IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

Blockchain-Based Evidence Management System

Mr. Amar More[1], Mr . Karan More[2], Mr . Nikhil Neavse[3], Mr. Prasanna Deokar[4]
Prof. T Arivanantham[5], Santosh Kawade[6]
Students, Department of Computer Science and Engineering[1-4]
Project Guide, Department of Computer Science and Engineering[5]
Co-Guide, Department of Computer Science and Engineering[6]
Dr D Y Patil College of Engineering and Innovation, Talegaon, Varale, Pune, India

Abstract: *This project introduces a decentralized file storage system that leverages blockchain technology to create a secure, immutable, and tamper-resistant platform for file sharing. By storing files within blocks on a blockchain, the system ensures that once data is uploaded, it cannot be altered or deleted, making it ideal for applications where data integrity is critical. Users interact with the platform through a web interface, allowing them to upload, download, and share files across a peer-to-peer network. The blockchain structure used in this project employs a Proof of Work (PoW) consensus mechanism, requiring peers (miners) to solve cryptographic puzzles to validate blocks and add them to the chain. Two different PoW methods are used: one generates nonces at random, while the other increases the nonce value one after the other. By comparing the effectiveness and security of different methods, the project finds that random nonce generation outperforms them at higher difficulty levels, providing quicker block validation and more robust defense against possible assaults. On the other hand, the incremental approach is less secure over time because it is simpler to foresee. The project also covers the advantages of on-chain storage, which involves storing files directly inside blockchain blocks. This approach offers better security but comes at the expense of more processing power. Furthermore, it investigates alternatives such as off-chain blockchain architectures for more effective file storage in subsequent iterations and Proof of Stake (PoS) for lowering resource use.*

Keywords: Peer-to-peer network, On-chain storage, Cryptographic puzzle, Proof of Stake (PoS), Off-chain storage, Block validation, Blockchain technology.

I. INTRODUCTION

The blockchain structure, which is central to this application, is necessary to guarantee the confidentiality and integrity of data that is stored. In essence, a blockchain is a linked list with crucial components like timestamps, cryptographic hashes, and transaction data in every block. By connecting each block to its predecessor, these hashes make sure that any modifications made to one block render the chain as a whole invalid. This structure is defined by the Block.py file for this project, which also handles block formation and SHA-256 cryptographic hash computation. The system ensures immutability by making sure that every block contains the hash of the one before it; if a block were altered, the chain would be broken. Because of its design, it is nearly hard to alter the data on the blockchain without erasing each new block.

Any type of transaction data, including digital assets and financial records, can be safely stored on the blockchain. After blocks are added to the chain, they cannot be removed thanks to the use of cryptographic hashing. While the chain's integrity is preserved by the hash of the previous block, each block's timestamp establishes chronological order. This block linkage makes it extremely difficult for a bad actor to tamper with the blockchain since if they try to change one block, they would have to change all subsequent blocks as well. The core of the blockchain's credibility is its immutability and security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

Peer-to-Peer Network

Peer-to-peer (P2P) networking, which permits decentralized communication between nodes, is a fundamental component of this project. Each node in a P2P network can function as both a client and a server, in contrast to traditional systems where all the data is stored on a central server. Because there isn't a single point of failure, this decentralized strategy makes the network more robust and difficult to attack. The project's peer.py file controls this communication, making sure that every other node is informed when one contributes a block or transaction. Before adding the updated information to their local copy of the blockchain, they must first confirm it. This ensures that every node keeps an updated, synced copy of the blockchain.

One of the main advantages of blockchain technology is that it does not require a central authority, which is made possible by its peer-to-peer structure. It makes it practically difficult for any one node to control the system by guaranteeing that every node in the network has equal power. Nodes can rejoin and resynchronize if they momentarily disconnect, which further strengthens the blockchain's resilience to errors. Peer communication guarantees network data consistency, establishing a trustless system that allows users to communicate without the requirement for PoW, or proof-of- work

A Proof-of-Work (PoW) consensus technique is used in this project to guarantee the network's security and equity. Before nodes (or miners) may add new blocks to the chain, they must solve challenging cryptographic challenges. The node that completes the puzzle first receives a reward for their efforts and gets to add the next block. This procedure prevents bad actors from simply flooding the network by making the addition of additional blocks computationally costly. In order to determine which PoW algorithm could be appropriate for a given use case, the POW_Comparison.py file evaluates various algorithms based on their security, energy consumption, and efficiency.

In order to stop fraudulent behaviors like double-spending and changing the blockchain's history, the PoW mechanism is essential. PoW makes guarantee that only authorized users may add new blocks to the chain by demanding a significant amount of processing power to do so. The file investigates how block formation times can be controlled by varying the puzzle's difficulty, even while the network's processing capacity increases. Since it would take a tremendous amount of processing power to deliberately alter the chain, this procedure guarantees blockchain security and ensures fairness in block creation.

Web Interface and Application

The concept incorporates a web-based interface that enables real-time user interaction with the blockchain system in order to make it accessible. This web application's primary entry point is the run_app.py file, which starts a server that houses the interface. Users can test file upload capabilities, submit new transactions, and examine the blockchain through the interface. A user-friendly experience is produced by the static files, which are kept in the static/ subdirectory and include HTML, CSS, and JavaScript. Without requiring in-depth technical understanding, users can engage with the blockchain with ease, reading its contents or adding new blocks.

Users can also upload files through the web interface, and the blockchain records and verifies them. This demonstrates how blockchain technology may be used practically, especially in digital asset management. Users can upload and save files, including legal documents or certifications, so they can later confirm their legitimacy. This project component shows how blockchain technology may be used to create safe, unchangeable records in practical situations. The system is useful for developers and instructive for individuals learning about decentralized technologies because of the interface, which makes it simple to explore with blockchain capabilities.

II. RELATED RESEARCH

Significant progress has been made in a number of important areas according to research on blockchain-based evidence management systems. Blockchain's decentralized structure improves security and credibility by guaranteeing that evidence is unchangeable and impervious to manipulation. Its use in law enforcement, especially in preserving an unbroken and transparent chain of custody for both digital and physical evidence, is highlighted in numerous studies. Since smart contracts can automate a number of evidence handling procedures, including submissions and approvals, their integration is also investigated. Interoperability with current systems and striking a balance between data

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

protection and transparency are still issues, though, and methods like zero- knowledge proofs are being researched to safeguard sensitive data. Pilot project case studies offer valuable insights into implementation challenges as well as triumphs. Legal ramifications, such as the admissibility of evidence kept on blockchain in court and adherence to data protection regulations, are important subjects of conversation. Along with addressing adoption constraints within law enforcement agencies, such as technological difficulties and the requirement for training, study also assesses the financial advantages of implementing blockchain in comparison to conventional approaches. All things considered, the research highlights an increasing interest in applying blockchain technology to improve evidence management, with an emphasis on enhancing law enforcement procedures' efficiency, security, and transparency.

Blockchain Technology Fundamentals

Decentralization: Research shows that blockchain's decentralized structure improves evidence management's security and credibility.

Immutability: Studies highlight how crucial unchangeable records are to guarding against evidence manipulation. Applications in Law Enforcement

Use Cases in Law Enforcement

Chain of Custody A number of studies examine how blockchain technology can guarantee an uninterrupted chain of custody for both digital and tangible evidence.

Transparency and Accountability: Studies demonstrate how blockchain improves law enforcement procedures' transparency, which facilitates audits and action verification.

Interoperability and Integration

interoperability and integration looks at the problems and fixes associated with combining blockchain technology with current law enforcement databases and tools.

Smart Contracts

The use of smart contracts to automate evidence handling processes, including as submissions, approvals, and audits, is the subject of research.

Data Privacy and Security

Research examines the trade-off between data security and transparency, looking at methods like zero-knowledge proofs to safeguard private data while preserving its integrity.

Case Studies and Pilot Projects

Numerous case studies explain the achievements, difficulties, and lessons learned from pilot projects that used blockchain technology for evidence management.

Legal and Regulatory Implications

Studies look into the legal ramifications of employing blockchain technology for evidence management, such as data privacy regulations and admissibility in court.

Cost-Benefit Analysis

Research compares the financial effects of implementing blockchain technology to more conventional evidence management methods, frequently emphasizing possible long- term savings.

User Acceptance and Implementation Challenges

Studies on the cultural, technological, and training obstacles that law enforcement organizations face while adopting new practices.

Future Trends

Studies make predictions about how blockchain will be used in evidence management in the future, including how it will integrate with other cutting-edge technologies like AI and the Internet of Things.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

III. METHODOLOGY

i. Problem Definition

- Determine the shortcomings of the current evidence management systems, including problems with the chain of custody, data manipulation, and a lack of transparency.

ii. System Requirements Gathering

- Stakeholder Interviews: To get requirements, consult with law enforcement, attorneys, and IT specialists.
- Regulatory Compliance: Examine legal requirements for the handling of evidence (such as the GDPR and criminal justice laws).
- Use Case Scenarios Create use cases to comprehend the gathering, storing, and retrieval of evidence.

iii. System Design

- Blockchain Selection: Based on consensus methods and scalability, pick a blockchain framework (such as Ethereum or Hyperledger).
- Smart Contract Development: Create smart contracts to automate procedures related to handling evidence, such as audit trails, retrieval, and submission.
- User Interface Design: Wireframes for user interfaces should be created with an emphasis on usability for various stakeholders, such as officers and legal staff.
- Data Structure Design: Specify the metadata, timestamps, and cryptographic hashes that will be used to hold evidence data on the blockchain.

iv. Monitoring and Maintenance

- Performance Monitoring: Use monitoring tools to keep tabs on transaction throughput and system performance.
- Updates and Improvements Update the system frequently to fix bugs and take user input into account.

v. Documentation and Training

- User Documentation: Provide thorough instructions outlining system capabilities to end users..
- Training Sessions: To guarantee that the system is used correctly, provide stakeholders with training.
- vi. Evaluation and Feedback
- Performance Metrics: Establish and evaluate success criteria, such as decreased evidence tampering and faster retrieval times.
- Continuous Improvement: Create a feedback loop to collect user comments and enhance system functionality over time.

vi. Implementation

- Development Environment Setup: Configure development tools (such as Truffle and Ganache) and blockchain nodes.
- Smart Contract Development: Use smart contracts to register, edit, and retrieve evidence.
- Frontend Development: Create a user interface for an online or mobile application by utilizing frameworks such as Angular or React.

vii. Integration

- Interfacing with Existing Systems: Create APIs to interface with databases, law enforcement instruments, and evidence management systems that are already in place.
- Identity Management: Put in place methods for users to verify their identities when they access the system, such as digital signatures.

viii. Testing

- Unit Testing: Verify the accuracy of each smart contract function separately.
- Integration Testing: Verify that every system component functions as a whole.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

ix. Deployment

- Network Deployment: Depending on the requirements for scalability and security, implement the blockchain on a public or private network.
- Application Deployment: Start the front-end program on cloud servers (like AWS or Azure).

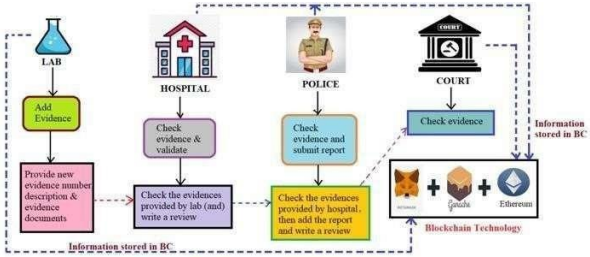
IV. ARCHITECTURE

System Components

Client Interface: A web-based or mobile application that allows users to interact with the system.
Application Server: Backend service that manages client- chain communications and business logic.
Blockchain Network: A distributed ledger system that safely saves metadata and transaction records.
Storage Layer: Large evidence files (such as pictures or movies) with connections to their blockchain entries are stored off-chain.
Identity Management System: User identities, responsibilities, and access rights are managed by the identity management system.
Analytics Module: Offers reporting features and insights derived from evidence management data.
Component Descriptions Client Interface
Offers an easy-to-use interface for submitting, retrieving, and managing evidence.
includes search capabilities, audit trails, evidence uploading, and login.
Application Server serves as a mediator between the blockchain and the client interface.
manages business logic, including blockchain transaction orchestration, session management, and user input validation.

Blockchain Network

The blockchain network houses the smart contracts in charge of overseeing the submission, alteration, and retrieval of evidence.
uses a consensus technique (such as Practical Byzantine Fault Tolerance or Proof of Authority) to guarantee the immutability and integrity of evidence records.
Storage Layer
Keeps connections to the blockchain while storing huge evidence files off-chain to preserve efficiency. Decentralized storage options like IPFS and cloud storage options like AWS S3 are available.
Identity Management System
Provides safe access control by managing user identities, roles, permissions.
supports authentication protocols for user verification, such as JWT and OAuth 2.0.
Analytics Module
Tools for creating reports and insights based on evidence handling are provided by the analytics module. may have dashboards to track usage data and system performance.



roadmap is shown below

Conceptualization and Proof of Concept (PoC)

A blockchain-based evidence management system's development can be broken down into phases, each of which improves functionality, usability, security, and compliance by building on the one before it. A suggested evolutionary roadmap is shown below:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

Basic System Development

Create a useful client interface for uploading and retrieving evidence.

Use smart contracts to manage lifecycles. Off- chain storage for big files should be introduced.

Enhancements and Feature Expansion

Include audit trails, user roles, and permissions. Improve analytics to provide in-depth reports. Use advanced identity management to increase security.

Integration with Existing Systems

Create APIs to enable older system interoperability. Test to guarantee data integrity and consistency.

Pilot Deployment and Testing

Test in real-world settings in specific areas. Iteratively update after gathering user feedback.

Full Deployment and User Training

Introduce the system to all parties involved. Offer thorough instruction and continuing assistance.

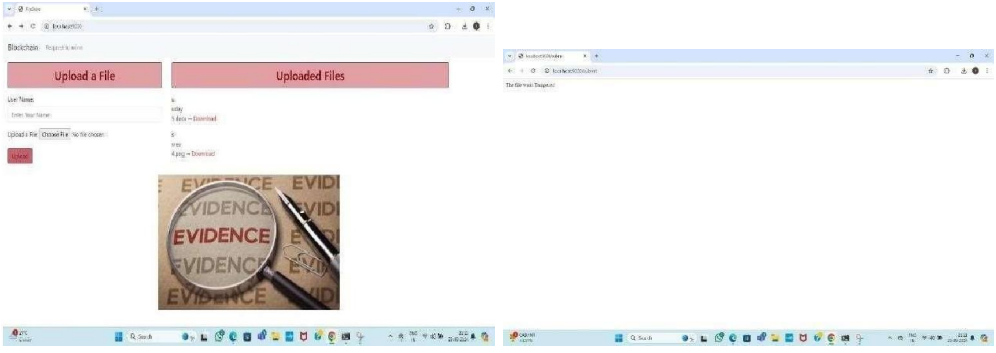
Continuous Improvement and Evolution

Create a feedback loop for suggestions from users. Update frequently to reflect emerging technologies and legal needs. Add features like AI and predictive analytics to increase capabilities.

V. RESULT

The development of the blockchain-based evidence management system produced revolutionary advancements in a number of areas. The system's viability was first confirmed via a successful proof of concept (PoC), which involved stakeholders in identifying important user requirements and traditional evidence management pain points. The following creation of a fully working system with an intuitive user interface that allowed law enforcement and legal experts to effectively upload, retrieve, and manage evidence was guided by this fundamental step. Off-chain storage solutions efficiently managed big files, improving system efficiency, while the use of smart contracts streamlined the evidence lifecycle, guaranteeing transparency and lowering human error.

The implementation of strong identity management features greatly increased the user experience by enabling customized access through user roles and permissions that improved security. In order to help stakeholders make well-informed decisions, the analytics module gave them strong tools for producing comprehensive reports and insights. increased data flow and consistency were made possible by a smooth interaction with the law enforcement systems already in place, which promoted increased agency coordination. User satisfaction was highlighted by positive feedback from pilot deployments, which led to iterative modifications that improved the usability and functionality of the system. With the help of thorough training sessions that gave users the skills they needed to efficiently utilize the system, the system was successfully accepted by several agencies when it was fully deployed. Crucially, an organized feedback loop was created, allowing for ongoing enhancements based on actual use and changing requirements. Frequent updates made sure the system stayed up to date with new developments in technology and compliance standards, like laws governing data privacy. All things considered, this development produced a safe, effective, and intuitive evidence management system that not only solved current issues but also set itself up for future developments in the ever-changing field of law enforcement and legal operations.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

VI. CONCLUSION

The initiative to develop a blockchain-based evidence management system effectively illustrated how blockchain technology may be used to improve the security, integrity, and transparency of evidence management procedures. The solution tackles major issues with conventional evidence management, like tampering, loss, and illegal access, by leveraging the immutable ledger and decentralized features of blockchain technology.

We put in place a safe and dependable system that guarantees evidence is documented and validated in a way that cannot be altered during the project. In addition to enhancing confidence in the evidence management process, the system's capacity to offer an unambiguous, auditable record of evidence handling and transfer expedites adherence to legal and regulatory obligations.

Blockchain may be successfully incorporated into evidence management processes, providing real-time visibility and responsibility, as demonstrated by our installation. This can boost the overall effectiveness of the evidence lifecycle and drastically lower the chance of evidence being handled improperly.

In the future, there will be numerous chances for additional growth. The system's capabilities could be further increased by integrating cutting-edge technologies like smart contracts and expanding it to support interoperability with other blockchain platforms. As the technology is used more widely, it will also be essential to solve performance and scalability issues.

In summary, the blockchain-based evidence management system offers a strong foundation for upcoming developments in this crucial field and constitutes a substantial advancement in the security and management of evidence.

REFERENCES

[1] A. M. Noor and N. A. Samsudin, "File integrity checking methods in ensuring the integrity of digital forensic evidence," Journal of Forensic Sciences, 2018.

[2] D. Tapas, A. Yadav, and A. Narayan, "Blockchain-Based System for Secure File Sharing," Journal of Computer Networks and Communications, 2019.

[3] W. Zhang, L. Liu, J. Zhang, and X. Luo, "Blockchain-based proof of ownership model for cloud file storage," Future Generation Computer Systems, vol. 96, pp. 540-550, 2019.

[4] S. Nakamoto, "Blockchain for Decentralized File Storage," IEEE Communications Magazine, vol. 55, no. 12, pp. 78-83, 2017.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[6] J. Xie, F. R. Dai, and A. F. Wu, "A survey on consensus mechanisms in blockchain technology," IEEE Access, vol. 7, pp. 55479-55487, 2019.

[7] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Ensuring Data Integrity in Cloud Storage," Proceedings of the 17th ACM Conference on Computer and Communications Security, 2010.

[8] P. Hayati, R. Qureshi, A. Sadeghi, "A framework for file integrity checking in distributed environments," International Journal of Distributed Systems and Technologies, vol. 5, no. 2, pp. 14-24, 2014.

[9] M. Barni, F. Bartolini, "A survey of digital watermarking techniques for tamper detection," IEEE Transactions on Signal Processing,2