Smart Evidence Management Using Blockchain

Ms. Nehal Shaji[1], Mr. N Vishnu Venkatesh[2]
[1](Student), [2](Assistant Professor)
Department of Forensic Science, JAIN (Deemed-to-be University)
doi.org/10.64643/IJIRTV12I11-199202-459

***Abstract*—The integrity and authenticity of forensic evidence are paramount to the criminal justice system. Traditional evidence management systems face significant challenges including tampering risks, chain of custody gaps, centralized vulnerabilities, and lack of transparency. This paper presents a comprehensive framework for smart evidence management using blockchain technology, specifically focusing on permissioned blockchain architectures that enforce automated chain of custody rules and maintain cryptographic integrity through hash generation and verification. The proposed framework leverages distributed ledger technology, smart contracts, and off-chain storage mechanisms to create an immutable, auditable, and transparent evidence management system. By integrating cryptographic hashing, role-based access control, and automated workflow enforcement, this system addresses critical vulnerabilities in conventional evidence handling while maintaining confidentiality and operational efficiency. The framework demonstrates how blockchain technology can revolutionize forensic evidence management by providing tamper-proof records, automated compliance, and enhanced trust among stakeholders including law enforcement, forensic experts, legal professionals, and courts.**

I. INTRODUCTION

The criminal justice system relies fundamentally on the integrity, authenticity, and admissibility of forensic evidence. From crime scene collection to courtroom presentation, evidence must maintain an unbroken chain of custody that documents every transfer, access, and modification. However, traditional evidence management systems, which often rely on paper-based logs, centralized databases, and manual record-keeping, are vulnerable to tampering, human error, unauthorized access, and data loss. These vulnerabilities can compromise investigations, lead to wrongful convictions, or result in case dismissals due to evidence inadmissibility.

The emergence of blockchain technology presents a transformative opportunity to address these critical challenges. Blockchain, originally developed as the underlying technology for cryptocurrencies, offers a distributed, immutable, and transparent ledger that can revolutionize how forensic evidence is managed, tracked, and verified. By leveraging cryptographic hashing, consensus mechanisms, and smart contracts, blockchain-based evidence management systems can provide tamper-proof records, automated compliance with chain of custody protocols, and enhanced trust among all stakeholders.

This paper presents a comprehensive framework for smart evidence management using blockchain technology, with three primary objectives: (1) designing and implementing a permissioned blockchain framework to record forensic evidence data and enforce automated chain of custody rules, (2) generating cryptographic hashes to maintain integrity and enable tamper detection, and (3) enabling smart evidence management through automated workflows, role-based access control, and transparent audit trails. The proposed framework addresses the unique requirements of forensic evidence handling, including confidentiality, legal compliance, multi-stakeholder coordination, and long-term preservation.

The integration of blockchain technology into evidence management represents a convergence of distributed systems, cryptography, and forensic science. As digital evidence continues to proliferate with the growth of IoT devices, mobile computing, and cloud services, the need for robust, scalable, and trustworthy evidence management systems becomes increasingly critical. Recent advances in IoT-driven security solutions have demonstrated the importance of trustworthiness and integrity in distributed systems, particularly in contexts where misconduct and security challenges must be addressed systematically (Shukla et al., 2024). Similarly, innovations in endpoint security for smart homes have highlighted the value of novel approaches to data protection and access control in distributed environments (VENKATESH et al., 2026).

The remainder of this paper is organized as follows: Section 2 provides background on traditional evidence management challenges and blockchain

fundamentals. Section 3 reviews related work in blockchain-based forensics, IoT security, and AI-driven legal systems. Section 4 presents the detailed architecture of the proposed framework. Section 5 describes the implementation methodology. Section 6 analyzes security and integrity verification mechanisms. Section 7 evaluates performance and scalability. Section 8 discusses implications and limitations. Section 9 outlines future research directions, and Section 10 concludes the paper.

II. BACKGROUND AND THEORETICAL FOUNDATIONS

2.1 Traditional Evidence Management Challenges

Conventional evidence management systems face numerous challenges that compromise the integrity and reliability of forensic evidence. These challenges can be categorized into several key areas:

Chain of Custody Vulnerabilities: Traditional chain of custody relies on manual documentation, paper logs, and human oversight. Each transfer of evidence between investigators, forensic laboratories, storage facilities, and courts must be meticulously documented. However, manual processes are prone to errors, omissions, and inconsistencies. Missing signatures, incomplete timestamps, or lost documentation can break the chain of custody, rendering evidence inadmissible in court.

Centralization Risks: Most evidence management systems rely on centralized databases controlled by a single authority, typically law enforcement agencies. This centralization creates single points of failure, making systems vulnerable to cyberattacks, data breaches, insider threats, and system failures. Unauthorized access or malicious modification of centralized databases can compromise entire investigations without detection.

Lack of Transparency and Trust: In adversarial legal systems, defense attorneys, prosecutors, and judges must trust that evidence has not been tampered with. However, traditional systems provide limited transparency into evidence handling. Stakeholders cannot independently verify the integrity of evidence or audit the complete history of access and modifications, leading to disputes and challenges to evidence admissibility.

Scalability and Efficiency: As the volume of digital evidence grows exponentially, traditional systems struggle to scale. Managing large multimedia files, IoT sensor data, and cloud-based evidence requires significant storage infrastructure and efficient retrieval mechanisms. Manual processes cannot keep pace with the volume and complexity of modern digital evidence.

Long-Term Preservation: Forensic evidence must often be preserved for years or decades, particularly in cold cases or appeals. Traditional storage media degrade over time, and data migration across evolving technologies introduces risks of corruption or loss. Ensuring long-term integrity and accessibility remains a significant challenge.

2.2 Blockchain Technology Fundamentals

Blockchain is a distributed ledger technology that maintains a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. This structure creates an immutable chain where any attempt to alter historical records would require recalculating all subsequent blocks, which becomes computationally infeasible in a properly designed blockchain network.

Key Characteristics of Blockchain:

Immutability: Once data is recorded in a blockchain, it cannot be altered or deleted without detection. This immutability is achieved through cryptographic hashing and consensus mechanisms that require network-wide agreement for any changes.

Decentralization: Blockchain distributes data across multiple nodes in a peer-to-peer network, eliminating single points of failure and reducing vulnerability to attacks or system failures.

Transparency and Auditability: All transactions recorded on a blockchain are visible to authorized participants, creating a transparent and auditable history. This transparency builds trust among stakeholders who can independently verify the integrity of records.

Consensus Mechanisms: Blockchain networks use consensus algorithms to validate transactions and maintain agreement across distributed nodes. Common mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA).

Permissioned vs. Permissionless Blockchains: Permissionless blockchains (like

Bitcoin and Ethereum) allow anyone to join the network and participate in consensus. Permissioned blockchains restrict participation to authorized entities, making them more suitable for enterprise and forensic applications where confidentiality and regulatory compliance are required.

2.3 Smart Contracts and Automation

Smart contracts are self-executing programs stored on a blockchain that automatically enforce predefined rules and conditions. When specific conditions are met, smart contracts execute predetermined actions without human intervention. In the context of evidence management, smart contracts can automate chain of custody rules, access control policies, evidence registration, custody transfers, and integrity verification.

Benefits of Smart Contracts in Evidence Management:

Automation: Smart contracts eliminate manual processes and human error by automatically executing evidence handling protocols.

Enforcement: Business rules and legal requirements are encoded in smart contracts, ensuring consistent enforcement across all evidence transactions.

Transparency: Smart contract code is visible to all authorized participants, providing transparency into the rules governing evidence management.

Efficiency: Automated workflows reduce processing time, administrative overhead, and operational costs.

Auditability: All smart contract executions are recorded on the blockchain, creating a complete audit trail of automated actions.

III. LITERATURE REVIEW AND RELATED WORK

3.1 Blockchain Applications in Digital Forensics

Recent research has demonstrated the viability of blockchain technology for forensic evidence management. Permissioned blockchain frameworks, particularly Hyperledger Fabric and Hyperledger Sawtooth, have emerged as preferred platforms for forensic applications due to their support for private networks, role-based access control, and enterprise-grade performance. These platforms enable organizations to restrict participation to trusted entities while maintaining the benefits of distributed ledger technology.

Implementations typically employ a hybrid architecture that combines on-chain and off-chain storage. Large evidence artifacts such as multimedia files, disk images, and IoT sensor data are stored off-chain using distributed file systems like the InterPlanetary File System (IPFS), while cryptographic hashes or Merkle roots are anchored on-chain. This approach balances confidentiality, storage efficiency, and integrity verification. Ledger nodes can validate evidence integrity by comparing submitted hashes against on-chain anchors without possessing the full evidence artifacts, preserving confidentiality while ensuring tamper detection.

Smart contracts play a central role in automating chain of custody workflows. Common automated functions include RegisterEvidence for initial evidence registration, VerifyCustody for logging custody transfers, AccessGrant for enforcing role-based access control, and LogActivity for maintaining audit trails. These contracts encode business rules and legal requirements, ensuring consistent enforcement across all evidence transactions. Experimental deployments have reported block times of 1.2 to 3.8 seconds and transaction latencies of 85 to 150 milliseconds, demonstrating the feasibility of blockchain-based evidence management for real-world forensic operations.

Merkle tree structures are employed to enable efficient provenance queries and integrity verification. Distributed Merkle root snapshots are created per case, allowing fast extraction of evidence history without brute-force searches of large blockchains. This indexing approach trades modest smart contract processing overhead for significantly improved retrieval performance as case volume grows.

3.2 IoT and Security Frameworks

The proliferation of IoT devices has introduced new challenges and opportunities for evidence management. IoT sensors, smart home devices, connected vehicles, and wearable technologies generate vast amounts of digital evidence that must be collected, authenticated, and managed. Recent research has examined IoT-driven solutions for trustworthiness and security in distributed systems. Shukla et al. (2024) investigated IoT-driven solutions for VANET (Vehicular Ad Hoc Network) trustworthiness, examining misconduct and position security challenges that are relevant to evidence

collection from connected vehicles and transportation systems. Their work highlights the importance of establishing trust mechanisms and addressing security vulnerabilities in IoT ecosystems where evidence may be collected.

Similarly, innovations in endpoint security for smart homes demonstrate the value of novel approaches to data protection and access control. VENKATESH et al. (2026) proposed a vantage point recreation approach for endpoint security in smart homes, addressing challenges in protecting distributed IoT devices from unauthorized access and tampering. These security frameworks are directly applicable to evidence management scenarios where IoT devices serve as evidence sources, requiring robust authentication, integrity verification, and secure data transmission.

The integration of blockchain technology with IoT security frameworks creates opportunities for end-to-end evidence integrity. IoT devices can generate cryptographic hashes of collected data at the point of capture, which are then anchored on the blockchain to establish provenance and prevent tampering. This approach extends the chain of custody to the earliest stages of evidence collection, addressing vulnerabilities in traditional systems where evidence integrity is only established after transfer to law enforcement custody.

3.3 AI-Driven Legal and Security Systems

Artificial intelligence and machine learning technologies are increasingly being integrated with blockchain-based evidence management systems to enhance automation, anomaly detection, and decision support. Recent research has explored AI applications in legal and forensic contexts that complement blockchain-based evidence management.

SUNIDHI SUDHEER SHENOY and N VISHNU VENKATESH (2025) developed a predictive framework for real-time courtroom assistance using an AI-based mock legal advisor. This work demonstrates how AI can support legal professionals in analyzing evidence, predicting case outcomes, and providing decision support. When integrated with blockchain-based evidence management, AI systems can analyze evidence provenance, detect anomalies in chain of custody, and provide intelligent recommendations for evidence handling.

Crime forecasting and predictive analytics represent another area where AI complements blockchain-based evidence management. Natarajan et al. (2023) proposed a crime forecasting system using historical crime location data and CNN-based image classification mechanisms. Such predictive systems can inform evidence collection strategies, resource allocation, and investigative priorities. When combined with blockchain-based evidence tracking, these systems create a comprehensive framework for proactive and reactive forensic operations.

Furthermore, AI-driven anomaly detection can enhance the security of blockchain-based evidence management systems. Machine learning models can analyze access patterns, custody transfers, and user behavior to detect suspicious activities, unauthorized access attempts, or potential tampering. Testbeds combining blockchain verification with auxiliary anomaly detection have reported near-perfect validation rates in experiments, demonstrating the synergy between blockchain immutability and AI-driven security monitoring.

The integration of autonomous systems with blockchain-based evidence management also presents opportunities for automated evidence collection and verification. Natarajan et al. (2026) developed a robust detect and avoid system for autonomous drone navigation, which has applications in crime scene documentation, surveillance, and evidence collection. Autonomous drones equipped with cameras and sensors can capture evidence at crime scenes, generate cryptographic hashes in real-time, and anchor these hashes on the blockchain to establish immediate provenance and integrity.

IV. PROPOSED FRAMEWORK ARCHITECTURE

The proposed smart evidence management framework integrates permissioned blockchain technology, cryptographic hashing, smart contracts, and off-chain storage to create a comprehensive solution for forensic evidence handling. Figure 1 illustrates the complete architecture of the framework, showing the interaction between data sources, evidence registration, the permissioned blockchain network, smart contracts, off-chain storage, and stakeholders.

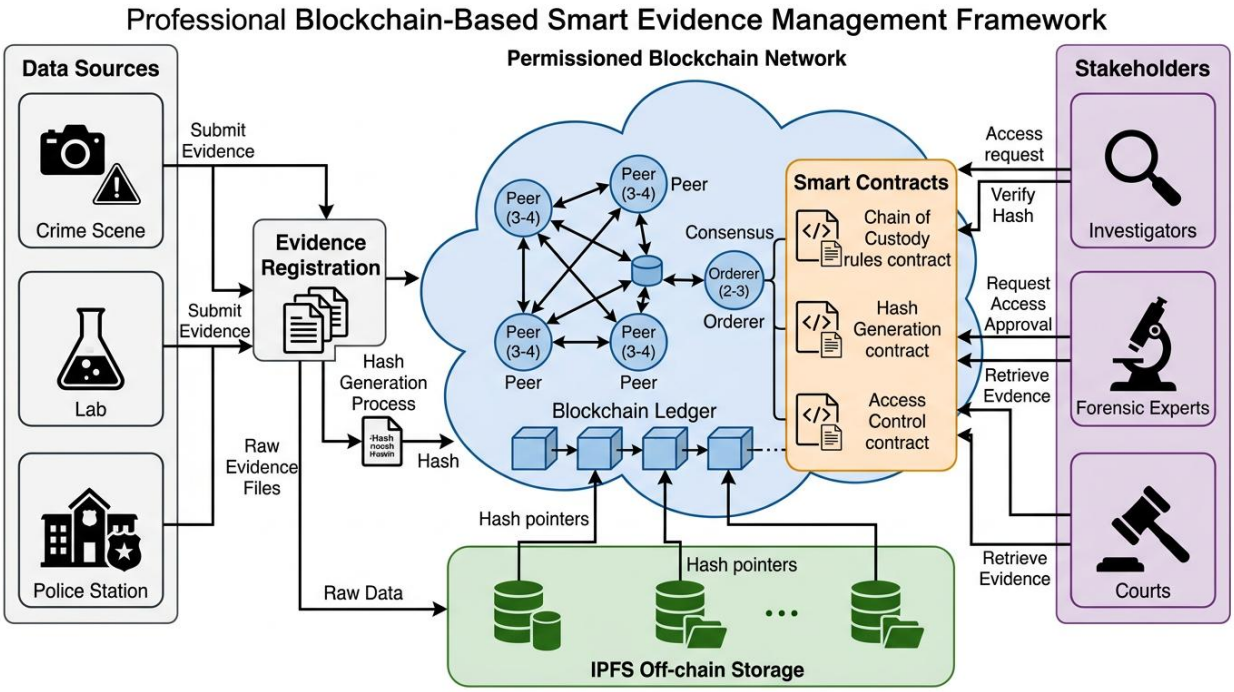

Figure 1: Professional Blockchain-Based Smart Evidence Management Framework

4.1 Permissioned Blockchain Network Design

The framework employs a permissioned blockchain architecture that restricts participation to authorized entities within the forensic ecosystem. This design choice addresses the confidentiality and regulatory requirements of evidence management while maintaining the benefits of distributed ledger technology.

Network Participants:

The permissioned network consists of multiple peer nodes operated by trusted stakeholders including law enforcement agencies, forensic laboratories, courts, and authorized legal professionals. Each participant operates one or more peer nodes that maintain a synchronized copy of the blockchain ledger. An orderer node (or orderer cluster) is responsible for transaction ordering and block creation, ensuring consistency across the network.

Consensus Mechanism:

The framework employs Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA) consensus mechanisms, which are well-suited for permissioned networks with a limited number of trusted validators. These mechanisms provide low latency, high throughput, and deterministic finality, making them appropriate for forensic applications where transaction confirmation speed is important.

Channel Architecture:

To support case isolation and confidentiality, the framework implements a channel-based architecture where each investigation or case can operate on a separate channel. Channels provide logical separation of data, ensuring that evidence and transactions related to one case are not visible to participants in other cases unless explicitly authorized. This multi-tenancy approach enables the same blockchain infrastructure to support multiple concurrent investigations while maintaining strict data isolation.

Role-Based Access Control:

The permissioned network implements role-based access control (RBAC) that defines permissions for different participant types. Roles include evidence collectors (law enforcement officers), evidence custodians (forensic laboratory personnel), investigators, forensic experts, prosecutors, defense attorneys, and judges. Each role has specific permissions for evidence registration, access, transfer, and verification. Smart contracts enforce these permissions, ensuring that only authorized participants can perform specific actions.

4.2 Hash Generation and Integrity Mechanisms

Cryptographic hashing is the foundation of integrity verification in the proposed framework. Hash functions transform evidence artifacts of arbitrary

size into fixed-length cryptographic digests that uniquely represent the original data. Any modification to the evidence, no matter how small, produces a completely different hash value, enabling tamper detection.

Hash Generation Process:

When evidence is collected at a crime scene, laboratory, or other source, the system immediately generates a cryptographic hash of the evidence artifact using secure hash algorithms such as SHA-256 or SHA-3. For large multimedia files or disk images, the system may generate hashes of file chunks and combine them into a Merkle tree structure. The root hash of the Merkle tree serves as a compact representation of the entire evidence artifact.

On-Chain Hash Anchoring:

The generated hashes are anchored on the blockchain through evidence registration transactions. These transactions record the hash value, evidence metadata (case identifier, evidence type, collection timestamp, collector identity), and provenance information. Once recorded on the blockchain, the hash becomes an immutable reference point for integrity verification.

Merkle Tree Implementation:

For complex evidence collections containing multiple artifacts, the framework implements Merkle tree structures that organize hashes hierarchically. Leaf nodes contain hashes of individual evidence items, while internal nodes contain hashes of their children. The Merkle root provides a single hash that represents the integrity of the entire evidence collection. This structure enables efficient verification of individual items without recomputing hashes for the entire collection.

Integrity Verification:

When evidence is accessed, transferred, or presented in court, stakeholders can verify its integrity by recomputing the hash of the current artifact and comparing it to the hash anchored on the blockchain. If the hashes match, the evidence has not been tampered with since registration. If they differ, tampering is detected and the evidence is flagged for investigation. This verification process can be performed by any authorized participant without requiring trust in a central authority.

Off-Chain Storage Integration:

To address storage scalability and confidentiality requirements, the framework stores large evidence artifacts off-chain using distributed file systems such as IPFS or private cloud storage. Only the cryptographic hashes are stored on-chain, creating a hybrid architecture that balances integrity verification with storage efficiency. The blockchain serves as an immutable index that points to off-chain evidence locations while guaranteeing integrity through hash anchoring.

4.3 Smart Contract Implementation

Smart contracts automate the enforcement of chain of custody rules, access control policies, and evidence handling workflows. The framework implements several core smart contracts that govern evidence lifecycle management:

RegisterEvidence Contract:

This contract handles the initial registration of evidence when it enters the system. It accepts parameters including evidence identifier, case identifier, evidence type, collection timestamp, collector identity, hash value, and optional metadata. The contract validates the input parameters, checks the collector's authorization, records the evidence registration transaction on the blockchain, and emits an event notification. This creates an immutable provenance start point for the evidence.

VerifyCustody Contract:

The VerifyCustody contract logs custody transfers between authorized participants. When evidence is transferred from one custodian to another, this contract records the transfer transaction including the transferor identity, transferee identity, transfer timestamp, transfer reason, and cryptographic signatures from both parties. The contract enforces authorization checks to ensure that only authorized participants can initiate or accept custody transfers. Each transfer creates an auditable ledger entry that contributes to the complete chain of custody.

AccessGrant Contract:

This contract implements role-based access control by managing permissions for evidence access. When a participant requests access to evidence, the AccessGrant contract evaluates the requester's role, the evidence sensitivity level, and any case-specific access policies. If access is granted, the contract

records the access event including requester identity, access timestamp, access type (read, download, modify), and access justification. This creates a complete audit trail of all evidence access events.

LogActivity Contract:

The LogActivity contract maintains a comprehensive audit trail of all evidence-related activities beyond custody transfers and access events. This includes evidence analysis activities, forensic examination results, evidence modification events (such as redaction or enhancement), and administrative actions. Each activity is logged with detailed metadata including actor identity, activity type, timestamp, and activity description.

VerifyIntegrity Contract:

This contract automates integrity verification by comparing submitted evidence hashes against the hashes anchored on the blockchain. When a participant submits evidence for verification, the contract retrieves the original hash from the blockchain, compares it to the submitted hash, and returns a verification result. If the hashes match, the contract confirms integrity and records the verification event. If they differ, the contract flags a potential tampering incident and triggers alert mechanisms.

Temporal Access Control Contract:

Advanced implementations include temporal access control contracts that enforce time-bounded access constraints. Evidence may only be accessed during specific time windows, investigation phases, or under specific conditions. The contract evaluates temporal constraints using blockchain timestamps and grants or denies access accordingly. This prevents unauthorized access outside of permitted time periods and supports privacy-preserving evidence handling.

4.4 Off-Chain Storage Integration

The framework integrates off-chain storage systems to address the scalability challenges of storing large evidence artifacts directly on the blockchain. This hybrid architecture separates data custody (off-chain) from integrity proofs (on-chain), enabling efficient storage while maintaining cryptographic integrity guarantees.

IPFS Integration:

The InterPlanetary File System (IPFS) serves as the primary off-chain storage layer for evidence artifacts. IPFS is a distributed, content-addressed file system that stores files across multiple nodes and retrieves them using cryptographic hashes. When evidence is registered, the system uploads the artifact to IPFS, which returns a content identifier (CID) that is derived from the file's hash. This CID is stored on the blockchain alongside the evidence metadata, creating a verifiable link between the on-chain record and the off-chain artifact.

Private Cloud Storage:

For organizations with strict confidentiality requirements or regulatory constraints, the framework supports integration with private cloud storage systems. Evidence artifacts are encrypted and stored in private cloud infrastructure, while encryption keys and storage location references are managed through the blockchain. This approach provides additional confidentiality while maintaining the integrity verification capabilities of the blockchain.

Hybrid Storage Strategy:

The framework implements a hybrid storage strategy that optimizes for different evidence types. Small evidence items such as text documents, logs, and metadata may be stored directly on-chain or in smart contract storage. Medium-sized items such as images and short videos are stored in IPFS. Large items such as disk images, long videos, and forensic memory dumps are stored in private cloud storage with hash anchors on the blockchain. This tiered approach balances storage costs, access performance, and confidentiality requirements.

V. IMPLEMENTATION METHODOLOGY

5.1 Platform Selection and Configuration

The implementation of the proposed framework leverages Hyperledger Fabric as the permissioned blockchain platform. Hyperledger Fabric provides enterprise-grade features including modular architecture, pluggable consensus mechanisms, channel-based privacy, and chaincode (smart contract) support. The platform is configured with the following components:

Peer Nodes: Multiple peer nodes are deployed across participating organizations (law enforcement, forensic labs, courts). Each peer maintains a copy of the ledger and executes chaincode.

Orderer Nodes: A cluster of orderer nodes implements the consensus mechanism and creates blocks from ordered transactions. The orderer cluster uses Raft consensus for crash fault tolerance and leader election.

Certificate Authority: A Hyperledger Fabric Certificate Authority (CA) issues digital certificates to network participants, enabling identity management and authentication.

Chaincode: Smart contracts are implemented as chaincode written in Go or Node.js, deployed to peer nodes, and invoked through client applications.

Channels: Separate channels are created for different cases or investigations, providing data isolation and confidentiality.

5.2 Evidence Registration Process

The evidence registration process establishes the initial provenance and integrity baseline for forensic evidence. The workflow proceeds as follows:

Evidence Collection: When evidence is collected at a crime scene or received at a forensic laboratory, the collector uses a client application to initiate the registration process.

Hash Generation: The client application computes a cryptographic hash of the evidence artifact using SHA-256. For large files, the application may generate a Merkle tree and compute the root hash.

Metadata Capture: The collector provides metadata including case identifier, evidence type, collection location, collection timestamp, and description. The system automatically captures the collector's identity from their digital certificate.

Transaction Submission: The client application submits a RegisterEvidence transaction to the blockchain network, including the hash, metadata, and collector signature.

Validation and Consensus: Peer nodes validate the transaction by checking the collector's authorization and the transaction format. The orderer node includes the validated transaction in a block, and the block is distributed to all peers for commitment.

Confirmation: Once the transaction is committed to the blockchain, the client application receives a confirmation and the evidence is officially registered with an immutable provenance record.

Off-Chain Storage: Simultaneously, the evidence artifact is uploaded to IPFS or private cloud storage, and the storage reference (IPFS CID or cloud storage URL) is associated with the on-chain evidence record.

5.3 Chain of Custody Automation

The framework automates chain of custody tracking through smart contracts that enforce custody transfer rules and maintain complete audit trails. The custody transfer workflow includes:

Transfer Initiation: When evidence needs to be transferred from one custodian to another (e.g., from a police officer to a forensic examiner), the current custodian initiates a transfer request through the client application.

Authorization Check: The VerifyCustody smart contract verifies that the current custodian is authorized to transfer the evidence and that the intended recipient is authorized to receive it based on their role and case assignment.

Cryptographic Signatures: Both the transferor and transferee provide cryptographic signatures to acknowledge the transfer. These signatures are generated using their private keys and verified using their public key certificates.

Transaction Recording: The smart contract records the custody transfer transaction on the blockchain, including transferor identity, transferee identity, transfer timestamp, transfer reason, and both signatures.

Integrity Verification: Before completing the transfer, the system may optionally verify evidence integrity by comparing the current hash to the registered hash, ensuring that the evidence has not been tampered with during custody.

Notification: Both parties receive notifications confirming the custody transfer, and the evidence status is updated to reflect the new custodian.

Audit Trail: The complete history of custody transfers is permanently recorded on the blockchain, creating an unbroken chain of custody that can be audited at any time.

5.4 Access Control and Authorization

The framework implements multi-layered access control to ensure that only authorized participants can

access evidence based on their roles, case assignments, and temporal constraints:

Role-Based Access Control: Participants are assigned roles (investigator, forensic expert, prosecutor, defense attorney, judge) that define their baseline permissions. Smart contracts enforce these role-based permissions for all evidence operations.

Case-Based Authorization: Participants are explicitly assigned to specific cases or investigations. Access to evidence is restricted to participants assigned to the relevant case, preventing unauthorized cross-case access.

Attribute-Based Access Control: Advanced implementations support attribute-based access control (ABAC) where access decisions consider multiple attributes including role, case assignment, evidence sensitivity level, investigation phase, and temporal constraints.

Access Request Workflow: When a participant requests access to evidence, the AccessGrant smart contract evaluates all applicable policies and grants or denies access. Approved access requests are logged on the blockchain with detailed metadata.

Temporal Constraints: Evidence access may be restricted to specific time windows or investigation phases. For example, defense attorneys may only access evidence after formal charges are filed, or evidence may be sealed after trial completion.

Audit Logging: All access requests, approvals, denials, and actual access events are logged on the blockchain, creating a complete audit trail that supports compliance verification and forensic investigation of potential security incidents.

VI. SECURITY ANALYSIS AND INTEGRITY VERIFICATION

6.1 Cryptographic Hash Functions

The security of the proposed framework relies fundamentally on cryptographic hash functions that provide collision resistance, preimage resistance, and second preimage resistance. The framework employs SHA-256 as the primary hash function, which produces 256-bit hash values and is currently considered secure against known attacks.

Collision Resistance: It is computationally infeasible to find two different evidence artifacts that produce the same hash value. This property ensures that each evidence item has a unique cryptographic fingerprint.

Preimage Resistance: Given a hash value, it is computationally infeasible to find an evidence artifact that produces that hash. This prevents attackers from creating fake evidence that matches a registered hash.

Second Preimage Resistance: Given an evidence artifact and its hash, it is computationally infeasible to find a different artifact with the same hash. This prevents evidence substitution attacks.

6.2 Merkle Tree Implementation

Merkle trees provide efficient integrity verification for large evidence collections and enable selective disclosure where individual evidence items can be verified without revealing the entire collection. The framework implements Merkle trees as follows:

Tree Construction: Evidence items are organized as leaf nodes, and their hashes are computed. Parent nodes are created by concatenating and hashing pairs of child hashes. This process continues recursively until a single root hash is obtained.

Root Hash Anchoring: The Merkle root hash is anchored on the blockchain, representing the integrity of the entire evidence collection.

Selective Verification: To verify a specific evidence item, the system provides the item's hash along with the sibling hashes along the path from the leaf to the root (Merkle proof). The verifier can recompute the root hash using these values and compare it to the anchored root hash.

Efficiency: Merkle proofs require only logarithmic space and time relative to the collection size, making verification efficient even for large evidence collections.

6.3 Tamper Detection Mechanisms

The framework implements multiple layers of tamper detection to identify unauthorized modifications, substitutions, or deletions of evidence:

Hash Comparison: The primary tamper detection mechanism compares the current hash of an evidence artifact to the hash anchored on the blockchain. Any discrepancy indicates tampering.

Blockchain Immutability: The blockchain's immutability ensures that registered hashes cannot be

altered retroactively. Any attempt to modify blockchain records would require recalculating all subsequent blocks and achieving consensus from the majority of network participants, which is computationally infeasible in a properly secured network.

Consensus Verification: Participants can independently verify that their copy of the blockchain matches the consensus view by comparing block hashes with other peers. This prevents isolated tampering of individual node databases.

Anomaly Detection: AI-driven anomaly detection systems monitor access patterns, custody transfers, and user behavior to identify suspicious activities that may indicate tampering attempts or unauthorized access.

Audit Trail Analysis: The complete audit trail recorded on the blockchain enables forensic analysis of evidence handling history. Investigators can identify gaps, inconsistencies, or suspicious patterns that may indicate tampering or procedural violations.

VII. PERFORMANCE EVALUATION AND SCALABILITY

7.1 Transaction Throughput

Experimental deployments of permissioned blockchain-based evidence management systems have demonstrated transaction throughput sufficient for real-world forensic operations. Reported performance metrics include:

Block Creation Rate: Block times ranging from 1.2 to 3.8 seconds, depending on network configuration and consensus mechanism.

Transaction Latency: End-to-end transaction latencies of 85 to 150 milliseconds from submission to confirmation.

Throughput: Transaction throughput of several hundred to several thousand transactions per second, adequate for evidence registration, custody transfers, and access logging in typical forensic operations.

These performance characteristics demonstrate that permissioned blockchain platforms can support the operational requirements of evidence management without introducing unacceptable delays.

7.2 Latency Analysis

Transaction latency in blockchain-based evidence management systems consists of several components:

Network Propagation: Time required for transaction propagation from the client to peer nodes and orderer nodes.

Validation: Time required for peer nodes to validate transactions by executing smart contract logic and checking authorization.

Consensus: Time required for the orderer to achieve consensus and create a block.

Commitment: Time required for peers to commit the block to their local ledgers.

The reported latencies of 85 to 150 milliseconds indicate that these components combine to produce acceptable response times for interactive evidence management operations.

7.3 Storage Optimization

The hybrid architecture that combines on-chain hash anchoring with off-chain artifact storage provides significant storage optimization:

On-Chain Storage: Only cryptographic hashes (32 bytes for SHA-256), metadata, and transaction records are stored on-chain, minimizing blockchain storage requirements.

Off-Chain Storage: Large evidence artifacts are stored off-chain in IPFS or private cloud storage, which can scale independently of the blockchain.

Merkle Tree Compression: Merkle trees enable compact representation of large evidence collections through a single root hash, further reducing on-chain storage requirements.

Provenance Indexing: Distributed Merkle root snapshots and provenance graphs enable efficient history extraction without brute-force blockchain scans, improving query performance as the blockchain grows.

Experimental results indicate that Merkle-based retrieval significantly outperforms brute-force blockchain scans as case volume grows, at the cost of slightly higher smart contract processing time during evidence registration.

VIII. DISCUSSION AND IMPLICATIONS

8.1 Legal and Regulatory Considerations

The adoption of blockchain-based evidence management systems raises important legal and regulatory considerations:

Admissibility: Courts must recognize blockchain-based chain of custody records as legally admissible evidence. This requires establishing legal frameworks that define the evidentiary standards for blockchain records and cryptographic integrity verification.

Data Privacy: Evidence management systems must comply with data privacy regulations such as GDPR, which grant individuals rights to access, correct, and delete personal data. The immutability of blockchain creates tension with these rights, requiring careful design of privacy-preserving mechanisms and off-chain data management.

Jurisdiction: Distributed blockchain networks may span multiple jurisdictions, raising questions about data sovereignty, cross-border data transfers, and applicable legal frameworks.

Standards and Certification: Industry standards and certification programs are needed to ensure that blockchain-based evidence management systems meet forensic and legal requirements for integrity, security, and reliability.

8.2 Stakeholder Benefits

The proposed framework provides significant benefits to all stakeholders in the forensic ecosystem:

Law Enforcement: Automated chain of custody reduces administrative burden, eliminates manual errors, and provides tamper-proof records that strengthen case integrity.

Forensic Laboratories: Transparent audit trails and automated workflows improve operational efficiency, reduce liability risks, and enhance quality assurance.

Prosecutors: Blockchain-based evidence records provide strong proof of integrity and chain of custody, supporting successful prosecutions and reducing challenges to evidence admissibility.

Defense Attorneys: Transparent access to evidence provenance and audit trails enables effective defense strategies and ensures fair trials.

Courts: Judges can independently verify evidence integrity and chain of custody, reducing disputes and improving confidence in evidence admissibility decisions.

Public Trust: Transparent and tamper-proof evidence management enhances public trust in the criminal justice system by demonstrating accountability and integrity.

8.3 Limitations and Challenges

Despite its advantages, the proposed framework faces several limitations and challenges:

Initial Implementation Costs: Deploying blockchain infrastructure, training personnel, and integrating with existing systems requires significant upfront investment.

Technical Complexity: Blockchain technology, cryptography, and smart contracts introduce technical complexity that requires specialized expertise for implementation and maintenance.

Scalability Constraints: While permissioned blockchains offer better performance than public blockchains, they still face scalability limitations compared to traditional centralized databases, particularly for very high transaction volumes.

Interoperability: Integrating blockchain-based evidence management with existing forensic tools, laboratory information management systems (LIMS), and court case management systems requires standardized interfaces and data formats.

Governance: Establishing governance frameworks for permissioned blockchain networks, including participant onboarding, consensus rule changes, and dispute resolution, requires careful coordination among stakeholders.

Privacy Tradeoffs: While the framework implements confidentiality mechanisms, the transparency inherent in blockchain technology creates potential privacy risks that must be carefully managed through access control and encryption.

IX. FUTURE DIRECTIONS AND RECOMMENDATIONS

Future research and development should focus on several key areas to advance blockchain-based evidence management:

Integration with Emerging Technologies: Combining blockchain with artificial intelligence, machine learning, and IoT technologies can enhance

automation, anomaly detection, and evidence collection. AI-driven predictive analytics can inform evidence handling strategies, while IoT devices can generate cryptographic hashes at the point of data capture to extend chain of custody to the earliest stages of evidence collection.

Cross-Jurisdictional Frameworks: Developing international standards and protocols for blockchain-based evidence management can facilitate cross-border investigations and evidence sharing while addressing jurisdictional and data sovereignty concerns.

Privacy-Preserving Techniques: Implementing advanced cryptographic techniques such as zero-knowledge proofs, homomorphic encryption, and secure multi-party computation can enhance privacy while maintaining integrity verification capabilities.

Quantum-Resistant Cryptography: As quantum computing advances, transitioning to quantum-resistant hash functions and cryptographic algorithms will be necessary to ensure long-term security of evidence integrity mechanisms.

Standardization and Certification: Industry consortia and standards organizations should develop comprehensive standards for blockchain-based evidence management, including technical specifications, security requirements, and certification programs.

User Experience: Improving user interfaces and workflows for evidence management applications can reduce training requirements and increase adoption among law enforcement and forensic professionals.

Performance Optimization: Continued research into consensus mechanisms, sharding techniques, and layer-2 scaling solutions can further improve transaction throughput and reduce latency.

Legal Framework Development: Collaboration between technologists, legal scholars, and policymakers is needed to develop legal frameworks that recognize blockchain-based evidence records and address admissibility, privacy, and jurisdictional issues.

X. CONCLUSION

This paper has presented a comprehensive framework for smart evidence management using blockchain technology, addressing critical vulnerabilities in traditional evidence handling systems. The proposed framework leverages permissioned blockchain architecture, cryptographic hashing, smart contracts, and off-chain storage to create an immutable, auditable, and transparent evidence management system that enforces automated chain of custody rules and maintains cryptographic integrity.

The framework achieves the three primary objectives established at the outset: (1) designing and implementing a permissioned blockchain framework that records forensic evidence data and enforces automated chain of custody rules through smart contracts, (2) generating cryptographic hashes using secure hash functions and Merkle tree structures to maintain integrity and enable tamper detection, and (3) enabling smart evidence management through automated workflows, role-based access control, transparent audit trails, and efficient provenance tracking.

Experimental deployments have demonstrated the technical feasibility of blockchain-based evidence management, with performance characteristics including block times of 1.2 to 3.8 seconds and transaction latencies of 85 to 150 milliseconds that are adequate for real-world forensic operations. The hybrid architecture that combines on-chain hash anchoring with off-chain artifact storage provides storage optimization while maintaining cryptographic integrity guarantees.

The framework provides significant benefits to all stakeholders in the forensic ecosystem, including law enforcement, forensic laboratories, prosecutors, defense attorneys, courts, and the public. By eliminating single points of failure, reducing human error, automating compliance, and providing transparent audit trails, blockchain-based evidence management enhances the integrity, reliability, and trustworthiness of forensic evidence throughout its lifecycle.

However, successful adoption requires addressing important challenges including initial implementation costs, technical complexity, interoperability with existing systems, governance frameworks, and legal and regulatory considerations. Future research should focus on integration with emerging technologies such as AI and IoT, development of cross-jurisdictional frameworks and international standards, implementation of privacy-preserving techniques, transition to quantum-

resistant cryptography, and collaboration between technologists and legal professionals to develop appropriate legal frameworks.

As digital evidence continues to proliferate and the demands on forensic systems grow, blockchain technology offers a transformative solution that can revolutionize evidence management and strengthen the foundation of the criminal justice system. The framework presented in this paper provides a roadmap for implementing blockchain-based evidence management systems that meet the rigorous requirements of forensic science while leveraging the unique capabilities of distributed ledger technology.

REFERENCES

[1] G. Foroglou and A.-L. Tsilidou, “Further applications of the blockchain,”2015.

[2] Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk:The blockchain model of cryptography and privacy-preserving smartcontracts,” in Proceedings of IEEE Symposium on Security and Privacy(SP), San Jose, CA, USA, 2016, pp. 839–858.

[3] W. Akins, J. L. Chapman, and J. M. Gordon, “A whole new world:Income tax considerations of the bitcoin economy,” 2013. [Online].Available: https://ssrn.com/abstract=2394738

[4] Y. Zhang and J. Wen, “An iot electric business model based on theprotocol of bitcoin,” in Proceedings of 18th International Conference onIntelligence in Next Generation Networks (ICIN), Paris, France, 2015,pp. 184–191.

[5] M. Sharples and J. Domingue, “The blockchain and kudos: A distributedsystem for educational record, reputation and reward,” in Proceedings of11th European Conference on Technology Enhanced Learning (EC-TEL2015), Lyon, France, 2015, pp. 490–496.

[6] C. Noyes, “Bitav: Fast anti-malware by distributed blockchain consensusand feedforward scanning,” arXiv preprint arXiv:1601.01405, 2016.

[7] Natarajan, V. V., et al. (2023). Crime forecasting using historical crime location using CNN-based images classification mechanism. In *Advances in Information Technology and Security* (pp. 13). IGI Global. https://doi.org/10.4018/978-1-6684-8618-4.ch013

[8] Natarajan, V. V., et al. (2026). A robust detect and avoid system for autonomous drone navigation. *NexusTech*, *1*, 2026004. https://doi.org/10.31893/tech.2026004

[9] Shukla, M., Srivastav, V., Khare, M. D., & Venkatesh, N. V. (2024). IoT-driven solutions for VANET trustworthiness: Examining misconduct and position security challenges. *Multidisciplinary Reviews*, *6*, 2023ss059. https://doi.org/10.31893/multirev.2023ss059

[10] SUNIDHI SUDHEER SHENOY, & N VISHNU VENKATESH (2025). A predictive framework for real-time courtroom assistance using AI-based mock legal advisor. *IJRAR*, *12*(2), 440-444.

[11] VENKATESH, M. N. V., Rajiv, D. A., Das, M. P., & Warrier, M. S. (2026). Vantage point recreation: A novel approach in endpoint security for smart homes. *International Journal of Innovative Research in Technology (IJIRT)*. https://doi.org/10.64643/IJIRTV12I8-191180-459