xCRM: Blockchain Interoperable Crime Report Management System By Utilizing Hyperledger Cacti & Private Data Collection (PDC)

Ruhul Amin
Department of Computer Science and Engineering
Sylhet Engineering College
Sylhet, Bangladesh
orcid.org/0000-0002-0200-5572

Rahat Ahmed Chowdhury
Department of Computer Science and Engineering
Sylhet Engineering College
Sylhet, Bangladesh
rahatahmedchy01@gmail.com

Shah MD Tanjim
Department of Computer Science and Engineering
Sylhet Engineering College
Sylhet, Bangladesh
tanjimahmed1161@gmail.com

Ashraful Islam
Department of Computer Science
University of Regina
Saskatchewan, Canada
AIY497@uregina.ca

Mohammad Shamsul Islam
Department of Computer Science and Engineering
Faridpur Engineering College
Faridpur, Bangladesh
shamsul.cse@sec.ac.bd

2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM) | 979-8-3503-1600-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/NCIM59001.2023.10212677

***Abstract*—The process of bringing criminals to justice can be complicated when reporter information and sensitive data related to the case are revealed and may involve international law enforcement cooperation, especially when a criminal flees to another country. To tackle this issue, an interoperable crime management system is necessary. This study proposes a blockchain-based interoperable crime management system that provides secure and decentralized communication between different blockchain-based platforms, ensuring anonymity, transparency, and immutability. We present a methodology for crime reporting, evidence management, forensic testing, a collaboration between investigation agencies, and resource sharing where anyone can report in two modes: anonymous mode, which is only for passing any information to the police, or generate mode, which will create an FIR (First Information Report) and subsequent procedures. To ensure the security of our data, we have implemented Hyperledger Fabric Private Data Collection (PDC) for each report and investigation. The PDC will consist of the team leader, investigation officer, reporter, and any other relevant users as members. All interactions will occur within the specific channel created for each report, and files and additional information will be shared through the PDC. This system uses Hyperledger Cacti to implement interoperability and allows investigation and collaboration with others, like courts, forensics, and special investigation agencies, even with foreign systems. This proposed system is effective and efficient, enhancing the performance of blockchain networks.**

***Index Terms*—Crime Reporting, Interoperability, Hyperledger Cacti, Hyperledger Fabric Private Data Collection (PDC), Distributed Ledger**

I. Introduction

Crime is defined as any activity that violates the law, and the criminal is to be punished by the legal system [1]. If a criminal flees to another country, the process of bringing them to justice can be complicated and may involve international law enforcement cooperation. It is one of the main reasons why criminals are more inclined to engage in criminal activities. To bring the criminal to justice, an interoperable crime management system is necessary. Blockchain interoperability is the efficient transmission of data and transactions between various blockchain networks without the need for intermediaries or third-party platforms [2] [3]. Interoperability allows different agencies to share information more easily and collaborate more effectively. With an interoperable system, law enforcement agencies can respond more quickly to emergencies and incidents. This will aid in reducing the crime rate, and people who feel safe and secure in their communities are more inclined to obey the law and contribute to society's general well-being. As a result, economic growth and development are boosted [4].

In the conventional system, in order to register an FIR, people have to visit the police station physically. As a result of an upsurge in criminal activity as well as the presence of corrupt police officials, they tend to refuse the registration of FIR/Complaints [5]. On the other hand, the safety of the crime reporter/whistleblowers is not being ensured by the officers [6]. As a result, there are different forms of retaliation from criminals, and encouraging more individuals to participate in reporting is difficult. Also, in order to make the whole process much faster and transparent, the stakeholders of a crime management system should be able to collaborate easily. To resolve this issue, one of the researchers proposed a web-based interoperable system [7]. Previously there was some work done in this field using blockchain but none of those supports interoperability [5] [8] [6] [9] [10]. In 2021, Arnab et. al [11] first proposed a blockchain-based smart policing system where they managed to build a collaboration system between stakeholders using Hyperledger Fabric and smart contracts.

In this study, we looked at how to establish a communication medium between two or more blockchain-based crime management systems. We can transfer case details, forensic reports, criminal records, investigation reports,

979-8-3503-1600-1/23/$31.00 ©2023 IEEE

and other resources from one blockchain to another through interoperability. To implement the interoperable feature, we will be using Hyperledger Cacti which aims to provide decentralized and secure integration between blockchain networks [12]. Interoperability allows investigation officers to access data from another platform and add it to their records. Also, as anonymity is the basic security requirement in the crime reporting system, this model will provide two reporting modes, general and anonymous.

Objective: The following are the key goals of this study :

- To provide a crime reporting system that is secured, transparent, and immutable.
- Ensuring anonymity to encourage more individuals to participate in crime reporting.
- Different blockchain-based platforms should collaborate with each other for sharing information and documents by following some set of guidelines.
- The overall performance of the blockchain networks must not get affected.

II. Background Study

A. Hyperledger Fabric

Hyperledger Fabric is a robust and scalable enterprise blockchain platform that uses a modular architecture to provide flexibility and customizability to users. Fabric is designed to support distributed networks with multiple organizations and can execute smart contracts. It uses a permissioned network model, which ensures that only authorized users can access the network [13]. Fabric supports multiple consensus protocols, including Byzantine Fault Tolerance, and also provides privacy features through the use of channels and PDC. Additionally, Fabric offers rich identity management capabilities through its Membership Service Provider architecture. It also supports a variety of consensus protocols, including Kafka, PBFT, and Raft, and allows for the use of different programming languages for writing smart contracts.

B. Hyperledger Fabric Private Data Collection (PDC)

Hyperledger Fabric's private data collection enables the private and secure administration and storage of sensitive data. As only authorized network users can see this data, it is prevented from being disclosed to unauthorized parties. With Hyperledger Fabric, private data gathering is carried out utilizing a separate private data store that is only accessible to approved network users. For businesses that must keep private information hidden from others in one channel, the private data collection (PDC) method is suggested. All peers in a channel store the PDC hash [14].

C. Hyperledger Cacti

The Hyperledger community of the Linux Foundation has created the open-source Hyperledger Cacti project, which intends to offer a foundation for creating interoperable blockchain networks. It offers a pluggable architecture for integrating various blockchain networks, making it possible for data to be transferred across them without any problems. By offering a framework for developing cross-chain apps and services, Hyperledger Cacti seeks to address the issue of fragmentation in the blockchain industry. It also supports several blockchain networks, including Hyperledger Fabric, Ethereum, and Corda and it provides a powerful and flexible platform for building interoperable blockchain networks [12].

III. Literature Review

In recent years, there are a few teams who worked on blockchain-based crime report management systems, criminal record management, securing FIR data and forensic evidence, etc. We were able to find some works connected to our field during our study. Such examples are as follows :

Ishwarlal et. al [5] developed a Public Ethereum blockchain-based system to manage police complaints. The evidence provided by users will be stored on a IPFS network. Specifically, the FIR filed by the police will be encrypted, and stored in the IPFS and a hash is added to the blockchain network.

In [6] Huaqun Wang et. al proposed a blockchain-based anonymous reporting and rewarding scheme for the first time using Bitcoin and Monero blockchains to tackle the problem of punishing criminals while protecting whistleblowers. Here, elliptic curve public key cryptography has been used.

Binyamin et. al [7] proposed a web-based interoperable crime management system that accepts input using an API. To implement the proposed idea, they used Laravel and to store case and criminal details they used PostgreSQL.

Sandamali et. al [8] developed an application to report any crimes anonymously which has been developed using React-Native, the web application has been developed using React-Js and REST API has been developed using Node-Js.

Nasir et. al [9] proposes a blockchain-based solution for addressing data integrity and false registration in e-FIR. This solution uses Ethereum and a smart contract-based framework.

The authors in [11] proposed a blockchain-based smart policing system that allows the collaboration between stakeholders of that system. They claimed that this is the first proposal on a blockchain-based crime reporting system that is built up by using Hyperledger Fabric and smart contracts.

Vikas et. al [15] proposed a Consortium blockchain architecture for the Indian police. In this system, the clients can register their FIR using a decentralized application.

In [16] Sonali Patil et. al developed a blockchain-based system for maintaining the reliability of digital forensic evidence. The system is implemented on the Ethereum platform and enhances the security of forensic evidence through immutability.

Limitations:

- Different agencies which are involved in law enforcement use different systems that are not compatible with each other, making it difficult to share information. An interoperable crime management system can eliminate these barriers by providing a shared platform for all. But the proposed systems don't offer interoperability [11] [15].
- A web 3.0 based application would be preferable for the implementation of such a project [7].
- Storing the evidence and reports on a public IPFS network will require a lot of resources [5].
- For the implementation of such a large-scale project, a permission-based blockchain would be vastly preferable [6] [9] [16].

- The developed application is limited to the Android platform only [8].

IV. Methodology

To report a crime, users must sign in or register and select either General or Anonymous mode. General mode sends notifications for updates while Anonymous mode does not. Then the police initiate the investigation. Along with each new crime report, a channel and a PDC are created to store the information. The police may send the evidence to the forensic department for a forensic test and the forensic department will send back the report after completing tests and analysis. In the process of solving the case, collaboration with other investigation agencies may be required, which includes sharing certain resources. If the charge is against an international criminal then the police can collaborate with the police network of their foreign allies. At any point in the investigation, the police may need to submit the investigation report to the court. As different institutions may have different blockchain technologies, they will interact and share resources with each other using Hyperledger Cacti.

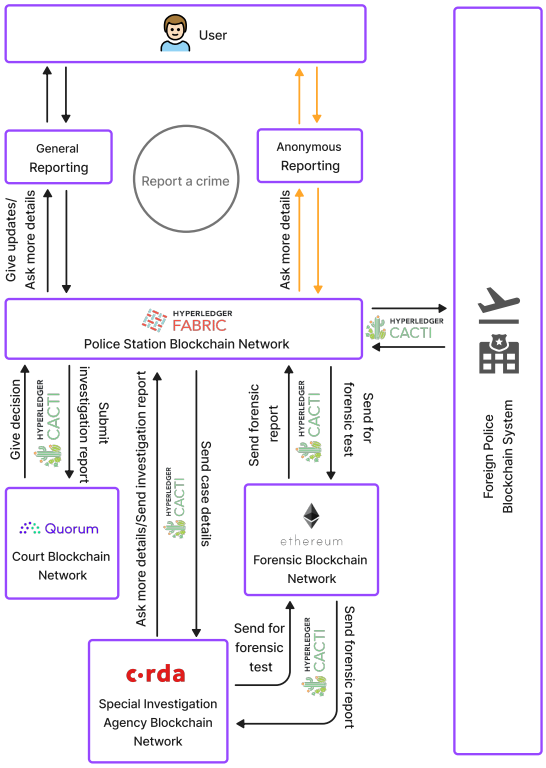


Fig. 1. Proposed system

A. Crime Reporting

First of all, the user logs in to the system, select a mode and reports about a crime. For each report, a channel and a PDC are created. Figure 2 provides a visual representation of this process.

Then if the reporting mode is General then an FIR is automatically created which is described in **Algorithm 1**. **Algorithm 1** allows users to report crimes by creating a new CrimeReport object with a description (C_m) and mode (C_d). It then creates a channel (ch_r) for the report and adds the user (User) who created the report to the channel. The algorithm also creates a PDC object (PDC_r) and adds the report to it. If the mode of the report is "General", the function creates an FIR object and adds it to the PDC object. The algorithm updates the status of the FIR and the CrimeReport object accordingly.

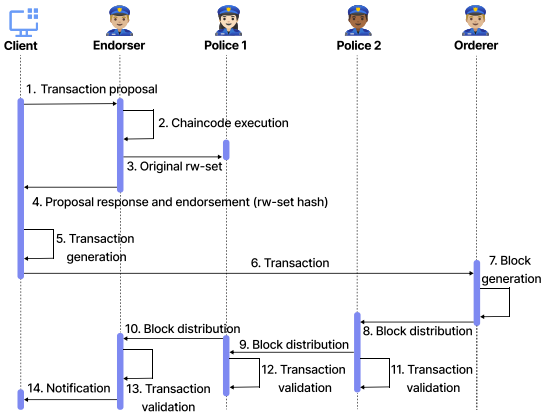


Fig. 2. Sequence diagram of transactions workflow in Unified Modeling Language (UML). where peer1, peer2 and peer3 are PDC members. The rw-set denotes the read/write set.

Algorithm 1 Report a crime

function CreateNewReport(C_d, C_m)
  $T_e \leftarrow Transaction\ initiator$
  Require that T_e is a User
  $r \leftarrow new\ CrimeReport(C_d, C_m)$
  $ch_r \leftarrow new\ channel(r)$
  $ch_r.addUser(User)$
  $PDC_r \leftarrow new\ PDC()$
  $PDC_r.addReport(r)$
  if $mode == General$ **then**
    $FIR \leftarrow new\ FIR(C_d, userDetails)$
    $PDC_r.addFIR(FIR)$
    $status \leftarrow FIR\ is\ recorded$
    $r.updateStatus(status)$
  end if
  return true
end function

After creating an FIR the officer-in-charge of the police station will initiate the investigation by assigning a team leader, which is described in **Algorithm 2**.

The **Algorithm 2** describes the process of initiating an investigation for a crime report with a given ID (ID_r). The transaction initiator is required to be the officer-in-charge. The algorithm checks the status of the report and assigns a team leader if the report's status is "FIR is recorded". The team leader's ID is added to the relevant PDC and channel, and the status of the report is updated to "Investigation Initiated". Then the investigation is done following the process of **Algorithm 3**.

Algorithm 2 Initiate Investigation

function INITIATEINVESTIGATION(ID_r)
  $T_e \leftarrow Transaction\ initiator$
  Require that T_e is an Officer in charge
  $r \leftarrow FindReportByID(ID_r)$
  $status \leftarrow r.status$
  if $status == FIR\ is\ recorded$ **then**
    $r.PDC_r.TeamLeader(ID_{tl})$
    $r.channel.addTeamLeader(ID_{tl})$
    $r.aassignTeamLeader(ID_{tl})$
    $status \leftarrow Investigation\ Initiated$
    $r.updateStatus(status)$
  end if
  return true
end function

Algorithm 3 Investigate

function INVESTIGATE(r)
  $T_e \leftarrow Transaction\ initiator$
  Require that T_e is the Team Leader
  $user \leftarrow r.reporter()$
  if $More\ information\ is\ required$ **then**
    $Q \leftarrow newMessage(r.id)$
    $r.AskForMoreInformation(user, Q)$
  end if
  if $Any\ update$ **then**
    $r.GiveUpdates(user, Update)$
  end if
  if $Any\ additional\ report\ is\ required$ **then**
    $assignTask(ID_i, Type)$
      $key \leftarrow keygen()$
      $r.PDC[Type][key] = newPDC()$
      $r.PDC[Type][key].addUser(ID_i)$
      $r.PDC_r.addUser(ID_i)$
  end if
  return true
end function

The **Algorithm 3** describes the steps involved in investigating a crime report. The transaction initiator is required to be the team leader. If any further information is required from the user, the team leader finds the user and asks for the required information (Q). If it is required to provide any updates to the user, the team leader finds the user and gives updates ($Update$). If any additional report is required, then the team leader will assign the task to an investigator (ID_i) and also inform which type of task it is ($Type$). Later, The User ID is added to the relevant PDC and channel.

To collaborate with other institutes like forensics, SIA, or foreign police, the investigator sends a collaboration request like **Algorithm 4**

The **Algorithm 4** takes the receiver Cacti instance's address ($Address_r$), the sender Cacti instance's address ($Address_s$), and the collaboration request object ($request$) which to be sent. It also takes the report type ($Type$) and a key that refers

Algorithm 4 Send Cacti Collaboration Request

function SENDCOLLABREQUEST($Address_r$, $Address_s$, ID_r, $request$, $type$, key)
  $T_e \leftarrow Transaction\ initiator$
  Require that T_e is an Investigator
  $conn \leftarrow$ createConnection($Address_r$)
  if $conn$ is not null **then**
    $t \leftarrow tokenGen(ID_r, type, key)$
    $message \leftarrow$ newMessage($Address_s$, $request$, t)
    conn.send($message$)
    conn.close()
    $status \leftarrow$ Request processing $type : Address_s$
    $r.updateStatus(status)$
    return true
  else
    return false
  end if
end function

to the PDC index (key). The transaction initiator is required to be the investigator. Next, it establishes a connection between the sender's address and the receiver's address. If a connection is possible, a token is generated and a message will be sent. The function returns true and the status of the connection is updated to "Request Processing".

Algorithm 5 Receive report

function RECEIVEREPORT($response$)
  $T_e \leftarrow Transaction\ initiator$
  Require that T_e is a Investigator
  $d \leftarrow FindDetailsByToken(response.token)$
  $r \leftarrow FindReportByID(d.ID_r)$.
  $key \leftarrow d.key$
  $type \leftarrow d.type$
  $r.PDC[type][key].update(response.data)$
  if $More\ information\ required$ **then**
    sendCollabRequest($response.Address_r$, $response.Address_s$,$r.id$ $request$, $type$, key)
  else
    $notifyUpdate(token)$
  end if
end function

Then any point in time, the investigator may need the reports from forensics, SIA, or foreign police, then he/she has to receive reports as **Algorithm 5**.

The **Algorithm 5** takes input as a report from any department ($response$). An investigator initiates the transaction and identifies the key and type of the report. If further information is needed, the investigator will send a collaboration request. Otherwise, they will notify the team leader of the update.

In order to re-investigate or close the investigation, the team leader will receive the investigation report and complete the required task as **Algorithm 6**

The **Algorithm 6** takes the investigation report as input ($response$). The transaction initiator is the team leader and

Algorithm 6 Update investigate Report

function INVESTIGATE($response$)
  $T_e \leftarrow Transaction\ initiator$
  Require that T_e is the Team Leader
  $d \leftarrow FindDetailsByToken(response.token)$
  $r \leftarrow FindReportByID(d.ID_r)$.
  $key \leftarrow d.key$
  $type \leftarrow d.type$
  $user \leftarrow r.reporter()$
  if $More\ information\ is\ required$ **then**
    $r.AskForMoreInformation(user, Q)$
  end if
  if $Any\ update$ **then**
    $r.GiveUpdates(user, Update)$
  end if
  if $Any\ report\ update\ is\ required$ **then**
    $message \leftarrow newMessage(token)$
    $ReInvestigate(token, message)$
  else
    $r.closeInvestivation(r, key)$
  end if
  return true
end function

he/she identifies the key and type of the report. If any further information is required from the user, the team leader finds the user and asks for the required information (Q). If it is required to provide any updates to the user, the team leader finds the user and gives updates ($Update$). Next, if any report update is required, the team leader will send the report to the investigating officer for re-investigation, otherwise close the investigation.

B. Collaboration

1) Forensic : If any forensic tests are required then the police or other investigation agency send the report and evidence for forensic tests using Hyperledger Cacti. The forensic department creates a report after completing tests and sends it to the police or other investigation agency using Hyperledger Cacti.

2) Court : If there is a judicial proceeding then the police need to submit the investigation report or other documents to the court. The police need to use Hyperledger Cacti to send the documents.

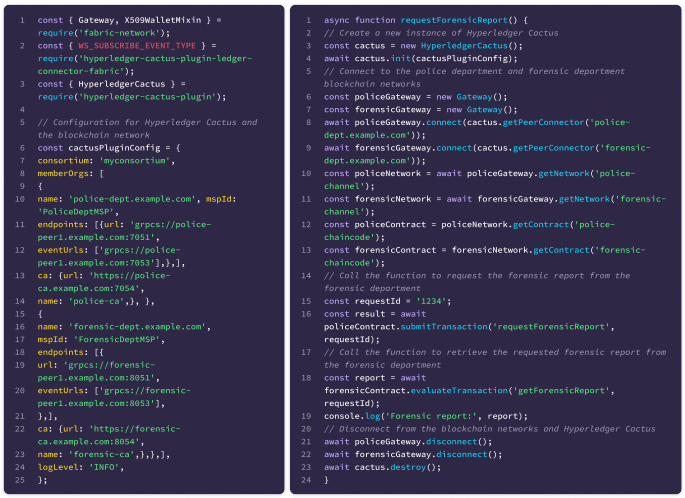
3) Special Investigation Agency : The police department may need the help of special investigation agencies. To collaborate with them, the team leader will need permission from the higher authority and request collaboration using Hyperledger Cacti.

4) Foreign Police : In some cases, the offender flees to a foreign country. In this scenario, the police will have to collaborate with the police department of that country so that they can share resources and updates. As the foreign police will have different blockchain technology, the interactions will take place using Hyperledger Cacti.

V. IMPLEMENTATION RESULT ANALYSIS

To implement a the prototype, the system is built on Hyperledger Fabric. The system's background service layer is built with the Nodejs SDK, and the front-end user interface built with ReactJS. We also used CouchDB as the database in this case.

Figure 3 is a program where Hyperledger Cacti is used which reflects how the police send requests (policeContract.submitTransaction) to the forensics department and receive the forensic reports (forensicContract.evaluateTransaction). This is done in the function "requestForensicReport". Other collaborations like collaborations with special investigations agencies, courts, and others will be done using Hyperledger Cacti.



```
const { Gateway, X509WalletMixin } =
require('fabric-network');
const { WS_SUBSCRIBE_EVENT_TYPE } =
require('hyperledger-cactus-plugin-ledger-
connector-fabric');
const { HyperledgerCactus } =
require('hyperledger-cactus-plugin');

// Configuration for Hyperledger Cactus and
the blockchain network
const cactusPluginConfig = {
consortium: 'myconsortium',
memberOrgs: [
{
name: 'police-dept.example.com', mspId:
'PoliceDeptMSP',
endpoints: [{url: 'grpcs://police-
peer1.example.com:7051',
eventUrls: ['grpcs://police-
peer1.example.com:7053'],},],
ca: {url: 'https://police-
ca.example.com:7054',
name: 'police-ca',}, },
{
name: 'forensic-dept.example.com',
mspId: 'ForensicDeptMSP',
endpoints: [{
url: 'grpcs://forensic-
peer1.example.com:8051',
eventUrls: ['grpcs://forensic-
peer1.example.com:8053'],
},],
ca: {url: 'https://forensic-
ca.example.com:8054',
name: 'forensic-ca',},},],
logLevel: 'INFO',
};
```

```
async function requestForensicReport() {
// Create a new instance of Hyperledger Coctus
const cactus = new HyperledgerCactus();
await cactus.init(cactusPluginConfig);
// Connect to the police department and forensic department
blockchain networks
const policeGateway = new Gateway();
const forensicGateway = new Gateway();
await policeGateway.connect(cactus.getPeerConnector('police-
dept.example.com'));
await forensicGateway.connect(cactus.getPeerConnector('forensic-
dept.example.com'));
const policeNetwork = await policeGateway.getNetwork('police-
channel');
const forensicNetwork = await forensicGateway.getNetwork('forensic-
channel');
const policeContract = policeNetwork.getContract('police-
chaincode');
const forensicContract = forensicNetwork.getContract('forensic-
chaincode');
// Call the function to request the forensic report from the
forensic department
const requestId = '1234';
const result = await
policeContract.submitTransaction('requestForensicReport',
requestId);
// Call the function to retrieve the requested forensic report from
the forensic department
const report = await
forensicContract.evaluateTransaction('getForensicReport',
requestId);
console.log('Forensic report:', report);
// Disconnect from the blockchain networks and Hyperledger Coctus
await policeGateway.disconnect();
await forensicGateway.disconnect();
await cactus.destroy();
}
```

Fig. 3. Interaction using hyperledger CactI (Police - Forensics Department)

Figure 4 shows the user reporting interface. The user will see a form including the reporting mode, subject, description, and a file uploader so that he/she can attach documents or pictures to add more details of the crime. The user can see his/her previous history and the updates of those reports.

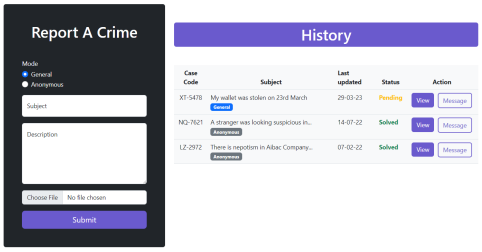


Fig. 4. User Reporting Interface

Figure 5 shows the investigator's dashboard. The investigator of a case can log in to his/her account and see the progress and updates of the case. Also, he/she will see some buttons to send the report to the forensic department or special investigation agencies, to collaborate with special investigation agencies or foreign police departments, and to contact the reporter if further details are required.

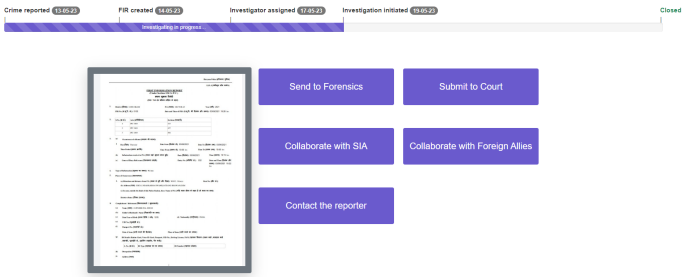


Fig. 5. Investigator's Dashboard

The performance of blockchains B1(Police) and B2(Forensic) was evaluated in different scenarios to observe changes in throughput and latency with varying transaction numbers. Inter-blockchain communication was also tested to determine average latency for query transactions between B1 and B2. Tests were run ten times and averaged using Hyperledger Caliper , an open-source benchmarking tool for blockchain network performance measurement. B1 and B2 are both Hyperledger Fabric networks.

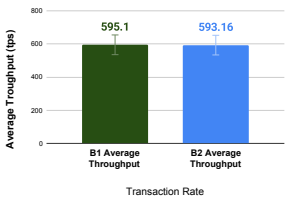


Fig. 6. Average throughput (tps)

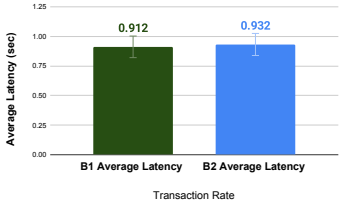


Fig. 7. Average latency (sec)

During a stable transaction load of 600, the peak performance of blockchains B1 and B2 were measured and averaged over ten rounds. B1 and B2 test networks achieved throughputs of 595.10 and 593.16 tps which is shown on **Figure 6**, and **Figure 7** shows the low latencies of 0.912 and 0.932 seconds. No failed transactions were recorded due to minimal CPU utilization. new request to the consortium (as in B2) resulted in a minor decrease in network performance, with B2 exhibiting a slightly higher latency of 0.049 s and a difference of 1.88 tps throughput compared to B1.

Interoperable operations between two independent Hyperledger Fabric blockchains (B1 and B2) were tested, where a client application on B1 sent a report request to B2. Hyperledger Cactai was utilized for the integration of the developed blockchains.In our case, the latency for inter-blockchain transactions was measured to be 1.102 s. This latency is influenced by the performance of the connected blockchains as well as the methodology used for the connection.

VI. Conclusion Future Work

The proposed system provides a solution to the challenge of bringing criminals to justice. This research has presented a blockchain-based interoperable crime management system using Hyperledger Cacti and private data collection that provides secure and decentralized communication between different blockchain-based platforms, allowing different agencies to share information more easily and collaborate more effectively. This system is more transparent and immutable and provides anonymity to encourage more individuals to participate in crime reporting. Here, Hyperledger Cacti implements interoperability, which enhances the overall performance of blockchain networks. The indicated proposed system will aid in reducing the crime rate, making communities safer and more secure, and contributing to economic growth and development.

To improve the stated system, integrating the machine learning algorithms will be a novel approach for predicting and preventing criminal activities, using AI to identify criminals and track their movements, and enhancing collaboration between investigation agencies with secure multi-party computation protocols.

References

[1] G. Lamond, "What is a crime?," *Oxford Journal of Legal Studies*, vol. 27, 2007.

[2] D. H. Tanvir, R. Amin, A. Islam, M. S. Islam, and M. M. Rashid, "Blockchain interoperability for a reputation-based drug supply chain management," in *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, pp. 1–6, March 2023.

[3] R. Amin, A. Islam, D. H. Tanvir, and R. I. Arif, "Hirex: A heterogeneous interoperable blockchain solution for hiring system," *2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, pp. 1–7, 1 2023.

[4] R. B. Freeman, "Chapter 52 the economics of crime," *Handbook of Labor Economics*, vol. 3 PART, pp. 3529–3571, 1999.

[5] I. Hingorani, R. Khara, D. Pomendkar, and N. Raul, "Police complaint management system using blockchain technology," *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, pp. 1214–1219, 12 2020.

[6] H. Wang, D. He, Z. Liu, and R. Guo, "Blockchain-based anonymous reporting scheme with anonymous rewarding," *IEEE Transactions on Engineering Management*, vol. 67, pp. 1514–1524, 11 2020.

[7] B. A. Ajayi, J. Nweke, and M. U. Ogah, "Developing an interoperable crime management system," *Proceedings of the 5th International Conference on Information Technology for Education and Development: Changing the Narratives Through Building a Secure Society with Disruptive Technologies, ITED 2022*, 2022.

[8] R. SANDAMALI, "Mobile based crime reporting app," 8 2021.

[9] N. D. Khan, C. Chrysostomou, and B. Nazir, "Smart fir: Securing e-fir data through blockchain within smart cities," *IEEE Vehicular Technology Conference*, vol. 2020-May, 5 2020.

[10] N. Iftekhar, S. Bin-Faisal, and D. Nandi, "Implementation of blockchain for secured criminal records," *ACM International Conference Proceeding Series*, pp. 220–226, 3 2022.

[11] A. Mukherjee and R. Halder, "Policechain: Blockchain-based smart policing system for smart cities," *ACM International Conference Proceeding Series*, 11 2020.

[12] "Introducing hyperledger cacti, a multi-faceted pluggable interoperability framework – hyperledger foundation."

[13] R. Amin, M. S. Islam, R. I. Arif, A. Islam, and M. M. Hossain, "Blockchain-based integrated application for forged elimination of hiring system using hyperledger fabric 2.x," in *2022 25th International Conference on Computer and Information Technology (ICCIT)*, pp. 1057–1062, Dec 2022.

[14] S. Wang, M. Yang, Y. Zhang, Y. Luo, T. Ge, X. Fu, and W. Zhao, "On private data collection of hyperledger fabric," *Proceedings - International Conference on Distributed Computing Systems*, vol. 2021-July, pp. 819–829, 7 2021.

[15] V. Hassija, A. Patel, and V. Chamola, "Police fir registration and tracking using consortium blockchain," pp. 785–794, 2021.

[16] S. Patil, S. Kadam, and J. Katti, "Security enhancement of forensic evidences using blockchain," *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, pp. 263–268, 2 2021.