EviChain: A Blockchain based Evidence Management System

A major project report submitted in partial fulfillment of the requirement for the award of degree of

Bachelor of Technology

in

Computer Science & Engineering

Submitted by

Abhimanyu Chauhan (211158), Purva Goyal (211320),
Saksham Angirash (211423)

Under the guidance & supervision of

Dr. Nancy Singla

Department of Computer Science & Engineering and Information Technology
Jaypee University of Information Technology, Waknaghat, Solan - 173234 (India)

May 2025

SUPERVISOR'SCERTIFICATE

This is to certify that the major project report entitled '**Evichain: A blockchain based Evidence Management System**, submitted in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science & Engineering, in the Department of Computer Science Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat, is a bonafide project work carried out under my supervision during the period from July 2024 to May 2025.

I have personally supervised the research work and confirm that it meets the standards required for submission. The project work has been conducted in accordance with ethical guidelines, and the matter embodied in the report has not been submitted elsewhere for the award of any other degree or diploma.

	Supervisor Name: Dr. Nancy Singla
Date: 09-05-25	Designation: Assistant Professor(SG)
Place: JUIT, Solan	Department: Dept. of CSE&IT

CANDIDATE’S DECLARATION

We hereby declare that the work presented in this major project report entitled **‘EviChain : A Blockchain based Evidence Management System’**, submitted in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science & Engineering**, in the Department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat, is an authentic record of our own work carried out during the period from July 2024 to May 2025 under the supervision of **Dr. Nancy Singla**.

We further declare that the matter embodied in this report has not been submitted for the award of any other degree or diploma at any other university or institution.

Name: Abhimanyu Chauhan	Name: Purva Goyal	Name: Saksham Angirash
Roll No.:211158	Roll No.:211320	Roll No.:211423
Date:09-05-25	Date: 09-05-25	Date:09-05-25

This is to certify that the above statement made by the candidates is true to the best of my knowledge.

Supervisor Name: Dr. Nancy Singla
Designation: Assistant Professor (SG)
Department: Dept. of CSE & IT

Date:09-05-25
Place: JUIT, Solan

ACKNOWLEDGEMENT

I am really grateful and wish my profound indebtedness to Supervisor **Dr. Nancy Singla, Assistant Professor(SG),** Department of CSE Jaypee University of Information Technology, Wakhnaghat. Deep Knowledge & keen interest of my supervisor in the field of "**Blockchain Development**" to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

I would like to express my heartiest gratitude to **Dr. Nancy Singla,** Department of CSE, for his kind help to finish my project.

I would also generously welcome each one of those individuals who have helped me straightforwardly or in a roundabout way in making this project a win. In this unique situation, I might want to thank the various staff individuals, both educating and non-instructing, which have developed their convenient help and facilitated my undertaking.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

Abhimanyu Chauhan (211158)

Purva Goyal (211320)

Saksham Angirash (211423)

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
AES	Advanced Encryption Standard
BERT	Bidirectional Encoder Representations from Transformers
CID	Content Identifier
CNN	Convolutional Neural Network
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
ETH	Ethereum
JMter	Java Meter (Apache JMeter)
NLP	Natural Language Processing
RNN	Recurrent Neural Network
UI	User Interface
XSS	Cross-Site Scripting
IPFS	InterPlanetary File System

ABSTRACT

Today, the major challenge is in all domains: legal, financial, and academic. The whole evidence becomes more and more digital with the passage of time. When centralized, evidence storage becomes easily manipulatable, hack-prone, and accessed by unauthorized users. EviChain is a decentralized evidence management system, enabled and powered on Ethereum, which promises to convert evidence management into a secure, transparent, and non-dupe system for retaining and validating digital evidence. All evidence stored on EviChain is decentralized by transferring the evidence storage onto a blockchain, eliminating single points of failure while significantly reducing the risks associated with data tampering. It involves information stored securely in cryptographically hashed formats and decentralized file systems such as IPFS, ensuring the permanence and verifiability of all data.

To heighten the reliability of the evidence, EviChain has integrated advanced fraud detection algorithms customized for analysis of different proof types. Example: Case of AI-validated Image and video evidence against manipulated content through Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs).

Protests: Documents and metadata inconsistencies in added algorithms specific to verification analyses are carried out. submits evidence Applicant may submit evidence anonymously while its authenticity through verification is needed. This guarantees confidentiality for whistleblowers, journalists, or any other individual providing sensitive material.

Cross-modal pervasive, distributed electronic evidence is stored within an environment rather than on a local computer or single point: the reality of file configurations kept by EviChain.

CHAPTER - 01: INTRODUCTION

1.1 INTRODUCTION

For this modern digital age that believes everything to be true, evidence stands as the foundation of truth, justice, and accountability among several areas, including the legal systems, financial operations, academic integrity, and corporate governance. As the dependence on digital information and data is high in the present times, so does the volume, type, and complexity of digital evidence. It is highly necessary to prevent this valuable information from being tampered , especially if it is evidence or valuable to our justice system . It is in the very germ of trust-making and decision-making that evidence plays a decisive role, with scrutiny being a matter of life and death for some.

In the light of evidence based more and more on digital media, there are a number of challenges ahead. Centralization or being controlled by a single organization or authority as well as the traditional evidentiary systems are prone to security breaches, data alterations, unauthorized information access, systemic collapse and in the worst case loss of justice . In any situation when a single channel is charged with all data storage and management, they represent a single point of failure that, if damaged by cyber-attacks, insider threats, or simple technical glitch, could lead to the paralysis of the whole repository of evidence. This issue then creates many concerns to question the validity of the stored information; instigates misinformation; and opens the doors for tampered data and fabricated claims-the precarious trustworthiness of digital interactions really comes to the forefront under serious situations like criminal investigation, whistleblower grievances, and financial fraud audits.The concepts of decentralization begins with the first crypto currency ever Bitcoin.[1]

Additionally, high-grade digital editing tools and AI-driven content manipulation techniques (for instance, deep fakes and document forgery) will further upgrade the risks of corrupted evidence. Videos, images, documents, and metadata might be altered maliciously to align with the interest of particular parties and difficult to be detected by conventional systems. This emerging menace landscape forces the urgent call for a next-generation solution for digital evidence that would ensure its integrity, immutability, verifiability, and privacy.

EviChain is developed to meet the said needs. It, therefore, is a paradigm shift in how digital evidence is stored, verified, and trusted. Basing it on Ethereum blockchain, EviChain creates a decentralized, secure, and tamper-proof platform that removes the risk involved in traditional centralized evidence systems. With EviChain leveraging blockchain's fundamental attributes of immutability, transparency, and distributed consensus, it provides an unalterable chain of custody ensuring that evidence, once recorded, can never be changed or erased. To maintain permanence and scalability, EviChain supports decentralized file storage systems like IPFS (InterPlanetary File System). The actual evidence files (whether they are images, documents, or videos) are kept off-chain on IPFS, and only their cryptographic hashes are written on the Ethereum blockchain. In this manner, the data remains decentralized and easy to retrieve, all while maintaining proof of existence.[2]

What really takes EviChain a step beyond is its AI-based advanced fraud detection infrastructure. Specialized algorithms analyze various types of digital evidence for tampering or inconsistencies:

- For visuals, such as images or videos, CNNs and RNNs recognize signs of alterations, compression anomalies, or traces of deep fakes.
- For textual documents and their metadata, anomaly detection models search for unusual patterns, metadata inconsistencies, or possible content manipulations.

Another cornerstone of EviChain is the privacy-preserving nature of the evidence submission. Consultants and whistleblowers, journalists, and victims of abuse can remain anonymous when submitting evidence for the system. By abstracting identity from submission, EviChain creates a safer world of justice for the otherwise silenced or threatened. This unique balance between transparency and privacy is something that really sets it apart from other digital evidence systems.

The possible use cases of EviChain are multitudinous and profound. The administration of justice can be entrusted with submission and provisioning of digital evidence with utmost reliability. In the financial arena, audit trails would be secured against any tampering. Academics would be left with an improved standing to fight against plagiarism and the issuing of forged credentials. To a certain extent, government and enterprise systems can be placed on a more solid footing by means of compliance through logs and disclosures.

At the end of the day, EviChain is meant to take the handling of evidence to entirely new standards in this digital realm. It contributes towards establishing infrastructure for digital justice and information reliability that is trust-driven and future-ready. In a world where data integrity is key and misinformation can guide an outcome, EviChain lays down a secure, intelligent, and decentralized foundation upon which truth can be verified.

1.2 PROBLEM STATEMENT

With the onset of new digital trends, the requirement for trusted evidence has increased in various sectors, such as in law, banks, journalism, or official institutions. But the classical methods of storing and managing evidence never kept up with the evolving landscape of new digital threats and technological advancement. Most importantly, these systems have critical drawbacks coming from their very centralized architecture.

The architecture of evidence storage systems, being centralized, entails a single point of failure, rendering it vulnerable to data leaks, unlawful access, and deliberate tampering. Once a system has been compromised, whether by hackers, internal actors, or through simple human accidental behaviors, the registered evidence may suffer everlasting damage: hardly any consequences elsewhere could be severe if such vulnerabilities faced an environment in which this evidence was to be used, like in a courtroom, regulatory audits, or other academic investigations-worse such cases may be accepted as known falsified evidences, or worse, may end up in actual data loss.

Furthermore, no accompaniment of intelligence has existed in the current systems to identify counterfeit or manipulated content. New advanced forgery techniques applied digitally, such as AI deep fakes, image spoofing, and document forgery, make it perhaps impossible to mark an evidentiary document as genuine or one that has been manipulated for its own good and thus would have exposed decision-makers to only manipulated or misleading information, hence decreasing trust in these institutions and in the credibility of the verdict or conclusion formed from such data.

Privacy and anonymity become an extra hurdle in these conventional systems. Whistleblowers, journalists, and victims looking to submit evidence have to face dangers of exposure, retaliation, and getting legally chased out because in actuality, in many conventional systems, their identities are poorly protected. The absence of a secure and anonymous channel pushes individuals to refrain from presenting vital evidence, especially under high-risk situations of corruption, abuse, or sensitive revelations.

Another facet of the layered complexity is the sheer number and diversity in the world of digital evidence today. From pictures and videos to metadata and documents, the modern-day generation of evidence is so large in scale that it chokes any such system Das traditionally was not built to bear such varieties and scales. From delays in processing and inefficient storing to yesterday's gap-filling in verification workflows, these systems simply do not work-in-performance, effectiveness, or scalability.

When these issues are set side by side, they directly oppose the reality of evidence being used securely, accurately, and trustworthily. The lack of modernity will invite greater chances of:

- Evidence being altered.

- False data making its way into major decisions.
- Sensitive contributors being discouraged from providing critical evidence.
- Systems failing to scale up to the expectations of the digital world.

Hence, transformation of the problem needs to be implemented, cracking out those central vulnerabilities, verifying credentials with intelligence, supporting anonymous submissions, and scaling and also adapting to different formats of digital evidence.

Issues of police corruption, some affective mirror, include the false authentication procedure; private commissions of fraudulent demonstrations; institutional sabotage; and anonymous forgery of third-party evidence, thus creating an uncredible and unsafe digital evidence mechanism provider. However, when the system receives the EviChain, it gives to the police an extraordinary and invaluable weapon that the police can use to oppose corruption. EviChain is a blockchain-based platform for evidence management that secures evidence and keeps it from being tampered with, as well as detection of fraud. With the immutable record of evidence on the Ethereum blockchain, the decentralized nature of Ethereum, and also with sophisticated algorithms capable of detection of fraud, EviChain provides a guarantee for the authentication, reliability, and anonymity of digital evidence. Its implementation further institutionalizes that trust in digital processes and also creates an opportunity for the individual to have sufficient trust from the risk posed by systematic threats to make a stand-based contribution securely.

1.3 OBJECTIVE

EviChain aims to develop a highly robust, decentralized, and safe platform for evidence storage, overcoming the inherent problems in traditional approaches. EviChain aspires to be a second-generation digital evidence management system that uses blockchain technology, mainly on the Ethereum network, combined with fraud detection mechanisms and a design respectful of privacy. The platform will provide services for multiple applications: legal proceedings, academic investigations, corporate compliance, and whistleblower protection.

Some of the very important eye-on goals of this project are as follows:

1. Decentralized Storing of Evidence

EviChain aims to reduce the threat of centralized storing systems by fully accepting decentralization through an Ethereum blockchain-side architecture. In this paradigm, all evidence gets stored tamper-proof, immutably, and with resistance to unauthorized scrutiny or alteration. Decentralized storage guarantees the continuity of any copyright over a digital proof, unlike traditional databases that can be manipulated and face data loss usually due to single points of failure. EviChain uses a combination of IPFS for P2P distributed storage of large files such as images, videos, and documents, with cryptographic hashes resting on the chain for verification.

2. Anonymous Proofing Mechanism

Fear of retaliation, surveillance, or counter lawsuits constitutes one of the real barriers to submitting evidence. EviChain solves this problem by supporting anonymous submissions so evidences can be put up without user identification. With privacy as a key concern for all users, the platform implements zero-knowledge protocols and wallet-based means of authentication without binding it to an identity. This aim is to facilitate legitimate disclosure while increasing the integrity and completeness of the evidence database.

3. User-Friendly Interface

EviChain is built with accessibility and ease of use in mind. The platform will avail of a clean, responsive, and intuitive web interface built on modern web frameworks, such as Next.js. This would enable users with varying degrees of technical expertise to interact effectively with the system. Whether it is submitting new evidence, navigating through files, checking for authenticity, or tracking blockchain activity, all parties, including legal professionals, forensic analysts, and regular users, should be able to operate the system without having to dive deep into blockchain or cryptography. User onboarding and feedback with real-time support, as well as guided workflows, are also put in place for enhanced usability.

4. Advanced Fraud Detection

Keeping pace with the inexoring pace of technological advancement of digital forgery and misinformation, EviChain incorporates AI-based fraud detection algorithms into the evidence validation pipeline. The pipeline includes Convolutional Neural Networks (CNNs) to detect image and video forgery, whereas NLP-based and anomaly-based approaches are applied to text-based evidence and metadata. The platform is thus capable of:

- Flagging forged media content,
- Detecting inconsistencies in file origin or timestamp,
- Providing a confidence score regarding authenticity.

Serving as a kind of fraud detector, this keeps the gate closed for anything that would otherwise cast doubt on genuine evidence, such that only genuine and credible evidence finds a home in the blockchain.

5. Trust and Security Assurance

EviChain is designed to give maximum trust to any data it handles. In order to make evidence tamper-proof, the platform relies on blockchain immutability, crypto hashing, IPFS content addressing, and encryption of user data when sensitive. This security setup makes EviChain a perfect choice to build upon applications that need a high degree of trust, such as court trials, research misconduct investigations, or anti-corruption investigations. Ensuring that every transaction is traceable without breaching privacy, the platform thus improves all stored digital evidences' transparency and validity.

6. Scalability and Adaptability

EviChain is made with the future in mind. The architecture is modular and scalable, allowing the system to cater to significantly larger volumes and varieties of digital evidence as user bases grow. New developments in fraud detection, blockchain upgrades, or data formats would be quickly assimilated by EviChain with plugin-based modules and smart contract extensions. The platform is also prepared for cross-platform integrations, via an API method, in order to allow seamless interfacing of external systems—for example, legal databases or academic registries—with EviChain.

When the above points are achieved, EviChain would become a solid and forward-looking digital evidence management system secured against threat, anonymous, keeping in mind human intelligence. It will protect the truth and privacy and nurture public trust on systems depending on digital evidence for a transparent and fair digital environment.

1.4 SIGNIFICANCE AND MOTIVATION OF THE PROJECT WORK

1.4.1 SIGNIFICANCE OF THE PROJECT

With technology pervading every aspect of human life, the importance of establishing secure, trustworthy, and transparent systems for evidence management has grown exponentially. Whether it happens in the context of legal disputes, financial audits, corporate investigations, academic misconduct cases, or whistleblower reporting, digital evidence must be credible and maintain integrity to foster justice, accountability, and trust. In this new-age digital ecosystem, the conventional systems of evidence handling reliant on centralized servers, manual verification, and digital storage will no longer suffice.

The EviChain system acts as a timely and innovative solution to the global problem. Using blockchain technology and artificial intelligence as engines, it seeks the provision of a decentralised, tamper-proof, and privacy-centric platform for digital evidence management. Being on the Ethereum blockchain, all transactions and entries become immutable, verifiable, and distributed on a range of nodes, thus eliminating single points of failure, unwanted data manipulation, and data loss. This presence of immutability given to the evidence inside the chain, achieved through consensus formation and cryptographic hashing, maintains that after recordings of the evidence on the blockchain, it cannot be altered or deleted, thereby preserved as original and admissible in courts.

1. Enhanced Security and Data Integrity

First, and most importantly, tampering and unauthorized alterations of evidence in storage are ruled out by EviChain. Traditional centralized systems are prone to compromise due to system vulnerabilities, insider threats, or poor cyber security. The decentralized design of EviChain precludes data control by a single authority, thereby largely eliminating the risks of data breaches, corruption, or loss.

2. Anonymity and Whistleblower Protection

The EviChain provides a very important mechanism of proof submission anonymously when the informants might face retaliation or may be otherwise under threat of having the law used against them for submitting such information. Whistleblowers, investigative journalists, victims of injustice, or employees reporting corporate fraud are allowed to use this platform while maintaining the secrecy of their identities. This, in turn, fosters increased participation and transparency by creating an environment where individuals are empowered to disclose valid and significant information without fear.

3. AI-Powered Fraud Detection

The sudden proliferation of detection systems, media manipulation, and document forgeries has placed authentication of digital content in the spotlight. EviChain incorporates state-of-the-art AI models that include Convolutional Neural Networks (CNNs) for tampering with images and videos and Recurrent Neural Networks (RNNs) for detecting anomalies in text. This suite of models further empowers the platform to automatically detect falsified evidence so that only genuine and credible proofs are referenced and stored.

4. Cross-Industrial Applications

Being an extraordinary platform, this also spans diverse domains. EviChain resolves the issue of chain-of-custody in the digital world for storing and verifying evidence in legal matters. In academic fields, it assists the validation of documents and submissions to defend against plagiarism and research fraud. In the finance domain, it attends to audit trails and regulation compliance to be traceable. Essentially, EviChain stands out because of its assistance that cuts across various industries, not just due to its technology.

5. Scalability and Future Readiness

Unlike rigid legacy systems, EviChain has been built on a modular basis for scalability. Should digital evidence volume escalate, the platform would meet the demand without any great sacrifice to performance or security. Its flexible architecture will allow for future integration with other blockchain networks or storage protocols or fraud detection tools, thus ensuring long-term sustainability and adaptability to an ever-changing technological and regulatory environment.

6. Establishing Trust in the Digital Era

Perhaps the utmost importance of the EviChain project lies in the establishment of a measure of trust amongst the general populace and among institutions. Offering an incorruptible and transparent manner of evidence storage grants all stakeholders-everyone from judges, investigators, auditors, and educators to the public-the assurance that the data they are working with are authentic and genuinely untampered with worthiness. This trust guarantees fair results during legal processes, academic evaluations, and financial audits.

1.4.2 MOTIVATION OF THE PROJECT

With the increase in digitalization at a new pace, the production and consumption of digital content has exponentially increased in all fields, such as for legal proceedings, financial transactions, reports in journalism, research, and the functioning of the government. Thus, digital evidence, namely documents, images, videos, audio clips, emails, and metadata, has become an integral part of the processes of taking decisions and enforcement. On the other hand, this mass reliance on digital content has brought to the forefront another significant challenge: authenticity, integrity, and security of digital evidence in this era where manipulation tools, resources, and technologies are evolving at a rapid pace.

1. The Escalating Threat of Digital Manipulation

Today, techniques such as signature detection system, AI-generated media (true-fakes), photoshopped documents, and fabricated text or metadata have all together increased the threat of digital misinformation and deception. There is a very thin line between manipulated evidence and genuine evidence; hence, manual verification is inefficient and prone to errors. Consequently, trust in digital content has been getting increasingly fragile, more so in scenarios where the validity of information is utterly nailed down, including criminal investigation, civil litigation, and financial auditing, as well as in academic publishing and public whistleblowing.

Due to the tampering through infinitely many insider threats, typical centrally controlled evidence storage facilities comprising a single-server database or an institutional cloud platform are rendered incapable of tamper-resistance or cyberattack resiliency. Such systems suffer single-point failures and unauthorized access, compromising data or deliberately altering evidence, thereby undermining the very premises of justice and accountability. [3]

2. EviChain: Responses to Critical Digital Challenges

EviChain, in essence, comes into being as a reaction to those chilling avenues of attack through which evidence destruction is almost becoming a vested right. The very wordstood for "EviChain" is built upon the robust architecture of the Ethereum blockchain to ensure that every piece of evidence submitted disappears into a timeless anti-fungible record that is verifiable, traceable, indelible, and distributed among every participant in the network. This architecture guarantees that no single entity can alter or delete any evidence, which guarantees that it's considered credible and accepted as legal evidence in many use cases.

EviChain intends to completely do away with second single points of failure in centralized systems and apply a scattered peer-to-peer paradigm for storage and verification of evidence. Thus even under physical hardware failures, actual cyber-attack threats, or the threat from an insider, stored evidence remains intact against all such evidence.

3. Protecting Those Who Speak the Truth

A central motivation in the development of this project involves the protection of persons handling sensitive or high-risk material. Whistleblowers, investigative journalists, activists, or citizens reporting wrongdoing usually do so under the threat of retaliation, harassment, or inflicting legal measures. Many times, potential submissions fail because the information holder was never guaranteed anonymity-this prevented the holder from revealing irrefutable evidence of corruption, fraud, or abuse of authority. Therefore, EviChain has been developed such that it allows for anonymous submissions while remaining credible evidence so that submitters' identities really would be kept concurrent with evidence credibility. This feature, which assures both justice and accountability to so-called gullible persons, gives the organizations and institutions a greater degree of transparency.

4. AI-Based Verification: Lessening Human Error and Increasing Efficiency

One of the major hurdles in the management of digital evidence is in the verification of authenticity, especially with the growing techniques for forgery. Manual processes are not scalable and are subject to human bias or overlook. EviChain incorporates advanced fraud detection algorithms powered by AI to safeguard against forgery. CNNs are for the analysis of images and videos for signs of tampering, while RNNs look for signs that text content has been manipulated or synthetically generated. These types of models provide an opportunity to engineer automated pipelines for authenticity verification integrating intelligence, thereby minimizing human error and enhancing the speed and reliability of validation.

As with other phases of the submission process, by automating the most critical part of validation, EviChain sets a new standard where efficiency and scalability are augmented as a counter to the ever-increasing challenge of digital forgeries and signature detection.

5. Towards a Trustworthy Digital Ecosystem

If put essentially, EviChain was conceived with an eye to restoring trust in digital evidence and the digital systems that act upon it. By combining the immutability of blockchain with AI-powered fraud detection, EviChain puts forth a holistic solution for the conception of a secure, open, and accountable digital environment. This project ensures that evidence gained trust not just from whom submitted it, but also through the means of verifying, storing, and safeguarding this evidence.

Ultimately, EviChain is also more than a technology; it is a promise in favor of digital truth, integrity, and justice. It thereby serves as a mighty instrument against digital misinformation, institutional opacity, and cyber-enabled fraud, for a future wherein digital content can regain the status of a trustworthy mirror of reality.

1.5 ORGANIZATION OF PROJECT REPORT

The purpose of this report is to communicate an organized and sufficient perspective about the EviChain project; that is, the concept, implementation, and impacts thereof. This organization ensures logic and gives value of easy progression for any reader in following and seeing how the project unfolds and what contributions it makes. The report sections into the following chapters:

Chapter 1: Introduction

This chapter lays the groundwork for the project by describing the background, problem statement, objectives, and motivation behind developing EviChain. It also explains the project significance and the key concepts and technologies involved in it, and finally describes the structure of the report for the reader's convenience finally.

Chapter 2: Literature Survey

An exhaustive literature survey on decentralized systems, blockchain, and fraud detection systems is taken up in this chapter. It details past research work, what is done in the industry, and the technological advancements in the focused areas concerning evidence management. The chapter clearly identifies some significant gaps in existing literature, justifying the need for a solution like EviChain.

Chapter 3: Problem Statement & Objectives.

This chapter precisely mentions the problems being faced due to evidence management via older systems such as centralization, tamper vulnerability as well as anonymity-related issues. It further states the goals of the project, including a complete decentralized platform as a secure evidence storage and verification system.

Chapter 4: System Architecture and Design

The architectural framework of EviChain will be discussed in this section, delving into its various parts and how they relate to one another. Blockchain integration, decentralized storage systems, and the fraud detection algorithm will also be covered. Also included are system design diagrams and technical specifications.

Chapter 5: Implementation

The implementation process is chronicled in this chapter, along with the tools and technologies that will be used during the development of the EviChain platform. These include the development of smart contracts; deployment on Ethereum; integration with IPFS for storage; and use of AI models for fraud detection. The challenges encountered during the implementation process have been discussed along with their remedies.

Chapter 6: Results and Analysis.

Results, part of the project revealing analysis of performance from the decentralized system and fraud detection algorithm, are also measured along other metrics such as accuracy, reliability, scalability as well as effectiveness in achieving secure evidence storage effectiveness.

Chapter 7: Applications and Use Cases.

This chapter illustrates real-world applications of EviChain in areas such as legal proceedings, financial audits, academic integrity checks, or whistleblower protection. Use cases elaborate on its functionality to demonstrate real-world impact and benefits.

Chapter 8: Final Conclusion and Future Work.

This final chapter summarizes what the project has achieved and contributes to the decentralized evidence management field. It also mentions the limitations observed and outlines paths for future research and development, such as enabling support for additional evidence types in the system and improving system scalability.

CHAPTER 02: LITERATURE SURVEY

2.1 OVERVIEW OF RELEVANT LITERATURE

Integration of blockchain technology and AI into evidence management and fraud detection has become a prominent research area in recent years. Growing concerns for authenticity and transparency in digital content have given rise to the need for a more fortified setup. Due to immutability, decentralization, and transparency, the blockchain infrastructure suits secure evidence storage, whereas deep learning-powered AI algorithms seem to offer great promise in detecting fraudulent patterns and computer-generated manipulated media. This chapter discusses in detail the literature survey regarding contributions, advancements, and limitations of existing research undertaken in five major areas: blockchain for evidence management, consensus mechanisms, integration with AI, fraud detection techniques, and core developments on blockchain systems.

2.1.1 BLOCKCHAIN IN EVIDENCE MANAGEMENT

The blockchain thus came into picture for tamperproof auditable systems in digital forensic and evidence management. Recently, frameworks have been proposed to use blockchains to maintain the integrity of digital records through the immutable logging of all evidence submissions. Bhuvaneshwarri and Sudha [6] proposed a blockchain-cloud architecture intended to maintain the authenticity of data while granting selective access to evidence. Their system took advantage of blockchain to cryptographically link blocks, so once data was submitted, it could not be altered. Despite data integrity being well maintained, the approach fell short on scalability and latency aspects, especially when it came to managing large volumes of evidence files for purposes of multimedia evidence.

On a similar note, some have emphasized the blockchain's ability to strengthen the "chain of custody"—a concept in legal forensics that ensures the evidence has not been tampered with from the moment of collection to presentation in a court. However, most researchers have highlighted a very few existences of actual implementation or real-world usage scenarios.

2.1.2 CONSENSUS MECHANISMS AND SCALABILITY

A consensus mechanism is the heart of blockchain technology and can make it more or less performant and secure. Zhou et al. [7] made a comparative study of consensus algorithms, namely PoW, PoS, and hybrids, to determine their suitability for evidence management systems. They found that PoS provides much better energy efficiency and transaction throughput than PoW. Also set forth as an attractive alternative were hybrid consensus models that combine PoS and Practical Byzantine Fault Tolerance (PBFT). However, a lack of empirical analysis and deployment examples prevented these models from being used in practice.

Other works proposed cryptographically secure protocols to improve transaction integrity and the confidentiality of data stored on blockchains. While these models removed vulnerabilities to double-spending and Sybil attacks, the problems of delayed consensus finality and inefficient resource consumption remained. These problems become exacerbated when confronted with large-scale digital evidence.

2.1.3 AI AND BLOCKCHAIN INTEGRATION

The synergy of these two technologies is a fairly new area with increasing potentials. Some researchers such as Phansalkar et al. attempted to study general frameworks wherein the blockchain is utilized as a secure and verifiable ledger while AI algorithms would provide the intelligence to recognize patterns and perform anomaly detection.

That cross-pollination would mean that AI operations can be implemented in a decentralized manner with traceable decision-making mechanisms- a remarkable gain for accountability in automated systems. Rabah [8] proposed a conceptual integration of AI, blockchain, and IoT to realize real-time verification of data integrity in a distributed environment. However, theoretically promising, the model did not enter into concrete implementation considerations, while its scalability was an issue because AI is highly computation-heavy.

The potential for such integrations to form intelligent, tamper-proof systems-one whose application could range from areas like e-health, digital identity, and legal forensics-have, therefore, been recognized exhaustively in the literature, thus paving the way for EviChain and the likes.

2.1.4 APPROACHES IN DETECTION FRAUD

AI-based approaches for detecting fraudulent acts have indeed ushered in a renaissance in the detection of subtle manipulations in texts, images, and videos. Deep learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are mostly used in media forensics for finding patterns.

Jones and Smith [9] reviewed a wide variety of tampering detection methods and described their independence and usefulness. CNN-based models are focused on the search for pixel-level anomalies in images and videos with good performance, whereas the RNNs detect unusual patterns in text-based submissions. However, the real-time integration of these models with blockchain remains another emerging challenge.

The primary drawbacks are the need for large amounts of labeled data before they can attain acceptable accuracy levels and the immense computational power required for real-time processing. However, notwithstanding these limitations, the use of AI is considered necessary for scaling fraud detection across diversified and evolving forms of digital evidence.

2.1.5 FUNDAMENTAL CONTRIBUTIONS TO BLOCKCHAINS

Satoshi Nakamoto's seminal paper on Bitcoin [1] set the foundations for a decentralized trustless system, depending on the PoW consensus mechanism. In essence, the PoW mechanism powers Bitcoin: a revolutionary idea that is now under scrutiny for its energy wastage and issues of throughput for transactions, thus making it less suitable for validating massive data sets.

Vitalik Buterin introduced the Ethereum [2] concept for smart contracts that enabled programmable transactions and dApp development. Ethereum has been crucial in helping to create such platforms as EviChain; nevertheless, it is held back by ever-increasing gas fees and temporal scalability restrictions within its finite capacity to process transactions.

Layer 2 solutions and other consensus mechanisms (like Proof of History as implemented in Solana, or DAG-based systems) are also researched, but they are still under evaluation for durability and suitability for evidence management use cases in the long term.

The summary of above all is given in the table 2.1 (below) :

Table 2.1 Literature Review

Study	Focus	Findings	Challenges
[1]	Bitcoin and PoW-based blockchain	Decentralized data management model	Scalability and energy inefficiency
[2]	Ethereum and smart contracts	Enabled decentralized applications like EviChain	High transaction fees and limited scalability

[3]	Cloud-integrated blockchain for evidence management	Ensures data integrity and secure access	Scalability issues with high-volume data
[5]	Fraud detection in digital evidence	Tamper-proof records for improved fraud detection	Requires broader validation across datasets
[7]	Security-enhanced blockchain protocols	Improved security using advanced encryption techniques	Speed and scalability limitations for large datasets
[8]	Convergence of AI, blockchain, and IoT	Theoretical potential of combined applications	Lack of practical implementation
[9]	AI-based tamper detection	Improved detection using CNNs and RNNs	Resource-intensive large-scale datasets
[13]	AI and blockchain for decentralized applications	Combines AI analytics with blockchain transparency	Significant technical hurdles

2.2 KEY GAPS IN THE LITERATURE

Among the many areas in which the current research makes notable strides in evidence management using blockchain and artificial intelligence applications, there are still several gaps that seem to hinder the practical adoption and application of such technologies. This section summarizes the few areas where limited work has been completed, thus setting the groundwork for future development:

2.2.1 SCALABILITY AND PERFORMANCE

Scalability has often been a fundamental limitation for any blockchain system, especially one relying on an energy-consuming consensus such as Proof of Work (PoW). More adoption of blockchains implies bigger volumes of transactions and data to be processed. Efficient handling of large datasets such as HD images, video recordings, and all sorts of digital evidence is therefore to be desired, particularly in demand-intensive applications like evidence management. Unfortunately, it is a huge challenge for blockchain systems-the ones that mostly center on PoW-to scale and meet these demands.

Multiple inquiries delve into the inability to face large volumes of transactions, thus slower transaction processing and greater cost, largely for more complicated forms of data. For example, the high gas fees and low throughput on systems like Ethereum stand in the way of bulk evidence submissions from being done in real time. Blockchain systems concerned with decentralization and security sacrifice transaction processing speed, thereby hindering them from accommodating vast amounts of digital evidence in very short time periods. Moreover, while being explored and showing promise in executing tasks to a larger scale, alternate consensus mechanisms such as PoS or hybrid models have, however, yet to be tested in high-traffic evidence-management use cases.

2.2.2 INTEGRATION HITCHES

Integration of AI and blockchain opens more room for technical and operational challenges in the way of fraud detection and evidence validation. AI-powered applications that detect and analyze fraudulent activities—especially with sophisticated machine learning algorithms like CNNs and RNNs—would benefit tremendously from this transparent and immutable framework provided by blockchain. Yet, the alignment of AI's ability to process large volumes of real-time data with the inherently decentralized and permissioned form of blockchain is still posing a daunting impediment.

Data interoperability ranks one of the top concerns. With such decentralization present, blockchain architecture makes a distinction in that external AI systems cannot access or manipulate the data stored on-chain unless specifically through-built bridges. This lack of interoperability hinders the efficient deployment of AI models that require real-time access to data in their performance of fraud detection or evidence validation. Added to this, many of today's blockchain protocols have fabricated towards the heavy-duty computational demands of AI systems, engendering inefficiencies and bottlenecks.

Those issues are accompanied by the absence of recognized standards to map existing AI systems onto blockchain solutions and vice versa, in an interoperable manner, to limit widespread adoption further. Indeed, without common standards, different blockchain platforms and AI systems cannot interact with each other, thus rendering the design of a unified secure evidence management and fraud detection system almost impossible.

2.2.3 EMPIRICAL VALIDATION

Despite various definitions and methods, there is a glaring gap in the literature regarding the lack of extensive empirical validation for blockchain and AI-based evidence management systems. Many theoretical models and some prototypes have been suggested for such systems, but very few of these systems have been tested rigorously in practical circumstances and on sufficiently diverse datasets. The dearth of empirical validation hinders any practical assessment of the implementations for scalability, robustness, and performance.

For instance, although evidence integrity secured by blockchain is one of the possibilities acknowledged, scant bibliography exists on whether this can scale up in bona fide scenarios of large-scale evidence transactions. Likewise, AI approaches have been proven to be able to detect manipulated media, but little is known about their actual efficacy in real-world fraud-detection scenarios, especially when the blockchain is part of the solution. Real-world testing is vital to establish whether the system can stand up to challenges, including user-unfriendliness and unforeseen glitches.

Until such time that these systems are validated empirically in real-world scenarios and tested against multiple real-world data sets, adoption of these solutions into mission-critical domains such as legal evidence management will remain doubtful.

2.2.4 COST AND ENERGY EFFICIENCY

In the environmental scenario, some might argue that a blockchain operating using energy-intensive consensus mechanisms like PoW is unsustainable in the longer term due to environmental hazards and operating costs. Such criticisms are particularly elevated for the massive energy consumption required to maintain blockchain networks like Bitcoin and Ethereum from an environmental sustainability perspective.

Nakamoto, in his Bitcoin [1] original design document, had envisaged a certain level of power usage; but, as blockchain networks scale in size, providing the infrastructure for the growing nodes incurs exponentially growing costs. This itself is a huge obstacle to large-scale adoption of blockchain technology for applications like evidence management, where there is an acute requirement of handling large data sets and processing transactions quickly. Furthermore, the exorbitantly high transaction fees associated with these systems stand in the way of acceptance, which grows worse during network congestion, complicating the use of blockchain for high volume evidence storage and retrieval with respect to feasibility.

Hence, to secure the feasibility of blockchain in actual applications, especially for evidence management, the more energy-efficient consensus mechanisms such as Proof of Stake (PoS) or hybrid consensus mechanics ought to be researched and implemented. Also, these options ought to minimize costs while conserving security and decentralization.

2.2.5 ABSENCE OF USER-CENTRIC APPROACHES

Current research on blockchain and AI for the management of evidence tends only to discuss technical aspects concerning scalability, security, and fraud detection. User-centric considerations such as ease of use, accessibility, and intuitiveness, however, are often overlooked. This especially poses a problem for realms like legal forensics, where the end users may not be tech experts.

Stakeholders such as investigators, lawyers, and whistleblowers may not be able to immerse themselves in complex blockchain systems by virtue of lacking the technical expertise required to do so. Thus, the urgency for top-notch user-friendly blockchain-based evidence management platforms that are easy for non-technical users to access stands unaddressed. Some studies like those of Jones & Smith [9] are concerned with the technical innovations of AI and blockchain but ignore the practical needs of end users, such as how well systems are designed in terms of the interface, the nature of training required, and whether they are user-friendly or not. These considerations play a big role in whether professionals in the field ever get around to using these technologies.

Adopting a user interface design philosophy that is intuitive, straightforward to use, and requires no technical expertise will bring a great deal of momentum to blockchain-based evidence management systems.

2.2.6 LITTLE ATTENTION TO NEW TECHNOLOGIES

While blockchain and AI have been under massive research individually, their composite approach towards evidence management is yet a niche. Jones and Smith [9] have tried to bridge some of the chasms that emerge between cutting-edge technologies like blockchain and tamper-detection algorithms; however, studies have mostly overlooked the synergy drawn from newly developed AI algorithms and hybrid blockchain models for evidence validation.

Further advancement of AI, for example, better deep learning algorithms, should radically enhance the accuracy and efficiency of fraud detection but are not often investigated in tandem with blockchain. Hybrid blockchain models, on the other hand, those that combine attributes from public and private blockchain, could really strike a fine balance between scalability, security, and privacy in the area of evidence management but are seldom looked at from the AI angle.

This gap creates an opportunity for future investigations on a synergistic combination of cutting-edge AI techniques and novel blockchain architectures, thus putting out more effective and scalable evidence management systems.

Chapter 03:SYSTEM DEVELOPMENT

3.1 REQUIREMENTS AND ANALYSIS

Before commencing development on the EviChain platform, these requirements must first be pursued in a structured manner to ensure that the platform remains capable of meeting the functional, technical, and security demands set before it. This section delineates the major requirements of the project along with an in-depth analysis breakdown toward which the platform's carrying objectives are set. In particular, the project would like to use cutting-edge technologies, such as blockchain-based decentralization and AI-based fraud-detection algorithms, to preserve the authenticity and security of evidence.

3.1.1 FUNCTIONAL REQUIREMENTS

Decentralized Storage of Evidence:

The primary concept of EviChain constitutes the decentralization of the storage of evidence. This negates the risks with the centralized kind of data storage: a single failure point, manipulation, or illegal access. Thus, the evidence must be prevented from being tampered with or corrupted by any central authority. The creation of blockchain technology ensures that no single one person has full control over the evidence, an element critical for sensitive data.

Infrastructure of Blockchain:

The evidence on the platform is a cryptographic hash generated from each piece of evidence, which is to be recorded on the Ethereum blockchain. The decentralized nature of Ethereum ensures security for the integrity of the evidence and a transparent, immutable record of the evidence itself. Integration of smart contracts will automate processes concerning the submission, storage, and validation of evidence so that every single act is carried out in a verifiable and secure manner.

Decentralized File Storage:

Rather than storing evidence files directly on the blockchain, which can be impractical due to size limitations, EviChain will utilize the **InterPlanetary File System (IPFS)** for decentralized file storage. IPFS is a distributed system that stores evidence across multiple nodes globally. This ensures that the evidence is permanent and tamper-proof, as the files are distributed and replicated across a network of decentralized storage providers. Pinata will be employed to pin evidence files to the IPFS network, guaranteeing their availability for long-term verification.

Proof Authentication and Validation:

The EviChain platform must authenticate and verify the evidence to ensure its truthfulness and authenticity. This involves using both cryptographic techniques and AI algorithms to confirm that evidence has not been altered or manipulated after submission. Evidence validation is vital for ensuring that only reliable and trustworthy content is accepted on the platform.

Tamper-Proof Datastore:

The core objective of EviChain is to ensure that evidence, once uploaded, remains immutable. The cryptographic hash of the evidence will serve as a "digital fingerprint" and will be stored on the Ethereum blockchain. This hash ensures that any changes made to the evidence file will result in a mismatch with the hash stored on the blockchain, thereby indicating tampering.

Fraud Detection:

The platform utilizes AI-based algorithms for detecting fraudulent evidence. CNNs are used for image and video analysis, RNNs for fraudulent pattern detection in video sequences, and NLP techniques to spot inconsistencies in the textual evidence, such as unusual phrasings or conflicting patterns. Thus, ensuring evidence undergoes strict checks for its authenticity before being submitted to the platform.

Anonymous Evidence Submission:

One of the critical aspects of the EviChain platform is that it allows users to submit evidence anonymously. The requirement is more important in cases involving whistleblowing or exposing corruption, where the submitter may fear retribution. While keeping users' identities secret, the chain guarantees that the integrity of the evidence is intact. Hence, anonymity will not compromise the evidence's verifiability or authenticity.

Cryptographic Anonymity:

Along with anonymous evidence submission, the platform will use advanced cryptographic techniques from zero-knowledge proofs, thus enabling users to testify about the submissions without revealing their identity. A zero-knowledge proof allows one party to prove to another party that a statement is valid, with no other information revealed. This will allow for a high level of trust in the platform without exposing users to any risks.

User-Friendly Interface:

The EviChain platform should be equipped with an interface that is intuitive and straightforward for its primary stakeholders, i.e., legal professionals, law enforcement agencies, journalists, and investigators. Despite complicated underlying technology, the platform should offer a straightforward user experience whereby a user may submit evidence, view evidence, or verify evidence. Given the requirement for a performant application optimized for search engines, Next.js serves as the perfect candidate as the front-end framework since it allows server-side rendering. And to give users the ability to submit and verify evidence through their MetaMask wallets, the Web3.js or Ethers.js library will be used to connect to the Ethereum blockchain.

Scalability and Performance:

EviChain is anticipated to necessitate the storage of huge volumes of evidence data, especially multimedia files, i.e., high-res images and videos. Hence, there arise the requisites for scalability and performance. The platform must ensure processing high numbers of transactions and evidence submissions while maintaining security and performance of the system. The architecture of the system should be such that it can take complete efficient steps as the data volume grows, thereby maintaining the best availability, and latency metrics.

Layer 2 Solutions:

Layer 2 solutions such as Polygon or Optimism are being integrated into the solution to overcome Ethereum's scalability issues. These Layer 2 solutions prevent more transactions from being funneled onto the Ethereum mainnet, causing congestion and exorbitant gas prices, thereby retaining Ethereum's security and decentralization characteristics. This is extremely relevant as EviChain scales to take on a large number of evidence submissions.

Cost-Efficient Smart Contract Development:

The Solidity language is to be used to write smart contracts meant for the submission, storage, and validation of evidence. These contracts must be made to work on an optimized basis in performance and cost, especially considering the exorbitant costs from gas fees in Ethereum. We shall apply optimizations that reduce gas costs during the contract execution, without compromising on uplift or security of the platform.

3.1.2 TECHNICAL REQUIREMENTS

The technical framework used to build the world's first EviChain platform must be robust enough to support the required decentralization, fraud detection, and user privacy mechanisms. The set of technical requirements stated above accounts for performance, security, scalability, and reliability of the solution. The core technical requirements in the blockchain domain include blockchain infrastructure, decentralized storage mechanisms, AI-powered fraud detection systems, and the upliftment of cutting-edge cryptographic tooling.

1. Blockchain Technology: Technical Specifications

Ethereum will serve as the backbone for the EviChain platform, selected for its maturity, widespread use, decentralized character, and smart contracts allowing for Turing completeness. Ethereum's capabilities include immutable record-keeping and the ability to deploy smart contracts that autonomously execute pre-defined logic, both of which are essential in guaranteeing trust and transparency in the evidence management process.

- **Smart Contracts with Solidity:** Smart contracts will be implemented in Solidity, which is the most common programming language for the Ethereum platform. These smart contracts provide for automation of evidence submission, hash generation, storing candidates on blockchain, and validating evidence integrity. To modularize various operations such as evidence submission, hash verification, metadata tracking, and audit trails, multiple smart contracts can be developed.
- **Local Testing And Development with Ganache:** For contractual deployment and testing on the Ethereum main network, development will be initiated using Ganache-this personal blockchain allows for quick testing and local development. It guarantees that contracts are tested safely in an environment where they do not bear the expenses or consequences of live deployment.
- **User Ethereum Wallet Integration using MetaMask:** The platform will integrate MetaMask as the browser-based Ethereum wallet user interface for blockchain interactions. It allows users to submit and verify evidence, sign transactions, and manage their Ethereum accounts securely. Besides allowing the users to manage their Ethereum accounts securely and conveniently, MetaMask has become the go-to interface connecting dApps such as EviChain through Web3 libraries.
- **Transaction Optimization:** Gas is the fee for execution on Ethereum, but its price keeps

fluctuating at almost every instance in real time. Thus the smart contract is designed to optimize gas by performing storage operations as little as possible and never doing redundant logic; it also tries to combine data and computations using efficient data structures. Besides, Layer 2 scaling solutions such as Polygon or Optimism will be investigated to reduce transaction fees while increasing throughput.

2. Decentralized Storage Infrastructure

The Ethereum blockchain only stores hashes and metadata since whole evidence files cannot be feasibly stored on-chain due to cost and size limitations. Hence, using these decentralized file storage systems, in tandem with the blockchain infrastructure, will be preferred by EviChain.

- **InterPlanetary File System (IPFS):** Evidence files will be uploaded and stored on IPFS, a peer-to-peer distributed file system. IPFS guarantees immutability and decentralization since files are content-addressed using cryptographic hashes. Any change in the file changes the address and thus makes tampering obvious.
- **File Permanence with Pinata:** To keep evidence files permanently available on the network, EviChain will use Pinata, an IPFS pinning service. Pinata attempts to make files persist on IPFS by pinning them on multiple nodes, thereby ensuring availability, fault tolerance, and permanency.
- **Linking Evidence and Blockchain:** The cryptographic hash of every file stored in IPFS will be linked on the Ethereum blockchain to a respective entry in the smart contract, allowing the retrieval of the file and further verification of the integrity of the file without storing it on-chain.

3. Fraud Detection Algorithms

The very essence of EviChain is put under jeopardy if the digital evidence loses its authenticity. Therefore, EviChain intends to build-in AI-based fraud detection systems with machine learning and computer vision apparatus to check evidence in text, image, and video forms for tampering or faking.

- **Image and Video Forensics using CNNs:** Convolutional Neural Networks will be used to identify image and video tampering. Such models can detect pixel-level irregularities, indicators of deep fakes, signs of image splicing, and other kinds of manipulations. Hence, models shall be trained and tested via datasets comprising tampered and bona fide media.
- **Temporal Analysis via RNNs:** Recurrent Neural Networks (RNNs) and their variants (such

as LSTMs or GRUs) will be used for sequential data such as videos to detect irregular transition of frames or temporal inconsistencies suggestive of video editing or forgery.

- **Natural language processing (NLP):** Textual evidence will be scrutinized via NLP techniques to highlight anomalies, including contradictions, inconsistent document formatting, plagiarism, or unnatural phrasing. spaCy, Transformers (BERT/DistilBERT), and n-gram analysis will extend the framework.
- **OpenCV for Preprocessing:** Preprocessing such as image enhancement, edge detection, noise filtering, and metadata extraction will be carried out by the OpenCV library, which will further aid in extracting key features for feeding into ML models.
- **Frameworks and Libraries:** We will use Python-based AI and ML libraries such as TensorFlow, Keras, and PyTorch to develop the models. These libraries, with their powerful set of tools for designing, training, and deployment of models, provide support for GPU acceleration and training on the cloud.

4. Security, Privacy, and Crypto

Security and privacy stand paramount in any evidence management system, particularly one imbibing sensitiveness, quite possibly weighing high on the stakes.

- **Zero-Knowledge Proofs (ZKPs):** To maintain total anonymity of the user without compromising system integrity, EviChain shall try Zero-knowledge proofs; these would allow a user to prove that their claim is valid without revealing anything about the data over which their claim is made. For example, a user may prove that they are a bona fide whistleblower without revealing their personal identity and/or metadata.
- **Public Key Infrastructure (PKI):** Submitters and verifiers will use public-private key pairs to sign and verify interactions with the system, ensuring non-repudiation and secure communication.
- **End-to-End Encryption:** Evidence shall be encrypted before uploading to IPFS. Although IPFS is a decentralised system, encryption would ensure that the file content is accessible only to authorised stakeholders using the decryption key.
- **Audit Logs and Immutable Trails:** These logs can be captured for every action performed, such as the uploading of files, and verification, all of which will be time-stamped on-chain and create an auditable and transparent trail of all events concerning a piece of evidence that the stakeholders can refer to with faults of anonymity.

3.1.3 CHALLENGES IN SPECIFIC REQUIREMENTS FULFILLING

While the EviChain platform proposes a technologically robust and innovative approach to decentralized evidence management, several implementation challenges must be overcome to ensure its practical viability, scalability, and usability. These challenges span across blockchain limitations, machine learning complexities, user experience considerations, and the delicate trade-off between privacy and transparency.

Blockchain Constraints:

Even though Ethereum provides a secure, decentralized infrastructure with established tooling and developer support, it has notable barriers that lower the efficiency of the EviChain platform:

- **Transaction Speed:** Average transaction throughput of Ethereum (~15–30 transactions per second) means delay due to heavy traffic periods. Such a delay affects real-time operations like urgent submission of evidence or verification.
- **Gas Fees:** Gas fees are very dynamic and high during network congestions. The conventional high gas fees can even deter end users, thus affecting the accessibility and affordability of a platform.
- **Scalability Bottlenecks**: Storage of metadata and hash values on-chain needs an optimized mechanism to avoid bloating the blockchain. Any unfeasibly optimized smart contract will increase gas usage, which in turn will affect cost and performance.
- **Mitigation Strategy:** To mitigate these problems, the platform will try to incorporate various Layer 2 scaling solutions such as Polygon, Optimism, or zkSync; these solutions, operating on the layer above the Ethereum mainnet, offer off-chain instant transaction processing and almost negligible gas fees. A trade-off with integration, however, is the added complexity in contract development and user wallet compatibility.

Fraud Detection Complications:

Some technical hurdles exist when building stronger fraud detection mechanisms with multimedia and textual evidence that stem mainly from the variety and complexity of tampering techniques:

- **Differentiated Evidence Modalities:** Different evidence types (images, videos, audio files, text documents) require different preprocessing pipelines, representations of data, and different machine learning models. For example, one might use a CNN to analyze pixels in a doctored image, while text inconsistencies could be identified through NLP and transformer models.

- **Data Availability and Annotation:** To build effective fraud detection systems, large annotated datasets with real or fake samples are required. Such datasets are rare to come by, especially for sensitive or legal evidence, owing to ethical and privacy concerns.
- **Model Generalization:** The attack techniques change fast. AI models need to be prepared for generalizing past the manipulation techniques they have ever witnessed in the training process. A continuous tugging of war will, therefore, still remain between precision and flexibility.
- **Computational Requirements:** Training and running AI applications, especially deep learning ones (e.g., CNNs, RNNs, Transformers), need substantial computational power. This may pose problems in ensuring the time verification process will always remain accessible to all."
- **The strategy of mitigation:** Modularity, building into task-specific modeling, continual learning, and cloud-based inference infrastructure, will aid in retaining precision and responsiveness in the solution. Tools like OpenCV, TensorFlow, and PyTorch can be used in developing scalable AI pipelines and integrating them with the solution.

User Adoption and Complexity of interface End user:

Without rise to anyone, blockchain technology-while very secure and transparent-reaches users unfamiliar with and afraid of fragile adoption barriers:

- **Limited Public Understanding:** Many persons are unsure about the way blockchain works or what makes it believable enough. Concepts like “wallet,” “gas fee,” and “hash” can be intimidating to average users especially legal, civic, or investigative domains.
- **Complicated Transactional Flow**: Users may be required to perform several steps when using blockchain-based platforms, including installing the wallet, connecting to the dApp, signing transactions, and paying the gas fees. Hence, these steps might rather be found to be cumbersome, removed from smooth onboarding.
- **Mitigation Strategy:** EviChain will operate with a user-centric approach to design that hopes to remove the perceived complexities of blockchain for its users. A clean, crisp, and intuitive front-front-end will be designed for users through frameworks like Next.js, providing handy tooltips, onboarding walkthroughs, and error handling during evidence submission and verification. Other features to ease interface interaction may include the potential use of gasless transactions or meta-transactions (through relayers).

Restoring and Preserving Data Privacy

Inherent complexities exist in preserving user privacy and maintaining verifiability:

- **Conflicting Purposes:** The blockchain is immutable and transparent by design, with possibilities opposing user preferences of anonymity, at least in cases like the protection of identity for whistleblower reports or sheltering confidential submissions. Traceability is demanded for verification and the establishment of accountability.
- **Re-identification Risk:** Even without the presence of PII (Personally Identifiable Information), some on-chain activities and metadata patterns can, through cross-referencing, inadvertently allow for the deanonymization of users.
- **Mitigation Strategy:** Balancing transparency with privacy calls for the use of advanced cryptographic techniques. Zero-Knowledge Proofs (ZKPs) is one of the best candidates for solutions: the user can prove ownership or acceptance of some information without ever revealing what that information is. Furthermore, to facilitate highly granular control over identity and data sharing, the platform may introduce anonymous credentials, one-time-use addresses, and selective disclosure protocols.

Data Privacy vs. Evidence Verifiability

The dual requirements of maintaining the confidentiality of users and ensuring verifiability and authenticity of the submitted evidence present a never-ending problem.

- **Regulatory Concerns:** The platform should first conform with data protection laws such as GDPR, which implies that users have the right to be forgotten-this conflicts directly with the immutability principle of the blockchain.
- **Encryption Complexity:** Encrypting the evidence prior to uploading it to a decentralized storage system such as IPFS ensures confidentiality; however, a bigger problem arises regarding managing the encryption keys: if a key is lost, then access to critical evidence is lost forever.
- **Mitigation Strategy:** Hybrid architecture can be chosen, whereby sensitive files are encrypted on the client side and subsequently stored on IPFS with only encrypted hashes and metadata committed to the blockchain. Cryptographic key-sharing mechanisms, such as Shamir`s Secret Sharing or threshold encryption, guarantee that multiple stakeholders must collaborate to decrypt files considered sensitive, thus eliminating single points of failure.

3.2 PROJECT DESIGN AND ARCHITECTURE

The EviChain platform is geared toward providing a digital evidence platform that is decentralized, secure, and scalable for purposes of storage, verification, and fraud detection. The architectural goal is to ensure tamper-proof handling of evidence and seamless user interaction, along with intelligent fraud detection mechanisms, carefully balancing transparency with privacy requirements. We now lay out the overall design along with an analysis of the major architectural components underpinning the platform's functionalities.

3.2.1 HIGH-LEVEL DESIGN

The High-Level Design of the EviChain specifies a design concept built for modularity and for the interoperability of decentralised technologies with intelligent computing. Each core component is truly crucial in achieving the system objectives:

1. Blockchain Network for Evidence Validation

The EviChain employs the Ethereum blockchain at the center, a well-adopted copy-resistant decentralized platform that offers the features of smart contracts and security. It helps in registering the cryptographic hash of submitted evidence and timestamp, along with the address of the submitting user (using wallet IDs). Smart contracts are written in Solidity; hence, once deployed, they enforce the protocol rules autonomously for evidence submission, requests for access to evidence, and the evidence validation procedure.

Smart contracts enforce these processes autonomously:

- Evidence submission
- Hash storage
- Hash retrieval
- User verification
- Interaction logging

Hence, an entry recorded on the ledger cannot be altered, so the integrity of the evidence is preserved because the ledger is tamper-proof and transparent.

2. Decentralized Storage of Evidence Files

For costly and restrictive storage of large files on-chain, IPFS is used by EviChain for decentralized file storage. IPFS guarantees that:

- Distributed content addressing is done through cryptographic hashes (CIDs)
- High availability granted through network replication
- Data immutability once published

Files would be uploaded to IPFS; the CIDs of which get then recorded or set forth on Ethereum. Pinata is incorporated as a pinning service to allow files to stay persistently available on the IPFS by preventing garbage collection.

3. Fraud Detection and Validation of Authenticity

EviChain utilizes high-end models employing artificial intelligence for fraudulent and tampered evidence. Systems support for:

- Image and Video Analysis: Detection of pixel-level or frame-level tampering with OpenCV and CNNs.
- Text Analysis: Use of NLP to detect unusual patterns, semantic inconsistencies, and indications of textual manipulation.
- Model Training: Fraud detection models were trained using TensorFlow or PyTorch on labeled datasets of genuine and forged samples. The models are continuously refined through feedback loops and user flagging.

4. UI for Smooth Interaction

The frontend is created with Next.js, a React-based framework that focuses on performance and scalability while also providing SSR features. It offers:

- Nice-looking clean dashboard for evidence submission
- File upload with live hash generation
- MetaMask integration for blockchain operation
- Real-time status update on evidence verification

3.2.2 ARCHITECTURE COMPONENTS

EviChain modules are structurally made to make everything flexible, scalable, and secure. The important components of the entire system include the following:

User Interface (Frontend):

Technology Stack: Next.js + CSS + Web3.js/Ethers.js

Functionality:

- Uploading evidence files
- Change display of verification results
- Connect to wallet using MetaMask
- Viewing evidence history and blockchain logs

Design Focus: Was on ease of use, responsiveness, and minimum learning curve for either a legal or a non-technical person.

Smart Contracts (Blockchain Layer):

- Language: Solidity
- Responsibilities:
  - Handle evidence submission logic
  - Store immutable records of the evidence hash, timestamp, and the ID of the submitter
  - Provide access control and verification endpoints
- Security: Contracts are audited and hardened against common vulnerabilities (e.g., reentrancy, integer overflows)

Smart Contract Interaction:

- Purpose: It fosters two-way interactions between the frontend and the blockchain.
- Integration:
  - Use Ethers.js/Web3.js to call the smart contracts' methods
  - Listen to events for real-time feedback from the blockchain
  - MetaMask signs and broadcasts transactions securely

Decentralized Storage (IPFS):

- Function: Storing actual evidence files in a decentralized fashion
- IPFS Contributions:
  - Gives unique CIDs to files
  - Checks for content integrity by hash-based addressing
- Pinata Services:
  - Scores the content legally and compatibility.

    - Administers Content Without Worries About Durability.

Fraud Detection Layer:

- Machine Learning (ML):
    - Image and video tampering detection via CNNs and optical-flow analysis.
    - Signature Verification using CNN and ANN.
- Frameworks Used: TensorFlow, PyTorch, Scikit-learn, OpenCV.
- Model Output:
    - Classification (forged vs. real)
    - Confidence scores for every prediction

Authentication & Anonymity Layer:

- Cryptographic Techniques:
    - Zero Knowledge Proofs (ZKPs): Serving as verification pieces of evidence without ever disclosing an identity
    - Elliptic Curve Cryptography (ECC): Provides digital signatures and wallet interactions during transaction processing
- User Identity Handling:
    - Users will interact with MetaMask via publicly identified Ethereum addresses
    - No KYC is required, ensuring users' anonymity
    - Private information will also never be stored on-chain nor kept in plaintext

3.3 DATA PREPARATION

Data preparation plays a major role in the successful functioning of the EviChain platform. Because of the processing of sensitive and legally significant kind of digital evidence, an evidence file with related user information has to be prepared with utmost care so that their integrity remains assured, and further so that the evidence arrangement, through a fraud detection system, is compatible to be realized along with the blockchain system. Henceforth, the present section focuses on detailing the data preparation process that occurs in many phases, including evidence ingestion, machine learning preparation, handling user information, and integration onto the blockchain.

3.3.1 EVIDENCE DATA COLLECTION AND PREPROCESSING

Digital evidence submitted to EviChain might consist of images, video footage, documents (such as

PDFs or Word files), and textual descriptions. Problems remain different in processing and security needs for these myriad formats and must be treated by separate, standardized workflows.

Normalization and Standardization

The working principle consists in treating all types of evidences equally in order to guarantee effective operation:

Images and videos are sized to a consistent resolution (for example, 256x256 or 512x512) while being converted into generic format JPEG, PNG, or MP4.

Textual documents are reviewed for the following cleaning operations:

- ○ Elimination of characters and symbols other than standard
- ○ Correction of OCR artifacts
- ○ Standardizing the encoding (UTF-8)
- ○ Sentence segmentation and structural normalization

This way, all input data becomes suitable for subsequent modules, including machine learning models, hash generators, or IPFS storage.

Cryptographic Hashing

Each evidence file is hashed using SHA-256, creating its fixed-length dependent cryptographic digest (hash). The hash serves as:

- ○ A digital fingerprint of the file
- ○ A means to verify its integrity
- ○ An immutable reference recorded on the Ethereum blockchain.

If anything is changed in the evidence file, down to one byte, a completely different hash will be generated, and so tampering is detected instantly.

Encryption of Sensitive Evidence

In cases when evidence may contain PII or information that is private, then this information is encrypted prior to storage:

- ○ Symmetric cryptography (AES-256 for example) is applied to functionally secure the content.
- ○ Hence, only authorized viewers, say, legal authorities, having the respective decryption keys

will be able to open the data.

- This encryption scheme combined with IPFS and smart contract metadata provides traceable private access.

3.3.2 DATA FOR FRAUD DETECTION

In order to generate strong and effective fraud-detection models, a carefully curated and preprocessed dataset is required, containing both genuine and manipulated evidence across all formats.

Nature of Training Data

- Images: Original unaltered images, and tampered images made by copy-move, splicing, blurring, morphing, etc.
- Videos: Alteration of frames, signature detection, time-based forgery.
- Text files: Forged documents with syntactic or semantic inconsistencies, plagiarism, or changes in metadata.

All datasets have labels: either genuine or tampered, which serve as a ground truth for supervised learning models.

Data Augmentation

To improve model generalizability and prevent over-fitting:

- For images, augmentation includes rotation, scaling, flipping, addition of Gaussian noise, and brightness changes.
- For videos, augmentation simulates compression artifacts, frame duplication, or frame corruption.
- For text, augmentation includes synonym replacement, paraphrasing, random insertions/deletions-as methods to mimic forged contents.

Such augmentations all mirror real-world manipulation techniques-the more subtle the cues of fraud, the more able the models are to detect them.

Balancing the Dataset

Digital forensic datasets are often unbalanced in nature, having far more examples of genuine data as compared to tampered ones. This skew can adversely affect machine learning models.

Possible solutions thereby include:

- Oversampling, such as by SMOTE (Synthetic Minority Oversampling Technique), to generate more tampered data samples.
- Using Generative Adversarial Networks (GANs) for synthesizing fake-but-realistic evidence, mostly in the image and video domains.
- Selective undersampling of the dominant classes (genuine samples) to allow for class balance without loss of essential sample diversity.

Balanced datasets then lead to better model accuracy, recall, and robustness in production environments.

3.3.3 MANAGING USER INFORMATION

User data is a crucial aspect to enable interaction with the EviChain platform while making sure accountability, integrity, and user privacy are upheld.

USER DATA COLLECTION

Users provide very minimal metadata during evidence submission:

- Email address: For communication and/or recovery (optional)
- Ethereum wallet address: To authenticate the identity through MetaMask
- Context for submission (optional): Might be a brief description or categorization of the evidence

Data that are personal are handled in a secure manner and are never put on-chain; therefore, privacy is maintained and the element of exposure risk is reduced.

PRIVACY AND ANONYMITY

EviChain takes a privacy-first approach by hiding the identity of either whistleblowers or contributors who wish to remain anonymous:

- Zero-Knowledge Proofs (ZKPs) are used to prove the validity of an action (e.g., evidence submission) without actually disclosing the identity of the user.
- Public-private key cryptography is used to authenticate without KYC, and all user actions are assigned only to anonymous wallet addresses.

Hence, this creates trust while respecting ethical standards and legal norms pertaining to privacy.

3.3.4 DATA STORAGE AND BLOCKCHAIN INTEGRATION

The platform bases itself on technologies like decentralization of storage and blockchain infrastructure to ensure availability, integrity, and immutability of evidence.

IPFS-Style Storage for Evidence

Evidence files are stored via a decentralized manner using the InterPlanetary File System:

- Files are uploaded, and have a Content Identifier (CID) generated, derived from the file's own content.
- These CIDs act as cryptographic addresses and are stored in Ethereum for traceability.
- Pinata is used for pinning them so that files are retained on the IPFS network, rather than being lost to garbage collection.

Advantages:

- Greatly reduces or eliminates any single points of failure
- Ensures availability and tamper-proofness
- Efficiently scales across global nodes

Integrity & Verification via Blockchain

The Ethereum blockchain stores:

- Hashes of the evidence files (from IPFS)
- Timestamp of the submission
- Associated transaction metadata (from: sender address, smart contract reference)

Benefits include:

- Immutable audit trail for each submission and verification
- Comparing the current file hash with the on-chain hash verifies submission in real-time
- Access logs are transparent and can never be altered retroactively

Hence, this union of decentralized storage and blockchain provides an environment that is verifiable, trustworthy, and censorship-resistant for the handling of digital evidence.

3.4 IMPLEMENTATION

3.4.1 DESIGN OF PROBLEM STATEMENT

The design of EviChain is a carefully architected system that integrates blockchain technology, decentralized file storage, and artificial intelligence to solve the number of fundamental problems in digital evidence management while still ensuring security, verifiability, and privacy of digital evidence. The central problem it aims to solve is that evidence handling systems by traditional means are vulnerable to tampering, unauthorized access, and single points of centralized failure, all of which are compounded by the increased challenge coming from digitally altered or fake content.

The three pillars upon which EviChain is based to resolve it are:

1. Blockchain-Based Storage for Metadata and Integrity

One of the crucial issues in digital evidence management is to ensure that once a piece of evidence has been submitted, it cannot be tampered with or deleted without a trace. EviChain addresses this by using the Ethereum blockchain to store the metadata of each evidence file:

- This metadata includes cryptographic hashes of the evidence file, timestamps of submission, and transaction details that together provide a complete and verifiable history.
- As blockchain records cannot be altered, they thus create a permanent record, allowing the guarantee of evidence integrity from submission onwards.
- Smart contracts record and validate this information in an automated fashion, without requiring manual validation or centralized trust.

In this way, the system provides full transparency, traceability, and proof against others modifying the record, making it apt for legal and forensic purposes.

2. Decentralized File Storage Using IPFS and Pinata

The blockchain is great for storing metadata and hashes but due to cost and size constraints, storing an image, video, or document is not feasible. EviChain, therefore, addresses this conflict by interfacing with the InterPlanetary File System (IPFS), a peer-to-peer, content-addressable storage network:

- Once uploaded, files are pinned using Pinata Cloud to ensure permanence and availability on the IPFS network.
- The file will have a content identifier (CID) which is a unique cryptographic hash on a file's content and is used to refer to retrieval and verification.
- The Ethereum blockchain is then used to store the CID to link the evidence file to the immutable metadata record.

The model of decentralized storage:

- Avoids having to depend on centralized servers that could easily get compromised or censored.
- Ensures that data persistence and access redundancy are guaranteed
- Ensures if by any chance a server is recently taken offline, the evidence will now be made accessible via other IPFS nodes.

Through this system, EviChain establishes a digital evidence storage infrastructure that is tamper-proof and censorship-resistant.

3. AI-Based Fraud Detection Mechanism

With the rising levels of sophistication in digital forging methods, from deepfakes to synthetic documents and manipulated metadata, the need for some automated means of ascertaining whether the submitted evidence has indeed been tampered with or forged has become quite pressing. EviChain incorporates machine learning-based fraud detection logic trained on datasets consisting of genuine evidence and the same, after having been tampered with:

- With image and video data, the models look into noise patterns, instances of inconsistencies in lighting or shadows, artifacts of edge blending, and irregularities in compression.
- With documents, the AI scrutinizes the consistency of fonts, anomalies in the layout, embedded metadata, and signs that could point to OCR-ing or manual editing.
- With text, NLP techniques come into play to unveil semantic inconsistencies or artificially generated content.

This AI layer offers:

- A preliminary harassment score at submission
- Flags suspicious submissions for further human or legal scrutiny
- The models improve continuously with feedback and by re-training on verified cases

EviChain thus goes a long way in keeping fabricated, altered, or misleading content from entering the system by adding an AI-based verification layer in the pipeline.

3.3.2 DATA FLOW DIAGRAMS

The design of EviChain revolves around: blockchain-based storage, decentralized file storage using

IPFS, and a fraud detection mechanism as shown in the Figure 3.1.

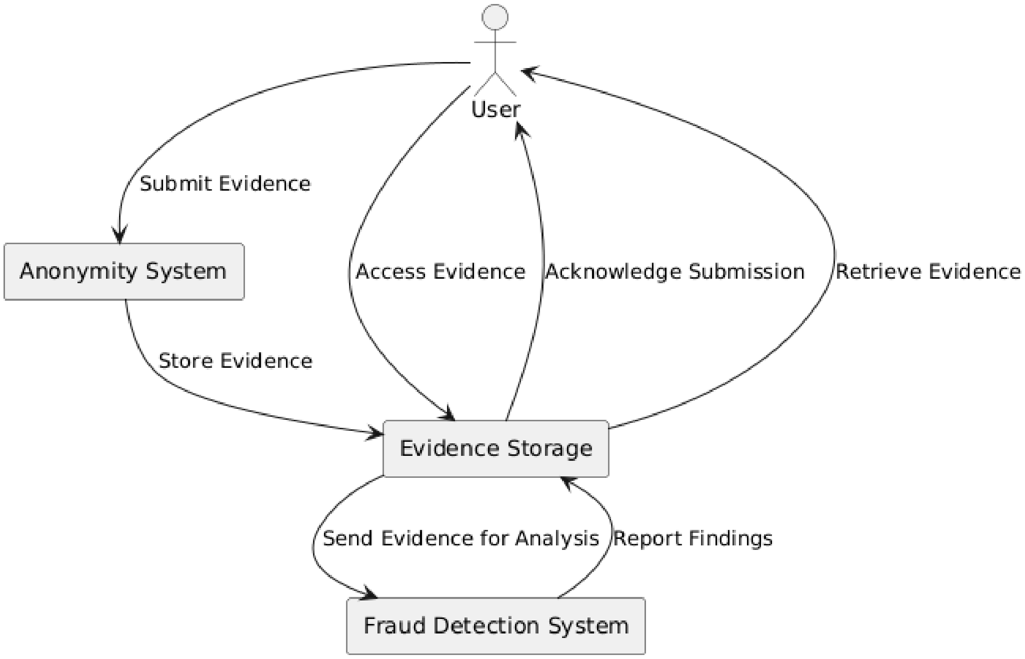


Figure 3.1 : Evichain (Blockchain and Fraud Detection System)

Blockchain ensures immutability and transparency by recording evidence metadata and proof hashes on the Ethereum network. For actual evidence files, the platform uses IPFS (InterPlanetary File System) integrated with Pinata Cloud to provide a scalable, tamper-proof storage solution. Additionally, the project incorporates AI-driven fraud detection algorithms to analyze and verify the authenticity of evidence, reducing the risk of fabricated or manipulated data.

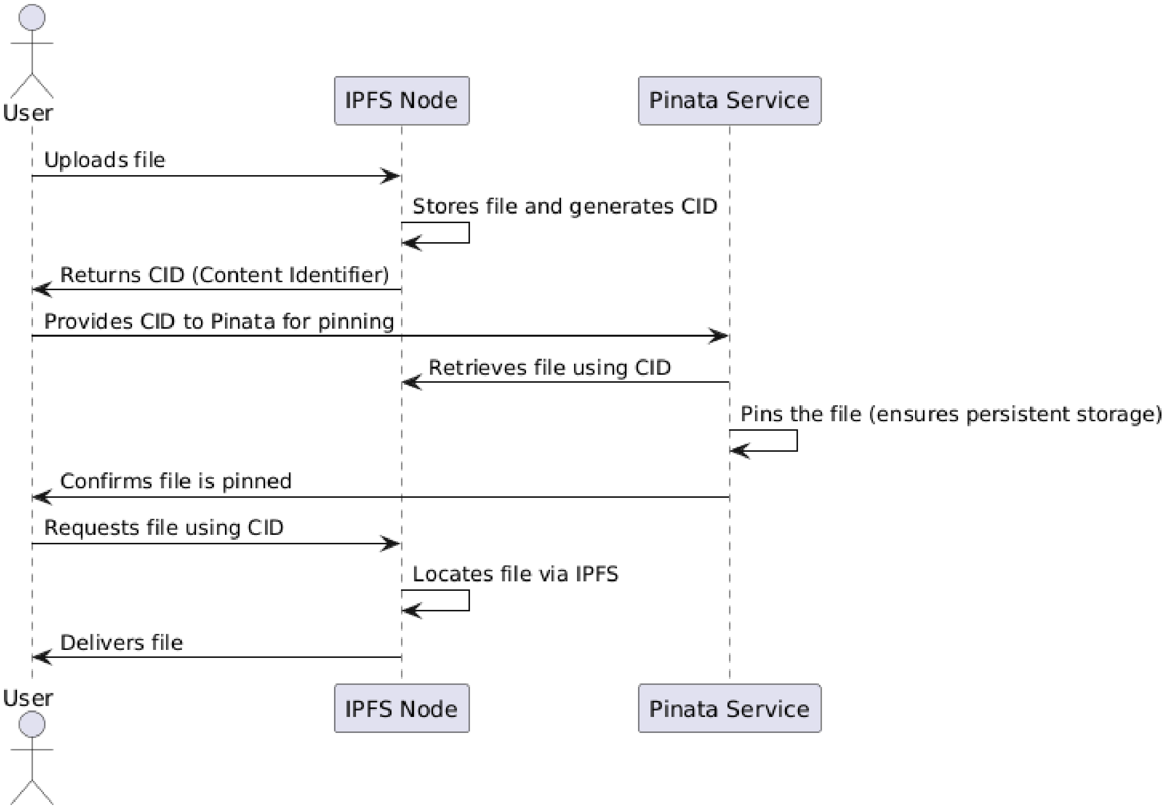


Figure 3.2 : Storage Mechanism And Smart Contract

The diagram in Figure 3.2 provides an example of files being stored and recovered via the use of IPFS (InterPlanetary File System) and the Pinata Service. The whole process starts with a file uploaded by a user to the node of the IPFS system; it saves the file and also generates the unique Content Identifier (CID) for the respective user. This CID is then sent to Pinata for storing it persistently. Pinata pins this file in the IPFS network and ensures a long time of availability and a file being confirmed pinned by Pinata. In this case, the user requests a file using its CID, which is available from the IPFS node for returning that file to the user ensuring a decentralized and safe storing possibility.

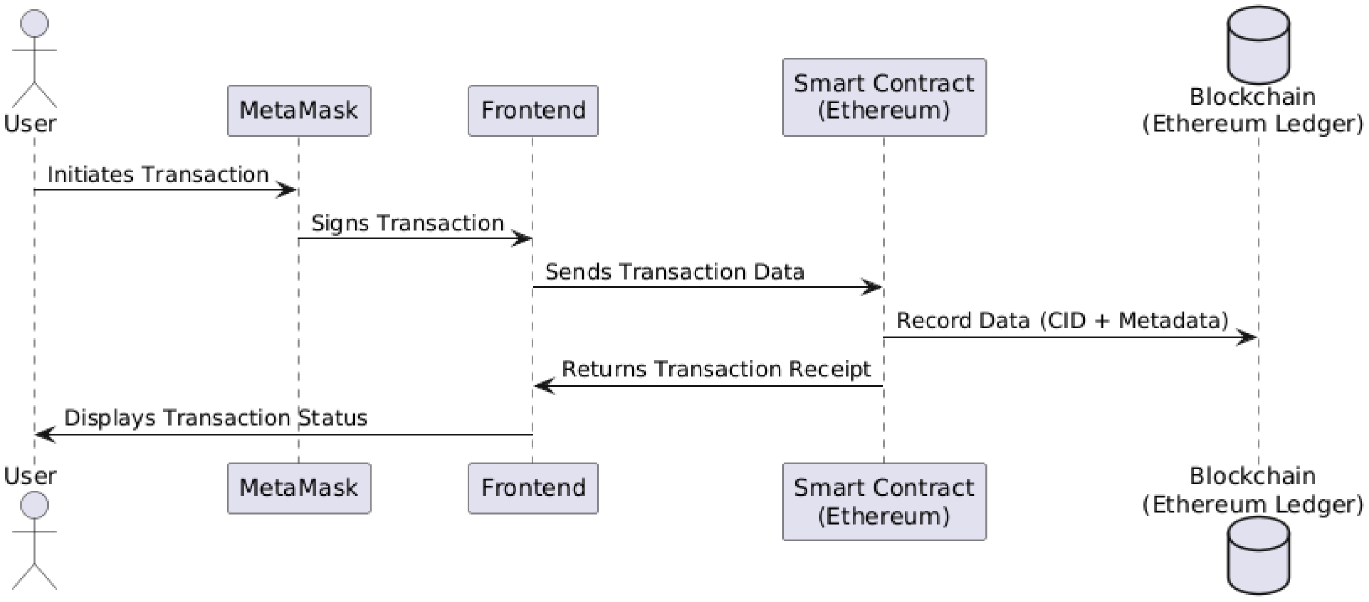

User
MetaMask
Frontend
Smart Contract (Ethereum)
Blockchain (Ethereum Ledger)
Initiates Transaction
Signs Transaction
Sends Transaction Data
Record Data (CID + Metadata)
Returns Transaction Receipt
Displays Transaction Status
User
MetaMask
Frontend
Smart Contract (Ethereum)
Blockchain (Ethereum Ledger)

Figure 3.3 : Blockchain Transaction

The transaction is processed by MetaMask, as seen in the sequence diagram in Figure 3.3 , and is further recorded using smart contracts on Ethereum. In this case, the user initiates a transaction via its frontend, calling MetaMask to sign the transaction. The smart contract processes the signed transaction data and CIDs (Content Identifiers) recorded along with the associated metadata on the blockchain (Ethereum ledger). Finally, the smart contract returns a transaction receipt to the frontend. The frontend application displays the results of this operation to the user based on the information received from the smart contract, ensuring confirmation and transparency of the operation.

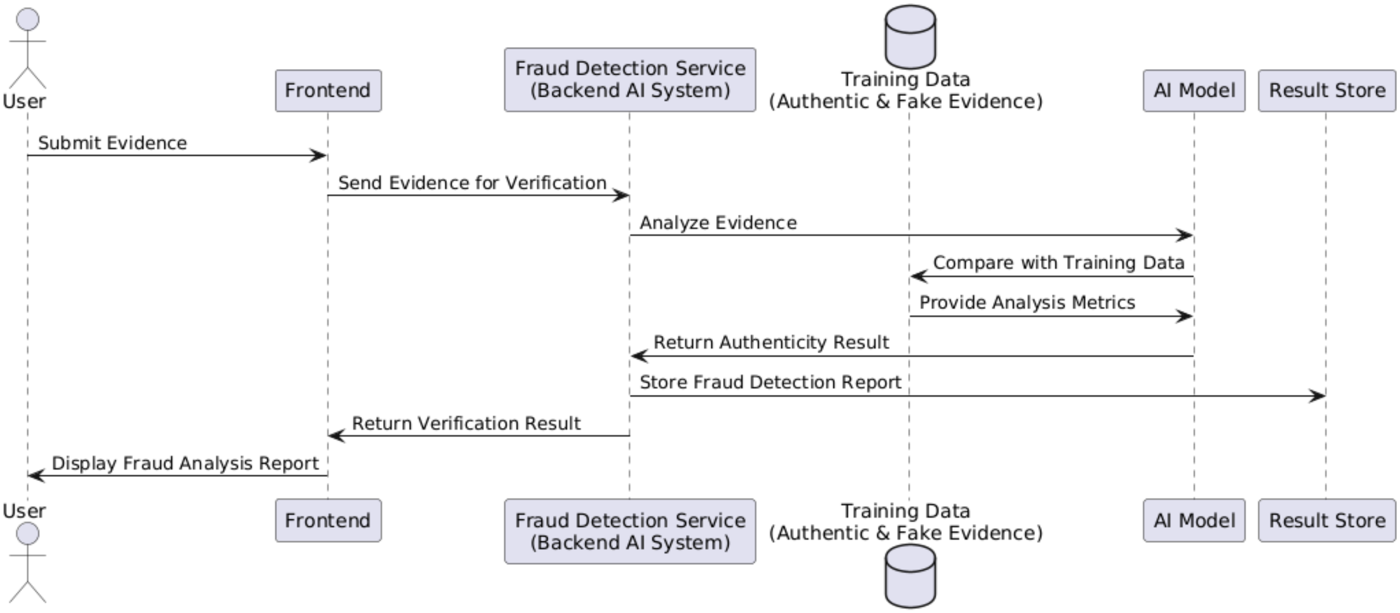


Figure 3.4 : Fraud Detection Model

The sequence diagram in Figure 3.4 displays a workflow of the Fraud Detection Model in which the user submits his/her evidence through the frontend for verification. The evidence is forwarded to the Fraud Detection Service, which applies this AI Model to analyze it. The model therefore compares the evidence against a different Training Dataset of both original and forged evidence, in order to assess how real that evidence is. With that, generated metrics can then be used to gauge whether the evidence is true or forged. The result is then saved in the Result Store for record-keeping. The return of the fraud analysis report occurs on the frontend, thus ensuring that the user sees a clear and transparent verification process

3.5 KEY CHALLENGES

The deployment of EviChain, which is a decentralized platform for evidence storage and fraud detection through AI, requires dealing with a series of complex technical, infrastructural, and consumer-centric problems. These challenges cut across all technology integration, system optimization, user privacy, and viability from an operational standpoint. To ensure that EviChain can stand out as a sturdy, scalable, and trusted solution in the arenas of legal procedures, digital forensics, and regulatory compliance, all these must be duly handled.

1. Blockchain and IPFS Integration

Integrating blockchain with IPFS-induced by lack of documentary and verifiable support-constitutes one of the foremost technical challenges for EviChain:

- The blockchain is perfect for storing hashes and metadata but is inappropriate for storing large files on account of size limitations imposed and high transaction (gas) fees.
- IPFS, in contrast, is perfect for storing large media and document files but provides no inscription or timestamping mechanism.
- There is an intricate coordination required in the operation of these two technologies to ensure that:
    - An IPFS CID is properly recorded on the blockchain in an immutable matter.
    - The content stored and indicated by the hash does not mismatch.
    - The content stays alive and retained throughout its entire lifecycle because unfixed structure on IPFS penalizes it from being retained by the network.

2. Scalability Problems and Blockchain Performance Capabilities

There are scalability problems to be dealt with when the number of users and the amounts of evidence submitted increase. They include:

- Very high gas fees during periods of network congestion make it financially impossible to submit evidence constantly or frequently, including its verification and updates.
- Delays in transaction submission and its confirmation of evidence may violate timeliness for some legal or regulatory actions.
- The present throughput level that Ethereum offers (especially mainnet) will not be capable of handling such frequent submissions unless some Layer 2 solutions or other scaling solutions are brought to play.

The mitigations to the problem, those being Layer 2 protocol options such as Optimism and Arbitrum, sidechains, or other blockchain alternatives, have to be carefully weighed for compatibility and security considerations.

3. Building an Effective Fraud Detection System

Offering a very powerful set of layered challenges to build a hardy and intelligent fraud detection mechanism:

Data Collection and Labeling

- Getting a large, diverse, labeled dataset of genuine and tampered evidence (image, video, document, and texts) is a hard-to-make feat.
- The tampered samples must be made to mimic actual forgeries: signature detection, document

edits, and manipulation of media metadata.

Model Generalization and Adaptability

- As deceptive techniques evolve fast, models must remain adaptable to new tampering methods.
- Avoiding adaptation to a particular type of forgery should yield a system that performs with good generalization across unobserved manipulations.

Real-Time Detection and Accuracy

- Perhaps even more detrimentally, the system must have the ability to perform in real-time, a concept with a lot of constraints laid by the decentralized application (dApp) themselves.
- The trade-off between complexity and inference time of the model should be carefully stitched carefully to provide a flawless user experience.

4. Ensuring Privacy And Anonymity Without Compromising on Integrity

Balancing the issues of anonymity for users and evidence accountability introduces complex cryptographic and ethical issues:

- There has to be a means provided within EviChain for anonymous evidence submission while simultaneously checking for integrity and origin of the submission.
- Technologies such as zero-knowledge proofs (ZKPs) can ensure this kind of balance, but they are computationally heavy and this can introduce performance trade-offs.
- Likewise, applicable data protection laws (such as GDPR) require that any data relating to users is processed transparently, upon a duly given consent, and that such processing operations are capable of lawfully supporting investigations where the law so requires.

This balance of technical feasibility against privacy guarantees and against regulations must form the crux of the evaluation for such cases to be legally admissible and acceptable in an ethical perspective.

Chapter 04: TESTING

4.1 TESTING STRATEGY

In any software development process, testing plays a very crucial role, especially projects such as EviChain which involve handling sensitive evidence to ensure the integrity of data. EviChain itself integrates blockchain, fraud detection algorithms, and decentralized storage, and thus a robust testing strategy is required to ascertain the intended functioning and real-world usability of the platform in secure and practical situations. The testing strategy is divided into many categories such as unit testing, integration testing, system testing, performance testing, and security testing, with each category serving a specific function for the verification of correctness and robustness of the system.

Testing would be an essential part of any software development process, particularly those dealing with sensitive evidence, like EviChain, to guarantee the integrity of data. The project contains a combination of blockchain, fraud detection algorithms, and decentralized storage, which all require testing to come up with the most favorable plan for ensuring that the platform functions properly, remains secure, and is capable of real-life use cases. The plan involves several phases: unit testing, integration testing, system testing, performance testing, and security testing-all providing different aspects of the rightness and robustness verification of the system.

4.1.1 UNIT TESTING

Unit testing tests individual components or modules of a system in isolation on the understanding that part works when tested alone. For EviChain, these tests entail the following:

Smart contracts: These are core parts of the EviChain platform because they handle evidence submission and verification and communicate with the blockchain. The contracts must be controlled and functional, for which purpose unit tests are written in Solidity using Hardhat or Truffle Testing which checks for:

- Correct logic in handling transactions (e.g., evidence submission, verification, and storage)
- Validity of input and output (evidence hashes must be stored correctly and validated)
- It does not allow unauthenticated access (ensures valid users are permitted to submit evidence)
- Edge cases like invalid evidence or attempts to replace submitted files by unauthorized access should be handled.

Fraud Detection Algorithms:These fraud detection algorithms are implemented in Python using libraries like TensorFlow and Scikit-learn. Unit tests ensure that every algorithm works as expected:

- Image tampering detection/corruption (using CNNs).
- Video tampering/corruption detection (using RNNs).
- Text analysis algorithms for detecting fake or altered documents. Unit tests cover that each algorithm can classify evidence as real or fake.

Decentralized Storage: Since evidence will be stored in IPFS and Pinata will be used for file pinning, tests have to prove that the proof will be securely stored, and retrieval will be done as required. Unit tests will check that files are properly uploaded to IPFS and that their corresponding hashes are stored accurately on the blockchain.

4.1.2 INTEGRATION TESTING

Integration testing checks if all components of the EviChain system integrate well to form a whole working system. This is necessary because EviChain comes up with a lot of technologies and tools (in a way, example is using Blockchain, decentralized storage, machine learning algorithms, etc.) together for integration testing to ascertain that they do operate well upon connection.

Smart Contracts and IPFS Integration.All integration tests ensure that the evidence submitted by a user is successfully stored on IPFS and that the corresponding hash correctly appears on an Ethereum blockchain. This serves to check interactions across the blockchain, IPFS, and the submission process.

Fraud Detection and Evidence Submission:After evidence submission, storage, the authenticity of the evidence is to be evaluated by the fraud detection system. Integration tests assess whether this evidence subsequently passes entirely through the detection algorithms for analysis and classified accordingly. This would prove that the fraud detection system would handle data from both blockchain and IPFS, making reliable predictions concerning that evidence.

Blockchain and User Interface Interaction:Evaluation of the integration between the user interface (built under Next.js) and Ethereum smart contracts to ensure that a user can submit evidence or interact with blockchain to receive responses on the frontend. Verification of the user interface for communicating correctly with the blockchain backend.

4.1.3 SYSTEM TESTING

System testing means testing the entire system as a unit to prove that it conforms to the required specifications, in particular the functioning of the system in real-life scenarios.

End-to-End Workflow Testing:The end-to-end workflow is tested so that everything from evidence submission to its storage on IPFS and blockchain, as well as fraud detection and validation, is working in a seamless manner. Test scenarios include evidence submission, fraud detection application, and verification of the results on the blockchain. This would prove that the platform made the process possible from start to finish.

Functional Testing:System testing also includes functional feature testing of the system. This entails checking on the following aspects:

- Users can submit evidence and receive confirmation.
- Correct hashing and storage of evidence on the blockchain.
- Resultant accuracy of fraud detection algorithms according to evidence types.
- Secure evidence that is retrievable when needed.

Non-Functional Testing:System testing also goes beyond functional testing to non-functional requirements that include performance, security, and scalability. These are vital for ensuring that the system can accurately accommodate high evidence submissions and retrieve them within a reasonable time.

4.1.4 PERFORMANCE TESTING

Performance testing defines performance of a system under different scenarios, such as heavy or high traffic conditions. Since EviChain would have to deal with big files and a lot of users, performance testing is very critical for ensuring that scalability exists.

Load Testing:Load tests are conducted to simulate many concurrent users and file uploads to evaluate system performance under stress. Thus, performance under heavy, multi-transaction load can be determined. Apache JMeter or Gatling may be used to create thousands of users interacting with the platform.

Stress Testing:Pushed beyond its threshold of capability, stress testing determines the breaking point of the system, above which its resources are maxed out, such as in cases where requests place an overload on the Ethereum blockchain or IPFS storage. This tests the platform's capacity to weather extremes.

Scalability Testing: Systems show how well the system scales as users, files, and data increase because these are the important aspects of testing concerning scalability tests. It is important especially for a decentralized such as EviChain, as the system can potentially fail due to scalability limitations from the blockchain (transaction throughput) and centralized storage (file retrieval speed).

4.1.5 SECURITY TESTING

Security is of utmost importance in any project dealing with sensitive evidence. Security testings ensure that the platform is invulnerable to various attack vectors such as hacking, fraud, and unauthorized access.

Smart Contracts Security: Smart Contracts are to be tested for security vulnerabilities such as re-entrancy attacks, integer overflow and gas limits. Tools like MythX or Slither are often employed for checking the smart contract code for such vulnerabilities.

Penetration Testing: Penetration testing is performed to discover potential vulnerabilities at the system level-as with everything, including front-end, back-end and block-chain. Simulated attacks are performed by ethical hackers to analyze the toughness of the security measures the platform has put in place.

Testing by Data Privacy and Encryption: Because the platform handles sensitive evidence, tests have been conducted to verify that user data are encrypted correctly and accessed only by authorized users. This includes checking the implementation of encryption algorithms for data stored on IPFS and verifying the integrity of encrypted evidence files.

Chapter 05: RESULTS AND EVALUATION

This chapter presents the outcomes/results of the EviChain project and also evaluates its performance aligned to the defined objectives. The results have been categorized into different aspects of the system, including the decentralized evidence storage mechanism, fraud detection capabilities (signature verification system) , and overall system efficiency.

5.1 DECENTRALIZED STORAGE RESULTS

The introduction of the IPFS for evidence storage has ensured decentralized, secure and tamper-proof storage of data. Pinata Cloud provided an additional advantage of pinning files in IPFS for continuous data retention and sharing. Different tests confirmed that the system could create different CIDs and fetch files with an incredibly low overhead delay, thus providing a scalable system for the storage of digital proofs and evidence.

This experimental implementation of IPFS (InterPlanetary File System) as evidence storage has actually ensured decentralized, secure and tamper-proof storage of data. Users are able to safely connect their already existing Metamask account or create a new Metamask account and leverage the feature of using the vault. It provides a durable and trustworthy option for the user to store files as evidence which are highly concerning.

Alongside this for document verification fraud detection , we implemented a signature verification system, that verifies the signature from already existing signatures , predicting it to be real or forged on the basis of a CNN and ANN model. Although there is a lot of scope of improvement in it as it doesn’t work as good as for the unseen images or patterns giving false outputs. This is due to the limitation of computational strength and dataset limitations.

5.2 USER FEEDBACK

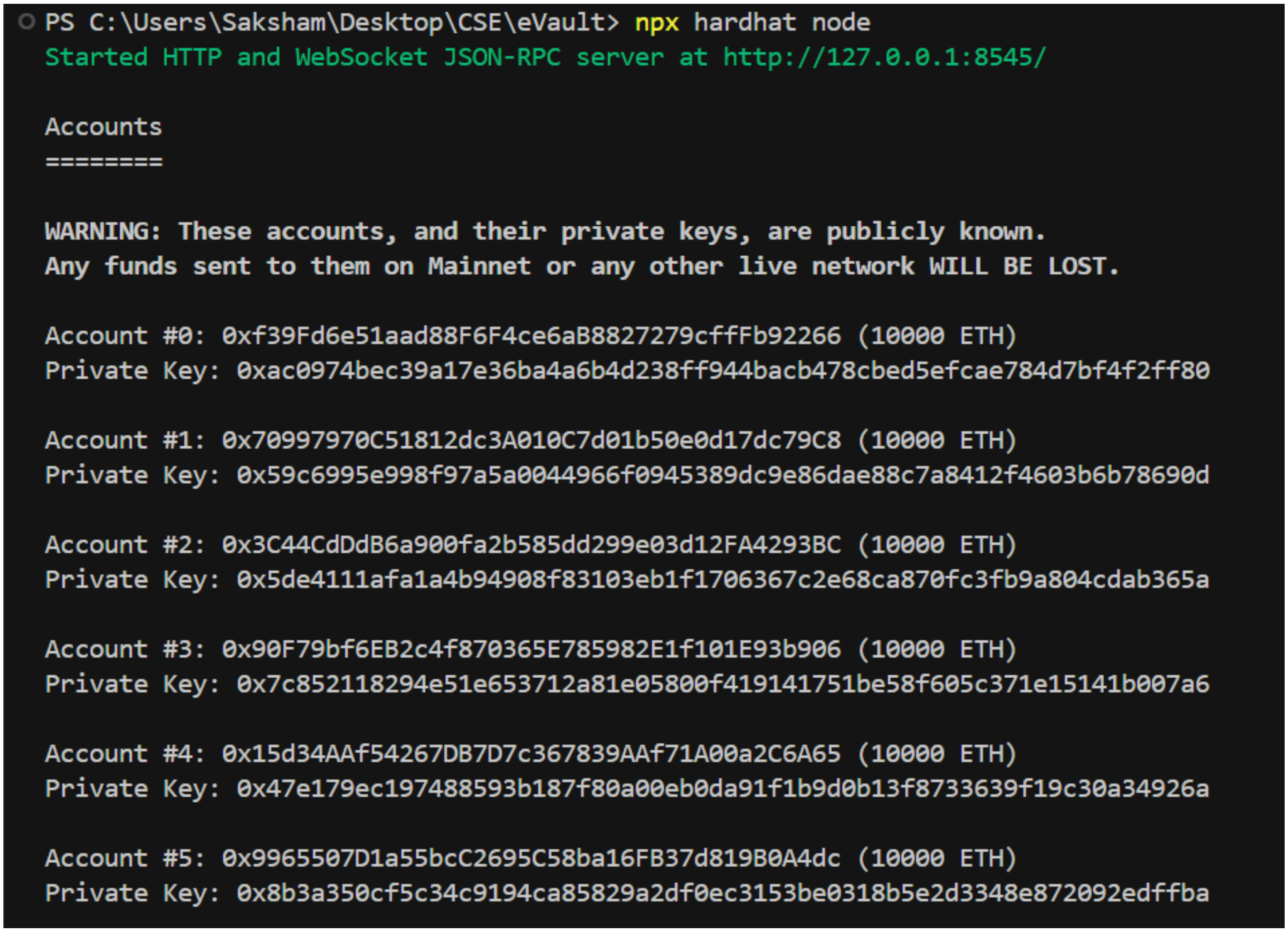
It was carried out user testing with the aim of evaluating usability and reliability within the platform. The comments were made in terms of the access to the blockchain using the MetaMask wallet and the simple and easy-to-use user interface in conjunction. Improvements were, however, suggested on speed and cost economics of transactions. We have then working on reducing the computational complexity of the smart contract by rewriting the functionalities, automatically reducing the speed and cost of transaction.

5.3 RESULTS

This successful decentralized and tamper-proof evidence storage solution is achieved through the integration of the InterPlanetary File System (IPFS), while the presence of Pinata Cloud offers robust data persistence and durability within the IPFS network for a longer time. System testing has been able to verify that EviChain is capable of generating unique Content Identifiers (CIDs) for each entry/transaction in an efficient manner and also enables retrieval and sharing of files or evidence with lesser delay. Thus, the approach of EviChain becomes scalable for secure digital proof storage systems.

5.4 SCREENSHOTS

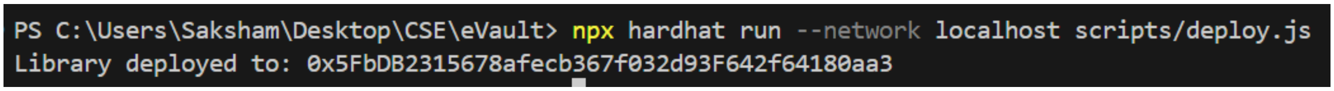
Following are the screenshots from the project Evichain showcasing all the work done as in front-end as well as back-end emphasising on clear understanding of the project.



```
○ PS C:\Users\Saksham\Desktop\CSE\eVault> npx hardhat node
  Started HTTP and WebSocket JSON-RPC server at http://127.0.0.1:8545/

  Accounts
  ========

  WARNING: These accounts, and their private keys, are publicly known.
  Any funds sent to them on Mainnet or any other live network WILL BE LOST.

  Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266 (10000 ETH)
  Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80

  Account #1: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8 (10000 ETH)
  Private Key: 0x59c6995e998f97a5a0044966f0945389dc9e86dae88c7a8412f4603b6b78690d

  Account #2: 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC (10000 ETH)
  Private Key: 0x5de4111afa1a4b94908f83103eb1f1706367c2e68ca870fc3fb9a804cdab365a

  Account #3: 0x90F79bf6EB2c4f870365E785982E1f101E93b906 (10000 ETH)
  Private Key: 0x7c852118294e51e653712a81e05800f419141751be58f605c371e15141b007a6

  Account #4: 0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65 (10000 ETH)
  Private Key: 0x47e179ec197488593b187f80a00eb0da91f1b9d0b13f8733639f19c30a34926a

  Account #5: 0x9965507D1a55bcC2695C58ba16FB37d819B0A4dc (10000 ETH)
  Private Key: 0x8b3a350cf5c34c9194ca85829a2df0ec3153be0318b5e2d3348e872092edffba
```

Figure 5.1 : Successful Execution Of Hard Hat Blockchain

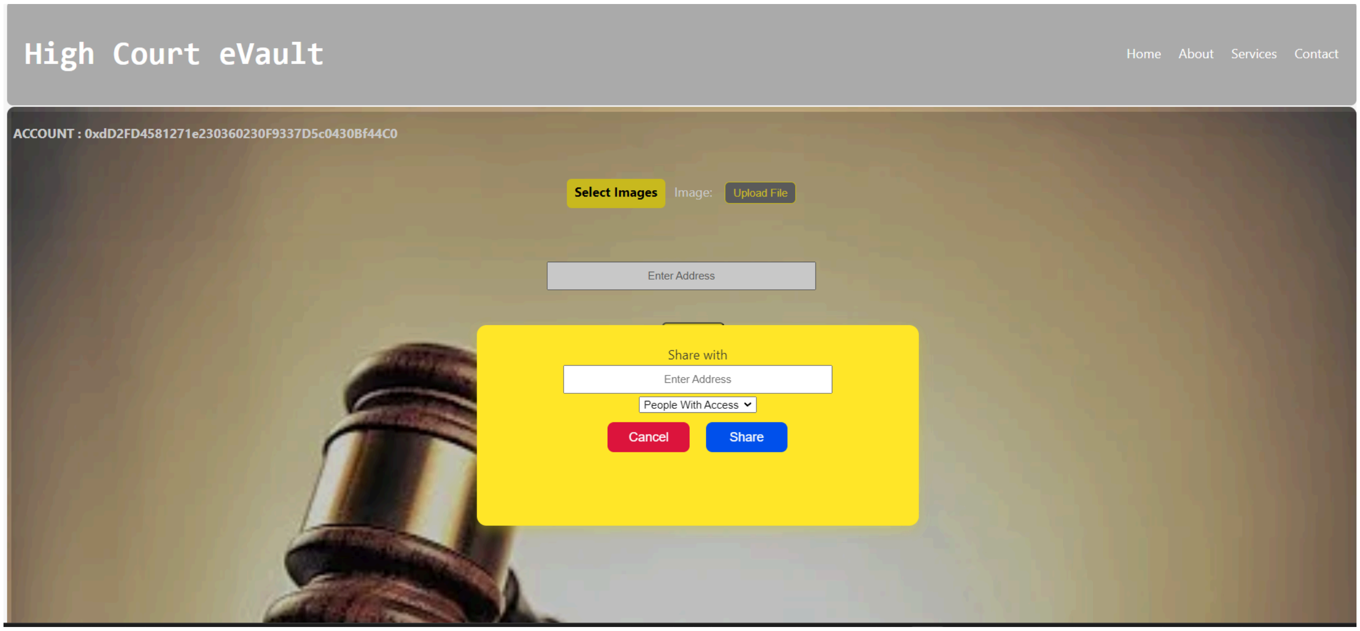
Figure 5.1 displays that this Hard-hat Network has a number of pre-funded test accounts with separate address and private key so that the developer can test a blockchain interaction without touching the mainnet or using real funds. For the EviChain project, this local blockchain environment is for deploying smart contracts, testing transaction execution, and validating the appropriate functioning of the system before putting it into a production network. Each test account has been initialized with 10,000 ETH (fake currency for testing) to permit evidence storage and retrieval processes to be tested thoroughly on the blockchain.



```
PS C:\Users\Saksham\Desktop\CSE\eVault> npx hardhat run --network localhost scripts/deploy.js
Library deployed to: 0x5FbDB2315678afecb367f032d93F642f64180aa3
```

Figure 5.2 : Deployment Of Smart Contract

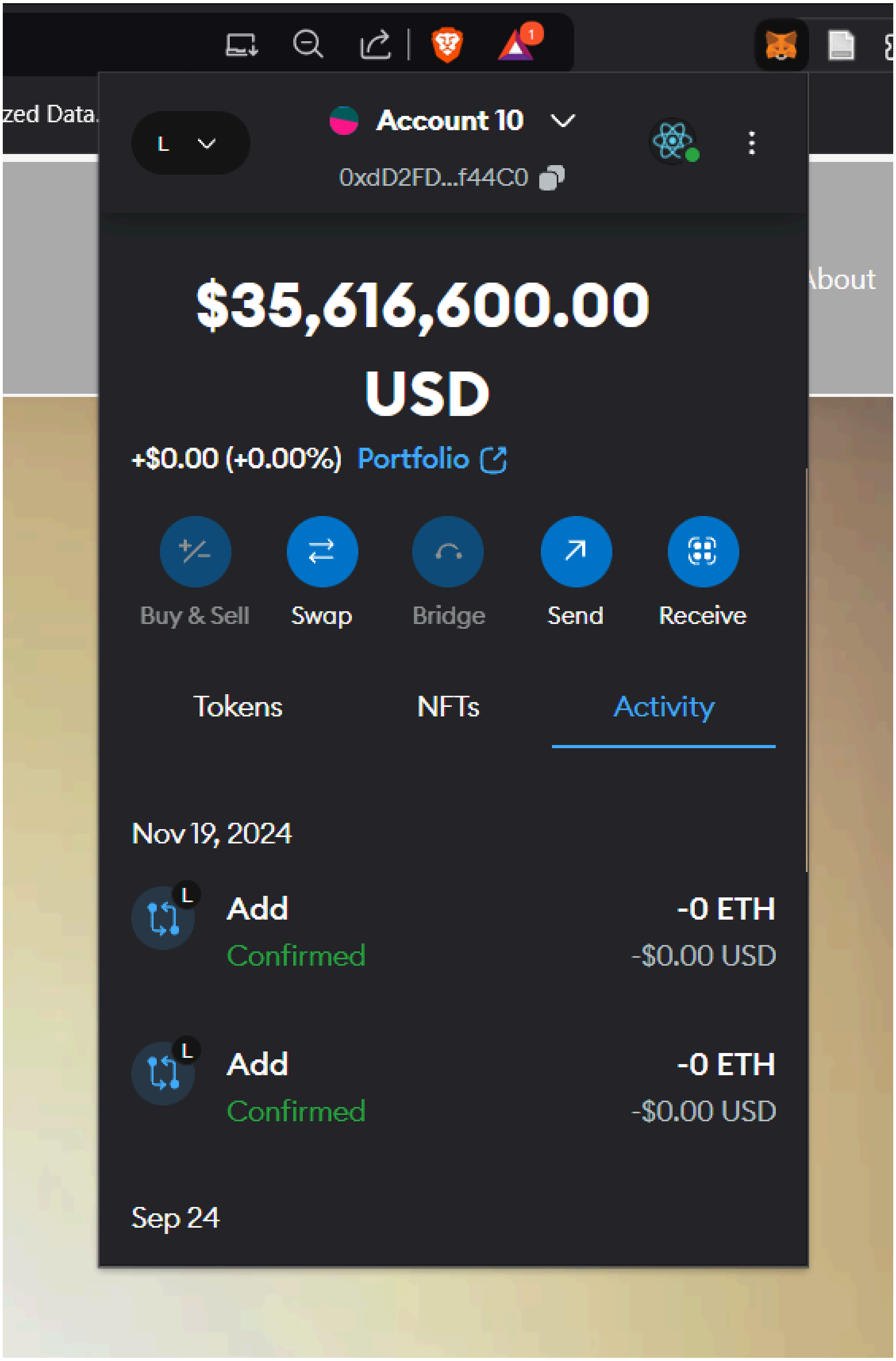
Figure 5.2 displays the successful deployment of the smart contract designed for the file management in the project. The contract is deployed to a localhost using deploy.js script written in ether.js.



ACCOUNT : 0xdD2FD4581271e230360230F9337D5c0430Bf44C0

Figure 5.3 (A) : Front-End

The screenshot in Figure 5.3 shows what is currently the front end of the EviChain project being developed. The interface can be referred to as High Court eVault, which is a user-friendly interface for uploading and managing digital evidence. Users can select pictures or upload files, associate the evidence with blockchain addresses, and share it with others by entering the recipient's address. The sharing features are also provided with controls for access permissions so that the evidence stays private. The design is all about keeping it simple yet efficient, as this is intended to be the best for the project goals of making seamless interaction on the decentralized storage system and blockchain network. This interface, indeed, forms an essential part of the platform, closing the gap between users and the underlying blockchain technology.



Account 10

0xdD2FD...f44C0

$35,616,600.00 USD

+$0.00 (+0.00%) Portfolio

Nov 19, 2024

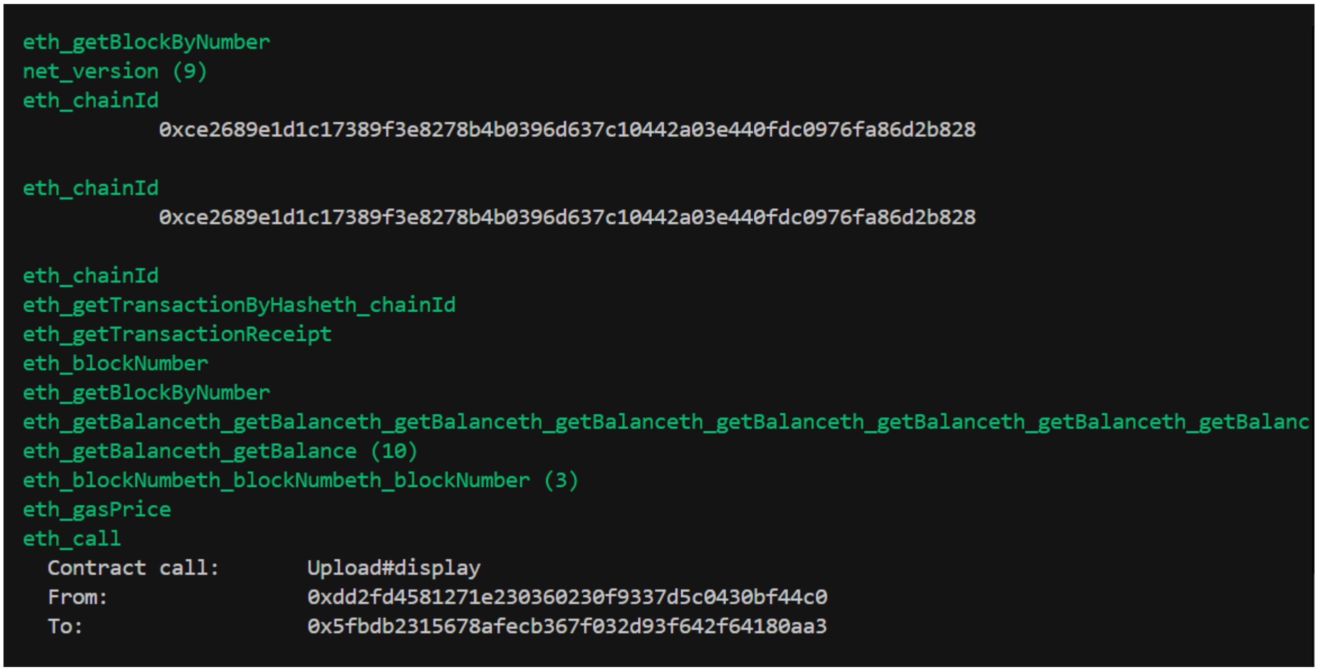
Add Confirmed -0 ETH -$0.00 USD

Add Confirmed -0 ETH -$0.00 USD

Sep 24

Figure 5.3(B) : Front-End

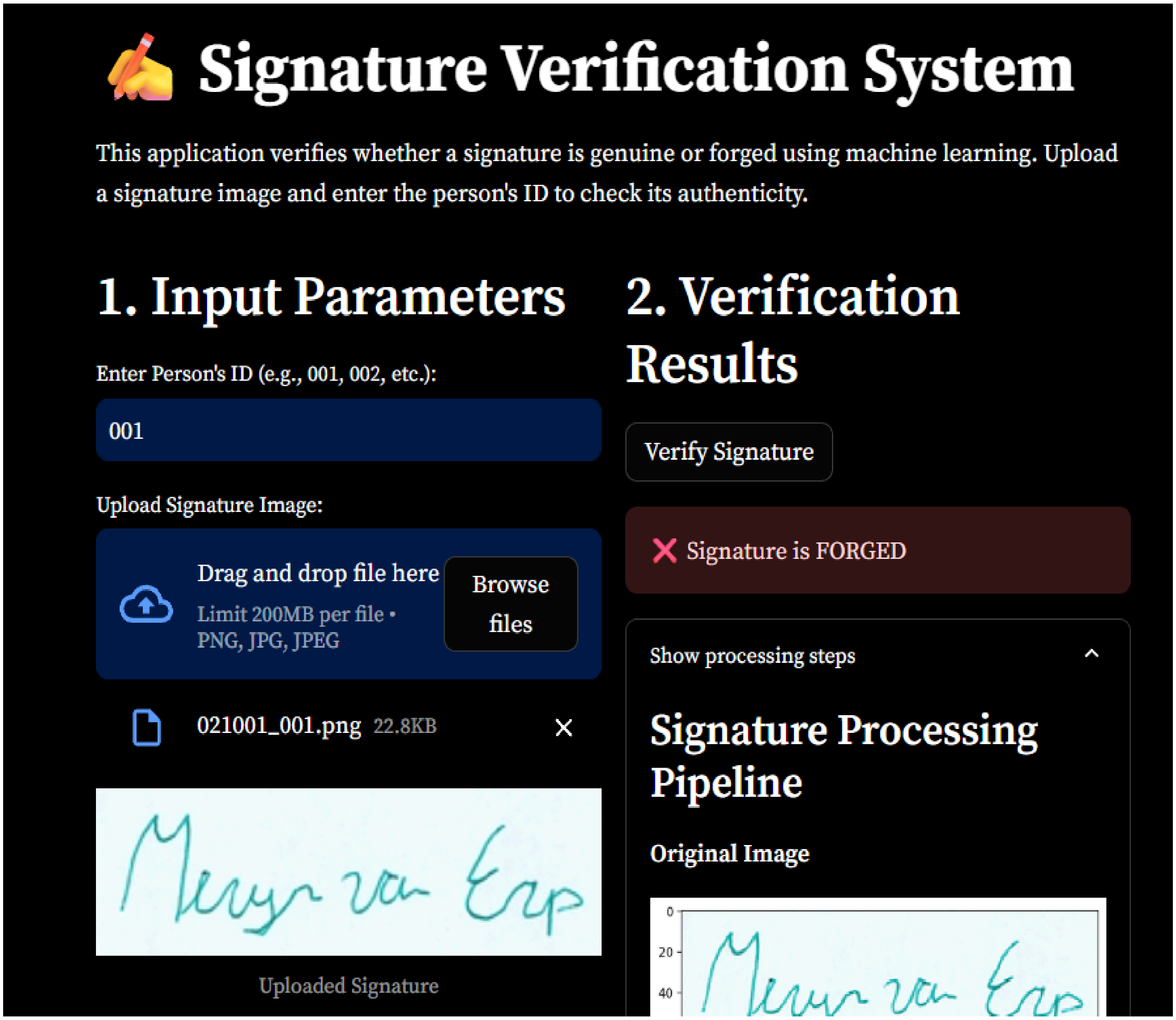
Showcasing the interface of the MetaMask wallet that comes within the EviChain platform for people's invocation of their Ethereum accounts, the wallet balance in USD along with transaction histories and activity logs, as it makes a great difference for human actions in a computerized secure blockchain. In layout are such infrastructures as token management, transaction confirmations, and smart contract interactions. All that is integrated into the frontend made by the software with which the user communicates with the Ethereum blockchain to verify, manage, and act out transactions. Furthermore, there are activity confirmation logs to ensure all parties involved trusted transparency that is necessary for the decentralized evidence storage and fraud detection goals of EviChain.



```
eth_getBlockByNumber
net_version (9)
eth_chainId
           0xce2689e1d1c17389f3e8278b4b0396d637c10442a03e440fdc0976fa86d2b828

eth_chainId
           0xce2689e1d1c17389f3e8278b4b0396d637c10442a03e440fdc0976fa86d2b828

eth_chainId
eth_getTransactionByHasheth_chainId
eth_getTransactionReceipt
eth_blockNumber
eth_getBlockByNumber
eth_getBalanceth_getBalanceth_getBalanceth_getBalanceth_getBalanceth_getBalanceth_getBalanceth_getBalanc
eth_getBalanceth_getBalance (10)
eth_blockNumbeth_blockNumbeth_blockNumber (3)
eth_gasPrice
eth_call
  Contract call:       Upload#display
  From:                0xdd2fd4581271e230360230f9337d5c0430bf44c0
  To:                  0x5fbdb2315678afecb367f032d93f642f64180aa3
```

Figure 5.4 : Transaction Details

Figure 5.4 image displays the history of transactions on the blockchain account regarding the interactions performed by multiple Ethereum addresses on the blockchain network. It also contains important components including the account addresses along with private keys (visible publicly in this simulated environment), and the current status of a transaction. The transparent ledger gets a view of history as it is in real-time with transaction, balances, and metadata attached. All transactions are validated through the consensus algorithm of the blockchain itself, assuring integrity and immutability of data. This feature becomes more important for EviChain since it allows the user secure tracking of evidence transactions to confirm their status and authenticity, making sure evidence is free of tampering and also well recorded on the blockchain.



✍️ Signature Verification System

This application verifies whether a signature is genuine or forged using machine learning. Upload a signature image and enter the person's ID to check its authenticity.

1. Input Parameters

Enter Person's ID (e.g., 001, 002, etc.):

001

Upload Signature Image:

Drag and drop file here

Limit 200MB per file • PNG, JPG, JPEG

Browse files

021001_001.png 22.8KB

Uploaded Signature

2. Verification Results

Verify Signature

❌ Signature is FORGED

Show processing steps

Signature Processing Pipeline

Original Image

Figure 5.5 : Signature Verification System

Figure 5.5 showcases the user interface of the Signature Verification System integrated within the EviChain project. This module is developed using Python ,Streamlit and machine learning techniques to verify whether a given signature is genuine or forged. The system takes two inputs: a person’s ID and a signature image in PNG, JPG, or JPEG format. After that, the user uploads the image and clicks “Verify Signature,” the model processes the signature through a feature extraction pipeline and displays the result.

In the example shown, the uploaded signature (021001_001.png) is identified as FORGED, which is indicated with a red alert box. The right panel also includes an expandable section labeled "Signature Processing Pipeline," which displays the pre-processed version of the signature image used for analysis. This functionality aids in transparency and explainability of the verification outcome.

This tool adds an additional security layer in the EviChain platform by helping validate signed documents, enhancing authenticity and forgery detection in digital evidence workflows.

CHAPTER 06: CONCLUSIONS & FUTURE SCOPE

6.1 CONCLUSION

The EviChain project signifies a remarkable stride in deploying the blockchain technologies for secure evidence storage and management. Incorporating state-of-the-art tools such as Ethereum blockchain, Pinata Cloud, and IPFS makes the data complete and locks digital evidence within these parameters. Immutability, transparency, and easy access are the essential features that perfectly meet the rising demand for reliable systems in legal, academic, and financial contexts in which integrity and authenticity play the most important roles.

One of the greatest newly spruced-up features of EviChain includes its own fraud detection module. This special feature makes use of highly sophisticated AI algorithms to verify and authenticate the stored evidence, thus adding another layer of reliability and trustworthiness. By taking into account all those possible risks, like fraudulent manipulation or unauthorized alteration, the platform builds up confidence among its users. Hence, it is a worthy platform for industries that require stringent validation of data, particularly in courtrooms, research institutions, and financial organizations.

Aside from the technology, EviChain also emphasizes the accessibility and involvement of the users. This value the platform has instilled to go hand-in-hand, because the user interface is friendly and could align with services like the MetaMask in making integration easier, therefore eliminating complexities one usually grapples with decentralized systems. It is meant for people who practice sophisticated technology to those who are not knowledgeable in this arena.

The Examination's assessments issued during this project prove EviChain's robustness against some of the most serious challenges facing digital evidence management. The platform has effectively managed threats of tampering, singular points of failure, and data integrity transformations. The decentralized structure also abolished over reliance on central entities, increasing the risk of data breaches and elevating security within the system as a whole. Further, the inherent transparency and immutability of blockchain can audit and trace all actions taken within the platform, increasing its credibility.

Also, EviChain does feature a future-oriented design of digital transactions. Proof of the infinite opportunity that could be brought about by new dermal technologies is evident to the extent that blockchain is made to accompany AI. Not only did this enhance fraud detection; it also allowed concepts like decentralized systems to open new avenues in the usage of intellectual property rights management, secure academic publishing, and verified financial transactions.

EviChain has been a highlight but not the complete picture of what remains of decentralized evidence management. Scalability, high transaction costs associated with blockchain networks, and the need for universal user adoption are key areas that continue to challenge ongoing research and development. But the project has a solid framework upon which all of these innovations can be added to optimize, for instance, other consensus mechanisms or layer 2 scaling solutions that further enhance platform performance.

Summing up, EviChain shows how blockchain technology can redefine critical spheres of addressing comprehensive evidence storage and fraud detection. By decentralization, AI-based validation, and attracting user experience, this model has already aligned it for animal pioneering purposes, in a digital era. Going with the continuum of development, this platform can best promise revolutions in evidence management and a new standard for secure, transparent, and efficient digital transactions across different sectors.

6.2 FUTURE SCOPE

This next stage of the project will concern the advanced incorporation of AI models into the fraud detection system. Such an improvement will focus on the precision and efficiency of detecting forged or manipulated evidence, along with deep learning and larger, more diverse datasets. Finally, the performance of the platform will be enhanced by reducing blockchain transaction costs and improving scalability.

In addition, it is foreseen that the system will facilitate real-time fraud detection while uploading evidence and will have information exchange capabilities for cross-platform compatibility. These improvements will ensure that EviChain will be the complete forward-looking solution for evidence management in a world where everything is increasingly digitized.

The EviChain project has strong potential for expansion and real-world impact, particularly in the fields of digital forensics, legal tech, and secure evidence management. Below are several avenues for future development:

- **Integration with Government and Judicial Systems**
  EviChain can be extended to work with court databases, police departments, and legal authorities to create a tamper-proof and transparent chain of custody for digital evidence. This

would significantly reduce the chances of evidence tampering or loss of data.

- **Multi-format Evidence Support**

  Future versions of EviChain can include support for audio, video, and PDF files, enabling a more comprehensive range of digital evidence types to be stored, verified, and shared securely on the blockchain.

- **Advanced AI-based Verification**

  The integrated signature verification system can be enhanced using deep learning models like CNNs and Siamese Networks, allowing it to handle unseen or untrained signatures with higher accuracy. With better computational resources or cloud-based training, the system could become highly robust and production-ready.

- **User Role Management and Access Control**

  Implementation of fine-grained access controls based on user roles (e.g., judge, lawyer, victim, proofer) could add more structure and security to how evidence is shared and accessed, aligning with real-world legal protocols.

- **Scalability and Interoperability**

  Deploying the system on scalable Layer 2 blockchain solutions or using cross-chain protocols can improve transaction efficiency and reduce costs. Furthermore, integration with identity management systems (e.g., Aadhaar, digital IDs) can enhance real-world adoption.

- **Mobile Application and Notifications**

  A dedicated mobile app with real-time notifications can be developed to keep users updated on evidence status, access permissions, and verification results—enhancing usability and engagement.

- **Legal and Ethical Compliance**

  The platform can be further refined to comply with national and international standards for digital evidence (e.g., IT Act, GDPR), ensuring its viability in legal proceedings.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” accessed 01-Oct-2023.[2] V. Buterin, “Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform,” accessed 01-Oct-2023.

[2] C. A. Cachin, “Architecture of the Hyperledger Blockchain Fabric,” in *Proceedings of the 2016 IEEE International Conference on High-Performance Computing and Communications (HPCC)*, 2016

[3] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, “A Systematic Review of Consensus Mechanisms in Blockchain,” *IEEE Access*, vol. 9, pp. 123456-123470, 2021.

[4]] I. Bhuvaneshwari and M. N. Sudha, “An Implementation of Secure Storage Using Blockchain Technology on Cloud Environment,” *International Journal of Cloud Computing and Services Science*, vol. 11, no. 1, pp. 45-56, 2021.

[5] K. C. Lee, J. S. Chen, and H. T. Hsu, “Challenges in Detecting Fraudulent Digital Evidence: Towards a Blockchain Solution,” *Journal of Digital Forensics, Security and Law*, vol. 16, no. 2, pp. 1-12, 2021.

[6] V. T. Truong and L. B. Le, “A Blockchain-Based Framework for Secure Digital Asset Management,” *Journal of Information Security and Applications*, vol. 54, no. 1, pp. 102-112, 2020.

[7] Y. Jiang, G. Sun, and T. Feng, “Research on Data Transaction Security Based on Blockchain,” *Journal of Network and Computer Applications*, vol. 169, pp. 102-115, 2020.

[8] J. S. Chen, J. W. Yang, and Y. H. Lin, “A Survey of Blockchain Technology in Digital Forensics,” *Journal of Forensic Sciences*, vol. 65, no. 6, pp. 1954-1965, 2020.

[9] A. Jones and B. Smith, “Detecting Tampered Digital Evidence: A Survey of Methods and Technologies,” *Digital Investigation*, vol. 27, pp. 1-10, 2019.

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “Blockchain Technology for Secure Data Sharing and Storage,” in *Future Generation Computer Systems*, vol. 81, pp. 1-11, 2018.

[11] K. Rabah, “Convergence of AI, IoT, Big Data, and Blockchain: A Review,” *Lake Institute Journal*, vol. 4, no. 2, pp. 45-55, 2018.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology,” in *Proceedings of the IEEE Congress on Big Data*, 2017.

[13] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, “A Systematic Review of Consensus Mechanisms in Blockchain,” *IEEE Access*, vol. 9, pp. 123456-123470, 2021.

[14] K. Fan, Y. Ren, H. Gong, and H. Li, "Blockchain-Based Efficient Privacy-Preserving and Data

Sharing Scheme of Content-Centric Network," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1853-1866, Mar. 2020

[15] S. Nakamoto and P. Heo, "Integrating Blockchain and AI for Fraud Detection in Digital Systems," *IEEE Access*, vol. 9, pp. 24412-24425, 2021

[16] Y. Yuan and F.-Y. Wang, "Blockchain: The State of the Art and Future Trends," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2744-2763, Aug. 2018

[17] J. Xu, A. Qadir, R. M. Pathan, and M. Asif, "Blockchain-Assisted Tamper-Resistant Evidence Storage and Verification System," in *Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Sydney, NSW, Australia, 2021

[18] J. Huang, W. Wang, and Y. Zhang, "A Blockchain-Based Secure Evidence Management Framework for Digital Forensics," *IEEE Access*, vol. 8, pp. 19665-19678, 2020

[19] M. K. Hasan, M. M. Islam, N. H. A. Basaruddin, and A. K. Bhuiyan, "Blockchain-Based AI Framework for Fraud Prevention in Evidence Submission," *IEEE Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 108-117, May 2021

[20] H. Zhang, H. Wang, and G. Guo, "Design and Implementation of a Blockchain-Based Digital Evidence Management System," in *Proceedings of the 2020 IEEE International Conference on Big Data (Big Data)*, Atlanta, GA, USA, 2020

[21] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” *Computer Communications*, vol. 120, pp. 10–29, 2018.

[22] M. Conti, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Blockchain Technology,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1168–1199, 2019.

[23] T. H. Nguyen, L. T. Do, and V. D. Nguyen, “A Blockchain-Based Approach for Secure Data Provenance in Cloud Environments,” *Future Generation Computer Systems*, vol. 129, pp. 72–85, 2022.

[24] A. T. Satchidanand and S. Sharma, “Leveraging Blockchain and AI for Forensic Integrity Verification: A Decentralized Model,” *Journal of Information Security and Applications*, vol. 68, pp. 103233, 2022.

[25] C. Esposito, A. Castiglione, K. K. R. Choo, and M. Palmieri, “Cloud Storage Security: A Survey of Architectures and Regulatory Issues,” *IEEE Access*, vol. 8, pp. 131376–131392, 2020.

Evichain

ORIGINALITY REPORT

1%	1%	1%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Stefano Tempesta. "Application Architecture Patterns for Web 3.0 - Design Patterns and Use Cases for Modern and Secure Web3 Applications", Routledge, 2024 Publication	<1%
2	www.spaceotechnologies.com Internet Source	<1%
3	login-official-blur-nft.gitbook.io Internet Source	<1%
4	fastercapital.com Internet Source	<1%
5	Submitted to INSEAD Student Paper	<1%
6	uec.repo.nii.ac.jp Internet Source	<1%

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

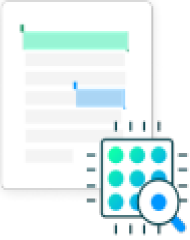
Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.



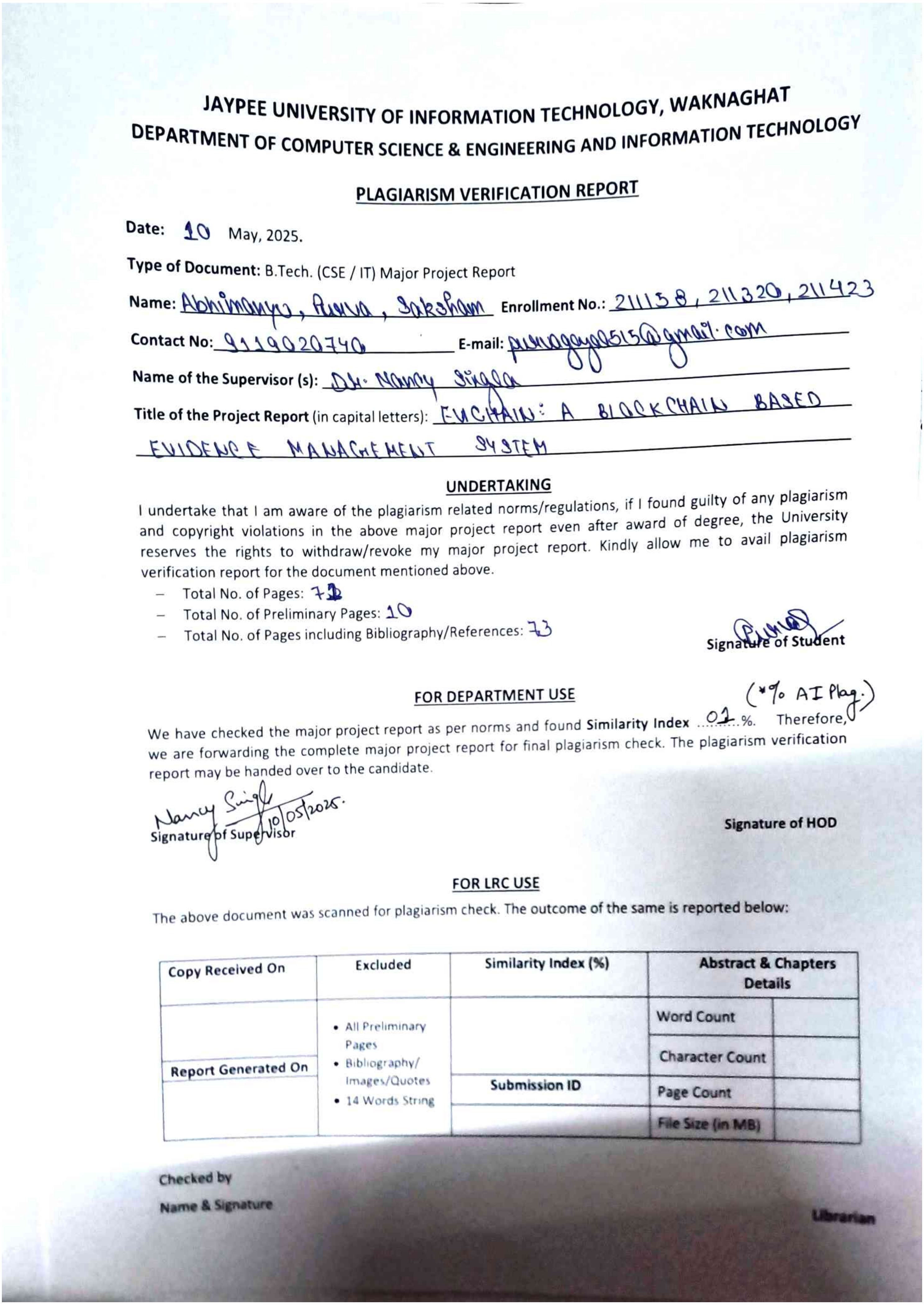
False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING AND INFORMATION TECHNOLOGY

PLAGIARISM VERIFICATION REPORT

Date: 10 May, 2025.

Type of Document: B.Tech. (CSE / IT) Major Project Report

Name: Abhimanyu, Purva, Saksham **Enrollment No.:** 211138, 211320, 211423

Contact No: 9119020740 **E-mail:** purvagoyal515@gmail.com

Name of the Supervisor (s): Dr. Nancy Singla

Title of the Project Report (in capital letters): EVCHAIN: A BLOCKCHAIN BASED EVIDENCE MANAGEMENT SYSTEM

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/regulations, if I found guilty of any plagiarism and copyright violations in the above major project report even after award of degree, the University reserves the rights to withdraw/revoke my major project report. Kindly allow me to avail plagiarism verification report for the document mentioned above.

- Total No. of Pages: 72
- Total No. of Preliminary Pages: 10
- Total No. of Pages including Bibliography/References: 73

Signature of Student

FOR DEPARTMENT USE

(*% AI Plag.)

We have checked the major project report as per norms and found **Similarity Index** 01 %. Therefore, we are forwarding the complete major project report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

Nancy Singla 10/05/2025.
Signature of Supervisor

Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received On	Excluded	Similarity Index (%)	Abstract & Chapters Details	
	• All Preliminary Pages • Bibliography/ Images/Quotes • 14 Words String		Word Count	
			Character Count	
Report Generated On		Submission ID	Page Count	
			File Size (in MB)	

Checked by
Name & Signature

Librarian