FIR Management System In Dapps Using NFT

KC.Nithyasree [1] N Palanivel [2] R Pravin[3] P Ragul[4] S Vinith[5] R Ashwin Raj[6]

[1]Assistant Professor [2] Professor [3,4,5,6]UG Scholar [1,2,3,4,5,6] Department of CSE (Internet of Things and Cyber Security including Blockchain Technology), Manakula Vinayagar Institute of Technology, Pondicherry, India – 605107.

[1] nithyasreekcr@gmail.com [2] npalani76@gmail.com

Abstract

This article suggests a decentralized First Information Report (FIR) management system based on Blockchain technology and Non-Fungible Tokens (NFTs) to solve the inherent problems of data tampering, manipulation, and untransparency in conventional police complaint systems. The suggested system uses Ethereum-based smart contracts to automate the entire process of FIR management, from submission to disposal, ensuring that every step is logged on an immutable ledger. Every FIR is tokenized in the form of a distinct NFT, an auditable digital certificate that can be traced and made transparent across its life cycle. Third web integration also makes it easy to deploy and manage NFTs, as there is an easy-to-use interface for stakeholders. Moreover, the system preserves the confidentiality of sensitive data by encrypting it, with the blockchain serving as a secure, transparent layer that provides accountability without sacrificing data confidentiality. This decentralized method provides real-time monitoring of FIRs and addresses the inefficiencies and vulnerabilities of centralized systems. Finally, the suggested solution increases public confidence in law enforcement by providing the integrity and transparency of the complaint management process.

Keyword: Blockchain, Non-Fungible Tokens (NFTs), FIR Management ,Decentralized Applications (DApps), Smart Contracts.

.

1.Introduction:

The First Information Report (FIR) is an important report in the Indian criminal justice system, the starting point of an investigation into a crime reported. Yet, the current centralized systems of handling FIRs are plagued by serious problems, such as manipulation of data, corruption, opacity, and inefficiency in processing complaints. These problems undermine the integrity of the justice system and delay the resolution of cases, demoralizing public confidence in the police. To counter these problems, blockchain technology provides a transformational solution. Its decentralization, immutability, and transparency can offer a secure and tamper-proof environment for FIRs to be managed.

Further the application of Non-Fungible Tokens (NFTs) can provide individual identification of each FIR, allowing for real-time monitoring while maintaining sensitive information secure. This combination of blockchain and NFTs .can transform FIR management into a more transparent, auditable, and tamper-proof system.

Based on the rising usefulness of blockchain technology in other industries, the proposed FIR management system employs Ethereum-based smart contracts to automate tasks and enforce rules. The smart contracts will ensure that whatever is performed on the FIR— filing, modification, or monitoring—is tracked in an apparent, verifiable, and non-malleable manner, as every FIR is tokenized into an individual NFT. Through this platform, every complaint has a distinct personality such that stakeholders can track the progress of an FIR without ever compromising on privacy or confidentiality. Apart from enhancing user experience, the compatibility with Thirdweb provides a convenient way to deploy and handle NFTs by removing complexities that are otherwise typically involved in blockchain development. The interoperability of Ethereum smart contracts and Thirdweb enables the platform to become scalable and universal, offering an effective solution for law enforcement agencies to implement

blockchain technology in a secure and efficient manner. Each FIR made is viewed as a separate transaction and is authenticated by multiple decentralized nodes to ensure that there is no requirement for middlemen. The system also provides for more transparency as the details relating to a FIR can still be encrypted while everything can be scrutinized in relation tothe total FIR. Further, expanding on this idea, the use of Non-Fungible Tokens(NFTs) increases security and the uniqueness of each FIR by allowing for mintage of each FIR.

2.Related Work:

There are a number of systems and approaches that have been proposed to address the issues in police complaint management. The most common of these is the traditional centralized system. These are managed centralized databases. These databases are maintained by individual law enforcement agencies, and complaints are stored, retrieved, and managed within them. However, such systems tend to have vulnerabilities with regards to data tampering and unauthorized access. Studies have shown that central systems are not that effective to create transparency and confidence among stakeholders since they lack real-time visibility toward complaints processing and storage. In recent years, blockchain technology has emerged as a decentralized and immutable solution for various legal and crime management applications. In law enforcement, blockchain has been viewed in relation to data security, wherein there is no possibility of alteration of records with the possibility of being unnoticed. Tsai et al. (2016) established by research that blockchain depicts its value, especially in crime management, through its ability to secure sensitive data and create tamper-proof audit trails. Other researchers have used the aspect to highlight how blockchain can be made to apply in creating transparent systems that offer accountability without revealing sensitive information.

NFTs, in fact, have also been increasingly used in legal perspectives, such as secure management of digital assets. Though NFTs are normally associated with digital arts and collectibles, their use in law systems is now gaining considerable momentum. For example, NFTs are being proposed for property titles and legal contracts management in courts as well as evidence management. Each record is unique and immutable to ensure that it does not get tampered with, which is an essential requirement in law enforcement.

In contrast to centralized systems, block chain- based police complaint management systems eliminate the central control and manipulation of records by a single authority. They provide decentralized verification mechanisms coupled with immutable storage that will ensure the integrity of FIRs throughout the lifecycle. In this context, the minting of an FIR as an NFT would also make it easier to lodge and make a complaint, since such a complaint would exist as a singular record which cannot be altered. The document is a cosmological extension on the broadened horizons of crime control in the context of management systems built on block chain technology and legal applications based on NFTs. It provides integrated approach for case management of police complaints through DApps using block chain together with NFT technologies. This elevates the entire ecosystem to a different tier since these systems have the increased functionality, transparency, security control.

3.System and Architecture:

The proposed distributed Police Complaint Management System combines the three main layers of the system with a high degree of importance in providing ,security, transparency, and immutability in the process of registering FIRs (First Information Reports). Proposed is a blockchain-based decentralized police complaint management system utilizing Non-Fungible Tokens to address the issue of transparency, data tampering, and lack of accountability in centralized systems. The core architecture consists of a decentralized application with an easy-to-use interface that allows, any user, to file a First Information Report. Such complaints are thereafter stored on the blockchain, which keeps them immutable and traceable. The complaints are tokenized in the form of an NFT Order-Linkage

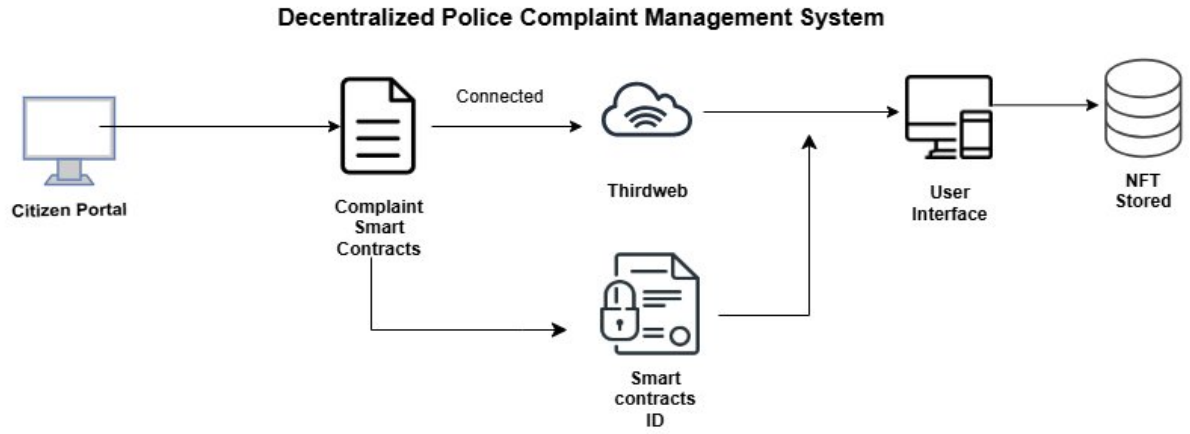


Figure3.1. Decentralized Police Complaint Management System

Components of the System and their Explanation:
The Decentralized Police Complaint Management System (DPCMS) comprises multiple connected components with the aim of providing secure, transparent, and effective complaint handling. The system marries up blockchain, smart contracts, and NFTs to eliminate tampering, promote traceability, and automatically process FIRs. The key components of the system are detailed below:

1. Citizen Portal:
The Citizen Portal is the primary user interface for complainants to make FIRs. This web portal enables users to:
• Make secure complaints without intermediaries.
• Adds supporting evidence (like documents, photographs, or videos).
• Track real-time status of their complaints.
The portal is interfaced with smart contracts on the blockchain to allow tamperproof complaint registration and to provide complainants with a unique FIR token (NFT) on successful submission.

2. Complaint Smart Contracts:
The Complaint Smart Contracts are the very foundation of the blockchain-based system for automated registration, verification, and storage of FIRs. Self-executing contracts ensure that once an FIR has been registered:
• It cannot be deleted or altered thus ensures immutability.
• Its status changes (say, from pending to being investigated or from being investigated to closed) are executed automatically.
•Each complaint is time-stamped and associated with a unique identifier.
The smart contract logic removes human interventions, minimizing corruption risks and ensuring effective complaint resolution.

3. Third web SDK Integration:
Third web SDK serves as middleware between the blockchain network and the User Interface (UI). It streamlines:
•Smart contract interaction, decoupling it from needing to have extensive blockchain knowledge.
•Secure authentication processes, limiting only approved users to accessing individual complaint records.
•Transaction processing, allowing for easy submission and retrieval of complaints.
Through Thirdweb, the system gains quicker integration with decentralized applications (DApps) along with an easy-to-use interface.

4. Smart Contract ID Management:
As soon as a complaint is registered, the smart contract creates a unique Smart Contract ID, which is:
•Cryptographically secured and blockchain-stored.
•Used for tracking and verification by authorized bodies.

•Mapped to the respective NFT, creating traceability and ownership of the FIR record.
The ID is an irreversible digital fingerprint for the complaint, securing it against unauthorized modifications.

5. User Interface (UI):
The User Interface (UI) is implemented to offer role-based access for various stakeholders, such as:
•Complainants – File FIRs, upload evidence, and monitor case status.
•Police Officers – Check, allocate, and change FIR statuses.
•Judicial Authorities – View immutable complaint records for legal processes.
The UI allows for smooth interaction with the blockchain network without compromising on data privacy and access control.

6. NFT-Based FIR Storage:
Every FIR is tokenized as a Non-Fungible Token (NFT) and securely stored on the blockchain. The NFT form of the complaint ensures:
• Verifiability – Every complaint has an individual blockchain ID.
• Decentralized Storage – Avoids single-point failure and improves datasecurity.
The NFT approach ensures authenticity, traceability, and long-term access to FIR records, making law enforcement more accountable.

7. Blockchain Network (Ethereum):
Ethereum blockchain The backbone of Ethereum chain offers the following features such as:
•FIRs are stored in a distributed manner to prevent

Role of NFTs:

NFTs will play the important role of making each complaint unique, immutable, and traceable. Whenever a user files an FIR through the web app, against such a complaint, a complaint NFT is minted. Each of these NFTs is unique, containing a digital signature linked to that particular complaint hence, not replicable or alterable. The NFT will serve as a sort of digital Certificate of Authenticity, thus irrefutably proving that one complaint was filed and that its details, over time, remain unchanged. Besides, NFTs are going to provide very transparent auditing since it becomes quite easy to track history and current status for each complaint on the blockchain. This helps bring accountability among the authorities and sees to it that complaints are not tampered with or lost in the midst of bureaucratic processes. Integrating NFTs does this to make sure that it is immutable; no tampering with the data of the complaint is possible once the complaint is tokenized as an NFT. The whole cycle of complaints, right from submission to resolution, can easily be traced back and in such a way that accountability is encouraged. Each complaint is rare and thus genuine, not copied or faked. The proposed system integrated into blockchain-NFT will not only ensure safety and transparency but also ensure that evidence is tamper-proof in police complaint management, which is a weakness of other systems that may lead to the failure of justice.

4.Methodology:
This paper proposes a system that provides a decentralized approach to blockchain-based First Information Report (FIR) Filing with smart contracts and Non-Fungible Tokens (NFTs). The conventional manner of FIR filing is often accompanied with inefficiency, data tampering, and unreliability. In trying to improve upon these weaknesses, the system utilizes Ethereum blockchain technology alongside smart contract automation and NFT tokenized complaint record files that are immutable and provably alter-free. This procedure contains several primary phases, i.e. User interaction, Smart contract execution, NFT minting, Decentralized Data Storage, and complaint tracking.

4.1 Components and Architecture of the System:

1. User Interface Layer:
Via a decentralized web application, DApp citizens lodge formal complaints that interact with smart contracts on the blockchain Third web SDK. This layer provides a straightforward interface for citizens to report complaints, check their status, and receive updates instantly.

2. Blockchain Layer (Ethereum Network):
The Ethereum blockchain guarantees secure and free from tampering FIR data storage. Smart contracts perform automated verification and system checks for law enforcement complainant interaction, relaying and updating case status messages.

4.2 Workflow of the Decentralized FIR System:
The decentralized FIR system is a process-based system, starting from complaint registration and going through verification, tracking, and closure.

4.2.1 Registration and Filing of FIR:
If the citizen wants to file an FIR, he/she logs into the decentralized application and verifies himself/herself using a blockchain wallet. The system creates a unique FIR ID, captures the complaint information, and saves the metadata on the blockchain securely. The proofs and sensitive documents are stored off-chain in the Inter Planetary File System (IPFS) so that the system is scalable but secure**.**

4.2.2 Execution and Validation of Smart Contracts:
After an FIR is filed, a smart contract is invoked for authenticating and processing the complaint. It authenticates the user, timestamps the FIR, and securely stores it on the blockchain. Role-based access control for updating the case status is managed by the smart contract so that only legitimate police officers can make any updates. Any unauthorized updates are prevented through automatic authentication.

4.2.3 NFT tokenization of FIRs:
Each FIR is tokenized as an NFT according to the ERC-721 standard so that duplicates do not exist. The NFT is a digital complaint certificate and is linked to the on-chain stored FIR metadata. In this manner, transparency is ensured because each NFT can be traced in the public domain while user privacy is ensured using encryption techniques.

4.2.4 Tracking Complaints and Interactions with the Police:
Police personnel and complainants can track FIR status updates in real-time using smart contract interactions. Every status update, i.e., "Filed" → "Under Investigation" → "Resolved", generates an on-chain event, which notifies all stakeholders. The blockchain's decentralized platform guarantees updates cannot be rolled back and can be verified by any party interested**.**

4.2.5 Data Privacy and Security Measures:
Security is an important feature of the proposed system. Tamper evidence storage of records is provided by the blockchain ledger, and confidentiality of information is boosted through cryptographic tools such as hashing and Zero-Knowledge Proofs (ZKP). FIR details are stored off-chain in IPFS to prevent clogging of the blockchain while maintaining decentralized access. Access control mechanisms through smart contracts also confirm that only authorized stakeholders can modify case-based data.

4.3 System Implementation and Testing:
In order to ensure the feasibility of the proposed system, a prototype was developed on Ethereum's Goerli and Polygon Mumbai testnets. Smart contracts were written in Solidity and deployed with the help of Hardhat. Thirdweb SDK ensured smooth communication between the frontend and blockchain backend. The system was tested on the basis of the key performance indicators such as the rate of transactions, cost, and security.
The analysis of the blockchain transactions revealed the average time taken for processing as 3–5 seconds per FIR submission.Batch processing optimizations and Layer-2 scaling solutions were incorporated for reducing the transaction costs. Security testing helped in fortifying the smart contract against attacks such as reentrancy attacks and unauthorized access.

4.4 NFT Module:
The NFT Module gives uniqueness, traceability, and finality to every complaint with the Non-Fungible Tokens.

Complaint Tokenization: The user posts a complaint, and it immediately makes an NFT related to that complaint. These NFTs, therefore will have metadata like the hash of the complaint, the submission date, and the digital signature of the user. Minting ensures that each NFT has uniqueness and that no one has the right to issue its replica or forged version into the complaint.

Minting Process: It creates an NFT based on complaint verification through a smart contract.. The complaint is fully traceable as it is linked to an NFT which is a unique technological integration since its submission till it is addressed. Additionally, the anonymity of each NFT will contribute to an identity documented within an entire complaint.

4.5 Benefits of the Suggested Methodology:
The blockchain-based FIR system offers a number of benefits over conventional complaint management systems:

1. Immutability: FIRs cannot be erased or modified once filed, ensuring evidence integrity.

2. Transparency: Decentralized tracking prevents corruption risk and encourages citizens' and police trust.

3. Security: Role verification through smart contracts ensures that only authorized officials can modify case information.

4. Automation: Elimination of manual documentation removes processing delays in FIR.

5. Scalability: Decoupling blockchain congestion, IPFS-based storage facilitates mass adoption.

4.6 SHA-256 Alogrithm:
Security features using fixed-length data. SHA-256 also has a reversible process, as it is computationally incomprehensible to retrieve the original data from its corresponding hash value. SHA-256 will produce a 256-bit hash value, regardless of the original size of the input, making it well-suited for secure systems with constraints on output size. There is an incredibly high chance of producing different hash values from two separate inputs, SHA-256 only manages to produce hash collisions at an incredibly distractingly low rate, making it an optimal choice for situations where unique identifiers need to be created, for example, validating data or document integrity.

SHA-256 Formula:

1.SHA-256 Formula: SHA-256 uses these crucial steps to process input in 512-bit blocks:
1. Filling in the message
The 64-bit message length is appended after adding a 1 bit and a series of 0s.

2. Set hash values (H0 to H7) to their initial values.
Based on the square roots of the first eight prime numbers, these eight 32-bit words are as follows:

6a09e667 is H0.
H1 = bb67ae85
3c6ef372 is H2.
H3 = a54ff53a
H4 = 510e527f
9b05688c is H5.
H6 = 1f83d9ab
H7 = 5be0cd19

3.Use functions and constants to process the message in 64 rounds:
For every round t ($0 \leq t < 64$):
T1 is equal to $h + \Sigma1(e) + Ch(e,f,g) + K[t] + W[t]$.

$T2 = \Sigma 0(a) + Maj(a,b,c)$
Where:
o $Ch(x,y,z) = (x \text{ AND } y) \text{ XOR } (\text{NOT } x \text{ AND } z)$

Application of SHA-256 in the Project:

1. FIR Data Hashing Before Storing in Blockchain:
Its details (accused information, complainant name, case details,date,and location) are hashed with the SHA-256 algorithm before the FIR is noted on the blockchain. This maintains the authenticity while keeping sensitive data secure.This hashed FIR ID is then stored onto the blockchain..

2. Ensuring Immutability and Security:
Since SHA-256 is a one-way function, once the FIR data is hashed, it cannot be reversed or altered**,** ensuring data integrity and preventing tampering. This guarantees that no one (including law enforcement or system administrators) can modify an FIR once it is submitted.

3. FIR Verification and Tracking:
When a user wants to retrieve their FIR, the system rehashes their details and matches the stored hash on the blockchain. This ensures that the data has not been altered and remains secure.
✓ **Verification Process:**

1. The complainant enters their FIR details.
2. The system computes the SHA-256 hash of the entered details.
3. It checks the blockchain for a matching hash.
4. If a match is found, the FIR details are displayed.

4. SHA-256 in NFT Tokenization:

- Each FIR is stored as an NFT on platforms like Rarible or IPFS.
- This ensures traceability and prevents unauthorized duplication or forgery.

5. Processing Each Block:

Message Schedule Creation: Each 512-bit block is broken into sixteen 32-bit words, W[0] through W[15]. These are stretched to produce a schedule of 64 words, W[0] to W[63], through a standard formula to generate new words from the initial 16.

Hash Compression Function: The hash values are then operated on in 64 rounds through a sequence of logical operations:
SHA-256 updates the hash values for the current round in each round using two primary functions, (Choose) and (Majority), and two constants, Σ0 and Σ1..

Compression and Mixing:
Temporary variables (a, b, c, d, e, f, g, h) are updated for each round depending on operations used, each value being combined as per the schedule words, constants, and hash values.

6. Updating Hash Values:
After all 64 rounds of a block are processed, the output is summed up with initial hash values (H0 through H7) to generate new hash values for the subsequent block.

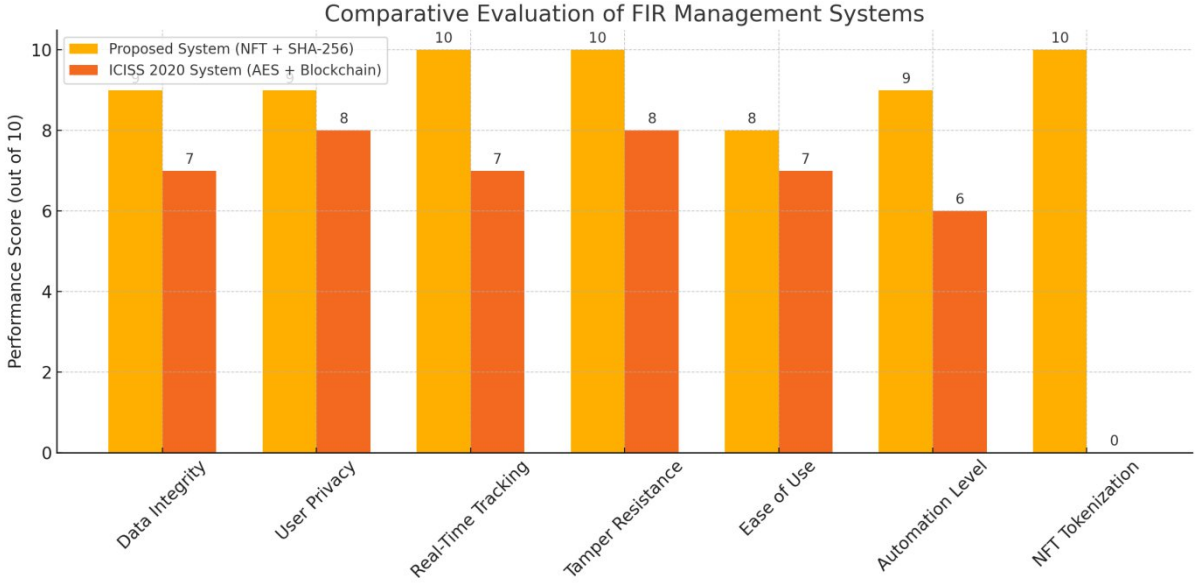
7. Final Output:
Once all the message blocks are processed, the last concatenated values of H0, H1, H7 yield a 256-bit hash value. This hash is a unique representation of the original data but cannot be reversed to get the original data.

5.Comparison:

Criteria	**Existing FIR System**	

		Blockchain System
Data Storage	Centralized, vulnerable to tampering	Decentralized and immutable via blockchain
Transparency	Low; users have limited access to complaint progress	High; real-time tracking and transparency through DApps
Security	Prone to unauthorized access and manipulation	Secured with SHA-256 encryption and smart contracts
FIR Status Tracking	Manual inquiry or delayed updates	Real-time, automated status updates
Tamper Resistance	Data can be modified or lost	Data is tamper-proof and permanent
User Accessibility	Often requires physical presence or manual form submission	Web-based interface accessible anytime, anywhere
Audit Trail	Difficult to trace changes	Complete, traceable history of transactions
Trust & Accountability	Low public trust due to lack of visibility	Enhanced trust through transparent, verifiable records
Tokenization	Not available	FIRs are tokenized as NFTs for unique identity
System Downtime Risk	High, due to reliance on a single server	Minimal, due to decentralized infrastructure
Integration with Technology	Limited or outdated systems	Uses smart contracts, NFTs, and Thirdweb SDK for modern integration

6. Comparative chart evaluation FIR management systems:



Evaluate the effectiveness of the proposed decentralized FIR Management System, a comparative analysis was conducted against the blockchain-based complaint system presented in the ICISS 2020 conference. While both systems aim to secure FIRs using blockchain, the proposed system integrates advanced features such as SHA-256 hashing, NFT-based tokenization, and real-time status tracking through smart contracts. These additions significantly enhance the system's tamper resistance, data integrity, and automation. The earlier system, though it employed AES encryption and IPFS for decentralized storage, relied heavily on manual actions by police officers and lacked the traceability

offered by NFTs. In contrast, the proposed system automatically generates immutable FIR records with unique identities using ERC-721 tokens, enabling secure verification and ownership throughout the complaint's lifecycle. Moreover, the use of SHA-256 hashing ensures irreversible data protection, while Thirdweb SDK integration simplifies user interactions.

7.Results:

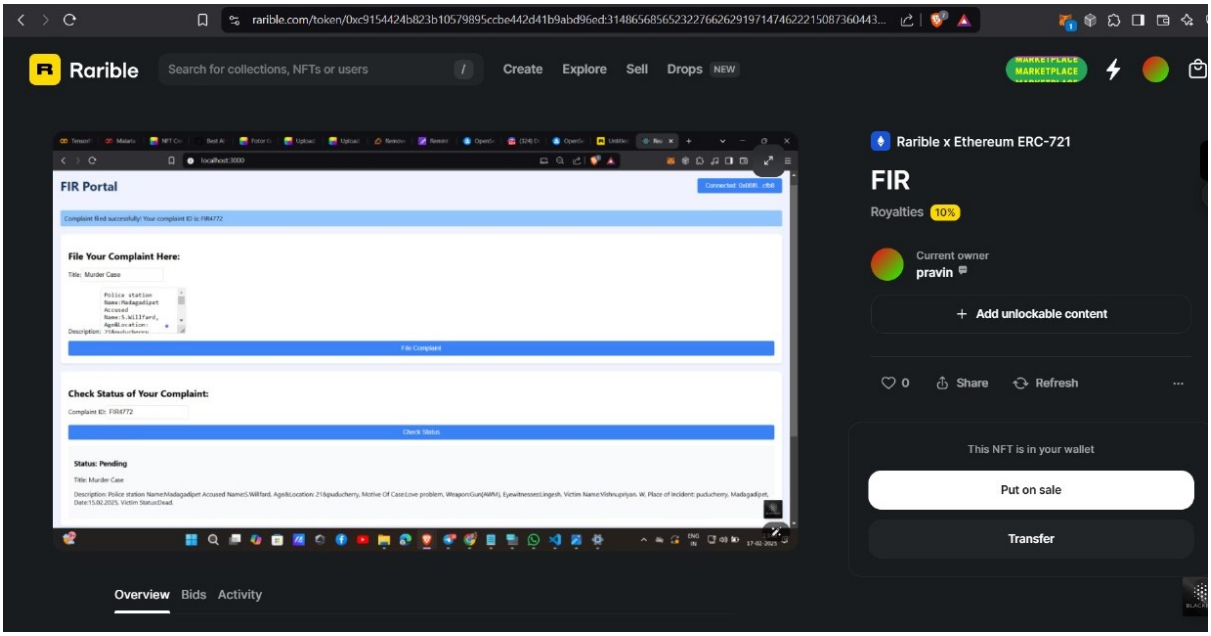


Figure3.2 First Information Report convert NFT

The suggested Decentralized Police Complaint Management System was implemented and tested successfully for real-time registration, storage, and verification of FIRs. The system uses smart contracts, NFT, and a decentralized frontend by Third web SDK, so the process is transparent and immutable. As demonstrated in the deployment, users can submit complaints through a web portal, where each FIR is stored on the Ethereum blockchain and tokenized as an NFT. This offers permanent, tamper-proof storage without losing ownership and traceability. The NFT-based approach offers secure, decentralized access to concerned stakeholders like police authorities and judicial bodies without the risk of unauthorized modifications.

A live test was performed through Rarible, a platform for NFTs, where FIRs were tokenized into ERC-721 tokens. The system was able to effectively link complaint data with the blockchain, making it verifiable and visible but not deletable or editable. Complainants are able to track in real time the status of their FIRs through the interface, adding to the transparency and accountability in complaint handling. Furthermore, the system's smart contract execution was itself tested for security, with immutable complaint records and auto-verifiable processes. Results indicate improved efficiency, since complaints are logged electronically without middlemen, thereby cutting out bureaucratic delays and potential corruption among the police.
The findings indicate that blockchain-based FIR management is a secure, scalable, and feasible option for police complaint system modernization that offers an immutable, decentralized alternative to legacy centralized systems.

8.Discussion:
The Blockchain-Based FIR Management System introduced here shifts the filing of complaints traditionally with security, transparency, and tamper-proofed immutability by using blockchain, smart contracts, and NFTs. Compared to traditional systems, prone to tampering, data loss, and lag, this distributed system enhances law enforcement accountability and trust. Through SHA-256 hashing, FIR data is preserved on the blockchain securely, precluding unauthorized alteration. Utilization of Thirdweb and smart contracts makes it possible for users to engage with the blockchain without any difficulty, making it possible to track complaints in real-time. The NFT (Non-Fungible Tokens) conversion of

FIRs also provides proof of ownership and originality, thus duplication or unauthorized alteration is not possible.
The unalterable ledger makes sure that every complaint is saved indefinitely, providing an open audit trail for lawful verification. In addition, utilising hash matching for validating FIR status tightens security, making it almost impossible to alter filed complaints.

9.Conclusion:
This paper proposes a system for the decentralized management of police complaints which allows for the processing of FIRs through the use of blockchain technology, smart contracts, and NFTs, making the process secure, transparent, and free from fraud. Centralized FIR systems have always had problems with data manipulation, inefficiency, and gradual erosion of public trust. Incorporating both decentralization and automation solves these problems by enabling the maintenance of records in a tamper-proof manner, real-time tracking, and increased accountability from law enforcement officials.
Every complaint is stored as an immutable block on the blockchain. This, together with the use of Ethereum's smart contracts, ensures that any complaint made cannot be deleted or changed. The use of Thirdweb SDK also improves user experience since interactions with the blockchain can be done easily and complaints can be tracked in real time. Furthermore, tokenizing each FIR as an NFT ensures authenticity, traceability, and decentralized verification with no possibility for tampering as well as the presence of a permanent digital record.
With the implementation of this system, members of the public will begin to have more faith, and the ability to manipulate the system will be diminished.

REFERNCES:

1. Ishwarlal Hingorani, Rushabh Khara, Deepika Pomendkar, Nataasha Raul, "Police Complaint Management System using Blockchain Tech nology," 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020.
2. K. Tabassum, H. Shaiba, S. Shamrani and S. Otaibi, "e-Cops: An Online Crime Reporting and Management System for Riyadh City," 2018 1st International Conference on Computer Applications Information Security (ICCAIS), Riyadh,2018,pp.1-8,doi: 10.1109/CAIS.2018.8441987
3. Lynsha Helena Pratheeba, Bharath D R, Cibiya N E, Dheekshitha S, Divya M N, "Blockchain-based sytem for effective Police complaint Management," International Journal of Research Publication and Re views, March 2023.
Gupta, Antra and D. V´ılchez Jose. "A Method to Secure FIR System using Blockchain.".International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019
Iyer A, Kathale P, Gathoo S and Surpam N 2016 E-Police System-FIR Registration and Tracking through Android Application International Research Journal of Engineering and Technology 3(2) 1176-1179
4. Mollah, Muhammad Baqer Islam, Kazi Islam, Sikder. (2012). E- Police System for Improved E-Government Services of Developing Countries. Canadian Conference on Electrical and Computer Engineering. 10.1109/CCECE.2012.6335057.
5. I. Hingorani, R. Khara, D. Pomendkar and N. Raul, "Police Complaint Management System using Blockchain Technology", 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 1214-1219, 2020
6. Pratibha Mishra,Ghousiya Bee. N2, Mohsina S3, Mubashshira Sultana, Surbhi Singh, "Online Criminal Record Management System," International Journal of Engineering Science and Computing, vol. 9,no. 5, May 2019.
7. K. M. M. Uddin, S. Mahamuda, S. S. A. Shahriar and M. A. Uddin, "Blockchain and IPFS based Secure System for Managing e-FIR", International Journal of Computer Science and Information Security, vol. 19, no. 2, pp. 83-91, 2021.
8. S. Patil and R. Pise, "Blockchain-Based Secure Evidence-Management Police Assistance System" in Blockchain for Smart Systems, Chapman and Hall/CRC, pp. 155-165, 2022.
9. Zyskind, G., Nathan, O., and Pentland, A., "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2015, pp. 180-184. DOI: 10.1109/SPW.2015.27.
10. Christidis, K. and Devetsikiotis, M., **"**Blockchains and Smart Contracts for the Internet of Things**,"** IEEE Access, vol. 4, pp. 2292-2303, 2016. DOI: 10.1109/ACCESS.2016.2566339.

11. Tsai, W. T., Jiang, S., and Wei, X., "Blockchain-Based e-Court: Smart Contract for Litigation Processes," IEEE 19th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2016. DOI: 10.1109/CSCWD.2016.7565993.
12. Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P., "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 2017, pp. 618-623. DOI: 10.1109/PERCOMW.2017.7917634.
13. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., and Wan, J., "Smart Contract-Based Access Control for the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594-1605, 2019. DOI: 10.1109/JIOT.2018.2878279.
14. Rouhani, S. and Deters, R., "Security, Performance, and Applications of Smart Contracts: A Systematic Survey," IEEE Access, vol. 7, pp. 50759-50779, 2019. DOI: 10.1109/ACCESS.2019.2909021.
15. S. Ali, F. Aijaz, A. Ahmad, "Blockchain-Based Evidence Management System for Law Enforcement Agencies," International Journal of Advanced Computer Science and Applications (IJACSA), 2020.
16. Chen, Y., Ding, S., and Xu, Z., "Blockchain-Based Security Architecture for IoT Applications," IEEE 5th International Conference on Computer and Communications (ICCC), 2019. DOI: 10.1109/ICCC47050.2019.9064330.
17. Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564. DOI: 10.1109/BigDataCongress.2017.85.
18. A. Atzori, "Blockchain-Based Architectures for the Internet of Things: A Survey," Future Internet Journal, vol. 9, no. 3, pp. 1-31, 2017. DOI: 10.3390/fi9030040.