about data," is also gaining prominence. This contextual information—like creation times, authors, and locations—is crucial for corroborating or refuting claims, making forensic tools for metadata extraction vital. Cloud computing and distributed data storage pose unique challenges for evidence collection across multiple servers and jurisdictions. Legal frameworks are evolving to facilitate lawful access to cloud data, often requiring international cooperation and addressing privacy and jurisdictional boundaries. The admissibility of social media evidence is another rapidly developing area. Despite its potential relevance, issues like user authentication, privacy settings, and potential manipulation necessitate careful scrutiny. Courts are working to establish clear guidelines for authenticating social media content.

The emergence of Artificial Intelligence (AI) and Machine Learning (ML) offers opportunities for analyzing large datasets and reconstructing information. However, the "black box" nature of some AI algorithms raises concerns about transparency and reliability, pushing courts to demand greater explainability for AI-powered forensic tools. Legal systems are now emphasizing proportionality and reasonableness in digital evidence collection, advocating for targeted and relevant data acquisition to avoid overly broad searches. Finally, judicial education and technological literacy are becoming critical. Judges and legal professionals need a

[4] Andrew M. Smith and Tess M.S. Neal, "The distinction between discriminability and reliability in forensic science" 61(4) Science & Justice 319 (2021).

[5] Ms. Sadhna Gupta & Ms. Meghali Das, "Criminal Investigation of Electronic Evidence: Challenges Faced with Digital Forensics" 2(2) JFJ 1 (2023).

fundamental understanding of digital technologies and forensic principles to effectively evaluate digital evidence in the evolving digital age.

5- EMERGING TRENDS IN THE ADMISSIBILITY OF DIGITAL EVIDENCE IN INDIA

India's rapid digital transformation has made digital evidence critical in legal proceedings, despite challenges like susceptibility to alteration and authentication complexities. A significant trend is the strengthened legislative framework, primarily through the Information

Technology Act, 2000,[6] and Section 65B[7] of the Indian Evidence Act, 1872, which provides a mechanism for admitting electronic records. Recent interpretations aim to streamline procedural requirements, acknowledging practical challenges with voluminous digital data.

Indian courts are increasingly emphasizing the authenticity and integrity of digital evidence due to its manipulability. This necessitates a rigorous examination of the chain of custody, with forensic procedures and expert analysis playing a crucial role in substantiating integrity. Metadata's admissibility is also gaining traction, as courts recognize its contextual value for corroborating digital content.

Social media evidence presents unique challenges, with courts developing guidelines for authentication often requiring corroborating evidence or forensic analysis. The rise of cloud computing and cross-border data storage complicates evidence access and admissibility, highlighting the need for Mutual Legal Assistance Treaties (MLATs) and international cooperation.

The emergence of Artificial Intelligence (AI) and Machine Learning (ML) in investigations introduces new complexities. While AI can analyze vast datasets, the admissibility of solely AI-derived evidence faces debate due to concerns about transparency, potential biases, and lack of human oversight. The legal framework will likely evolve to validate AI-generated findings.

Indian courts are also stressing relevance and necessity in digital evidence admissibility, scrutinizing overly broad data requests. Finally, there's a growing recognition for enhanced

[6] The Information Technology Act, 2000 (Act 21 of 2000).
[7] The Indian Evidence Act, 1872 (Act 1 of 1872), s. 65B.

digital literacy within the judiciary and legal fraternity to effectively evaluate digital evidence in the evolving digital age.

5.1- FORENSIC ANALYSIS OF BLOCKCHAIN, CRYPTOCURRENCY AND AI RELATED CRIMES:

The rise of blockchain, cryptocurrencies, and AI has introduced new criminal avenues, demanding advanced forensic analysis and legal frameworks. India's legal system is adapting, with several key trends emerging in how it handles these technology-related crimes.

Emerging Legal Trends in India: Indian courts are increasingly recognizing the probative value of digital evidence, including blockchain transaction records, cryptocurrency wallet information, and AI-generated content. There's a strong focus on authentication and integrity, requiring robust chain of custody and specialized tools to ensure evidence reliability. Cryptocurrency forensics is evolving, with law enforcement developing capabilities in on-chain analysis to trace transactions and link virtual identities to real-world individuals. As AI becomes implicated in crimes, legal frameworks are beginning to grapple with the admissibility of AI-generated evidence (e.g., deepfakes) and evidence related to attacks on AI systems. Given the borderless nature of these crimes, cross-jurisdictional cooperation with international counterparts is becoming increasingly vital.

Impact of the Bharatiya Sakshya Adhiniyam, 2023 (BSA): The Bharatiya Sakshya Adhiniyam, 2023,[8] marks a significant modernization of India's evidence law. The BSA broadens the definition of "document" and "evidence" to explicitly include electronic and digital records and statements given electronically, crucial for admitting blockchain data, cryptocurrency information, and AI-generated reports. A significant shift is the classification of electronic records as "primary evidence" if produced from proper custody, streamlining their admissibility. However, the BSA retains the requirement for certificates for electronic records under Section 63,[9] ensuring authenticity and reliability, especially for complex digital evidence. The inclusion of "statements given electronically" as oral evidence and the recognition of digital signatures further strengthen the legal basis for authenticating digital evidence.

[8] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[9] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63.

Challenges and Future Directions: Despite these progressive changes, several challenges remain. The technical complexity of these technologies demands specialized forensic expertise that is still developing. The rapid pace of technological evolution necessitates continuous updates to legal frameworks. Cross-border legal hurdles in obtaining evidence and navigating differing international standards persist. Ensuring data privacy while accessing digital evidence requires careful consideration. Finally, judicial capacity building is crucial, requiring continuous training for judges and legal professionals to understand the technical nuances of digital evidence and effectively navigate this evolving landscape.

6- EMERGING LEGAL TRENDS IN THE ADMISSIBILITY OF DIGITAL EVIDENCE AND FORENSIC ANALYSIS OF TECHNOLOGY-RELATED CRIMES IN MAJOR FOREIGN COUNTRIES

Major foreign countries are rapidly adapting their legal frameworks and forensic capabilities to address the challenges of digital evidence and crimes involving blockchain, cryptocurrency, and AI.[10]

Admissibility of Digital Evidence: A key trend is the broadening definition and acceptance of electronic and digital records as legitimate evidence in the US, UK, and EU. There's a strong emphasis on authentication and integrity, with legal frameworks like the US Federal Rules of Evidence and the UK's Criminal Justice Act 2003 stressing verifiable processes and robust chain of custody.[11] Many jurisdictions are developing specific legal frameworks, such as the EU's eIDAS Regulation, for digital evidence and cybercrime. Courts are also increasingly encountering novel forms of digital evidence, including blockchain records and AI-generated content, leading to evolving legal precedents, particularly concerning their reliability and

[10] Pranjal Chaturvedi, "Emerging Technology Trends And Its Effect On Criminal Justice System", LiveLaw, 6 February 2025, available at <https://www-livelaw-in.cdn.ampproject.org/v/s/www.livelaw.in/amp/law-firms/law-firm-articles-/criminal-justi ce-system-central-bureau-of-india-cyber-crime-forensic-artificial-intelligence-biometric-metadata-283122?amp_ gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=From%20%251%24s&aoh=1746636 3241469&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fwww.livelaw.in%2Fla w-firms%2Flaw-firm-articles-%2Fcriminal-justice-system-central-bureau-of-india-cyber-crime-forensic-artificia l-intelligence-biometric-metadata-283122> (last visited on 6 July 2025).

[11] Jose González-Rodríguez, Mark G Baron, et.al., "Forensic science in UK. Part III: Regulation of Forensic Science in England and Wales. The role of the Forensic Science Regulator" 32(1) Forensic Science Review 3-4 (2020).

potential for manipulation.[12] The global nature of digital data necessitates cross-border data access through agreements like MLATs, though differing legal standards remain a challenge.

Forensic Analysis of Technology-Related Crimes: Major foreign countries are developing specialized forensic capabilities. Dedicated cryptocurrency forensic units have been established in agencies like the FBI and NCA, employing blockchain analytics tools (e.g., Chainalysis) for on-chain analysis and tracing illicit funds. New forensic approaches are being developed to address AI-facilitated crimes, such as detecting AI-generated content and analyzing malicious algorithms. Countries are also adapting legal frameworks for the seizure and confiscation of cryptocurrencies. International collaboration and information sharing through organizations like Interpol and Europol are paramount. Finally, public-private partnerships with crypto exchanges and blockchain analytics firms are becoming increasingly important for providing expertise and data access in investigations.

7- COMPARATIVE ANALYSIS BETWEEN INDIAN AND FOREIGN COUNTRIES

The rise of blockchain, cryptocurrencies, and AI presents global challenges for forensic analysis and the admissibility of digital evidence. A comparative look at India and major foreign countries reveals both progress and areas for further development. Here is the comparative analysis for admissibility of digital evidence:

Legal Frameworks: In India, the Information Technology Act, 2000, and the new Bharatiya Sakshya Adhiniyam, 2023 (BSA), govern digital evidence. The BSA aims to streamline admissibility by classifying electronic records as primary evidence, subject to certification. In contrast, countries like the USA (Federal Rules of Evidence), UK (Criminal Justice Act 2003),

Pranjal Chaturvedi, "Emerging Technology Trends And Its Effect On Criminal Justice System", *LiveLaw,* 6 February 2025, *available at* <https://www-livelaw-in.cdn.ampproject.org/v/s/www.livelaw.in/amp/law-firms/law-firm-articles-/criminal-justi ce-

[12] 1Dr. R. Bharath Kumar, Dr. Abhishek Baplawat, et.al., "Artificial Intelligence in Forensic Sciences: Bridging Systematic Challenges with Next-Generation Applications" 14(5s) J. NEONATAL SURG 640 (2025).

and EU (eIDAS Regulation) have more established and broader frameworks, often emphasizing authentication through witness testimony, system integrity, and reliable processes.

Authentication and Integrity: Indian courts increasingly demand robust authentication and integrity proof for digital evidence, focusing on Section 65B certificates (now Section 63 BSA). Foreign courts, however, employ a wider range of authentication methods, including expert testimony, hash value comparisons, and digital forensic reports, offering greater flexibility than India's historically certificate-centric approach.

Novel Forms of Digital Evidence (Blockchain, AI): India's legal framework for blockchain records and AI-generated evidence is nascent, with specific precedents still developing despite the BSA's broadened definition of "electronic record." Foreign jurisdictions like the USA and UK are seeing emerging case law that addresses the admissibility of blockchain evidence, often focusing on its immutability, while carefully scrutinizing AI-generated evidence for authorship and manipulation.

Metadata: Both India and foreign countries increasingly recognize metadata's probative value in corroborating digital evidence, with forensic analysis routinely involving its extraction and presentation.

Here is the comparative analysis for forensic analysis of technology-related crimes

Cryptocurrency Forensics: India is in the early stages of developing specialized cryptocurrency forensic expertise, with law enforcement beginning to establish dedicated units and collaborate with analytics firms. Major foreign countries, including the USA, UK, EU, and Canada, have made significant strides, with dedicated units (e.g., FBI, NCA, Europol) utilizing advanced blockchain analytics tools and having more established legal frameworks for seizing and confiscating cryptocurrencies.

AI-Related Crime Forensics: India's capabilities in analyzing AI-related crimes (e.g., deepfakes, data poisoning) are still nascent. Foreign jurisdictions are investing heavily in R&D to develop techniques for deepfake detection, analyzing malicious AI algorithms, and tracing AI-driven attacks, often in collaboration with research institutions and private companies.

Legal Framework for Seizure and Confiscation: While India's framework for asset seizure, including cryptocurrencies, is evolving (e.g., through PMLA), foreign countries like the USA have more specific legislation and established legal precedents for the seizure and forfeiture of digital assets, with clearer definitions of virtual assets as property.

International Cooperation: India is increasing its engagement in international cooperation via MLATs, but navigating differing legal standards remains a challenge. Major foreign countries have well-established international collaborations (Europol, Interpol) for combating transnational cybercrime involving these technologies.

While India has progressed significantly with the BSA and increasing recognition of digital evidence, a comparative analysis highlights areas where it lags behind more mature foreign jurisdictions. Key areas for India's development include investing in specialized training and infrastructure for blockchain, cryptocurrency, and AI forensics; developing more specific legal guidelines for novel digital evidence; enhancing international cooperation and streamlining cross-border data access; establishing clearer legal frameworks for virtual asset seizure; and fostering greater public-private partnerships to bolster forensic capabilities.

8- JUDICIAL APPROACH

Indian courts have significantly shaped the admissibility of digital evidence. The landmark

Anvar P.V. vs. P.K. Basheer & Ors.[13] established the mandatory Section 65B(4) certificate (now Section 63 of BSA, 2023) for electronic records as secondary evidence, crucial for proving blockchain, cryptocurrency, and AI data authenticity. While ***Shafhi Mohammad vs. State of Himachal Pradesh,***[14] offered slight relaxation when the device isn't possessed by the

adducing party, ***Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal & Ors.,***[15][16] reiterated the certificate's importance. Crucially, ***State of Karnataka vs. T. Naseer @ Nasir @ Thandiantavida Naseer @ Umarhazi @ Hazi & Ors.,***[16] clarified that the Section 65B certificate isn't required for primary electronic evidence and can be produced at any trial stage, vital for original blockchain records or direct AI system data. ***Thana Singh vs. Central Bureau***

[13] (2014) 10 SCC 473.

[14] (2018) 2 SCC 801.

[15] (2020) 7 SCC 1.

[16] (11) TMI 1211 (SC).

of Narcotics,[17] recognized digital charge sheets, highlighting early judicial acceptance of digital formats.

Specific Indian judgments exclusively on blockchain and cryptocurrency forensic analysis are still emerging. However, cases involving cyber fraud and money laundering with cryptocurrencies are increasing, with forensic analysis of crypto transactions playing a vital role. The Supreme Court's decision to suppress the RBI's crypto trading ban (***Internet and Mobile Association of India v. Reserve Bank of India,***[18]***)*** indicates judicial engagement with crypto legality, indirectly influencing how related evidence is handled. Similarly, direct judgments on AI-related crime forensics (e.g., deepfakes, AI cyberattacks) are in nascent stages. Precedents from cases involving general misuse of technology and manipulation of digital media will inform the approach to more sophisticated AI evidence.

Foreign judgments offer valuable insights. ***United States v. Silk Road,***[19] showcased the admissibility of blockchain transaction records and the use of forensic tools to trace Bitcoin. ***R v. Goscinski***,[20] though about WhatsApp, highlighted authentication principles relevant to AI-facilitated communications. The ***European Court of Human Rights' Szabó and Vissy v. Hungary***[21] emphasized data protection and legal safeguards for accessing digital evidence from blockchain and AI systems. Rulings on eIDAS Regulation in EU member states provide a framework for trusting digital transactions. Emerging US and EU case law on AI in policing and facial recognition raises questions about the admissibility of evidence from potentially biased AI algorithms, underscoring the need for scrutiny of AI-driven forensic tools.

9- CONCLUSION AND SUGGESTIONS

Global trends show increasing reliance on digital evidence, with India's Bharatiya Sakshya Adhiniyam, 2023 (BSA) marking progress. However, a gap remains compared to major foreign countries like the USA, UK, and EU, which boast broader legal frameworks, more flexible authentication methods, and mature forensic capabilities for blockchain, cryptocurrency, and AI-related offenses. These nations also have established mechanisms for seizing digital assets and robust international cooperation. India's evolving legal landscape, while progressive, needs

[17] (2013) 2 SCC 590.
[18] (2020) 10 SCC 693).
[19] 14-cr-00066 (S.D.N.Y.).
[20] [2018] EWCA Crim 2029 (UK).
[21] no. 24562/16 (2021).

further development to effectively combat sophisticated, technologically driven crimes. Here are the suggestions to enhance India's capabilities:

1. Invest in specialized training and infrastructure for blockchain, cryptocurrency, and AI forensics.

2. Develop specific legal guidelines for novel digital evidence like blockchain records and AI-generated content.

3. Promote diverse authentication methods beyond strict certification, aligning with international best practices.

4. Strengthen legal frameworks for virtual assets, clarifying seizure and confiscation procedures.

5. Enhance international cooperation through MLATs and other agreements for cross-border investigations.

6. Foster public-private partnerships with tech companies and academia for access to tools and expertise.

7. Invest in research and development for advanced forensic tools in blockchain, crypto, and AI analysis.

8. Enhance judicial and legal professional digital literacy through comprehensive training programs.