A Transparent Blockchain for Tracking Police Complaints

Rohini Pise, Vaishnavi Swami, Monika Hajgude, Swamini Godse, Kaveri Thombare

Abstract*: Blockchain technology is one the emerging technology today. Using blockchain the primary goal that is achieved is security. Along with security many other aspects can be achieved using blockchain. Blockchain is nothing but a chain of blocks which are connected by hashing. We can see that every new technology has become a part of our life. This technology is proving to be helpful in all the fields like education, agriculture, business, government and many more. We can also understand how beneficial it is, as it saves the time, money and human power. But this never-ending technology is lacking to provide security. The Indian Police Department has replaced the manual system with the centralized online process to register the complaint. There are many malpractices in resolution of complaints. So, to avoid them a system is proposed which helps complainer to track the complaint, get ongoing details, and enforce police officers to solve the complaints within stipulated time to avoid unnecessary delay. The main objective of this system is to provide a method to secure the FIR system using blockchain technology. The principal components of blockchain technology viz. security, transparency, decentralization, immutability prove to be helpful for securing this digitalized process. The system uses transparency of blockchain technology as the user can track the complaint at any time. The system uses hashing to provide immutability so that no one can tamper the data entered by the complainer. Smart contracts are used to avoid delay in solving the case. This will avoid malpractices and provide satisfiable results.

***Keywords*: Blockchain, transparency, decentralization, immutability, FIR**

I. INTRODUCTION

A blockchain, originally chain of blocks, is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain. We have proposed a system which makes use of blockchain technology for security. The main motive of the system is to file a complaint in a secure way. There are many malpractices in resolution of complaints. So, to avoid them a system is proposed which helps complainer to track the complaint, get ongoing details, and enforce police officers to solve the complaints within stipulated time to avoid unnecessary delay. The system uses transparency of blockchain technology as the user can track the complaint at any time. The system uses hashing to provide immutability so that no one can tamper the data entered by the complainer. Smart contracts are used to avoid delay in solving the case. These all will attempt to achieve good quality secure and trustful system. The aim of project is to provide a system that secures all the documents involved and generated during police complaints, along with providing transparency about the case to the complainer. The main objective of the project are:

- Avoid tampering of documents (involved in police complaints) by securing them using concepts of blockchain.
- Provide transparency to the complainer, by allowing him/her to track the status or the state of the case registered.
- Making the process fast, by adding penalties for not doing the task in required time.
- Decentralizing the whole process to avoid corruption.

II. LITERATURE REVIEW

Blockchain is one of the emerging technologies. It solves problem of mutability by storing the data in blocks that has hash value of previous stored block. It also solves the problem of centralized authority by establishing peer to peer network. The first application of blockchain was bitcoin introduced by Satoshi Nakamoto [1]. In this application the cash transaction is recorded in open ledger, where all peers are able to view the transaction done. It introduced the concepts of block mining, consensus algorithm.

In paper [2] we studied architecture of blockchain, the structure of block. Different consensus algorithm like proof -of work, proof-of-stake, PBTF, Ripple and Tendermint and their difference was also mentioned in the paper. Proof of work is most widely used consensus algorithm. The details of Proof of work, its advantages, limitation are studied by analysing system that uses PoW.

Revised Manuscript Received on April 25, 2020.

***** Correspondence Author

Prof. Rohini Pise , Information Technology Pimpri Chinchwad College of Engineering, Pune, India Email: rohinipise@gmail.com.

Vaishnavi Swami , Information Technology Pimpri Chinchwad College of Engineering, Pune, India Email: swamivaish29@gmail.com

Monika Hajgude, Information Technology Pimpri Chinchwad College of Engineering, Pune, India Email: monikahajgude@gmail.com.

Swamini Godse Information Technology Pimpri Chinchwad College of Engineering, Pune, India Email: swamini.25@gmail.com

Kaveri Thombare Information Technology Pimpri Chinchwad College of Engineering, Pune, India Email: kaverithombare@gmail.com

These Blockchain algorithms can be basically classified into two groups. One of them is proof-based consensus, in which the nodes joining the network need to prove that they are more qualified, more powerful than others, to do add the new block. The second group is voting-based consensus, in which nodes in the network interchange their results of validating a new block or a transaction, before making the final decision. These different consensus algorithms give us an idea, how nodes in the verifying network agree with each other about the ledger that they hold. Blockchain consensus algorithms are methods to bring equality and fairness in the online world. The agreement method used in this is called a consensus theorem. In paper [3]. It is found that even the problem complexity is high, PoW can mine the block in less time.

FIR system based on blockchain concept is developed in paper [4]. The user involved in this system are complainer, suspect, witness, investigation officer. The user needs to first login to the system. The user is further verified by Aadhaar card and password. The user can perform their task in respective category. In this system complainer can register complain, see the status of case, update information about the case. Suspect can write the defending points, fetch case information, and update the case information. Witness can file the complaint about the crime. Investigation officer can verify the user, check the originality of the evidence, update the investigation details about the case and provide information to the court. Different platforms are available to develop software based on blockchain like Ethereum, Hyperledger, Corda etc. Comparison of these platform is done in paper [5]. Hyperledger is one the new and emerging blockchain platform. It is open source blockchain development project under Linux foundation. It is further divided into five framework that are Burrow, fabric, Indy, Iroha and Sawtooth.

III. PROPOSED METHOD

In our proposed system there will be mainly three modules

1.Victim:

The person who logs the complaint i.e. victim, will be responsible for registering new complaint. The usual process of logging complaint towards the sub-inspector will take place. But this will be done on the system rather than on paper. After registering the complaint, the victim can view complaint process by using his login.

2.Sub-inspector:

He is responsible for registering new complaint whenever victim logs new complaint. Whenever new complaint is registered by him a new block gets created. This will be communicated to the corresponding victim to view his complaint and inspector to add further updates.

3.Inspector

Whenever the complaint is registered by sub-inspector, inspector will receive it and can view the details of case. Once he investigates the case, he will add blocks to the chain about the data related to the case. These blocks will be communicated to other nodes.

These all modules are the nodes of our system. As the block once created is communicated to all nodes, distribution can be achieved. SHA-256 will be used to generate the hash values of each block. Due to this hashing any of the node can tamper the data. Whenever a new block needs to be added to the chain, proof of work concept can be used to prove genuineness of the block. Using consensus helps to add the block to chain. The blocks can be viewed by victim which provides transparency. As shown in fig. 1, whenever victim comes and asks for registering complaint new block i.e. genesis block will get created at the back end with the help of sub-inspector login. After creating genesis block, further blocks will get added by inspector, as and when updates are available in that particular case.

SHA-256

The SHA (Secure Hash Algorithm) is one of the popular cryptographic hash functions. A cryptographic hash can be used to make a signature

for a text or a data file. The SHA-256 algorithm generates an almost-unique, fixed-size 256-bit (32-byte) hash. This is a one-way function, so the result cannot be decrypted back to the original value. [10]

Algorithm:

public static String encryptThisString(String input)

{

1. getInstance() method is called with algorithm SHA-1
2. digest() method is called to calculate message digest of the input string returned as array of byte
3. Convert byte array into signum representation
4. Convert message digest into hex value
5. Add preceding 0s to make it 32 bit
6. return the HashText

}

SHA-256 role in bitcoin system

In a bitcoin transaction, there is a random number in the header of the transaction called a Nonce. Miners in the network have to find that Nonce using its fingerprint, and the only way to find the Nonce is to produce quadrillions of hashes operations. And to perform these operations, they have to use a very important precious resource: energy.

This algorithm is at the core of bitcoin, it is used to secure the network through proof-of-work. So, just by looking at the fingerprint, I know for sure that the miner had to spend a lot of electricity. Which means that miners had a financial cost, and that is really important for the security of the bitcoin network. Because it creates an economic system where in order to participate, you have to spend resources, and miners do that for the possibility of reward. And the possibility of reward, is determined by whether your blocks meets the consensus rules. Which means you spend money, and if you play fair by the rules, you get money in return. If you spend money, and you try to cheat, you don't get money back. So, you lose money, therefore, it doesn't pay to cheat. [11]

Proof of work

Proof of work is a type of consensus algorithm. This helps to validate a block when adding to the chain.

Here is an algorithm to check the validity of the block

mineBlock(difficulty)

{while loop, condition used is a quick trick to make the substring of hash values exactly the length of difficulty

{incrementing the nonce value every time the loop runs.

1.recalculating the hash value}

}

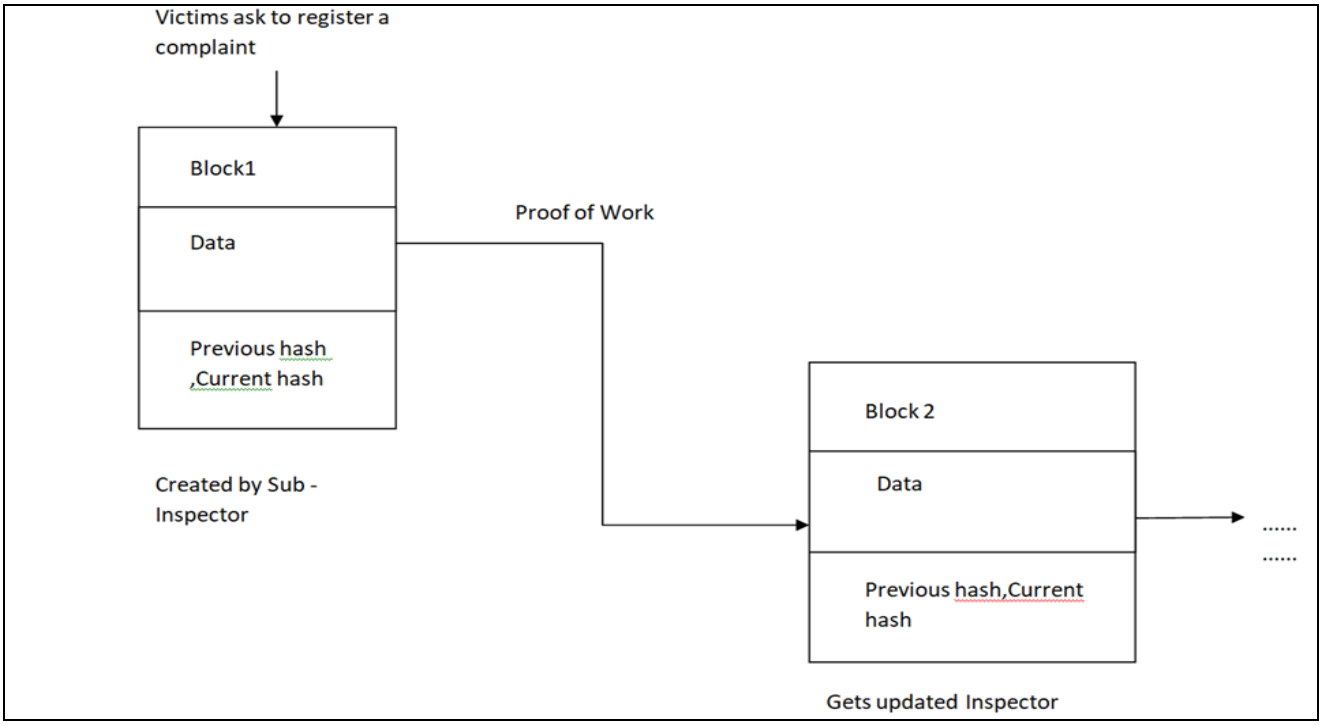

Fig. 1. Working of system

The following algorithm is used to check if the chain of blocks is valid:

```
isChainValid()
{   for(let i = 1; i < chain length; i++)
  {     if(currentBlock.hash!== currentBlock.calculateHash())
            return false;
      if(currentBlock.previousHash !== previousBlock.hash){
            return false;   }
 } return true; [14]
```

IV. CONCLUSION

We proposed transparent and light weight blockchain system. We implemented the system through web application interface with nodes communicating through a TCP/IP network and evaluated its throughput, latency, and storage. Results show that the proposed system has a small block creation time, which is in the order of seconds, and lower average transaction time. The system has a higher throughput with a linearly increase in the amount of storage needed at each block.

The proposed system is helpful in achieving the main concepts of blockchain for tracking of police complaint. Immutability- Whenever the complaint will have any progress new block will get added to the blockchain. Once the block is created if anyone tries to change, then whole chain will get destroyed. As this is not possible, we can say it is immutable. Transparency -The victim will be able to see the progress of his complaint at any time which will help to achieve transparency. Decentralized system- Whenever new block gets added it is communicated to the corresponding victim, sub-inspector and inspector.

When the case does not get resolved and is communicated to the court, we can add new node and the judgements given by court can be added to the chain by adding new block.

V. RESULTS

We have implemented the proposed system using java framework. JDBC Hibernate is used for object relational mapping and servlet is also used. For storing hash, we have used SHA-256. Business logic contains blocks, mining algorithm and cryptographic algorithms.

sub-inspector and inspector are the main modules of the system. They are given their respective access and transparency and immutability are achieved. The sub-inspector can only ad new complaint and view the updates thereafter. Whereas the inspector is able to only update the complaints. Whenever new complaint is added new blockchain is getting created and whenever new update is there for existing complaint block is getting added to the existing system. For client endpoint html and jsp is used. The experiment is conducted on intel core i3 processor and 8 GB memory laptop having windows-10 running on system.

We simulated the data that is coming from distributed servers and use the web applications Application Programming interface endpoints to broadcast the data. Each node on the network runs locally on the machine on a separate local host port. We first experimented with five nodes and generated one thousand blocks with 5, 10, 20 and 40 transactions in each block to evaluate the block creation time and transaction time. The table shows that 90% of the time, the block creation time is smaller than 0.3 seconds. For reference, note that the Bitcoin network requires around 10 minutes for a single block creation [13]. As shown in the figure, in the table the time taken for creation of block is less for first few blocks and it goes on increasing. The time required for creation of genesis block is less as we don't have to check previous hash for that.

Blockchain considered	Time required for creation of block as number of blocks added in milliseconds.			
	5	10	20	40
1	0.0125	0.0138	0.0144	0.1043
2	0.0131	0.0132	0.0155	0.1141
3	0.0128	0.0142	0.101	0.1221
4	0.0140	0.0241	0.052	0.134

Fig. 2. Experimental results

These results show the proposed system has high performance in terms of block creation time, and average transaction time as the blockchain grows as compared to that of a Bitcoin blockchain. The proposed system can also handle a large number of transactions per second as compared to the traditional blockchain. Because a transaction is reported only when update is there on the complaint the number of transactions is less.

REFERENCES

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System, www.Bitcoin.Org, p. 9, 2008.
2. Giang-Truong Nguyen, Kyungbaek Kim. "A Survey about Consensus Algorithms Used in Blockchain" ,2018
3. Amitai Porat, Avneesh Pratap, Parth Shah, and Vinit Adkar, "Blockchain Consensus: An analysis of Proof-of-Work and its applications"
4. Antra Gupta, Deepa. V. Jose, "A Method to Secure FIR System using Blockchain"
5. Chinmay Saraf, Siddharth Sabadra: "Blockchain Platforms: A Compendium"
6. William Pourmajidi, Andriy Miranskyy, "Logchain: Blockchain-assisted Log Storage"
7. Blockgeeks website: https://blockgeeks.com/guides/what-is-blockchain-technology/
8. Blockchain website: https://101blockchains.com/consensus-algorithms-blockchain
9. Techtarget: https://whatis.techtarget.com/definition/consensus-algorithm
10. SHA-256: https://www.baeldung.com/sha-256-hashing-java
11. SHA and proof of work:https://www.sesterce.com/post/what-is-sha-256
12. Elli Androulaki,Christian Cachin,Christopher Ferris, "A Distributed Operating system for permissioned blockchains
13. Bitcoins website: https://learnmeabitcoin.com/beginners/blocks
14. Zohar, A., "Bitcoin: under the hood," Communications of the ACM, vol. 58, no. 9, pp. 104–113, 2015.
15. https://cryptocurrencyhub.io/implementing-a-simple-proof-of-work-algorithm-for-the-blockchain-bdcd50faac18

AUTHORS PROFILE

Prof. Rohini Pise , Information Technology Pimpri Chinchwad College of Engineering, Pune, India
Email: rohinipise@gmail.com.

Vaishnavi Swami , Information Technology Pimpri Chinchwad College of Engineering, Pune, India Email: swamivaish29@gmail.com

Monika Hajgude, Information Technology Pimpri Chinchwad College of Engineering, Pune, India
Email: monikahajgude@gmail.com.

Swamini Godse Information Technology Pimpri Chinchwad College of Engineering, Pune, India
Email: swamini.25@gmail.com

Kaveri Thombare Information Technology Pimpri Chinchwad College of Engineering, Pune, India Email: kaverithombare@gmail.com