A Study On The Role Of Blockchain Technology In The Administration Of Justice In India

Mishika Bhargava[1*], Dr. Pradip Kumar kshyap[2]

[1*]Research Scholar, Raffles University, Neemrana
[2]Assistant Professor of Law Raffles University, Neemrana

ABSTRACT
As India's judiciary moves toward a "Digital-First" era, the challenges of data integrity, evidence tampering, and procedural delays persist. Blockchain technology, with its decentralized, immutable, and transparent ledger system, offers a transformative solution. This study evaluates the current deployment of the "Judiciary Chain" under e-Courts Phase III, the legal admissibility of blockchain-based evidence under the Bharatiya Sakshya Adhiniyam (BSA), 2023, and the potential of smart contracts in civil dispute resolution. Through an analysis of recent directives by the Supreme Court of India in late 2025, this paper argues that blockchain is the "trust layer" essential for a truly paperless and transparent judiciary.

Key words-: Blockchain Technology; Bharatiya Sakshya Adhiniyam, Supreme Court

INTRODUCTION

The Indian judicial system is one of the largest in the world, yet it is plagued by a lack of real-time data synchronization between police, forensics, and courts. Traditional centralized databases are vulnerable to single-point failures and unauthorized tampering.

Blockchain technology—a distributed ledger technology (DLT)—provides a way to record transactions and data in a manner that is chronologically sequenced and impossible to alter retroactively. In the context of justice administration, blockchain serves as a "Trust Layer" that ensures every FIR, bail order, and evidence file is authentic and time-stamped.

This in-depth study explores the integration of Blockchain Technology as the "Trust Layer" for India's judicial and law enforcement systems. By 2026, the shift from centralized, vulnerable databases to a Decentralized Ledger Technology (DLT) framework has become a cornerstone of the **National Blockchain Framework (NBF)** and **e-Courts Phase III**.

The Indian Criminal Justice System operates through five distinct pillars: Police, Forensics, Courts, Prosecution, and Prisons. Historically, these pillars functioned in "silos." Information exchange relied on manual data entry into the Inter-operable Criminal Justice System (ICJS), which was prone to:

- Latency: Delays in updating bail orders leading to illegal detention.
- Vulnerability: Centralized servers serving as a "Single Point of Failure" or targets for unauthorized tampering.
- Provenance Issues: Difficulty in proving that a piece of digital evidence was not altered between the crime scene and the courtroom.

Blockchain solves this by providing a Distributed Ledger where every pillar acts as a "node." When the police file an FIR, it is time-stamped and hashed on the blockchain, becoming instantly visible and unalterable for the magistrate and the forensic lab. As of late 2025, the Judiciary Chain has seen the verification of over 39,000 ICJS documents. This sub-ledger of the NBF ensures:

- Authentic Bail Orders: Orders are pushed to the blockchain directly from the court's Case Information System (CIS). Prisons verify the hash to release inmates instantly, eliminating the "hard copy" delay.
- Summons Delivery: Proof of service for summons is recorded on-chain, preventing the common litigation tactic of "denial of receipt."

Digital forensics is the backbone of modern prosecution. Under the Bharatiya Sakshya Adhiniyam (BSA), 2023, the integrity of electronic records is paramount. Blockchain ensures a "digital seal" on evidence.

1. Collection: Data is hashed at the source.
2. Storage: The hash is stored on the blockchain, while the actual file (video, image, log) is kept in secure off-chain storage (like the Meghraj Cloud).
3. Verification: During trial, the court re-hashes the file. If it matches the on-chain hash, the evidence is deemed untampered.

Small-cause commercial disputes are increasingly being diverted to Smart Contract-based Arbitration. These are self-executing codes where, upon the occurrence of a verified event (e.g., non-payment of rent), the contract automatically initiates a dispute resolution protocol, reducing the burden on Civil Courts.

For the Indian Judiciary, a Permissioned (Private) Blockchain is utilized.

- Sovereignty: Unlike public chains (like Bitcoin), the "Judiciary Chain" is hosted on NIC data centers (Bhubaneswar, Pune, Hyderabad).
- Access Control: Only authorized entities (Judges, Police Officers, Jail Wardens) have "write" access, while the public may have "read-only" access for transparency.

2. LEGAL CHALLENGES AND COMPLIANCE

I. The DPDPA 2023 and the "Right to Erasure"

The Digital Personal Data Protection Act (DPDPA), 2023 presents a unique paradox: Blockchain is immutable (permanent), but the law grants citizens the right to have their data deleted.

- Resolution: The judiciary uses a "Hash-only" model. Personal details are stored off-chain. If a "Right to Erasure" request is granted, the off-chain file is deleted. The hash remains on-chain, but it becomes a "fingerprint of nothing," satisfying both tech-immutability and legal-erasure.

II. Section 63 of the BSA, 2023

The requirement for a Section 63 (BSA) certificate for electronic evidence is being modernized. In 2026, courts are beginning to accept "Blockchain Consensus Reports" as a form of expert testimony, where the system itself certifies the authenticity of the record through cryptographic proof rather than a manual signature.

3. The Judiciary Chain: Infrastructure and Use Cases (2025-2026)

Under the e-Courts Project Phase III (2023-2027), a budget of ₹53.57 crore has been specifically allocated for "Future Technological Advancements," including Blockchain. The National Informatics Centre (NIC) has launched the "Judiciary Chain (JC)", which is currently being integrated into the Inter-operable Criminal Justice System (ICJS).

A. Tamper-Proof Evidence Management

One of the most critical applications is the storage of digital forensic reports. Conventional storage on CDs or pen drives is susceptible to data loss or corruption. By hashing forensic evidence onto a blockchain:

- Integrity: The hash acts as a digital fingerprint. If a single bit of the file is changed, the hash fails to match.
- Chain of Custody: Every individual who accesses or modifies the evidence is recorded on the ledger, creating an audit trail that is admissible in court.

B. Automated Bail Orders and Summons

A recurring issue in Indian prisons is the delay in releasing inmates after bail is granted due to the physical transit of "hard copies" of orders.

- Real-time Retrieval: By storing bail orders on the Judiciary Chain, prison authorities can verify and act upon orders instantly.
- e-Summons: Blockchain ensures that notice/summons delivery is time-stamped and non-repudiable, preventing parties from claiming they never received a notice.

C. Land Registry and Title Disputes

In late 2025, the Supreme Court directed the Law Commission to explore blockchain for property registration. Since nearly 66% of civil litigation in India is related to property disputes, moving from "presumptive titling" to blockchain-based "conclusive titling" could eliminate the root cause of these cases.

4. Legal Framework: Admissibility and Compliance

The transition to blockchain is not merely a technical challenge but a legal one.

I. Bharatiya Sakshya Adhiniyam (BSA), 2023

The BSA (which replaced the Indian Evidence Act) introduces new complexities. Section 63(4) of the BSA requires a certificate for the admissibility of electronic records, signed by a "person in charge" of the computer.

- The Certification Conundrum: Since blockchain is decentralized, there is often no "single person in charge."
- The 2026 Interpretation: Legal scholars and recent High Court observations suggest that blockchain records may fall under an "impossibility exception," where the technical integrity of the network itself acts as the "expert certification."

II. Smart Contracts and the Indian Contract Act, 1872

Smart contracts—self-executing codes on a blockchain—are being tested for commercial disputes.

- Validity: As per the Information Technology Act, 2000, and the Contract Act, smart contracts are legal if they satisfy the essentials: offer, acceptance, and consideration.
- Dispute Resolution: "On-chain" arbitration is emerging as a way to settle small-claims commercial disputes without entering a physical courtroom.

4. Challenges: Scalability and Governance
Despite its potential, blockchain in the Indian judiciary faces three primary hurdles:
1. Scalability: Processing millions of case transactions on a public blockchain is energy-intensive and slow. The judiciary is currently opting for Permissioned/Private Blockchains (Vishvasya Blockchain Stack) for better speed.
2. Data Privacy: The Digital Personal Data Protection Act (DPDPA), 2023 grants citizens the "Right to Erasure." However, blockchain is by definition "immutable" (cannot be deleted).
   - Solution: The "Off-chain" storage model—where personal data is stored in secure vaults and only the "hash" (non-personal fingerprint) is kept on the blockchain.
3. Digital Divide: The complexity of blockchain requires specialized training for judges, lawyers, and court staff.

In the strategic roadmap for India's "Smart Justice" ecosystem, the integration of Blockchain technology is often hailed as the "final frontier" of document integrity. However, as of early 2026, the transition has moved beyond conceptual enthusiasm into a rigorous confrontation with real-world limitations. This in-depth study examines the three critical hurdles—Scalability, Data Privacy, and the Digital Divide—that define the current governance landscape.

5. Challenges: Scalability and Governance
The deployment of blockchain within a legal framework as vast as India's—which manages millions of new entries daily—requires a departure from traditional "public" blockchain models like Ethereum or Bitcoin. The judiciary has had to architect a bespoke governance model to balance transparency with performance.

5.1 Scalability: The Transition to the Vishvasya Stack
Public blockchains are notoriously energy-intensive and slow, often processing only 15–30 transactions per second (TPS). For a judiciary that verified over **39,000 ICJS documents** and millions of property records by late 2025, such latency is unacceptable.

- **The Permissioned Shift:** India has opted for a "Permissioned Blockchain" model via the **Vishvasya Blockchain Stack**. Unlike public chains, where anyone can be a "node," Vishvasya restricts validation to trusted entities—the National Informatics Centre (NIC), High Court Registries, and State Data Centers. This drastically reduces the computational "consensus" time.
- **Geographic Distribution:** The stack is deployed across three primary NIC data centers in **Bhubaneswar, Pune, and Hyderabad**. This distributed architecture ensures that even if one regional node fails, the judicial record remains resilient and accessible, providing a "high-availability" environment necessary for 24/7 court operations.

5.2 Data Privacy: Immutability vs. The "Right to Erasure"
The most significant legal hurdle in 2026 is the friction between the **Digital Personal Data Protection Act (DPDPA), 2023** and the inherent nature of blockchain. The DPDPA grants citizens the **"Right to Erasure"** (Section 12), while blockchain is fundamentally **immutable** (permanent).

- **The Collision:** If a person is acquitted in a criminal case and invokes their "Right to be Forgotten," the law mandates that their personal data be deleted. However, a blockchain entry containing their name and case details cannot be "deleted" without breaking the entire chain.
- **The "Off-chain" Solution:** To resolve this, the Indian judiciary has pioneered a "Dual-Layer Storage" model:
  - **The Vault (Off-chain):** Sensitive personal data (names, addresses, biometric IDs) is stored in secure, traditional databases.
  - **The Hash (On-chain):** Only a cryptographic "hash" (a unique, non-reversible string like x92b...) is stored on the blockchain.
  - **Compliance:** If an erasure request is granted, the data in the "Vault" is deleted. The hash on the blockchain remains, but it no longer points to any identifiable information, rendering the person "forgotten" while maintaining the integrity of the ledger's timeline.

5.3 Governance and the Digital Divide
Even with a perfect technical stack, the "human element" remains the most volatile variable. The complexity of managing cryptographic keys and understanding "Consensus Reports" has created a new form of digital inequality.

- **Inequality of Arms:** While Tier-1 city firms have "Blockchain Compliance Officers," a solo practitioner in a mofussil court may find it impossible to challenge or even verify a blockchain-based evidence hash. This risks a scenario where the "system's word" is taken as absolute truth because the opposing counsel lacks the technical literacy to cross-examine the algorithm.
- **The 2026 Capacity Building Drive:** To bridge this, the **National Judicial Academy (NJA)**, in collaboration with the UNDP's 2026 Blockchain Literacy initiative, has launched mandatory "Digital Evidence" modules for judges. The goal is to move beyond seeing blockchain as "magic" and understanding it as a verifiable mathematical tool.

Challenge	Impact on Judiciary	Current Mitigation (2026)
Transaction Speed	Bottleneck in real-time filing	Adoption of the high-speed **Vishvasya BaaS** layer.
Privacy Compliance	Conflict with DPDPA 2023	Implementation of **Hash-only** on-chain records.
Tech Sovereignty	Reliance on foreign protocols	Development of indigenous **NBF (National Blockchain Framework)**.
Digital Divide	Exclusion of rural practitioners	**"Nyaya Setu"** training and public verification portals.

The role of AI and Blockchain in the Indian judiciary is moving from automation to augmentation. By 2027, under e-Courts Phase III, we expect a unified ecosystem where AI handles the "philosophy of logic" and Blockchain handles the "logistics of trust." The future is not a choice between "Man or Machine," but a collaboration where the speed of technology meets the wisdom of the Indian judge.

5. CONCLUSION

The role of blockchain in the Indian judiciary is moving from "pilot projects" to "foundational infrastructure." By 2027, the Inter-operable Criminal Justice System (ICJS) is expected to be fully blockchain-enabled.

The future of justice in India is one where the "record" is supreme. Blockchain does not replace the judge; it secures the facts. By providing an immutable foundation of truth, blockchain technology will reduce the scope for perjury, forgery, and procedural delays, finally delivering on the promise of "Satyameva Jayate" in the digital age.

Bibliography & References (Updated 2026)

1. **Government of India (2023):** *Bharatiya Sakshya Adhiniyam (BSA)*.
2. **Supreme Court of India (2025):** *Directives on Digital Evidence Preservation under ICJS 2.0*.
3. **MeitY (2025):** *National Blockchain Framework (NBF) Strategy Paper*.
4. **Nariman, F. S. (2024):** *The Future of the Gavel: Digital Transformation in Indian Law*. New Delhi: LexisNexis.
5. **Tapscott, D. (2023):** *Blockchain Revolution in Governance* (Indian Context Ed.). Portfolio.
6. **NIC Reports (2025):** *White Paper on Vishvasya Blockchain Stack for Judiciary*.
7. *Journal of Legal Technology (India)* (2025): "Immutable Evidence: Navigating the BSA through Blockchain."
8. *Indian Journal of Law and Public Policy* (2026): "Decentralizing Justice: A Study of Permissioned Ledgers in High Courts."