

Blockchain-Based Tamper-Evident Chain of Custody for Criminal Evidence: A Proposed Framework for Bangladesh

Mr. MD. SAZZAD HOSSAIN¹, Mr. Ariful Haque²

Independent Researcher*

Abstract: Criminal justice systems depend on an unbroken, verifiable chain of custody (CoC) to prove that evidence presented in court is the same evidence collected at the crime scene, unaltered and unsubstituted. In Bangladesh, custody records remain largely paper-based, tracked through police malkhana (property room) ledgers vulnerable to loss, forgery, and unrecorded handling, with no unified mechanism linking crime-scene seizure, forensic analysis, and courtroom production. This paper proposes a permissioned blockchain framework binding physical exhibits to tamper-evident tagged containers and digital exhibits to content-addressed hashes, recording every custody transfer as an immutable, multi-signed ledger transaction. The framework defines five stakeholder roles, a seven-state custody lifecycle enforced by chaincode, and a governance model in which Bangladesh Police, the Police Bureau of Investigation, the Criminal Investigation Department, and the judiciary each operate a validating node, preventing unilateral alteration of custody records. The design is evaluated qualitatively against eight existing blockchain chain-of-custody proposals, none of which jointly address physical-evidence tagging, offline-first operation, and alignment with Bangladesh evidentiary statutes. A narcotics-seizure scenario illustrates the workflow, and a threat model examines insider tampering, key loss, and collusion resistance. The paper concludes with implementation challenges and a phased adoption roadmap.

Keywords: Blockchain; Chain of Custody; Digital Forensics; Criminal Evidence; Tamper-Evident Systems; Hyperledger Fabric

I. INTRODUCTION

A. Background and Motivation

Evidence is the currency of criminal adjudication: a conviction or an acquittal ultimately rests on whether the exhibit produced in court can be shown, beyond reasonable doubt, to be identical to the exhibit recovered at the scene and untouched by unauthorised hands in the interim. The procedural record that carries this guarantee is the chain of custody (CoC) - a chronological log of every person who collected, transported, stored, examined, or otherwise possessed an item of evidence, together with the date, purpose, and condition of each transfer [1], [2]. A single undocumented gap in this chain is often sufficient grounds for a defence challenge to admissibility, irrespective of the underlying probative value of the evidence itself.

Bangladesh's criminal justice system continues to rely on manual, paper-based custody registers maintained at police stations (thanas) and in malkhanas, the physical property rooms where seized exhibits - narcotics, weapons, currency, documents, and digital devices - are stored pending trial. Independent assessments of Bangladesh's investigative practice describe recurring procedural weaknesses in crime-scene management and evidence preservation: investigating officers frequently reach crime scenes only after the site has been compromised, standard evidence-collection kits are inconsistently available or used, and a substantial share of officers report being unable to secure the crime scene from contamination by bystanders or fellow responders [3].

A nationwide review of malkhanas across Bangladesh's roughly 622 police stations found that seized exhibits are commonly tracked with nothing more than a handwritten Property Register (PR) number, with no photographic record, condition log, or systematic inventory beyond that single entry; investigators reported exhibits damaged by rats, monsoon flooding, and improvised open-air storage, and cited these conditions as a contributing factor behind a backlog of roughly 3.7 million pending court cases nationwide [4]. Because a malkhana's PR register is the only record linking a stored exhibit to its case file, an exhibit that is lost, damaged, or misplaced within the property room - as opposed to being deliberately tampered with - leaves no independent trail from which its custody history can be reconstructed.

The scale of this vulnerability was demonstrated starkly during the mass uprising of July-August 2025, when arson attacks on police installations damaged an estimated 460 stations, outposts, and other facilities nationwide and burned at least 526 police vehicles. Thirteen Dhaka Metropolitan Police stations were burned on 5-6 August 2025 alone, destroying documentation for roughly 1,200 cases and physical evidence - including forensic and DNA reports - for around 1,100 more [5]. Because each station's paper-based custody register was the sole copy of its case history, no institution outside the affected thana retained any record of custody for the destroyed cases - precisely the kind of single-point-of-failure vulnerability that a replicated, multi-institution ledger is designed to remove.

Forensic capacity compounds the problem even without such extraordinary events. Bangladesh operates a small number of forensic laboratories capable of DNA and trace analysis, and case backlogs routinely delay analysis by months, during which samples sit in storage with limited environmental or access control [6], [7]. Legal commentary on the admissibility of digital evidence further notes that many thanas lack officers trained to handle electronic exhibits, that frequent transfers of trained personnel erode institutional capacity, and that electronic evidence is exposed to manipulation between seizure and trial with no technical mechanism to detect tampering

after the fact [8]. A recent assessment of Bangladesh's forensic science sector similarly links resource constraints and limited institutional capacity to case backlogs and delayed trials [9].

Blockchain technology - a distributed, append-only ledger in which each block is cryptographically linked to its predecessor - offers a structural answer to exactly this class of problem. Once a custody event is recorded and accepted by the network, altering it would require rewriting every subsequent block and obtaining the consent (or compromising the keys) of a quorum of independent validators, a property that shifts the trust model from "a single custodian's word" to "cryptographic proof plus institutional consensus" [11]. A substantial body of research since 2018 has explored blockchain-based chain-of-custody systems for digital evidence, and a smaller body has begun to examine physical-evidence tracking, but no existing proposal integrates physical-exhibit tagging, offline-tolerant field operation, and the specific statutory and institutional landscape of Bangladesh.

B. Problem Statement

Three concrete gaps motivate this work. First, Bangladesh's custody record for physical evidence is a paper ledger: entries can be back-dated, pages can be replaced, and there is no cryptographic proof that a given exhibit corresponds to the seizure entry that describes it. Second, where digital evidence is concerned, hash values are sometimes computed at the forensic laboratory but rarely at the point of seizure, so the chain of custody cannot prove that the file examined in the lab is bit-for-bit identical to the file that existed on the seized device at the moment of collection. Third, no shared ledger connects the investigating officer, the malkhana, the forensic laboratory, the prosecution, and the court; each institution keeps its own paper trail, and reconciling them after the fact - often years later, when a case finally reaches trial - is itself a source of error and dispute.

C. Contributions

- A permissioned blockchain architecture that unifies custody tracking for both physical exhibits (via tamper-evident RFID/QR-tagged containers) and digital exhibits (via SHA-256 content hashing and IPFS-based off-chain storage).
- A seven-state custody lifecycle - Seized, Logged, In Transit, Under Forensic Analysis, In Storage, Produced in Court, Disposed - enforced by chaincode, with multi-signature confirmation required at every state transition.
- A governance and validator model that distributes ledger-write authority across Bangladesh Police, the Police Bureau of Investigation, the Criminal Investigation Department, and the judiciary, so that altering a historical record would require collusion across institutions that are not otherwise aligned.
- An offline-first design accommodating thanas with intermittent connectivity.
- A mapping between the technical design and Bangladesh's existing evidentiary statutes, identifying where the framework can operate under current law and where amendment would be required.
- A qualitative comparison against eight prior blockchain chain-of-custody systems, an illustrative end-to-end scenario, and a threat-model analysis grounded in a documented real-world tampering case.

D. Paper Organisation

Section II reviews prior blockchain-based chain-of-custody research. Section III analyses the gap this work addresses relative to that literature. Section IV presents the proposed methodology: design goals, stakeholder roles, system architecture, physical- and digital-evidence binding, the custody lifecycle, and legal alignment. Section V describes the experimental (evaluation) setup. Section VI presents results and discussion, including a comparative analysis, an illustrative scenario, a threat-model analysis, implementation challenges, limitations, and future work. Section VII concludes the paper.

II. LITERATURE REVIEW

Interest in applying blockchain to evidence management dates to the late 2010s, driven by the observation that a distributed ledger's immutability and multi-party verifiability map naturally onto the chain-of-custody requirement, first articulated for cryptocurrency [10]. This section groups prior work into three strands before identifying the gap this paper addresses in Section III.

A. Digital-Evidence Chain-of-Custody Frameworks

Bonomi, Casini, and Ciccotelli proposed B-CoC, a permissioned Ethereum-based system in which an evidence log records hashes and custody metadata while the evidence itself is kept in a separate database, demonstrated with a Geth/IBFT prototype [11]. Tian, Li, Qiu, Sun, and Su proposed Block-DEF, which uses a loosely coupled design separating evidence content from evidence information and an optimised Byzantine fault-tolerant consensus mechanism together with multi-signature schemes to balance traceability against privacy [12]. Lone and Mir presented Forensic-Chain, a Hyperledger Composer proof-of-concept aimed at bringing tamper resistance to the digital-forensics custody process [13]. Ahmad, Khanji, Iqbal, and colleagues proposed a real-time, tamper-proof evidence-management framework enabling continuous tracking and cross-agency collaboration [14]. Burri, Casey, Bollé, and Jaquet-Chiffelle developed an independently verifiable electronic chain-of-custody history record using blockchain technology [15].

Alruwaili's CustodyBlock combines a private blockchain protocol with smart contracts to support control, transfer, analysis, and preservation-monitoring phases of custody [16]. Yan, Shen, Cao, and Dong proposed a digital-evidence custody protocol built on revocable ciphertext-policy attribute-based encryption combined with BLS signatures and blockchain logging [17]. Lavín and Llanos reviewed blockchain-based chain-of-custody solutions against the ISO/IEC 27037 standard [28] and reported that most existing systems fall short on auditability, scalability, and legal-admissibility criteria [18].

B. IoT, Vehicular, and Networked-Device Forensics

Cebe, Erdin, Akkaya, Aksu, and Uluagac proposed Block4Forensic, a lightweight blockchain framework tailored to forensic investigation of connected vehicles [19]. Pourvahab and Ekbatanifard designed a forensics architecture for software-defined networking and IoT environments that uses blockchain to preserve the integrity of network-derived evidence [20]. This strand is narrower in scope than the general criminal-evidence custody problem addressed here, since it is optimised for device telemetry rather than the seizure-to-courtroom workflow governing physical exhibits and general-purpose digital devices.

C. Physical Evidence and Standards Alignment

Physical-evidence custody has historically been addressed through non-blockchain means such as RFID and barcode tracking in police

property rooms, which improve location tracking and access logging but do not provide cryptographic tamper-evidence for the underlying custody record itself [21], [22]. A systematic literature review by Batista et al. examining blockchain applications specifically for the physical-evidence chain of custody reviewed twenty-six published sources and concluded that, in contrast to the substantial body of digital-evidence work, the application of blockchain to controlling physical-evidence custody has received comparatively limited research attention [23]. Building in part on that gap, Hung, Dung, and Tu subsequently designed a Hyperledger Fabric-based system in which each step of an exhibit's handling is recorded as a permanent ledger entry separate from the exhibit itself, with every step signed and timestamped so that interference with the record can be detected after the fact [24].

III. RESEARCH GAP

Table I summarises the coverage of representative prior systems against six criteria relevant to a deployable national framework: support for physical-evidence tagging, support for digital-evidence hashing, offline-tolerant field operation, multi-institutional governance (as opposed to a single operator), explicit alignment with a national evidentiary statute, and a defined courtroom-production workflow. No reviewed system jointly satisfies all six criteria. Systems reviewed in Section II-A are digital-evidence-only; the systems in Section II-B are domain-specific to IoT or vehicular telemetry; the physical-evidence-oriented work in Section II-C does not integrate digital-evidence hashing or address a specific national legal framework. None of the reviewed systems were designed with, or evaluated against, the connectivity constraints of rural or under-resourced police stations, a practical concern central to deployability in Bangladesh and comparable jurisdictions.

TABLE I. COVERAGE OF REPRESENTATIVE BLOCKCHAIN CHAIN-OF-CUSTODY PROPOSALS AGAINST DEPLOYMENT-RELEVANT CRITERIA

System	Physical Tagging	Digital Hashing	Offline-Tolerant	Multi-Inst. Governance	Statute Alignment	Court-Prod. Workflow
B-CoC [11]	No	Yes	No	No (single)	No	Partial
Block-DEF [12]	No	Yes	No	No (single)	No	No
Forensic-Chain [13]	No	Yes	No	No (single)	No	Partial
Ahmad et al. [14]	No	Yes	No	Partial	No	Partial
Custody Block [16]	No	Yes	No	No (single)	No	No
Yan et al. [17]	No	Yes	No	No (single)	No	No
Block4 Forensic [19]	Partial (vehicle)	Yes	No	No	No	No

System	Physical Tagging	Digital Hashing	Offline-Tolerant	Multi-Inst. Governance	Statute Alignment	Court-Prod. Workflow
Physical - evidence SLR [23]	Yes	No	No	No (single)	No	Partial
Proposed Framework	Yes	Yes	Yes	Yes (4-party)	Yes (Bangladesh)	Yes

The framework proposed in Section IV is designed to close this combined gap: it jointly supports physical-evidence tagging, digital-evidence hashing, offline-tolerant operation, multi-institution governance, and alignment with Bangladesh's evidentiary statutes, within a single architecture.

IV. PROPOSED METHODOLOGY

A. Design Goals

- Tamper-evidence, not just tamper-resistance: every custody event must be independently verifiable by any authorised party, not merely difficult to forge.
- Coverage of both physical and digital exhibits within one ledger.
- No single point of institutional control: no one agency should be able to unilaterally alter a historical custody record.
- Operability under intermittent connectivity, reflecting the reality that many thanas outside major metropolitan areas lack reliable continuous internet access.
- Minimal disruption to existing seizure procedure.
- Legal traceability: the technical record should map onto the custody information required under Bangladeshi evidentiary statutes.

B. Stakeholders and Roles

The framework defines five principal roles, each holding a distinct cryptographic identity issued through a permissioned certificate authority: Seizing Officer (SO), who recovers an exhibit and creates the first ledger entry; Malkhana Custodian (MC), responsible for the property room and who countersigns every physical handover; Forensic Examiner (FE), laboratory personnel who log examination events; Prosecutor (PR), who requests exhibit production for trial; and Court Registrar (CR), who confirms receipt at trial and authorises final disposal.

C. System Architecture

The framework is built on a permissioned blockchain. Hyperledger Fabric is used as the reference platform rather than an account-based platform using Byzantine-fault-tolerant consensus directly on a single shared ledger, because two of its native features map directly onto this framework's requirements: channels, which give each operational domain (police, forensic, judicial) its own segregated ledger and membership, and flexible endorsement policies, which let a transaction type require approval from a specific quorum of organisations without custom chaincode logic. Fig. 1 summarises how a single transaction moves through the network: a client application submits a proposal to endorsing peers, which simulate

and sign the transaction; the client forwards the endorsed transaction to the ordering service, which sequences it into a block using the Raft consensus protocol; the block is distributed to every peer in the channel, each of which validates the endorsement policy before committing it. Every validating institution holds an identical copy once a block commits, which is what gives the four-institution governance model (Section IV-H) its practical effect.

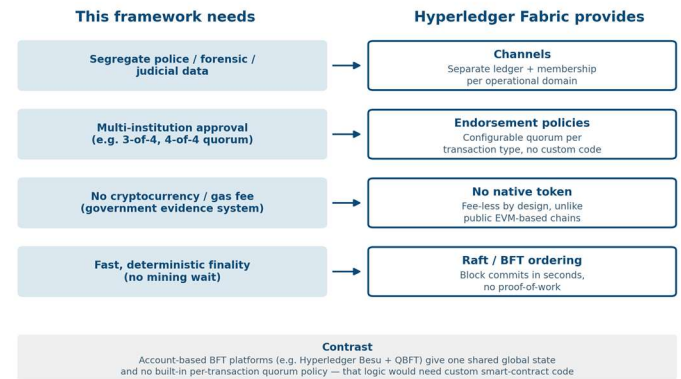


Fig. 1. Why Hyperledger Fabric fits this framework's requirements, in contrast to an account-based BFT platform such as Hyperledger Besu with QBFT.

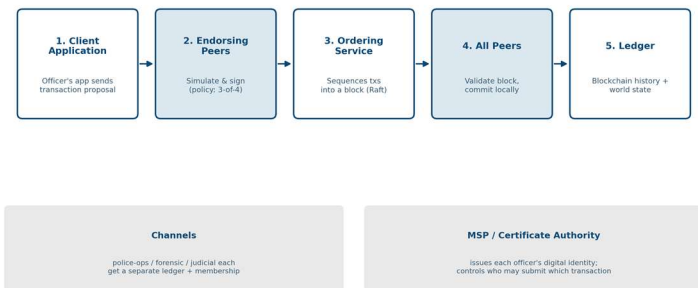


Fig. 2. Hyperledger Fabric transaction lifecycle: proposal, endorsement, ordering, validation, and commitment to the ledger.

A police-operations channel carries seizure, transport, and malkhana events; a forensic channel carries laboratory examination events; and a judicial channel carries court-production and disposal events. Four institutions - Bangladesh Police, the Police Bureau of Investigation (PBI), the Criminal Investigation Department (CID), and the judiciary - each operate a validating peer node. A transaction commits only after endorsement by a policy-defined quorum (e.g., any three of the four for a routine transfer, all four for disposal), so that no single institution can rewrite history unilaterally. Digital exhibit content itself is not stored on-chain; files are stored in a permissioned InterPlanetary File System (IPFS) cluster operated jointly by the four institutions, and only the resulting content hash is written on-chain, following the same loose-coupling principle used in Block-DEF and B-CoC.

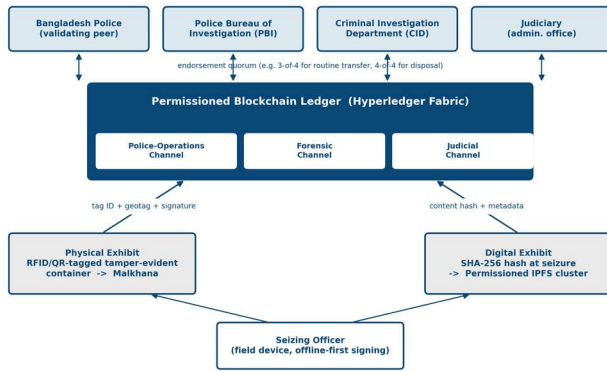


Fig. 3. Permitted four-institution validator architecture: channel segregation, on-chain hash binding for physical and digital exhibits, and off-chain IPFS storage.

D. Binding Physical Evidence to the Ledger

At the point of seizure, the Seizing Officer places the physical exhibit into a tamper-evident evidence bag or container fitted with a unique, non-reusable RFID tag or a printed QR code bonded to a frangible security seal, technology already used in evidence-tracking deployments elsewhere [21], [22], such that any attempt to open the container without breaking the seal is physically detectable. The SO's field device reads the tag identifier, captures a geotagged timestamp and photographs, and computes a seizure record. Where network connectivity is unavailable, this record is signed and stored locally, queued for submission once connectivity is restored. From this point forward, the tag identifier is the exhibit's permanent reference key on the ledger.

Not every physical exhibit can be tagged or preserved intact. Forensic testing consumes chemical or biological samples, and some evidence cannot be seized as a discrete transportable object at all. For consumable or non-transportable evidence, the framework's contribution is limited to the surrounding documentation - photographs, laboratory consumption logs, and hashes of any resulting digital record - each logged as its own custody event.

E. Binding Digital Evidence to the Ledger

For digital exhibits, the Seizing Officer or a forensic first responder computes a SHA-256 hash of the acquired image at the point of collection, and this hash - not the file itself - is written to the ledger together with acquisition metadata. Any later party can independently recompute the hash and compare it against the on-chain value; a mismatch is immediate, mathematical proof of alteration. This directly addresses the gap identified in Section I-B, where hash values are today typically computed only once evidence reaches a forensic laboratory.

F. Custody Lifecycle and Transfer Workflow

The chaincode enforces a seven-state lifecycle for every exhibit, illustrated in Fig. 4 and detailed in Table II: Seized, Logged, In Transit, Under Forensic Analysis, In Storage, Produced in Court, and Disposed. Each transition requires a transaction signed by the initiating role and countersigned by the receiving role, so a transfer can never be recorded unilaterally. Transitions that skip a state are rejected by the chaincode.



Fig. 4. The seven-state custody lifecycle enforced by chaincode (SO: Seizing Officer, MC: Malkhana Custodian, FE: Forensic Examiner, PR: Prosecutor, CR: Court Registrar).

TABLE II. CUSTODY LIFECYCLE STATES, AUTHORISED INITIATOR, AND REQUIRED COUNTERSIGNATURE

State	Authorised Initiator	Required Countersignature	Trigger Event
Seized	Seizing Officer	— (tag/hash creation)	Recovery of exhibit at crime scene
Logged	Seizing Officer	Malkhana Custodian	Physical/digital intake at thana or malkhana
In Transit	Malkhana Custodian	Receiving party (FE or CR)	Dispatch for analysis or court production
Under Forensic Analysis	Forensic Examiner	Malkhana Custodian (return ack.)	Receipt at forensic laboratory
In Storage	Forensic Examiner	Malkhana Custodian	Return of exhibit/report to malkhana
Produced in Court	Prosecutor	Court Registrar	Court order or trial exhibit request
Disposed	Court Registrar	All four validating institutions	Final judicial order for disposal/return

A correction to a previously recorded value is never made by editing a committed transaction; instead, a correction is a new, separately signed transaction that references and supersedes the earlier entry, while the original remains visible in the ledger's history.

G. Malkhana Digitisation and Storage Integrity

Within the malkhana, shelf- or bin-level RFID readers continuously verify that tagged exhibits remain in their assigned location; any unscheduled movement without a corresponding on-chain transfer transaction triggers an alert and is itself logged as an anomaly event, converting the malkhana from a passively-registered storage room into an actively monitored environment.

H. Alignment with Bangladesh's Legal Framework

The Evidence Act 1872 does not currently define a specific procedure for blockchain-attested records, but its general admissibility provisions for documentary and electronic evidence provide a basis on which a blockchain custody log could be tendered in the same way that other electronic custody records are tendered today [8], [26]. The DNA Act 2014 requires that DNA samples be protected from tampering; the framework's malkhana monitoring and

forensic-transfer logging provide a technical mechanism for the tamper-protection the Act already requires, without altering its substantive provisions [27]. Two legal gaps remain: Bangladeshi law does not yet explicitly recognise a distributed ledger record as a form of custody documentation with defined evidentiary weight, and cross-agency data-sharing arrangements would need a formal memorandum of understanding to establish the shared validator governance described in Section IV-C.

A further consideration is the exposure of sensitive case details to every institution holding a validating node on the relevant channel. Channel segregation limits this exposure to institutions genuinely involved in a given exhibit's custody, but Bangladesh does not yet have a comprehensive data-protection statute comparable to the EU's GDPR, so field-level encryption of sensitive metadata is identified as necessary future work rather than a solved problem in the present design.

V. EXPERIMENTAL SETUP

This study follows a design science research (DSR) methodology, the approach commonly used in information systems research for developing and rigorously evaluating artefacts intended to solve an identified organisational problem [30], structured around the six-activity process model of Peffers et al. [31]: problem identification and motivation (Section I), definition of objectives (Section IV-A), design and development (Sections IV-B to IV-H, informed by the literature review and gap analysis in Sections II-III), demonstration (Section VI-B), evaluation (Sections VI-A and VI-C), and communication (this paper).

Because no working prototype has been implemented or tested under operational load, the evaluation reported in Section VI is necessarily analytical and comparative rather than quantitative. It comprises three components, each with its own evaluation setup: (i) a structured qualitative comparison against the eight prior systems identified in Section III, scored against the six criteria in Table I and three further design-choice dimensions in Table III; (ii) a walkthrough of an illustrative narcotics-seizure scenario constructed to exercise every state of the custody lifecycle in Table II and every stakeholder role defined in Section IV-B; and (iii) a threat-model analysis in which candidate threat scenarios were drawn from the attack surfaces exposed by the architecture in Section IV-C together with a documented real-world tampering case, and each scenario was assessed against the specific architectural control intended to mitigate it.

VI. RESULTS AND DISCUSSION

A. Comparative Analysis

Table III extends the structural comparison in Table I to specific design choices, summarising why each choice was preferred over the corresponding alternative used in prior work.

TABLE III. DESIGN CHOICES IN THE PROPOSED FRAMEWORK RELATIVE TO REPRESENTATIVE PRIOR SYSTEMS

Design Element	Proposed Framework	Typical Prior Approach
Physical exhibit reference	Tamper-evident RFID/QR-tagged container bound on-chain at seizure	Not addressed, or handled by separate non-blockchain RFID system [21], [22]

Design Element	Proposed Framework	Typical Prior Approach
Digital exhibit reference	SHA-256 hash computed at seizure, IPFS off-chain storage	Hash often computed only at forensic laboratory intake [11], [12]
Consensus / governance	4-institution quorum endorsement	Single-operator permissioned chain [11], [13], [16]
Connectivity model	Offline-first: local signing, queued sync	Assumes continuous connectivity
Legal alignment	Explicit mapping to Evidence Act 1872, DNA Act 2014	Not jurisdiction-specific

B. Illustrative Scenario: Narcotics Seizure

To illustrate the end-to-end workflow, consider a narcotics seizure during a routine patrol. The Seizing Officer recovers a sealed packet, places it into a tamper-evident bag fitted with an RFID tag, and records a Seized transaction from a field device; because the patrol area has no data connectivity, the transaction is signed locally and queued. On return to the thana, the device synchronises and the transaction commits, endorsed by the Bangladesh Police validating peer and at least two of the remaining three peers. The exhibit is physically handed to the Malkhana Custodian, who scans the tag and countersigns a Logged transaction; the malkhana's fixed RFID readers subsequently confirm the tag remains within the designated storage zone.

When laboratory testing is requested, a Malkhana Custodian-initiated In Transit transaction is created, and the Forensic Examiner countersigns intake, moving the exhibit to Under Forensic Analysis. Months later, when the case reaches trial, the Prosecutor's production request generates a Produced in Court transaction, and the Court Registrar confirms receipt. Fig. 5 illustrates the resulting view for a judge or other authorised court user: entering the case or tag ID retrieves the exhibit's full custody timeline, the endorsing institutions for each transfer, and a hash-verification check confirming that the digital record matches the laboratory's own copy.

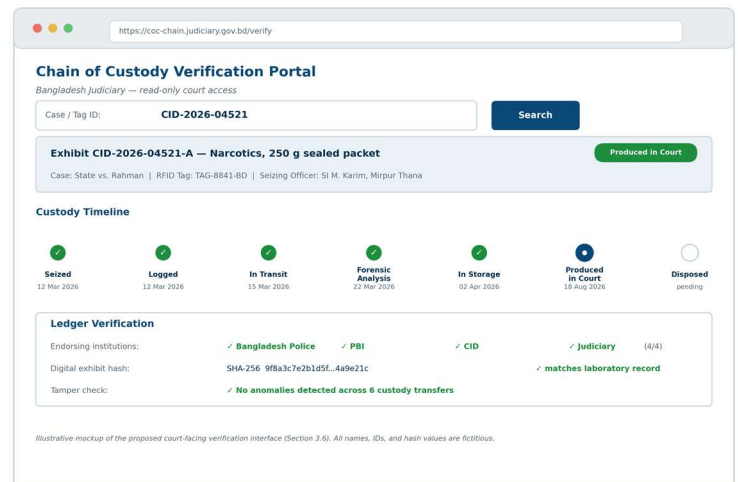


Fig. 5. Illustrative mockup of the court-facing verification interface: case/tag ID lookup, custody timeline, and ledger verification panel.

C. Threat and Failure-Mode Analysis

TABLE IV. THREAT SCENARIOS AND FRAMEWORK MITIGATIONS

Threat Scenario	Risk	Framework Mitigation
Malkhana custodian unilaterally alters a stored exhibit's record	High (single-institution insider)	Multi-signature transfer requirement; 4-institution endorsement quorum
Compromised or coerced officer private key used to sign a false transaction	Medium	Countersignature requirement; credential revocation via institutional CA
Field device lost before synchronisation	Medium (offline-first design)	Tamper-evident physical seal acts as fallback integrity check
Collusion across all four validating institutions	Low but non-zero	Acknowledged residual risk; mitigated by institutions' divergent oversight, not eliminated by design alone
RFID tag cloning or spoofing	Medium	Non-reusable tags bonded to frangible seals; tag ID alone insufficient without matching signature and geotag
Digital evidence altered between seizure and laboratory intake	High under current paper-based process	Seizure-time SHA-256 hashing enables independent mismatch detection
Physical destruction of a thana (fire, riot, natural disaster)	High - demonstrated in practice [5]	Custody ledger is replicated across all four institutions' nodes, so records survive station loss
Fabricated evidence at the point of seizure (planted or misdescribed item)	Not mitigated by the ledger	Outside the framework's technical scope; requires procedural safeguards (body-worn cameras, witnesses, oversight)
Sensitive case data exposed to all institutions on a shared channel	Medium, given no comprehensive data-protection statute	Channel segregation limits exposure; field-level encryption identified as future work

This is not a hypothetical risk. In one documented case, the officer-in-charge of a thana in Bogura district was accused of deleting video evidence from a mobile phone seized in a rape investigation before the device reached the forensic laboratory, allegedly after accepting payment from the accused's side; the case took roughly three years to progress from the original complaint to an arrest warrant against the officer [25]. Under the framework proposed here, the seizure-time hash of the device image would have been visible on the ledger to all four validating institutions from the outset, so any deletion or alteration would surface as a hash mismatch rather than remaining undetected for years.

A distinct and more fundamental limitation, sometimes called the oracle problem in blockchain literature, is that the framework can

only guarantee that a record has not been altered after it was committed - it cannot guarantee that the record was true when it was first created. An officer who fabricates a seizure produces a custody record that is internally consistent and passes every technical check described in this paper, because the tampering occurs before the first ledger entry. The framework therefore secures the chain of custody from the point of seizure onward; it does not, and cannot by itself, secure the honesty of the seizure itself. This limitation is not unique to blockchain-based systems; it applies equally to the paper-based process the framework replaces.

D. Implementation Challenges Specific to Bangladesh

Deploying the framework nationally would confront several practical constraints. Connectivity remains uneven outside major cities, which the offline-first design addresses but does not eliminate. Hardware provisioning represents a recurring procurement and maintenance cost that would need to be budgeted centrally given the resource disparities documented across Bangladesh's forensic and investigative infrastructure. Training is a further constraint, given the same institutional-capacity gaps that limit forensic and digital-evidence handling today. Inter-agency governance - reaching and sustaining the four-institution validator arrangement - is as much a policy undertaking as a technical one.

The roughly 3.7 million cases already pending under the existing paper-based system present a migration question the framework does not resolve retroactively: exhibits seized before the system's adoption have no seizure-time hash or tag binding them to a ledger entry. A practical rollout would need to treat existing pending cases as a distinct, clearly labelled legacy-intake category rather than retrofitting a false impression of seizure-time verification. The policy environment for this kind of reform appears favourable: in July 2026, Bangladesh's High Court directed the formation of a high-powered committee - including an information-technology expert - specifically to devise a modernised system for handling seized items nationwide [29].

E. Limitations

- This paper presents a proposed architecture and a qualitative evaluation; it has not been implemented as a working prototype or tested under real operational load.
- The framework assumes that seizing officers reliably follow the tagging and hashing procedure at the point of seizure; a seizure conducted outside the prescribed procedure would leave a corresponding gap the technology cannot retroactively fill.
- Legal recognition of blockchain-attested custody records in Bangladeshi courts is not automatic and would benefit from an explicit legislative or judicial practice direction.
- The threat model addresses insider tampering and key compromise but does not extend to a full formal security proof of the chaincode's state-transition logic.
- Sensitive case data is visible to every validating peer on the relevant channel; the current design does not include field-level encryption within a channel.
- The framework has not been evaluated at the transaction volume a national rollout across roughly 622 police stations would generate.

F. Future Work

- A pilot deployment within a single metropolitan district, covering a limited exhibit category, to obtain field data before wider rollout.
- Integration with Bangladesh's e-Judiciary initiatives.
- Extension of the governance model to support cross-border evidence-sharing requests.
- A formal throughput and storage-growth evaluation under simulated national-scale seizure volumes.
- Field-level encryption and attribute-based access control within a channel for especially sensitive case categories.

VII. CONCLUSION

This paper has proposed a permissioned blockchain framework for tamper-evident chain of custody covering both physical and digital criminal evidence, designed around the institutional and infrastructural realities of Bangladesh's criminal justice system: uneven connectivity, resource-constrained forensic capacity, fragmented paper-based custody records, and an evidentiary statute base not yet adapted to distributed-ledger technology. By binding physical exhibits to tamper-evident tagged containers and digital exhibits to seizure-time cryptographic hashes, enforcing a strict multi-signed custody lifecycle, and distributing ledger-write authority across four independent institutions, the framework aims to close specific documented gaps identified in the Bangladesh forensic and criminal-investigation literature. A qualitative comparison against eight prior blockchain chain-of-custody systems shows that no existing proposal jointly addresses physical-evidence tagging, offline-tolerant operation, and alignment with a specific national legal framework. Realising the framework in practice will require legislative clarification of the evidentiary status of blockchain-attested records, sustained inter-agency governance, and a phased, piloted rollout beginning with a limited exhibit category and district before national deployment.

References

- [1] J. R. Vacca, *Computer Forensics: Computer Crime Scene Investigation*, 2nd ed. Boston, MA, USA: Charles River Media, 2005.
- [2] A. Nieto, R. Roman, and J. Lopez, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," *IEEE Network*, vol. 30, no. 6, pp. 34-41, Nov.-Dec. 2016.
- [3] Human Development Research Centre (HDRC), "A study of forensic services in criminal investigation in Bangladesh: Impacts, challenges, and capacity building issues," *Criminal Investigation Department, Bangladesh Police, Dhaka, Bangladesh, Tech. Rep.*, 2020.
- [4] S. Islam and S. Mollah, "Evidence preservation: Police stations and its mess in maalkhanas," *The Daily Star*, Dhaka, Bangladesh, Jan. 2021.
- [5] S. Mollah and M. J. Khan, "Challenges to law and order: hundreds of case investigations stalled in burnt police stations," *The Daily Star (Bangla)*, Dhaka, Bangladesh, Nov. 1, 2025.
- [6] The Business Standard, "Forensics delayed is justice denied," *The Business Standard*, Dhaka, Bangladesh, Sep. 2025.
- [7] The Daily Star, "The critical need for forensic infrastructure in Bangladesh," *The Daily Star*, Dhaka, Bangladesh, Sep. 2025.
- [8] M. S. Labib, "Admissibility of digital evidence in court: In light of changes in Bangladesh evidence law," *International Journal of Research and Scientific Innovation (IJRSI)*, Sep. 2024.
- [9] Z. Islam, "Strengthening forensic science in Bangladesh's criminal justice system: Challenges, opportunities, and strategies for improvement," *International Journal of Research and Innovation in Social Science*, vol. 9, no. 16, pp. 21-34, 2025.
- [10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [11] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A blockchain-based chain of custody for evidences management in digital forensics," in *Proc. Int. Conf. Blockchain Economics, Security and Protocols (Tokenomics 2019), OASiCs*, vol. 71, 2020, pp. 12:1-12:15.
- [12] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151-165, 2019.
- [13] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," *Digital Investigation*, vol. 28, pp. 44-55, 2019.
- [14] L. Ahmad, S. Khanji, F. Iqbal, and F. Kamoun, "Blockchain-based chain of custody: Towards real-time tamper-proof evidence management," in *Proc. 15th Int. Conf. Availability, Reliability and Security (ARES '20)*, Association for Computing Machinery, 2020, Art. no. 88.
- [15] X. Burri, E. Casey, T. Bollé, and D. Jaquet-Chiffelle, "Independently verifiable electronic chain of custody history record using blockchain technology," *Forensic Science International: Digital Investigation*, vol. 33, pp. 28-34, 2020.
- [16] F. F. Alruwaili, "CustodyBlock: A distributed chain of custody evidence framework," *Information*, vol. 12, no. 2, Art. no. 88, 2021.
- [17] W. Yan, J. Shen, Z. Cao, and X. Dong, "Blockchain based digital evidence chain of custody," in *Proc. 2nd Int. Conf. Blockchain Technology (ICBCT 2020)*, Association for Computing Machinery, 2020, pp. 19-23.
- [18] I. Lavín and D. R. Llanos, "An analysis of blockchain solutions for digital evidence chain of custody under ISO 27037," in *Blockchain*, Springer, 2025/2026.
- [19] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50-57, 2018.
- [20] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," *IEEE Access*, vol. 7, pp. 99573-99588, 2019.
- [21] Southwest Solutions Group, "RFID and barcode evidence tracking for police property and evidence rooms," *technical product documentation*, 2025.

[22] Police1 / Zebra Technologies, "RFID asset tracking and RFID inventory management for police," industry report, 2025.

[23] D. Batista, A. L. Mangeth, I. Frajhof, P. H. Alves, R. Nasser, G. Robichez, G. M. Silva, and F. P. D. Miranda, "Exploring blockchain technology for chain of custody control in physical evidence: A systematic literature review," *Journal of Risk and Financial Management*, vol. 16, no. 8, p. 360, 2023.

[24] T. X. Hung, L. T. Dung, and T. A. Tu, "A blockchain-based chain of custody for digital evidence: Design and evaluation," *Journal of Science and Technology on Information Security*, vol. 3, no. 26, pp. 25-38, 2025.

[25] RisingBD, "Arrest warrant issued against former Dhunot OC Kripa Sindhu Bala over destruction of evidence in a rape case," RisingBD, Bogura, Bangladesh, Oct. 2025.

[26] Government of the People's Republic of Bangladesh, *The Evidence Act, 1872 (Act No. I of 1872)*.

[27] Government of the People's Republic of Bangladesh, *The Deoxyribonucleic Acid (DNA) Act, 2014*.

[28] ISO/IEC 27037:2012, *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*, International Organization for Standardization, 2012.

[29] The Daily Star, "HC orders high-powered committee for better management of seized items," *The Daily Star*, Dhaka, Bangladesh, Jul. 2026.

[30] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75-105, 2004.

[31] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45-77, 2007.