Security of Police Case Database using Blockchain.pdf

By Security of Police Case Database using Blockchain

WORD COUNT 6834

TIME SUBMITTED 02-SEP-2022 10:34AM

PAPER ID 90104992

Ensuring Security of Police Case Database using Blockchain Technology with the Help of Smart Contact

Shirmin Ahmed Labonno and Afroza Akter

A Thesis in the Partial Fulfillment of the Requirements

for the Award of Bachelor of Computer Science and Engineering (BCSE)

Department of Computer Science and Engineering

College of Engineering and Technology

IUBAT – International University of Business Agriculture and Technology

Spring 2022

Ensuring Security of Police Case Database using Blockchain Technology with the Help of Smart Contact

Shirmin Ahmed Labonno and Afroza Akter

A Thesis in the Partial Fulfillment of the Requirements for the Award of Bachelor of Computer Science and Engineering (BCSE)

The thesis has been examined and approved,

____

Prof. Dr. Utpal Kanti Das

Chairman and Professor

____

Dr. Muhammad Hasibur Rashid Chayon

Co-supervisor, Coordinator and Associate Professor

____

M.M.Rakibul Hasan

Senior Lecturer,

CSE Department, IUBAT

Department of Computer Science and Engineering

College of Engineering and Technology

IUBAT – International University of Business Agriculture and Technology

Letter of Transmittal

1 September 2022
The Chairman
Thesis Defense Committee
Department of Computer Science and Engineering
IUBAT–International University of Business Agriculture and Technology
4 Embankment Drive Road, Sector 10, Uttara Model Town
Dhaka 1230, Bangladesh

Subject: Letter of Transmittal.

Dear Sir,

It gives me enormous pleasure to work on “Ensuring Security of Police Case Database using Blockchain Technology with the Help of Smart Contact” as per instructions. I expect this research work to be informative as well as comprehensive.

While conducting the thesis paper I have gathered lots of knowledge about the securing Police case database system . I have tried my level best to collect the relative information as comprehensively as possible in preparing the thesis. During preparation of the research paper, I have experienced a lot that will help me greatly in my career. I will be able to explain anything for clarification if necessary.

I would like to thank you for giving me the opportunity to do a research work on the above mention topic.

Yours sincerely,

______________	______________
Shirmin Ahmed Labonno	Afroza Akter
18303048	18303055
BCSE	BCSE

Student’s Declaration

I hereby declare that this thesis is based on results obtained from my own work. All the materials that were used for the purpose of completing this thesis are acknowledged and mentioned in the reference. This thesis. Neither in whole nor in part, has been previously submitted to any other University or Institute for the award of any degree or diploma. We carried out our research under the supervision of M.M.Rakibul Hasan.

_____________	_____________
Shirmin Ahmed Labonno	Afroza Akter
18303048	18303055
BCSE	BCSE

Supervisor's Certification

The supervisor‟s certification of your thesis report is going to be added here. Keep the format as it is.

____

M.M.Rakibul Hasan

Senior Lecturer

Department of Computer Science and Engineering

IUBAT–International University of Business Agriculture and Technology

Abstract

A police case database system stores very confidential data of every individual crimincaldatas.In every case custody these criminal information goes through a different hands on the process of solving the case & investigation .But the existing system of the police case data is not that much secure right now. Each and every police station has a system to store the criminal records but that's not maintaining the transparency of the data transaction. Many of the police stations are still running on manual systems. A criminal's data is very confidential. If any dishonest act happened it could make injustice to the victims as well. As it is secure that much so it can be easily hacked .So. We are proposing a secure platform that offers the accuracy and privacy of current police case schemes, while providing the transparency and flexibility offered by smart contract based systems has been a challenge for a long time. In this draft article, we assess a blockchain service application to construct a distributed smart contract-based police case database. In order to ensure the security of the police case database using blockchain technology with the aid of smart contracts, the paper suggests a secure police case database based on blockchain that addresses some of the shortcomings in existing systems and evaluates some of the well-known blockchain frameworks.We are building the smart contract on Go Ethereum platform of blockchain with POA consensus algorithm for verifying the user and give a transparency of securing criminal records and evidence.Our proposed system is based on private blockchain but in a distributed network for the maximum security of the transection of data.We analyze the potential of distributed ledger technology in particular by describing a case study, focusing on the security process and the use of a blockchain-based system to enhance security and decrease the time and space of managing a manual system.

Acknowledgements

In the name of Almighty Allah who is the most merciful and most graceful. We would like to thank the late Professor Dr.Md. Alimullah Miyan,Vice-chancellor of IUBAT- International University of Business Agriculture & Technology gave us permission to study in this university which is the most beautiful and renowned, the first non –government university in this country.

We would like to thank and convey the respect to our present honorable vice chancellor Professor Dr.Abdur Rab, IUBAT- International University of BusinessAgriculture & Technology .

We would like to give gratitude toProf. Dr. Utpal Kanti Das , chairman of Department of computer science and Engineering, IUBAT-International University of Business Agriculture & Technology, gave permission to study in the Department of Computer science & Engineering and allow us to see the bright future in the technological field of the new era.

We are very appreciative to Dr. Muhammad Hasibur Rashid Chayon ,respected co-ordinator and professor,Department of computer science & Engineering, IUBAT- International University of Business Agriculture & Technology, for his better direction and sustain throughout the semester.

We are really pleased and proud to express our feeling of gratefulness and profound respect to our respected faculty, M.M.Rakibul Hasan, Senior Lecturer, Department of computer science & Engineering,IUBAT for his scholastic guidance,helpful and untiring efforts to execute our research work..

Finally we would like to thank our parents and our teachers who have been a great source of inspiration to us.

Table of Contents

Letter of Transmittal iii

Student's Declaration IV

Supervisor's Certification V

Abstract VI

Acknowledgements ....……………………………..…VII

Chapter I: Introduction 10

1.1. Introduction 10

1.2.Rational of the study……………………………………………………………………..13

1.3 Problem Statement ………………………..……………………………………...……14

1.4 Objective……………………………………………………………………………….15

Chapter II: Literature Review 16

Chapter III: Research Methodology 21

Chapter IV:Result and Discussion...32

Chapter V:Conclusion.. 35

5.1 Conlusion………………………………………………………………………....34

5.2 Limitations Research work…………………………………………………..….35

5.3 Future work of research work….………………………………………………..…35

References..24

Table Of Figures

Figure 1: Proof of Authority flow chart…………………………………………….24

Figure 2: An overview of proposed system……………………………………….25

Figure 3: Plan of work………………………………………………………………26

Figure 4: Process of securing police case database as smart contract………………..30

Chapter I: Introduction

1.1 Introduction

Securing a police case database management system which could help police officers to find out the criminal records easily and make the data transaction more reliable and maintain the tarnsperency of data transection as well.Criminal evidence paly a vital roles on the criminal investigation.Guaranteeing the integrity, authenticity, and audit of criminal evidence as it progresses through various layers of from the first responder to higher authority responsible for conducting investigations on criminal investigation.Every Police station is under getting on digitilizaton so all the criminal record are storing on the system. But in this process its not secure enough and donot maintain the transparency of data transection is happened on the system.Its only required a log in password to enter the system as it is a confidential matter it should taken under a proper security .As the criminal evidence is the major part of police case investigation. So, we are providing a security to our police to maintain the honesty and transparency of the investigation process and do justice to the victim.

We are willing to help our police because the management system of the police isn't quite well furnished and secured .We tried to help police to secure their current data base with the help of blockchain technology and controlling the easy accessible system make it more confidential with popper two step verifaction with the help of smart contract which will be written on the blockchain technology.The capacity of blockchain technology to sectionalize thorough reads of transactions back to origins holds enormous promise for the rhetorical community. In essence, it is a distributed information system that upholds a continuously expanding tamper-proof arrangement of blocks that include batches of individual transactions. Originally developed for the Bitcoin money, it implements a decentralized fully replicated append-only ledger in a peer-to-peer network. Every node that takes part keeps a complete local copy of the blockchain. The blockchain is made up of a series of blocks that each contain a single ledger transaction. The order of transactions within blocks is chronological, and each block includes a cryptographic hash of the block before it in the chain.A timestamp and data link pointing to an earlier block are included in every Blockchain. The ledger, cryptography, consensus, and business logic are the four aspects of blockchain that are duplicated. A initiative of the Linux Foundation, The Hyperledger is an open-source cooperative effort aimed to improve Blockchain technologies used across industries.

Blockchain is a decentralized, unchangeable, and transparent public ledger. Three key characteristics of this new technology include:

(i) **Immutability:**Any proposed “new block” to the ledger must reference the past adaptation of the ledger. This makes a permanent chain, which is where the blockchain gets its title from, and anticipates tampering with the judgment of the past passages.

(ii) **Verifiability**:The record is decentralized, duplicated and distributed over numerous areas. This guarantees high availability (by disposing of a single point of disappointment) and provides third-party unquestionable status as all hubs keep up the consensus adaptation of the record.

(iii) **Distributed Consensus**:A conveyed agreement protocol to decide who can add the following unused exchange to the record. A larger part of the arranged hubs must reach an agreement some time recently any modern proposed piece of entries becomes a changeless portion of the record.

These options are partially achieved through advanced cryp-tography, providing a security level bigger than any previously famous record-keeping system. Blockchain technology is thought of by several , as well as to have a substantial potential as a tool for implementing a replacement secured database.

This paper evaluates the use of blockchain as a service to implement a secure police case database management system. The paper makes the following original contributions: (i) propose a blockchain-based database system that uses "permissioned blockchain", and (ii) review of existing blockchain frameworks suited for constructing blockchain-based policecase database system. So we are implementing the smart contract on Ethereum blockchain where it will distributed to all the district nood from the boot node every police station under the network will called as district node.Admin will set up smart contract on each police station.And selected officer can enternd on the system with 2 step verifications from bootnode and the district node with the unique id and transaction id will be stored in both bootnode as well as on the new block or hash.

Our proposed system is based on a private blockchain network.Blockchain technology is used to design and develop a model with advanced features for reducing forgery in police cases.Smart contracts are programs where all the terms & conditions are specified and execute on Ethereum blockchain.Smart contracts have been proposed to improve evidence preservation for ensuring security,validity,integrity and transparency of the data. We are using PoA consensus algorithm for that purpose.The proposed work is less expensive than other current ideas in terms of time involved in its implementation,

1.2 Rational of Study

The existing police case database management system that claims to manage police casesand store the data.But the present system is not secure enough that can fully prevent unauthorized access or hacking as well as secure data transaction from one police station to another one.But the system is not providing proper security and also all the system is not interconnected if the criminal change the location they may have to deliver the information one to another location but it not secure enough right now.

To solve this problem ensure the securty of the criminal evidence as well as polic Case database we are introducing a Blockchain based police case management system with Smart contract. That will Ensure the security, integrity of the police cases and fully automated system.

1.3 Problem statement

Existing systems claim to handle huge data records of police cases but not providing enough security . It's very easy to break down the system as it is not highly secure. But a police case data is essential both for the case of custody and proper investigation. Managing any system is easy but providing the high security is harder. So we are willing to solve this problem and our police to handle Thier confidential data transaction with security and transparency.we are introducing a Blockchain based police case database management system with Smart contract to ensure the security, integrity of the evidence and fully automated system.

1.4 Objective

Borad objective

The main objective is to Provide a secure and automated police case management system and Eliminate unauthorized access. We can also ensure the authenticity, integrity of the criminal records.We are using smart contracts based on Ethereum for police case management and set up a Ethereum private Proof-of-Authority (POA) blockchain to achieve these goals

Specific objective

Our specific objective is to implement the Blockchain based system to secure police case records.

- Implementing the PoA network as boot node of the system
- Set up smart contract as set of program in Blockchain at every police station which will define as district node
- Implementing blocks or hash which will store the transaction id.
- System will allow a method of secure authentication via an identity verification service.
- System will provide transparency of data transaction in the form of verify able assurance to the each officer without risking their privacy.
- System will prevent any third party to do tampering with any evidence.
- System will allow only eligible authority to enter the system.

Chapter II: Literature Review

2.1 Literature Review

Paper-1: Title: Blockchain-Based E-Voting System

Author's name: Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson

Published in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)

It has long been difficult to create a safe electronic voting system that provides the transparency and flexibility provided by electronic systems, while maintaining the fairness and privacy of present voting schemes. In this draft article, we assess a blockchain application for implementing distributed electronic voting systems. The study offers a novel blockchain-based electronic voting system that tackles some of the drawbacks of current systems and assesses some of the well-known blockchain frameworks in order to build a blockchain-based e-voting system.Through the explanation of a case study, namely the election process and the deployment of a blockchain-based application, which increases security and lowers the cost of hosting a national election, we specifically assess the potential of distributed ledger technology.

Paper-2: Title: A Blockchain-based Process Provenance for Cloud Forensics

Author's name: Yong Zhang, Songyang Wu*, Bo Jin, Jiaying Du

Published in 2017 3rd IEEE International Conference on Computer and Communications (ICCC)

The dispersed nature of cloud computing allows for the storage and processing of data across jurisdictional boundaries. In this situation, cloud computing digital evidence collection calls for multiparty cooperation. To our knowledge, there is currently no technical solution for enhancing the reliability of the interaction records of all parties in cloud forensics. This paper presented a process provenance that uses blockchain and cryptography group signature technologies to give proof of existence and privacy preservation for process records. The chain of custody's credibility is improved by the process provenance for cloud forensics..

Paper-3: Title: Crypto-voting, a Blockchain based e-Voting System

Author's name: Francesco Fusco1 , Maria Ilaria Lunesu2 , Filippo Eros Pani2 and Andrea Pinna2

Published in 2018 10th International Conference on Knowledge Management and Information Sharing

Vote confidentiality is required in the majority of electoral situations. This restriction is not required during the collection of signatures because those signatures are already available to the public. This stage comes before things like the electoral roll composition or popular initiative referendums, for example. Many electronic voting systems (also known as e-voting systems) have failed in the past due to their inability to ensure complete security with regard to the preservation of voter privacy, particularly over the long- to medium-term and in the face of brute force attacks. This study's goal is to introduce and define Crypto-voting, a novel electronic voting mechanism. This system is based on the blockchain-enabled secret sharing strategy developed by Shamir. Using this technology, we can seamlessly handle all of the stages and events that make up an election. These activities include the system setup, the handing out of credentials, the voting, the gathering of ballots, the tally of preferences, the posting of results, and so forth. Additionally, our technology seeks to provide direct audit and traceability mechanisms for voting activities.

Paper-4: Title: Decentralizing Privacy: Using Blockchain to Protect Personal Data

Author's name: Guy Zyskind; Oz Nathan; Alex 'Sandy' Pentland

Published in 2015 IEEE Security and Privacy Workshops

The recent increase in reported incidents of police work and security breaches compromising users` privacy decision into question the present model, during which third-parties collect and management large amounts of private information. Bit coin has incontestible within the money house that trusted, auditable computing is feasible employing a suburbanised network of peers in the midst of a public ledger. during this paper, we have a tendency to describe a decentralized personal data management system that ensures users own and control their data. we have a tendency to implement a protocol that turns a block chain into an automatic access-control manager that doesn't need trust during a third party. in contrast to Bit coin, transactions in our system don't seem to be strictly money -- they're wont to carry instructions, comparable to storing, querying and sharing data. Finally, we have a tendency to discuss potential future extensions to dam chains that might harness them into a all-round resolution for trustworthy computing issues in society.

Paper-5: Title: Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications

Author's name: Gulshan Kumar,Rahul Saha,Chhagan Lal,Mauro Conti

Published in 2021 Elsevier Future Generation Computer Systems

- We suggest a framework for digital forensics investigation that makes use of blockchain for managing digital forensic evidence and IoT as the underlying technology for communication and evidence gathering.
- The architecture makes use of consortium blockchain to maintain a safe chain of custody via the case-chain during the duration of the investigation.
- By utilizing the idea of consortium blockchain, the framework takes the cross-border paradigm for forensic processes into consideration.
- The work's main goal is to find a solution to the issue of investigation transparency in digital evidence forensics.

Chapter III: Research Methodology

We have used several methods to implement our proposed system of securing police case database by blockchain technology with the help of smart contract which has been discussed in this chapter:

1. **Smart contract:**

   Smart contract Is a computer program where all the terms & conditions are specified and store in Blockchain which is decentralized. Mostly used in Ethereum Blockchain.Use solidity to write the program of smart contract.It has no trust issues and is distributed in open distributed ledger.It has no chance of hacking and involvement of third party,automated.Simply, smart contracts are blockchain-based algorithms that execute when certain criteria are met. They are often used to automate the implementation of an agreement so that all parties can be certain of the conclusion right away, without the need for any intermediaries or wasted time.

   A smart contract does not always represent a legally binding agreement. Legal scholars disagree, asserting that smart contracts are merely mechanisms for carrying out responsibilities derived from other contracts, such as liabilities involving the transfer of tokens or cryptocurrencies or obligations involving the automation of payment obligations. Furthermore, according to some academics, the imperative or declarative character of programming languages may have an effect on the legitimacy of smart contracts.

2. Ethereum based Blockchain:

Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts.The Ethereum blockchain is powered by its native cryptocurrency, programmable block chain.Ethereum's blockchain technology makes it possible to establish and maintain openly accessible secure digital ledgers. Although Bitcoin and Ethereum share many characteristics, they have different long-term goals and constraints.

Ethereum is a permissionless, non-hierarchical network of computers (nodes) that constructs and reaches consensus on the blockchain, a continuously expanding collection of "blocks" (bundles of transactions). Each block has a unique identifier for the chain that must come before it in order for it to be regarded as genuine. The ETH balances and other storage values of Ethereum accounts are changed whenever a node adds a block to its chain by carrying out the transactions in the block in the order they are listed. The "state," or collection of these balances and values, is kept on the node independently of the blockchain in a Merkle tree.

Each node's "peers" are a relatively limited subset of the network. Every time a node wants to add a new transaction to the blockchain, it sends copies of the transaction to all of its peers, who then send copies to all of their peers, and so forth. It spreads throughout the network in this way. All of these fresh transactions are kept track of by a group of nodes known as miners, who use them to build new blocks and distribute them to the rest of the network. Every time a node receives a block, it verifies the validity of the block and of each transaction included therein. If the block is found to be valid, it is added to the blockchain and all transactions contained therein are carried out.A node may receive numerous blocks that are vying to succeed a specific block since block generation and broadcasting are permissionless. The node records each valid chain that results from this and routinely discards the shortest one: The Ethereum protocol states that the longest chain is to be taken into consideration at any given time.

3. PoA(Proof of Authority) consensus algorithm:

Proof of Authority (PoA) is a reputation-based consensus algorithm that introduces a practical and efficient solution for blockchain networks (especially the private ones).Based on reputation of the trusted party. Limited number of validators. Select trustworthy identity for verification of transaction.Suitable for private Blockchain network.More scalable.No need of data mining.No need heavy resources.Prevent 51% attack.Transactions and blocks in PoA-based networks are verified by authorized accounts referred to as validators. The software used by validators enables them to group transactions into blocks. Since the procedure is automated, validators are not required to keep an eye on their computers constantly. However, it does necessitate keeping the computer (the authority node) secure. Gavin Wood, a co-founder of Parity Technologies and Ethereum, is credited with coining the phrase.

People with PoA have a motivation to hold onto the position they have attained since they must earn the privilege to be validators. By tying an identity's reputation to it, [9] validators are encouraged to preserve the transaction process [9] since they do not want their identities to be associated with a bad reputation. It is thought that this is more reliable than proof-of-stake (PoS), which, while a stake between two parties may be equal, does not account for each party's entire holdings. As a result, incentives may not be balanced. On the other side, PoA restricts block approval from a single [9] validator to non-consecutive blocks, which means that the authority node is at greater danger of suffering significant harm. PoA is appropriate for distributed trust environments seen in both private and public networks, such as POA Network.

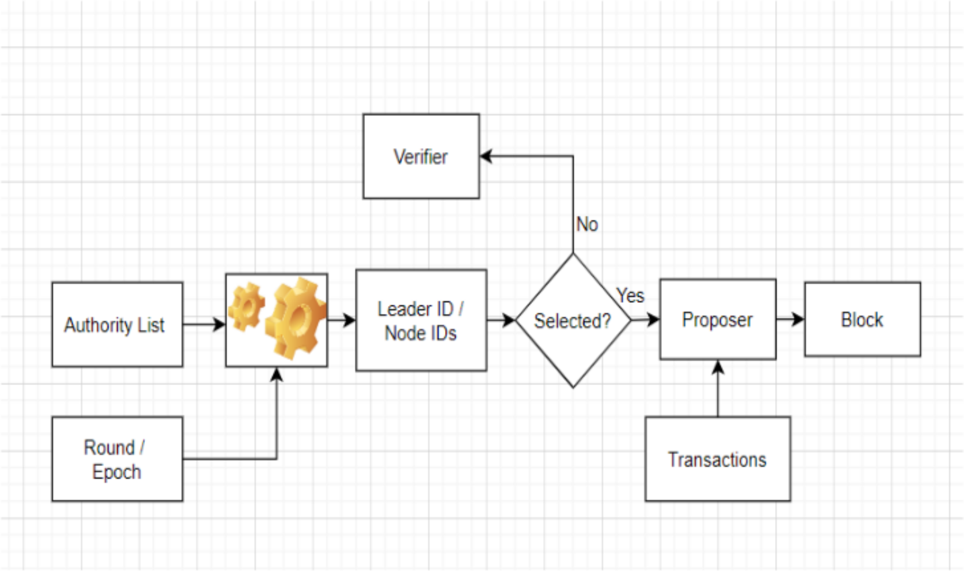

Figure 1 : Proof of Authority Flow chart

Set up of our proposed system:

Police Officers will need to store their police case information in a controlled setting in order to meet the privacy and security standards for storing data and to guarantee that unauthorized access is not permitted by the admin officer. In order to accomplish these objectives, we put up a Go-Ethereum permissioned Proof-of-Authority (POA) blockchain in our work. A consensus technique based on identification as a stake is used by POA to deliver transactions very quickly. In section C, a justification for employing Go-Ethereum for the blockchain infrastructure is given.

The organization of the blockchain, which primarily consists of two different kinds of nodes

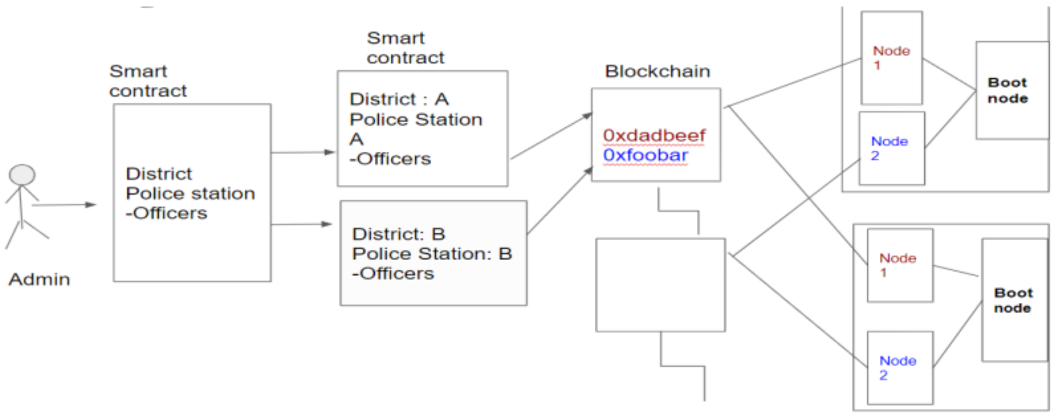

Figure 2 : An overview of proposed system

(i)**District node**: It represents each police station on the district level. There is a software agent on each district node that autonomously communicates with the "boot node" and controls the smart contract life cycle on that node where the police case database system has been set up. A smart contract is disseminated and deployed once police case data stored in the database is created by an administrator (see the smart contracts section).onto the relevant district node. Each of the related district nodes is given access to interact with their corresponding contract when the smart contracts are formed. The police case data is validated by the majority of the associated district nodes when each police officer of the police stations stores data and enters the system from their corresponding smart contract, and each police case data that they concur upon is added to the blockchain

.

(ii) **Bootnode**: Each institution runs a boot node that has authorized access to the network. A boot node is a coordination and discovery service that aids with district node discovery and communication. In order to let district nodes locate their neighbors more quickly, the boot node operates on a static IP and does not maintain any state of the blockchain The next stage is to develop and deploy a smart contract that reflects the process of securing of police case database on the blockchain infrastructure after creating a secure and private blockchain.

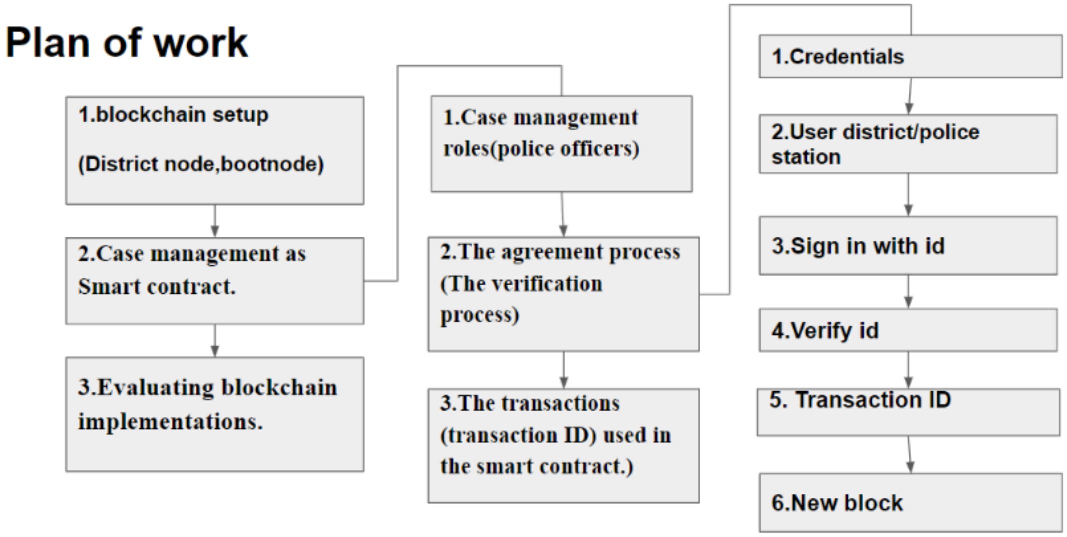
Plan of work
1.blockchain setup
(District node,bootnode)
2.Case management as Smart contract.
3.Evaluating blockchain implementations.
1.Case management roles(police officers)
2.The agreement process (The verification process)
3.The transactions (transaction ID) used in the smart contract.)
1.Credentials
2.User district/police station
3.Sign in with id
4.Verify id
5. Transaction ID
6.New block

Figure 3 : Plan of work

- **Securing police case database as a smart contract**

A smart contract definition has three parts: (1) IdentificationDefinition of roles included in the agreement (selection)(2) Consensus Process (i.e. Selection process) and (3) the transaction(police case data transaction) used with a smart contract.

1) **Roles:** Smart contract roles include the officers that must participate in a contract. This process of securing police case data has the following roles:

i)System Roles: The parties who must take part in the agreement are among the roles in a smart contract. The following roles play a part in the securing database system process:

- **Administrator:** To oversee and store data on the police case database whole lifespan. Several reputable organizations and businesses might be included in this function. The administrator team who are assigned for managing the system of police case database designate permissioned nodes, register officers and the smart contract. Some admin will manage the officer and the system and other will handle the smart contract section.
- (ii) **Police Officers:** An individual who is eligible to enter the system. Officers can authenticate themselves, verify themselves for entering the system & get data from the system .we are using here 2 steps verification process for entering the system get permitted confidential data if they are only authorized.

2) **Securing database process:** In our work, each database of every police station is under process is represented, by a set of smart contracts, which are deployed on the blockchain by the administrators. A smart contract is defined for each of the police stations in the district which is connected to the blockchain network. The following are the main activities in the ensure security process:

3) Smart Contract Creation: Administrators are assigned to creat smart contract at each and every police case database system of every police station who are included to the blockchain network.For each police station on district, the administration defines a list of officer. Then, the smart contracts are added to the blockchain where district nodes are given access to communicate with equivalent smart contracts.

(ii) **Officer Registration:** The registration of officers is conducted by the administrators. When an smart contract create on police case database is made the decision directors must define Limitations and apply. a deterministic list of qualified officers. This might re- quire a component for a government character verification service to safely confirm and authorize eligible individuals. Utilizing such a benefit is fundamental to satisfy the prerequisite of secure verification as this is not ensured, by default, when employing a blockchain infrastructure. In our work, for each qualified officer, a corresponding character wallet would be produced. A unique wallet is produced for each officer for each database system including on blockchain network that the officer is qualified to take part in managing and can get access the system.

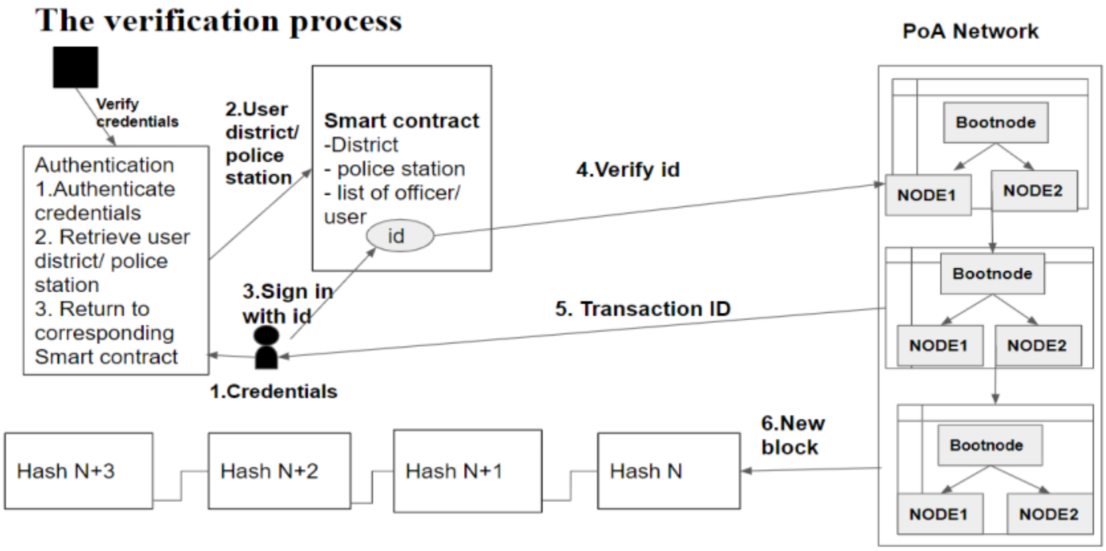

Figure 4 : The process of securing police case database by setting up smart contract

iii) **User Verification:** On this process the smart contract we have written on the blockchain on every police case database on the network it will verify the user with the conditions written on smart contract will match that with the unique id for every valid user unique id that define on the boot node of the blockchain network which is a PoA network. User when they sign up with the unique ID that is set by the administration it will get verified at 2 steps one is on the smart contract another with the bootnode where the valid users informations are stored.

iv) Data transaction process: Each valid user interacts with smart contract for her corresponding police station district. This smart contract interacts with the blockchain via the corresponding district node, which are connected to the blockchain. Each individual user receives the Data transaction ID for their for verification purposes if they enter on the system and gets any data from the system. Every Data transaction that is agreed upon, by the majority of the corresponding district nodes, is recorded as a transaction and then appended on the blockchain.. A transaction in our proposed system has information on i) the transaction ID, ii) the block which the transaction is located at,iii) to which smart contract the transaction was sent - which indicates from which voting district the vote was cast, and iv) the value of the transaction, i.e. the data transaction, indicating which entity (party) the user accesse at the system for getting the data. A data transaction in our system, therefore, reveals no information about the individual user who get access to the system and get data. And this transaction id will pass to the boot node and then it will store on new block and stored in hash.

Chapter IV:Result Discussion

When evaluating a model's performance, we must consider three qualities: testing accuracy, epoch, and loss function. It displays the correctness rate of a given model when assessing accuracy per epoch, and it specifies the difference between our generated and accurate results when the testing loss is established. As earlier mentioned, the last one is used to calculate the model's error rate. We chose the highest possible epoch while also utilizing a large enough dataset to ensure that the model was appropriately trained on the given data to get the minimum feasible loss function in our experiment.we have uses PoA (proof of Authority) Algorithm which is suitable for private network based blockchain.Our system is distributed but the main node or the boot node is under the private network.Among all the consensus algorithm PoA is most effective for this kind of project and preventing the attacked.

Existing System: Existing system of Police case database system is storing the criminal data on their system. It is acessable by simple log in with email & password fill upped some field and can easily accessed by website. Its verification process is not that much secure enough although this type of system required high security. It can be hacked and information can be steal easily by the dishonesty.

This system is for a particular police station with out the high security. In our country police keep criminal's data in files it is tough to find and store. when we file a case against someone police can't catch him if he/she change the district/division because other police station doesn't have any data of that case.But if the criminal evidence need to transact from one district police station to another police station . As this information is confidential so it had to transfer with proper security.And it is not possible to interconnect to another police station from other district with in one system with maintaining the transparency of the data transaction. And the verification process is not secure enough right now.

Proposed System: As the existing system of our police case database although it is very obvious this should be secured enough but it is not distributed or in a network.Many Times need to transfer the data with proper security with other district police station. So we are using a private Blockchain technology with smart contract and using POA algorithm.Smart contract will store the condition as set of program on Ethereum Blockchain and POA algorithm will find the verified user who can access to the system. Hera we are setting up a main node where all the information of valid user will be stored and the other district police station will be define as district node they are connected to the boot nodes. Boot nodes will selected some verified users. In every district node or police station the admin will set up smart contract as valid condition the valid user will sign up with the unique I'd and it will verified by smart contract as well as the boot node. After 2 steps verification if any data transaction happened it will store the transaction id in the boot node and transfer into the new block or hash the transaction id will store there.

As we are using POA algorithm we are hoping it will prevent 51% attacks from unauthorized action.Our main central node which called boot node under a private and confidential network where some admin team has worked as decided the valid user so this is under the PoA or proof of Authority network which ensure the verified user earlier and the smart contract is set of program that will witten on the each police station district node as condition for verifying the valid user and the transection id secured at the hash as well as central main node. So these verification process of preventing unauthoriesd action has made our proposed system ore strong and secure.

Chapter V: Conclusion

5.1Conclusion

With the goal of protecting the police case database in Bangladesh using a blockchain-based system, we looked for the simplest way to manage the enormous amount of difficult-to-organize data.The proposed approach might facilitate communication amongst our police officers.They can readily read the information on the suspect. Any relevant station communication may be shared with other duty officers as part of this project. Finally, we can assert that using a blockchain network built on smart contracts is the simplest method to manage all difficult situations. Our goal was to aid the police by handling difficult tasks in the simplest way possible.

- The proposed solution is effective and feasible.
- We tried to meet the easiest process to handle huge data record which is hard to organize as well as secure.
- An industrial standard system can be developed based on the concept that we proposed to develop our system by using smart contract in blockchain technology

5.2 Limitations of research work

1. Changing (if any error occur) Smart contract almost impossible.
2. If selected validator is not ethical at POA(Proof of Authority) maybe misuse the data or get corrupted.
3. Making error correction in Smart contract highly costly.
4. Programing language (**Solidity**)used for implementing smart contract in Ethereum Blockchain is not familiar.
5. Lack of technical knowledge among the user and moderators.
6. Lack of Knowledge about Smart contract and Blockchain among mass people.

5.3 Future works of the research

- Police case management will be more easier and secure.
- It will help to solve police cases.
- Make the investigation process more reliable.
- The proposed method smart contract can be implemented in different sectors to secure the system.

References

Agora Technologies (2018). Agora - bringing our voting systems into the 21st century. https://www.agora.vote/s/Agora Whitepaper.pdf. Accessed: 2018-07-25.

coalichain.io (2018). coalichain.io (2018). Coalichain - people direct democracy. https://www.coalichain.io/images/pdf/coalichain.pdf.Accessed: 2018-07-25.

1 Andrew Barnes, Christopher Brake and Thomas Perry. (2016). Digital Voting with the use of Blockchain technology Available at: https://www.economist.com/sites/default/files/plymouth.pdf

1 Ajit Kulkarni, (2018), "How To Choose Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018.

2 Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram,P. (2017). Blockchain for iot security and privacy:The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on, pages 618–623. IEEE.

10 Ethdocs.org. (2018). What is Ethereum? — Ethereum Homestead 0.1 documentation. [online] Available at: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

10 Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth.ethereum.org/

3 Jonathan Alexander, Steven Landers and Ben Howerton (2018). Netvote: A Decentralized Voting NetworkAvailableat :https://netvote.io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf

Jelurida,"Jelurida",2017.Available at:https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf

2 Kappos, G., Yousaf, H., Maller, M., and Meiklejohn, S.(2018). An empirical analysis of anonymity in zcash. arXiv preprint arXiv:1805.03180.

Khan, K. M., Arshad, J., and Khan, M. M. (2018). Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research (IJEGR), 14(1):53–62.

Lenarduzzi, V., Lunesu, I., Marchesi, M., and Tonelli, R.(2018). Blockchain applications for agile methodologies. In the 19th International Conference on Agile Processes in Software Engineering and Extreme Programming. XP, volume 2018.

McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter PrivacyAvailable at: https://eprint.iacr.org/2017/110.pdf.

Nicholas Weaver. (2016). Secure the Vote Today Available at:https://www.lawfareblog.com/secure-vote-today.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Neff, C. A. (2001). A verifiable secret shuffle and its application to e-voting. In Proceedings of the 8th ACM conference on Computer and Communications Security, pages 116–125. ACM.

Pinna, A., Tonelli, R., Orru, M., and Marchesi, M. (2018). A petri nets model for blockchain analysis. Computer Journal, pages 1–15.

Porru, S., Pinna, A., Marchesi, M., and Tonelli, R. (2017).Blockchain-oriented software engineering: Challenges and new directions. In Proceedings of the 39th International Conference on Software Engineering Companion, ICSE-C ’17, pages 169–171, Piscataway, NJ, USA. IEEE Press.

Rubtcova, M. and Pavenkov, O. (2018). Using of blockchain in electronic elections in russia.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I.,Tromer, E., and Virza, M. (2014).

Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/.

Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11):612–613.

Salanfe, Setup your own private Proof-of-Authority Ethereum network with Geth, Hacker Noon, 2018. Available at: https://tinyurl.com/y7g362kd.

Spanos, N., Martin, A. R., and Dixon, E. T. (2017). System and method for securely receiving and counting votes in an election. US Patent App. 15/676,959.

TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it. Available at: https://techcrunch.com/2018/02/24/liquid-democracy-uses-blockchain/

Tonelli, R., Pinna, A., Baralla, G., and Ibba, S. (2018). Et-hereum smart contracts as blockchain-oriented microservices. In International Workshop on Microservices:Agile and DevOps Experience (MADE18) - XP2018 proceedings companion.

Vitalik Buterin. (2015). Ethereum White Paper Available at: https://github.com/ethereum/wiki/wiki/White-Paper.

Wang, B., Sun, J., He, Y., Pang, D., and Lu, N. (2018).Large-scale election based on blockchain. Procedia Computer Science, 129:234–237.

"What Are Smart Contracts? A Beginner's Guide to Smart Contracts", Blockgeeks, 2016. Available at: https://blockgeeks.com/guides/smart-contracts/

Zyskind, G., Nathan, O., et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. InSecurity and Privacy Workshops (SPW), 2015 IEEE, pages 180–184. IEEE.

Zerocash: Decentralized anonymous payments from bitcoin. In 2014 IEEE Symposium on Security and Privacy (SP), pages 459–474. IEEE.

Security of Police Case Database using Blockchain.pdf

ORIGINALITY REPORT

39%
SIMILARITY INDEX

PRIMARY SOURCES

1	www.researchgate.net Internet	411 words — 6%
2	scitepress.org Internet	245 words — 4%
3	Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa, Gisli Hjalmtysson. "Blockchain-Based E-Voting System", 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018 Crossref	243 words — 3%
4	Submitted to International University of Business Agriculture and Technology Your Indexed Documents	218 words — 3%
5	www.scitepress.org Internet	173 words — 2%
6	Submitted to International University of Business Agriculture and Technology Your Indexed Documents	158 words — 2%
7	en.wikipedia.org Internet	139 words — 2%
8	www.ijcstjournal.org Internet	114 words — 2%

9	Seri, Pavan Reddy. "Blockchain Based e-Voting", Southern Illinois University at Carbondale, 2021 ProQuest	81 words — 1%
10	skemman.is Internet	52 words — 1%
11	"Digital Forensics using Blockchain", International Journal of Recent Technology and Engineering, 2019 Crossref	51 words — 1%
12	cps-vo.org Internet	51 words — 1%
13	www.semanticscholar.org Internet	46 words — 1%
14	Submitted to International University of Business Agriculture and Technology Your Indexed Documents	42 words — 1%
15	www.irjmets.com Internet	42 words — 1%
16	Submitted to International University of Business Agriculture and Technology Your Indexed Documents	39 words — 1%
17	anubhav Mishra, Anuroop Mishra, Abhyudya Bajpai, Abhinav Mishra. "Implementation of Blockchain for Fair Polling System", 2020 International Conference on Smart Electronics and Communication (ICOSEC), 2020 Crossref	39 words — 1%
18	core.ac.uk Internet	39 words — 1%

19	ieeexplore.ieee.org Internet	37 words — 1%
20	spritz.math.unipd.it Internet	35 words — 1%
21	repository.sustech.edu Internet	34 words — < 1%
22	ijsrset.com Internet	31 words — < 1%
23	academy.binance.com Internet	27 words — < 1%
24	edepositireland.ie Internet	25 words — < 1%
25	kamiltaylan.blog Internet	25 words — < 1%
26	"Illumination of Artificial Intelligence in Cybersecurity and Forensics", Springer Science and Business Media LLC, 2022 Crossref	24 words — < 1%
27	nccur.lib.nccu.edu.tw Internet	19 words — < 1%
28	Ch. Rupa, Divya Midhunchakkaravarthy. "Preserve Security to Medical Evidences using Blockchain Technology", 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020 Crossref	17 words — < 1%
29	Mukesh Soni, Dileep Kumar Singh. "Blockchain Implementation for Privacy preserving and	17 words — < 1%

securing the Healthcare data", 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2021
Crossref

---

30 link.springer.com
Internet
17 words — < 1%

---

31 hdl.handle.net
Internet
15 words — < 1%

---

32 Gulshan Kumar, Rahul Saha, Chhagan Lal, Mauro Conti. "Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications", Future Generation Computer Systems, 2021
Crossref
14 words — < 1%

---

33 www.scinapse.io
Internet
14 words — < 1%

---

34 Bharti Sharma, Kanika Maheshwari, Dharamveer Kumar, Anvesa Jaiswal. "Mobile Friendly Fully Decentralized Voting System using Blockchain Technology and IPFS", 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), 2021
Crossref
13 words — < 1%

---

35 etd.repository.ugm.ac.id
Internet
12 words — < 1%

---

36 drops.dagstuhl.de
Internet
11 words — < 1%

---

37 www.ijeat.org
Internet
11 words — < 1%

38	Yong Zhang, Songyang Wu, Bo Jin, Jiaying Du. "A blockchain-based process provenance for cloud forensics", 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017 Crossref	10 words —	< 1%
39	"Artificial Intelligence Techniques for Advanced Computing Applications", Springer Science and Business Media LLC, 2021 Crossref	9 words —	< 1%
40	"IC-BCT 2019", Springer Science and Business Media LLC, 2020 Crossref	9 words —	< 1%
41	harvest.usask.ca Internet	9 words —	< 1%
42	www.uwstout.edu Internet	9 words —	< 1%
43	Lecture Notes in Computer Science, 2014. Crossref	8 words —	< 1%
44	Muhammad Shoaib Farooq, Zareen Kalim, Adnan Abid. "A Blockchain-based Framework for Distributed Agile Software Development", IEEE Access, 2022 Crossref	8 words —	< 1%
45	Noe Elisa, Longzhi Yang, Fei Chao, Yi Cao. "A framework of blockchain-based secure and privacy-preserving E-government system", Wireless Networks, 2018 Crossref	8 words —	< 1%
46	netlib.sandia.gov Internet	8 words —	< 1%

47	www.mdpi.com Internet	8 words — < 1%
48	Submitted to International University of Business Agriculture and Technology Your Indexed Documents	7 words — < 1%
49	Louise Axon, Michael Goldsmith, Sadie Creese. "Privacy Requirements in Cybersecurity Applications of Blockchain", Elsevier BV, 2018 Crossref	7 words — < 1%
50	Zyskind, Guy, Oz Nathan, and Alex 'Sandy' Pentland. "Decentralizing Privacy: Using Blockchain to Protect Personal Data", 2015 IEEE Security and Privacy Workshops, 2015. Crossref	7 words — < 1%
51	Submitted to International University of Business Agriculture and Technology Your Indexed Documents	6 words — < 1%
52	Submitted to International University of Business Agriculture and Technology Your Indexed Documents	6 words — < 1%
53	Sarah Al-Maaitah, Mohammad Qatawneh, Abdullah Quzmar. "E-Voting System Based on Blockchain Technology: A Survey", 2021 International Conference on Information Technology (ICIT), 2021 Crossref	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE SOURCES	OFF
EXCLUDE BIBLIOGRAPHY	OFF	EXCLUDE MATCHES	OFF