RESEARCH ARTICLE

Using IPFS and Hyperledger on Private Blockchain to Secure the Criminal Record System

Mamun Ahmed, Akash Roy Pranta, Mst. Fahmida Akter Koly,
Farjana Taher, and Mohammad Asaduzzaman Khan

ABSTRACT

In today's modern world, digitizing criminal records is a need for a nation. It contains criminal information that is securely and digitally stored. Blockchain technology allows us to store highly secure and efficient data. In this system, each transaction is permanent, which makes changing data or hacking the system nearly impossible. In our paper, hyperledger based on a low-cost private blockchain and IPFS are used to track any media file as evidence. Although the owner had access to all the capabilities for handling criminal records, the system did restrict users' access in several ways. More security, privacy, and authorization are prioritized by this. We use the concept for updating fugitive criminal records.

Keywords: Blockchain, criminal record, fugitive criminal, hyperledger, IPFS.

Published Online: January 5, 2023

ISSN: 2736-5492

DOI :10.24018/ejcompute.2023.3.1.81

M. Ahmed*
Department of CSE, Bangladesh Army International University of Science and Technology, Cumilla, Bangladesh.
(e-mail: mamun@baiust.edu.bd)
A. Roy Pranta
Department of CSE, Bangladesh Army International University of Science and Technology, Cumilla, Bangladesh.
(e-mail: akashroy1305@gmail.com)
Mst. F. Akter Koly
Department of CSE, Bangladesh Army International University of Science and Technology, Cumilla, Bangladesh.
(e-mail: fahmidakoly7019@gmail.com)
F. Taher
Department of CSE, Bangladesh Army International University of Science and Technology, Cumilla, Bangladesh.
(e-mail: ftaher842@gmail.com)
M. A. Khan
Department of CSE, Bangladesh Army International University of Science and Technology, Cumilla, Bangladesh.
(e-mail: mak@baiust.edu.bd)

Corresponding Author

I. INTRODUCTION

Criminal records detract from a person's previous criminal history, and authorities may easily identify criminals by looking at them. The authorities can simply maintain the country safe by penalizing offenders by looking at their criminal records. As a result, a criminal record is a highly sensitive document for countries. The failure of creating and maintaining a secure system Hyperledger fabric extends a new method to the consensus that allows for high performance while maintaining anonymity might end in criminal record fabrication. The ability to wipe all traces of a criminal record transaction, according to the preceding rationale, renders the criminal record system extremely vulnerable. Because it is impossible to delete or remove any record of transactions from a block of the Blockchain, the criminal record system using Blockchain technology may be considered safe.

II. PROPOSED APPROACH

We used a private hyperledger blockchain and IPFS to construct a criminal record digitization system where every transaction is immutable and not accessible to everyone. An administrator or owner can generate a criminal record asset and a fugitive criminal asset, both of which are linked to a criminal asset. Every criminal asset has a unique asset ID and IPFS number that is used to identify it. If the criminal is arrested, this part is not necessary. The fugitive criminal asset should be updated if the criminal is a wanted by the law. It can be modified if there are any mistakes or inaccuracies in the needed data. All transactions will be recorded, and no one will be able to change or modify them. Since all transactions are recorded, there is no danger of fraud, making the system safe and more secure than others.

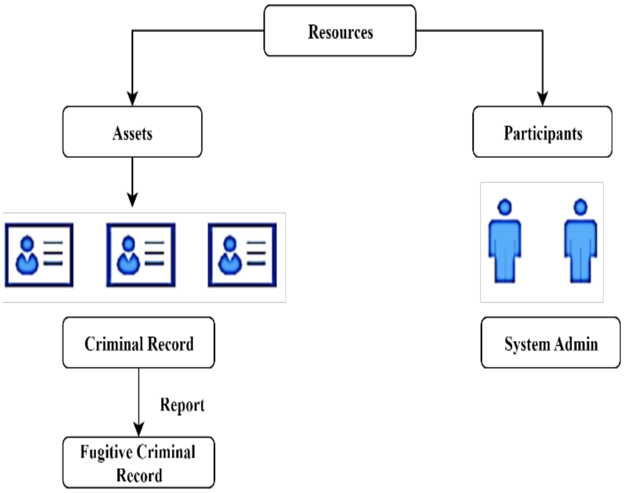


Fig. 1. Resources of the proposed system.

III. Related Works

In paper [1], the objective of this thesis is to demonstrate how to safeguard data using a private Blockchain Technology. In paper [2], proposed a two-tier Blockchain architecture, with hot and cold Blockchains for digital evidence. Information that changes regularly is stored on the hot Blockchain, whereas material that does not change, such as videos, is saved in the cold Blockchain. Blockchain is a perfect method for ensuring transparency up to the highest levels of government by employing a decentralized peer-to-peer network to store immutable data. Evichain adds the same decentralized network's transparency and security into the criminal investigative process. As written [3], the researchers proposed a solution for evaluating and Scrutinizing Crime using BlockChain with Evichain. This is an application that stores all relevant investigation-related data in a Blockchain with restricted access to just a small number of users. Evichain is not acceptable everywhere because it is less secure than other Blockchains and it is not familiar as popular Blockchains like bitcoin, Ethereum, and Hyperledger. In paper [4], the Blockchain concept was devised to provide security to the Bitcoin cryptocurrency network, where trust is formed by providing a publicly shared ledger with an agreed-upon and immutable record of transactions between participants. The investigation concludes that a public Blockchain has benefits in terms of transaction robustness, availability, and built-in non-repudiation, but that additional safeguards, such as content encryption and limited re-use of identities, are required to prevent information leakage and to provide a non-repudiation path for content access. As written [5], to overcome these issues, they offered a novel distributed A&A protocol based on Blockchain technology for smart grid networks. The suggested protocol combines a unique Blockchain approach with dispersed authentication and immutable ledger characteristics of Blockchain architectures appropriate for the power system to accomplish resource authentication and identity authentication for smart grid systems. In paper [6], they presented a Blockchain-based architecture for that digital archive that provides decentralized, efficient, and cost-effective security and availability. In addition, the architecture provides the opportunity to restore the catalog's contents in a tamper-proof manner. In paper [7], for the catalog, the researchers proposed a Blockchain-based architecture. They also used an off-chain data storage technique for performance and economic considerations which is not efficient as a hyperledger. In paper [8], the researcher's goal is to use blockchain technology to build a revolutionary system that keeps the prisoner's credentials and efficiently verifies them. The suggested solution is built on the Hyperledger framework, and the testing results show that it is advantageous to both current and future research departments. In paper [9], to guarantee the consistency and lack of manipulation of the evidence transfer record, they suggested a Blockchain network for tracking evidence transfer occurrences throughout various court departments. They used a text chain to implement their system and the test chain is not secure and acceptable as a Blockchain. In paper [10], using fabric's smart contract technology, this study presents a protective mechanism for automating the whole digital rights life cycle on the Blockchain. In paper [11] In the data, this paper helps us to prevent unlawful changes. Implementing Blockchain technology introduces us to a criminal record storage system and this helps to keep privacy and gain integrity. In which way the authority can be efficient, this system presents. The security depends on its databases team. It helps to overcome any possible failure problems of software/hardware. In writing [12], they proposed a method for decentralized storage of citizen criminal records using a permissioned Blockchain, utilizing few of its properties to make sure the privacy, security, immutability, and accessibility of sensitive stored data. This system would be superior to the current one since it can cryptographically ensure that data has not been modified after it has been stored by anybody other than a competent authority. In paper [13], the researchers developed a digital forensic chain of custody system based on the Ethereum Blockchain. The Blockchain-based digital forensics chain of custody had the potential to significantly asset forensic applications by maintaining integrity and transparency. Their drawback is that they built their system on Ethereum, which is a public Blockchain that everyone can access. In paper [14], they presented a secure peer-to-peer (p2p) file storage network using a distributed, decentralized Blockchain technology for storing evidence (IPFS). Only authorized staff will be able to access or keep the evidence because of the system’s Hyperledger Sawtooth construction and custom transaction family, which records each transaction from the moment the documentation is acquired. In paper [15], they recommended for a custodial Blockchain architecture to help with the security and transparency of digital evidence in criminal investigations. The system employs Ethereum smart contracts to ensure the validity and integrity of digital evidence during the initial investigation, case management, and court phases. However, Ethereum is a public Blockchain, making it accessible to all users, which is a drawback. In the paper [16], they provided a reliable mobile phone forensics solution built on Blockchain and memory analysis which combines the advantages of both technologies. Blockchain is used across the whole system process to guarantee the validity, honesty, and auditability of evidence. On paper [17], It is proposed to use the MF-Ledger, a Blockchain hyperledger sawtooth-enabled novel, secure, and effective digital forensic investigation architecture, in which participating stakeholders generate a private network to swapping information and reach consensus on various inquiry activities before those activities being recorded on the Blockchain ledger. The recommended architectural method offers a trustworthy mechanism for information integrity, prevention, and preservation for storing proof (chain of custody) in a private permissioned encoded Blockchain ledger forever and immutably. The goal of this study is to add to the notion of the Digital Evidence Cabinet (DEC) by merging IPFS with Hyperledger Fabric (HF) as a repository storage system. It is viable to accomplish ease of data transmission, improved data trust, and data ownership preservation by proposing an alternative way to the IPFSChain paradigm [18]. The transaction record cannot be altered by a single user. Their proposed approach could assist the Indonesian government in protecting citizens' personal information and improving information management openness [19].

IV. Proposed Procedure

This solution enables private Blockchain on the Hyperledger platform. Each asset on the Blockchain will provide a hash that is identifiable. If the hash is altered, it will no longer match the original. As a result, the hash is unchangeable. A transaction will be created for each create, update, and delete. The following is the system's overall structure:

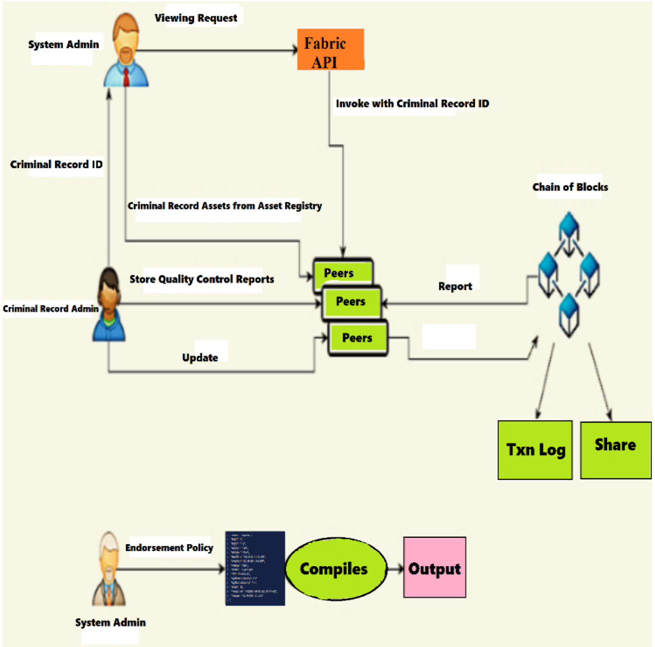


Fig. 2. System information flow among the peer to peer and interaction with output ledger.

A. Constructing The Assets

Each criminal record will be recorded on the Hyperledger Blockchain as an asset. The asset contains sensitive criminal record information such as name, date of birth, nationality, religion, hair color, and so on. All assets are gathered and stored in the private Blockchain's asset registry. Asset registry is very important for gathering information from officers and storing it in the authority's assets for further process. Fugitive transactions will be added to the criminal record transaction that was previously made. The asset transaction is the only way to create and amend asset information, demonstrating the Blockchain's immutability. The history of criminals can be preserved in this way.

B. Execution of Transaction

Our proposed Blockchain-based protocol operates in the same manner as other Blockchain systems for all transactions. Figure 1 demonstrates the execution of transactions being used. To create, access, and update the assets, this system needs to execute the transactions being used. A transaction becomes immutable after it is recorded to one of the chain's blocks, making it impossible to change it without executing a significant attack, such as the consensus attack, which is extremely hard to execute. When a new asset is generated, new criminal information is also included. And the Fugitive criminal record was added to the previously created criminal record.

C. Identifying Participant Types

In our system, users are expected to determine the mechanism for access control. The system administrator oversees the operation. The next parts go through each participant's role.

1) System Admin

The system administrator is in charge of the entire system and has access to all of its data. The assets and history records are accessible to the admin. He can also make changes, like creating or modifying it. Administrators can personalize new participants and review the record. The system administrator can take proper measures to prevent any type of breach.

D. Retaining Assets on Recorded in Asset Registry

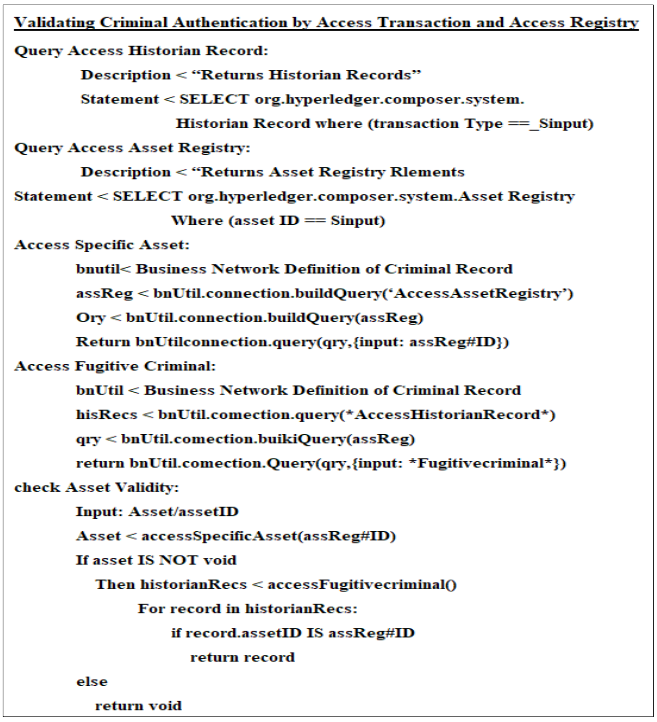
The asset registry will have a record of every asset in our ecosystem, which is seen in Fig. 2. When an administrator adds a new asset, the asset registry is updated. No asset may be removed from the record since Blockchain has immutable qualities. If an administrator wants to remove any asset ID, it also is recorded. The asset registry will also include the criminal history of the fugitive. The modified information is also added to the asset registry.

E. Transaction from the Historian's Record

There are essentially two transactions in our system: create transactions and update transactions in the Blockchain system, transactions are maintained in immutable blocks. The transaction details can be obtained from the historical record for this feature. A unique ID is assigned to each historian record. so that the information can be retrieved the transaction ID as well as the historian ID, is required. It is possible to determine whether or not a transaction exists. The asset registry and historical record have a function that may be used to check for updates. Based on transaction records, we can classify criminal activities. The historian's database will keep track of every attempt to see or get evidence from another officer.

F. Transaction Query in Historian Record

Every asset in our system is maintained in the asset registry, and every transaction is noted in the historical record. In addition to the transaction ID, the historical record is additionally indexed by the participant ID, which is in charge of the transaction's execution, and the transaction type. An admin has access to view, update, and modify.

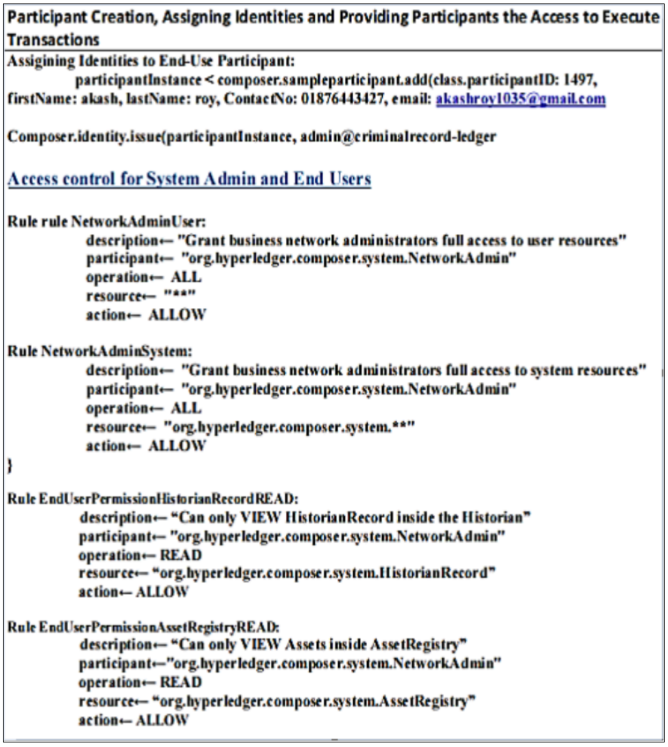


```
Validating Criminal Authentication by Access Transaction and Access Registry
Query Access Historian Record:
        Description < "Returns Historian Records"
        Statement < SELECT org.hyperledger.composer.system.
                    Historian Record where (transaction Type ==_Sinput)
Query Access Asset Registry:
        Description < "Returns Asset Registry Rlements
Statement < SELECT org.hyperledger.composer.system.Asset Registry
                    Where (asset ID == Sinput)
Access Specific Asset:
        bnutil< Business Network Definition of Criminal Record
        assReg < bnUtil.connection.buildQuery('AccessAssetRegistry')
        Ory < bnUtil.connection.buildQuery(assReg)
        Return bnUtilconnection.query(qry,{input: assReg#ID})
Access Fugitive Criminal:
        bnUtil < Business Network Definition of Criminal Record
        hisRecs < bnUtil.comection.query(*AccessHistorianRecord*)
        qry < bnUtil.comection.buikiQuery(assReg)
        return bnUtil.comection.Query(qry,{input: *Fugitivecriminal*})
check Asset Validity:
        Input: Asset/assetID
        Asset < accessSpecificAsset(assReg#ID)
        If asset IS NOT void
          Then historianRecs < accessFugitivecriminal()
                For record in historianRecs:
                    if record.assetID IS assReg#ID
                        return record
        else
          return void
```

Fig. 3. Authentication of criminal record validity by transaction query.

G. Creating Permissions Regulations

Access to system resources including economic models, transaction histories, asset data, and transactions may be managed through the Hyperledger Fabric Access Control function. With a few exceptions, program administrators can choose from a variety of materials and activities. In our system, the end-users are the people of authority such as the officers of the passport office, and the government investigating officers. They can read the record of any criminal for any investigation.



```
Participant Creation, Assigning Identities and Providing Participants the Access to Execute Transactions
Assigining Identities to End-Use Participant:
        participantInstance < composer.sampleparticipant.add(class.participantID: 1497,
firstName: akash, lastName: roy, ContactNo: 01876443427, email: akashroy1035@gmail.com

Composer.identity.issue(participantInstance, admin@criminalrecord-ledger

Access control for System Admin and End Users

Rule rule NetworkAdminUser:
          description← "Grant business network administrators full access to user resources"
          participant← "org.hyperledger.composer.system.NetworkAdmin"
          operation← ALL
          resource← "**"
          action← ALLOW

Rule NetworkAdminSystem:
          description← "Grant business network administrators full access to system resources"
          participant← "org.hyperledger.composer.system.NetworkAdmin"
          operation← ALL
          resource← "org.hyperledger.composer.system.**"
          action← ALLOW
}

Rule EndUserPermissionHistorianRecordREAD:
         description← "Can only VIEW HistorianRecord inside the Historian"
         participant← "org.hyperledger.composer.system.NetworkAdmin"
         operation← READ
         resource← "org.hyperledger.composer.system.HistorianRecord"
         action← ALLOW

Rule EndUserPermissionAssetRegistryREAD:
         description← "Can only VIEW Assets inside AssetRegistry"
         participant←"org.hyperledger.composer.system.NetworkAdmin"
         operation← READ
         resource← "org.hyperledger.composer.system.AssetRegistry"
         action← ALLOW
```

Fig. 4. Authentication and key agreement limiting access to Blockchain

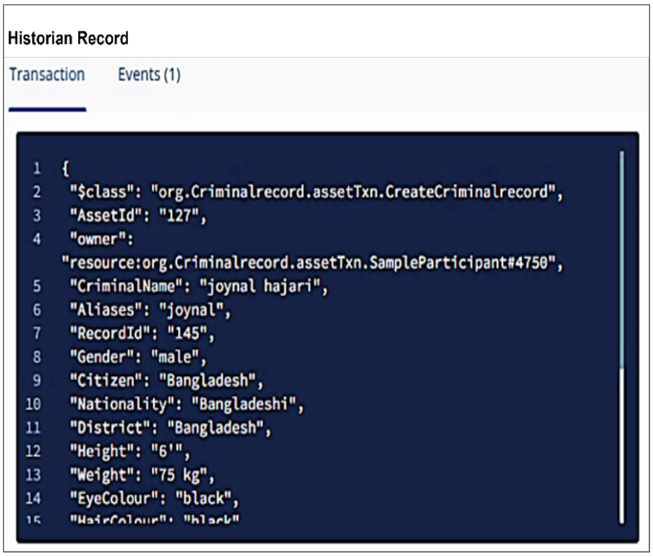
V. Results Evaluation

We take some sample criminal information randomly to create a criminal record for our systems. A sample of criminal details is given below:

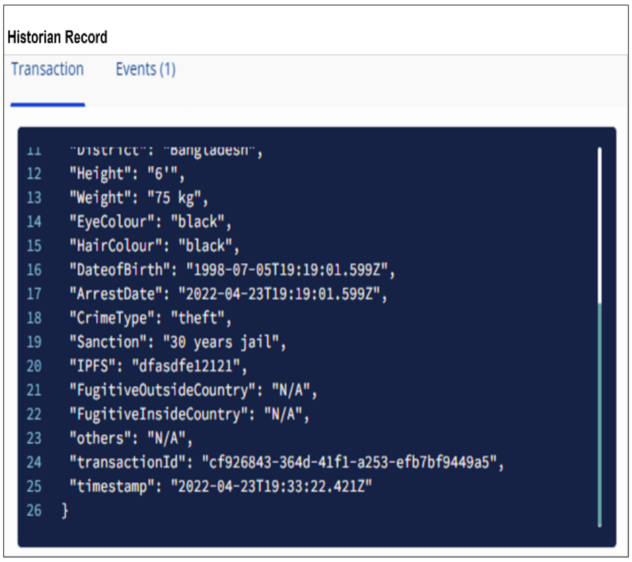
TABLE I: Criminal Details for Our System Overview Repurpose

Serial No	Criminal Name	Record Id	Date of Birth	Arrest Date	Current Situation
01	Mastan Mirza	1545	05.02.1926	12.11. 1994	Dead
02	Dawood Ibrahim	1542	26.12.1955	N/A	Fugitive in Karachi
03	Chota Rajan	1540	13.01.1959	25.10. 2015	N/A
04	Eden Paul	1539	05.06.1978	12.03. 2008	In prison
05	Joe Adonis	1420	27.07.1990	15.04. 2009	In prison

By using the CreateCriminalrecord transaction in figure 5 we can create the criminal record with a unique asset ID including CriminalName, Aliases, RecordID, Gender, Citizen, Nationality, District, Height, Weight, Eye Color, Hair Color, DateofBirth, ArrestDate, CrimeType, Sanction, IPFS and all necessary information which are used.



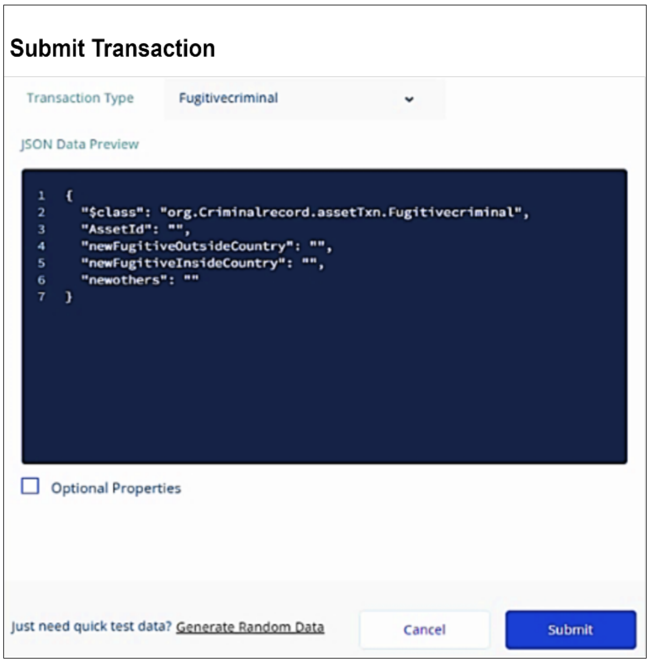
```
{
 "$class": "org.Criminalrecord.assetTxn.CreateCriminalrecord",
 "AssetId": "127",
 "owner":
"resource:org.Criminalrecord.assetTxn.SampleParticipant#4750",
 "CriminalName": "joynal hajari",
 "Aliases": "joynal",
 "RecordId": "145",
 "Gender": "male",
 "Citizen": "Bangladesh",
 "Nationality": "Bangladeshi",
 "District": "Bangladesh",
 "Height": "6'",
 "Weight": "75 kg",
 "EyeColour": "black",
 "HairColour": "black"
```



```
 "District": "Bangladesh",
 "Height": "6'",
 "Weight": "75 kg",
 "EyeColour": "black",
 "HairColour": "black",
 "DateofBirth": "1998-07-05T19:19:01.599Z",
 "ArrestDate": "2022-04-23T19:19:01.599Z",
 "CrimeType": "theft",
 "Sanction": "30 years jail",
 "IPFS": "dfasdfe12121",
 "FugitiveOutsideCountry": "N/A",
 "FugitiveInsideCountry": "N/A",
 "others": "N/A",
 "transactionId": "cf926843-364d-41f1-a253-efb7bf9449a5",
 "timestamp": "2022-04-23T19:33:22.421Z"
}
```

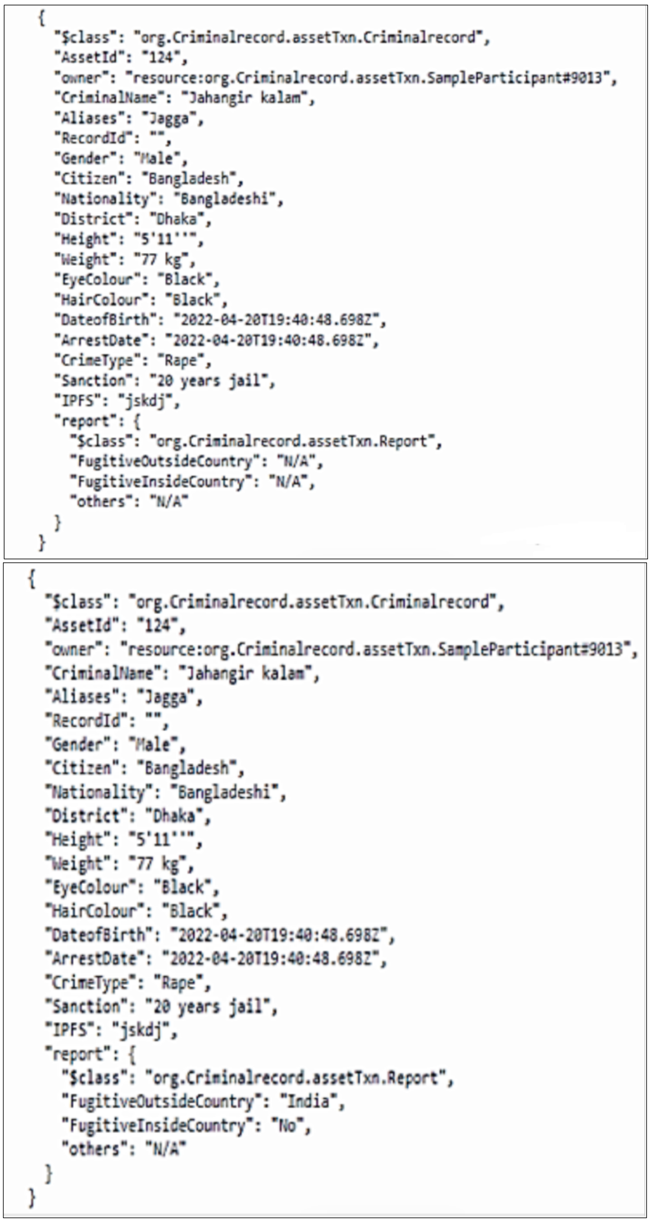
Fig. 5 and 6. Create asset transaction with information.

DOI: http://dx.doi.org/10.24018/ejcompute.2023.3.1.81



```
{
  "$class": "org.Criminalrecord.assetTxn.Fugitivecriminal",
  "AssetId": "",
  "newFugitiveOutsideCountry": "",
  "newFugitiveInsideCountry": "",
  "newothers": ""
}
```

Fig. 7. Fugitive criminal transaction.



```
{
  "$class": "org.Criminalrecord.assetTxn.Criminalrecord",
  "AssetId": "124",
  "owner": "resource:org.Criminalrecord.assetTxn.SampleParticipant#9013",
  "CriminalName": "Jahangir kalam",
  "Aliases": "Jagga",
  "RecordId": "",
  "Gender": "Male",
  "Citizen": "Bangladesh",
  "Nationality": "Bangladeshi",
  "District": "Dhaka",
  "Height": "5'11''",
  "Weight": "77 kg",
  "EyeColour": "Black",
  "HairColour": "Black",
  "DateofBirth": "2022-04-20T19:40:48.698Z",
  "ArrestDate": "2022-04-20T19:40:48.698Z",
  "CrimeType": "Rape",
  "Sanction": "20 years jail",
  "IPFS": "jskdj",
  "report": {
    "$class": "org.Criminalrecord.assetTxn.Report",
    "FugitiveOutsideCountry": "N/A",
    "FugitiveInsideCountry": "N/A",
    "others": "N/A"
  }
}
```

```
{
  "$class": "org.Criminalrecord.assetTxn.Criminalrecord",
  "AssetId": "124",
  "owner": "resource:org.Criminalrecord.assetTxn.SampleParticipant#9013",
  "CriminalName": "Jahangir kalam",
  "Aliases": "Jagga",
  "RecordId": "",
  "Gender": "Male",
  "Citizen": "Bangladesh",
  "Nationality": "Bangladeshi",
  "District": "Dhaka",
  "Height": "5'11''",
  "Weight": "77 kg",
  "EyeColour": "Black",
  "HairColour": "Black",
  "DateofBirth": "2022-04-20T19:40:48.698Z",
  "ArrestDate": "2022-04-20T19:40:48.698Z",
  "CrimeType": "Rape",
  "Sanction": "20 years jail",
  "IPFS": "jskdj",
  "report": {
    "$class": "org.Criminalrecord.assetTxn.Report",
    "FugitiveOutsideCountry": "India",
    "FugitiveInsideCountry": "No",
    "others": "N/A"
  }
}
```

Fig. 8 and 9. Final created asset information.

TABLE II: TIME REQUIRED TO COMPLETE A TRANSACTION USING DIFFERENT BLOCKCHAIN TECHNOLOGIES

Number of transaction	Time of Hyperledger	Time of Ethereum	Time of Bitcoin
350	7.53 seconds	40.9 seconds	42.89 seconds
300	6.43 seconds	32.89 seconds	35.67 seconds
250	4.58 seconds	25.5 seconds	27.68 seconds
200	3.26 seconds	19.85 seconds	21.538 seconds
150	2.45 seconds	12.9 seconds	15.26 seconds
100	1.98 seconds	5.35 seconds	7.185 seconds

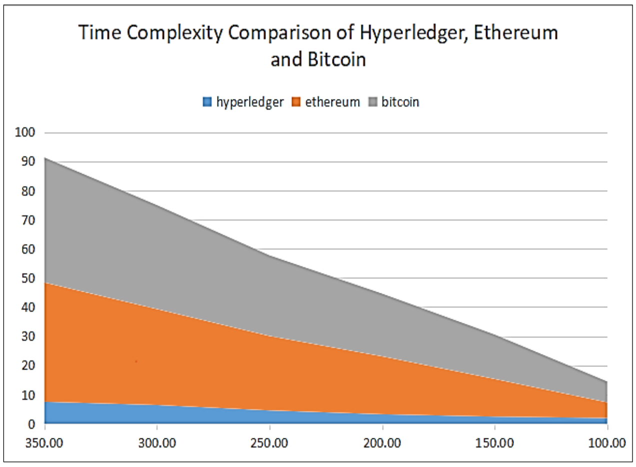


Fig. 10. Time complexity area chart for hyperledger, Ethereum, and bitcoin.

VI. CONCLUSION

By utilizing IPFS and hyperledger, our approach is more secure, immutable, and reliable. Hyperledger's permissioned and sensitive nature enables the system to function consistently in all areas. Cryptocurrency is not allowed, so it's safe. We use IPFS for any media file as crime evidence. Transparency and traceability are provided for data shared over a network. On the other hand, Ethereum is not suitable for use in developing a system for tracking criminal activities because criminal records are extremely sensitive and Ethereum is a public blockchain that anybody can access. As a result, Hyperledger is the ideal platform for our criminal history database.

REFERENCES

[1] Zunair H, Muhammad I, Ammbar N. Forensics to Government Agencies Data using Hyper Ledger Fabric (HLF). *JCBI*. 2022; 3(1): 208-229.

[2] Kim D, Ihm S-Y, Son Y. Two-Level Blockchain System for Digital Crime Evidence Management. *Sensors*. 2021; 21(9): 1-17.

[3] Shabaz M, Smiley G. Evichain: Evaluating and Scrutinizing Crime using Block Chain. *IJRTE*. 2021: 8(3): 3992-3994..

[4] Barclay I. Innovative Applications of Blockchain Technology in Crime and Security. M.S. Thesis, Cardiff University; 2017.

[5] Zhong Y, Mi Z, Jiangnan L, Jiahui C, Yan L, Yun Z, Muchuang H, et al. Distributed blockchain-based authentication and authorization protocol for smart grid. *Wireless Communications and Mobile Computing*. 2021; 2021(15): 1530-8669.

[6] Basile M, Dini G, Marchetti A, Bacciu C, Duca AL. A blockchain-based support to safeguarding the Cultural Heritage. *EVA Proceedings of the Electronic Imaging & the Visual Arts, edited by V. Cappellini*. 2019; 64-73.

[7] Alghazwi M, Turkmen F, Velde JV, Karastoyanova D. Blockchain for genomics: a systematic literature review. *Distributed Ledger Technologies: Research and Practice*. 2021; 1(2): 1-28.

[8] Shukla P, Tyagi R, Tyagi A. Implementation of blockchain on criminality record checker. *Int. J. Engineering Research & Technology (IJERT)*. 2020; 9(04): 682-686.

DOI: http://dx.doi.org/10.24018/ejcompute.2023.3.1.81

[9] Guo J, Wei X, Zhang Y, Ma J, Gao H, Wang L, Liu Z, et al. Antitampering scheme of evidence transfer information in judicial system based on blockchain. *Security and Communication Networks*. 2022; 2022.

[10] Liu Y, Zhang J, Wu S, Pathan MS. Research on digital copyright protection based on the hyperledger fabric blockchain network technology. *PeerJ Computer Science*. 2021; 7: e709.

[11] Tasnim MA, Omar AA, Rahman MS, Bhuiyan M, Alam Z. Crab: Blockchain based criminal record management system. *In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*. 2018: 294-303.

[12] Dini AT, Abete EG, Colombo M, Guevara J, Hoffmann BS, Abeledo MC. Analysis of implementing blockchain technology to the argentinian criminal records information system. *In 2018 Congreso Argentino de Ciencias de la Informática y Desarrollos de Investigación (CACIDI)*. 2018: 1-3.

[13] Lone AH, Mir RN. Forensic-chain: Ethereum blockchain based digital forensics chain of custody. *Sci. Pract. Cyber Secur*. 2018; 1(1): 21-27.

[14] Borse Y, Patole D, Chawhan G, Kukreja G, Parekh H, Jain R. Advantages of Blockchain in Digital Forensic Evidence Management. *Proceedings of the 4th International Conference on Advances in Science & Technology (ICAST2021)*. 2021.

[15] Tsai, Fu-Ching. The Application of Blockchain of Custody in Criminal Investigation Process. *Procedia Computer Science*. 2021; 192: 2779-2788.

[16] Hu S, Zhang S, Fu K. TFChain: Blockchain-based Trusted Forensics Scheme for Mobile Phone Data Whole Process. *In 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC)*. 2022; 6: 155-165.

[17] Khan AA, Uddin M, Shaikh AA, Laghari AA, Rajput AE, et al. MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. *IEEE Access*. 2021; 9: 103637-103650.

[18] Hanafi J, Prayudi Y, Luthfi A. IPFSChain: Interplanetary File System and Hyperledger Fabric Collaboration for Chain of Custody and Digital Evidence Management. *International Journal of Computer Applications*. 2021; 183(41): 24-32.

[19] Fathiyana RZ, Yutia SN, Hidayat DJ. Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology. *JOIV: International Journal on Informatics Visualization*. 2022; 6(1): 109-116.