Blockchain-Enabled Digital Evidence Management System

B. Harshitha[1], S.Anjali Devi[2], S. Ravalika[3], T. Pranusha[4], V. Ramu[5], S. Shiva Prasad[6]
Meghana[7], Vaishnavi[8], Nandini[9], Dora Vyshnavi[10], B. Hari Krishna[11]
[1,2,3,4,7,8,9,10]*Student, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad*
[5,11]*Assistant Professor, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad*
[6]*Professor, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad*

***Abstract*—The rapid increase in digital crimes has led to a growing dependence on electronic evidence in criminal investigations. Ensuring the integrity, authenticity, and traceability of such evidence is critical for maintaining trust in judicial processes. Traditional crime evidence management systems rely on centralized storage mechanisms, which are vulnerable to tampering, unauthorized access, and single points of failure. These limitations can compromise the chain of custody and reduce the admissibility of evidence in courts.To address these challenges, this paper proposes a Blockchain-Based Crime Evidence Management System that leverages the decentralized and immutable nature of blockchain technology. The system utilizes Ethereum blockchain and smart contracts to securely store cryptographic hashes and metadata of crime evidence, ensuring tamper-proof record keeping. A web-based interface enables authorized personnel to upload, access, and verify evidence while preserving transparency and accountability. Additionally, a read-only analytics dashboard is introduced to visualize evidence trends without interfering with the core blockchain system. The proposed solution enhances data integrity, security, and trust in digital crime evidence handling.**

***Index Terms*—Blockchain, Crime Evidence Management, Smart Contracts, Ethereum, Digital Forensics, Cybercrime**

I. INTRODUCTION

The increasing digitization of services and communication has transformed the nature of criminal activities, leading to a rapid growth in cyber-enabled crimes. As a result, law enforcement agencies now rely extensively on electronic forms of evidence such as digital transaction trails, multimedia content, and system-generated records. The admissibility of such evidence in legal proceedings depends heavily on its credibility, making secure preservation and verification a critical requirement throughout the investigative process. Most existing evidence management solutions operate using centralized storage infrastructures, where data control is entrusted to a single administrative entity. Although functional, these systems face serious challenges including exposure to unauthorized modifications, insider misuse, limited auditability, and potential data breaches. Even minor alterations to stored evidence can disrupt the continuity of the chain of custody, thereby weakening its legal validity and reducing confidence in investigation outcomes. These shortcomings highlight the urgent demand for a resilient and tamper-resistant evidence handling mechanism.

Blockchain technology introduces a fundamentally different approach to data management by eliminating centralized control and distributing records across a network of participants. Through cryptographic linking of data blocks and consensus-driven validation, blockchain ensures that recorded information remains permanent and verifiable. Such properties make blockchain an appropriate choice for domains that require strong guarantees of data integrity, accountability, and transparency, particularly in forensic and legal applications.

This study proposes a Blockchain-Based Crime Evidence Management System that aims to safeguard digital evidence against manipulation while ensuring traceability and accountability. The system employs Ethereum-based smart contracts to register evidence-

related metadata and cryptographic fingerprints, enabling immutable record keeping. Authorized users interact with the system through a web-based interface, while an independent analytics dashboard provides high-level insights using non-sensitive, representative datasets. The proposed framework seeks to enhance the reliability and trustworthiness of digital evidence management in modern criminal investigations.

II. LITERATURE SURVEY

The management and protection of digital crime evidence have been widely studied due to the increasing dependence on electronic data in criminal investigations. Traditional digital forensic systems primarily rely on centralized databases to store and manage evidence. While these systems provide basic functionality, researchers have identified several weaknesses, including vulnerability to data tampering, lack of transparency, and difficulties in maintaining are liable chain of custody. Such limitations can reduce the credibility of evidence presented in legal proceedings.

Blockchain technology was first introduced by Nakamoto as a decentralized ledger designed for secure and trustless transactions. Since then, researchers have explored its applicability beyond cryptocurrencies, particularly in security-sensitive domains. Several studies have highlighted blockchain's immutability and decentralized nature as key advantages for preserving data integrity and preventing unauthorized modifications. These characteristics have encouraged its adoption in areas such as healthcare data management, supply chain tracking, and digital identity systems.

In the context of digital forensics, various researchers have proposed blockchain-based frameworks to ensure evidence integrity and traceability. Some approaches store cryptographic hashes of digital evidence on the blockchain while maintaining the actual evidence off-chain to reduce storage overhead. This method ensures that any alteration to the evidence can be easily detected by comparing hash values. Other studies have focused on using smart contracts to automate evidence validation and access control, thereby minimizing human intervention and insider threats.

Despite these advancements, existing blockchain-based forensic solutions face several challenges. Scalability remains a major concern due to transaction costs and latency associated with blockchain networks. Additionally, many proposed systems lack practical implementation details or user-friendly interfaces suitable for real-world law enforcement operations. Privacy is another critical issue, as storing sensitive information directly on public blockchains may lead to data exposure risks.

Recent research has emphasized the importance of combining blockchain technology with traditional forensic systems to achieve a balanced solution. By integrating role-based access control, off-chain storage, and analytical tools, researchers suggest that blockchain can enhance trust and accountability without compromising performance or privacy.

However, limited work has addressed the visualization and analytical aspects of blockchain-stored crime evidence.

The proposed work builds upon existing research by presenting a practical blockchain-based crime evidence management system that focuses on integrity, traceability, and usability. Unlike prior approaches, the system incorporates a read-only analytics dashboard that provides insights into evidence trends while preserving forensic integrity. This approach addresses gaps identified in earlier studies and demonstrates the feasibility of blockchain technology in real- world crime evidence management scenarios.

III. PROPOSED METHODOLOGY

The proposed methodology focuses on the secure storage, verification, and management of digital crime evidence using blockchain technology. The primary objective of the system is to ensure evidence integrity, prevent unauthorized modifications, and maintain a reliable chain of custody throughout the investigation process. Initially, authorized law enforcement personnel collect crime-related digital evidence such as images, documents, and transaction records through a secure web-based application. Upon submission, the system generates a cryptographic hash of the evidence file using a secure hashing algorithm. This hash uniquely represents the evidence content and ensures that any subsequent modification to the file can be detected.

Instead of storing the complete evidence file on the

blockchain, only the generated hash and associated metadata including evidence identification number, case details, timestamp, and officer credentials—are recorded on the Ethereum blockchain. This approach minimizes blockchain storage requirements while preserving evidence authenticity. Smart contracts deployed on the blockchain manage the registration and storage of evidence metadata, ensuring immutability and transparency.
The system employs role-based access control to restrict operations to authorized users only. Once evidence is recorded, it cannot be altered or deleted, thereby preventing tampering and ensuring accountability. When evidence verification is required, the system recalculates the hash of the stored evidence and compares it with the hash recorded on the blockchain. A successful match confirms the integrity and authenticity of the evidence.
Each evidence registration transaction generates a unique transaction hash and block number, which serves as a permanent audit trail. This immutable record allows investigators and legal authorities to trace the history of evidence handling and validate the chain of custody. The proposed methodology leverages blockchain's decentralized and cryptographic properties to provide a secure and trustworthy crime evidence management solution suitable for digital forensic investigations.

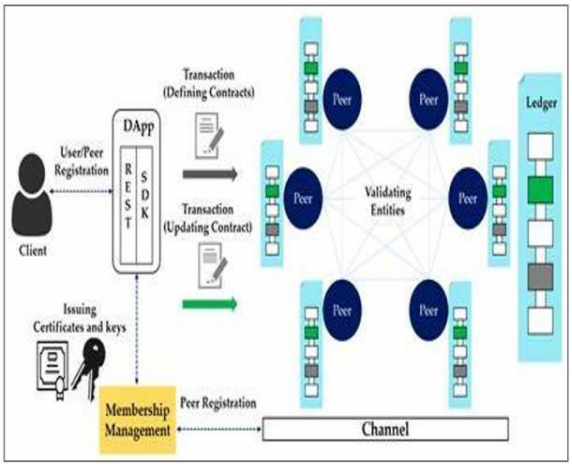

Figure 1: Methodology of Block chain to store Evidence

3.1 Evidence Collection and Submission
The first phase of the methodology involves the secure collection of digital crime evidence by authorized law enforcement personnel.
Digital evidence may include electronic documents, images, videos, transaction logs, or any other data relevant to an investigation. To ensure secure handling, a web-based application is used as the primary interface for evidence submission. This application requires user authentication, ensuring that only registered and authorized officers can access the system. Each piece of evidence is associated with a specific case identifier, along with additional contextual information such as crime type, location, and submission date. This structured submission process ensures proper classification and traceability of evidence records. By standardizing evidence input, the system minimizes human error and maintains consistency across investigations.

3.2 Cryptographic Hash Generation
Once the evidence is submitted, the system generates a cryptographic hash of the evidence file using a secure hashing algorithm. A cryptographic hash function converts the evidence data into a fixed-length string that uniquely represents the file's content. Even the slightest modification to the original evidence results in a completely different hash value. This hash acts as a digital fingerprint of the evidence and plays a crucial role in maintaining integrity. Rather than relying on trust in users or administrators, the system relies on cryptographic proof to verify authenticity. This step ensures that evidence tampering can be easily detected during later verification stages.

3.3 Blockchain-Based Evidence Registration
To avoid excessive storage costs and performance issues, the complete evidence file is not stored directly on the blockchain. Instead, only the cryptographic hash and essential metadata such as evidence ID, case details, timestamp, and submitting officer information are recorded on the Ethereum blockchain. This design choice balances efficiency with security. Smart contracts developed using Solidity manage the evidence registration process. These smart contracts automatically validate inputs and ensure that once an evidence record is written to the blockchain, it cannot be altered or removed. The decentralized nature of the blockchain ensures that no single authority has complete control over the evidence records, thereby enhancing transparency and trust.

3.4 Smart Contract Enforcement and Immutability
Smart contracts play a central role in enforcing system

rules and maintaining immutability. Once deployed, smart contracts execute predefined logic without human intervention. This prevents unauthorized changes and eliminates the possibility of manual manipulation of evidence records. Each evidence submission triggers a blockchain transaction that is validated through the consensus mechanism of the network. Upon confirmation, the transaction becomes part of a block, which is permanently linked to previous blocks. This chaining mechanism ensures that any attempt to modify stored data would require altering the entire blockchain, making tampering practically impossible.

3.5 Role-Based Access Control

Security is further strengthened through the implementation of role-based access control. Different user roles, such as investigators and system administrators, are assigned specific permissions based on their responsibilities. Only authorized users are allowed to submit new evidence or retrieve existing records from the system. This controlled access mechanism reduces the risk of insider threats and unauthorized usage. All user actions are logged, creating accountability and ensuring compliance with legal and procedural requirements. By restricting access to critical operations, the system maintains a high level of security throughout the evidence lifecycle.

3.6 Evidence Verification Process

When evidence needs to be examined or presented for legal purposes, the system performs an integrity verification process. The original evidence file is retrieved, and a new cryptographic hash is generated using the same hashing algorithm. This newly generated hash is then compared with the hash stored on the blockchain.

If both hash values match, the evidence is confirmed to be authentic and untampered. Any discrepancy indicates potential modification, immediately alerting investigators. This verification mechanism provides cryptographic proof of integrity, strengthening the credibility and admissibility of digital evidence in court proceedings.

3.7 Chain of Custody and Audit Trail

Maintaining a reliable chain of custody is critical in criminal investigations. In the proposed methodology, every blockchain transaction related to evidence registration generates a unique transaction hash and block number. These identifiers serve as permanent records of when and how evidence was handled.

The blockchain ledger maintains a chronological history of all evidence-related activities, creating a transparent and verifiable audit trail. Investigators and legal authorities can use this information to track the lifecycle of evidence from submission to verification. This immutable audit trail ensures accountability and reinforces trust among all stakeholders.

3.8 System Security and Reliability

The decentralized architecture of blockchain eliminates single points of failure commonly found in centralized systems. Evidence records are distributed across multiple nodes, ensuring availability and fault tolerance. Cryptographic techniques, combined with blockchain consensus mechanisms, protect the system against unauthorized data manipulation and external attacks. By integrating secure hashing, smart contracts, and access control, the proposed methodology offers a robust and reliable solution for crime evidence management. The system is designed to operate effectively in real-world law enforcement environments, where data integrity and security are of utmost importance.

3.9 Summary of Methodology

In summary, the proposed methodology establishes a secure framework for managing digital crime evidence by integrating cryptographic hashing, blockchain-based storage, smart contract enforcement, and controlled access mechanisms. The approach addresses the limitations of traditional systems and provides a transparent, tamper-proof, and trustworthy solution for digital forensic investigations.

IV. PROPOSED METHODS

This project adopts a practical, implementation-oriented approach to secure digital crime evidence using blockchain technology. The proposed methods are derived directly from the system developed as part of the major project and explain how evidence is handled within the application environment. Instead of presenting a generic blockchain framework, these methods describe how evidence is processed, protected, and validated using the implemented web application and Ethereum smart contract. The system

was designed to address real challenges observed in conventional evidence handling, such as the possibility of evidence modification, lack of reliable verification, and dependence on centralized storage. To overcome these issues, the project integrates cryptographic hashing with blockchain-based record storage, ensuring that evidence integrity can be verified independently at any stage of investigation. Each method reflects an actual functional component of the implemented system.Evidence Upload and Case Association Method

In the developed system, digital crime evidence is uploaded through a web-based interface built using the Django framework. Evidence submission is restricted to authorized users who log in using valid credentials. During upload, each evidence file is explicitly linked to a specific case identifier and stored along with descriptive information such as case details and submission time.This method ensures that evidence is logically organized and traceable within the system. By associating every file with a case reference at the time of upload, the system prevents ambiguity regarding evidence origin and context. This approach mirrors real investigative workflows, where evidence must always be linked to a registered case.

4.1 Evidence Hash Creation Method

After successful upload, the system generates a cryptographic hash of the evidence file within the application layer. This hash represents the exact state of the evidence at the moment of submission. The original evidence file remains unchanged after hashing, ensuring that the hash accurately reflects the uploaded content. The generated hash is treated as the primary integrity reference for the evidence. Any future verification process relies on this hash rather than subjective inspection. This method allows the system to mathematically prove whether the evidence has been altered, which is critical for forensic validation.

4.2 Blockchain Recording Using Ethereum Smart Contract

The project uses an Ethereum smart contract to permanently record evidence-related information. Instead of storing the actual evidence file on the blockchain, only the hash value and minimal metadata are recorded. This decision was made to reduce blockchain storage costs and improve system performance.

Interaction with the smart contract is handled through the Web3 library, allowing the Django application to submit evidence records as blockchain transactions. Once a record is stored, it becomes immutable and cannot be modified by any user, including system administrators. This method ensures long-term protection of evidence records.

4.3 Authorized Evidence Access Method

Access to evidence records within the system is controlled based on user roles defined in the application. Only authorized users are permitted to view evidence details or perform verification operations. This access control mechanism ensures that sensitive evidence data is not exposed to unauthorized parties.

All access actions are logged internally, allowing investigators to trace who accessed evidence and when. This method supports accountability and aligns with legal requirements related to evidence handling and chain of custody.

4.4 Evidence Integrity Verification Method

When evidence verification is required, the system recalculates the cryptographic hash of the original evidence file and compares it with the hash stored on the blockchain. This comparison is performed using the same hashing logic used during initial upload.

If both hash values match, the system confirms that the evidence has not been altered since registration. If a mismatch is detected, the evidence is flagged as potentially compromised. This verification process provides a reliable and objective method for validating evidence integrity during investigations or court proceedings.

4.5 Blockchain Transaction Reference Method

For every evidence registration, the Ethereum blockchain generates a unique transaction hash and block reference. These values are stored and displayed within the application for audit purposes. Investigators can use these references to independently verify the existence of evidence records on the blockchain.

This method strengthens the chain of custody by providing a permanent blockchain-based timestamp and proof of registration. It also enables third parties to validate evidence authenticity without relying solely on the application database.

4.6 Combined Integrity Protection Approach

The project combines application-level security with blockchain immutability to provide comprehensive protection for crime evidence. While cryptographic hashing ensures file-level integrity, blockchain storage ensures that integrity references cannot be altered retroactively.

This layered approach reflects the actual implementation of the system and provides stronger assurance than traditional centralized methods. The combination of hashing, blockchain recording, and controlled access forms the core security model of the project.

V. RESULTS

The results are based on running the developed Django application integrated with the Ethereum blockchain using smart contracts and the Web3 interface.

Figure 3: Admin Login and Dashboard

The Admin Login screen allows authorized administrators to access the system using valid credentials. After login, the Admin Dashboard provides options to add new officers, view officer details, view crime evidences, and log out, serving as the main control panel for managing the application.

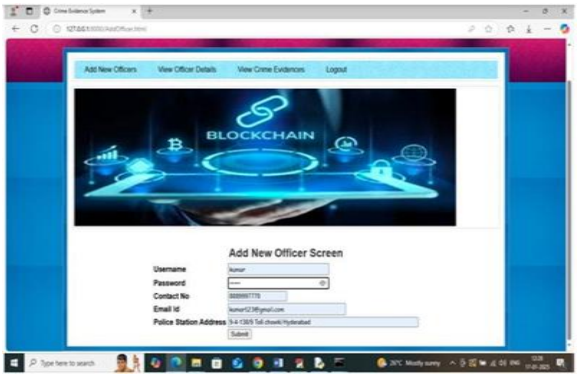

Figure 4: Add New Officer and Officer Details

The Add New Officer screen enables the administrator to register police officers by entering their basic details, while the View Officer Details screen displays the list of all registered officers in a table format. These screens support secure user management within the system.

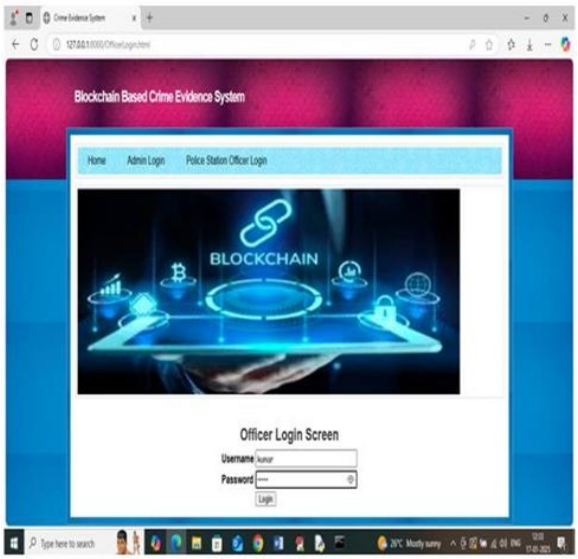

Figure 5: Officer Login and Dashboard

The Officer Login screen allows registered officers to authenticate themselves. Upon login, the Officer Dashboard provides options to add new crime evidence, access available evidence, and log out, acting as the working interface for officers.

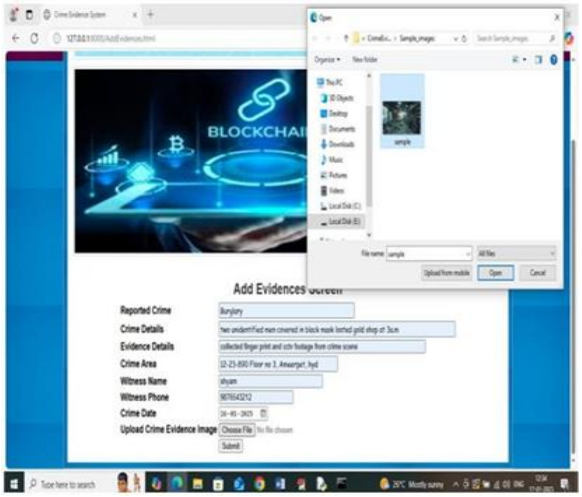

Figure 6: Add Evidence Screen

The Add Evidence screen is used by officers to enter crime and evidence details and upload evidence files. After submission, the system generates a hash and

stores the evidence details on the blockchain, ensuring secure registration.

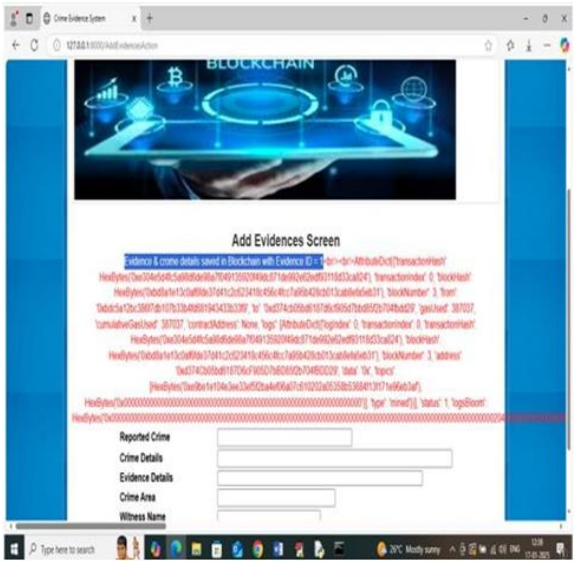

Figure 7: Blockchain Confirmation

This screen displays the evidence ID along with blockchain transaction details such as transaction hash and block number, confirming that the evidence has been successfully recorded on the blockchain.

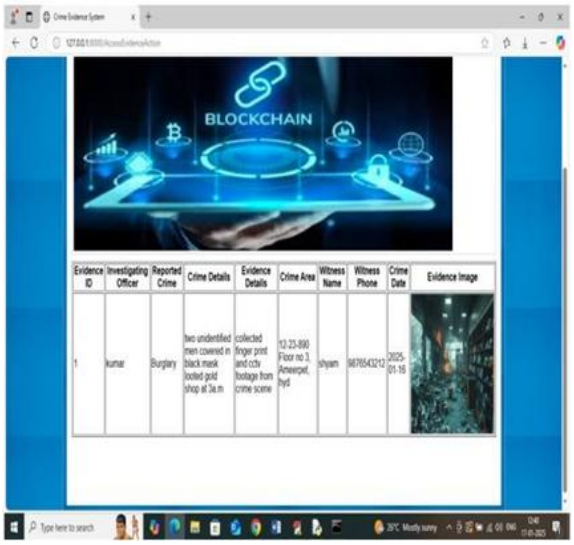

Figure 8: Access and View Evidence

The Access Evidence screen allows officers to select an evidence ID, and the Evidence Details screen displays the complete crime and evidence information along with the uploaded file. This supports secure retrieval and verification of evidence records. Together, these screens demonstrate the complete workflow of the system, from authentication and officer management to evidence upload, blockchain storage, and secure access, validating the implementation of the Blockchain Based Crime Evidence System.

5.1 System Execution and Module Testing

The application was executed on the local server, and all functional modules were tested. The administrator was able to log in and register officers, while officers could log in and access evidence-related functions. Modules such as add evidence, view evidence, and access evidence operated correctly, confirming that the system workflow described in the project was successfully implemented.

5.2 Evidence Upload and Blockchain Registration

When officers uploaded digital evidence through the web interface, the system generated a cryptographic hash and sent it to the Ethereum smart contract. For each upload, the blockchain returned a unique transaction hash and block number, which were displayed by the application. These outputs confirmed that every evidence record was successfully written to the blockchain.

5.3 Evidence Integrity Verification

During verification, the system recalculated the hash of the stored evidence file and compared it with the hash value retrieved from the blockchain. If the evidence file remained unchanged, both hash values matched and the system confirmed the record as valid. When modifications were made to the file, a mismatch was observed, and the system identified the evidence as altered. This demonstrated the effectiveness of the hashing and verification mechanism.

5.4 Immutability of Stored Records

Once evidence details were stored on the blockchain, attempts to modify or delete them through the application were not permitted. Previously recorded blockchain entries remained unchanged during repeated access. This result confirmed the immutability of evidence records enforced by the smart contract.

5.5 Role-Based Access Control

The system was tested with different user roles. Administrators could manage officer accounts, while officers were allowed to upload and view evidence.

Unauthorized users were restricted from accessing system functions. This showed that the role-based access mechanism worked as intended and protected sensitive evidence data.

5.6 Traceability Using Blockchain Transactions

For every evidence entry, the system displayed blockchain transaction information such as transaction hash and block number. These values were used to trace when and where the evidence was recorded on the blockchain. This feature provided a clear audit trail and supported the chain of custody requirement described in the project.

VI. CONCLUSION

The work carried out in this project explored the use of blockchain as a supporting technology for handling digital crime evidence. Instead of depending on conventional databases, the system was built to rely on blockchain records to confirm whether evidence details remain unchanged after submission. Through the developed application, evidence files were processed to obtain hash values, which were then written to the Ethereum network using a smart contract. Once this step was completed, the system treated the blockchain entry as the reference point for that evidence. During verification, the same process was repeated to check if the evidence still matched its original state. The behavior observed during execution showed that the system could clearly distinguish between original and altered files. It was also seen that stored blockchain entries remained stable and could not be modified through the application. User roles were enforced so that only permitted users could interact with sensitive functions. Based on these observations, the project demonstrates that blockchain can be used as a practical tool to improve confidence in digital evidence handling. The implementation does not replace existing forensic practices but adds a secure layer that strengthens trust in stored evidence. The system can be extended further to support additional features and broader usage scenarios.

REFERENCES

[1] Nakamoto,S.(2008)
[2] Bitcoin: A Peer-to-Peer Electronic Cash System This is the original whitepaper that introduced blockchain technology and its decentralized, tamper-proof architecture.Link
[3] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018)
[4] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends In 2017 IEEE International Congress on Big Data (BigData Congress) DOI: 10.1109/BigDataCongress.2017.85