CVR COLLEGE OF ENGINEERING

Department of CSE(Cyber Security)
B.Tech CSE(CS) IV Year I Semester

Project Stage-1
Review-2
Date: 15.10.2025

CVR COLLEGE OF ENGINEERING

CUSTAIN:Evidence Management Using BlockChain Technologhy

TEAM MEMBERS

N.Divya Sree 22B81A6209

K.Ruthika 22B81A6239

B.Veekshana 22B81A6257

Under the guidance of

Mr.K.Praskasha Chary

Assistant Professor

Domain Introduction

- **Domain:** Cybersecurity
- **Introduction:** Cybersecurity is the field dedicated to protecting computer systems, networks, and digital information from unauthorized access, attacks, or damage. Its roots trace back to the 1970s with the rise of computer networking, but it has become critical in today's era of cloud computing, IoT, and digital transactions. As cyber threats grow more advanced, cybersecurity now integrates emerging technologies such as AI, Blockchain, and Machine Learning to build robust and resilient systems.

Key concepts & Technologies

➢**Key Concepts:**

- Confidentiality, Integrity, and Availability (CIA Triad)
- Authentication and Authorization
- Encyption and Cryptography
- Network Security and Incident Response

➢**Technologies:**

- Firewalls, Intrusion Detection Systems (IDS), and SIEM tools
- Blockchain for tamper-proof data storage
- AI/ML for threat detection
- Public Key Infrastructure (PKI)

Applications & Advancements

➢**Applications:**

- Secure communication and data protection
- Intrusion and malware detection
- Identity and access management
- Evidence Management Systems ensuring integrity and traceability of digital evidence

➢**Recent Advancements and Trends:**

- Use of Blockchain for data integrity and digital forensics
- Zero Trust Architecture in enterprise security
- AI-driven threat intelligence systems
- Quantum-resistant encryption algorithms
- Increased focus on cyber resilience and incident response automation

Significance

- Cybersecurity is essential for protecting individuals, businesses, and governments from cyber threats and ensuring trust in the digital ecosystem. In fields like law enforcement and digital evidence management, it guarantees data authenticity, confidentiality, and accountability. By leveraging blockchain, cybersecurity systems can create immutable records, preventing manipulation and strengthening legal trust — a crucial step toward a safer digital society.

Literature Review

Paper Title 1: Blockchain Technology in Forensic Evidence Management

Authors & Publication: Mettu Sravani, Pulime Satyanarayana, P. Senthil Kumar, R. Dinesh Kumar, 2025, Lecture Notes in Networks and Systems (Springer), ICAISE 2024

URL: https://link.springer.com/chapter/10.1007/978-3-031-90921-4_77

Contribution: Addresses the challenge of tamper-proof forensic evidence storage and proposes a blockchain-based solution to maintain integrity and chain of custody.

Methodology: Utilizes Hyperledger Fabric as a permissioned blockchain framework. Implements smart contracts for access control and hashing for evidence verification. The system architecture includes peer nodes, ordering services, and certificate authorities to ensure secure transactions.

Limitations: The paper lacks real-world deployment scenarios and performance benchmarking under high transaction loads. It does not address interoperability with existing forensic tools or scalability for large evidence datasets.

Literature Review

Paper Title 2: Decentralized Evidence Management using Blockchain for Digital Forensics

Authors & Publication: Nelli Sreevidya et al., 2025, Grenze International Journal of Engineering and Technology

URL: https://thegrenze.com/pages/servej.php?fn=156_22.pdf

Contribution: Proposes a decentralized Blockchain-based Evidence Management System (BEMS) to ensure integrity and confidentiality of digital forensic evidence.

Methodology: Implements a permissioned blockchain with cryptographic hashing and Zero-Knowledge Proofs for privacy. Smart contracts automate evidence registration and verification. Performance evaluation includes latency and throughput tests under simulated forensic workflows.

Limitations: Scalability remains a concern for large multimedia evidence. Off-chain storage integration is not optimized, and the system lacks compliance validation against forensic standards like ISO 27037.

Literature Review

Paper Title 3: The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review

Authors & Publication: Oshoke Samson Igonor et al., 2025, Blockchains Journal, MDPI

URL: https://www.mdpi.com/2813-5288/3/1/5

Contribution: Provides a comprehensive review of blockchain applications in digital forensics, identifying gaps and future research directions.

Methodology: Conducts a systematic literature review of blockchain-based forensic frameworks, categorizing them by architecture, consensus mechanism, and security features.

Limitations: The paper is purely theoretical and lacks experimental validation. It does not propose a unified framework or address practical deployment challenges.

Literature Review

Paper Title 4: Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions

Authors & Publication: Hany F. Atlam et al., 2024, Electronics, MDPI

URL: https://www.mdpi.com/2079-9292/13/17/3568

Contribution: Reviews blockchain-based forensic techniques and highlights legal and technical challenges in evidence management.

Methodology: Analyzes 46 selected articles using PRISMA guidelines. Identifies blockchain integration models for forensic workflows and evaluates their security and performance aspects.

Limitations: Does not provide implementation details or performance benchmarks. Legal compliance and privacy-preserving mechanisms are discussed but not practically validated.

Literature Review

Paper Title 5: Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review

Authors & Publication: Danielle Batista et al., 2023, Journal of Risk and Financial Management, MDPI

URL: https://www.mdpi.com/1911-8074/16/8/360

Contribution: Examines blockchain's role in maintaining chain of custody for physical evidence in forensic investigations.

Methodology: Reviews 26 resources and evaluates blockchain-based custody control mechanisms. Discusses smart contract-based automation for custody tracking.

Limitations: Focused primarily on physical evidence; lacks technical depth for digital evidence handling. No prototype or performance evaluation provided.

Literature Review

Paper Title 6: Two-Level Blockchain System for Digital Crime Evidence Management

Authors & Publication: Donghyo Kim et al., 2021, Sensors, MDPI

URL: https://www.mdpi.com/1424-8220/21/9/3051

Contribution: Introduces a two-level blockchain system separating hot and cold data for efficient evidence storage.

Methodology: Implements dual blockchain architecture—one for frequently accessed evidence and another for archival storage. Evaluates performance for video evidence handling under simulated crime scenarios.

Limitations: High complexity in managing two blockchains. Scalability and cost implications for large datasets remain unresolved.

Literature Review

Paper Title 7: Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric

Authors & Publication: Junho Jeong et al., 2020, Journal of Information Processing Systems

URL: https://pure.dongguk.edu/en/publications/design-and-implementation-of-a-digital-evidence-management-model-

Contribution: Proposes a Hyperledger Fabric-based model for secure digital forensic evidence handling.

Methodology: Implements distributed access control and smart contracts for evidence lifecycle management. Tested in a controlled environment with simulated forensic cases.

Limitations: Limited scalability and lack of integration with law enforcement systems. Does not address privacy-preserving mechanisms for sensitive evidence.

Literature Review

Paper Title 8: B-CoC: A Blockchain-Based Chain of Custody for Evidence Management in Digital Forensics

Authors & Publication: Silvia Bonomi et al., 2019, OASIcs Tokenomics Conference Proceedings

URL: https://drops.dagstuhl.de/storage/01oasics/oasics-vol071-tokenomics2019/OASIcs.Tokenomics.2019.12/OASIcs.Tokenomics.2019.12.pdf

Contribution: Introduces B-CoC framework for automating chain of custody using Ethereum blockchain.

Methodology: Develops a prototype on Ethereum with smart contracts for custody tracking. Evaluates transaction speed and integrity under controlled conditions.

Limitations: High transaction costs and lack of privacy-preserving mechanisms. Ethereum's public nature raises confidentiality concerns.

Literature Review

Paper Title 9: Blockchain-Based Chain of Custody Models for Tamper-Proof Evidence Preservation in Digital Forensics

Authors & Publication: Elvis Nnaemeka Chukwuani et al., 2019, ResearchGate

URL: https://www.researchgate.net/publication/392966602_BLOCKCHAIN-BASED_CHAIN-OF-CUSTODY_MODELS_FOR_TAMPER-PROOF_EVIDENCE_PRESERVATION_IN_DIGITAL_FORENSICS_INVESTIGATIONS

Contribution: Proposes Hyperledger Fabric-based CoC model with role-based access control and hash-based fingerprinting.

Methodology: Simulates adversarial scenarios to test robustness. Benchmarks security and performance under different network configurations.

Limitations: Limited interoperability with existing forensic tools. Scalability and compliance with legal standards remain unaddressed.

Literature Review

Paper Title 10: An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody

Authors & Publication: Irene Lavín, Diego R. Llanos, 2018, UVaDoc Repository

URL : https://uvadoc.uva.es/bitstream/handle/10324/75760/_blockchain_2025_Chain_of_custody_under_iso.pdf?sequence=1

Contribution: Reviews blockchain solutions against ISO 27037 standards for digital evidence handling.

Methodology: Provides taxonomy-based analysis of blockchain frameworks and evaluates compliance with forensic standards.

Limitations: Does not propose new solutions; focuses on comparative analysis only. No experimental validation or performance metrics included.

Challenges

1.Scalability Issues

- Difficulty handling large multimedia datasets.
- Performance degrades significantly under high transaction loads.

2.High Latency and Poor Performance

- Systems like Hyperledger Fabric and Ethereum exhibit high latency.
- Unsuitable for real-time or large-scale forensic operations.

3.Lack of Integration with Forensic Tools

- Limited or no compatibility with widely used digital forensic tools.
- Makes adoption in investigative workflows difficult.

4.Non-Compliance with Legal Standards

- Lack of adherence to standards such as ISO 27037. Affects the legal admissibility of evidence records.

Challenges

5.Limited Real-World Validation

- Most systems are tested only in theoretical models or small-scale simulations.
- Absence of performance benchmarking in real-world scenarios.

6.Privacy Concerns

- Public blockchains expose sensitive information.
- Confidentiality is difficult to ensure without advanced privacy mechanisms.

7.High Cost of Operation

- Public chains incur high transaction (gas) fees.
- Cost-prohibitive for continuous or large-scale evidence logging.

8.System Complexity

- Permissioned systems introduce significant design and maintenance overhead.
- Complex architectures hinder deployment and scalability.

Problem Statement

Traditional evidence management systems often face issues like data tampering, unauthorized access, and lack of transparency, which can compromise the integrity of digital evidence. To overcome these challenges, this project aims to develop a Blockchain-based Evidence Management System that ensures secure, immutable, and transparent handling of digital evidence, thereby strengthening trust and reliability in legal and investigative processes.

The system will maintain an immutable chain of custody for every piece of evidence and enable authorized verification and retrieval, reducing the risk of manipulation and enhancing accountability.

Existing Methodologies

➢ **Methodology 1:** Centralized Digital Evidence Systems

- Traditional systems like Axon Evidence.com and Forensic Toolkit (FTK) store evidence in centralized databases managed by authorities.
- While easy to use, they suffer from data tampering risks, limited transparency, and no immutable audit trail.

➢ **Methodology 2:** Blockchain-based Chain of Custody

- The Block4Forensic framework (IEEE, 2019) uses blockchain to record each evidence transaction, ensuring a transparent chain of custody.
- However, it faces scalability issues, integration challenges, and slow transaction speeds.

Existing Methodologies

➢**Methodology 3:**

- ForenChain (IEEE, 2020) combines IPFS for storing large files with blockchain for storing their hashes.
- It ensures integrity but struggles with data persistence, access control, and synchronization problems.

➢**Methodology 4:**

- The EvidenceChain system (Springer, 2021) uses Ethereum smart contracts to automatically verify and timestamp digital evidence.
- Its main challenges are smart contract bugs, high gas fees, and legal acceptance issues.

Existing Methodologies

➢**Methodology 5:**

- Platforms like Hyperledger Indy and Sovrin (2021) use blockchain for decentralized identity verification to control evidence access.
- Key challenges include key management, interoperability, and low user adoption.

Proposed Solution

The proposed solution is a Blockchain-based Evidence Management System that leverages the decentralized and immutable nature of blockchain technology to securely store, verify, and track digital evidence. Each piece of evidence is recorded as a unique transaction on the blockchain, ensuring transparency and preventing any unauthorized modifications.

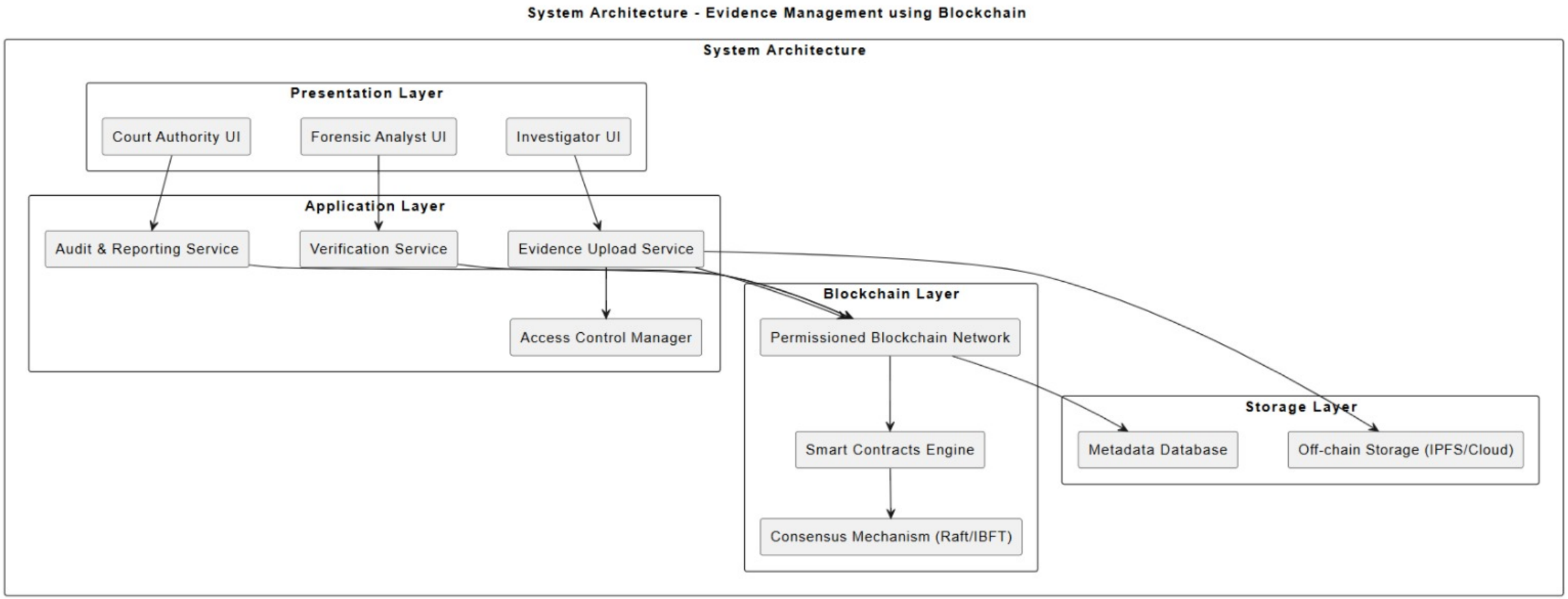
The system enables authorized users, such as police officers and investigators, to submit, verify, and access evidence through a secure interface. Smart contracts are used to automate validation and access control, ensuring that every interaction with evidence is traceable, tamper-proof, and auditable, thus strengthening the overall reliability of the judicial and law enforcement process.

Proposed Design

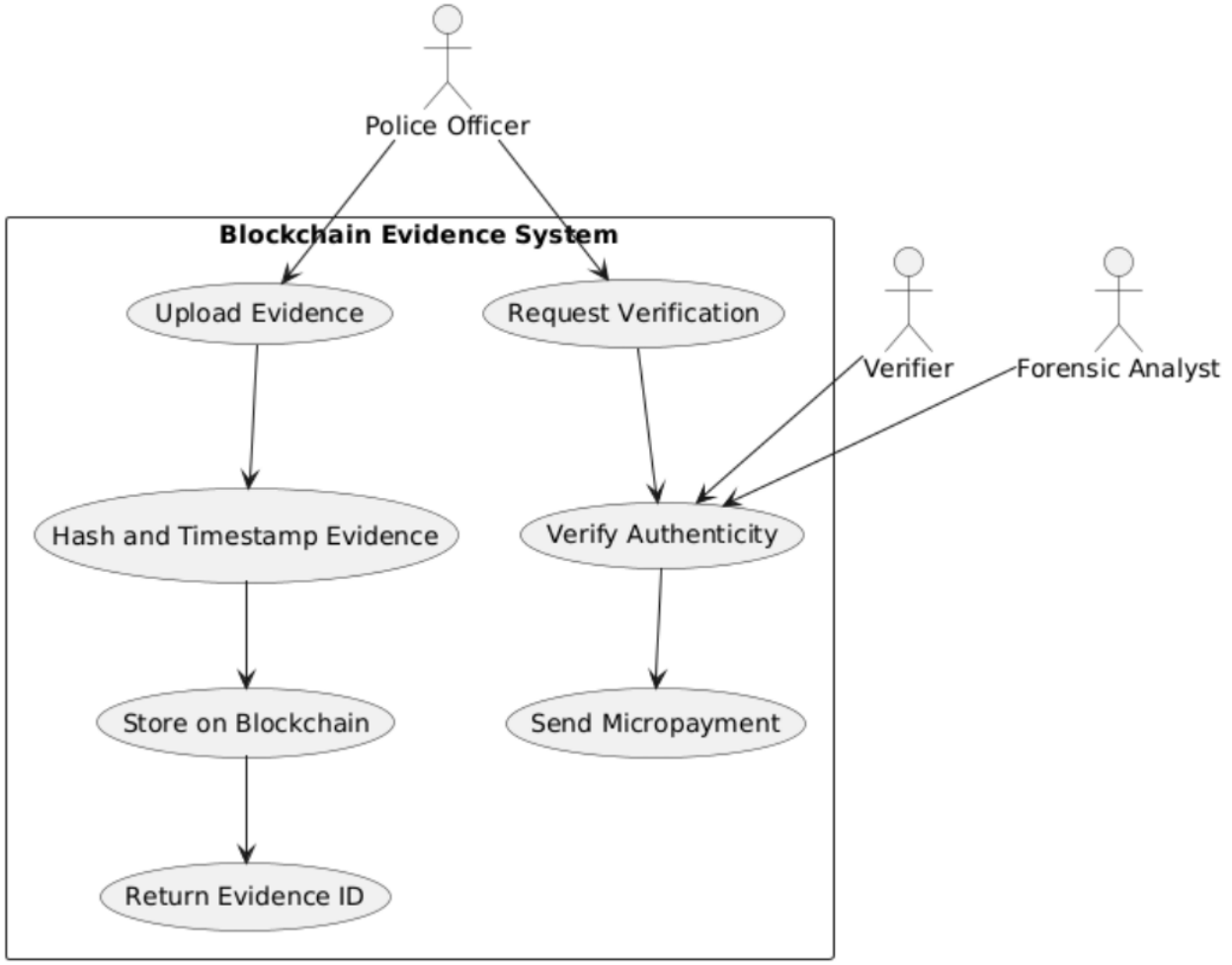
- **System Design:**

The system is designed with a three-tier architecture consisting of the user interface, application logic, and blockchain network. The frontend allows authorized users to upload, verify, and view evidence. The backend handles request processing, user authentication, and interaction with the blockchain. The blockchain layer stores evidence metadata as immutable transactions, ensuring transparency and tamper-proof records. Smart contracts manage access permissions and verification processes, ensuring secure and traceable evidence management throughout the system.

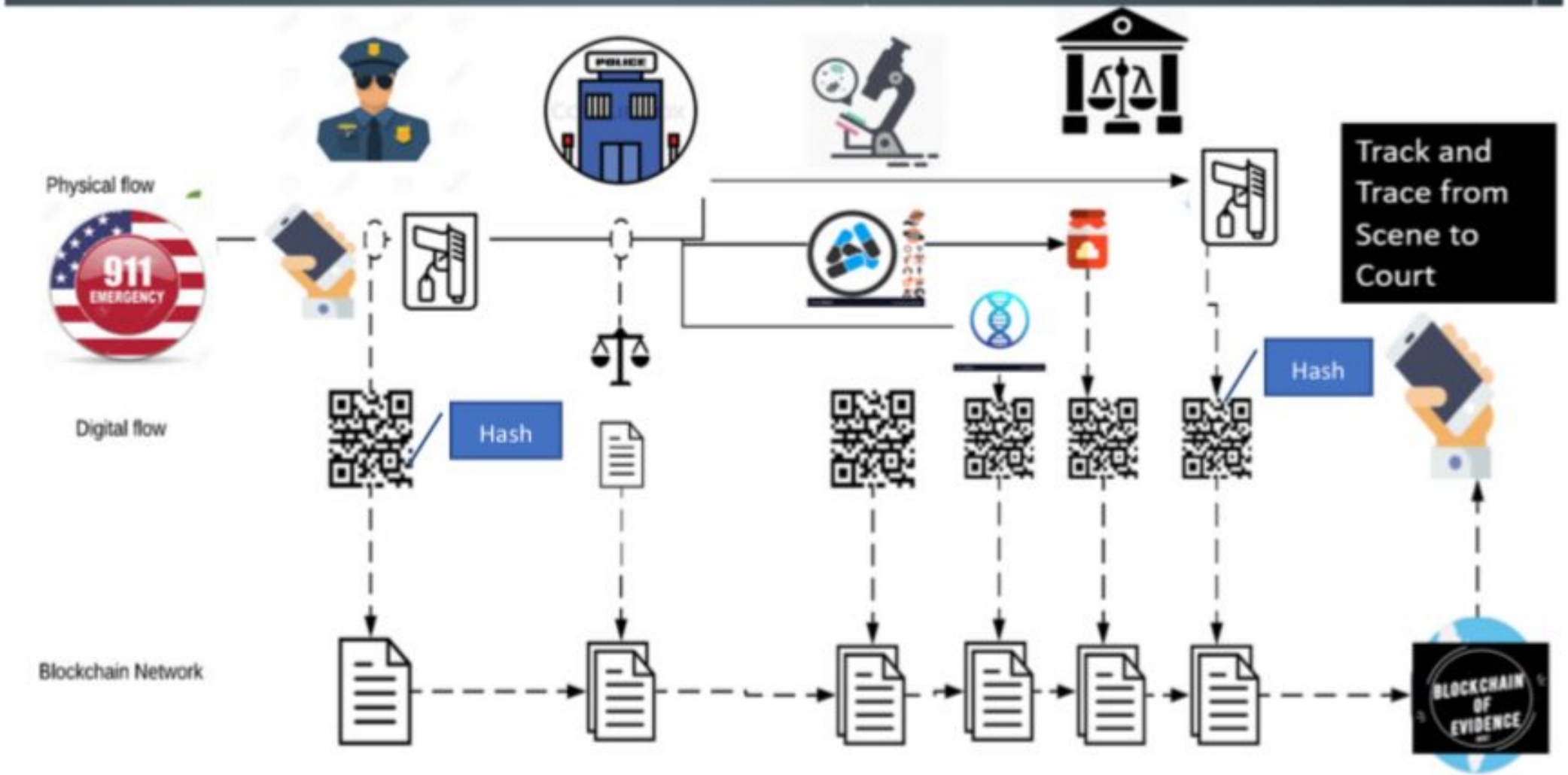
System Architecture



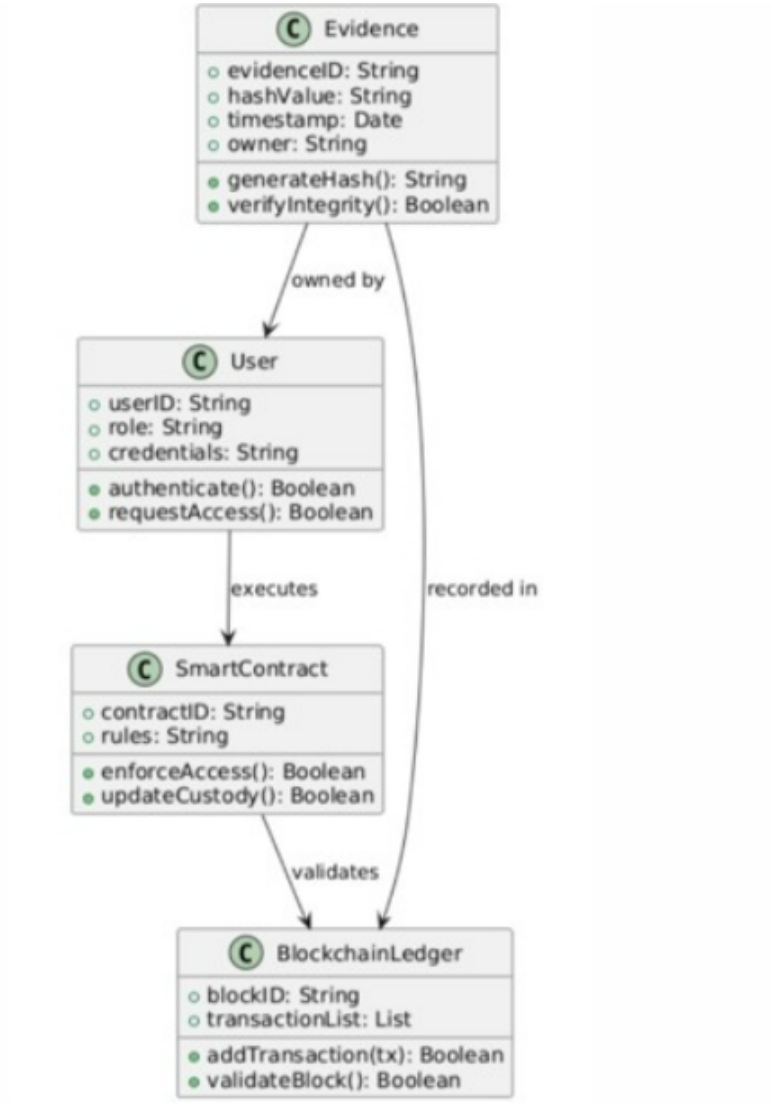
Use case Diagram



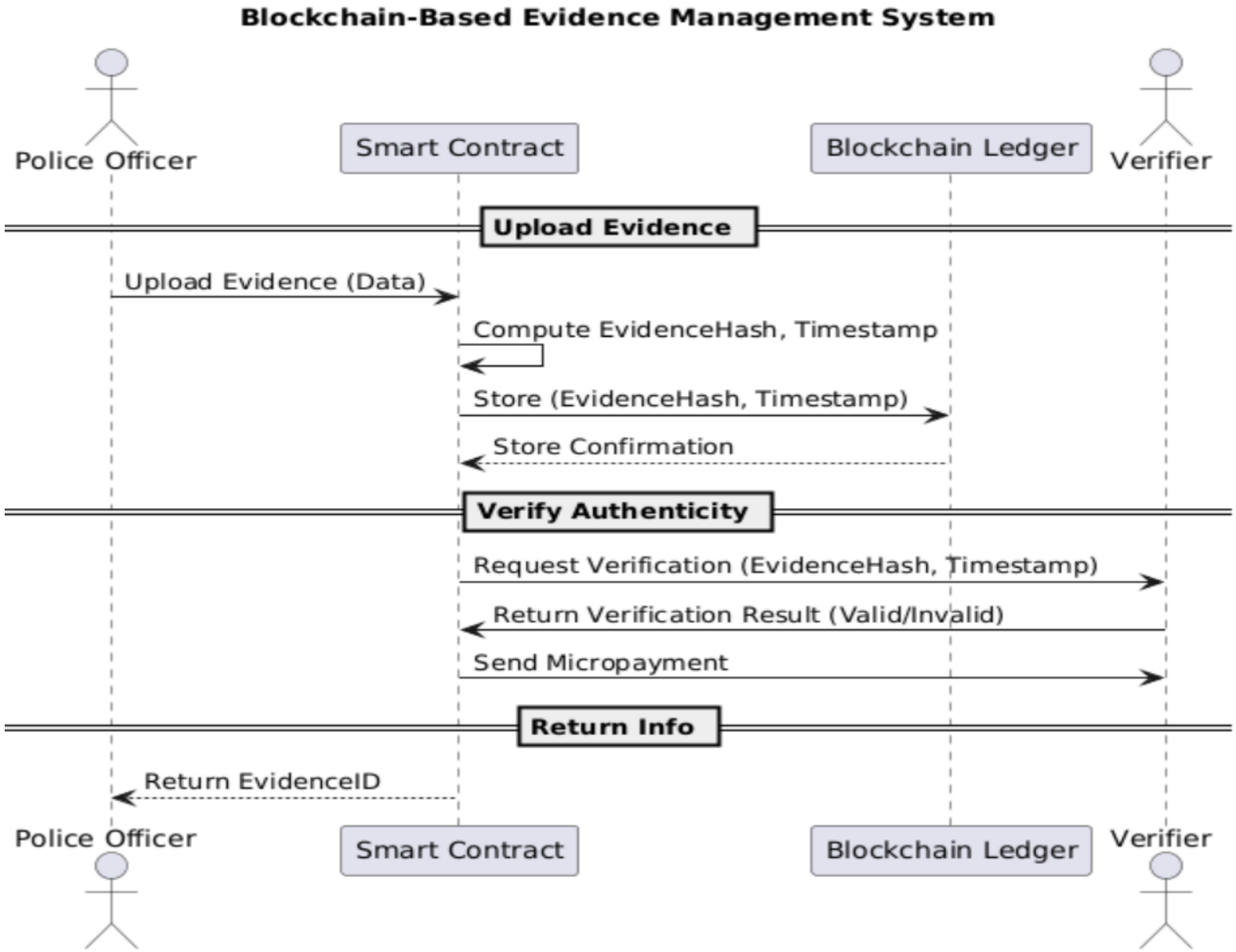
Supply Chain of Evidence



Class Diagram



Sequence Diagram



Proposed Modules

- **Module 1:** User Management Module

  Purpose: Manage roles and access rights for all participants.
- **Module 2:** Evidence Collection Module

  Purpose: Capture and register new evidence into the system.
- **Module 3:**.Blockchain Record Management Module

  Purpose: Handle all blockchain-related operations.
- **Module 4:** Evidence Verification Module

  Purpose: Ensure that evidence has not been tampered with.
- **Module 5**. Chain of Custody Module

  Purpose: Track and record every transfer or access of evidence.

Hardware and Software Requirements

- Hardware Specifications
  - CPU RAM – 16 GB
  - Processor – Core i7, 14 Gen
  - Stable Internet Connection
- Software Specifications
  - Windows OS
  - Python
  - Solidity
  - MySQL

The start date and end date can be modified according to your project

Timeline for next review

TASK ID	TASK NAME	START DATE	END DATE	DURATION in days	WEEKS													
					1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Research and Analysis	27/11	10/12	12	✓	✓	✓	✓										
2	Requirements	11/12	12/12	2	✓	✓	✓	✓										
3	Literature Review	13/12	20/12	8	✓	✓	✓	✓										
4	Documentation	26/12	28/12	3	✓	✓	✓	✓										
5	Review-1																	
6	Design																	
7	Documentation																	
8	Review-2																	

References

1. M. Sravani, P. Satyanarayana, P. Senthil Kumar and R. Dinesh Kumar, "Blockchain Technology in Forensic Evidence Management," *Lecture Notes in Networks and Systems*, ICAISE 2024, Springer, 2025, pp. xx–xx, doi:10.1007/978-3-031-90921-4_77.

2. N. Sreevidya, A. P. Divya, D. Anusha, M. Padmaja and K. Pavani, "Decentralized Evidence Management using Blockchain for Digital Forensics," *Grenze International Journal of Engineering and Technology*, 2025, pp. xx–xx.

3. O. S. Igonor, K. M. Eshiet and A. O. Adekunle, "The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review," *Blockchains*, vol. 3, no. 1, 2025, pp. xx–xx, doi:10.3390/blockchains3010005.

4. H. F. Atlam, R. J. Walters, G. B. Wills and A. Alenezi, "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions," *Electronics*, vol. 13, no. 17, 2024, pp. xx–xx, doi:10.3390/electronics13173568.

5. D. Batista, A. C. Barbosa, J. C. Dias, R. L. Moreira and D. C. Silva, "Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review," *Journal of Risk and Financial Management*, vol. 16, no. 8, 2023, pp. xx–xx, doi:10.3390/jrfm16080360.

References

6. D. Kim, D. Lee, S. Oh and S. Yoon, "Two-Level Blockchain System for Digital Crime Evidence Management," *Sensors*, vol. 21, no. 9, 2021, pp. xx–xx, doi:10.3390/s21093051.

7. J. Jeong, H. Cho, H. Jeong and Y. Kim, "Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric," *Journal of Information Processing Systems*, vol. 16, no. 5, 2020, pp. xx–xx.

8. S. Bonomi, A. Taddei and M. Conti, "B-CoC: A Blockchain-Based Chain of Custody for Evidence Management in Digital Forensics," *OASIcs Tokenomics Conference Proceedings*, vol. 71, 2019, pp. xx–xx.

9. E. N. Chukwuani, M. E. Eze, N. I. Udoh and K. C. Onoh, "Blockchain-Based Chain of Custody Models for Tamper-Proof Evidence Preservation in Digital Forensics," 2019, pp. xx–xx.

10. I. Lavín and D. R. Llanos, "An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody," *UVaDoc Repository*, 2018, pp. xx–xx.