



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 10, October 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.625



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com



Blockchain Based Tamperproof FIR Chain

Seher Shah, Kaustubh Dev, Nirmala Salam

Student (B.Tech-Final year), SENG Department, SNDT Women's University, Mumbai, India

Student (MCA-Final year), SENG Department, Hiray College, Mumbai, India

Scientist F, SENG Department, C-DAC, Mumbai, India

ABSTRACT: This project investigates the application of blockchain technology to the First Information Report (FIR) management system within law enforcement agencies. The primary objective is to address prevalent issues in traditional FIR management, such as loss, tampering, unauthorized access, and manipulation of FIR [1]. By leveraging blockchain's immutable ledger and decentralized nature, the proposed system aims to enhance transparency, security, and accountability within the FIR management process. This ensures that FIR are accurately preserved, reducing the risk of wrongful actions against police officers and unjust outcomes for defendants. The project will outline the specific challenges associated with implementing a blockchain-based FIR management system and present a robust, efficient solution to overcome these obstacles

KEYWORDS: FIR, Blockchain, IPFS

I. INTRODUCTION

In recent years, the integration of blockchain technology has surged, offering transformative solutions for various industries, including finance, healthcare, and supply chain management. One area where blockchain's potential is particularly promising is in law enforcement and public safety, specifically in the management of First Information Reports (FIR). This research paper introduces the FIR Chain Management System, an innovative platform designed to enhance the efficiency, transparency, and security of FIR management using cutting-edge technologies such as Hyperledger Besu and InterPlanetary File System (IPFS), integrated into a React.js-based web application. The FIR Chain Management System enables users to register and log in securely to the platform, where they can file complaints related to criminal activities. The system categorizes these complaints into two types: cognizable and non-cognizable. Cognizable complaints, which are more serious and require immediate police intervention, are stored on the blockchain network to ensure their immutability and tamper-proof nature. Non-cognizable complaints, while still tracked and managed, do not require the same level of security and are not stored on the blockchain.

Blockchain Technology: Blockchain is a decentralized network that provides data integrity and enhances transparency. Each block in the blockchain contains a list of transactions, and these blocks are cryptographically linked to each other in a chain. It is a database of record of transactions which is distributed, and which is validated and maintained by a network of computers around the world. Instead of a single central authority such as a bank, the records are supervised by a large community and no individual person has control over it and no one can go back and change or erase a transaction history[2]. The consensus mechanisms employed by blockchain networks, such as Proof of Work (PoW) or Proof of Stake (PoS), validate and add transactions to the blockchain, preventing fraud and double-spending. By utilizing blockchain in the FIR Chain Management System, the platform ensures that cognizable complaints are securely recorded in an immutable ledger, preventing any unauthorized modifications and ensuring the trustworthiness of the data. This immutability is crucial for maintaining the integrity of legal records and for ensuring transparency in law enforcement processes. Fig. 1 depicts the flow of transactions, illustrating how each step is securely validated and recorded on the blockchain, ensuring a transparent and tamper-proof system.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

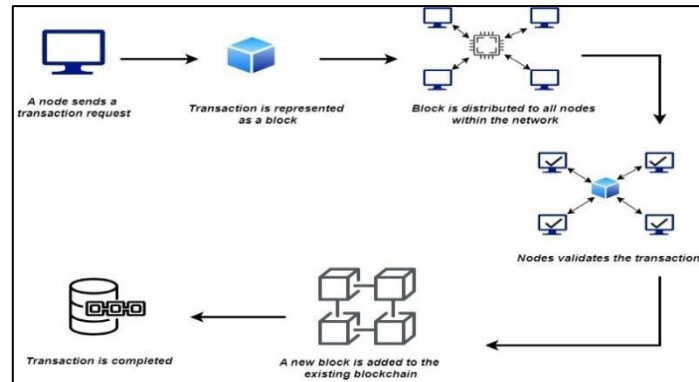


Fig.1.Workflow Diagram

Ethereum: Ethereum is a decentralized platform that enables developers to build and deploy smart contracts and decentralized applications (dApps). Ethereum's native cryptocurrency, Ether (ETH), is used to fuel transactions and computational services on the network. The Ethereum Virtual Machine (EVM) provides a runtime environment for smart contracts. Every node in the Ethereum network runs under EVM and executes its instructions. The smart contracts are translated into EVM code and then executed by the nodes. One of the most popular programming language for writing smart contracts is Solidity[3]. By leveraging Ethereum's capabilities, the FIR Chain Management System can utilize smart contracts to automate and enforce the rules governing the filing and management of FIRs. This ensures that the process is transparent, efficient, and tamper-proof, further enhancing the reliability and security of the system. Hyperledger Besu: Hyperledger Besu is an Ethereum client designed to be enterprise-friendly for both public and private permissioned network use cases. It can also be run on test networks such as Rinkeby, Ropsten, and Goerli [4]. Hyper ledger Besu supports various consensus algorithms, including PoW and IBFT (Istanbul Byzantine Fault Tolerance), making it versatile for different blockchain applications. By employing Hyperledger Besu in the FIR Chain Management System, the platform leverages Ethereum's decentralized architecture, which ensures that the data recorded on the blockchain is transparent and immutable. This choice also allows the system to benefit from a wide range of Ethereum tools and libraries, further enhancing its functionality and reliability.

InterPlanetary File System (IPFS): IPFS is a peer-to-peer hypermedia protocol to make the web faster, safer, and more open. IPFS synthesizes many of the best ideas from the most successful systems to date. Bit Swap Protocol is one of the best ideas we think that makes IPFS different from other block storage distributing system [5]. IPFS is a distributed file storage system that enhances data availability and resilience. Unlike traditional centralized servers, IPFS uses a peer-to-peer network to store and share files. This decentralized approach ensures that files are not reliant on a single server and can be accessed more reliably. In the FIR Chain Management System, IPFS is used for storing complaint details in a distributed manner, reducing the load on the blockchain network and ensuring that data remains accessible and durable even if some nodes in the network go offline. The decentralized nature of IPFS enhances data storage capabilities, allowing for efficient and scalable management of FIR records. By integrating IPFS with blockchain, the system ensures that while the critical data is securely logged on the blockchain, the supporting information is distributed across the IPFS network, providing a balanced approach to security and efficiency

BACKGROUND

The management of First Information Reports (FIR) is crucial in law enforcement, documenting complaints about criminal activities. Traditional FIR systems face challenges such as data tampering, delays, lack of transparency, and inefficient data handling. These issues undermine the integrity and trust in law enforcement processes. Emerging technologies like blockchain and the Interplanetary File System (IPFS) offer solutions to these challenges. Blockchain guarantees the immutability and transparency of data, safeguarding it against any tampering. Hyperledger Besu, an enterprise-grade Ethereum client, supports secure and private networks suit able for handling sensitive data. IPFS provides distributed file storage, enhancing data availability and security. The FIR Chain Management System



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

integrates Hyperledger Besu and IPFS to revolutionize FIR management. Blockchain ensures that cognizable complaints remain immutable and transparent, while IPFS offers scalable and secure storage for complaint details.

RESEARCH MOTIVATION

The motivation behind the FIR Chain Management System arises from the urgent need to address significant issues in traditional FIR management. FIRs are crucial in the criminal justice system as they initiate the investigation process for reported crimes. However, current FIR systems suffer from vulnerabilities such as data tampering, lack of transparency, operational inefficiencies, and poor data management. Ensuring the integrity and security of FIR records is essential to maintain public trust and uphold justice, which blockchain technology can achieve through its immutable ledger. Additionally, the lack of transparency in the FIR filing and tracking process often leads to public mistrust. By leveraging blockchain's transparent nature, the system aims to provide real-time updates and visibility into the status of complaints, thereby enhancing public confidence in law enforcement.

OBJECTIVES

The primary objective of the FIR Chain Management System project is to develop and implement a secure, transparent, and efficient platform for managing First Information Reports (FIRs) using blockchain and IPFS technologies.

The specific objectives include:

1. Implementing a blockchain-based system using Hyperledger Besu to ensure the immutability and security of FIR records.
2. To create a transparent platform where users can file complaints and track their status in real-time, thereby increasing public trust in the law enforcement process through the immutable and transparent nature of blockchain.
3. Designing a React.js-based web application that is intuitive and accessible for both law enforcement officers and the public. Using IPFS for distributed storage of complaint details, ensuring high availability and resilience against data loss.
4. Users (both public and law enforcement officers) can register and log in securely to the system. User authentication and authorization are managed to ensure that only authorized personnel can access sensitive features.
5. Users can file new complaints through an intuitive form. Complaints are categorized into cognizable and non-cognizable based on predefined criteria.
6. Cognizable complaints are recorded on the blockchain to ensure immutability and prevent tampering. Detailed complaint descriptions and related documents are stored on IPFS to ensure scalability and data availability. By achieving these objectives, the FIR Chain Management System aims to create a more secure, transparent, and efficient process for managing First Information Reports (FIRs), thereby enhancing public trust and the effectiveness of law enforcement processes.

II. LITERATURE REVIEW

The authors in [6] introduce a blockchain-based evidence management system designed to address the challenges faced by traditional evidence management systems in law enforcement. The system aims to mitigate issues such as loss, theft, tampering, and manipulation of evidence. By leveraging blockchain technology, the system ensures the integrity and security of the evidence chain, thereby protecting police officers and defendants from wrongful termination and false imprisonment. The project highlights the specific challenges associated with storing evidence on a blockchain and proposes an efficient solution to overcome these hurdles.

The authors in [7] propose a blockchain-based system for FIR registration, highlighting the enhanced security and tamper-resistance of blockchain technology. This system addresses the limitations of traditional manual FIR registration by ensuring data integrity and authorized access, significantly improving the efficiency and transparency of recording and accessing critical information. In [7], a system is introduced that allows users to file complaints anonymously and includes a password system to ensure that only police can access relevant files. This approach addresses the barriers in the manual police system and provides a secure and efficient way to manage and investigate complaints. In their paper "Smart FIR: Securing e-FIR Data through Blockchain within Smart Cities" the authors [8]



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

address the vulnerabilities of centralized e-FIR databases, particularly regarding data integrity and the risk of false registrations. They propose a consensus-based distributed blockchain solution utilizing Ethereum smart contracts and the Web3 RPC protocol to secure e-FIR data. The system architecture involves secure user authentication through a national database, blockchain registration of police stations, and a meticulous process for filing and approving e-FIRs. The use of hashing ensures data immutability, and false e-FIRs can be audited by higher authorities. Their simulations indicate a trade-off between hashing algorithm security levels and the number of transactions per blockchain block, underscoring the effectiveness of their approach in enhancing e-FIR data integrity within smart cities.

Shyam Mehta, K. Shantha Kumari, Paras Jain, Harshal Raikwar, and Shubham Gore collectively present in their paper titled “Blockchain driven Evidence Management System” a focus on tackling issues related to data transparency and integrity within electronic First Information Report (e-FIR) systems. By leveraging blockchain technology, specifically using Ethereum and smart contracts, the study proposes a decentralized framework to manage FIRs and non-cognizable reports [9]. This system ensures that e-FIRs are immutable and secure, reducing the risk of false registrations and unauthorized alterations. The blockchain’s consensus mechanism and cryptographic hashing provide a robust solution for maintaining data integrity and security. The study highlights the implementation of a private, federated blockchain that ensures only validated and authorized changes are recorded, enhancing trust in the police complaint management process.

III. PROPOSED SYSTEM METHODOLOGY

The proposed system leverages blockchain technology within the law enforcement chain of custody, specifically focusing on the management of First Information Reports (FIRs). This FIR Chain Management System aims to address issues prevalent in traditional complaint management, such as loss, theft, tampering, and manipulation of complaint records. By utilizing blockchain technology, the system safeguards both law enforcement officers and complainants from chain of custody problems that can lead to wrongful actions or false allegations.

The FIR Chain Management System begins with user and administrator registration, followed by their respective logins. Upon successful registration and login, users access their dash board to file complaints. These complaints are then displayed on the administrator’s dashboard, where they are reviewed and categorized into cognizable or non-cognizable complaints. Cognizable complaints, which are serious and require immediate action, are securely stored using the InterPlanetary File System (IPFS). IPFS provides a decentralized method of storing and sharing files, ensuring that complaint files are securely stored and easily retrievable. The hash generated by IPFS for each complaint file is then stored on the blockchain, ensuring that the data remains tamper-proof and verifiable. Non-cognizable complaints, which are less severe and do not require immediate action, are stored in a conventional database for further processing.

This proposed system addresses several key challenges associated with traditional FIR management:

- **Immutability and Integrity:** Blockchain technology ensures that once a complaint is recorded, it cannot be altered or deleted, preserving the integrity of the complaint records.
- **Decentralization:** By using a decentralized network, the system avoids the risks associated with centralized servers, such as hacking or server crashes, ensuring continuous availability and reliability.
- **Transparent Audit Trail:** The blockchain provides a transparent audit trail of all actions taken within the system, promoting accountability among law enforcement officers and administrators.
- **Secure Storage:** IPFS offers a secure and efficient solution for storing large complaint files, ensuring they are easily accessible while protecting them from tampering and unauthorized access.
- **Enhanced Trust:** The integration of blockchain and IPFS enhances trust in the complaint management process, as stakeholders can verify the authenticity and integrity of the stored complaints.

The motivation for applying blockchain technology in this project stems from the need to address issues of false accusations and wrongful actions within the law enforcement process. By ensuring a secure and immutable chain of custody for complaints. Blockchain’s immutability and transparency ensure that complaint records are handled with the highest degree of integrity, reducing the risk of tampering or loss. Additionally, the decentralized nature of IPFS ensures that complaint files are distributed across multiple nodes, making them resistant to single points of failure and



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

unauthorized access. The integration of blockchain with IPFS in this FIR management system illustrates how advanced technologies can be employed to improve the reliability, security, and efficiency of complaint management in the criminal justice system.

The workflow of the system begins with user and administrator registration, followed by login. Users access their dashboard to file complaints, which are then visible to administrators. Administrators review and categorize these complaints, storing cognizable complaints on IPFS and recording their hashes on the blockchain, while non-cognizable complaints are stored in a database. This process ensures that all complaints are securely managed and that critical information is preserved in an immutable and transparent manner, ultimately enhancing the overall integrity of the criminal justice system. By leveraging cutting-edge technologies, this system not only improves the efficiency and security of FIR management but also sets a precedent for future advancements in law enforcement processes. The implementation of such a system can significantly contribute to building a more transparent and trustworthy environment in criminal justice.

IV. IMPLEMENTATION

A. Workflow of the System

The diagram represents the process flow for a “First Information Report (FIR) Chain Management System” from both user and admin perspectives. It outlines steps for registration, login, complaint filing, categorization, and storage using IPFS and blockchain technology.

User Workflow:

1. FIR Chain Management System: Start point.
2. Select Dashboard: User chooses between User and Admin Dashboard
3. User Dashboard: If User Dashboard is selected, proceed to User Dashboard.
4. Registration and Login: User registers and logs in.
5. File Complaint: If the user is valid, they can file a complaint which is then displayed on the Admin Dashboard. If the user is not valid, they are returned to the registration process.

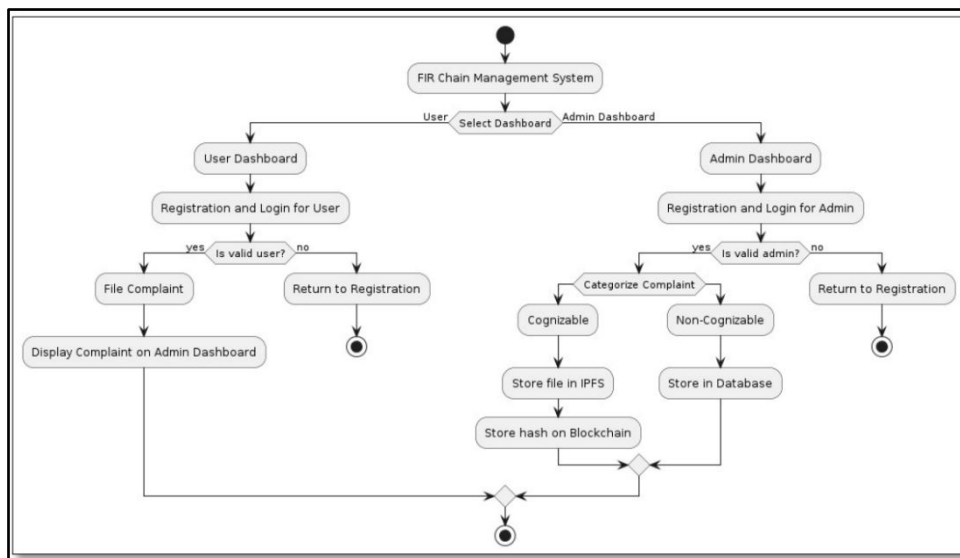


Fig.2.Workflow Diagram

Admin Workflow

- 1) Admin Dashboard: If Admin Dashboard is selected, proceed to Admin Dashboard.
- 2) Registration and Login: Admin registers and logs in.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- 3) Categorize Complaint: If the admin is valid, they can categorize complaints as Cognizable or Non-Cognizable.
 - Cognizable: Store file in IPFS and store hash on Blockchain
 - Non-Cognizable: Store in Database.
- 4) If the admin is not valid, they are returned to the registration process.

Storage and Display:

- Display Complaint on Admin Dashboard: Displays user complaints for admin review.
- Store file in IPFS: Stores cognizable complaint files in IPFS.
- Store hash on Blockchain: Stores hash of cognizable complaint file on blockchain.
- Store in Database: Stores non-cognizable complaints in database

B. User Dashboard Functionalities

The User Dashboard in the FIR Chain Management System is designed to provide a user-friendly interface that allows registered users to efficiently manage and file their complaints. The key functionalities of the User Dashboard are as follows:

1. User Registration and Login: Users can register for an account and log in securely to access the dashboard. This ensures that only authenticated users can file complaints.
2. File a Complaint: Users can file a new complaint by providing necessary details such as the nature of the complaint, description, and any supporting documents. The admin categorizes the complaint as either cognizable or non-cognizable based on predefined criteria.
3. View Complaint Status: Users can view the status of their filed complaints, including updates and actions taken by the authorities. This feature provides transparency and keeps users informed about the progress of their complaints.

C. Admin Dashboard Functionalities

The Admin Dashboard in the FIR Chain Management System is designed to equip administrators with the necessary functionalities to efficiently manage and process complaints. The primary functionalities of the Admin Dashboard include:

1. Admin Registration and Login: Administrators can register for an account and log in securely to access the dashboard, ensuring that only authorized personnel can manage and process complaints.
2. View Complaints: Administrators can view all filed complaints, including details such as the nature of the complaint, description, and any supporting documents. This allows administrators to have a comprehensive view of all complaints submitted to the system.
3. Categorize Complaints: Administrators can categorize complaints as cognizable or non-cognizable based on the information provided by the user. Cognizable complaints, which require immediate action, are processed and stored on the blockchain for security and immutability. Non-cognizable complaints, which do not require immediate action, are stored in a conventional database for further processing.
4. Manage Complaint Status: Administrators can update the status of complaints, providing users with information about the progress and actions taken on their complaints.
5. Store Complaint Files: Administrators can securely store complaint files using the InterPlanetary File System (IPFS). The IPFS hash of each file is recorded on the blockchain to ensure tamper-proof and verifiable storage for cognizable complaints. Non-cognizable complaint files are stored in a conventional database.

The admin interface showcases complaints filed by users, particularly focusing on First Information Reports (FIRs). It allows the admin to categorize FIRs as either cognizable or non-cognizable.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Admin Dashboard

FILE COMPLAINT

Complaint ID	Name	Date	Complaint Description	Complaint Type	Status	PDF of FIR
	sakshi dev		lost cell phone by me	<input type="radio"/> Cognizable <input checked="" type="radio"/> Non-Cognizable	Status Accept	PDF
CMP-2024-72911	Kaustubh		robbery is happened here	<input type="radio"/> Cognizable <input checked="" type="radio"/> Non-Cognizable	Status In-Process	PDF
CMP-2024-38933	Seher S		landlord cuts the wifi and harass	<input type="radio"/> Cognizable <input checked="" type="radio"/> Non-Cognizable	Status Accept	PDF
CMP-2024-76286	ABC		landlord cuts the wifi and harass	<input type="radio"/> Cognizable <input checked="" type="radio"/> Non-Cognizable	Status Reject	PDF

Blockchain Based FIR Management System

COMPLAINT FORM

Cognizable Complaint

Non-Cognizable Complaint

Fig.3. User and Admin Dashboard, Categorization of Complaints.

D. IPFS Integration for Cognizable Complaint Management

The system employs the InterPlanetary File System (IPFS) for the storage of cognizable complaints. IPFS functions as a decentralized and distributed file system, ensuring the secure and efficient storage of complaint files. When a cognizable complaint is filed, its associated file is uploaded to the IPFS network. IPFS generates a unique cryptographic hash for each file, serving as its identifier within the network. This hash, representing the content of the complaint file, is then stored on the blockchain. By integrating IPFS with the blockchain, the system ensures the immutability and transparency of complaint records, as the hash stored on the blockchain provides a verifiable reference to the original complaint file stored in IPFS. The figure 4 displays the response received from the IPFS upon submitting a cognizable complaint. The response includes the transaction hash. This ensures the immutability and transparency of the complaint record, as the blockchain provides a secure and verifiable method for storing the hash generated by IPFS.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

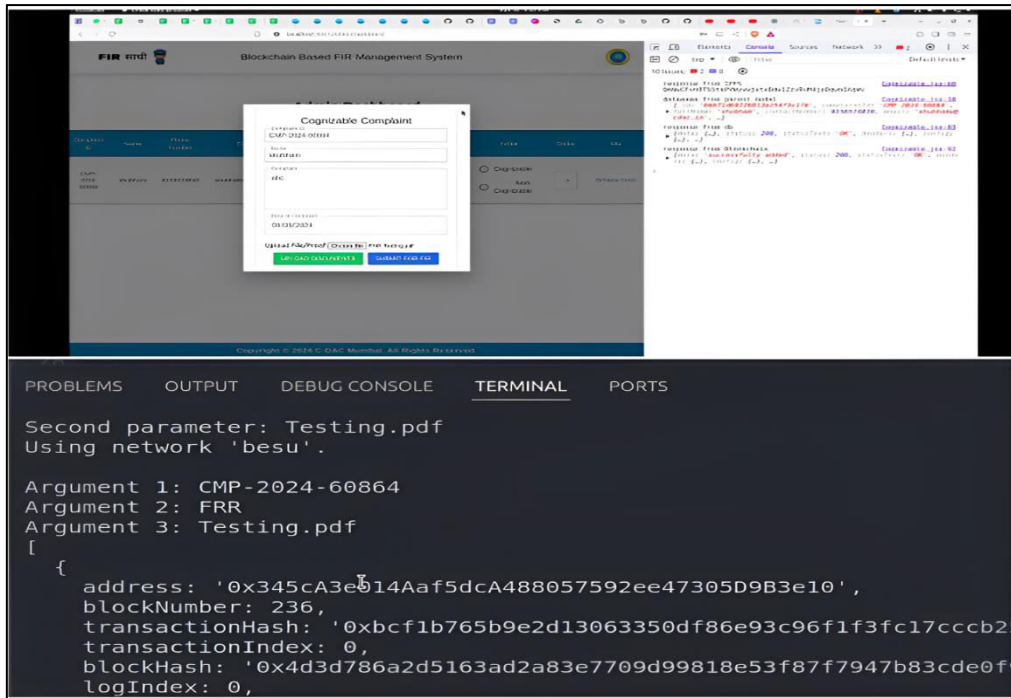


Fig.4. Blockchain response showing transaction hash and block number for a stored cognizable complaint

V. RESULTS

This research explores the FIR Chain Management System, highlighting its architecture, features, benefits, and implications for law enforcement. Utilizing Hyperledger Besu for blockchain integration, the system offers enhanced scalability, Ethereum network compatibility, and robust smart contract support, making it ideal for decentralized storage integration. The system allows the users to automates the filing and categorization of complaints, enhancing efficiency and accuracy in complaint management. Figures 3 and 4 depict the user complaint filing process and admin categorization workflow. Cognizable complaints are securely stored using the InterPlanetary File System (IPFS), with their hashes recorded on the blockchain for tamper-proof integrity. Non-cognizable complaints are stored in a conventional database.

Figure 4 shows the blockchain response upon adding a cognizable complaint, displaying the transaction hash and block number, ensuring secure and immutable complaint records. The process of storing cognizable complaints in IPFS and recording their hashes on the blockchain is illustrated in Figure 4. This integration ensures that complaints are securely stored and easily retrievable, enhancing the system's overall integrity and reliability. By leveraging blockchain technology, the FIR Chain Management System ensures immutability and integrity of complaint records and enhancing trust in the law enforcement process.

The use of IPFS for decentralized storage protects complaint files from tampering and unauthorized access. The FIR Chain Management System significantly improves the efficiency, security, and transparency of complaint management, making it a valuable option for law enforcement agencies and addressing longstanding issues within the criminal justice system.

VI. CONCLUSION AND FUTURE WORK

The FIR Chain Management System leverages Hyperledger Besu and IPFS to enhance the efficiency, security, and transparency of complaint management in law enforcement. This integration ensures the immutability and integrity of complaint records and enhances trust in the law enforcement process. Hyperledger Besu's scalability and compatibility



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

with Ethereum networks, combined with IPFS's decentralized storage, offer robust protection against tampering and unauthorized access.

Future work will focus on improving system scalability to handle a higher volume of complaints efficiently. Integrating the system with other law enforcement databases and enhancing security measures, such as multi-factor authentication and advanced encryption, will further protect sensitive data. Additionally, refining the user experience and expanding the application of these technologies to other areas of the criminal justice system, such as evidence management and judicial processes, will enhance overall transparency and efficiency. By addressing these areas, the FIR Chain Management System can continue to evolve, providing greater benefits to law enforcement agencies and the communities they serve.

REFERENCES

1. K. Ning, C. Liu, S. Lin, X. Geng, and G. Han, "A blockchain shardingbased data sharing scheme for internet of vehicles," in 2023 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing Communications (GreenCom) and IEEE Cyber, Physical Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), 2023, pp. 7–12.
2. S. S. Sarmah, "Understanding blockchain technology," *Computer Science and Engineering*, vol. 8, no. 2, pp. 23–29, 2018.
3. Vujčić, D. Jagodić, and S. Ranić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in 2018 17th international symposium infoteh-jahorina (infoteh). IEEE, 2018, pp. 1–6.
4. S. Dalla Palma, R. Pareschi, and F. Zappone, "What is your distributed (hyper) ledger?" in 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). IEEE, 2021, pp. 27–33.
5. Y. Chen, H. Li, K. Li, and J. Zhang, "An improved p2p file system scheme based on ipfs and blockchain," in 2017 IEEE International Conference on Big Data (Big Data), 2017, pp. 2652–2657.
6. M. M. Sudhakar, K. Madanu, B. M. Kumar, V. S. Sankeerthana, and D. S. K. Naik, "Blockchain based evidence management system," *Journal of Survey in Fisheries Sciences*, pp. 2631–2636, 2023.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details