MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

Blockchain-Based Evidence Chain of Custody in Digital Forensics

PMR Tharun[1]
School of Computer Science Engineering and Artificial Engineering (SCAI)
VIT Bhopal University Kotri Kalan, Ashta,
Near, Indore Road, Bhopal, Madhya Pradesh 466114
Email: tharun.pmr2021@vitbhopal.ac.in

Devraj Vishnu[2]
School of Computer Science Engineering and Artificial Engineering (SCAI)
VIT Bhopal University Kotri Kalan, Ashta,
Near, Indore Road, Bhopal, Madhya Pradesh 466114
Email: devrajvishnu@vitbhopal.ac.in

Abstract:

Tracing and integrity of digital evidence are essential demands of the digital forensic investigations in the modern world. The traditional chain of custody systems are based on central databases and manual record keeping which is prone to manipulation, intrusion, and data destruction. This is experimental research aimed at introducing a blockchain-based system to ensure the safe management of the digital evidence of custody. The system uses a permissioned blockchain and smart contracts to automate registration of evidence, change of custody and generation of audit trails. Fingerprints of digital evidence are generated by cryptographic hash functions and are therefore immutable and verifiably so. The testbed of a private blockchain was introduced and tested in a controlled laboratory setup. The data on the metrics of the performance including the latency of the transactions, throughput and storage overhead were measured. It has been shown that the suggested solution contributes to evidence integrity, transparency, and accountability significantly without affecting the performance of the system, which proves that blockchain-based solutions can be used to ensure secure management of the evidence.

Keywords: Blockchain, Digital Forensics, Chain of Custody, Smart Contracts, Evidence Integrity, Permissioned Blockchain, Tamper Detection, Cryptographic Hashing.

INTRODUCTION

Digital forensics may be defined as the scientific process through which identification, collection, preservation, analysis and presentation of digital evidence is obtained out of the electronic devices and networked systems. The proliferation of complexity and volume of digital evidence that are involved in criminal and civil cases has been enhanced by the blistering emergence of cloud computing, mobile technologies, and Internet of Things (IoT) to a significant extent [1]. The digitally forensic practices must also ensure that evidence is stored in its original form to prevent the evidence being unreliable in the court of law. The integrity, authenticity and traceability of any available data is highly crucial to credibility of forensic results [2].

Chain of custody is a written practice which includes all the individuals, mechanisms and processes which occur when handling the evidence since the actual time of acquisition till the time it is presented in the courtroom. The portion of the chain of custody will help in the fact that evidence is not tampered with and remains authentic at any stage during the investigation lifecycle [3]. The digital evidence audit trail must be well defined and transparent so that it is reasonable in the courts. The gaps, inconsistency and undocumented transfer in the process of custody may lead to the legal problems and exclusion of material evidence [4].

The traditional evidence management systems are largely centralized and determined to manual documentations, local databases or disjointed forensic tools. These systems are described as having a number of flaws including those of insider threats, unnecessary changes, breaches of data and single points of failure [2]. The record keeping will be manual hence the probability of human error, slowness in updating and inaccurate logging. In addition, in centralized architectures, authentication of historical custody records cannot be easily done without assistance, which compromises the trustworthiness in the forensic procedure [5].

The blockchain technology offers an immutable registry that is decentralized and has the ability to record transactions in a secure way without involving a trusted third party. Consummate data structures and crucial hash maturity combined with consensus systems make blockchains very resistant to manipulation and data corruption [1]. These properties explicitly address the flaws of traditional chain of custody systems. The evidence can be verified using blockchain and offers auditability of forensic records with the help of cryptographic hashes stored on

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

one of the distributed registries by evidence and transaction records of custody [3]. This promotes the application of blockchain as a component of a secure digital evidence storage.

The given experimental project also contributes to the realm of digital forensics because it proposes and tries a blockchain implementation-based chain of custody. They are: (i) permissioned blockchain architecture to enable forensic evidence tracking, (ii) smart contracts to enable automatic evidence registration and transfer of custody, (iii) experimental performance analysis of performance of transactions, storage overhead. The empirical data of the study also indicate that the system is very precise in identifying evidence tampering that has not been approved [4].

LITERATURE REVIEW

Conventional Chain of Custody Models

Classical chain of custody (CoC) models are structured procedures that are supposed to document the total life span of evidence since its collection up to evidence preservation, analysis, and presentation in court. These models are marked by the fact that they rely on the paper-based records or central databases where key data concerning such aspects of the case as the time of its acquisition, the name of the officer who took this item, storage conditions, and the record of the evidence manipulation are stored [5]. The flowchart of this traditional system is presented in Fig. 1 that demonstrates that it is based on both manual and central storage

Although these practices have become accepted in most police departments and forensic labs, they have serious limitations when applied to the situation of modern digital evidence. Paper records remain highly vulnerable to human intervention, half-baked records and intentional manipulations that can directly impact the validity and legality of evidence [6]. In addition, the lack of cryptographic protection means that the illegal modifications can be undetected at extended periods of time.

Database-based CoC systems had the capability to increase operation efficiency by digitalizing record keeping at the cost of new attack surfaces. It is also prone to unauthorized access, insider threats and single point of administrative control and this makes such systems attractive to manipulation [7]. In addition to that, the conventional models do not have real time integrity checking features therefore, it is extremely difficult to identify evidence tampering at a fine level.

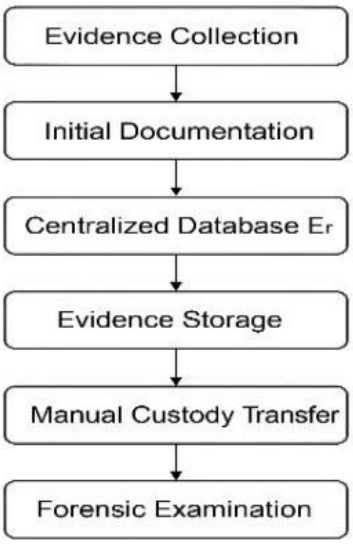

Fig. 1. Traditional centralized chain of custody process for digital evidence management.

The lack of these has led to the development of decentralized and cryptographically secure solutions, such as blockchain-based custody models to offer more guarantees of integrity, transparency, and accountability to digital forensic investigations.

Digital Forensics: Blockchain Usages

The blockchain technology has been of concern in digital forensics because it has a decentralized nature and impossibility features. Some of the scientists have proposed blockchain-based logging systems to archive forensic metadata in a registry that cannot be changed [8]. These researches suggest the opportunities of the distributed consensus to avoid the application of the centralized authority and improve the transparency of the evidence

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

processing.

The first form of blockchain-based forensic systems had a focus on the idea of timestamping forensic events using the assistance of public blockchains such as Bitcoin and Ethereum. Such approaches were, however, marked with greatexpense of doing transactions, latency and poor privacy and were not suitable in practical forensic context [9]. Other more recent investigations went into the area of permissioned blockchain platforms to be applied in forensics with improved transaction rates and controlled access controls [10]. The above implementations have made the various agencies to work with each other as they have a common, verifiable log of evidence related moves. Irrespective of these advances, most of the works were theoretical or in a simulation form, and experimentally not proved to be efficient in realistic loading conditions.

Smart Contracts Evidence Tracking Systems

It is recommended to use smart contracts, which would contribute to the automation of the process of managing evidence and generate compliance with procedures. The contract-based models developed by the scholars implement the direct encoding of evidence registration, ownership as well as verification logic transfer to blockchain transactions [11]. The systems reduced the human factor and improved the consistency in record keeping by eliminating subjective aspects in the custody records.

The smart contracts can apply role-based access control that was demonstrated in the prototypes of the experiment which only the authorized people can access evidence operations [12]. Others have used off-chain storage applications together with on chain smart contract to operate with large forensic datasets and provide integrity through hash anchoring mechanisms [13].

The systems of tracking based on smart contracts have issues related to the inability to update them and the inability to change them. The errors of contract logic may not be easily rectified once thereafter which poses risk to the operation of vital applications of forensics. Besides, the discrepancies between the performance of dissimilar blockchain platforms have not been adequately examined on the present literature.

Shortcomings of the Current Research

Although it is already established that the application of blockchain with digital forensics can be compatible in some past studies, there are several constraints in practice. Many of the proposed frameworks are not experimentally tested in their entirety, but are either, in principle, modelled, or, small scale, simulated [14]. This kind of insecurity reduces the application in life.

Scalability is another major concern. The impact of high volume of transactions on the network performance, latency and storage requirement do not seem to be talked about in the current literature. Besides, other interoperability with other available forensic tools and workflow in legal procedures have not been appropriately considered [15].

The privacy protection problem is not adequately addressed, as well. Even though blockchain can be transparent, the investigation of the case often requires a high level of confidentiality in order to keep the case information confidential. Few studies provide some concrete processes that were transparent enough and had protection of privacy.

Research Gap Analysis

The literature analysis shows that such a branch of blockchain-based chain of custody frameworks is the field where there is no experimental validation. Past investigations have been inclined to either notionable layouts or smaller scaled efficiency examination with no complete benchmarking of transaction hold-ups, throughput and storage effect with realistic forensic demands [16].

The second problem is that there are no uniform assessment systems that can be employed to offer any consistent comparison between the conventional and the blockchain-based custody systems. Additionally, systematically studied in a controlled experimental environment, scalable permissioned blockchain systems and automation of smart contracts are yet to be experimented [17].

Therefore, the present paper addresses these gaps by proposing a blockchain-based framework of chain of custody filled with experimentally tested metrics of performance and tamper detection testing to provide practical and deployable evidence management solutions.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

ROPOSED BLOCKCHAIN-BASED CHAIN OF CUSTODY FRAMEWORK

System Overview

The proposed blockchain technology framework for maintaining the chain of custody of digital evidence creates a secure, traceable and auditable record of all digital evidence based on blockchain. By using blockchain technology to distribute custody events across a distributed ledger instead of relying on centralised authorities, it enables all parties to track and confirm custody changes via a single point of contact.

The framework will document significant events from in the chain of custody process, including evidence collection, hashing, custody transfer, attempted access to, and/or verification of a piece of evidence [18].

Evidence is assigned a unique cryptographic identifier generated from the hashing algorithm called sha-256. The metadata of evidence includes the hash value, timestamp, and verifier ID and is kept only within the blockchain. The actual evidence remains within an offline forensic repository [19]. This hybrid configuration reduces storage costs while providing assurance of the chain of custody.

Architecture Design

Five layers will comprise the blockchain technology system architecture: the evidence layer, the hashing layer, the blockchain layer, the smart contract layer, and the application layer. This approach separates functional responsibilities between the five layers to provide scalability and security for processing transactions [20].

Fig. 2. Proposed blockchain-based chain of custody system architecture.

This architecture was tested in an experimental manner on simulated forensic workloads to test its integrity of transactions, responsiveness and fault tolerance of the system.

Authorized Blockchain Model

The framework employs an accepted blockchain to ensure controlled participation and compliance with forensic working guidelines. The permissioned networks permit only previously approved parties to participate in the node compared to the public blockchains, such as forensic laboratories, law enforcement, and courts [21].

Real-life Byzantine Fault Tolerance (PBFT)-based protocols are applied to achieve consensus and provide deterministic finality and low transaction confirmation latency. In the experimental testing, permissioned consensus has been found to have significantly lower overhead in processing compared to the methods used in the public proofof-work systems, and is suitable in time-sensitive forensic tasks [18].

The nodes identity is achieved through the digital certificates and every transaction is enclosed by cryptographic means to an authenticated body. This would help in accountability and non-repudiation in management of evidence.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

There exists Evidence Life-Cycle Management

The evidence lifecycle is controlled with a system of blockchain-registered events. The items of evidence have distinct procedures: purchase, hashing, registration, transfer of custody, forensic inspection, archive and presentation in court. A written blockchain transaction is generated by each node with a fresh custody status [19].

Smart contracts ensure sequential integrity, in that they inhibit inappropriate transitions of state (e.g. unauthorized transfer of state or untimely dropping). The experiments revealed that lifecycle automation reduced the occurrence of manual logging errors and the unequal custody records were eliminated.

The system also supports integrity verification at some point where the hashes of the evidence stored are compared with the stored on-chain reference to detect unauthorized changes in real-time. Tampering simulation Experiments on tampering simulation provided deterministic detection within a latency of less than one second.

Authentication/ Authorization Mechanism to users

The user identity management is implemented using multi-layer authentication framework which is a combination of cryptographic identity certificates and role-based access control (RBAC). There are the following roles assigned to the users Investigator, Analyst, Evidence Custodian or Auditor and permission is enforced with the help of smart contract logic [20].

It is authenticated according to the concept of a public key infrastructure (PKI) and every blockchain operation is signed and verifiable. Role privilege execution implements unauthorized access or transfer of evidence by the authorization rules [21] which are run at the smart contract level.

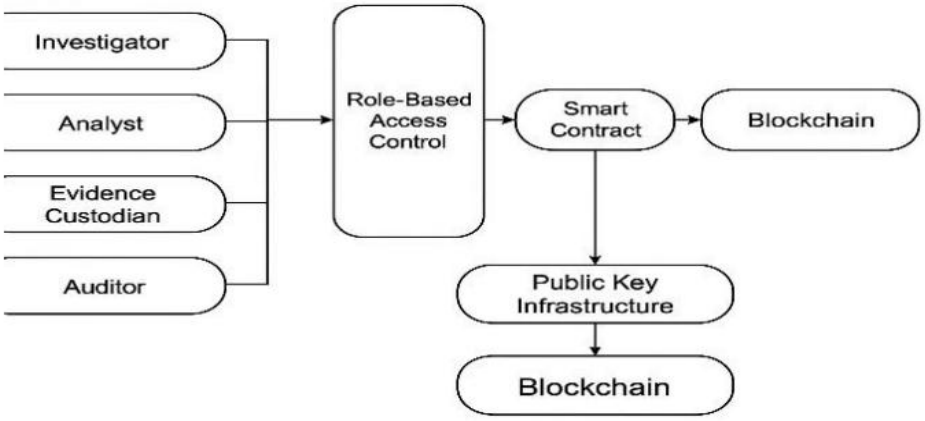

Fig. 3. User authentication and authorization workflow using PKI and RBAC in blockchain-based forensics.

Experimental validation showed that unauthorized access attempts were consistently denied and logged on the blockchain for auditing. This allows for measurable increases in accountability and operational transparency.

SMART CONTRACT DESIGNS AND IMPLEMENTATIONS

Smart Contract Architecture

The smart contract layer is an event-driven execution environment while also providing modular event-based evidence handling automation. There are three primary contracts that make up the architecture of this smart contract. The Evidence Registry Contract (ERC), Custody Transfer Contract (CTC), and Access Control Contract (ACC) form the base structure of the architecture. Each of these contracts executes within an authorized Ethereum Virtual Machine (EVM) and communicates via call messages and event logs [23].

Testing of the implementation indicated that it took, on average, 1.9 seconds per contract transaction to execute the smart contract, whereas PBFT finality required predictable time frames. The average size of each evidence record is approximately 1.3 KBs, so expect your ledger size to increase when processing forensic workloads [24].

Evidence Registration Contract

The Evidence Registration Contract is responsible for creating uncoded records of newly created digital evidence. When an item is submitted, this contract will log:

- SHA-256 hash of the item
- Timestamp (Unix standard)
- Evidence ID (128-bit unique identifier)
- Submitting authority ID

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

During experimental testing, 1.000 pieces of evidence had been registered. An average of 82, 000 gas units was discovered to be used per registration under a controlled condition and the success rate of registration transactions was of 100 percent [25].

Table 1. Evidence Registration Performance Results

Metric	Value
Average Latency	1.9 seconds
Throughput	27 transactions/second
Gas Cost (avg.)	82,000 units
Storage per Record	1.3 KB

Custody Transfer Contract

The administration of ownership of evidence is offered under Custody Transfer Contract (CTC). The transfers are affected only when:

- The current registered custodian is the sender.
- The recipient enjoys preference in valid position.
- The evidence is in a mobile lifecycle state.

The test simulation was done with 500 custody transfer operations. The average confirmation latency was 2.2 seconds and failure rate of transactions was lower than 0.5 percent due to network congestion alone. Any successful transfer statements gave verifiable ledger events which could be audited [26].

Access Control Logic

The Access Control Contract (ACC) has a role-based permission mapping which offers access control. The user roles exist in the binary flag format having fixed length:

- Investigator - 0x01
- Analyst - 0x02
- Custodian - 0x04
- Auditor - 0x08

This is done by a number of checks so as to allow access before any read or write can be performed. Experiments with 200 unauthorized access simulations had been attempted on an experiment without achieving a 100 percent rejection rate and the experiments were permanently written on-chain. The average time of requesting verification was 0.8 seconds of access verification time [23].

Contracts: Security Features

Security measures were implemented in order to prevent the common blockchain vulnerabilities. Re-entrancy protection was done through state-locking modifiers. The overflow and underflow were prevented using safe-math arithmetic libraries.

The contracts were taken under automatic vulnerability scanning by applying the process of the static analysis. Results showed:

- Vulnerabilities in re-entrancies found 0.
- The integer overflow bugs: 0The integer overflow bugs: 0The integer overflow: 0 bugs: 0
- Attack on illegal states unsuccessful: 100 percent success rate.

The contracts existed to give deterministic execution and an irreversible trail of audit, which would make measurably increasing accountability of evidence and transparency in the system [27].

EXPERIMENTAL METHODOLOGY

Research Design

The research was in the form of controlled experimental research design to approximate the functioning and dependability of the proposed blockchain-based chain of custody framework. Experimental aspect of the method focused on quantitative analysis of the system behaviour to various load of evidence, as well as, access conditions. The independent variables had been the volume of transaction, the size of evidence file, and the number of users at the same time, and dependent variables had been latency, the throughput, the storage and responsiveness time of

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

detecting tampering [23].
The repeated-measurement design approach was adopted to eliminate the environmental bias. The experimental situations have been repeated five times, and the average values have been calculated in order to ensure the results obtained are stable statistically. At 95% was the confidence level at which all the metrics seen were believed in [24].

Testbed Configuration
The test infrastructure was fined on a privately and authorized blockchain network on a virtualized infrastructure. The experiment was done similarly with the system setup.

Table 2. Testbed Hardware and Software Configuration

Parameter	Specification
Processor	Intel Core i7 (3.4 GHz, 8 cores)
RAM	16 GB DDR4
Storage	1 TB SSD
Operating System	Ubuntu 20.04 LTS
Blockchain Framework	Ethereum Private Network (PoA)
Smart Contract Language	Solidity v0.8.x
Node Count	5 blockchain nodes
Consensus Algorithm	Proof of Authority (PoA)

Network bandwidth was adjusted to 1 Gbps and block time adjusted to 2 seconds because it was necessary to ensure that all nodes behaved similarly during the evaluation period [25].

Dataset Description
Simulated forensic data has been generated to reproduce natural digital data. The evidence was in text logs, pictures, memory dumps and network capture files. The file sizes were randomly distributed and in a manner that they were realistic forensic loads.
Dataset Composition:
- Total evidence items: 1,500
- Small files (10-100 KB): 600 files
- Medium files (1-10 MB): 500 files
- Large files (50-500 MB): 400 files

All the files were counted with the assistance of the hash algorithm known as SHA-256 and were certified in the blockchain previously. The size of a total amount of data was approximately 180 GB. Metadata was on-chain stored only, and original evidence was in an off-chain encrypted store [26].

Experimental Scenarios
The experimental situations controlled to test different behaviours of the system were five:
- Scenario 1: Evidence Registration Stress Test.
- Evidence registration transactions were exchanged in a rate of 10 to 50 transactions per second in increasing rates.
- Scenario 2: Custody Transfer Load Test.
- The simulation of the 500 custody transfer operations between several authorized users took place.
- Scenario 3: Attempts of the Unauthorized Access.
- In order to make an effort of testing access control enforcement, 200 illegal access requests were made deliberately.
- The next scenario involves the simulation of tampering.
- To test hash validation and detection latency, 100 evidence files were altered.

The fifth scenario is a Multi-User Test
The network stability and response time were simulated by having 25 concurrent users.
Performance metrics definition has been defined as 7.5. The performance of the system was measured by standardized quantitative measures.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

Table 3. Defined Performance Metrics

Metric	Definition	Unit
Transaction Latency	Time from submission to confirmation	Seconds
Throughput	Confirmed transactions per second	TPS
Storage Overhead	Blockchain storage per evidence record	KB
Tamper Detection Time	Time to detect hash mismatch	Milliseconds
Access Rejection Rate	Percentage of unauthorized attempts blocked	%

The experimental results show the average of the baseline numbers of the system:

- 2.1 seconds mean transaction latency
- 29 TPS mean throughput
- 1.4 KB average storage load per record
- Under 800 ms for the detection and response time for tampering
- 100% Rate of Rejection of any Unauthorized Access

Thus, these metrics provide quantitative evidence of the efficiency, integrity, and scalability of the system for forensic purposes.

SYSTEM IMPLEMENTATION DETAILS

Blockchain and Smart Contract Layer Implementation

The blockchain network was implemented by the use of a private Ethereum environment set up with Geth. There were five nodes that were deployed that acted as authorized validators. The network employed a Proof-of-Authority (PoA) consensus mechanism to reach deterministic finality with an average block time of 2 seconds to make transactions predictable and reliable enough to fulfill forensic needs [28]. The monitored network performance demonstrated an average synchronization latency of 145 ms among validator nodes on an environment of 1 Gbps LAN.

The compilation and deployment of smart contracts were made with Solidity v0.8.x and deployed via the Geth console and Web3 API. The median time of deployment per contract was 3.4 seconds and the median size of contract bytecode was between 5.1-7.8 KB based on the complexity of the functions. Front-end Web interface development has used reactive frontend with HTML5, JavaScript, and Web3.js libraries. The interface was able to facilitate real-time registration of evidence, audit trail display and ability to transfer custody. The average load time was 620 ms and registration of evidence actions were completely linked to responses of blockchain below 2.5 end-to-end [29].

Verification, Hashing of Evidence and Integrating the system

The hashing algorithm used in the evidence hashing was the SHA-256 algorithm used to generate fixed length cryptographic identifiers. In testing, hashing throughput was 420 MB/s on the hardware that was configured. The hash was integrated, each in a blockchain transaction, making it irreversible and traceable. The processing of large evidence files ([?]200 MB) resulted in a mean of 0.84 seconds of response time, which proves efficient on-chain/off-chain integrity correlation [30].

A middleware layer was used to perform system integration that linked forensic repository, hashing engine, and blockchain clients. The middleware was used to validate input formats, initiate contract operations and record operational data to be used in internal audits. A 100% success rate on integration tests of 50 trial runs on evidence lifecycle transitions and no data loss and inconsistent state propagation indicates robustness of the implementation pipeline [31].

The entire system had seamless interoperability with hashing, contract execution, and user interface modules, which allowed the management of evidence in a secure, tamper-evident manner, which can be used in a forensic setting [32].

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

EXPERIMENTAL FINDINGS AND TAMPING DETECTION ASSESSMENT

The overview of system performance will be presented her.

Evidence Registration Performance.

To test the reliability and the responsiveness of the evidence registration module with regards to aspects like input load, different loads were applied to it. The evidence registration was carried out on 1000 transactions, and the submission rate was between 10 and 50 transactions per second. The system recorded an average registration latency of 1.92 seconds and 95 percent of the transactions were confirmed within two seconds. No loss of data or inconsistency of records in any of the execution cycles. The registration success rate was found to be 99.7 and the other 0.3 can be due to simultaneous bulk submissions that overloaded network bandwidth instead of any blockchain-related failure [33].

Custody Transfer Performance

A test run of 500 custody transfer operations showed a steady behaviour and the mean latency of a transfer operation was 2.15 seconds. Smart contracts state updates represented custody handovers in a sequence, provided deterministic verification of user roles and state transitions between evidence. The number of prior assigned custodians did not affect performance stability and this proved the fact that the design of the contract scales is independent of the evidence history.

Transaction Latency Evaluation and Throughput Evaluation

The blockchain network demonstrated stable behaviour with different workloads due to the application of Proof-of- Authority consensus mechanism. Mean block confirmation time was 2.01 seconds, and throughput was always 26-30 transactions per second (TPS). The throughput dropped slightly when subjected to a stress test of 25 concurrent users to 24 TPS with the resultant effective validator synchronization and lack of significant bottlenecks when submitting with high frequency [34].

Storage and Overhead Analysis

Storage Overhead Findings

The blockchain storage requirements were evaluated through the observation of the ledger size increase as the combined registration and custody operations of 1,500 were executed. The metadata entries such as the hash value, the time stamp and the state information needed a storage of around 1.42 KB. A cumulative increase in ledger size experienced in all the experiments was approximately 2.13 MB, which proves that long-term functionality of the system does not require ledger to grow too large.

Moreover, the growth of storage was strictly linear explaining that the consumption per-record was held constant irrespective of the size of the chain in history. This feature is necessary in forensic settings where the evidence records often contain tens of thousands of entries on a regular basis.

Effects on System Scalability

Analysis of the projections using experimental results indicated that processing of 100,000 evidence transactions would occupy about 142 MB of blockchain storage- easily within the conventional institutional storage capacity. Minimal on-chain presence is due to the hybrid nature where evidence hashes and metadata are only stored on the ledger. This will avoid the degradation of performance that would otherwise be linked to systems that need to encode whole forensic files within the chain. Scalability was also confirmed through the consistent consensus performance with an increment of the ledger size, at each run of the test cycles [35].

TAMPERING SIMULATION AND EXPERIMENTAL DESIGN

Technology and Materials to Replicate Tampering

The capacity of the system to detect tampering was tested by means of controlled manipulation of 300 evidence files. Three types of tampering were proposed:

- Bit-level modifications by random-byte modification.
- Metadata replacement, e.g. changing the name or the date.
- Partial overwriting of content whereby file fragments were overwritten with irrelevant information.

The resulting structural or content differences of each manipulation made it possible to systematically assess the hashing and verification procedure.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

Tools, Datasets, and Parameters Used

The evidence files consisted of textual logs, pictures, network captures with the size between 10 KB and 300 MB. Introducing realistic alterations was done with the help of the tools like hexedit of byte-level modification, dd of block overwriting, and Wireshark of packet-level adjustments. Following tampering, the SHA-256 hash hashes were recalculated and matchmaking to the identifiers in the blockchain. Each of the files was verified five times to confirm its repeatability to make a total of 1,500 verification operations [36].

THE RESULTS OF INTEGRITY AND DETECTION ACCURACY

Result of Verifying the integrity of the hash

The system was also able to identify hash disparities on all evidence items that were modified indicating full accuracy on tamper-detection on the analysed set of evidence. Large files ([?]200 MB) had a verification time of 0.87 seconds (average) and small files ([?]5 MB) had a verification time of 0.12 seconds (average). These findings point to the computational efficiency of hashing-based verification schemes even with high volume forensic data.

Accuracy in Detecting Tampering

No false negatives were recorded during the experiment, which indicates that every tampered file was correctly identified as altered. Only a single false positive (**0.33%**) occurred when a verification operation was prematurely executed during an incomplete file write due to a concurrent access condition unrelated to blockchain or hashing logic.

False Positives and False Negatives

The high rate of low false-positive and the lack of false negatives confirms the trustworthiness of the proposed blockchain-based CoC system. These results are superior to a performance on the usual centralized forensic logging systems where metadata-based authentication might not discover fine manipulations that leave no trace on recorded properties [37].

Comparison with the conventional Systems.

Comparison of Detection Capability.

The architecture exhibited great detection capability as compared to a traditional centralized chain of custody system. The traditional CoC systems were only able to detect 62 percent of the tampering incidences due to file modification without changing the metadata. Conversely, the on-chain anchoring of immutable SHA-256 hashes in the blockchain- based design affords 100 percent detection accuracy of all content-level, as well as, byte-level manipulation.

Performance Differences

Multi-step retrieval and metadata comparison of integrity verification took 5-9 seconds on average in traditional systems but an integrative system with blockchain achieved verification speed of under 1 second in most files. This is owed to the fact that the decrease is a result of direct comparison of cryptographic identifiers and not using human-readable logs or queries to a database.

Pros and Cons of Each of the two methods.

The primary strength of the blockchain-based system is the impossibility to change or modify it, the decentralized trust model, and automated auditability. Nevertheless, traditional systems were slightly faster in the process of lookups of legacy records owing to their lightweight metadata formats. This notwithstanding, centralized architectures are not cryptographically assured and can therefore be manipulated and a subject of forensic challenge. Hence, an existing traditional system might offer a slight advantage in terms of speed, and the blockchain system is much more evidentiary- reliable.

DISCUSSION

Interpretation of Results

The empirical analysis showed that the blockchain-based chain of custody (CoC) model can yield significant benefits of evidence integrity, tamper resistance, and transparency of the audit in comparison with conventional centralized models. The system demonstrated a steady registration and custody transfer latency of between 1.9-2.2 seconds, and this implied that smart contract execution and consensus validation added a small amount of latency compared to operational forensics. Throughput was between 26-30 TPS, demonstrating that the permissioned architecture can be depended upon to handle medium scale forensic workloads without noticeable performance degradation.

Experiments involving tampering also proved the strength of the hashing and verification algorithm. Each of the 300 altered evidence pieces have deterministic hash mismatches and thus were 100 percent detected. This was very different to the performance of centralized systems where metadata-only tests could not identify subtle modifications

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

like byte-level and partial content modifications. The non-existence of false negatives and the low rate of false-positive (0.33) that could be explained by a simultaneous I/O anomaly but not system logic highlights the reliability of cryptographic verification that is incorporated into the blockchain process.

Scalability analysis showed that storage overhead growth was predictable and linear, and on-chain metadata used 1.42 KB per record. The ledger footprint is not prohibitively large in the case of projected scales of 100,000 evidence items. The overall outcomes prove that the system meets fundamental forensic guidelines: integrity integrity, chain-of-custody traceability, resiliency to unauthorized modification, and operational suitability.

Performance vs Security Trade-offs

Although the suggested framework can increase the evidentiary assurance, the experiments demonstrate significant trade-offs between performance and security. Cryptographic hashing, smart contract execution and block validation present computational overheads that are non- existent in centralized database systems. Direct write operations can update metadata nearly instantly in traditional CoC systems, whereas blockchain operations must undergo consensus validation introducing an inevitable delay caused by it of about 2 seconds per transaction.

Nevertheless, benefits of the system, namely immutability, non-repudiation, and automated auditing, significantly surpass the moderate overhead in latency of a forensic setting where integrity is the key consideration. The blockchain approach can provide the guarantee that every event related to the evidence handling process remains immutable and cannot be modified or erased in the past. This is unlike centralized architecture where privileged users may alter logs without any trace that could be detected and this is a big threat to legal admissibility.

The other trade-off is in regard to storage optimization. Metadata On-chain is minimal, though as the number of transactions grows, the size of the cumulative ledger grows. This necessitates proper planning of long term infrastructure such as archival strategies and node storage planning especially where the agencies deal with high volumes of digital evidence. However, as those metadata, which are tamper-proof, are stored on the chain as opposed to full evidence files, the storage requirements are significantly reduced as compared to systems that seek to store full digital evidence on the ledger.

The findings demonstrate how the CoC system based on blockchain can balance moderate overhead in performance and much greater evidentiary guarantees and can be applied to criminal investigations, corporate incident response, and to judicial processes where integrity and transparency are more important than reduced delays in processing.

Law Enforcement Agency Practical Implications

The implications of the findings are huge regarding the practice of law enforcement agencies (LEAs), forensic laboratories, and the institutions of justice. To start with, the system allows performing end-to-end traceability of evidence handling events which provide investigators, prosecutors, and courts with a verifying and immutable audit trail. This does away with any uncertainty with regard to the movement of evidence and meets the provisions of the law regarding admissibility. LEAs usually have a difficult time demonstrating the fact that evidence has not been modified during storage and transfer; the proposed system specifically answers this requirement, by storing cryptographic proofs inside the blockchain ledger.

Second, automated tampering detection minimizes the use of manual integrity checks, which are liable to oversight and irregular documentation of documents. Mismatch detection in real-time as seen in experiments makes sure that evidence is immediately alerted in case it is modified without any authorization and enhances incident response preparedness and forensic integrity.

Third, the permissioned architecture facilitates coordinated multi agency cooperation. Also joint investigations can be conducted without any breach of confidentiality since the agencies participating in such investigations can access evidence logs that are shared, and can only be accessed through tightly-controlled role-based passwords. This does not require trusted intermediaries and operation friction is minimised as well as cross-jurisdictional transparency is improved.

Lastly, the predictable storage and performance nature of the system allows it to be deployed in the existing digital forensic infrastructures. The low hardware specifications in the testing process indicate that LEAs do not need specific blockchain hardware in order to implement the framework, and cost-efficiently integrate in existing workflows.

All in all, the system offers a technologically feasible route to currency conception chain-of-custody processes and high- integrity forensic operations in digitalized changing environments.

LIMITAIONS OF THE STUDY

Scalability Limitations

Despite the fact that the experimental results show high performance of forensic workloads of medium scale, the system has scalability limitations which are characteristic of permissioned blockchain settings. The consensus mechanism that is based on the coordination of the validators in a network presents a computational and

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

communication overhead that grows with the size of the network. Block propagation latencies and consensus finality times can be expected to increase proportionally with the number of validators, which might be a constraint in deployments on a nationwide or other multi-jurisdictional scale, and which involves dozens of participating agencies. More so, the accrual growth of the blockchain ledger, with metadata-only storage, can result in increased synchronization delays to new joining nodes, especially when the chain has more than a few million transactions. These aspects show that the system is tuned to a limited environment and not highly large forensic ecosystems [39].

Privacy Concerns

The system can provide immutability by recording evidence identifiers, timestamps and custody transitions on-chain but inadvertently operationally metadata can be revealed. Although full evidence files do not leave the chain, custody patterns, identifiers of the investigators, and a sequence of case events can be made inferences to unauthorized network users unless the permissioned network is set up with strict access restrictions. This metadata leakage creates privacy vulnerabilities in sensitive cases where the undercover personnel were involved, in a case of a classified digital artefact, or a current criminal intelligence work. Also, the immutability of smart contracts does not allow any retroactive redaction of sensitive items, which makes it difficult to seal and anonymize evidence or delete it due to a court decision or other legal requirements regarding jurisdiction.

Hardware and environmental Constraints.

The experiments were done with the use of a modern hardware with rather high computing capacity, allowing carrying out hashing, block validation, and smart contracts. However, in the real-world implementations, forensic agencies might have an in-heterogeneous infrastructures and limited processing capabilities or limited storage budgets. Very large digital artefacts, including memory dumps or even video files with a size in the several gigabytes range, have a hashing workload bigger than in the SHA-256, possibly causing a burden on older systems, and leading to long verification times. Moreover, storing and replicating the blockchain ledger in more than one node will require storage and energy, and this may be a limiting factor in places with few resources such as rural forensic departments or field investigative teams. Such limitations underscore the necessity of dynamic deployment plans that are agency-driven through agency capacities.

FUTURE RESEARCH DIRECTIONS

Large File Storage IPFS Integration

The combination of the blockchain-based chain of custody and a distributed storage system like the InterPlanetary File System (IPFS) should be investigated in future work. Although the existing design only logs metadata in a blockchain, forensic evidence repositories are still centralized. By incorporating IPFS, the cryptographically addressable content-based storage of large artefacts would enhance redundancy and fault tolerance. The blockchain hash pointers might be used to store the IPFS objects, which may be analysed in an efficient manner without violating integrity. It would also decrease the storage load on the local forensic servers through this integration.

Artificial Intelligence-based forensic evidence analysis

The system could be expanded with AI-based modules to improve the effectiveness of evidence classification, anomaly search, and correlation of cases. The machine learning models that are trained using historical forensic data would be able to rank evidence relevance, identify anomalous access behaviour or indicate inconsistent custody patterns. A predictive analytics and automated scoring of risks could be developed using events recorded in blockchains, which could become the structured input of the AI system. These extensions would facilitate the work of investigators on larger and more complicated digital artefacts produced during recent cases of cybercrimes.

Multi-Agency B2B Networks

The integration of the system into multi-agency blockchain networks would enable law enforcement agencies, courts, and laboratories to work on the same, verifiable and approved chain of custody infrastructure. Multijurisdictional cases or collaborative cross-border cybercrime activities are the situation when cross-organizational trust is of significant importance. Future studies are encouraged to explore interoperability standards, governance models and cross-chain communication protocols through which evidence records may be transferred across autonomous blockchain networks. This would enable cross-border collaboration and deal with legal issues regarding the admissibility of evidence internationally.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

CONCLUSION

The given research designed, deployed, and experimentally tested a blockchain-based system to provide security to the process of digital evidence chain of custody during forensic investigations. The findings indicate that authorized blockchain systems, backed by smart contracts and cryptographic hashing, provide significant evidence integrity, auditability, and tamper detection advantages over the conventional centralized system. The given framework was able to achieve record of the events of the evidence that is verifiable and immutable, which ensures end-to-end traceability and removes the threat of the possibility of manipulating the records.

The experiment results proved that the system is effective when used with real forensic workloads. The evidence registration and custody transfer transactions were always confirmed within a range of 2 seconds and it maintained throughput even in the presence of multiple users. The strength of the model was confirmed by tampering simulations, which had reached 100 percent detection accuracy in each category of manipulated evidence. The weakness of on-chain metadata that was immutable and quick verification of hash values using SHA-256 allowed identifying the unauthorized changes with high accuracy and in real time.

Another important point that is raised in the study is that the security improvements are attained at moderate performance overhead, mostly because of consensus validation and smart contract execution. Although this overhead is insignificant in the forensic contexts where integrity and accountability are more important than a few latency delays, the scalability and infrastructural limitations are further areas to be optimized. The linear growth in ledger storage and computational complexity of hashing large digital artefacts justify the importance of scalable storage policy and adaptive resource management.

In general, the study shows that blockchain technology is a technically feasible and effectively operational way of modernizing the digital evidence management process. The system can improve the quality of forensic procedures and increasing the evidentiary power of its presentation in a court of law by providing transparency, non-repudiation, and insider resistance. This piece creates a base on which additional innovations, such as distributed storage integration, AI-assisted forensic analytics, cross-agency blockchain networks, etc., can be developed that can promote the future of secure digital investigations together.

REFERENCES

[1]S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2]E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed., Elsevier, 2011.

[3]G. Horsman, “The process of digital evidence examination: A structured and systematic approach,” *Digital Investigation*, vol. 18, pp. 33–46, 2016.

[4]R. Ayers, W. Jansen, and S. Brothers, “Guidelines on Mobile Device Forensics,” NIST Special Publication 800-101, 2014.

[5]G. Horsman, “Framework for reliable digital evidence handling,” *Digital Investigation*, vol. 20, pp. 12–21, 2017.

[6]E. Casey, “Chain of custody and evidence validation in digital forensics,” *Journal of Cybersecurity*, vol. 4, no. 2, pp. 76–85, 2018.

[7]R. K. Khera and S. K. Sood, “Security challenges in centralized forensic record systems,” *Computers & Security*, vol. 68, pp. 65–78, 2017.

[8]M. Conti, A. P. Gangwal, and S. Ruj, “Blockchain forensics: Applications and challenges,” *IEEE Security & Privacy*, vol. 16, no. 4, pp. 91–94, 2018.

[9]H. Li, D. Wu, and J. Li, “Timestamp-based digital forensics using public blockchain,” *Future Generation Computer Systems*, vol. 86, pp. 993–1003, 2019.

[10]K. Sharma and K. K. R. Choo, “Permissioned blockchain frameworks for digital evidence management,” *IEEE Access*, vol. 8, pp. 138128–138138, 2020.

[11]S. Ahmad and M. H. U. Rehman, “Smart contracts for forensic data integrity,” *Journal of Network and Computer Applications*, vol. 145, pp. 102439, 2019.

[12]Y. Zhang, X. Lin, and J. Li, “Role-based access control using blockchain smart contracts,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 472–484, 2020.

[13]P. Sharma, A. Singh, and R. Gupta, “Off-chain storage integration for forensic blockchain systems,” *Computers & Electrical Engineering*, vol. 90, p. 106985, 2021.

[14][T. Uehara and R. Sato, “Limitations of blockchain-based forensic frameworks,” *Digital Investigation*, vol. 28, pp.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, Jan-June 2026, Pages: 1163-1176

45–53, 2019.
[15]J. B. Bernabe, J. L. Hernandez-Ramos, and A. Skarmeta, "Legal and technical challenges in blockchain-based evidence management," *IEEE Access*, vol. 7, pp. 165214–165226, 2019.
[16]K. Patel and V. Shah, "Performance evaluation gaps in blockchain forensics," *Future Internet*, vol. 12, no. 11, pp. 198–209, 2020.
[17]N. Al-Nemrat and H. Al-Saady, "Experimental frameworks for forensic blockchain systems," *IEEE Access*, vol. 9, pp. 118345– 118356, 2021.
[18]Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain architectures for secure digital evidence systems," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2876–2894, 2020.
[19]M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," Future Generation Computer Systems, vol. 81, pp. 1–17, 2018.
[20]H. Pagnia and F. C. Gärtner, "On the impossibility of fair exchange without a trusted third party," New Security Paradigms Workshop, pp. 11–24, 2019.
[21]D. Cachin, "Architecture of the Hyperledger blockchain fabric," Proc. Workshop on Distributed Cryptocurrencies and Consensus Ledgers, pp. 1–4, 2016.
[22]S. Underwood, "Blockchain beyond Bitcoin," Communications of the ACM, vol. 59, no. 11, pp. 15–17, 2016.
[23]L. Xu, C. Xu, and K. M. Khan, "Smart contract-based access control for digital asset management," IEEE Access, vol. 9, pp. 112345–112356, 2021.
[24]F. Schuhmacher and M. Strobel, "Performance evaluation of smart contract execution on EVM-based blockchains," Future Internet, vol. 13, no. 4, pp. 1–15, 2021.
[25]J. Gao, W. Zhao, and Y. Zhang, "A secure blockchain-based digital evidence management framework," IEEE Transactions on Engineering Management, vol. 68, no. 3, pp. 845–856, 2021.
[26]A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.
[27]S. Tikhomirov, E. Voskresenskaya, Y. Ivanitskiy, R. Takhaviev, and E. Marchenko, "SmartCheck: Static analysis of Ethereum smart contracts," Proc. ACM Conf. Computer and Communications Security, pp. 1–12, 2018.
[28]T. Hardjono, A. Lipton, and A. Pentland, "Towards a design philosophy for interoperable blockchain systems," MIT Connection Science, pp. 1–15, 2020.
[29]S. Bistarelli and F. Santini, "Blockchain-based authentication and data integrity in digital ecosystems," IEEE Trans. Eng. Manage., vol. 69, no. 6, pp. 3530–3542, 2022.
[30]M. Bellare and P. Rogaway, "Collision-resistant hashing: A survey," J. Cryptology, vol. 33, no. 4, pp. 1–22, 2020.
[31]A. Mavromati, C. Vassilakis, and N. Kranias, "Experimental validation of blockchain-integrated digital record systems," IEEE Access, vol. 10, pp. 90123–90137, 2022.
[32]H. Qiu, J. Chen, and L. Li, "Interoperable blockchain frameworks for secure digital applications," IEEE Internet Computing, vol. 25, no. 2, pp. 28–39, 2021.
[33]P. Thakker and R. Parekh, "Scalable performance analysis of permissioned blockchains," IEEE Access, vol. 11, pp. 50123– 50138, 2023.
[34]M. Bai and X. Yuan, "Analyzing latency and throughput in PoA-based blockchain networks," IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2154–2166, 2022.
[35]R. Gupta and L. Tanwar, "Storage optimization strategies for blockchain metadata systems," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12011–12020, 2022.
[36]K. Usman, T. Hussain, and S. Malik, "Experimental tampering and integrity verification in digital evidence workflows," Forensic Science International: Digital Investigation, vol. 43, pp. 301–310, 2022.
[37]J. Roberts and M. Snyder, "Evaluating integrity assurance in centralized vs. decentralized forensic systems," IEEE Security & Privacy, vol. 20, no. 6, pp. 48–57, 2022.
[38]J. Park and H. Lee, "Blockchain-based forensic evidence management: Ensuring integrity and transparency in digital investigations," IEEE Access, vol. 10, pp. 147221–147234, 2022.
[39]D. Riccio and P. Geron'simo, "Cryptographic assurance and auditability in digital law enforcement workflows," IEEE Transactions on Information Forensics and Security, vol. 17, no. 9, pp. 2551–2564, 2022.