ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

NBATS: Banknote Authentication and Cash-Compliance Intelligence (A Tiered, Privacy-Preserving Framework for Counterfeit Detection and Cash Provenance in India)

Sachin G. Udepurkar

Partner & Management Consultant |Qualified Independent Director (IICA)|PGDFM (MBA–Finance & Microfinance), IIFM Bhopal |Occupational Therapist – Ergo medicine ,GMC, Nagpur | Certified in Base & Advanced SAS|R Programming |Licentiate Insurance |Corporate Social Responsibility IICA, India & Audencia Nantes School of Management, France |AI Mastery Programme ,Coursiv, Navi Mumbai / Nagpur

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150800130

Received: 07 September 2026; Accepted: 12 September 2026; Published: 22 September 2026

ABSTRACT

Cash remains a dominant medium of exchange in India despite rapid digital-payment growth, and its physical nature makes counterfeiting, duplicate circulation, and untraceable high-value cash movement persistent challenges for monetary authorities. The Reserve Bank of India (RBI) already operates a mature framework for detecting and reporting counterfeit currency at banks and currency chests, yet this framework is largely confined to designated touchpoints and does not extend authenticated verification across the broader cash ecosystem. This paper proposes the National Banknote Authentication and Traceability System (NBATS), a conceptual architecture that authenticates physical banknotes through multi-feature verification - serial-number recognition, security-thread and watermark analysis, and optical/ultraviolet characteristics while recording only selected, purpose-limited cash-handling events rather than continuous holder-level possession. The architecture is organised into five layers: the banknote itself, an authentication device, an event ledger, an alert engine, and a tiered investigation interface, supported by a proposed Cash Provenance Confidence Score that combines authenticity, serial validity, issuance consistency, and historical anomaly indicators into a single risk metric. Three participation tiers like voluntary public verification aligned to guidelines within applicable framework, mandatory verification for regulated cash-intensive businesses, and integrated banking/currency-chest authentication are proposed to balance feasibility against comprehensiveness. The paper explicitly foregrounds privacy-by-design, data minimisation, purpose limitation, and role-based access as central design constraints, situating the proposal within India's Digital Personal Data Protection Act, 2023, and within international literature on privacy-preserving digital-currency architectures. Five research questions and five testable hypotheses are formulated to guide future empirical work, including pilot studies and accuracy benchmarking of multi-feature authentication against serial-number-only verification. The paper concludes that a phased, tiered, and privacy-constrained architecture is more implementable and more defensible than a universal note-tracking mandate, and identifies pilot design, cryptographic protocol selection, and stakeholder-acceptance studies as priorities for subsequent research.

Keywords: banknote authentication, counterfeit detection, cash traceability, privacy-preserving systems, financial compliance

INTRODUCTION

India continues to rely heavily on cash for retail and informal-sector transactions even as digital payments expand rapidly (Reserve Bank of India [RBI], 2024a). Physical currency's core vulnerability is that, once printed, a note's authenticity, custody history, and movement through the economy are largely invisible to any central authority except at the limited number of points which includes bank counters, ATMs, and currency chests where machines examine notes before recirculation (RBI, 2024b). This creates three linked problems. First, counterfeit notes can circulate for extended periods before detection, since verification is reactive rather than continuous. Second, a

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

banknote's serial number, while unique in principle, is not by itself proof of authenticity or of a single legitimate origin, because printing errors, replacement note series, and deliberate counterfeiting can all produce serial-number anomalies that require further investigation rather than automatic conclusions (RBI, 2024b). Third, high-value cash movement outside the banking system is difficult to observe, which limits the cash-flow intelligence available to tax and financial-compliance authorities.

This paper originates from a practitioner-proposed idea for a device capable of scanning a banknote's serial number to verify its authenticity and track its movement, with the stated aim of curbing counterfeiting and improving tax compliance. In its original form, the idea implied continuous, holder-level tracking of every note in circulation. On examination, that formulation raises substantial privacy, proportionality, and civil-liberty concerns, and is not readily defensible in an international research context. Accordingly, this paper reframes and matures the idea into the National Banknote Authentication and Traceability System (NBATS): a conceptual architecture that separates authentication (verifying that a note is genuine) from traceability (recording selected cash-handling events under strict purpose limitation) and that treats privacy-by-design as a central research contribution rather than an afterthought.

The specific objectives of this paper are to (i) articulate a technically grounded, multi-feature banknote authentication model that goes beyond serial-number lookup; (ii) propose an event-based, tiered participation model for cash traceability that avoids universal holder-level surveillance; (iii) introduce a composite metric, the Cash Provenance Confidence Score, for expressing authentication and provenance confidence in a single interpretable value; (iv) embed privacy-by-design, data-minimisation, and role-based-access principles consistent with India's Digital Personal Data Protection Act, 2023 (Ministry of Electronics and Information Technology [MeitY], 2023); and (v) situate the proposal relative to RBI's existing counterfeit-detection framework so that the research contribution is clearly incremental rather than duplicative. The paper is conceptual and architectural in nature; it does not report an implemented system or empirical accuracy results, and it explicitly frames all claimed benefits in probabilistic, hedged language pending empirical validation.

BACKGROUND AND LITERATURE REVIEW

Currency management and counterfeit detection - Central banks worldwide combine physical security features of watermarks, security threads, optically variable ink, microprinting, and fluorescent elements with institutional detection procedures at banks and cash-processing centres (RBI, 2024b). In India, RBI's Master Direction on Counterfeit Notes (2024) consolidates instructions requiring that banknotes tendered at counters and back offices be examined through machines, that counterfeit notes be impounded rather than returned or destroyed, and that detection data be compiled and reported through Nodal Bank Officers to RBI, the Financial Intelligence Unit-India, and the National Crime Records Bureau (RBI, 2024b; Taxguru, 2024). A subsequent 2026 circular reiterated and strengthened these obligations, mandating machine-based examination, staff training on security features, and structured reporting of detection patterns (RBI, 2026). This institutional framework demonstrates that denomination, serial number, security-parameter breach information, and investigation references are already recognised as reportable data elements within India's currency-management ecosystem which is an important point of continuity for any proposed extension of the framework.

Machine-vision approaches to note recognition - Automated denomination and serial-number recognition using optical character recognition, ultraviolet/infrared imaging, and machine-learning classification has been explored extensively in the broader currency-recognition literature, typically for assistive devices, vending and banking automation, or targeted counterfeit-screening tools. These approaches generally combine several observable features of print pattern, security-thread position, fluorescence under ultraviolet light, and serial-number legibility into a composite authenticity judgment rather than relying on any single feature, consistent with the multi-layer approach proposed in this paper.

Cash traceability and financial-crime analytics - Financial-intelligence literature on cash-based financial crime emphasises that large or anomalous cash movements are a recognised risk indicator, but that indicators of this kind support risk-based investigation rather than automatic legal conclusions, a distinction this paper adopts explicitly in cash-flow and tax-intelligence point mentioned below.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

Privacy-preserving digital-currency architectures - Central bank digital currency (CBDC) research offers the closest analogue to the privacy questions raised by note-level traceability, because CBDC design faces an equivalent tension between auditability and user privacy. The Bank for International Settlements (BIS) has surveyed proposals for "cash-like" privacy in CBDC systems, including the use of zero-knowledge proofs and application programming interfaces that constrain data exchange to the minimum required for a given transaction, while also noting that technical design alone cannot fully resolve concerns about state surveillance (BIS, 2021; Auer & Böhme,2021). More recent work catalogues privacy and compliance design options for offline CBDC systems and argues that privacy must be designed into the information architecture itself through data-minimised transaction statements and cryptographic commitments rather than added afterward (Michalopoulos et al.,2025). A systematic review of CBDC privacy literature likewise identifies zero-knowledge proofs, secure multiparty computation, and federated learning as the principal technical tools for reconciling auditability with privacy, while cautioning that their practical implementation remains resource-intensive (Ilori et al.,2024). This paper draws on that literature to argue that a national banknote architecture should adopt tiered information disclosure analogous to CBDC privacy tiers rather than a single, fully transparent ledger of note custody.

Data-protection law in India - India's Digital Personal Data Protection Act, 2023, establishes principles of lawful processing, purpose limitation, data minimisation, and accountability for any system that processes personal data (MeitY,2023). Any architecture that could, even indirectly, link a banknote's movement to an identifiable individual falls within the Act's scope and must be designed accordingly from the outset.

Existing Indian Currency Management Framework

RBI issues and manages the design, security features, and circulation of Indian banknotes, currently comprising the ₹10, ₹20, ₹50, ₹100, ₹200, ₹500, and ₹2,000 denominations, the last of which has been withdrawn from active circulation while retaining legal-tender status (RBI, 2024a). Historical RBI records also report ₹2 and ₹5 denominations from earlier series. Security features are periodically upgraded to stay ahead of counterfeiting techniques (RBI, 2024b). Detection currently occurs primarily at three points - bank branch counters, back offices, and currency chests, all of which are required to use note-sorting or authentication machines; ATMs are covered indirectly through cash-replenishment protocols. Detected counterfeit notes are stamped, impounded, logged in a prescribed register, and reported through a bank's Forged Note Vigilance Cell and Nodal Bank Officer to RBI, the Financial Intelligence Unit-India, and the National Crime Records Bureau (RBI, 2024b). Reportable data already includes denomination, serial number, the specific security parameter found to be deficient, tenderer details were available, the branch or currency chest concerned, and an investigation reference number. Banks are also required to monitor detection patterns and escalate suspicious trends to RBI or police authorities (RBI, 2024b). A 2026 circular further tightened compliance by requiring documented staff-training timelines and periodic Action Taken Reports (RBI, 2026).

This existing framework is institutionally mature but structurally limited to notes that pass through the formal banking system for processing. Cash that circulates directly between individuals, small businesses, or within the informal economy is not authenticated or observed unless and until it eventually reaches a bank counter or currency chest. This structural gap rather than an absence of counterfeit-detection capability is the true point of departure for this paper's proposed research contribution.

The scale of this gap can be illustrated with recent figures. On the counterfeit side, RBI data indicate that the face value of Fake Indian Currency Notes (FICN) detected within the formal banking system was approximately ₹7.98 crore in FY 2023–24 and approximately ₹5.88 crore in FY 2024–25, a period in which detections of the ₹500 denomination alone rose by roughly 37 per cent year-on-year even as total pieces detected declined marginally (RBI, 2024b, 2025). The National Crime Records Bureau's Crime in India report separately recorded FICN seizures worth ₹26.03 crore across 1,135 cases in calendar year 2024, with cumulative seizures since 2017 exceeding ₹638 crore once National Investigation Agency recoveries are included (NCRB, 2024). At the time of writing, RBI's annual report for FY 2025–26 had not yet been published, so a directly comparable detected-value figure for that year is not presently available; this paper treats the FY 2025–26 figure as an open empirical data point to be incorporated once RBI publishes it. These are detected values within the banking system, not

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

estimates of undetected circulation, and should be read as a lower bound consistent with the broader point made in existing Indian currency management framework mentioned above.

Research Gap

RBI's existing framework should not be characterised as absent or inadequate; rather, it is deliberately scoped to designated touchpoints in the cash-processing chain. The research gap this paper addresses is therefore not "India lacks counterfeit detection" but the narrower and more defensible claim that existing systems primarily focus on detection and reporting of counterfeit currency at designated points in the cash ecosystem, while a substantial share of cash circulation outside those points remains unauthenticated and unobserved. This paper proposes an interoperable, privacy-preserving architecture capable of extending authenticated banknote verification and controlled provenance intelligence across a broader segment of the cash ecosystem, without requiring universal, continuous, holder-level tracking of every note. The distinguishing contribution is architectural and conceptual: a tiered participation model, an event-based (rather than continuous-possession) data model, a composite provenance-confidence metric, and an explicit privacy-governance layer designed against contemporary data-protection law.

Proposed Nbats Architecture

The proposed National Banknote Authentication and Traceability System (NBATS) is organised into five conceptual layers.

Layer 1: Banknote. Each note is treated as carrying multiple independently observable characteristics: denomination, serial number and prefix, security thread, watermark, printing characteristics, fluorescence and ultraviolet response, substrate characteristics, optical variable elements, and any other RBI-approved security feature. No single feature is treated as sufficient evidence of authenticity.

Layer 2: Authentication Device. Authorised devices perform a sequence of optical and physical examination, serial-number recognition via optical character recognition, security-feature verification using ultraviolet/infrared sensing and machine-learning classification, and computation of an authenticity score. The device output is categorised as genuine (high confidence), suspected counterfeit (referred for manual verification), invalid or duplicate serial event (flagged for investigation), or unreadable (requiring manual verification). This is a substantially stronger evidentiary basis than serial-number lookup alone, because it corroborates the serial number against independently verifiable physical characteristics.

Layer 3: Event Ledger. Rather than continuously recording who possesses a note, the system records discrete Cash Verification Events (CVEs) generated when an authorised device authenticates a note or a batch of notes. A CVE captures an entity identifier appropriate to the participation tier (see point cash event and provenance model), a timestamp, a location, the transaction or batch value, the number and denominations of notes involved, and the authentication result. Critically, a CVE need not create a persistent, government-visible record of a named individual's current possession of a specific serial number at the lowest participation tier it can be fully anonymous.

Layer 4: Alert Engine. The alert engine applies rules and anomaly-detection models across the event ledger to identify suspected counterfeits, serial-number combinations inconsistent with known issuance ranges, repeated suspicious reappearance of the same serial number in incompatible locations or timeframes, unusual geographic movement patterns, and repeated failed authentications. Alerts are risk-scored rather than treated as conclusive findings.

Layer 5: Investigation Interface. Identity-linked information is exposed only to authorised agencies operating under clearly defined legal conditions, consistent with the tiered-disclosure model described in privacy preserving governance framework point mentioned below.

The proposed system deliberately avoids designating distributed-ledger technology as a required component. Rather than committing to "blockchain for every note," the architecture should remain technology-neutral:

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

distributed-ledger or other tamper-evident mechanisms may be appropriate for specific sub-components such as the audit log, but the overriding design criteria are scalability, privacy, governance, and auditability, which for a system processing billions of cash events may be better served by a conventional high-performance government database with cryptographic audit trails than by a fully decentralised ledger.

Banknote Authentication Model

The authentication pipeline can be represented as a sequential model: physical banknote → optical/physical examination → serial-number recognition → security-feature verification → authenticity scoring. Optical character recognition extracts the serial number and prefix; ultraviolet and infrared sensing evaluate fluorescent security threads and printing characteristics that are difficult to replicate outside RBI's authorised printing process; machine-learning classifiers trained on genuine and counterfeit note images provide a probabilistic authenticity estimate that is combined with rule-based checks (for example, whether the extracted serial number falls within a known issuance range for its prefix and series). This corrects a central technical weakness in the original proposal, in which the serial number alone was implicitly treated as sufficient proof of authenticity. RBI's own counterfeit-detection framework already requires machine-based examination of physical security parameters rather than serial-number verification alone (RBI, 2024b), and the proposed authentication model is consistent with, and extends, that existing institutional practice.

Cash Event And Provenance Model

The architecture's most significant conceptual departure from the original proposal is its rejection of continuous, holder-level possession tracking in favour of event-based recording, organised across three participation tiers.

Level 1: Public voluntary verification. An individual who wishes to verify a suspicious note may do so through a public-facing authorised device or application or devices are built in a manner through apt kyc (know your customer) having unique ID with no public disclosure of individual identity where if there is cash exchanges between individuals it goes through these devices. The device returns a genuine/suspected/refer-to-bank result. No permanent, individually identifiable record needs to be created; if a record is retained at all, it can be limited to aggregate counterfeit-detection statistics.

Level 2 : Regulated businesses. Entities operating above a prescribed cash-handling threshold cash-intensive retailers, jewellery and high-value goods businesses, cash-logistics companies, and similar regulated entities use authorised devices to generate Cash Verification Events for qualifying transactions. These events record entity identity, timestamp, location, transaction value, note count and denominations, and authentication result.

Level 3 : Banking and currency-chest ecosystem. Banks, currency chests, and other authorised government financial nodes operate fully integrated authentication infrastructure, consistent with and extending RBI's existing Master Direction obligations. Deeper analytics, cross-referencing, and mandatory reporting occur at this tier under clearly defined legal authority.

This tiered structure means that ordinary peer-to-peer cash transactions between individuals, and cash held at home, are not captured by the system at all unless a party voluntarily initiates Level 1 verification including risk of fake notes that respective individuals may be having. The system therefore observes a defined subset of the cash economy chosen for its relevance to counterfeit circulation and financial-compliance risk rather than attempting universal coverage, which this paper argues is both more technically feasible and substantially less privacy-invasive.

Privacy Preserving Governance Framework

Privacy-by-design is treated in this paper as a primary research contribution rather than a compliance afterthought, because an architecture that could reveal which individual currently possesses a given banknote would raise serious proportionality and civil-liberty concerns and would be difficult to justify to international reviewers or to defend under India's data-protection law. The proposed governance model borrows the tiered-

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

disclosure logic developed in CBDC privacy research (BIS, 2021; Michalopoulos et al.,2025) and adapts it to three information levels.

Level A: Device level. The authenticating device itself knows only the note's denomination, serial number, and authenticity result at the moment of scanning; it need not transmit or retain identity information about the person presenting the note.

Level B: Central authentication infrastructure. The central system records the authentication event, the device identity, the time, the location, and relevant transaction metadata, but at Levels 1 and 2 this need not be linked to a verified personal identity beyond what the regulated entity itself already collects for other compliance purposes.

Level C: Government investigation. Identity-linked information is disclosed only when an authorised agency meets clearly defined legal conditions for example, a documented counterfeit-circulation investigation or a financial-crime inquiry under existing statutory authority rather than being continuously available for routine querying.

This structure operationalises four principles drawn directly from India's Digital Personal Data Protection Act, 2023 (MeitY, 2023): purpose limitation (data collected for authentication is not repurposed without legal basis), data minimisation (only the minimum data needed for each tier's function is retained), role-based access (investigation-level disclosure is restricted to authorised roles under defined conditions), and auditability (every access to identity-linked information is itself logged and reviewable).The paper argues that adopting this framework transforms the proposal from “every note belongs to a citizen and government continuously knows where it is” into a bounded, purpose-specific, and legally accountable system, which is a materially different and more defensible research proposition.

Counterfeit And Duplicate-Detection Algorithm

A duplicate serial-number event two physically distinct notes bearing the same denomination and serial number is a genuinely interesting anomaly, but it cannot be treated as automatic proof that one note is counterfeit, because India's currency-issuance framework includes legitimate exceptions such as the Star Series, a distinct numbering arrangement introduced for the replacement of defectively printed notes (RBI, 2024b). Treating “duplicate serial equals fake” as an automatic rule would therefore generate a high rate of false positives against legitimately issued replacement notes. The proposed algorithm instead treats a duplicate serial event as an anomaly requiring further authentication and provenance analysis, comparing the serial number, prefix, denomination, series, physical security-feature profile, issuance information, and available scan history of both notes before any classification is made. Only when the corroborating physical-feature comparison is inconsistent with the note's claimed series and issuance batch does the event escalate toward a suspected-counterfeit classification. This staged approach is more defensible academically and operationally than a single-rule heuristic, and provides a natural basis for the empirical testing proposed in Hypothesis 2 (Future research point as mentioned below).

Cash-Flow and Tax-Compliance Intelligence

The event ledger described in cash event and provenance model point mentioned as above can, in principle, generate cash-flow intelligence useful to financial-compliance and tax authorities for example, by flagging entities whose declared cash turnover is substantially inconsistent with the volume of Cash Verification Events associated with them. However, this paper deliberately avoids the claim that such a system would, by itself, stop tax evasion. Cash volume alone is not evidence of wrongdoing, and a system that automatically inferred illegality from cash-handling volume would be both legally and methodologically unsound. Instead, the proposed use is explicitly risk-based: a cash anomaly generates a risk score, which may trigger authorised investigation, which allows the taxpayer or entity to provide an explanation, all conducted through existing legal and tax-administration processes rather than through automated accusation. Framed this way, the system's contribution is best described as generating an additional source of cash-flow intelligence that, when lawfully integrated with existing financial and tax systems, may improve risk-based identification of unexplained cash activity a hedged and testable claim rather than a guarantee of enforcement outcomes.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

Several recent enforcement episodes illustrate why untraceable high-value cash movement, and high-value cash stored outside any authenticated channel, is a live rather than hypothetical concern. Income Tax Department search operations in December 2023 against entities linked to a sitting Rajya Sabha member recovered over ₹351 crore in cash from premises in Odisha and neighbouring states, the largest single cash recovery in the department's history at that time (CBDT, 2024). Search action against a listed manufacturing group in December 2023–January 2024 similarly surfaced approximately ₹1,000 crore in unaccounted cash sales alleged to be outside the group's recorded books, alongside over ₹400 crore in unaccounted cash payments routed through a distributor (CBDT, 2024). Separately, in March 2025 an accidental fire at the official residence of a sitting Delhi High Court judge led firefighters to discover several crore rupees in burnt and semi-burnt currency stored in a storeroom of the premises, a subsequent in-house judicial inquiry found the room to have been under the judge's covert or active control, though the exact amount was never officially confirmed (Supreme Court Observer, 2025). Each of these cases involves cash that had already left, or never entered, any point in the formal cash-processing chain described in existing Indian currency management framework point mentioned as above, and in each case the cash surfaced only incidentally through an investigation triggered by unrelated intelligence or an accidental fire rather than through any systematic authentication or provenance check. This is precisely the class of unobserved, unaccounted cash movement that the event-based Cash Verification Events described in cash event and provenance model point are intended to make partially visible at Level 2 and Level 3 participation, without requiring continuous surveillance of private cash holdings at Level 1.

To make this contribution more precise and empirically testable, the paper proposes a composite metric, the Cash Provenance Confidence Score (CPCS), computed for each authenticated cash unit or event as a function of five components which are authenticity confidence (A), serial-number validity (S), issuance consistency (I), provenance or event consistency (P), and historical anomaly indicators (H), such that CPCS = f(A, S, I, P, H). An illustrative interpretive scale might treat scores of 90–100 as high-confidence genuine, 70–89 as genuine but with incomplete provenance, 40–69 as requiring additional verification, and 0–39 as high-risk or anomalous; the precise functional form and thresholds are matters for future empirical calibration rather than claims made here. The value of the CPCS as a research construct is that it converts a qualitative authentication judgment into a metric that can be modelled, validated, and empirically tested against ground-truth counterfeit and genuine-note datasets.

Implementation Framework

Given the transaction volumes, device-deployment costs, network requirements, and privacy risks that a universal, individual-level scanning mandate would entail, this paper recommends a phased and hybrid implementation pathway rather than simultaneous nationwide deployment. The recommended sequence begins with a limited pilot confined to a small number of bank branches and currency chests, extending RBI's existing machine-based authentication infrastructure with the enhanced multi-feature model described in Banknote authentication model point and cash event and provenance model point mentioned as above. A second phase would extend mandatory participation to regulated, cash-intensive businesses above a defined cash-handling threshold, consistent with Level 2 of the proposed tiered model. A third phase would integrate the resulting event data with existing banking and currency-chest reporting channels already mandated under RBI's Master Direction (RBI, 2024b, 2026), rather than creating a parallel reporting structure. Voluntary public verification (Level 1) can be introduced at any stage, since it requires no mandatory participation and carries the lowest privacy risk. Government risk-based investigation access (Level 3 disclosure) should be activated only once the legal and procedural safeguards described in privacy preserving governance framework point mentioned as above are formally established. This sequencing prioritises operational feasibility and stakeholder acceptance over comprehensiveness, consistent with Hypothesis 5 (Future research point).

Economic And Social Impact

If validated empirically, the proposed architecture could offer benefits across several areas, each of which should be understood as a potential rather than a demonstrated outcome pending pilot evidence. In counterfeit-currency management, multi-feature authentication combined with anomaly detection could enable earlier identification of counterfeit notes than reliance on serial-number checks or manual inspection alone. In currency management

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

more broadly, event-level data from regulated businesses and banking nodes could improve RBI's intelligence about physical-cash circulation patterns. In financial compliance, the proposed risk-based cash-flow indicators could supplement existing methods for identifying unexplained cash activity without displacing due-process protections. In law enforcement, provenance and anomaly data could provide investigative leads in counterfeit-currency cases, subject to the legal-access conditions described in privacy preserving governance framework point mentioned as above. In monetary-policy research, aggregated and anonymised event data could improve understanding of physical-cash velocity and usage patterns. Finally, for public confidence, the voluntary Level 1 verification channel could give ordinary citizens and small businesses an accessible means of checking a suspicious note, which is not widely available today outside bank counters. Each of these potential benefits should be read with the qualifiers "potential," "could," and "may" until empirical evidence from pilot deployment establishes actual effect sizes.

Risk And Limitations

Several risks and limitations should be acknowledged explicitly rather than minimised. First, a poorly governed implementation could drift toward the very surveillance model this paper explicitly rejects the tiered-disclosure safeguards in privacy preserving governance framework point mentioned as above are necessary but not sufficient without independent oversight and periodic audit. Second, device cost and deployment logistics at Level 2 and Level 3 scale are non-trivial, particularly for smaller regulated businesses, and may require subsidy or phased thresholds to avoid disproportionate compliance burden. Third, machine-learning-based authenticity classifiers can misclassify genuine notes as suspect or vice versa, false-positive and false-negative rates must be empirically established and communicated transparently before any mandatory deployment. Fourth, sophisticated counterfeiters may eventually attempt to replicate observable security features closely enough to defeat automated classifiers, which argues for continuous feature updates consistent with RBI's existing practice of periodically upgrading banknote security features (RBI, 2024b). Fifth, network connectivity and infrastructure gaps in rural or low-connectivity regions could create uneven authentication coverage, potentially disadvantaging regions least served by banking infrastructure. Sixth, any future extension toward broader participation thresholds carries a structural risk of scope creep toward the universal tracking model this paper explicitly argues against; statutory limits on future threshold expansion should be considered as an institutional safeguard. Finally, because this paper is conceptual, all quantitative interpretive scales including the CPCS thresholds proposed in cash flow and tax compliance-intelligence point mentioned as above are illustrative pending empirical calibration against real authentication data, and should not be treated as validated operational parameters.

Future Research

Future work should proceed in four stages consistent with the conceptual maturation reflected in this paper. First, a structured pilot design should specify the authentication device's feature set, sample size, and evaluation metrics against a labelled dataset of genuine and counterfeit notes, enabling direct empirical testing of Hypothesis 1 (multi-feature authentication accuracy relative to serial-number-only verification) and Hypothesis 2 (false-positive reduction from combining serial and physical-feature analysis). Second, a technical specification of the Event Ledger, Alert Engine, and cryptographic audit-log design should be developed, drawing on the privacy-preserving techniques identified in the CBDC literature (BIS,2021; Michalopoulos et al.,2025), to test Hypothesis 3 empirically against the data-volume requirements of continuous holder-level tracking. Third, stakeholder-acceptance research surveying banks, regulated businesses, and citizens should test Hypothesis 4 concerning whether privacy-preserving access controls improve acceptance relative to an unrestricted-traceability design. Fourth, an implementation-feasibility study comparing phased banking/regulated-business deployment against a hypothetical universal deployment would test Hypothesis 5. Collectively, these research questions and hypotheses are intended to convert the architectural proposal advanced in this paper into a testable empirical research programme.

Research Questions

RQ1: Can a national banknote authentication architecture improve the detection of counterfeit Indian currency

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

compared with conventional verification mechanisms?

RQ2: Can serial-number recognition combined with physical security-feature verification identify duplicate or anomalous banknote events with acceptable accuracy?

RQ3: What level of cash-event traceability is necessary to improve financial compliance without creating disproportionate surveillance of citizens?

RQ4: Can privacy-preserving technologies enable authorised verification while limiting unnecessary disclosure of individual transaction histories?

RQ5: What are the economic, technological, and institutional requirements for nationwide implementation?

Hypotheses

H1: A multi-feature banknote authentication system will demonstrate higher counterfeit-detection accuracy than serial-number-only verification.

H2: Combining serial-number information with physical security-feature analysis will reduce false-positive identification of counterfeit notes.

H3: Event-based cash traceability will provide useful financial-compliance intelligence while requiring less personal data than continuous holder-level tracking.

H4: Privacy-preserving access controls will improve stakeholder acceptance of the proposed system compared with unrestricted cash traceability.

H5: A phased implementation through banks and regulated cash-intensive businesses will provide higher operational feasibility than universal mandatory deployment among individuals.

CONCLUSION

This paper has reframed an initial proposal for individual-level banknote tracking into the National Banknote Authentication and Traceability System (NBATS), a five-layer, privacy-constrained architecture that authenticates banknotes through multi-feature verification, records cash-handling activity through discrete events rather than continuous possession, and tiers information disclosure according to purpose and legal authority. The proposed Cash Provenance Confidence Score offers a testable, quantifiable expression of authentication and provenance confidence, while the three-tier participation model voluntary public verification, regulated-business authentication, and integrated banking/currency-chest infrastructure offers a more operationally feasible pathway than universal deployment. By building explicitly on RBI's existing counterfeit-detection framework rather than claiming to replace it, and by treating privacy-by-design as a central research contribution consistent with India's Digital Personal Data Protection Act, 2023, the proposal is positioned as an incremental but substantive extension of India's currency-management ecosystem. This paper has deliberately used hedged, probabilistic language throughout when describing potential benefits, since the architecture remains conceptual pending pilot implementation and empirical validation of the research questions and hypotheses set out above. Future work operationalising the pilot design, technical specification, and stakeholder-acceptance studies proposed in Future research point is required before any claims of demonstrated impact can be made.

REFERENCES

1. Auer, R., & Böhme, R. (2021). Central bank digital currency: The quest for minimally invasive technology (BIS Working Paper No. 948). Bank for International Settlements. https://www.bis.org/publ/work948.pdf

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VIII, August 2026

2. Bank for International Settlements. (2021). Central bank digital currencies: A guided tour (BIS Working Paper No. 976). https://www.bis.org/publ/work976.pdf
3. Ilori, O., et al. (2024). Privacy implications of central bank digital currencies (CBDCs): A systematic review of literature. Journal of Payments Strategy & Systems. https://www.tandfonline.com/doi/full/10.1080/07366981.2024.2376794
4. Michalopoulos, P., Olowookere, O., Pocher, N., Sedlmeir, J., Veneris, A., & Puri, P. (2025). Privacy and compliance design options in offline central bank digital currencies. IEEE Transactions on Network and Service Management, 22(5), 3748–3762.
5. Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act, 2023. Government of India. https://www.meity.gov.in/
6. Reserve Bank of India. (2024a). Annual report on currency management. https://www.rbi.org.in/
7. Reserve Bank of India. (2024b). Master direction on counterfeit notes, 2024 – Detection, reporting and monitoring. https://www.rbi.org.in/
8. Reserve Bank of India. (2026, July 31). Circular RBI/2026-27/220: Strengthening detection, reporting and monitoring of fake Indian currency notes. https://www.rbi.org.in/
9. Taxguru. (2024, April 1). Master direction on counterfeit notes, 2024 – Detection, reporting & monitoring. https://taxguru.in/rbi/master-direction-counterfeit-notes-2024-detection-reporting-monitoring.html
10. World Economic Forum, Digital Currency Governance Consortium. (2021). Privacy and confidentiality options for central bank digital currency. https://www3.weforum.org/docs/WEF_Privacy_and_Confidentiality_Options_for_CBDCs_2021.pdf
11. Reserve Bank of India. (2025). Annual report 2024-25. https://www.rbi.org.in/
12. National Crime Records Bureau. (2024). Crime in India 2024. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/
13. Central Board of Direct Taxes. (2024). Press statements on search and seizure operations, December 2023-January 2024. Ministry of Finance, Government of India. https://www.incometax.gov.in/
14. Supreme Court Observer. (2025). Justice Varma cash inquiry: The story so far. https://www.scobserver.in/journal/justice-varma-cash-inquiry-the-story-so-far/