# A Method to Secure FIR System using Blockchain

**Antra Gupta, Deepa. V. Jose**

***Abstract:*** ***In India, we can see that technology has touched in every aspect of our life. There exist technology in all the fields e.g. education, agricultural, business, government etc. and we can also understand how beneficial it is, as it saves the time, money and human power. In spite of being technologically advanced, the system lacks in security perspective. When we talk about today, India has moved to the era of digitalization after the launch of the campaign "Digital India", the Indian Police Department has replaced the manual system with the centralized online process to register the complaint. The main objective of this paper is to provide a method to secure the FIR system using blockchain technology. This introduces to the essential principal of blockchain technology and its future in the police department of India. Blockchain technology will also explain to protect the FIR from the malfeasance.***

***Index Terms: FIR, Police, Blockchain, Security, Cryptography, Security Attack***

## I. INTRODUCTION

Imagine a ledger in a distributed network fabric, which contains all the transactions, plus updates itself whenever there is a fresh transaction. The ledger is not in the aids of a centralized administration, and each individual in the distributed network fabric carries a portrait of the ledger. However there is a challenge; once an article is recorded on the ledger, it cannot be destroyed. That signified the concise summary about blockchain technology. In the primary journal about the blockchain technology, the first application which was addressed was Bitcoin. At present this technology is maintained to preserve the bitcoin transactions, this digital record doesn't fall below one administration. Individual transactions are recorded on the bitcoin network, in this, every individual system is a node. These nodes act autonomously during executing the mathematical functions, computing the transactions. The aforementioned transaction will be communicated to other nodes in the decentralized fabric network by a multi-hop broadcast. The critical component is combining a transaction.

A valid transaction makes a block and various valid blocks are connected collectively to develop a blockchain network. The blocks are verified and attached to the chain once they have an adequate consensus. Fundamentally, when we want to attach a block in blockchain we should prove its genuineness. A block requires a minimum number of consensus whenever it is added in the network. The popular consensus mechanism used is proof of Work[1], proof of Stack[2] and the Byzantine fault tolerance[3] to authorize the block. When the freshly generated block is chained with the other block it counterfeits itself with the additional nodes present in the distributed fabric network. Every time an individual demands to nullify a verified block from the blockchain, all the subsequent blocks need to be transformed in the network which is computationally impracticable. Momentarily, visualize the transparency it delivers when the blockchain is developed for sustaining the police statements including the First Investigation Reports [FIR]. In this system, an individual zone is a node of the distributed fabric network having the copy of the blockchain. Whenever there is a new complaint which is recorded there will be an FIR connected with that complaint which is timestamped by the system. The respected complaint can be provided with a cryptographically generated hash key so that the integrity of the block can be authenticated. To prove the genuineness of the block, we will be applying the consensus mechanism. The valid block will be announced to all the nodes present in the distributed fabric network with the timestamp[4]. The end-user needs to register from their mobile to file a complaint, to register an individual should have their unique AADHAAR number for verification. The app will require the location so that the complaint can efficiently be transferred to the nearby police station. The validation of the block is easy, we merely have to associate with the hash key. Once the block signifies a valid block it will be securely connected to the previous blocks which will make the invalidation computationally very complicated, challenging implying an oversimplification. The innumeable confirmations a block grows, the further decentralized the hash power.

**Revised Manuscript Received on May 22, 2019**

**Antra Gupta,** Department of Computer Science, CHRIST (Deemed to be University. India.

**Deepa.V.Jose,** Departmentnof Computer Science, CHRIST (Deemed to be University). India.

## II. SECURITY IN BLOCKCHAIN

The main characteristics of the blockchain technology is the level of security it provides to the network. This technology uses the cryptographically engineered block to make the information secured, the use of SHA-256[1] and hash tree[1] are the few algorithms used in this. When we are performing these algorithms, we are basically hiding the identity of an individual – this will help to create a no trust network. When a case is filed, the user that is the complainer, suspect, witness and the officer will not know the individual's identity then there will not be any manual intervention in the case – the proceeding of the case will carry out smoothly. The decentralization[5] of blockchain is an add-on benefit as there would not be a central govern person to interfere. When there is a single administration there is a single point of failure, the deletion of the data is easy in the network. The system that we are going to address will avoid all these security threats, we will be developing this system from the open source marketplace, which will rely on the Blockchain technology.

## III. LITERATURE REVIEW

The concept of Blockchain technology was first proposed by Satoshi Nakamoto[1], it is a cryptographically engineered software platform to store ledger using peer to peer network. It is a sequential chain of blocks where every block contains a cryptographically hash value of previous block, time-stamp and the block information. From the above method we can ensure the integrity and security of the block and we can identify the invalid block. The first application of this technology was Bitcoin, which allows cash transaction using internet, through peer to peer network without a central authority and in a trustless network. The author gave a resolution to the problem of double spending. The system uses the method of timestamp by hashing the block into continuous chain based of proof of work mechanism.

The introduction of the DAPP and smart contract comes was mentioned in this paper[2]. We have blocks in the Ethereum blockchain, these blocks are linked together and each blocks we have list of transaction similar to bitcoin. Inside these transaction we do have timestamp and other parameters which we can programme it. Ethereum blockchain gets stored in every miners computer which is called a node, it uses the proof of work algorithm to verify the network. The block contains the smart contract which has the code snippet that runs in each block, when the code computation is successfully executed in each miner's computer. It is sent to whole network so that the other miners can agree. The successful verification of the block will be added to the chain. The author did a thorough study about the IPFS[6]. According to the author they want to make the web completely distributed by running it top of the peer to peer networks, it will work similarly how bit-torrent[7] works. In the current scenario when we want to download the content from the web, we have to provide the exact location which we call a URL. Present-day, the model which is followed to download the content is centralize i.e. it is govern by a particular organization – this is called location-based addressing, but if the server is down then we will not get the content. There is a chance that there must be someone who will have the copy of that content in their device which we were searching yet we won't be able to get that. To solve this issue IPFS works from location-based addressing to content-based addressing. All the files in the internet will have a unique figure print. When we want to download the file we have to compare the hash value and the content will be available. In IPFS there are different types of file that we can store, an object is created in which files are stored, and these object can only store up to 256kb of data. So to store a file like a video n-1 number of objects are created and in n object all the n-1 objects are linked in a sequential manner. This can be used as a file system. The biggest disadvantage of this system is to keep the file available. So to avoid this we can incentivize people to keep the file available or we can proactively make the file distributed so that the file is available – this defines the system of Filecoin[8]. This paper[3] describes about the software that can be used to create blockchain based solution for businesses. Hyperledger is an open source platform, in 2015 people from different industry came together to make blockchain more accessible to the world. In this platform the member who are linked to the transaction will only be notified, this create privacy and confidentiality of the transaction. Hyperledger fabric came up with the concept of permissioned blockchain technology. In this paper[9] the author talks about decentralized crowd based platform that will identify the scams in internet and it will also provide notification to the other people about the scams in the internet, due to the growth of the cryptocurrency the scams have also increased like phishing website, fake projects and various scam scheme have grown these days. It works with the help of any browser. When a person will do any transaction through the internet there will be a flag which will appear in the browser which will say whether the website is safe or not if these notification does not appear then that person can provide them a report about the website and the crypto police give them a reward. The report will be verified by the officers of crypto police. The main task of crypto police is to report fraud in the cryptocurrency market. In this paper, the author[4] discusses about the importance of blockchain in the medical field. The sensitive data in the medical field is getting manipulated this enfeeble the integrity of data.

The author spoke about the proof of concept which will work by timestamping the data.

In this paper the author[10] wants to create the examination evaluation self-sustained without the need of centralize authority and to obtain the certificate or a degree the candidate have to prove their skills over the subject.

To make the blockchain transparent the questions and answer are hashed together and stored in the blockchain based network.

Blockchain technology is providing many contingency to develop new type of system. In this paper [11] the author introduce about electronic voting system that can be used for national and local election. By the use of authentication, anonymity, accuracy and verifiability a trusted platform is created.

## IV. PROPOSED METHOD

The workflow to maintain the security of the FIR system is as follows:

1. The Complainer, suspect and the witness will have to register to the User Interface[12], this will act as a protector so that we can verify them. The users will have the AADHAAR CARD[13] so that the verification can be done in a better way. The officers will be given a unique ID to register and see the case which is allotted to them. The investigating officer will also be given a Unique ID so that they can work with the case along with the user i.e. complainer, suspect and witness.

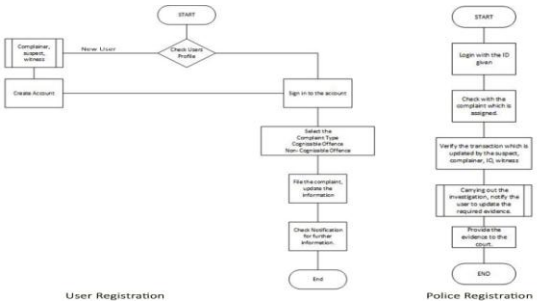


**Fig I. Registration Flowchart**

2. After the verification of the user the system will segregate them in different category, the system will provide them with a key (private and a public) so that they can interact with the blockchain for that particular case. The verification of the user will be done by the Officers who is in charge of the case. The identity of the Officer will not be disclose to anyone. The user will be notified once the verification is done. The key will be removed by the system after the case is solved.
3. Once the key for the user is generated by the system the they can do the following task:

**a. Complainer:**

i. File a complaint about the crime which has happened.
ii. Fetch the information about the case.
iii. Update information about the case. The information can be of anything images, voice recording, videos etc. If the evidence is not digital it should be submitted to the mentioned police station with a verification proof so that it can be updated in the system.
iv. The evidence which is already there, they can comment on that. Suppose the information which is updated about the case is false then, the officers in charge can look into the matter.

**b. Suspect(s):**

i. Write their point to defend themselves.
ii. Fetch the information about the case.
iii. Update the information about the case. The information can be of anything images, voice recording, videos etc. If the suspect is in the jail then the evidence can be submitted by any close member and it should be mention in the block. Evidence is not digital it should be submitted to the mentioned police station with a verification proof so that it can be updated in the system.

**c. Witness(s):**

i. File a complaint about the crime which has occurred. The information of the witness will not be disclosed.
ii. The witness can also update and fetch the information about the case.

**d. Officer(s):**

i. Verifications of the user.
ii. Appointing Investigation officer.
iii. Verification of the evidence and finding out its originality.
iv. Providing their views about the evidence through voting mechanism will be done by the officers in charge.
v. The identification of the officer in charge will not be disclose to anyone.

**e. Investigation officer:**

i. The evidence which is provided by the user, Investigating Officer will check its originality.
ii. Fetching the information and updating any new information will be done.
iii. To provide information to the court or further investigation.

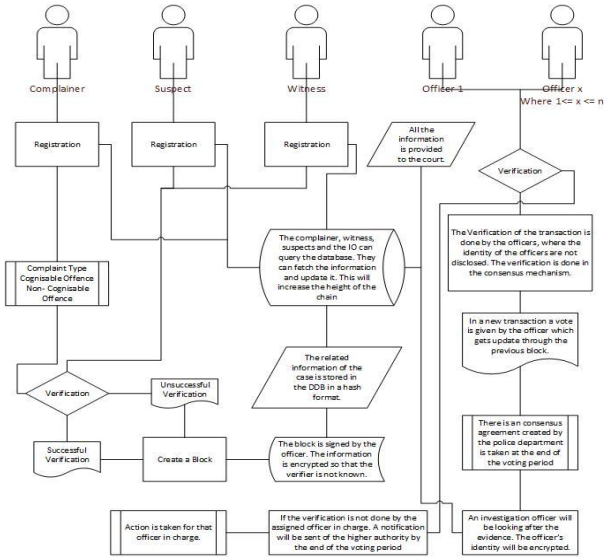


**Figure II. Flow Diagram of the Security of FIR System**

4. The reward can be provided to the Investigation officer to be the part of the Officer's in-charge team, the deciding authority of the case.
5. All the officer-in-charge team identity will not be disclosed within the team and outside.
6. The identity of the witness should not be disclosed to anyone to avoid manipulation of the decision. The witness will be identified by their hash value.
7. The investigation officers is not performing their precise task, then a warning will be given and there will action taken by the department of the police.
8. All the transaction which is happening in the case is timestamped.
9. This system is very much transparent, as mentioned all the user's identity will not be disclose but the information will be viewed.
10. There can be a 3-4 teams of the officer's in-charge, selected by the system working for case. Depending upon the work the officer will be rewarded.
11. As the model is conceptual to maintain the security of the FIR, the detailing can be done by the Department of police.

## V. CONCLUSION

We are proposing this system to secure the FIR system. We are trying to make the system simple and efficient. The decentralized network which we are building does not rely on any trust. The registered user can file a complaint through any device which is connect with an internet. The blockchain will make the network more secure, immutable and decentralized, we can say that it will be a corruption free network. The limitation and the implementation of the system will be addressed in the future paper.

## REFERENCES

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008.
2. B. V. Buterin, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM," no. January, pp. 1–36, 2009.
3. "Hyperledger Whitepaper."
4. G. Irving and J. Holden, "How blockchain-timestamped protocols could improve the trustworthiness of medical science.," *F1000Research*, vol. 5, no. May, p. 222, 2016.
5. K. Croman *et al.*, "On scaling decentralized blockchains (A position paper)," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9604 LNCS, pp. 106–125, 2016.
6. Protocol Labs, "IPFS." [Online]. Available: https://docs.ipfs.io/.
7. J. A. Johnsen, "Peer-to-peer networking with BitTorrent," 2005.
8. P. Labs, "Filecoin : A Decentralized Storage Network," pp. 1–36, 2017.
9. "WHAT IS CRYPTOPOLICE ?"
10. R. Acharya and S. Binu, "Blockchain based examination system for effective evaluation and maintenance of examination records," vol. 7, pp. 269–274, 2018.
11. A. Ben Ayed, "A C ONCEPTUAL S ECURE B LOCKCHAIN - BASED E LECTRONIC V OTING S YSTEM," vol. 9, no. 3, pp. 1–9, 2017.
12. M. B. Mollah, S. S. Islam, and E. Engineering, "Proposed E-Police System for Enhancement of E-Govemment Services of Bangladesh," 2012.
13. Government of India, "Digital India." [Online]. Available: https://digitizeindia.gov.in/.

## AUTHORS PROFILE

**Antra Gupta is** perusing her Master in Computer Application from Department of Computer Science, CHRIST (Deemed to be University. She has keen interest in Blockchain, AI and Machine learning.
antra.gupta@mca.christuniversity.in

**Deepa.V.Jose** is the faculty in Department of Computer Science, CHRIST (Deemed to be University). Her area of research interest include network security, AI and Machine Learning.
deepa.v.jose@christuniversity.in