iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74242

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IX Sep 2025- Available at www.ijraset.com

Blockchain and Decentralized Digital File Management for Transparent and Inclusive Governance in India

Dineshkumar Kumawat[1], Shruti Yadav[2]
[1]*Department of Information Technology and Mathematics, The S.I.A. College of Higher Education,*
[2]*Dombivli Gymkhana Road, Dombivli (E), Dist. Thane, PIN 421 203*

Abstract: ***Governance in India faces persistent challenges of transparency, accountability, and accessibility across federal, state, and local levels. Traditional file and records management systems often suffer from inefficiencies, tampering risks, and limited inclusivity due to linguistic barriers. This research proposes a Digital File and Records Management System (DFRMS) that leverages blockchain (Hyperledger Fabric) and decentralized storage (IPFS) to redefine public administration transparency. The system integrates MeriPehchaan single sign-on for identity-bound access, automated redaction pipelines for privacy, and multilingual dashboards for inclusivity. Comparative analysis with Estonia, Georgia, and Dubai demonstrates global feasibility. The blueprint aligns with India's IT Act, RTI Act, and Digital India Mission, offering a scalable, citizen-centric governance framework.***

Keywords: e-Governance, Blockchain, IPFS, MeriPehchaan, RTI, Transparency, Digital India, Public Administration

I. INTRODUCTION

The rapid pace of global digitalization has placed unprecedented emphasis on ensuring secure and transparent governance systems. Advances in e-governance, public administration, and blockchain technology have made new forms of citizen-centric recordkeeping possible while simultaneously raising challenges of privacy, interoperability, and accountability. India's governance ecosystem operates at Union, State, and Local levels, generating vast volumes of official records, notes, and annexures. Historically, records were maintained manually in physical registries, vulnerable to tampering, misplacement, and bureaucratic delays. With the advent of information technology, efforts such as the National Informatics Centre's eOffice, DigiLocker, and RTI portals attempted to digitize government workflows. However, these systems remain fragmented, with records scattered across silos, limited interoperability, and insufficient guarantees of authenticity. Citizens still encounter long delays and inconsistencies in accessing records, while officials face challenges in ensuring secure, tamper-proof provenance.

Global digitalization trends highlight the need for verifiable, transparent, and inclusive systems. Estonia's adoption of the KSI blockchain to ensure integrity of e-government registries, Georgia's blockchain-anchored land registry, and Dubai's regulatory-backed Paperless Strategy exemplify transformative applications. India's context, however, introduces unique challenges: a multilingual population spanning 22 scheduled languages, federated administrative structures, and legal frameworks like the Information Technology Act (2000, amended 2008) [1–3] and the Right to Information (RTI) Act (2005) [4]. The study presents a blockchain-enabled Digital File and Records Management System (DFRMS) that integrates provenance mechanisms, decentralized IPFS storage, and MeriPehchaan-linked role-aware access.

II. PROBLEM IDENTIFICATION

Despite decades of reforms, record-keeping in India remains fragmented. Paper files still dominate, while digital systems often function in isolation. Key challenges include tampering risks, delays in RTI responses, lack of multilingual accessibility, and weak admissibility of digital evidence in courts. Incidents such as Aadhaar-related privacy breaches highlight tensions between administrative efficiency and citizen trust, while the discontinuation of TradeLens underscores the risks of unsustainable consortium governance. Without verifiable, tamper-proof, and inclusive systems, both citizen confidence and administrative efficiency are compromised. The proposed blockchain-enabled Digital File and Records Management System (DFRMS) addresses these gaps by integrating blockchain proofs, decentralized file storage, and federated identity access with audit-ready workflows.

III. LITERATURE SURVEY

A. Literature Review

The Cadbury Report (1992) [5] is a landmark in corporate governance, establishing disclosure, accountability, and control as fundamental pillars. It conceptualizes governance as more than compliance, framing transparency and oversight as mechanisms to ensure organizational integrity. Its contribution lies in demonstrating how disclosure fosters trust—an insight highly relevant to the design of public record systems. However, the report is limited in scope to corporate boards and assumes centralized decision-making, making direct transferability to India's federated bureaucratic structures problematic. Moreover, it does not address citizen–state transparency as mandated under the Right to Information (RTI) Act.

Nakamoto (2008) [6] introduced blockchain as a decentralized, immutable ledger, addressing the double-spending problem in digital currencies. Its proof-of-work consensus created a paradigm for tamper-proof recordkeeping without reliance on trusted intermediaries. For governance, the key contribution is the demonstration that immutability can provide verifiable trust in records. However, immutability also generates conflicts with privacy and data protection regimes, where rectification or erasure of sensitive data is legally required.

The Second Administrative Reforms Commission (2009) [7] emphasized citizen-centric governance in its 12th report, Citizen-Centric Administration—The Heart of Governance. It recommended transparency, accountability, and administrative reforms to build citizen trust. Although it provides strong policy direction, the report lacks specific technical solutions for achieving verifiable, tamper-proof digital records. For digital governance frameworks, it provides normative justification but requires translation into technology-enabled models.

Buterin (2013) [8] expanded on Nakamoto's foundation with Ethereum, introducing smart contracts for programmable logic. This concept is directly relevant to governance, where automated access control and notarization policies are required. However, the paper does not discuss governance in federated states or inter-agency coordination, leaving a gap in its applicability to India. Its contribution lies in enabling policy logic, but real-world adaptation demands governance mechanisms for multi-agency workflows.

Eccles, Ioannou, and Serafeim (2014) [9] empirically demonstrate the correlation between corporate transparency and organizational performance. Their findings confirm that disclosure improves efficiency and trust, providing empirical grounding for transparency as a performance driver. While this study offers strong evidence, it focuses exclusively on corporate sustainability and ignores the complexities of government transparency, inclusivity, or citizen accountability.

Swan (2015) [10] surveys blockchain as a socio-technical phenomenon, cataloging its potential applications beyond finance. The book highlights transparency and decentralization as core benefits. However, it provides little discussion of legal admissibility or RTI-style frameworks. Its contribution lies in expanding the imagination of blockchain applications, but governance must operationalize these ideas under statutory frameworks.

Vukolić (2015) [11] contrasts proof-of-work with Byzantine Fault Tolerance (BFT) consensus, recommending BFT for permissioned networks. This insight aligns with India's governance context, where permissioned platforms like Hyperledger Fabric are more appropriate than energy-intensive proof-of-work systems. The study, however, does not address document-heavy administrative processes, requiring adaptation to annexure-driven workflows.

Crosby et al. (2016) [12] explore blockchain beyond Bitcoin, proposing hybrid architectures where only hashes are stored on-chain and full data off-chain. This model directly informs the design of a Digital File and Records Management System (DFRMS). Still, it does not address citizen-facing inclusivity, multilingual dashboards, or RTI-grade disclosures.

Narayanan et al. (2016) [13] provide a rigorous cryptographic treatment of blockchain, detailing adversarial models and consensus mechanisms. Their work is invaluable in ensuring tamper-proof guarantees in hostile environments. Yet, it remains theoretical and does not engage with the complexities of public administration or citizen access rights.

Tapscott and Tapscott (2016) [14] popularize blockchain's potential for decentralization and reducing reliance on central authorities. While influential in highlighting blockchain's transformative potential, the work is broad and lacks technical or legal depth for public-sector governance.

Mougayar (2016) [15] frames blockchain as a business innovation, emphasizing network effects and adoption governance. While useful in highlighting incentive models, it does not address how incentives would translate in public-sector or federated contexts like India.

Exonum/Bitfury (2016) [16] detail Georgia's blockchain-anchored land titling pilots. These projects demonstrated transparency and efficiency gains but were limited to land registries, lacking broader administrative integration. For India, the lesson is to prioritize high-value registries like land or municipal permits before scaling.

Zheng et al. (2017) [17] provide a systematic overview of blockchain architecture, consensus mechanisms, and scalability issues. Their survey is particularly useful for anticipating bottlenecks in government-scale deployments but lacks consideration of multilingual, document-heavy workflows that are typical in Indian administration.

Digital Dubai (2018) [18] outlines the Paperless Strategy, a regulatory-backed mandate to eliminate paper in governance workflows. Its KPI-driven approach illustrates how regulatory support accelerates digitalization. However, it relies on trusted registries without consistent blockchain use.

Zohar (2019) [19] reviews blockchain security, focusing on consensus vulnerabilities and attack surfaces. While it strengthens understanding of protocol risks, the analysis is primarily financial-sector oriented and does not translate to RTI-driven disclosure systems.

Tricker (2019) [20] conceptualizes governance as an information flow system balancing stakeholder interests. This model highlights how governance depends on structured flows of verifiable information, aligning with blockchain-enabled audit trails. Its limitation is applicability to citizen-facing contexts, as it gives little attention to multilingual transparency or RTI-style disclosure.

Cai et al. (2020) [21] review blockchain applications in financial services, focusing on efficiency and trust in sensitive transactions. While offering insights into scalability and integrity, the work is sector-specific and not directly translatable to governance record systems.

Sedlmeir et al. (2020) [22] analyze the energy consumption of blockchain networks, debunking myths and highlighting realistic efficiency strategies. This research is critical in addressing concerns about sustainability, but its focus remains on public blockchains, not permissioned systems like those needed in governance.

e-Estonia (2022) [23] documents the KSI blockchain and X-Road system, which together guarantee integrity of government registries and enable secure federated data exchange. While exemplary in demonstrating large-scale integrity anchoring, the model does not address linguistic inclusivity or digital marginalization, which remain critical issues for India.

IPFS Morpheus Case Study (2022) [24] highlights the use of IPFS for decentralized supply chain documentation. It demonstrates content addressing and pinning strategies but also identifies latency and redundancy challenges. Its limitation lies in its enterprise focus, with no consideration for citizen-facing dashboards.

Maersk TradeLens (2022) [25] illustrates how global supply chain ledgers can standardize documentation, but also how failures in consortium governance can cause system collapse despite technical success. For public governance, the lesson is that technical soundness must be paired with strong institutional incentives.

MeriPehchaan (2022) [26] integrates multiple Indian identity systems into a single sign-on (SSO) framework, enabling federated digital identity across platforms. Its evolution highlights the importance of identity-bound access for any governance blockchain.

B. Literature Summary

Recent literature illustrates a rich but fragmented discourse on how governance theory, digital innovations, and blockchain foundations can be leveraged to enhance transparency in administration. Theories such as **Cadbury (1992)** and **Tricker (2019)** establish the enduring principles of disclosure, accountability, and information flow, which are directly applicable to public administration. These works emphasize that trust in institutions is a product of transparent and verifiable information sharing, a principle central to RTI-grade governance. On the technological side, foundational contributions such as Nakamoto (2008) and Narayanan et al. (2016) provide the cryptographic and consensus frameworks that underpin immutable, tamper-evident ledgers. Buterin (2013) extends this to programmable smart contracts, enabling automated policy enforcement that could redefine how administrative decisions are recorded and accessed.

International case studies provide further insights into the possibilities and limitations of blockchain for governance. Estonia's use of the KSI blockchain and X-Road shows how integrity anchoring and federated data exchange can operate at national scale. Georgia's land registry pilots illustrate the benefits of starting with high-value registries to build trust, while Dubai's Paperless Strategy demonstrates the role of regulatory mandates and KPIs in accelerating adoption. Yet, despite their successes, these case studies often lack provisions for inclusivity, particularly in multilingual and digitally divided societies such as India.

Enterprise-oriented case studies such as Morpheus (IPFS-based) and TradeLens (Maersk-IBM) further enrich the debate. Morpheus highlights the promise of content addressing and decentralized file persistence, though it was designed primarily for enterprise supply chains and not citizen-facing transparency. TradeLens, on the other hand, illustrates that even technically robust platforms can fail if consortium governance and stakeholder incentives are not aligned. Together, these works point to a recurring pattern: while the theoretical and technological foundations for transparent governance exist, they rarely address the socio-political realities of citizen rights, linguistic inclusivity, or the federal complexities of countries like India.

C. Research Gap

Despite notable progress in governance theory and blockchain experimentation, several research gaps remain unaddressed. First, existing models fail to deliver multilingual, RTI-grade citizen dashboards, a crucial element for inclusivity in India's 22 scheduled languages. Most international case studies assume homogeneity of language and digital literacy, overlooking the diversity that defines Indian governance [4], [20], [23].

Second, the privacy–immutability conflict persists. While blockchain's immutability ensures tamper-proof records [6], it complicates compliance with data protection laws such as India's *Digital Personal Data Protection Act, 2023* [3], which mandate rectification, erasure, or redaction of personal information. Solutions such as off-chain storage, encrypted payloads, and redaction pipelines remain underexplored in the context of large-scale public systems [12], [15], [19].

Third, the absence of standardized, court-grade proof packs for digital evidence undermines legal admissibility. Current blockchain systems often provide cryptographic proofs but fail to structure them in formats easily verifiable by courts and oversight bodies, despite the legal provisions of the *Information Technology Act, 2000/2008* [1], [2].

Fourth, consortium governance challenges remain unresolved. As evidenced by the collapse of TradeLens [25], even technically sound systems can fail without clear governance rules, incentive alignment, and upgrade pathways. This highlights the need for robust multi-stakeholder governance frameworks in the Indian federal context.

Finally, the literature provides little guidance on vicinity-aware citizen access—the ability for citizens to view only those government files and decisions that directly affect them, while ensuring redacted privacy and auditability [7], [22], [24].

The proposed blockchain-enabled Digital File and Records Management System (DFRMS) explicitly targets these gaps. By combining multilingual dashboards, privacy-aware redaction pipelines, exportable proof bundles aligned with Indian legal requirements, and on-chain governance registries compatible with India's federal diversity, it extends beyond existing models. This positions the framework not just as a technological innovation but as a socio-technical blueprint for inclusive, transparent, and accountable governance, aligned with the vision of *Digital India* and *Amrit Kaal 2047*.

IV. RESEARCH METHODOLOGY

A. The studies included in this review were chosen using three main criteria:

1) Relevance to governance and transparency: Foundational works that establish theoretical or policy bases for accountability, disclosure, and citizen trust, such as the Cadbury Report [5], Tricker's model of governance [20], and the Second Administrative Reforms Commission (ARC) [7].
2) Technological depth: Studies explaining blockchain, decentralized storage, and identity frameworks applicable to large-scale public records management, including Nakamoto's Bitcoin white paper [6], Narayanan et al.'s cryptographic treatment [13], Buterin's proposal of Ethereum smart contracts [8], and Crosby et al.'s hybrid blockchain models [12].
3) Applied case evidence: Documented government or enterprise deployments that demonstrate feasibility, benefits, and challenges. These include Estonia's KSI blockchain and X-Road system [23], Georgia's blockchain-based land registry pilots [16], Dubai's Paperless Strategy [18], the IPFS-based Morpheus case study [24], and the TradeLens platform [25].

In addition, key policy documents like the *Information Technology Act, 2000/2008* [1], [2] and the *Right to Information Act, 2005* [4] were incorporated to ground the technical design within India's legal and administrative environment. This ensured that the corpus combined conceptual, technical, and applied sources, making the review comprehensive and multidisciplinary.

B. Method of Analysis

A five-facet coding framework, derived from governance theory and information science, was applied to each reviewed work:

1) Identity: Mechanisms binding actors to actions (e.g., digital identity, single sign-on, role- or attribute-based access control).
2) Integrity: Mechanisms ensuring tamper-evidence and verifiability of records (e.g., hashes, blockchain anchoring, timestamps).
3) Interoperability: The capacity for federated and cross-agency data exchange (e.g., X-Road, APIs, schema registries).
4) Inclusivity: Accessibility for citizens across India's linguistic diversity, literacy levels, and digital divides.
5) Legal Admissibility: Alignment with national laws, evidentiary rules, and the creation of court-grade proof packs.
6) Each study was coded across these dimensions to evaluate how it contributed to the design of a transparent and inclusive Digital File and Records Management System (DFRMS).

C. Comparison and Analysis

The comparative coding revealed that no single deployment satisfied all five facets simultaneously.

1) Estonia demonstrates national-scale feasibility of integrity anchoring and federated data exchange through KSI and X-Road but neglects multilingual inclusivity [23].
2) Georgia illustrates phased trust-building in land registries with blockchain anchoring but lacks scalability to broader federal systems [16].
3) Dubai validates KPI-driven adoption through its Paperless Strategy but is not consistently blockchain-anchored across all workflows [18].
4) Enterprise systems such as Morpheus and TradeLens highlight technical robustness, including content-addressable storage and interoperability, but fail to address public-facing inclusivity or sustainable governance incentives [24], [25].

From this cross-case analysis, three patterns emerged:

a) High performance in Integrity and Interoperability correlates strongly with adoption success in government deployments.
b) Weaknesses in Inclusivity and Legal Admissibility undermine citizen trust and court recognition, especially in federated democracies like India.
c) Consortium governance, though not originally defined as a facet, emerged as a recurring weakness across enterprise deployments, where unclear rules or misaligned incentives often led to failure (e.g., TradeLens).

These findings directly informed the blueprint for the proposed DFMS. By combining Estonia's integrity anchoring, Georgia's phased rollout approach, and Dubai's KPI-driven regulatory model, while explicitly solving gaps in inclusivity and legal admissibility, the design aims to offer a socio-technical system capable of delivering trustworthy, citizen-centric digital governance in India.

V. DISCUSSION

A. Synthesis of Global Lessons

The findings from literature and international case studies converge on a clear design principle: identity binding, cryptographic integrity anchoring, and interoperability are indispensable for transparent governance. Estonia's KSI blockchain demonstrates how tamper-evident integrity can be implemented at national scale, while the X-Road system shows that federated interoperability reduces reliance on centralized brokers. Georgia's blockchain-anchored land registry pilots highlight the effectiveness of phased adoption in high-value domains, which can build trust incrementally. Dubai's Paperless Strategy illustrates the power of regulatory mandates and KPI-driven rollout for accelerating digital adoption. Yet, none of these experiences fully achieve inclusivity or legal admissibility in linguistically diverse and federated societies. This synthesis suggests that a governance system in India must not only integrate technical robustness but also adapt to citizen-centric and legal contexts.

B. Implications for Indian Governance

For India, the implications are profound. A blockchain-enabled Digital File and Records Management System (DFRMS) aligns directly with the *Information Technology Act (2000/2008)* [1], the *Right to Information Act (2005)* [4], and the broader *Digital India Mission*. Unlike existing siloed e-governance portals, a unified system can leverage MeriPehchaan SSO integration, ensuring every transaction is attributable to a verified officer or citizen. By publishing redacted yet verifiable versions of official documents, such a system operationalizes the RTI mandate of proactive disclosure while preserving individual privacy. This elevates the framework beyond a technical artifact into a policy instrument, capable of advancing the citizen-centric reforms envisioned by the Administrative Reforms Commission and the long-term goals of *Amrit Kaal Vision 2047*.

C. Inclusivity and Accessibility Challenges

Despite these strengths, inclusivity poses a persistent challenge. India's governance system must serve a population with 22 constitutionally recognized languages, varying literacy levels, and stark digital divides. If transparency mechanisms rely only on English or Hindi, large segments of the population risk exclusion. Moreover, interfaces must balance verifiability with simplicity, avoiding technical jargon that deters citizen engagement. A future-ready DFMS should incorporate NLP-driven multilingual redaction pipelines, voice-based interfaces, and WCAG-compliant dashboards to make access equitable across demographics. Continuous usability testing and citizen feedback loops will be essential for ensuring that inclusivity is not just aspirational but realized in practice.

D. Privacy-Immutability Tensions

Another major concern is the tension between privacy and immutability. Blockchain's immutability guarantees tamper resistance but complicates compliance with data protection frameworks such as the *Digital Personal Data Protection Act (2023)* [3], which mandates rights of rectification and erasure. Estonia sidesteps this by storing only hashes, but India's legal environment demands stronger privacy-preserving tools. Potential solutions include off-chain encrypted storage, policy-controlled key rotation to allow effective erasure, and publication of redacted derivatives for public transparency. While these mechanisms mitigate the conflict, sustained dialogue with regulators, courts, and civil society is required to reconcile immutable infrastructure with evolving privacy norms.

E. Consortium Governance Risks

The sustainability of such a platform depends as much on governance as on technology. The collapse of TradeLens [25] demonstrates how misaligned incentives and weak governance structures can derail even technically robust projects. In India's federal democracy, Union, State, and Local bodies often pursue divergent priorities, increasing the risk of deadlock. Embedding on-chain governance registries, voting workflows, and canary channels for upgrades can mitigate technical risks. However, political buy-in, inter-state cooperation, and incentive alignment remain indispensable for national-scale adoption. Governance frameworks must therefore balance autonomy with accountability, ensuring that all stakeholders perceive tangible benefits.

F. Future Research and Pilots

To validate and refine the framework, future research should prioritize pilot deployments in high-value registries such as land titles, municipal permits, and welfare disbursements. These domains directly affect citizens and offer measurable trust benefits. Pilots should publish monthly transparency dashboards, tracking KPIs such as ledger latency, redaction precision, RTI fulfillment times, and user satisfaction. Researchers should also explore incentive structures for sustainable inter-agency governance, integration with national platforms like DigiLocker, and privacy-preserving analytics on redacted data corpora. Through iterative pilots and open benchmarking, the system can evolve from a conceptual blueprint to a scalable, citizen-trusted governance infrastructure

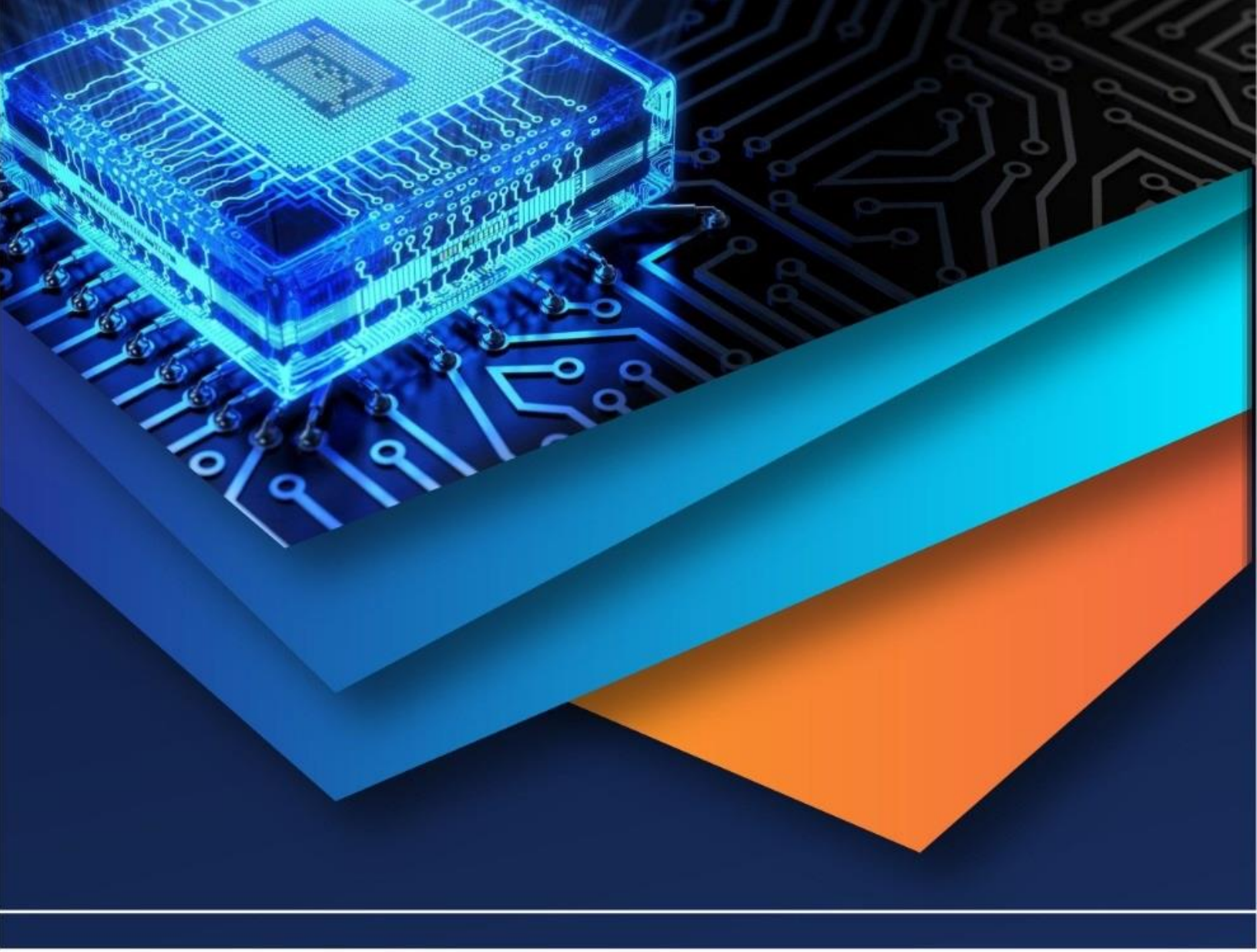
VI. CONCLUSION

India's governance demands systems that move beyond digitization to ensure transparency, accountability, and inclusivity. Existing records remain fragmented, delaying citizen access and undermining trust. International models highlight blockchain's strengths in integrity and interoperability but also expose gaps in inclusivity and sustainable governance. A blockchain-enabled Digital File and Records Management System (DFRMS) tailored to India addresses these gaps by binding records to MeriPehchaan identities, anchoring provenance cryptographically, and publishing multilingual, redacted, verifiable records. With phased rollouts in high-value registries and KPI-driven monitoring, such a system offers a scalable reform pathway for achieving India's *Amrit Kaal Vision 2047*.

REFERENCES

[1] Government of India, The Information Technology Act, 2000. New Delhi: Ministry of Law, Justice and Company Affairs, 2000.
[2] Government of India, The Information Technology (Amendment) Act, 2008. New Delhi: Ministry of Law and Justice, 2008.
[3] Government of India, The Digital Personal Data Protection Act, 2023. New Delhi: Ministry of Law and Justice, 2023.
[4] Government of India, Right to Information Act, 2005. New Delhi: Ministry of Law and Justice, 2005.
[5] A. Cadbury, *Report of the Committee on the Financial Aspects of Corporate Governance*. London, U.K.: Gee Publishing, Dec. 1992. ISBN 0-85258-913-1.
[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[7] Government of India, Second Administrative Reforms Commission, "Twelfth Report: Citizen-Centric Administration The Heart of Governance," New Delhi, India, Feb. 2009.
[8] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2013. [Online]. Available: https://ethereum.org/en/whitepaper/
[9] R. G. Eccles, I. Ioannou, and G. Serafeim, "The impact of corporate sustainability on organizational processes and performance," *Management Science*, vol. 60, no. 11, pp. 2835–2857, Nov. 2014. doi:10.1287/mnsc.2014.1984
[10] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly, 2015.
[11] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop on Open Problems in Network Security (iNetSec)*, Zurich, Switzerland, 2015, pp. 112–125.
[12] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–10, 2016.

[13] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*. Princeton, NJ, USA: Princeton Univ. Press, 2016.
[14] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York, NY, USA: Penguin, 2016.
[15] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken, NJ, USA: Wiley, 2016.
[16] Exonum/Bitfury, "Improving the security of a government land registry," 2016. [Online]. Available: https://exonum.com/story-georgia
[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. 2017 IEEE Int. Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.
[18] Digital Dubai, "Dubai Paperless Strategy," 2018 (launch). [Online]. Available: https://www.digitaldubai.ae/initiatives/paperless
[19] A. Zohar, "Bitcoin: Under the hood," *Communications of the ACM*, vol. 62, no. 9, pp. 103–113, Sept. 2019.
[20] R. I. Tricker, *Corporate Governance: Principles, Policies, and Practices*, 4th ed. Oxford, U.K.: Oxford Univ. Press, 2019.
[21] N. Cai, R. Zeng, and X. Zhang, "Blockchain technology in financial services: A comprehensive review," *Journal of Financial Services Research*, vol. 57, no. 2, pp. 269–290, 2020.
[22] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The energy consumption of blockchain technology: Beyond myth," *Business & Information Systems Engineering*, vol. 62, no. 6, pp. 599–608, Dec. 2020.
[23] e-Estonia, "KSI blockchain provides truth over trust," 2022. Online]. Available: https://e-estonia.com/ksi-blockchain-provides-truth-over-trust/
[24] IPFS Docs, "Case Study: Morpheus.Network," 2022. [Online]. Available: https://docs.ipfs.tech/case-studies/morpheus/
[25] Maersk, "Discontinuation of TradeLens," Nov. 29, 2022. [Online]. Available: https://www.maersk.com/news
[26] Government of India, "MeriPehchaan—National Single Sign-On (NSSO)," 2022. [Online]. Available: https://www.india.gov.in/website-meripehchaan-national-single-sign-nsso (Accessed: Sep. 2025).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY