I.J. Information Engineering and Electronic Business, **2023, 1, 29-40**
Published Online on February 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2023.01.03

Blockchain and IFPS based Secure System for Managing e-FIR

Khandaker Mohammad Mohi Uddin*
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: jilanicsejnu@gmail.com
ORCID iD: https://orcid.org/0000-0002-5401-0437
*Corresponding Author

Sadia Mahamuda
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: anika21.nextin@gmail.com
ORCID iD: https://orcid.org/0000-0002-9795-7567

Sikder Sajib Al Shahriar
Department of Computer Science and Engineering (CSE), Dhaka International University (DIU), Dhaka-1205, Bangladesh
E-mail: sajib.rw99@gmail.com
ORCID iD: https://orcid.org/0000-0002-7386-6927

Md Ashraf Uddin
Department of Computer Science and Engineering (CSE), Jagannath University, Bangladesh
E-mail: ashraf@cse.jnu.ac.bd
ORCID iD: https://orcid.org/0000-0002-4316-4975

Received: 23 September, 2022; Revised: 22 October, 2022; Accepted: 12 December, 2022; Published: 08 February, 2023

Abstract: In recent times, various forms of crime have been happening worldwide. The law-and-order department of any country officially records a crime in electronic forms or on paper when the crime is reported by a victim or someone on behalf of the victim. The document that is prepared to file any perceptible committed crimes including dowry, kidnap, murder, rape, theft, and others is called First Information Report(FIR). Nowadays, online FIR also known as e-FIR has been used worldwide. Every day a number of e-FIR are filed, and they are maintained in a centralized database with the aid of third-party trust. Consequently, malicious entities including insiders and outsiders' dishonest personnel, and third-party authorities may tamper with e-FIR that questions the transparency and integrity of FIR reports. To address this exposure, in this paper, we propose a blockchain based FIR system to store all kinds of offense-related records to assure security, fidelity and privacy of FIR records. In this proposed system, the blockchain technology that refers to a decentralized and distributed ledger across peer-to-peer networks continually updates the shared ledger and strictly maintains synchronization among all network nodes. Though blockchain technology guarantees tamper-proof of the data, it cannot store a large amount of data due to the replication of ledger among all network nodes. To solve this issue, we adopt the Inter-Planetary File system (IPFS) protocol to store data in the blockchain. IPFS is a distributed file-sharing system that can be leveraged to store and share large files. The blockchain based FIR system has been tested on an Ethereum environment using blockchain and IPFS technology.

Index Terms: e-FIR, Blockchain, Decentralized, Inter-Planetary Filesystem (IPFS), Ethereum.

1. Introduction

Our research objectives are to create a temper-proof, secure FIR record management system. Usage of IPFS into blockchain technology makes our work different and unique. All the existing solutions for keeping FIR records are

based on e-FIR or blockchain technology. But we used the IPFS model combined with blockchain technology which makes us different from all the traditional solutions. Because of using IPFS we can solve storage problems as well as browsing problems. This was the main objective that we hoped to achieve successfully.

The era of 4th Industrial Revolution (4IR) has been underway. 4IR includes diverse kinds of technologies including robotics, blockchain (BC), Internet of Things (IoT), quantum computing, genetic engineering, artificial intelligence (AI), and more [1]. With this revolution, industrial applications have been automated in daily life. Several years back, in many developing countries like Bangladesh, to file an FIR people needed to go to a police station which would take a long time to manually file an FIR. Further, to physically record FIR, there would need more numbers of law and order maintaining professionals. Bangladesh does not have enough police personnel to handle FIR in a traditional way. The ratio of police against citizens of the commonwealth countries is shown in table 1. Table 1 presents that one police is assigned for 1138 citizens in Bangladesh [2]. This imbalanced ratio of police personnel and citizens significantly hampers the quality of service.. To address this issue, south-Asian countries, such as Bangladesh, Pakistan, and India have already switched from manual FIR to electronic FIR (e-FIR) for filing crimes such as abduction, murder, threat, robbery, and rape [3].

Table 1. Police to People ratio in some commonwealth countries [2].

No.	Country	Police-People ratio
01	Bangladesh	1:1138
02	India	1:728
03	Pakistan	1:625
04	Singapore	1:614
05	Malaysia	1:450

Bangladesh has seen a rise in the number of different crimes between 2000 and 2017, according to crime statistics shown in Fig. 1.

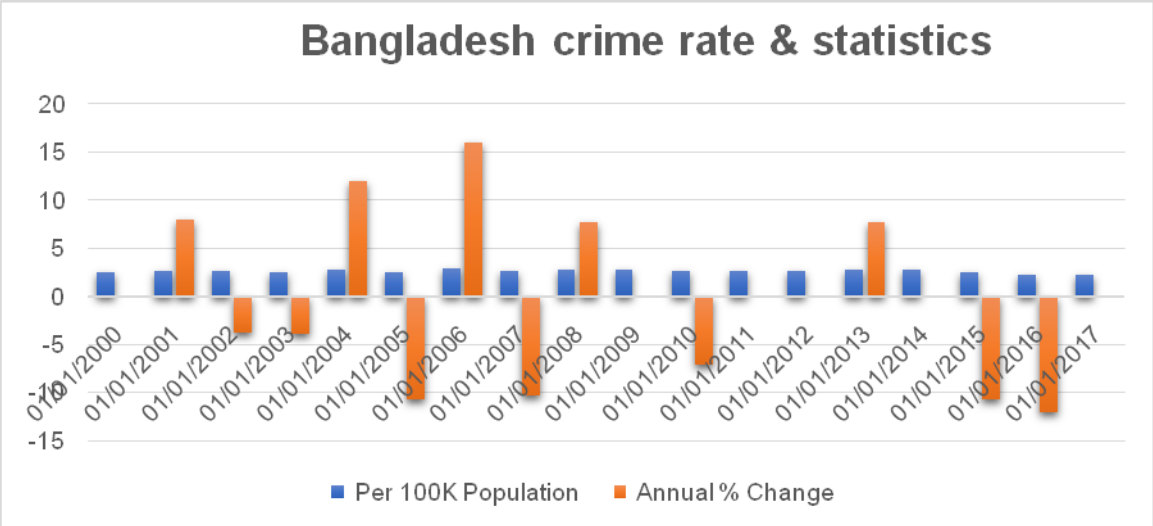

Fig. 1. Bangladesh crime rate & statistics [4].

With the increasing population and number of crimes, many FIRs are filed and processed in a central database. A bottleneck and single point of failure occur in the centralized database. Furthermore, since the database is maintained by third-party officials, malicious individuals from both inside and outside may modify an FIR [5]. To solve these problems, we have developed a secure e-FIR data storage system where authorities and users can access the system with proper authorizations. The blockchain technology with IPFS protocol has been applied to make the FIR system decentralized. Blockchain operates on a decentralized peer-to -peer network that facilitates distributed hash tables of IPFS protocol.

Blockchain technology consists of different established fields including cryptography, mathematics, algorithm and economical model. BC refers to a decentralized and digitized public ledger that handles transactions generated from cryptocurrency systems [6, 7, 8]. Blockchain manages all transactions of users in a distributed database that is hosted by many computers in a peer-to-peer network [9, 10].

We aim to implement a secure blockchain based e-FIR system to ensure the transparency of FIR records. The system can store a large volume of FIR records using IPFS protocol. In the conventional FIR system, users may be denied registering FIR due to centralized control of such a system. However, no one controls the ledger of blockchain. Consequently, none can prevent users from filing crime related reports or tamper the FIR. Further, blockchain based

e-FIR systems can notify all entities about any attempt of change or modifications in FIR.

Our contributions to our proposed system are given below:

1. Our proposed system is more secure and more confidential than other existing traditional systems because of the IPFS model.
2. We successfully solved the storage problem that all other existing solutions can't overcome.
3. By using the IPFS model we are able to remove duplication in our FIR record that Blockchain itself can't.
4. IPFS enables high performance that can efficiently distribute a high volume of data quickly. That is a very important part of the FIR system.

The rest of the paper is organized as follows. In section 2, we review related works. In section 3, the proposed system is presented. The design and implementation are described in section 4. The result is analyzed in section 5 before concluding the paper in section 6.

2. Research Background

Nowadays, Blockchain [11] has gained popularity owing to its distributed features, which allow multiple entities to interact without the requirement of mutual trust among them. The two key forms of blockchain are private and public network blockchains, with Bitcoin [12] and Ethereum as public blockchains and Hyperledger-fabric as a private blockchain. Ethereum and Bitcoin are popularly known as cryptocurrency systems that utilize smart contract technology for facilitating other kinds of applications including IoT, eHealth [13, 14, 15], governance, and supply chain [16, 17]. Antra et al. [18] introduced a blockchain-based FIR system where complainer, suspect and witness can file an FIR. In this system, the officer-in-charge handles the pre-registration and user credentials are stored in a local database, which can lead to data manipulation and change in the user authentication data. In this work, the authors did not solve the issue of handling false FIR. Without third parties' intervention, smart contracts that are stored in every node on blockchain can execute the user's program. The smart contract refers to a software-defined protocol or program that is digitally verified by every node on the blockchain network [19].

Maisha et al. [20] presented a blockchain-based application for recording digests of criminal information. Unauthorized users cannot illegally change any information in the system. The clients require to register to the BC and registered users can access criminal reports that are stored in the Cloud server.

Kirti et al. [21] suggested a portal-based e-FIR system that can be verified by administrators. The administrators ensured the genuineness and accuracy of the FIR data as it was documenting the pre-registered FIR inside the nearby database, allowing for e-governance to be more straightforward.

Mollah et al. [22] proposed an e-police system in which all police stations in a city in Bangladesh can be linked to the home ministry. The framework will have a component called the 'Third Eye,' whose purpose is to keep track of police station activities and records if they were being overseen by home ministry authorities. The framework will maintain a central database. The general public has access to information and the home ministry can efficiently monitor the overall operation of the e-police system. However, such a system requires ensuring greater security and privacy for the public. A central database is vulnerable to different kinds of cyber-attacks including Denial of Service (DoS), Ransomware attacks, etc. The paper did not address these security and privacy concerns.

To address these problems, blockchain technology has been explored to make a secure platform for e-FIR. However, a blockchain that has been successfully utilized in the cryptocurrency systems is not appropriate for general purpose usages like e-FIR. For example, if 0.1GB is added to the Bitcoin ledger every day, the entire ledger will take up about 200GB, putting a massive strain on data storage[23, 24, 25]. To cope with this, a network coding-based distributed storage (NCDS) framework is proposed by Dai et al. [24] where transactions are divided into different blocks and blocks are divided into different sub-blocks. Sub-blocks are encoded and dispersed to all the nodes within the network. The authors decreased the transaction size to some extent but at the same time due to the encoding and decoding process, complexity has been increased.

Dorriet. al. [26] proposed a technique that can record in the block. However, the technique didn't concern the terminated transaction history. For reducing the block size Palaiet. al. [27] proposed a technique where the records that are kept on the blockchain are active and old transactions are removed from the block. The main drawback of this technique is old history can't be retained. The account-tree techniques are proposed by Zhenget. al. [28] where transactions are added to the block which is generated by the nodes of that network. This technique reduced the file size, but they also didn't include the old transaction information.

The e-FIR system normally generates a huge amount of data that can burden the storage in a blockchain system. The existing works attempted to address the storage issue on the blockchain to some extent. To address this issue, we propose a blockchain-based secure e-FIR system for police and general users where the storage problem is handled using the IPFS protocol. Our work differs from the existing e-FIR system in the way we handle storage requirements. We have implemented an e-FIR record maintaining system with Inter-Planetary File system (IPFS) protocol where the uploaded data files are encrypted with user private keys. Those files can be accessed with public keys and decrypted with private keys. The IPFS protocol aids to store a large amount of data and any kind of image. The transaction is

stored in the IPFS and IPFS hash is stored in a block of the blockchain [29]. The SHA-256 algorithm is faster than most of the other hash algorithms and is used to produce hash code.

3. Proposed BC Based e-FIR System

In this paper, we develop a system where criminal records are managed on a public blockchain that applies public/private key cryptography to ensure the security and privacy of the records. As this system is mostly used by the general public, we have implemented the e-FIR on Ethereum public blockchain platform using Proof-Of-Work (POW) concept. Two kinds of infrastructures: police stations and Ethereum blockchain constitute the system. The police stations act as network nodes to store the hash of e-FIR. An e-FIR document is time stamped before sending it to the BC network.

Every police station maintains a copy of the e-FIR with the aid of blockchain. As a result, once an e-FIR is added to the system, the document cannot be modified or altered which ensures transparency of the record. Fig. 2 shows the high-level view of the proposed system. Different technologies that have been utilized to design the system are described below.

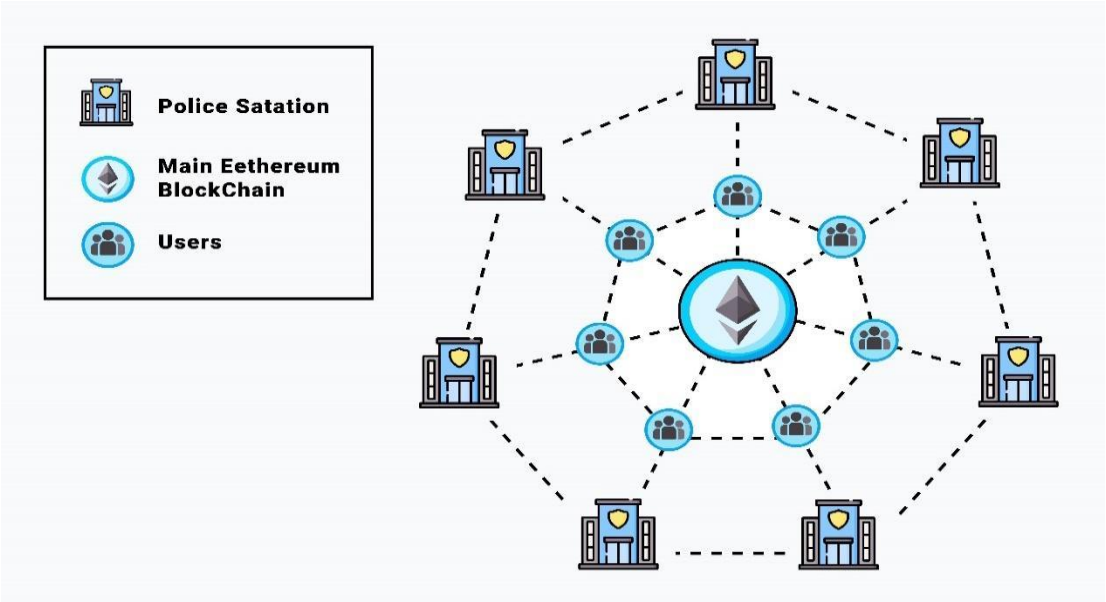

Fig. 2. Our proposed system model

This proposed system has applied SHA-256 to generate the hash code of the block and Proof-Of- Work (POW) as consensus protocol. IPFS protocol has been used to manage large-size e-FIR documents. These protocols and methods are discussed below.

SHA-256 is a secure hashing algorithm that produces a fixed size of 256 bits for any arbitrary length of text. In the Bitcoinblockchain, the SHA-256 function receives input of 20 Bytes and renders the hash value in a hexadecimal number.

Proof of Work: This consensus algorithm [30] is applied to select a miner for generating the next block. In PoW, miners compete to calculate a target hash value. To produce the target hash value, every node repeatedly computes a hash of a block by changing the block by incrementing the nonce value of the block [31, 32]. The miner that comes up with the target hash first is declared as winner. The winner node broadcasts the block throughout the network and other nodes add the block to the current chain after verifying the block. This process is called mining. Bitcoin and Ethereumblockchain use this PoW consensus algorithm. Recently, the Ethereum blockchain has shifted to PoS(Proof of Stake From PoW as the PoW requires a high computing cost.

IPFS Protocol: The blockchain ledger is not suitable for storing a large volume of documents as multiple nodes in the BC network store the entire ledger. For storing a large file in the blockchain, the IPFS protocol was used in this system. IPFS is a peer-to-peer hypermedia protocol that is designed to make the web faster, safer and more open. IPFS stores a file as an object. An IPFS object can hold 256 KB of data. An IPFS object can point to another object. This makes an IPFS object possible to store a file whose size is larger than 256KB.

In this work, the IPFS protocol relates to the blockchain using port 5001. Here, an e-FIR file first is sent to the IPFS protocol. Next, the IPFS converts the file into binary value to produce the hash value by applying SHA-256[33, 34]. A unique address is generated when the file is inserted into the IPFS network. The digest of the file content and hash value of the address of the file are concatenated. This concatenated hash value is stored in the blockchain to ensure the integrity and transparency of the e-FIR file.

The uploaded documents are encrypted with the user's private keys. Here, the user indicates the victim of the e-FIR and other authorized users such as police, and relatives of the victim. The document can be tracked by the victim's signature throughout the whole network. The documents can be accessed with the user's public keys and decrypted with the user's private keys. Fig. 3 shows the process of uploading e-FIR in the blockchain using the IPFS protocol.

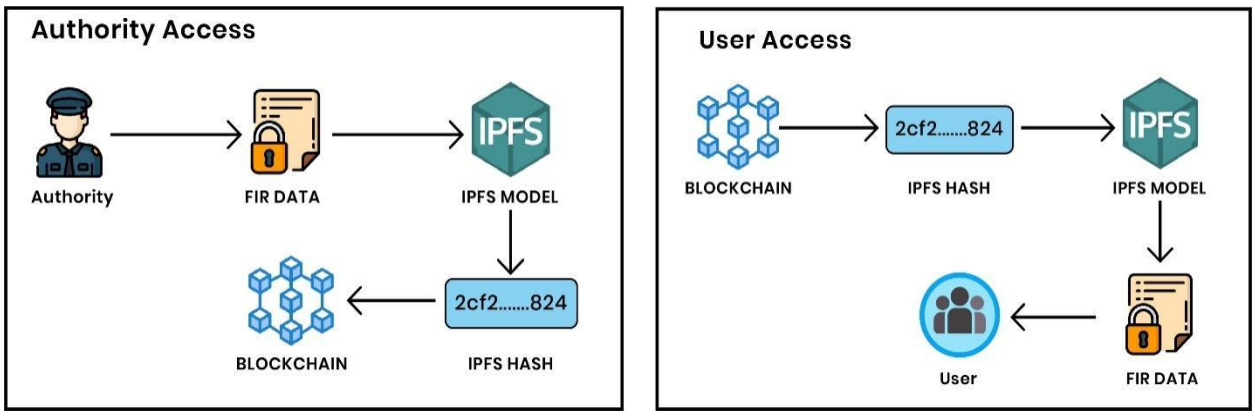

Fig. 3. Block diagram of IPFS model in the proposed system

4. Design & Implementation

A dApp (Decentralized Application) for e-FIR was developed. The app provides a user interface to interact with the Ethereumblockchain. The smart contract that stores the hash of the file was written using solidity, which is a scripting language. The truffle framework was used to execute the smart contract. In order to deploy and test the smart contract on the local Ethereum, Ganache was used. Ganache performs the mining process through which the transaction is validated and added to the blockchain. The browser extension named Metamask interacts with dApps and Ganache. To create a user-friendly web interface for dApp, we used web3.js which is a software library that allows the website to easily communicate with the Ethereumblockchain and interact with the IPFS protocol. The blocks of the blockchain contain all the necessary detailed information of the criminal report. The necessary tools for implementing our proposed system are presented in Fig. 4 and Interactions between BC, IPFS, and dApp are shown in Fig. 5.

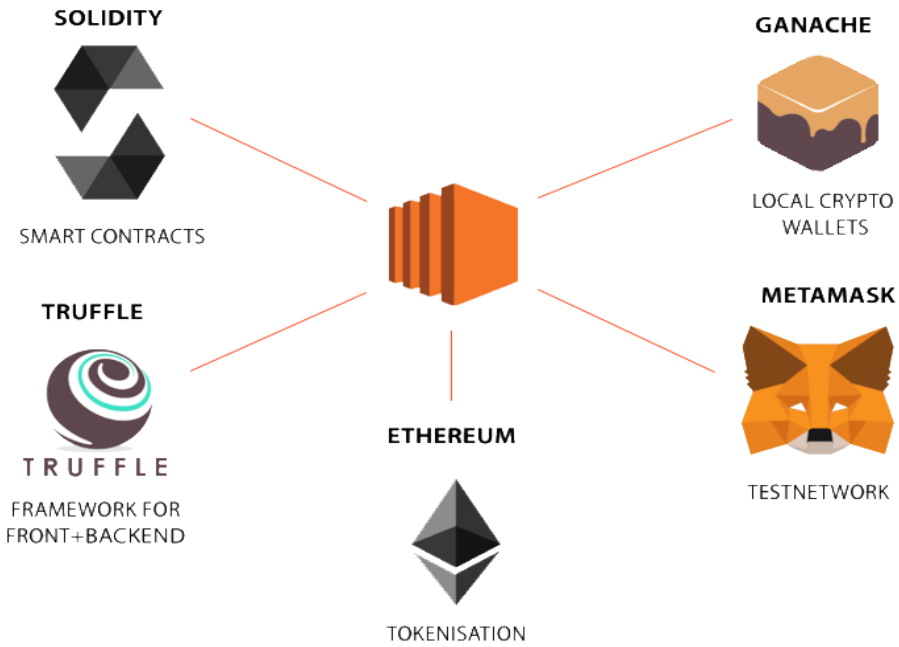

Fig. 4. Necessary tools for our proposed system

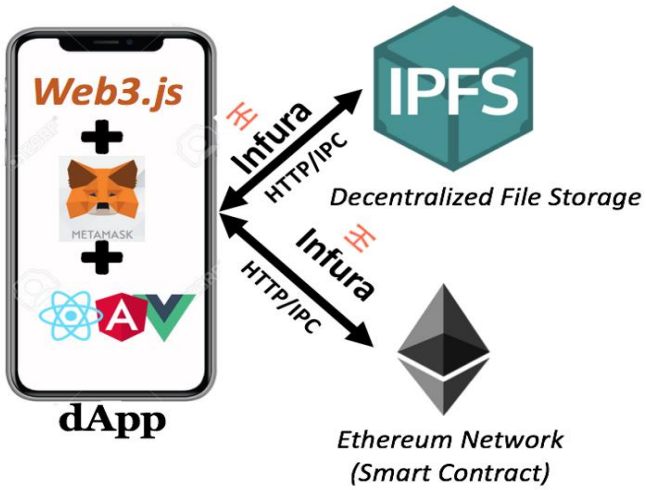

Fig. 5. Interactions between BC, IPFS and dApp

Steps that are involved in the data flow of the proposed system are presented below and the data flow diagram of the proposed BC based e-FIR system is illustrated in Fig. 6.

- The system allows both user and admin to access data on the blockchain.
- The victim's interface calls a smart contract to file e-FIR in the blockchain. The smart contract interacts with IPFS and blockchain.
- The smart contract is deployed on the blockchain that stores the hash of the FIR generated by the IPFS protocol.
- All the nodes including the police station and user can access the smart contract. The user gets a notification when a new block is added in the blockchain network through the smart contract.
- The user's FIR data is encrypted using a symmetric key before putting the FIR in the IPFS network. The IPFS generates the hash value of the chiper text. This hash value is stored in the blockchain with the aid of smart contract.

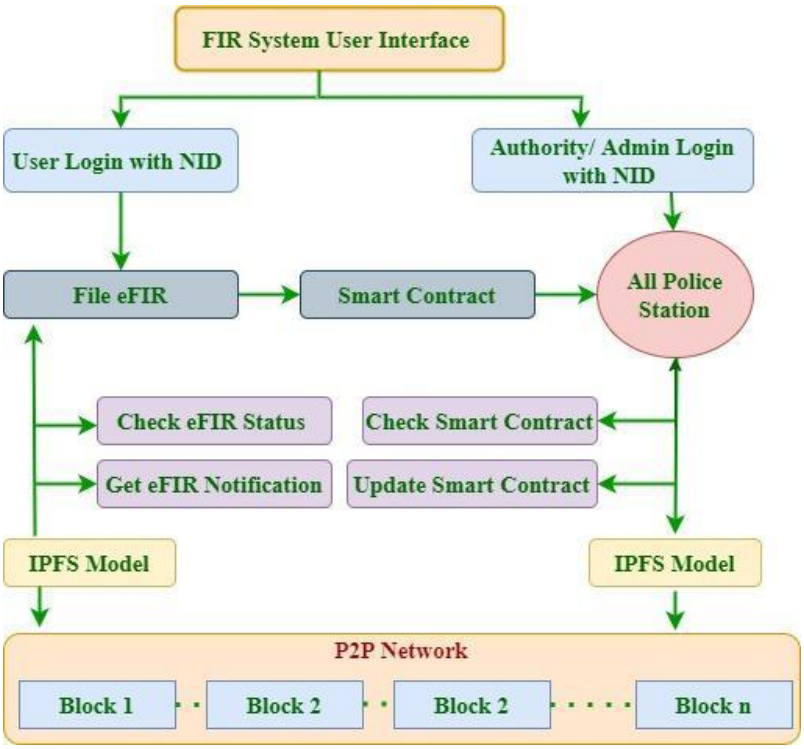

Fig. 6. Data Flow Diagram of the Proposed System

Our proposed system has been implemented and tested on a PC having the following specifications as shown as in Table 2 and the user interface of the proposed system is illustrated in Fig. 7.

Table 2. Specifications of the execution environment.

System RAM	8 GB
Hard Drive	HDD (minimum Space 1 GB)
System Core	Intel Core i7
Operating System	Windows 10

Fig. 7. Home page of the proposed system.

Fig. 8. shows a user interface that is created for the authority or public users to access FIR data.

Fig. 8. UI for writing an FIR.

IPFS is a distributed peer-to-peer hypermedia protocol designed to make the web faster, safer and more open. Storing large amounts of files in the blockchain is expensive. That's why for storing a large amount of data, we developed the system with the IPFS model in our blockchain. IPFS contains a huge amount of data and any kind of image. Large file is uploaded on the IPFS to get a hash value. If any user wants to access their document on the IPFS, it just needs to paste the hash value in the download box and then the IPFS system shows the user's document. The Ethereum transaction is made of the hash code of the original document to ensure the integrity and transparency. User interface of IPSF is shown in Fig. 9.

Fig. 9. UI for IPFS Protocol.

5. Result Analysis

In this section, the results are analyzed of the blockchain based e-FIR system. The proposed system is developed in the Ethereum environment using the truffle framework and Ganache.

5.1 Hashing Algorithms

We tested our development using different kinds of hash functions. Fig. 10 shows gas prices needed for different hashing algorithms. Gas refers to the fee, or pricing value, required successfully conducting a transaction or executing a contract on the Ethereumblockchain platform. SHA-256 is the most advanced and secure hashing algorithm, but it uses more Gas than other hashing techniques. Considering the security aspect, in this proposed system SHA-256 is used as the hashing algorithm.

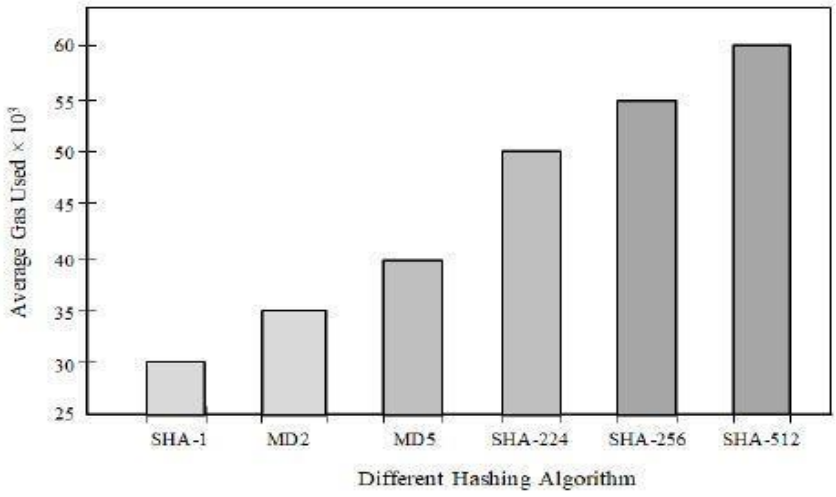

Fig. 10. Different Hashing Algorithm.

5.2 Consensus Algorithm

The e-FIR system is implemented on a public blockchain called Ethereum, the Ethereumblockchain uses PoW (Proof of Work) as a consensus algorithm to confirm transactions and produce new hash values. PoW provides 50% Byzantine fault tolerance and fast verification speed with strong scalability. Table 3 shows a comparison of different consensus algorithms.

Table 3. Comparison of the five Consensus Algorithms.

Characteristics	**Consensus Algorithm**				
	PoW	**PoS**	**DPoS**	**PBFT**	**RAFT**
Byzantine fault tolerance	50%	50%	50%	33%	N/A
Crash fault tolerance	50%	50%	50%	33%	50%
Verification speed	>100s	<100s	<100s	<10s	<10k
Throughput (TPS)	<100	<1000	<1000	<2000	>10K
Scalability	Strong	Strong	Strong	Weak	Weak

5.3 Smart Contract

A smart contract refers to the computation executed when a transaction is performed. It can be regarded as a stored procedure invoked upon a transaction. The inputs, outputs and states affected by the smart contract execution are agreed on by every node. For developing a smart contract, we used the Ethereumblockchain using solidity language. Smart contracts the building blocks we use to create blockchain applications. They are programs that we can write with source code and deploy to the blockchain. They are written in the Solidity programming language. Smart contracts are immutable, which means that once they've been created, they cannot change. Once a smart contract is deployed to a blockchain, its code cannot be updated like a normal application. That's because it represents a digital contract or agreement. In this proposal, we wrote a smart contract for storing the hash value of a FIR on the blockchain ledger.

5.4 Successful Transaction

In this term, we need to connect our Metamask by the private key of ganache. This requires some ether and cost gas value. And then the transaction will be successful. In Fig 11, we have shown our successful transaction which will increase by adding e-FIR data to the blockchain.

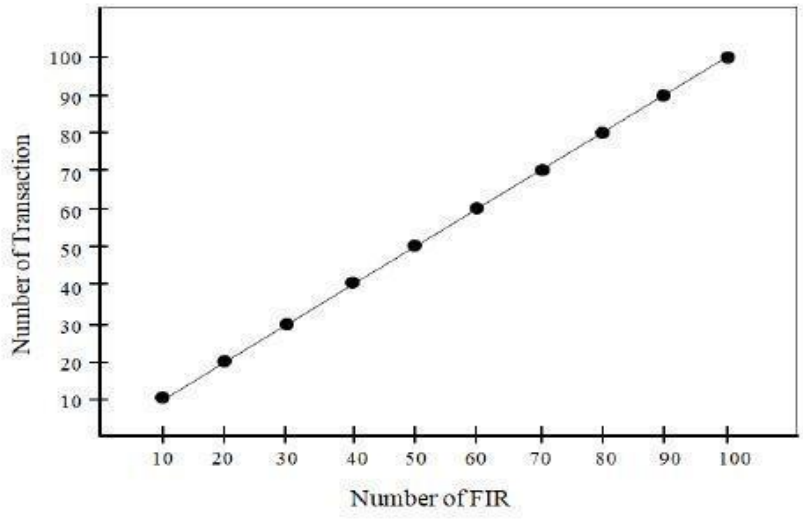

Fig. 11. Number of transactions vs Number of e-FIR in blockchain

5.5 Mine Blocks

After a successful transaction, blocks are mined in the ganache. And also, we can see our transactions in those blocks. All the data is stored in those blocks which can’t temper and delete. Now let’s see a simple block and transaction in the In Fig. 12 and 13.

Fig. 12. A single block in Ethereumblockchain.

Fig. 13. Transaction of a single block in Ethereumblockchain.

5.6 Blockchain Vs Traditional Database

In our system, blockchain works as a database. Blockchain database differs from a traditional database. Many advantages involve using blockchain instead of a traditional database. The difference between blockchain and traditional database is provided in Table 4:

Table 4. Comparisons of features for blockchain and Traditional database

Feature	Blockchain	Traditional Database
Storage System	It is a decentralized system.	It is a centralized system.
Redundancy Type	Redundant	Non-redundant
Mutability	It is immutable.	It is mutable.
Transparency	Every user can verify the validity of data in a blockchain.	Only database administrators can verify the validity of data.
Cost	For increasing the amount of data, it decreases the cost.	Cost increases with increasing data size.

6. Conclusion

In our daily life, we encounter various kinds of crimes. People go to the police station to file an FIR. In the police station, people face difficulty in manually documenting their complaints. e-FIR data can be tampered with by the various parties in the present system. The proposed system which is based on blockchain technology and the IPFS model can solve these issues. In the system, large volumes of files are managed using IPFS and no one can tamper with the data. If authorities give access to the public people only then they can see their records. In the future, we will implement our work using consortium blockchain because it is more secure than public Blockchain and to implement it with the main Ethereum network. We will also create a mobile app using flutter where users and authorities both would be able to access the blockchain network from anywhere and on any mobile or tablet device.

References

[1] [Online: October 27, 2020] Fourth industrial revolution; https://www.salesforce.com/blog/what-is-the-fourth-industrial-revolution-4ir/
[2] [Online: October, 2011] Bangladesh Police's Website, Police to People Ratio; http://www.police.gov.bd/index5.php?category=48
[3] [Online: March, 2019] Website of US department of justice for reporting a crime; https://www.justice.gov/actioncenter/report-crime
[4] Bangladesh Crime Rate & Statistics 2000-2021, https://bit.ly/3alcwV0,Last accessed on 17.03.2021.
[5] Khan,N. D.,Chrysostomou, C., and Nazir,B., "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, doi: 10.1109/VTC2020-Spring48590.2020.9129428.
[6] Han,M., Yan, M. , Li, J.,Ji, S.,and Li,Y., Generating uncertain networks based on historical network snapshots, in International Computing and Combinatorics Conference, Springer, Berlin, Heidelberg, 2013, 747–758
[7] Ai,C., Han,M., Wang, J., and Yan,M., An efficient social event invitation framework based on historical data of smart devices, in 2016 IEEE International Conferences on Social Computing and Networking (SocialCom), IEEE, 2016, 229–236.

[8] Security implications of blockchain cloud with analysis of block withholding attack.,2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 458.
[9] Z. Duan, M. Yan, Z. Cai, X. Wang, M. Han and Y. Li, Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems, Sensors, 16 (2016), p481.
[10] Han,M., Yan, M., Li,J.,Ji,S., and Li,Y., Neighborhood-based uncertainty generation in social networks, Journal of Combinatorial Optimization, 28 (2014), 561–576.
[11] Uddin,M. A.,Stranieri,A.,Gondal, I., and Balasubramanian,V., A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions, Blockchain: Research and Applications, 2021, 100006, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2021.100006.
[12] Nakamoto,S., "Bitcoin: A peer-to-peer electronic cash system," white paper, 2008.
[13] Uddin,M. A.,Stranieri,A.,Gondal, I., and Balasubramanian,V., "A decentralized patient agent controlled blockchain for remote patient monitoring," in 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2019, pp. 1–8.
[14] Uddin,M. A.,Stranieri,A.,Gondal, I., and Balasubramanian,V., "Blockchain leveraged task migration in body area sensor networks," in 2019 25th Asia-Pacifific Conference on Communications (APCC). IEEE, 2019, pp. 177–184.
[15] Uddin,M. A.,Stranieri,A.,Gondal, I., and Balasubramanian,V., "Dynamically recommending repositories for health data: a machine learning model," in Proceedings of the Australasian Computer Science Week Multiconference, 2020, pp. 1–10.
[16] T. T. A. Dinh et al., "Un-tangling Blockchain: A Data Processing View of BlockchainSystems,"in IEEE Transactions on Knowledge and Data Engineering, vol. 30, no.7, pp. 1366-1385, 1 July, 2018.
[17] Jean Bacon et al., "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers", 25 RICH. J.L. and TECH., no. 1, 2018.
[18] Antra Gupta et al., "A Method to Secure FIR System using Blockchain", IJRTE, Vol. 8, Issue-1, 2019.
[19] Reyna et al., "On blockchain and its integration with IoT. Challenges and opportunities." Future Generation Computer Systems, vol 88, 2018.
[20] Maisha A. Tasnim et al., "CRAB: Blockchain Based Criminal Record Management System", SpaCCS, LNCS 11342, pp. 294–303, 2018.
[21] KirtiMarmat et al., "E-FIR using E-Governance", IJIRST, vol. 3, 2016.
[22] Muhammad BaqerMollah et al., "Proposed E-Police System for Enhancement of E-Govemment Services of Bangladesh", IEEE/OSA/IAPR, 2012.
[23] Nakamoto, S., (2008). Bitcoin: A peer-to-peer electronic cash system.
[24] Dai, M., Zhang, S., Wang, H., & Jin, S. (2018). A low storage room requirement framework for distributed ledger in blockchain. IEEE Access, 6, 22970-22975.
[25] Clark, J. B. A. M. J., Edward, A. N. J. A. K., &Felten, W. (2015). Research perspectives and challenges for bitcoin and cryptocurrencies. url: hps://eprint. iacr. org/2015/261. pdf.
[26] Dorri, A., Kanhere, S. S., &Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In Proceedings of the second international conference on Internet-of-ings design and implementation (pp. 173- 178). ACM.
[27] Palai, A., Vora, M., & Shah, A. (2018, February). Empowering light nodes in blockchains with block summarization. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE
[28] Zheng, Q., Li, Y., Chen, P., & Dong, X. (2018, December). An Innovative IPFS-Based Storage Model for Blockchain. In 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (pp. 704-708). IEEE.
[29] Benet, J. (2014). Ipfs-content addressed, versioned, p2p le system. arXiv preprint arXiv:1407.3561.
[30] Pahlajani,S.,Kshirsagar,A. and Pachghare,V., "Survey on Private Blockchain Consensus Algorithms," 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), Chennai, India, 2019, pp. 1-6, doi: 10.1109/ICIICT1.2019.8741353.
[31] Vukolic,M., The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in International Workshop on Open Problems in Network Security, Springer, 2015, 112-125.
[32] Security implications of blockchain cloud with analysis of block withholding attack., 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 458.
[33] Kumar, A., Ghrera, S. P., &Tyagi, V. A comparison of buyerseller watermarking protocol (BSWP) based on discrete cosine transform (DCT) and discrete wavelet transform (DWT). In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1 (pp. 401-408). Springer, Cham (2015).
[34] Kumar, A., Ghrera, S. P., &Tyagi, V. Modified buyer seller watermarking protocol based on discrete wavelet transform and principal component analysis. Indian Journal of Science and Technology, 8(35), 1-9, (2015).

Authors' Profiles

Khandaker Mohammad Mohi Uddin is an academic researcher and an Assistant Professor in the Department of Computer Science and Engineering at Dhaka International University. He has done his B.Sc. and M.Sc. (Research) in Computer Science and Engineering from Jagannath University. His research interests are in the field of Machine Learning/Deep Learning, Wireless Networking, Computer Vision and Image Processing, and IoT.

Sadia Mahamuda was born in 1997 in Rajbari, Bangladesh. She completed his B.Sc in Computer Science and Engineering degree from Dhaka International University, Dhaka, Bangladesh in 2021. She has experience working as a React App Developer and continuing this till now.

Sikder Sajib Al Shahriar was born in 1999 in Dhaka Bangladesh. He completed his B.Sc in Computer Science and Engineering from Dhaka International University, Dhaka, Bangladesh in 2020 and continuing his M.Sc in Cyber Security at the University of Hertfordshire, England, United Kingdom. He has experience working as a Web Developer for two years.

Md Ashraf Uddin received his B.Sc. and M.Sc. degrees in computer science and engineering from the University of Dhaka. He has completed his Ph.D. at Federation University Australia. He is serving as an Associate Professor in the Department of Computer Science and Engineering, at Jagannath University, Dhaka, Bangladesh. His research interests include privacy and security in Remote Patient Monitoring, Blockchain, modeling, analysis, and optimization of protocols and architectures for underwater sensor networks, artificially intelligent, data mining, and so forth.

How to cite this paper: Khandaker Mohammad Mohi Uddin, Sadia Mahamuda, Sikder Sajib Al Shahriar, Md Ashraf Uddin, "Blockchain and IFPS based Secure System for Managing e-FIR", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.15, No.1, pp. 29-40, 2023. DOI:10.5815/ijieeb.2023.01.03