IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review On Enhancing Transparency And Security In Fir Using Blockchain Technology

1Shivendra Pratap Singh, 2Mohit Rajput, 3Ashish Kushwaha, 4Nandini Goel, 5 Sumathi S

1,2,3,4,5Department of Computer Science and Engineering

JSS Academy of Technical Education, Noida, India

Abstract:

This review paper explores the integration of blockchain technology with the First Information Report (FIR) to address the challenges which are faced nowadays like data integrity, transparency in the judicial system and security in our data management agencies. Our traditional FIR system faces challenges such as data tampering, unauthorized access, and lack of transparency as its centralized and only authorized persons can access it. With the use of blockchain technology in FIR management we are making the system decentralized, immutable and secure. In this way we are making our FIR system totally secure and no unauthorized person can tamper the data thus making it trustworthy. In our model we are using Proof of Stake protocol and smart contracts which helps to secure the data and makes the registration, modification process fully transparent. With the use of advanced cryptographic techniques like SHA hashing, we are making the data encrypted and blockchain ensures that sensitive FIR data remains secure and only authorized users such as investigators or the person who has lodged the FIR can view it online. This approach not only enhances the reliability and trustworthiness of FIR records but also significantly improves the efficiency of law enforcing agencies by making the process of data management in FIR automatic. Ultimately, the integration of blockchain technology in FIR holds the potential to revolutionize law enforcement data handling, ensuring accountability, transparency and security in FIR investigations.

Index Terms — Blockchain, Smart Contract, Decentralized, Security, Information

Introduction

In today's date, the world's biggest democracy India is dealing with a high and increasing crime rate while ensuring speedy and transparent clearance of criminal cases. Extremely well-developed legal setup has been provided. Owing to the complexities present while procedures followed in case of registration and disposal of the FIRs, in which this system is coupled by delay and also diminish the law enforcing agencies capacity so that they could have handled the situation accordingly on arising of the crime case. The integration of Information and Communication Technology has become inevitable in smart cities to enhance urban governance. It has the capability to contribute to economic development, optimal use of resources, and improved mobility, besides

safeguarding citizens' privacy and security. One of the applications of ICT in law enforcement is digitalization of police complaints. The new technology that promised solutions to streamline and secure FIR is blockchain.

Blockchain technology that brought the application of cryptocurrencies into prominence, such as Bitcoin, represents a decentralized, secure, and transparent approach towards data management. It thereby provides a strong remedy against the issues of data integrity and security that afflict the conventional centralized systems. Data relating to FIRs is currently kept in local servers that are susceptible to manipulation and unauthorized access by the law enforcement agencies. Blockchain technology introduced in the e-FIR system allows the registration of every FIR transaction on an immutable and transparent ledger. Once data is imprinted on the blockchain, it cannot be modified, and hence it becomes tamper-proof, and resistant to fraud. Since blockchain is distributed, the case information will be available and exchangeable between police departments or agencies while getting secured in a timely manner with data integrity.

This paper describes two prominent contributions aimed at meeting the above challenges in FIR management. First, a blockchain-based framework has been proposed to ensure the integrity and security of electronic FIR data in particular within the smart city scenario. It's based on the decentralized characteristic of the blockchain to produce an open and permanent record of all FIRs submitted with minimal possibilities of false or unauthorized alterations. This makes the process of e-FIR minimize the possibility of false registrations of FIRs by the presence of smart contracts. Smart contracts are self-executing agreements characterized by specified conditions. They can automatically validate, which ensures that only authentic complaints are recorded, thus lowering the possibility of fraudulent submissions in the FIR system.

Besides security of data, blockchain technology also increases transparency and accountability within the police department. This will guarantee that all activities with respect to FIRs are recorded and traceable, ensuring an audit trail which authorized persons can trace. Apart from improving the public trust between the public and police, this enhances greater case processing efficiency. In addition, the block chain framework is very resistant to hacking and cyber threats and therefore difficult to lose data or manipulate illegal changes. The use of blockchain technology ensures that FIR data is permanently stored and accessed by those who are authorized and thus makes the different units of law enforcement agencies collaborate even better in criminal inquiry processes.

The subsequent sections of this paper have been designed as follows: Section II discusses an exhaustive review of the previous work done in this field. Section III discusses the proposed methodology on how we are going to implement the system. discusses the system architecture that encompasses the use of blockchain technology within the e-FIR registration process to enhance security and lower false registration cases. In Section IV, findings of implementation and assessment of the system will be presented to indicate that the proposed blockchain-based system has proved effective in making FIR management more efficient, secure, and reliable. Finally, Section V draws concluding remarks and discusses further research areas to continue working on this area with blockchain technology. With blockchain technology, huge improvements are created in the quality of law-enforcement services within smart cities, creating a safer, more secure environment for the population.

LITERATURE REVIEW

Here we are going to explore some of the reviews which were done on this technology in the past:

1. This new system, in support of blockchain technology, further improves the FIR process since operations are conducted more effectively, and records are not penetrable while making practices even more transparent among law enforcement agencies. A new system like this therefore indicates how emerging technologies can handle some of the traditional problems associated with the management of FIR but a few issues of scalability, privacy, and conformity to regulation have to be addressed. It concludes that incorporating smart contracts automatically

facilitates FIR tasks and reduces human error while increasing operational efficiency. Further research should focus on other consensus mechanisms, advanced encryption techniques, and cooperation with regulatory bodies in order to build a basis for a revolutionary FIR system that satisfies the digital needs of the 21st century. [1]

2. This paper explores the possibility of blockchain technology in developing an integrated policing system, based on the hierarchical structure of law enforcement organizations. Blockchain will improve security, immutability, and accountability in addition to bridging the communication gap between police departments across states and jurisdictions. The blockchain technology will overcome the problems of the existing system and bring it to a larger population by reducing the physical dependency on filing FIRs. Although currently only running on a limited test network, this system could have significant enterprise-level implementation. Future improvements to improve consensus mechanisms as well as scale the system to support private data transactions will help better protect sensitive information and increase victim privacy in prosecutrix cases. [2]

3. This research discusses the problems of data manipulation and security vulnerabilities inherent in the current police record management system. It introduces a solution based on blockchain technology to ensure integrity of offense data kept within police databases, while maintaining standards of privacy. The system proposed here employs a consensus-driven approach to secure data and encourages filing complaints by citizens, with an assurance that their reports will be recorded reliably. Simplification of the process for filing FIR brings benefits to police officers. Frontend has been carried out using React.js while Node.js is used as the backend; Ethereum was used for integrating blockchain while the database was Firebase. The proposed decentralized system circumvents the concept of reliance on trust from the stakeholder's perspective and saves against acts of dishonesty. Future research will tackle dynamic selection of hashing methodology based on criticality levels of offense and grouping. [3]

4. This paper examines the use of blockchain technology to address data manipulation and false reporting issues within police station record management systems. It presents a consensus-based approach that will ensure the integrity of offense data stored in police databases. The proposed system combines Matlab with the Ethereum blockchain using Python and Web3 RPC to securely oversee e-FIR transactions through smart contracts. The simulation will show the trade-off between transaction volume per block and different levels of hashing security for e-FIR data. Future work involves dynamic selection of hashing algorithms depending on the data classification and criticality and optimizes the usage of Gas by Ethereum to make the transaction efficient. [4]

5. This paper delves into a project aimed at enhancing security, transparency, and the efficiency of the e-FIR process by adopting the blockchain technology concept. The system offers increased data security, through the decentralized and immutable blockchain feature that ensures it becomes impossible to alter or temper FIR records without proper authorization. Also, it brings in increased responsibility and trust within the system. Future Scope of the Project Optimizing scalability and performance to be integrated with existing systems Real-world deployments Further Research The techniques such as sharding, sidechains, and layer 2 solutions for scalability and transaction throughput; continuous improvement in security; collaboration among law enforcement agencies. [5]

6. This paper examines the benefits of blockchain technology to guarantee integrity in digital records, reinforce information security, and enhance knowledge sharing among organizations. Blockchain, being decentralized, offers immutability, which mitigates data breaches and validates data origin, hence making transactions significantly safer in cryptocurrencies. In this paper, it is further pointed out how blockchain resolves issues concerning internet protocols with special references to Bitcoin transactions. Though the focus of the paper is on data trustworthiness and inter-organizational knowledge sharing, it draws out the fact that much research is needed to discover blockchain's potential in other industries. The paper calls for empirical approaches, like surveying based on TAM or UTAUT models, to understand blockchain adoption within organizations and firm-level data analysis to understand benefits through blockchain. More, the paper is advocating research into managerial challenges and challenges faced with widespread adoption of blockchain technology which may reveal more insight in overcoming such barriers and the improvement in technological development. [6]

7. This paper proposes a blockchain-based FIR data management system that would solve the issues of tampering with data, unauthorized access, and a lack of transparency that accompany the traditional FIR systems. Blockchain is decentralized, making this system provide data immutability, security, and transparency. The smart contracts will automate the registration and access of FIR data while having a secure user interface that grants access to FIR data only to the law enforcement officers and court administrators authorized. The framework applies hashing of SHA-256 toward evidence protection and FIR encrypted data to enhance the overall security measures. The proposed framework ensures increasing efficiency, effectiveness, as well as reliability of management over FIR for better use of law enforcement organizations. [7]

GAP ANALYSIS

PROPOSED METHODOLOGY

There are basically two types of user roles in the system. They are: Police and Citizen (User). Each kind has access to a type of web-based interface, providing the different functionalities. Design takes into account making it smooth and efficient, with security and transparency at all stages.

The system architecture is comprised of three key components:

Front End-Interface: This is an interactive web development application built using React.js. It allows the filing of FIRs and keeps tabs on the status of those FIRs while interacting with the system. The interface in itself is responsive, allowing proper functioning across devices. Also supports multiple languages to help provide information to a wider variety of people and has a chatbot to assist the users during the process of filing.

For blockchain backend: Ethereum and Solidity will be used for implementing the smart contracts in a blockchain system. The execution of submitting, approving, and updating the status of FIRs will be executed automatically by the smart contracts. Data of FIR are hashed that including details and metadata thereof to the blockchain for immutability and transparency. Blockchain gives an auditable tamper-proof record of any change done on the FIRs for preserving data integrity.

Off-chain Storage (IPFS): Since large files cannot be stored on the chain, evidence files, such as images, videos, or even documents which are a part of the FIR, are stored by using the InterPlanetary File System. The blockchain only stores the hash of such files; therefore, integrity is maintained and no one can modify those files. Thus, inefficiencies brought about by the storage of evidence on-chain are circumvented while integrity is still maintained.

The first step is when the user logs in to the system. Once having registered and validated his identity, the user gains entry to the FIR filing form. Such a form solicits relevant details of the incident-from what crime was committed to how much time it was the time and where. More importantly, the user will have the option of attaching his evidence in the form of photos, videos, and documents. Once done with the form, it shall be submitted to the system.

Upon submission, the FIR data is encrypted for its confidentiality and security. The encrypted data is then passed through a cryptographic algorithm (for instance, SHA-256) to generate a unique identifier for the FIR. That hash is then written to the Ethereum blockchain, which then makes the record immutable and transparent.

In case of larger files like images or videos, the evidence is uploaded to IPFS, and only its hash is kept on the blockchain. Thus, they are stored securely off the chain while the integrity of the files is maintained through the blockchain hash.

After submitting the FIR, it is passed to review where police personnel or concerned persons are given permission by logging into the system so that the verification of and approval for FIR could take place. It's in smart contracts wherein validation information takes place for checking completion, thereby making this more efficient.

The smart contract ensures that there is an absolute transparency in the process as no one can amend the FIR once it's filed. Once the FIR has been approved, its status automatically gets updated on the blockchain, and the user will also get a notification in respect of such an update.

Police officers can also update the status of the FIR filed in respect to the present case to be "under investigation, " "resolved, " or "closed" as investigations progress. All information about the parties is live through blockchain updations as well.

The citizen can check the status of his or her FIR by viewing its status in real time through the user dashboard. In this way, the citizen will get transparency and know what steps have been taken on his or her reported incident. Once the FIR has been approved and has been investigated, then the system will generate the PDF copy of the FIR, which the user will be able to download. This document contains all information required, and it also has been e-signed, thereby proving its authenticity.

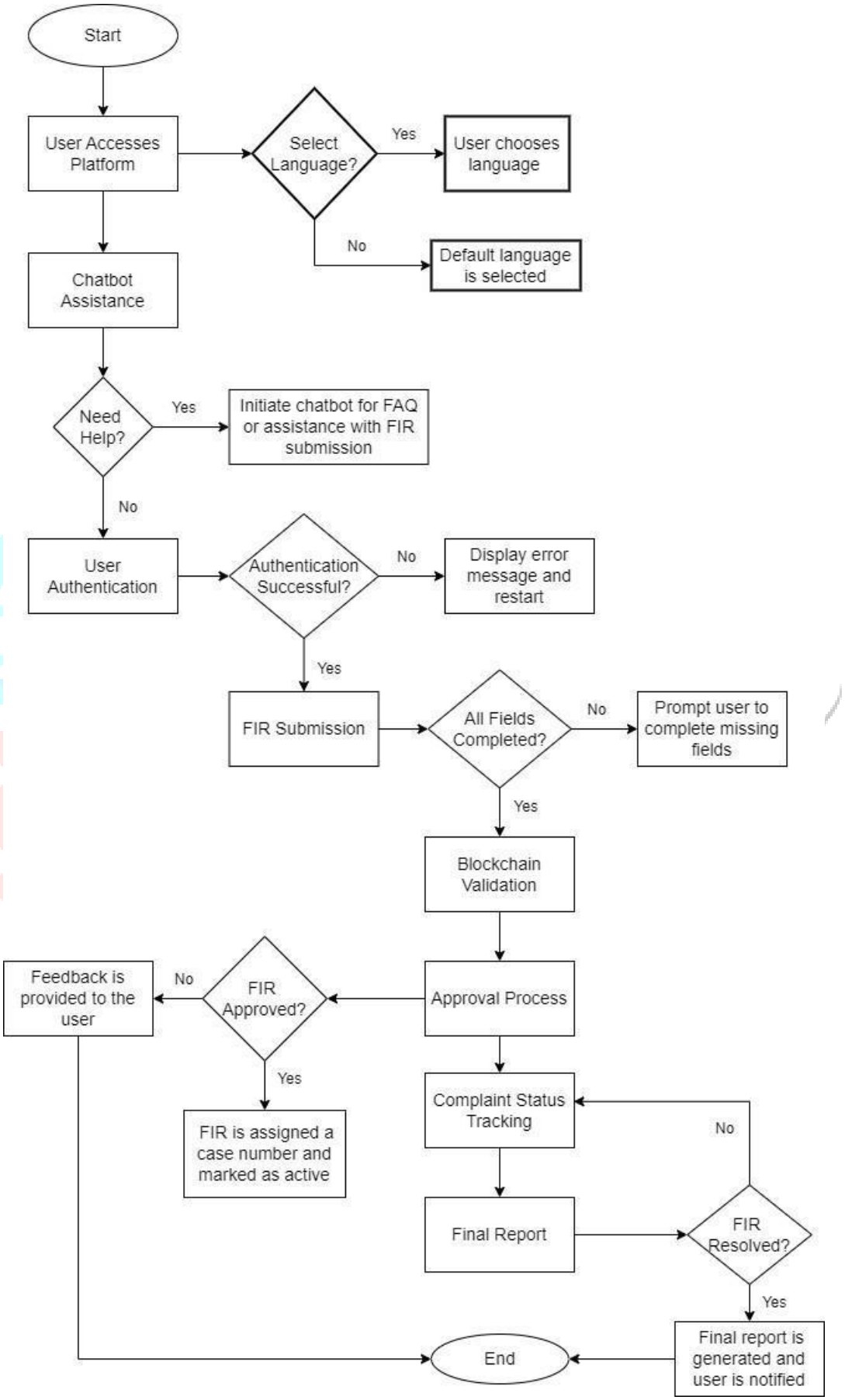

Fig 1. Blockchain based FIR management system

Proposed Methodology

The paper outlines the blockchain framework in two main constituents:

A decentralized and tamper-proof framework of blockchain ledgers and smart contracts for guarantees over authenticity of eFIRs, with proposed use: substituting with Ethereum, for the sake of simplicity.

User and admin credentials on the blockchain are collected and stored; hence, auditability will be ensured to prevent fraudulent submission of e-FIR.

The basic part of the framework is the public Ethereum blockchain that follows the proof-of-work consensus protocol. At the same time, it provides high-level transparency, ensuring there is encrypted privacy of information. The application programs running inside the framework produce unalterable records due to the nature of the smart contract applications developed to work on the Ethereum. The system puts such contracts into the blockchain while encryption protocols applied during such an integration process are totally elaborate. Both the security module and evidence that the user provides are put on a decentralized IPFS network. The transparent nature of Ethereum ensures that all the people involved in the blockchain gain access to the complaint data while keeping it private in nature and adhering strictly to security protocols. Within the network, there's the corresponding hash of the encrypted complaint and related proofs. A police officer, already present in the network, can invite more officers and crime reports and statistics will only be accessible to authorized people. The police take the FIR and transform it into a PDF encrypting it as outlined in the security module, noting appropriate hash on the Ethereum blockchain. The encrypted document then is stored in the IPFS network. A general idea on how IPFS works can be seen in fig 2.

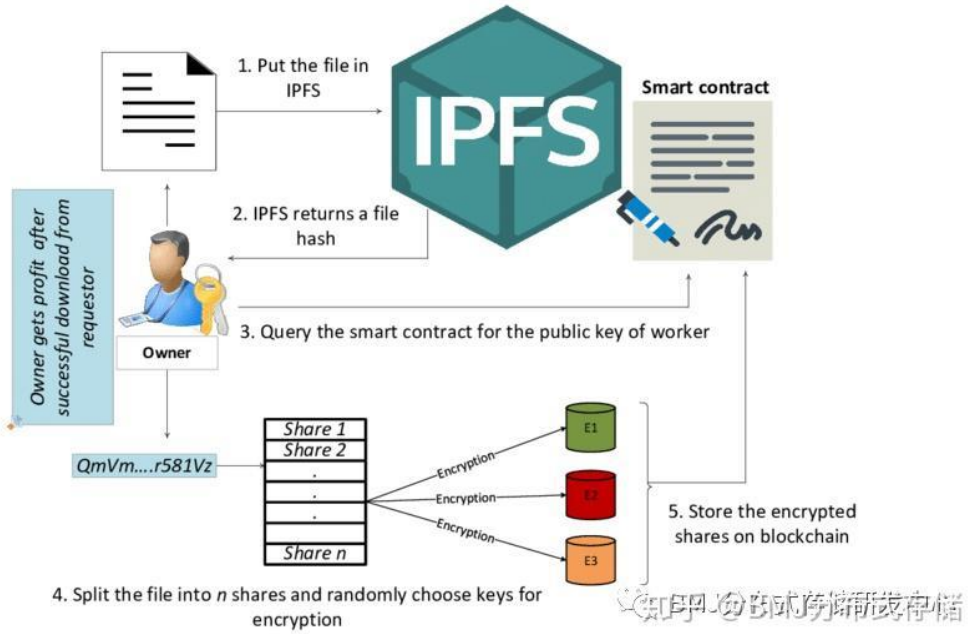

Fig 2. Blockchain integration using IPFS

Tools and Technology Used

In order to create and develop the proposed technology, the following softwares are used:

Technologies Used

CONCLUSION

In conclusion, blockchain proves to be an innovative answer to the centuries-old dilemmas of data tampering, inefficiency, and lack of transparency in record management processes within the systems of law enforcement. With its decentralized and immutable characteristic, blockchain increases the safety and reliability of sensitive information, such as FIRs and police records, besides increasing accountability and trust in stakeholders. This approach enables smooth interdepartmental communication and procedural workflow streamlining; it reduces dependency on traditional methods that might be error-prone. Scalability, privacy, and regulatory compliance remain areas of research. Thereupon, it will easily achieve a strong yet not least efficient blockchain-enabled policing framework meant to revolutionize the concept of how law enforcer systems are operated as well as accessed in a digital and new age.

REFERENCES

T. S. Mistry, B. B. Gor, R. K. Shukla and R. Sharma, "Easy-to-Use First Information Report (FIR) System Using Blockchain," 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2024, pp. 1655-1660

A. M. Das and N. Subramanian, "Implementable Smart FIR Management," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-5.

S. Mehta, K. S. Kumari, P. Jain, H. Raikwar and S. Gore, "Blockchain driven Evidence Management System," 2023 3rd International conference on Artificial Intelligence and Signal Processing (AISP), VIJAYAWADA, India, 2023, pp. 1-6

N. D. Khan, C. Chrysostomou and B. Nazir, "Smart FIR: Securing e-FIR Data through Blockchain within Smart Cities," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020, pp. 1-5

Pawar, S., Lahane, S., Mandhare, O., Begade, N., Phalke, D., & Metre, V. Application of Blockchain to Secure e-FIR. International Journal for Research in Applied Science and Engineering Technology. 2023

Huang, K., Lo, S., & Sutthiphisal, D. From Data Transparency and Security to Interfirm Collaboration-A Blockchain Technology Perspective. ABAC Journal. 2023

Divyaa. S. K, Kiruthika. K, Shahin Ashra. S, Sindhuja. J, Bhavani.N FIR Security System Using Blockchain Technology. International Journal for Research in Applied Science and Engineering Technology. 2023