

How Quickly is Mumbai's Financial Sector Picking Up Blockchain-based KYC Solutions in Preventing Identity Fraud?

By Gyaana Khanna

ABSTRACT

Mumbai's fast-growing financial sector faces escalating identity fraud due to the inefficiency and security vulnerabilities of traditional, siloed Know Your Customer (KYC) processes. This paper evaluates the potential of a DLT/Blockchain-based shared KYC utility to deliver a highly secure, immutable, and cross-institutional identity verification system, which has been pilot-tested by consortia like BankChain. Crucially, it resolves the conflict between the DLT's immutability and India's Right to Erasure (DPDP Act, 2023) by proposing architectures like Off-Chain Hashing, and highlights the necessary synergy with Machine Learning for real-time, continuous fraud monitoring. The ultimate conclusion is that transitioning from isolated pilots to an RBI-mandated, regulated Compliance Digital Public Infrastructure is an urgent strategic necessity for securing Mumbai's financial ecosystem and maintaining its competitiveness.

INTRODUCTION

KYC - Know Your Customer or Know Your Client - is the process used by banks to identify and verify the customer's identity while opening an account and periodically after that as well (Kotak Mahindra Bank, n.d.). It is used to identify if information shared by clients is genuine by checking the mandatory KYC documents, such as identity and address proofs, to ensure a robust transaction and avoid fraudulent activities or financial crimes like money laundering (HDFC Bank, n.d.).

KYC procedures are crucial in combating identity fraud and provide several benefits:

- **Verification of Identity:** KYC processes require businesses to authenticate personal information, typically by collecting government-issued identification or address proofs, to prevent criminals from opening accounts under false pretenses (Lightico, 2023).
- **Mitigating Risks:** By understanding a customer's background and financial behaviors, businesses can identify potential threats and take appropriate measures to mitigate the risks of money laundering, identity fraud, and terrorist financing (IDnow, n.d.).
- **Compliance with Regulations:** Implementing KYC is a legal requirement set by regulatory bodies such as SEBI (in India) to combat financial crimes (Reserve Bank of India, 2025). Non-compliance can lead to severe penalties, as KYC helps protect the integrity of the financial system (TrustDecision, 2024).
- **Enhancing Customer Trust:** Robust KYC measures increase consumer trust, as customers feel more secure in their transactions knowing their identities are being verified and protected (DashDevs, 2024).
- **Protection against Data Breach:** Effective KYC measures include data protection methods to prevent data breaches, which can cause identity theft, by ensuring the secure storage of personal information (Fingerprint, 2024).
- **Blocking Fraud Schemes:** KYC measures like identity verification and transaction monitoring are essential in blocking fraud schemes that can arise throughout a customer's journey (Checkout.com, 2024).
- **On-going Monitoring:** KYC requires continuous customer transaction monitoring and periodic re-verification to detect frauds and suspicious activities early, allowing institutions to act swiftly (Fraud.net, n.d.).

Traditional KYC methods are increasingly ineffective in today's fast-paced financial world, especially in Mumbai's growing financial sector (Youverify, 2024). Traditional methods rely on manual verification, making them time-consuming and prone to human error, which increases the risk of inaccuracies (Coorpid, 2023). Customers also face repetitive data collection requirements across multiple institutions, leading to frustration and application abandonment (HyperVerge, 2024). Moreover, traditional KYC uses a centralized database which is highly vulnerable, making it an easy target for cybercriminals (iDenfy, 2024). These systems struggle to adapt to evolving fraud techniques, lacking the real-time monitoring and flexibility needed to counteract sophisticated frauds and thefts (Regula Forensics, 2024).

Challenges of Traditional KYC:

- **Evolving Regulatory Framework:** Financial institutions must stay updated on varying jurisdictions, which is resource-intensive, especially for international organizations (Coorpid, 2023).
- **High Resource Requirements:** Substantial human and financial resources are required for trained personnel and technology investment, which can strain small organizations (Stylianou, 2023).
- **Vulnerability to Cybercrime:** Data breaches highlight the need for advanced verification methods due to sophisticated criminals exploiting vulnerabilities (InfoSec Awareness, n.d.).
- **Labor-Intensive Monitoring:** Continuous monitoring to detect suspicious activity is labor-intensive and prone to error if performed manually (Smile ID, 2024).
- **Poor Customer Experience:** Lengthy KYC forms lead to irritation and abandonment, resulting in lost business opportunities (TrustDecision, 2024).

In a rapidly growing economy, innovative solutions are of utmost importance to solve the most obvious problems of the KYC processes (The Paypers, 2024). One such solution is using blockchain technology to improve KYC security and protection, which would potentially solve the question of consumer trust by creating an extremely robust method of preventing fraudulent schemes (Financial Crime Academy, 2024).

BACKGROUND AND MOTIVATION

A. Overview of Distributed Ledger Technology (DLT)

Blockchain technology offers structural solutions to the inherent vulnerabilities of centralized KYC. Its core principles include:

- **Decentralization:** The network is maintained by a group of trusted nodes, removing any single point of control and directly solving the data silo problem prevalent in traditional banking (RecordsKeeper.AI, 2024).
- **Immutability:** Once identity data (or a cryptographic hash of that data) is recorded, it cannot be altered or tampered with, ensuring data integrity for regulatory audit trails and secure identity verification (Hannan et al., 2023).
- **Enhanced Security:** The cryptographically secured ledger is almost impossible to hack, as it would require attacking every single block at once, protecting the data stored (John, 2025).

In summary, Blockchain improves the KYC process by creating a secure, decentralized system that enhances data security, reduces costs, and speeds up onboarding (Hannan et al., 2023). Users submit encrypted information to a blockchain-based platform. Authorized institutions can efficiently verify this information through a tamper-proof, shared ledger, with the user retaining control over data access. This eliminates the need for repeated checks, allowing verified information to be shared across institutions with user permission, creating a single, reusable identity (RecordsKeeper.AI, 2024).

B. Current Challenges and Compliance Costs in the Financial Sector

The current KYC regime in India requires repetitive, resource-intensive Customer Due Diligence (CDD) and periodic re-KYC processes mandated by regulatory bodies such as the RBI and SEBI (Reserve Bank of India, 2025). Financial Institutions (FIs) maintain segregated, proprietary databases, leading to duplicated processes every time a customer onboards a new service provider, which costs time and resources. This creates severe bottlenecks, hindering the seamless, efficient digital banking system customers expect (McKinsey & Company, 2023).

India's regulatory environment is dynamic, averaging 42 legal updates per day, which introduces significant management complexity. This complexity translates into overwhelming financial costs; for example, manufacturing MSMEs in a single state face over 1,450 regulatory obligations annually and up to ₹17 lakh in compliance expenses. These high, repetitive KYC costs act as a substantial drag on efficiency and profitability, particularly in a high-volume financial hub like Mumbai (McKinsey & Company, 2023). Implementing a shared, technology-driven KYC system transforms compliance from a recurring operational expense (OpEx) into an amortized infrastructure investment (CapEx), directly improving the long-term competitiveness of Indian FIs (Hannan et al., 2023).

C. The Identity Fraud Threat Landscape

The success of the Digital India initiative, with over 86% of households connected to the internet, has inadvertently increased the risks for cyber fraud due to rapid digitization and financialization. This is also compounded by a lack of awareness about cyber crimes in some regions (InfoSec Awareness, n.d.). Cybersecurity incidents and threats have doubled from 2022 to 2024, necessitating that the next evolution of India's Digital Public Infrastructure (DPI) prioritize a high-security layer for digital identity compliance.

The digital threat landscape is defined by the dominance of sophisticated identity-based crimes. Third-party Account Takeover (ATO) remains the single largest category of fraud, accounting for 55% of all fraud incidents in India, demonstrating that identity theft and compromise are the primary vectors for financial loss. Furthermore, the systematic use of money mules is a "massively underreported plague," with devices involved in this activity logging into an average of 35 accounts each. Traditional centralized verification systems fail to recognize these crucial cross-institutional linkages.

Blockchain delivers an evolutionary leap for KYC processes by establishing Secure Digital Identity (DID) based on cryptographic verification (John, 2025). The key advantage for the financial sector is cross-institutional data sharing and efficiency. The DLT platform allows participating institutions to access shared, verified customer data efficiently, significantly reducing the time and effort required for repetitive information gathering (Hannan et al., 2023). The DLT provides guarantees of data integrity, transparency, and real-time updates. Automation via smart contracts can automate complex compliance checks, ensuring adherence to regulations across different entities and borders, and reducing costs associated with compliance changes. Establishing a compliant, seamless blockchain-based KYC utility in Mumbai will secure the domestic market and reinforce India's position as a digital leader by serving as an exportable regulatory technology (Financial Crime Academy, 2024).

METHODOLOGY AND RESULTS

A. Methodology

Primary data was collected via purposive sampling of senior stakeholders in Mumbai, including Chief Technology Officers and Heads of Compliance from major institutions. Mumbai was selected as the operational focus due to its concentration of financial headquarters and DLT pilot contributors, such as State Bank of India (SBI) and HDFC Bank, alongside prominent FinTech organizations. Interview protocols focused on DLT-DPDP conflict resolution, interoperability requirements, and regulatory comparison with global centers like Singapore and the UAE.

Secondary data research confirms that the market for DLT adoption is disproportionately driven by identity management needs. The projected Compound Annual Growth Rate (CAGR) for the Indian Blockchain Identity Management Market (70.80%, reaching USD 15.16 Billion by 2033) significantly outpaces the overall Indian Blockchain Market CAGR (65.60%) (IMARC Group, 2023). The regulatory review centered on the Central KYC Registry (CKYCR) framework and the conflict posed by the Digital Personal Data Protection (DPDP) Act, 2023, which introduces the mandatory Right to Correction and Erasure.

B. Empirical Findings and Commercial Benefits

Adoption is spearheaded by consortium projects, notably the BankChain initiative, which includes inputs from major financial players like SBI and HDFC Bank and is pilot-testing smart contracts and centralized KYC applications on a DLT platform (The Paypers, 2024). This activity suggests a deliberate strategy to augment the existing Central KYC Registry (CKYCR) framework. Furthermore, the involvement of major Mumbai institutions (SBI, HDFC Bank) in the Reserve Bank of India's eRupee (CBDC) pilot confirms a strong level of internal technical familiarity and readiness with DLT architecture.

DLT is poised to enhance operational efficiency by enabling real-time, seamless data sharing across institutions, eliminating redundant KYC procedures, lowering costs, and mitigating risks (McKinsey & Company, 2023). While specific public metrics from major Indian pilots are scarce, commercial FinTech vendors report substantial gains, including greater than 50 percent reductions in Turnaround Time (TAT) for customer verification.

Crucially, DLT acts as an immutable foundational layer integrated with Artificial Intelligence (AI) and Machine Learning (ML) systems (John, 2025). AI/ML algorithms analyze the secured datasets to identify patterns of suspicious activity and flag deviations, enhancing risk management, reducing fraud, and lowering regulatory compliance costs by detecting finer changes in customer behavior. Beyond direct financial benefits, DLT-KYC solutions address financial inclusion by lowering the prohibitive barriers to entry for underserved populations. By enabling secure and frictionless verification, the technology aligns with the broader policy goal of enhancing the 'Ease of Doing Business' and integrating socio-economically diverse segments into the formal financial ecosystem.

DISCUSSION: TECHNICAL AND REGULATORY ARCHITECTURE

A. Synergy with Machine Learning for Continuous Monitoring

Traditional KYC models, which are often periodic, are inadequate because they fail to capture critical changes in customer risk profiles between mandatory review cycles. These reviews are governed by a risk-based approach (RBA), which allocates scrutiny in proportion to the risk a customer presents, allowing for Enhanced Due Diligence (EDD) on high-risk customers (Reserve Bank of India, n.d.).

Machine Learning (ML) addresses this gap by facilitating the ongoing, continuous monitoring of customer transactions and behaviors, mediating and reducing possible risks of frauds or identity theft (Hannan et al., 2023). ML fundamentally modernizes the Anti-Money Laundering (AML) risk scoring model, which traditionally relies on manual transaction monitoring and simple rule-sets that lead to a high volume of false positives and negatives. ML enables dynamic scoring models tailored by industry sector and customer base.

The synergy between DLT and ML is powerful.

- DLT's Role: Provides the robust, tamper-proof, and shared historical record of transactions and verified identity status (John, 2025).
- ML's Role: Analyzes this immutable data ledger using sophisticated techniques, such as AI-based risk scoring engines that learn from evolving user behavior, geolocation, and transaction data (Hannan et al., 2023). This is critical for detecting complex digital scams and the pervasive mule networks active in the financial sector.

The ML application enhances system performance. ML's role in automating compliance checks and focusing continuous monitoring only on high-risk triggers ensures that the DLT only needs to process high-assurance verification events and secure audit logs, optimizing the DLT system and making enterprise adoption more viable. Upon detecting anomalies via the ML risk engine, a real-time KYC revalidation process is automatically triggered, securing Mumbai's high-value transaction environment.

B. Resolving Regulatory and Architectural Conflicts (DPDP Act, 2023)

A transition to DLT in India has a multitude of complex problems, the biggest being the regulatory and architectural conflicts related to data privacy. India's Digital Personal Data Protection (DPDP) Act, 2023, establishes the fundamental legal Right to Erasure ("Right to be Forgotten") (Reserve Bank of India, 2025). This right allows individuals to demand deletion of their information if no legitimate grounds for retention exist. This mandate creates an irreconcilable conflict with blockchain's immutability. Uploading sensitive KYC data directly onto a distributed ledger creates a persistent, unerasable record, directly violating the DPDP Act.

To reconcile DLT integrity with DPDP compliance, specific privacy-preserving architectures must be implemented and mandated.

- Strategy 1: Off-Chain Storage and On-Chain Hashing: Sensitive personal data must be maintained off-chain in secure, encrypted central or personal data vaults. Only a cryptographic hash—a unique digital fingerprint of the data—is recorded on the distributed ledger (Hannan et al., 2023). If the Right to be Forgotten is exercised, the FI deletes the off-chain personal data, which renders the corresponding hash key useless and untraceable to the original identity, satisfying the erasure requirement.
- Strategy 2: Homomorphic Encryption (HE) for Confidential Computation: HE is a specialized encryption scheme that permits computations (such as risk aggregation) to be performed directly on the encrypted data (ciphertext) without requiring decryption. This technology provides end-to-end confidentiality, allowing the DLT network to verify and score risk across aggregated, encrypted data from multiple FIs, preserving data privacy while maximizing efficiency (John, 2025).

Additionally, privacy compliance under the DPDP Act also mandates explicit user consent. Smart contracts can be utilized to serve as dynamic consent managers, automatically revoking access rights, deleting data references, or enforcing access permissions upon the user's instruction.

Table 2: Mitigating Blockchain Limitations for DPDP Act Compliance

Limitation/Conflict	Regulatory Requirement (India)	Technical Mitigation Strategy	Impact on Compliance/Security
Immutability	Right to Erasure/Forgotten (DPDP Act, 2023)	Off-Chain Data Storage (Store only cryptographic hash on-chain, off-chain)	Allows deletion of personal data while preserving ledger integrity.
Data Visibility and Privacy	Data Minimization	Homomorphic Encryption (HE) for computation on encrypted data	Enables shared risk scoring across institutions without revealing underlying sensitive information.
Data Control and Withdrawal	User Consent	Smart Contracts programmed for access revocation and consent management	Embeds legal consent parameters directly into the identity infrastructure.

C. Strategic Alignment with India's Digital Public Infrastructure (DPI)

India's robust DPI, including the Aadhaar digital ID system and the Unified Payments Interface (UPI), has already achieved mass scale and democratization of access. A shared, blockchain-based KYC system fits logically as the next essential layer—a dedicated compliance and identity validation utility (McKinsey & Company, 2023). The success of verification for existing documents like the Aadhaar Card is already supported by governmental sources. The DLT should function as the secure, shared ledger for the verified status provided by these government-backed verification processes, rather than replacing them entirely.

The RBI's quiet pilot to tokenize Certificates of Deposit (CDs) using the wholesale CBDC (WCBDC) rails is highly significant as it establishes the necessary institutional acceptance, technical expertise, and infrastructural foundations within the central bank for broader DLT adoption. This move from asset tokenization to identity tokenization (KYC) is a logical and inevitable progression (The Paypers, 2024). Implementing the blockchain-based KYC procedure will ensure that the rapid growth and financialization of the economy has the high-security standards needed to protect the important economic activities mostly centered in Mumbai (IMARC Group, 2023).

Table 3: Harmonious Application of Blockchain and Machine Learning in KYC/AML

Function	Blockchain Role	Machine Learning (ML) Role	Strategic Outcome
Identity Verification	Immutable record of validated identity status	Automated document authentication (tampering detection)	High-Assurance, Automated Onboarding/Re-KYC
Risk Assessment	Shared, tamper-proof transaction and activity history	Real-time risk scoring based on behavioral anomalies	Dynamic AML/CFT Compliance (Shift to proactive detection)
Re-KYC/Updates	Decentralized, secured identity profile accessible by permission	Continuous monitoring trigger and automated data renewal prompting	Reduced Compliance Lag and Cost

CONCLUSION AND BLUEPRINT

A. Case Study: Indian Industry Consortia and Pilot Projects

One example of using Blockchain in KYC and AML processes is the Indian Industry Consortia and Pilot Projects, mainly the BankChain case study. BankChain, founded in 2017 by major institutions

including State Bank of India (SBI), ICICI Bank, and Kotak Mahindra Bank, grew into a consortium of 27 members (The Paypers, 2024). Its Clear-Chain project was explicitly designed as a permissioned blockchain utility for integrated and shared KYC and AML/CFT, establishing the technological feasibility of shared KYC within India (John, 2025). However, NITI Aayog's analysis highlighted that widespread operational success depends heavily on securing industry-wide consensus and ensuring the individual bankers' intention to integrate and utilize the platform. To secure Mumbai's entire financial ecosystem, the solution must evolve beyond a private, member-based consortium to a regulated utility—a Compliance Digital Public Infrastructure (DPI).

B. Strategic Blueprint for Implementation in Mumbai (Modernizing BankChain)

To transition from pilots to operational necessity, a three-phase blueprint for Mumbai's financial institutions is proposed:

- **Phase 1: Regulatory Endorsement and Standards:** The RBI must formally endorse and regulate the shared DLT utility, establishing a regulatory framework for the major FIs (Reserve Bank of India, 2025). The RBI must finalize and issue architectural standards that explicitly mandate the use of privacy-preserving techniques (like Off-Chain Hashing) to preempt legal challenges under the DPDP Act.
- **Phase 2: Technical Buildout and Integration:** The technical buildout must use high-assurance enterprise platforms and prioritize links with existing high-volume government verification services (Aadhaar, Passport Seva) (McKinsey & Company, 2023). ML/AI risk engines must be fully integrated for continuous monitoring, initially focusing on high-risk sectors.
- **Phase 3: Mandatory Parallel Running and Education:** This phase involves the mandatory parallel running of the new DLT KYC system alongside existing legacy systems across Mumbai's FIs. Education and training are crucial to secure widespread acceptance among compliance and operations staff (Stylianou, 2023).

Implementing this technology is a prerequisite for maintaining India's global financial standing and resilience against digital threats, especially as Mumbai seeks to compete as a booming and developing financial center. However, constraints regarding large-scale adoption exist, as initial studies often did not provide a "proper sense of scalability" for deployment across the sheer volume of operations characteristic of Mumbai's financial sector (Hannan et al., 2023).

C. Final Conclusion

To ensure compliance with the DPDP Act, institutions must adopt hybrid architectural strategies, specifically: Off-Chain Storage for PII and Cryptographic Revocation (where smart contracts irreversibly revoke all network access rights to the data hash and the off-chain PII) as legal 'Erasure' (John, 2025).

The importance lies in regulatory compliance and sovereignty: India must demonstrate how to architect DLT solutions that simultaneously guarantee data integrity (immutability) and the citizen's right to control personal data (Right to Erasure), using advanced techniques like Off-Chain Storage and Homomorphic Encryption. By transitioning to a shared DLT utility, the financial industry can drastically

cut operational costs and friction, accelerating the efficiency and growth trajectory of the nation's financial capital (McKinsey & Company, 2023). The integrity and sustained growth of Mumbai as a global financial center depend on swift, decisive action to build this regulated, shared compliance infrastructure, leveraging the foundational success established by initiatives like BankChain.

REFERENCES

- Checkout.com. (2024, January 15). *Identity theft and KYC*. <https://www.checkout.com/blog/identity-theft-kyc>
- Coorpid. (2023, November 19). *One of the five major KYC challenges banks face: Rapidly changing and increasingly stringent regulatory requirements*. <https://www.coorpid.com/one-of-the-five-major-kyc-challenges-banks-facing-rapidly-changing-and-increasingly-stringent-regulatory-requirements/>
- DashDevs. (2024, March 10). *Know how to know your customers*. <https://dashdevs.com/blog/know-how-to-know-your-customers/>
- Financial Crime Academy. (2024). *The rise of blockchain: Enhancing AML efforts in the digital age*. <https://financialcrimeacademy.org/blockchain-technology-and-aml>
- Fingerprint. (2024, February 1). *KYC (Know Your Customer) and how it prevents financial fraud*. Fingerprint.com. <https://fingerprint.com/blog/kyc-know-your-customer-financial-fraud/>
- Fraud.net. *KYC (Know Your Customer)*. <https://fraud.net/d/kyc-know-your-customer/>
- Hannan, M. A., Shahriar, M. A., Ferdous, M. S., Chowdhury, M. J. M., & Rahman, M. S. (2023). A systematic literature review of blockchain-based e-KYC systems. *Computing*, 105(10), 2089–2118. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10103756/>
- HDFC Bank. *Understanding KYC fraud and how to prevent it*. <https://www.hdfcbank.com/personal/resources/learning-centre/vigil-aunty/understanding-kyc-fraud-and-how-to-prevent-it>
- HyperVerge. (2024, February 20). *Top KYC challenges and solutions*. <https://hyperverge.co/blog/kyc-challenges>
- iDenfy. (2024, January 27). *KYC challenges and how to solve them*. <https://www.idenfy.com/blog/kyc-challenges/>
- IDnow. *What is KYC?* <https://www.idnow.io/regulation/what-is-kyc/>
- IMARC Group. (2023). *India Blockchain Identity Management Market Report - 2033*. <https://www.imarcgroup.com>
- InfoSec Awareness. *KYC frauds*. <https://infosecawareness.in/concept/system-admin/kyc-frauds>
- John, B. (2025, June 5). *Blockchain-based KYC and access verification for financial institutions*. ResearchGate. [suspicious link removed]
- Kotak Mahindra Bank. *What is KYC?* <https://www.kotak.com/en/stories-in-focus/accounts-deposits/savings-account/what-is-kyc.html>
- Lightico. (2023, June 22). *How KYC helps prevent and reduce account fraud in the financial industry*. <https://www.lightico.com/blog/kyc-prevent-reduce-account-fraud-financial-industry/>
- McKinsey & Company. (2023, October). *Solving the KYC puzzle with straight-through processing*. <https://www.mckinsey.com>
- RecordsKeeper.AI. (2024). *Blockchain-based identity verification for KYC compliance*. <https://recordskeeper.ai>

SCHOLARLY DEBUT

by Scholarly Review

Winter 2025/2026

Regula Forensics. (2024, February 10). *KYC challenges and trends in 2024*. <https://regulaforensics.com/blog/kyc-challenges/>

Reserve Bank of India (RBI). (2025, August 14). *Know Your Customer (KYC) Direction, 2016 (Updated as on August 14, 2025)*. <https://rbi.org.in>

Reserve Bank of India (RBI). *FAQs on Master Direction on KYC*. <https://rbi.org.in>

Smile ID. (2024, March 5). *KYC challenges: How to overcome them*. <https://usesmileid.com/blog/kyc-challenges>

Stylianou, A. (2023, December 14). *Challenges in KYC and CDD: What you can do after the EBS-issued travel rule*. LinkedIn.

<https://www.linkedin.com/pulse/challenges-kyc-cdd-what-you-can-do-ebs-issued-travel-rule-stylianou-h7n5e>

The Paypers. (2024, April 25). *State Bank of India taps blockchain tech for KYC management*. <https://www.thepayers.com/crypto-web3-and-cbdc/news/state-bank-of-india-taps-blockchain-tech-for-kyc-management>

TrustDecision. (2024, February 28). *KYC in banking: Key challenges and best practices explained*. <https://trustdecision.com/resources/blog/kyc-in-banking-key-challenges-and-best-practices-explained>

Youverify. (2024, January 12). *KYC challenges: Everything you need to know*. <https://youverify.co/blog/kyc-challenges>