NITYA: A DECENTRALISED CRIMINAL JUSTICE SYSTEM

MAJOR PROJECT REPORT

Submitted in partial fulfillment of requirements for the award of the degree of

Bachelor of Technology

In

Information Technology

by

Narender Singh	*Sarvottam Kumar*	*Pranav Saxena*
40851203116	*41551203116*	*60151203116*

Guided by

Ms. Shafali Dhall

(Assistant Professor)

DEPARTMENT OF INFORMATION TECHNOLOGY

BHARATI VIDYAPEETH'S COLLEGE OF ENGINEERING

(AFFILIATED TO GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI)

PASCHIM VIHAR, NEW DELHI-110063

APRIL, 2020

CANDIDATE’S DECLARATION

It is hereby certified that the work which is being presented in the B. Tech Minor Project Report entitled **“Nitya: A Decentralised Criminal Justice System"** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** and submitted in the **Department of Information Technology** of **BHARATI VIDYAPEETH’S COLLEGE OF ENGINEERING, New Delhi (Affiliated to Guru Gobind Singh Indraprastha University, Delhi)** is an authentic record of our own work carried out during a period from January 2020 to April 2020 under the guidance of Ms. Shafali Dhall, Assistant Professor.

The matter presented in the B. Tech Minor Project Report has not been submitted by us for the award of any other degree of this or any other Institute.

Narender Singh	**Sarvottam Kumar**	**Pranav Saxena**
40851203116	**41551203116**	**60151203116**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge. He/She/They are permitted to appear in the External Major Project Examination.

Ms. Shafali Dhall
Assistant Professor

Prof.(Dr.) Vanita Jain
HOD, IT Dept.

Project Coordinator ***Project Coordinator*** ***(Signature of External Examiner)***

ABSTRACT

Owing to the pan-india campaign “Digital India”, almost every department of government has moved to the digital platform replacing the manual system with online process. For instance, citizen can register and track their FIR over the internet using the e-police service.

Along the same line, the cyber crime also has risen to the level that it can make the current system inefficient and vulnerable to several cyber attack. Since the digital criminal justice platforms are based on the centralised model involving multiple client communication to the single server, it poses a central point of failure that may disrupt the whole system.

Also, one of the main element in any case is the evidence which always need to be secure. Hence, there are changes that it could be tampered through various ways without leaving a trace to catch.

Hence, Nitya, a decentralised system, based on the Blockchain technology can smartly sweep off all the shortcoming of the current centralised system. Nitya aims to enhance the security, transparency, integrity and most important immutability to the evidence.

ACKNOWLEDGEMENT

We express our deep gratitude to **Ms. Shefali Dhall**, Assistant Professor, Department of Information Technology for his valuable guidance and suggestion throughout my project work. We are thankful to **Dr. Gopal and Mr. Anurag Aggarwal,** Project Coordinators, for their valuable guidance.

We would like to extend my sincere thanks to **Head of the Department, Prof. Vanita Jain** for his time to time suggestions to complete my project work. I am also thankful to **Dr. Dharmender Saini , Principal** for providing me the facilities to carry out my project work.

Narender Singh	**Sarvottam Kumar**	**Pranav Saxena**
40851203116	**41551203116**	**60151203116**

TABLE OF CONTENTS

CANDIDATE'S DECLARATION **i**

ABSTRACT **ii**

ACKNOWLEDGEMENT **iii**

TABLE OF CONTENTS **iv**

LIST OF FIGURES **v**

Chapter 1: Introduction **1-3**

1.1 Objective 2

1.2 Motivation 3

Chapter 2: Literature Survey **4-9**

2.1 Pen & Paper 4

2.1 E-FIR 5

2.1 Nitya 7

Chapter 3: Tools & Technologies **10-22**

3.1 Blockchain Technology 10

3.1.1 How Does Blockchain works? 12

3.2 Ethereum 14

3.2.1 Components 15

Chapter 4: Nitya System **22-28**

4.1 Requirements 22

4.2 System interaction & workflow 25

Chapter 5: Result & Discussion **29-31**

Chapter 6: Conclusion **32**

Chapter 7: Future Scope **33**

REFERENCES **34-35**

LIST OF FIGURES

Figure 1	Client-Server model	11
Figure 2	Decentralised network	11
Figure 3	E-FIR web app working architecture	12
Figure 4	Nitya web app working architecture	13
Figure 5	Merke Tree	17
Figure 6	State Root tree	18
Figure 7	Block Header	21
Figure 8	Ganache Personal Blockchain	23
Figure 9	Metamask	25
Figure 10	Admin functions	25
Figure 11	Agency functions	26
Figure 12	Complainant functions	26
Figure 13	Web portal of Nitya	27
Figure 14	Metamask login	27
Figure 15	Register complaint	28
Figure 16	Smart Contract Deployed in Blockchain	29
Figure 17	List of transactions	30
Figure 18	Detail of individual transaction	30
Figure 19	List of Blocks mined	31
Figure 20	Detail of one block containing transaction	31

CHAPTER 1 : INTRODUCTION

The digital platform may have ease the life of people by performing any actions in just a fraction of seconds. Especially the criminal justice system that involves various participants such as complainant, lawyer, courts and police.

In addition, the system is also automated to keep all records at every stages of trials which any participate can trace back at any point of time from any place.

It is very easy to maintain the timeline of event of crime with all the data stored digitally and share with anyone without hassle.

Summing up the advantages of current digital model, it undoubtedly possess a potential to replace the old, slow and inaccessible pen and paper method.

But as every system possess a loophole so does the current e-police system. Of course, the cyber attack is the major threat to the platform. But the loophole has a larger and direct effect to the core component of the whole criminal justice system i.e. data.

Every proceeding are carried out on the basis of data and evidence. After registering a case, Police look out for all possible evidence. Prosecutor ask to victim and Judge resolves the case by analysis the data presented by prosecutors.

Long story short, all scenes revolves around the evidence. Hence, it becomes crucial to secure and integrate all data uploaded to the online platform. However, there are other issues with current digital system as well.

Hence, our decentralised criminal justice system — Nitya perfectly suits to settle down all the problem related to the current digital system. Based on the prevalent Blockchain technology, Nitya brings a three pillar, secure, immutable and transparency to strengthen and integrate the criminal justice system even more.

Instead of storing data by each member of criminal justice system in their separate centralised server, Nitya maintains a single ledger containing all the transaction of data and distribute among all the stakeholder of the criminal justice system. The single ledger are then distributed among each member to brings more transparency and trust.

Also, there is no point of failure as Nitya forms a distributed network where each node (participant) can independently communicate with each other. Since every record are stored in a ledger and shared with each participant, any changes to the evidence or data are tracked and copied to the each participant's database.

Another peculiarity of blockchain is that data can't be altered as data are stored as a separate block with timestamps forming a chain in a ledger and has to pass through consensus mechanism. Consequently, data is relatively tamper proof and immutable as any invalid changes to data can be terminated through a consensus. then the valid block will be announced to all the nodes i.e. police, court, etc. present in the distributed network with the timestamp.

1.1 OBJECTIVE

The objective for building the Nitya is to eliminate all the shortcoming of the digital system that threatens criminal justice system. Indirectly, Nitya safeguards the fundamental right of justice to the citizen by protecting the core element data and evidence.

Nitya aims to develop an online crime reporting and management system which is easily accessible to the public, the police Department and the administrative department. Evidence is an important document that set the process of criminal justice in motion, hence, it has to be secure and indestructible.

The person giving Information or making a complaint has a right to demand that the information is recorded by the police be read to him or her. Once the Information has been recorded by the police it must be signed by the person giving the information and make sure there is no tampering with it.

It also aim to Interlink Police Stations, State and National Data Centres through a data network which make them work fluently and efficiently on any cases to process it fast by basically establishing State and National Crime & Criminal Database which could be using for auditing of crimes and henceforth for maintain Law and Order in the society and punish the criminals.

1.2 MOTIVATION

I remember the sensational nirbhaya case, where the chemical examination report was fudged by the officers concerned leading to huge uproar. Though the manipulation was brought to light, it revealed the grim reality that the distortion of facts was possible even in high profile cases.

Recently, there has been many cases where evidence has been tampered or destroyed by the police department also to interrupt the investigation by CBI.

“Complainant in Home Guard scam set fire to evidence [1]”

“Lot of Saradha evidence destroyed, Kolkata Police not cooperating: CBI chief Nageshwar Rao said [2]”

“CBI says Haryana police destroyed evidence in Ryan murder case[3]”

In most of the cases, it doesn’t get into news or not get detected that lead to injustice or escape of the culprit.

In India only about 16 out of 100 people booked for criminal offences are finally convicted. Low rate of conviction points to the inefficiency of the Criminal Justice System of India – which includes the police, prosecutors, and the judiciary. This results in a big problem of people losing faith in the Criminal Justice System of India – which is very dangerous.[4]

CHAPTER 2: LITERATURE SURVEY

2.1 PEN & PAPER

According to the Indian Jurisdiction and Law, a citizen can lodge a complaint for a cognizable offence. For any such offence, an FIR can be registered either by the victim of the offence or by someone else on his/her behalf. The report can be made either orally or in writing to the police. FIR is a crucial first step towards registration of complaint because only after the FIR has been registered the police can start investigation on the committed offence.

The earlier scenario was that any person who had witnessed the commission of any such offence, had to rush to a Police Station in order to tell about the proceedings and lodge a complaint. A physical transfer of the person was required from the spot of crime to the police station. Many a times it so happened that important details about the offender was missed out by the victim due to this commute. Moreover the problem resides in availability of police station nearby, which might add on to the time between occurrence of the offence and investigation being started on it.

So, this pen & paper and physically appearing method led to the following problems:

- **Waste of Time:** It leads to waste of time as there is much paper work.
- **Difficulty in filling FIR:** Reluctance by police stations to show a higher crime rate for their region, complaints against rich and powerful people where police may show hesitation to act, expectations of money in the form of bribes.
- **Time consuming:** Every work is done manually so we cannot generate report in the Middle of the session or as per the requirement because it is very time consuming.
- **False FIR:** People file a false complaint or give wrong information to the police.
- **Loss of data:** If a crime is committed, the victim must go to the police station. The duty officer in the station fills an FIR. This is a paper based process and paper records may easily be manipulated or lost.
- **Data maintainence:** It was also very complex task to maintain huge amount of paper work of the case which led to mismanagement of the data and evidence. History of records of each phases of data was expensive task.

2.2 E-FIR

So, due to the evolution in the computer technology and modernization, there is huge shift of the paperwork to digital. People started using mobile phone for carrying out their most of the works.

So due to digitization of the world, government started promoting the digital india programme to make the country digital by enabling all of the servies online and on digital platform for the ease of the citizens and the work load.

The Indian Police Department has ever since remained manually driven for most of its routine chores. The officials have been adopting the basic fundamental methods of carrying out the proceedings with the traditional "pen and paper" method being highly prevalent. These traditional practices were comfortable in earlier days, when population was far less, and the crime rates were also comparably minimal.

But in today's India, when the evil elements of the society are in a boom and so many cases being registered every day, it has become a very tedious task to manage the case and all its related documents, manually. Digitization in Police department is the need of the hour. The traditional method of visiting a police station for registering a police complaint and getting updates needs to be replaced with an online process.

Hence an E-police system is being developed which will collect complainant's data through a mobile application, sends the information over to the Police department on their web portal, and in this way the entire interaction occurs online, with information exchanges over the application and the web portal.[5]

This also led to enactment of the digital police by developing E-FIR system[5] with improved facilities using e-governance and to provide transparency and easy access to the people to register complaint from anywhere. This method overcome all the limitations in the previous paper system. The system provides proper security and reduces the manual work. Users can easily file an FIR using the E-FIR system from anywhere and anytime.

There are various advanctage of the E-FIR system such as:

1) Time and Energy Saving

The system prevents the complainant from the need to manually go to a police station to lodge a complaint. Using the online platform in his/her mobile phone or computer, one can easily register the complaint with the police. Also the complainant does not need to repeatedly go to the police station for getting updates on his case as he/she would be notified through the application.

2) Ease of Accessibility for Public

It is often observed that people refrain from going to the police station. Many think it is time consuming and that they would have to bribe the police to get the work done, while many are simply hesitant to lodge a complaint due to societal factors. This system allows anybody to lodge complaint and communicate directly with the police authorities.

3) Promotion of E-Governance

With the recent advancement of Creation and Maintenance of police Database, Indian government is now planning to maintain database of 1.5 Crore criminals. The E-Police System is an additional facility and will aid this process of record maintenance with e-documents.

4) Secure and Transparent Process of Investigation and Tracking

Since only the investigating officer can access the particular FIR id, the information is private and secure. The process carrying out online, in full knowledge of the complainant ensures transparency.

5) Improving the standards of Indian Police system

With many countries like USA, Singapore and many other developed countries in the world already having a fully functional e-police system, India must also develop upto with world standards.

6) No delays in catering the FIR

As the police has to directly update the complainant over the application about the proceedings of the case, with proof, any delay in the work is instantly noticed by the citizens and thus the scopes of false promises is highly reduced.

7) Central Database for Statistics and Auditing

The digital portal provides a National Database of crime and criminals which can be used for the statistical data that help to curb the crime by analysing the regionally and wholly. This will improve national security and revolutionise the way police works in the country.

8) Integration with other agencies

The digital system can be enhanced to integrate the Police data with other pillars of the criminal justice system namely -- Courts, Prisons, Prosecution, Forensics and Fingerprints and juvenile homes.

But as crime continues to grow, and criminals turn tech-savvy, police investigators across States face a tough challenge to bring the law-breakers to justice. This system started facing challenges of cyber crime and attack which makes it inefficient and unsafe of the criminal data. Police departments are increasingly the targets of cyberattacks, either for criminal purposes or as acts of "hacktivism." Since the evidence and data of the polices case are stored on the digital platform which is the main element for resolving any cases. It became essential to protect it from any attack or theft.

2.3 NITYA

Our project introduced the Nitya system which resolve most of the issues and threats that E-FIR system faces. It makes the criminal justice system more secure, trustful and immutable so that justice can be given to the citizen on the basis of the truthful data and evidence.

This system is based on the Blockchain technology. The concept of Blockchain technology was first proposed by Satoshi Nakamoto[6], it is a cryptographically engineered software platform to store ledger using peer to peer network. It is a sequential chain of blocks where every block contains a cryptographically hash value of previous block, time-stamp and the block information. From the above method we can ensure the integrity and security of the block and we can identify the invalid block. The first application of this technology was Bitcoin, which allows cash transaction using internet, through peer to peer network without a central authority and in a trustless network. The system uses the method of timestamp by hashing the block into continuous chain based on proof of work mechanism.[7]

And then bitcoin inspired other to build Ethereum blockchain [8]. We have blocks in the Ethereum blockchain, these blocks are linked together and each blocks we have list of transaction similar to bitcoin. Inside these transaction we do have timestamp and other parameters which we can programme it.

Ethereum blockchain gets stored in every miners computer which is called a node, it uses the proof of work algorithm to verify the network. The block contains the smart contract which has the code snippet that runs in each block, when the code computation is successfully executed in each miner's computer. It is sent to whole network so that the other miners can agree. The successful verification of the block will be added to the chain.

Present-day, the model E-FIR system follow is centralize i.e. it is govern by a particular organization – this is called location-based addressing, but if the server is down then we will not get the content. There is a chance that there must be someone who will have the copy of that content in their device which we were searching yet we won't be able to get that.

Hence, our Nitya which is based on blockchain technology built using ethereum platform makes the previous digital system more efficient by providing the following advantages:

1. Greater transparency

Transaction histories are becoming more transparent through the use of blockchain technology. Because blockchain is a type of distributed ledger, all network participants share the same documentation as opposed to individual copies. That shared version can only be updated through consensus, which means everyone must agree on it.

To change a single transaction record would require the alteration of all subsequent records and the collusion of the entire network. Thus, data on a blockchain is more accurate, consistent and transparent than when it is pushed through paper-heavy processes. It is also available to all participants who have permissioned access. To change a single transaction record would require the alteration of all subsequent records and the collusion of the entire network.

2. Enhanced security

There are several ways blockchain is more secure than other record-keeping systems. Transactions must be agreed upon before they are recorded. After a transaction is approved, it is encrypted and linked to the previous transaction.

This, along with the fact that information is stored across a network of computers instead of on a single server, makes it very difficult for hackers to compromise the transaction data. In any industry where protecting sensitive data is crucial — financial services, government, healthcare — blockchain has an opportunity to really change how critical information is shared by helping to prevent fraud and unauthorized activity.

3. Improved traceability

Since tracing back the history of the cases is required in any period of time, it become crucial to maintain the data efficiently so that it can be to trace back to its origin. When data are recorded on a blockchain, it forms the block which are linked with the previous block which actually store all the data. This historical transaction data can help to verify the authenticity of data and prevent fraud.

4. Increased efficiency and speed

When we use traditional, paper-heavy processes, trading anything is a time-consuming process that is prone to human error and often requires third-party mediation. By streamlining and automating these processes with blockchain, transactions can be completed faster and more efficiently. Since record-keeping is performed using a single digital ledger that is shared among participants, we don't have to reconcile multiple ledgers and we end up with less clutter.

And when everyone has access to the same information, it becomes easier to trust each other without the need for numerous intermediaries in the criminal justice sytem. Thus, clearing and settlement can occur much quicker.

5. Reduced costs

Reducing costs is a priority in all the fields. With blockchain, we don't need as many third parties or middlemen to make guarantees. Instead, we just have to trust the data on the blockchain. We also won't have to review so much documentation to complete a trade because everyone will have permissioned access to a single, immutable version.

CHAPTER 3: TOOLS & TECHNOLOGIES

3.1 Blockchain Technology

The core technology over which our system is based is blockchain technology. Blockchain can be described as a data structure that holds transactional records and while ensuring security, transparency, and decentralization. It can be think as a chain or records stored in the forms of blocks which are controlled by no single authority. A blockchain is a distributed ledger that is completely open to any and everyone on the network. Once an information is stored on a blockchain, it is extremely difficult to change or alter it.

Each transaction on a blockchain is secured with a digital signature that proves its authenticity. Due to the use of encryption and digital signatures, the data stored on the blockchain is tamper-proof and cannot be changed.

Blockchain technology allows all the network participants to reach an agreement, commonly known as consensus. All the data stored on a blockchain is recorded digitally and has a common history which is available for all the network participants. This way, the chances of any fraudulent activity or duplication of transactions is eliminated without the need of a third-party.

There are three pillar of Blockchain Technology which have helped it gain widespread acclaim are as follows:

1. Decentralization

In E-FIR system[9], there is centralized services i.e. it has centralized portal that stored all the data , citizen enters and they've to interact solely with this to get whatever information they required or need to add in the ongoing trial.

It is based on the traditional client-server model[10] having several vulnerabilities. Such as, because they are centralized, all the data is stored in one spot. This makes them easy target spots for potential hackers. If the centralized system were to go through a software upgrade, it would halt the entire system.

What if the centralized entity somehow shuts down for whatever reason? That way nobody will be able to access the information that it possesses.

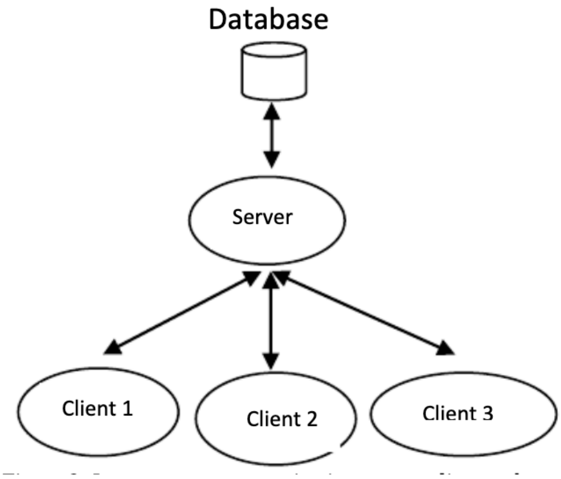
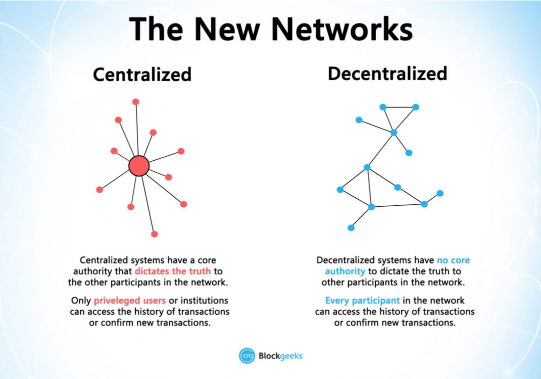


Figure 1. Client-Server Model

But in a decentralized system [11], the information is not stored by one single entity. In fact, everyone in the network owns the information. In a decentralized network, if any party of criminal justice system wanted to interact with other party then they can do so directly without going through a third party.


The New Networks

Centralized

Decentralized

Centralized systems have a core authority that dictates the truth to the other participants in the network.

Only priveleged users or institutions can access the history of transactions or confirm new transactions.

Decentralized systems have no core authority to dictate the truth to other participants in the network.

Every participant in the network can access the history of transactions or confirm new transactions.

Figure 2. Decentralised network

2. Distributed

With the use of Blockchain, the interaction between two parties through a peer-to-peer model is easily accomplished without the requirement of any third party. Blockchain uses P2P protocol which allows all the network participants to hold an identical copy of transactions, enabling approval through a machine consensus. For example, if one party of criminal justice system wish to send private data to another party, they can do that with blockchain all by themselves within a few seconds. Moreover, any interruptions or extra charges will not be deducted in the transfer.

3. Immutability

The immutability property of a blockchain refers to the fact that any data once written on the blockchain cannot be changed. Once the data has been processed by citizen or police, it cannot be altered or changed. In case of the blockchain, if anyone try to change the data of one block, he'll have to change the entire blockchain following it as each block stores the hash of its preceding block. Change in one hash will lead to change in all the following hashes. It is extremely complicated for someone to change all the hashes as it requires a lot of computational power to do so. Hence, the data stored in a blockchain is non-susceptible to alterations or hacker attacks due to immutability and makes evidence and all important data needed for investigation indestructible and immutable.

3.1.1 How Does Blockchain Work?

Let's look at a web application of E-FIR system and how it works.

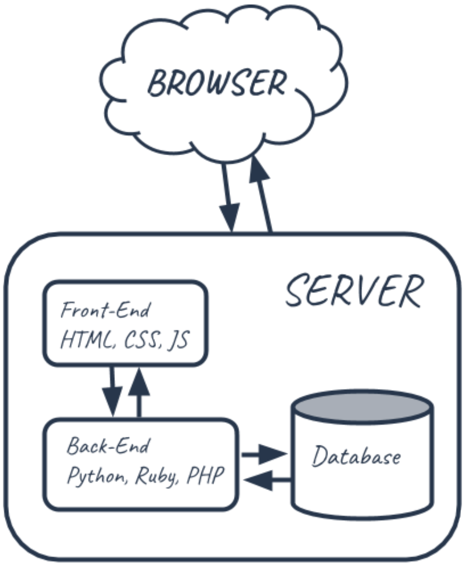


Figure 3. E-FIR web app working architecture

Normally when we want to register a complaint, we use a web browser to use web portal that connect to a central server over a network. All the code of this web application lives on this central server, and all the data lives in a central database. Anytime any party interact with application, must communicate with this central server on the web.

But the problem with it is that the data on the database could be changed. It could be counted more than once, data changed or removed entirely. The source code on the web server could also be changed at any time.

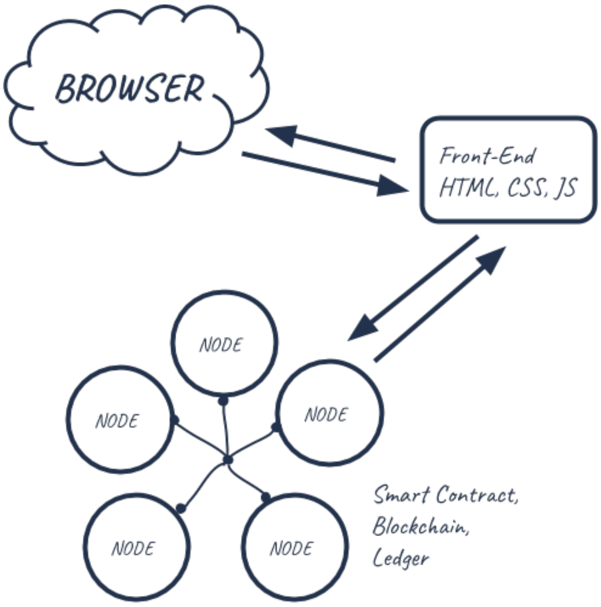


Figure 4. Nitya web app working architecture

Instead of having a network, a central server, and a database, the blockchain is a network and a database all in one. A blockchain is a peer-to-peer network of computers, called nodes, that share all the data and the code in the network. So, if any party connected to the blockchain, they act as a node in the network, and they talk to other computer nodes in the network. Each having a copy of all the data and the code on the blockchain. There are no more central servers. Just a bunch of computers of each party of criminal justice system that talk to one another on the same network.

All the new upload or update is shared across the nodes in the blockchain that contained in bundles of records called blocks, which are chained together to create the public ledger. This public ledger represents all the data in the blockchain. All the data in the public ledger is secured by cryptographic hashing, and validated by a consensus algorithm. Nodes on the network participate to ensure that all copies of the data distributed across the network are the same.

In a nutshell, here’s how blockchain allows transactions to take place:

1. A blockchain network makes use of public and private keys in order to form a digital signature ensuring security and consent.

2. Once the authentication is ensured through these keys, the need for authorization arises.
3. Blockchain allows participants of the network to perform mathematical verification and reach a consensus to agree on any particular value.
4. While making a transfer, the sender uses their private key and announces the transaction information over the network. A block is created containing information such as digital signature, timestamp, and the receiver’s public key.
5. This block of information is broadcasted through the network and the validation process starts.
6. Miners all over the network start solving the mathematical puzzle related to the transaction in order to process it. Solving this puzzle requires the miners to invest their computing power.
7. Upon solving the puzzle first, the miner receives rewards in the form of bitcoins. Such kind of problems is referred to as proof-of-work mathematical problems.
8. Once the majority of nodes in the network come to a consensus and agree to a common solution, the block is time stamped and added to the existing blockchain. This block can contain anything from money to data to messages.
9. After the new block is added to the chain, the existing copies of blockchain are updated for all the nodes on the network.

3.2 ETHEREUM

To build the Nitya, we have used the ethereum platform which provides tools for building the decentralised application. This new blockchain is specifically used for smart contract execution, decentralized apps (largely known as DApps today), and autonomous organizations.

Ethereum has its own digital currency called Ether. Ether is largely known today as cryptocurrency or a “token”. This is important, because whenever there is execution of a smart contract or transaction occur using the Ethereum blockchain, there is need of enough “gas”, aka ether to run the program. We’ve to pay ether to run program code on ethereum. Ethereum uses the “proof of work” methodology [12].

3.2.1 COMPONENTS

- **Smart Contract**

All of the code on the blockchain is contained in smart contracts, which are programs that run on the blockchain. They are the building blocks of blockchain applications.

Smart contracts are written in a programming language called Solidity, which looks a lot like JavaScript. All of the code in the smart contract is immutable, or unchangeable. Once we deploy the smart contract to the blockchain, we won't be able to change or update any of the code. This is a design feature that ensures that the code is trustless and secure.

- **EVM (Ethereum virtual machine)**

The Ethereum Virtual Machine (EVM) is a virtual state machine that functions as a runtime environment for smart contracts in Ethereum. Smart contract code that executes in the EVM is isolated from the network, filesystem, and other processes of Ethereum.

The EVM is a quasi Turing-complete system. This means that the EVM is capable of executing code of arbitrary algorithmic complexity in order to solve any computable problem, given that enough resources are dedicated. However, the amount of possible computations is intrinsically bounded by gas, which is why the EVM is only 'quasi' Turing-complete.

- **Gas**

Gas is what we pay to execute code on the blockchain and to transfer ether to another address. For each instruction on the Ethereum Virtual Machine we pay a certain amount of gas. Some instructions are expensive and some are cheap.

If we call a function and we run out of gas while executing this function call, all changes performed by the function will be rolled back and we will lose all the gas that we provided.

- **Accounts**

The global “shared-state” of Ethereum is comprised of many small objects (“accounts”) that are able to interact with one another through a message-passing framework. Each account has a **state** associated with it and a 20-byte **address**. An address in Ethereum is a 160-bit identifier that is used to identify any account.

There are two types of accounts:

- Externally owned accounts, which are controlled by private keys and have no code associated with them.
- Contract accounts, which are controlled by their contract code and have code associated with them.

- **Account state**

The account state consists of four components, which are present regardless of the type of account:

1. nonce: If the account is an externally owned account, this number represents the number of transactions sent from the account's address. If the account is a contract account, the nonce is the number of contracts created by the account.
2. balance: The number of Wei owned by this address. There are 1e+18 Wei per Ether.
3. storageRoot: A hash of the root node of a Merkle Patricia tree (we'll explain Merkle trees later on). This tree encodes the hash of the storage contents of this account, and is empty by default.
4. codeHash: The hash of the EVM (Ethereum Virtual Machine — more on this later) code of this account. For contract accounts, this is the code that gets hashed and stored as the codeHash. For externally owned accounts, the codeHash field is the hash of the empty string.

- **World state**

Ethereum's global state consists of a mapping between account addresses and the account states. This mapping is stored in a data structure known as a Merkle Patricia tree.

A Merkle tree is a type of binary tree composed of a set of nodes with:

- a large number of leaf nodes at the bottom of the tree that contain the underlying data
- a set of intermediate nodes, where each node is the hash of its two child nodes

- a single root node, also formed from the hash of its two child node, representing the top of the tree

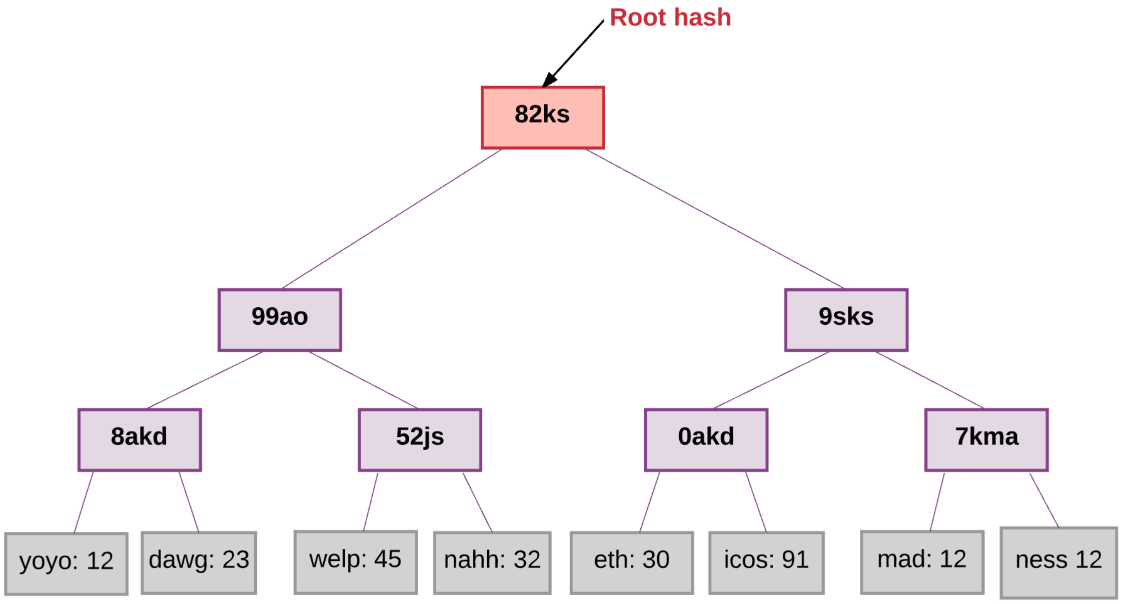


Figure 5. Merkel Tree

The data at the bottom of the tree is generated by splitting the data that we want to store into chunks, then splitting the chunks into buckets, and then taking the hash of each bucket and repeating the same process until the total number of hashes remaining becomes only one: the root hash.

This tree is required to have a key for every value stored inside it. Beginning from the root node of the tree, the key should tell you which child node to follow to get to the corresponding value, which is stored in the leaf nodes. In Ethereum's case, the key/value mapping for the state tree is between addresses and their associated accounts, including the balance, nonce, codeHash, and storageRoot for each account (where the storageRoot is itself a tree).

This same trie structure is used also to store transactions and receipts. More specifically, every block has a "header" which stores the hash of the root node of three different Merkle trie structures, including:

- State trie
- Transactions trie
- Receipts trie

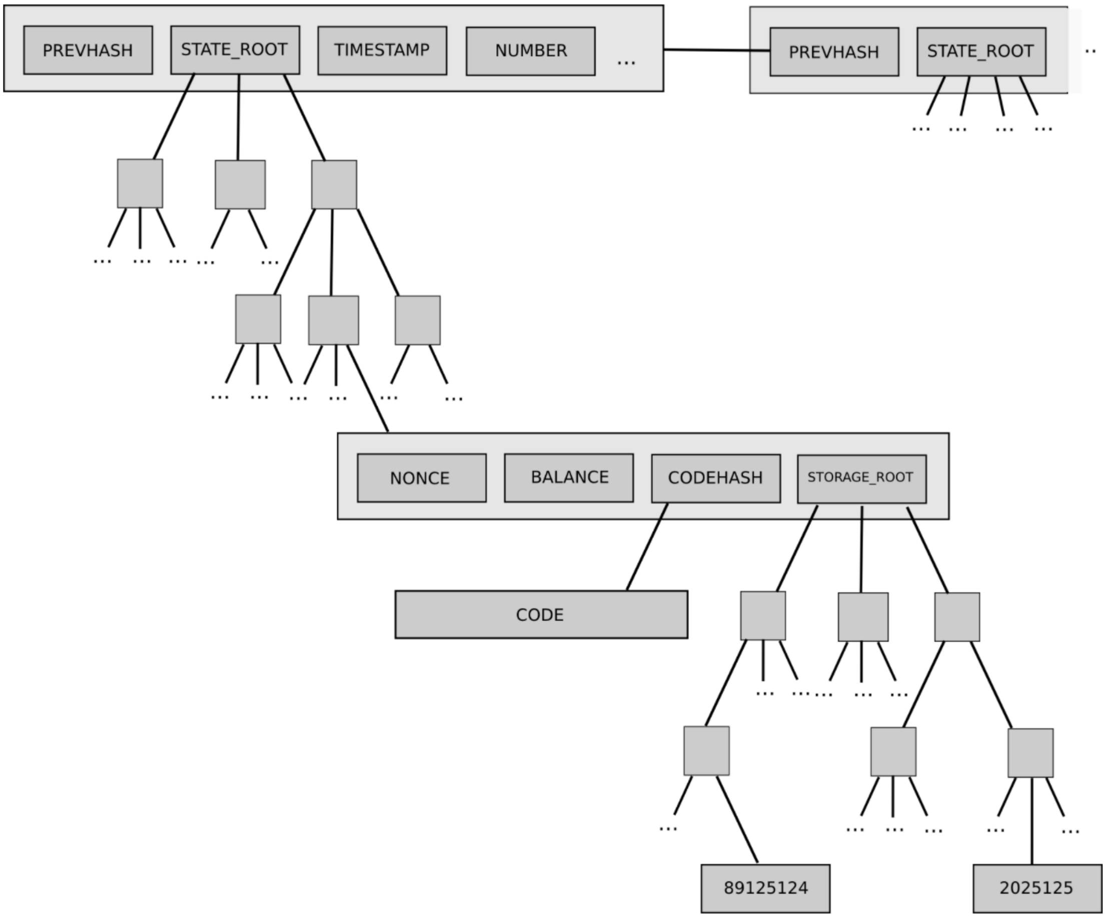


Figure 6. State root tree

The ability to store all this information efficiently in Merkle tries is incredibly useful in Ethereum for what we call “light clients” or “light nodes.” Remember that a blockchain is maintained by a bunch of nodes. Broadly speaking, there are two types of nodes: full nodes and light nodes.

A full archive node synchronizes the blockchain by downloading the full chain, from the genesis block to the current head block, executing all of the transactions contained within. Typically, miners store the full archive node, because they are required to do so for the mining process. It is also possible to download a full node without executing every transaction. Regardless, any full node contains the entire chain.

But unless a node needs to execute every transaction or easily query historical data, there’s really no need to store the entire chain. This is where the concept of a light node comes in. Instead of downloading and storing the full chain and executing all of the transactions, light nodes download only the chain of headers, from the genesis block to the current head, without executing any transactions or retrieving any associated state. Because light nodes have access to block headers, which contain hashes of three tries, they can still easily generate and receive verifiable answers about transactions, events, balances, etc.

The reason this works is because hashes in the Merkle tree propagate upward — if a malicious user attempts to swap a fake transaction into the bottom of a Merkle tree, this change will cause a change in the hash of the node above, which will change the hash of the node above that, and so on, until it eventually changes the root of the tree.

Any node that wants to verify a piece of data can use something called a “Merkle proof” to do so. A Merkle proof consists of:

- A chunk of data to be verified and its hash
- The root hash of the tree
- The “branch” (all of the partner hashes going up along the path from the chunk to the root)

Anyone reading the proof can verify that the hashing for that branch is consistent all the way up the tree, and therefore that the given chunk is actually at that position in the tree.

In summary, the benefit of using a Merkle Patricia tree is that the root node of this structure is cryptographically dependent on the data stored in the tree, and so the hash of the root node can be used as a secure identity for this data. Since the block header includes the root hash of the state, transactions, and receipts trees, any node can validate a small part of state of Ethereum without needing to store the entire state, which can be potentially unbounded in size.

- **Blocks**

All transactions are grouped together into "blocks." A blockchain contains a series of such blocks that are chained together.

In Ethereum, a block consists of:

- the block header
- information about the set of transactions included in that block
- a set of other block headers for the current block's ommers.

- **Block header**

A block header is a portion of the block consisting of:

- parentHash: a hash of the parent block's header (this is what makes the block set a "chain")
- ommersHash: a hash of the current block's list of ommers
- beneficiary: the account address that receives the fees for mining this block
- stateRoot: the hash of the root node of the state trie (recall how we learned that the state trie is stored in the header and makes it easy for light clients to verify anything about the state)
- transactionsRoot: the hash of the root node of the trie that contains all transactions listed in this block
- receiptsRoot: the hash of the root node of the trie that contains the receipts of all transactions listed in this block
- logsBloom: a Bloom filter (data structure) that consists of log information

- difficulty: the difficulty level of this block
- number: the count of current block (the genesis block has a block number of zero; the block number increases by 1 for each each subsequent block)
- gasLimit: the current gas limit per block
- gasUsed: the sum of the total gas used by transactions in this block
- timestamp: the unix timestamp of this block’s inception
- extraData: extra data related to this block
- mixHash: a hash that, when combined with the nonce, proves that this block has carried out enough computation
- nonce: a hash that, when combined with the mixHash, proves that this block has carried out enough computation

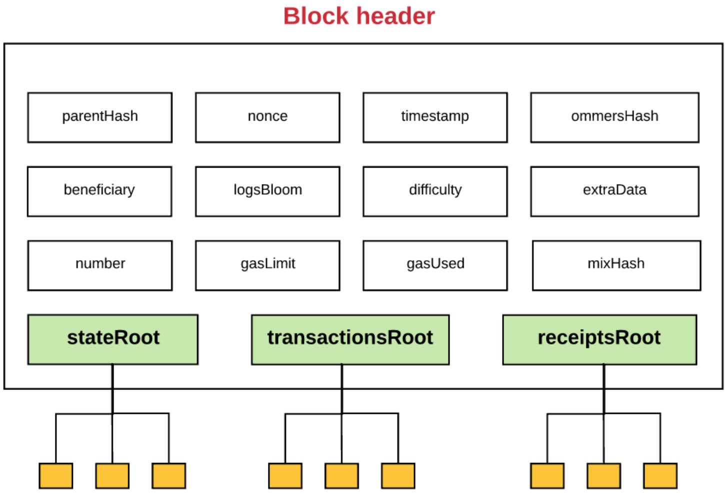


Figure 7. Block Header

Notice how every block header contains three trie structures for:

- state (stateRoot)
- transactions (transactionsRoot)
- receipts (receiptsRoot)

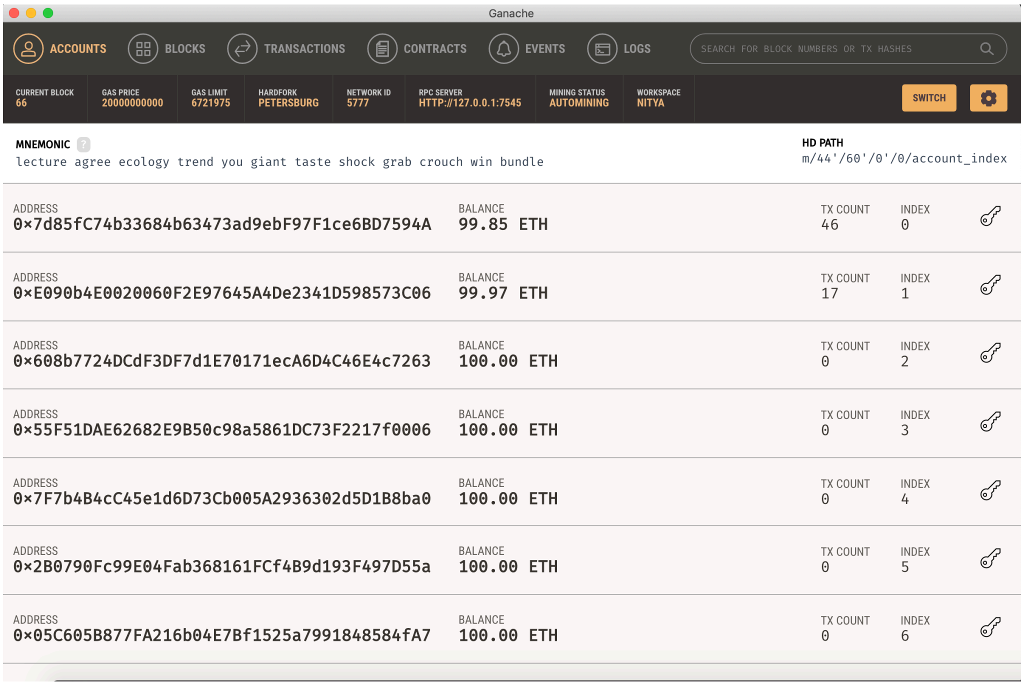
These trie structures are nothing but the Merkle Patricia tries.

CHAPTER 4: NITYA SYSTEM

4.1 REQUIREMENTS

1. Ganache Personal Blockchain

For the development purpose, we're using the ganache personal blockchain[13], which is a local development blockchain that can be used to mimic the behavior of a public blockchain for Ethereum development. It is used to deploy smart contracts, develop applications, and run tests.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
66	20000000000	6721975	PETERSBURG	5777	HTTP://127.0.0.1:7545	AUTOMINING	NITYA

MNEMONIC
lecture agree ecology trend you giant taste shock grab crouch win bundle

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×7d85fC74b33684b63473ad9ebF97F1ce6BD7594A	99.85 ETH	46	0
0×E090b4E0020060F2E97645A4De2341D598573C06	99.97 ETH	17	1
0×608b7724DCdF3DF7d1E70171ecA6D4C46E4c7263	100.00 ETH	0	2
0×55F51DAE62682E9B50c98a5861DC73F2217f0006	100.00 ETH	0	3
0×7F7b4B4cC45e1d6D73Cb005A2936302d5D1B8ba0	100.00 ETH	0	4
0×2B0790Fc99E04Fab368161FCf4B9d193F497D55a	100.00 ETH	0	5
0×05C605B877FA216b04E7Bf1525a7991848584fA7	100.00 ETH	0	6

Figure 8. Ganache Personal blockchain

It provides ten list of accounts connected to the network. Each account has been credited with 100 ether.

2. Node.JS

Another dependency need is Node Package Manager, or NPM, which comes with Node.js which is need for developing the smart contract and configure it with current environment. It can be used to install other packages that will be required for developing front-end of the application.

3. Truffle Framework

It provides a suite of tools for developing Ethereum smart contacts with the Solidity programming language.

These are the functionality provided by the Truffle Framework:

- Smart Contract Management - write smart contracts with the Solidity programming language and compile them down to bytecode that be run on the Ethereum Virtal Machine (EVM).

- Automated Testing - write tests against your smart contracts to ensure that they behave the way you want them to. These tests can be written in JavaScript or Solidity, and can be run against any network configured by Truffle, including public blockchain networks.

- Deployment & Migrations - write scripts to migrate and deploy smart contracts to any public Ethereum blockchain network.

- Network Management - connect to any public Ethereum blockchain network, as well as any personal blockchain network you might use for development purposes.

- Development Console - interact with smart contracts inside a JavaScript runtime environment with the Truffle Console. You can connect to any blockchain network that you've specified within your network configuration to do this.

- Script Runner - write custom scripts that can run against a public blockchain network with JavaScript. You can write any arbitrary code inside this file and run it within your project.

- Client Side Development - configure your truffle project to host client side applications that talk to your smart contracts deployed to the blockchain.

4. Metamask Ethereum Wallet

To turn web browser into a blockchain browser, there is need of browser extension that allows to connect with blockchain network. Metamask[14] will also allow us to manage our personal account when we connect to the blockchain, as well as manage our Ether funds that we'll need to pay for transactions.

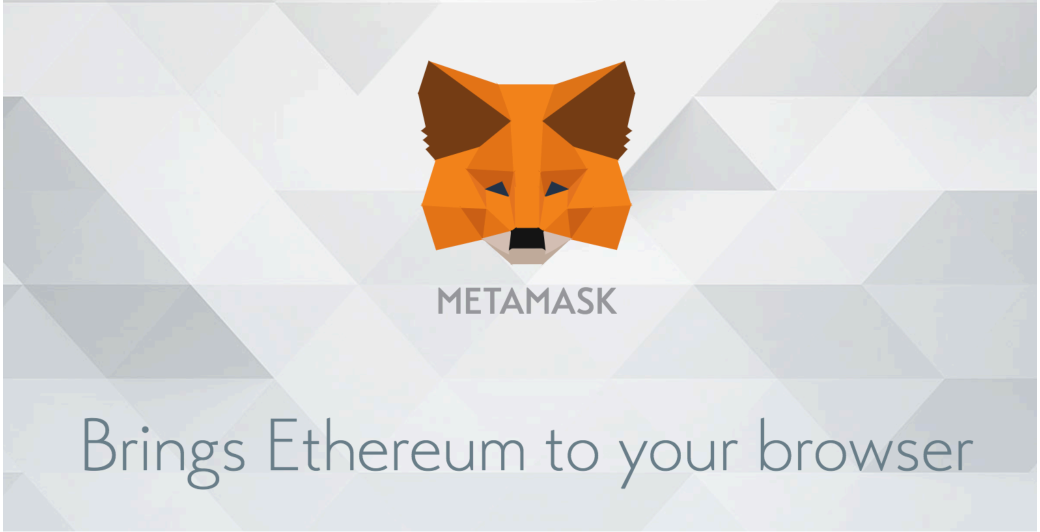


Figure 9. Metamask

4.2 System interaction & workflow

Criminal justice system consist of various agencies like police, citizen, court, forensics, CBI, etc. Each acting as a node in the Nitya network. Each node also possess certain roles and functions which they can perform in the Nitya system.

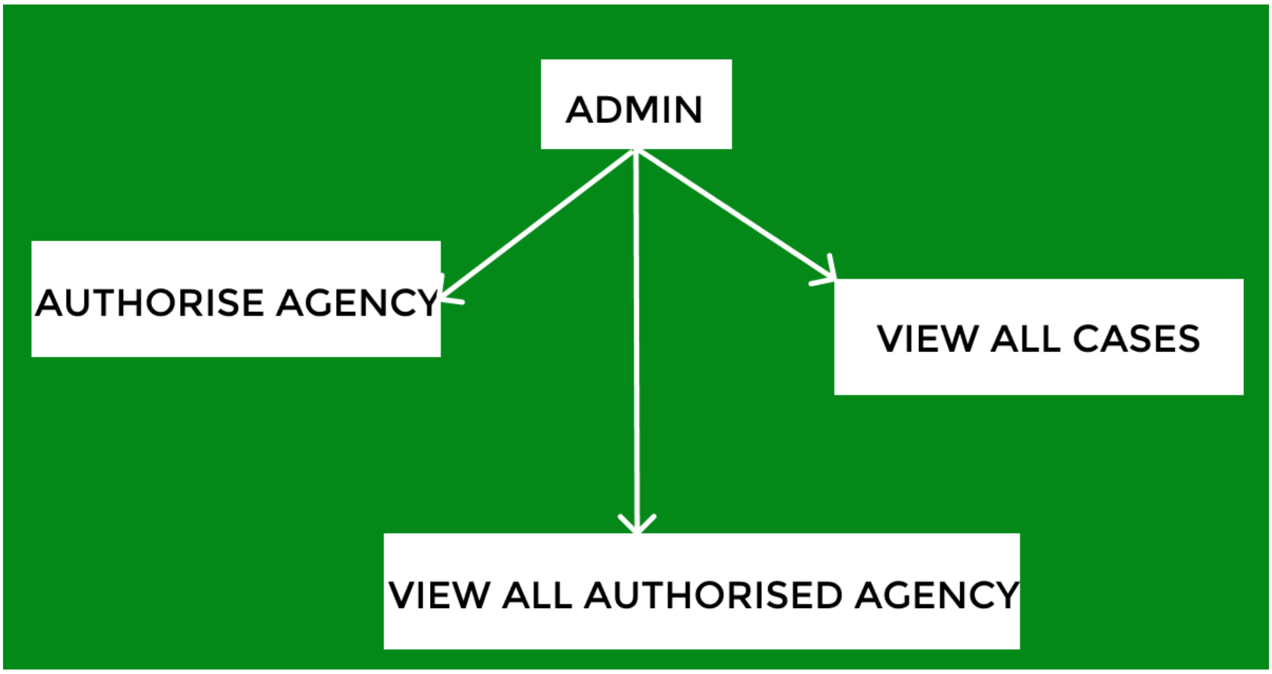


Figure 10. Admin functions

As given in figure 10 illustrate all the functions of the admin like verifying the accounts of the criminal justice system parties and agencies.

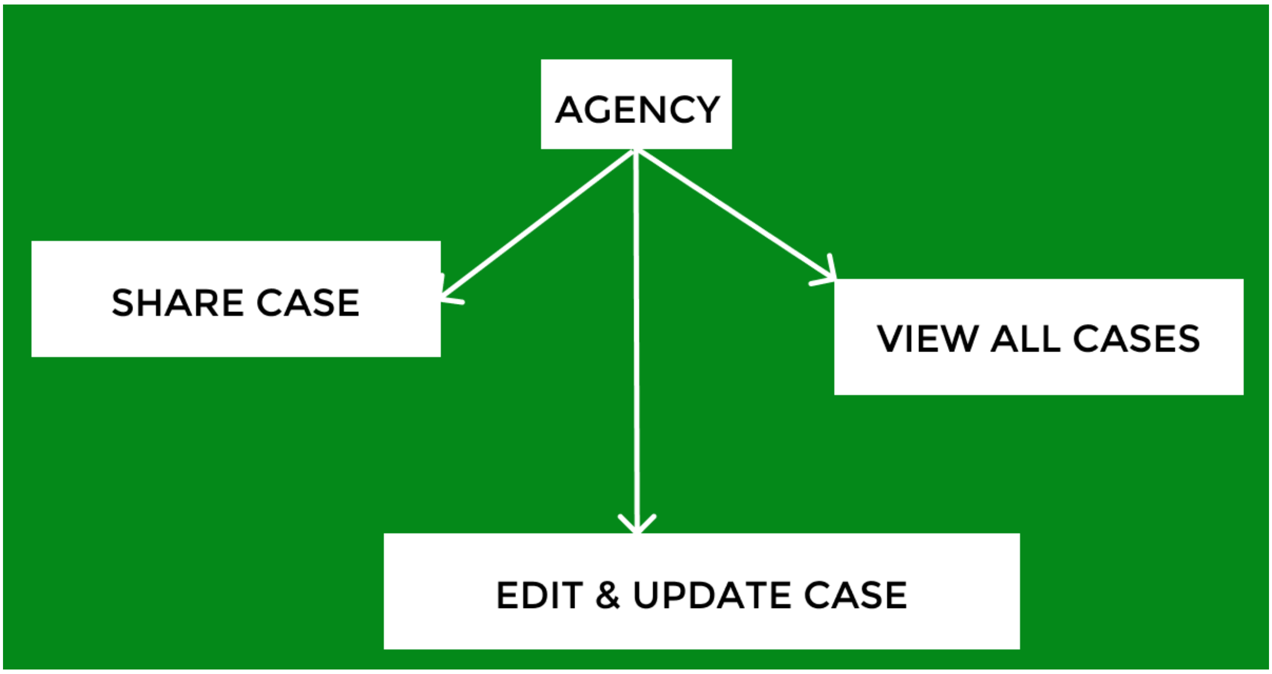


Figure 11. Agency functions

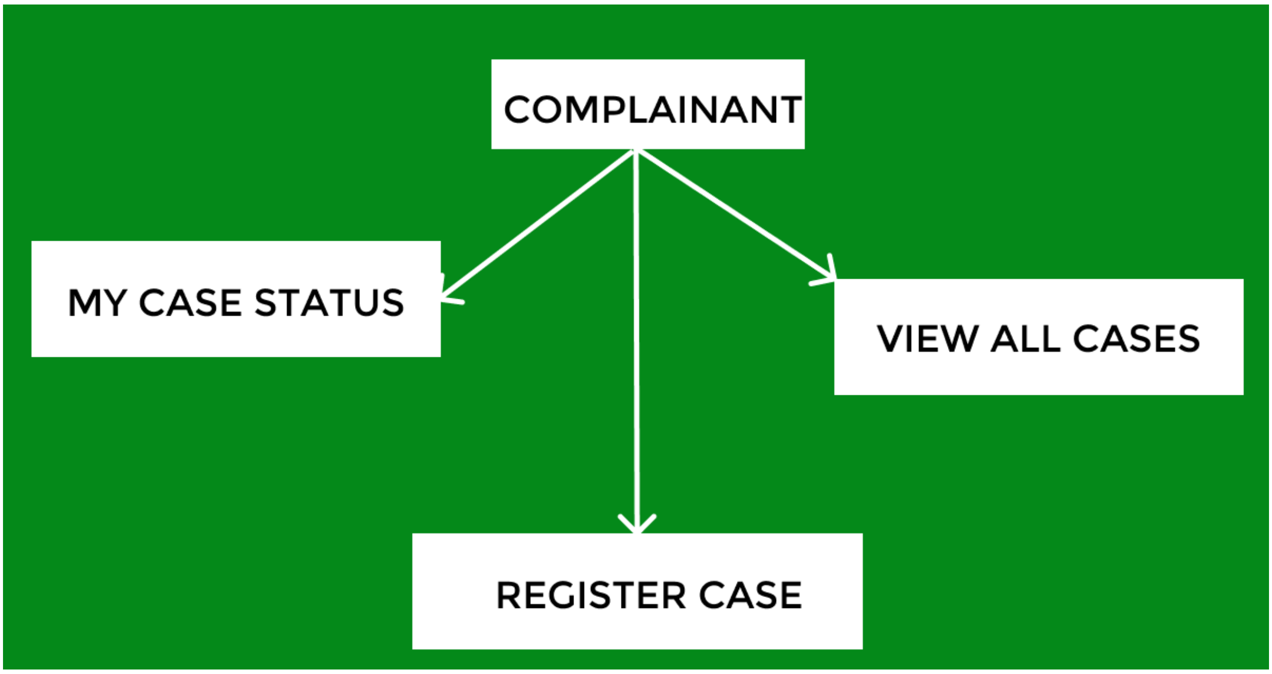
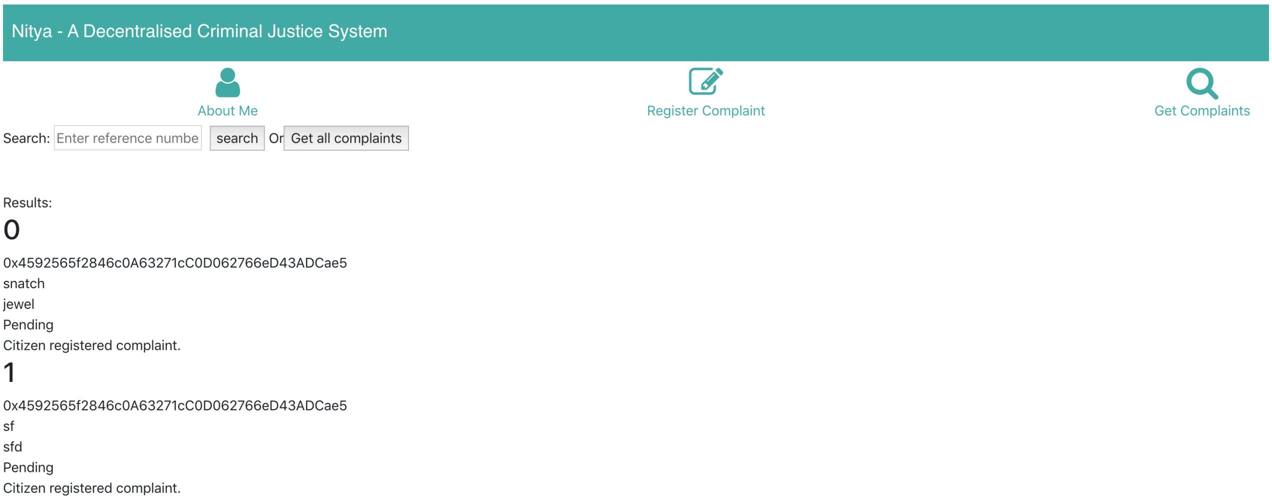


Figure 12. Complainant functions

In figure 11 and 12, there is illustration of the function of all agencies and complainant. Complainant can register their complaint and check the status of cases. Any agency can modify the cases update at any point of time and generate the FIR for the case.



Search: Enter reference numbe search Or Get all complaints

Results:

0

0x4592565f2846c0A63271cC0D062766eD43ADCae5
snatch
jewel
Pending
Citizen registered complaint.

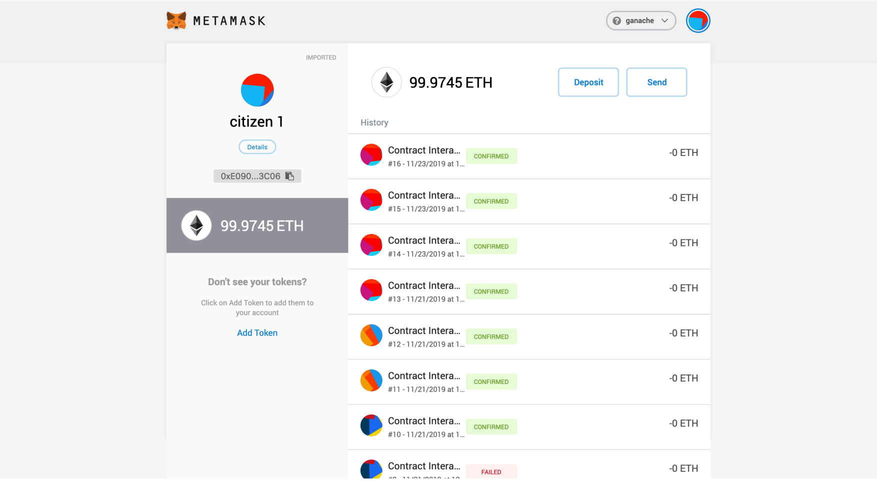
1

0x4592565f2846c0A63271cC0D062766eD43ADCae5
sf
sfd
Pending
Citizen registered complaint.

Figure 13. Web portal of Nitya

This is the web portal of the Nitya where there are various servies provided for the user to interact and register their complaint which will be directed to the blockchain network.

So to interact with the system, there are procedure that everyone needs to follow which is illustrated using the images.



citizen 1
0xE090...3C06
99.9745 ETH

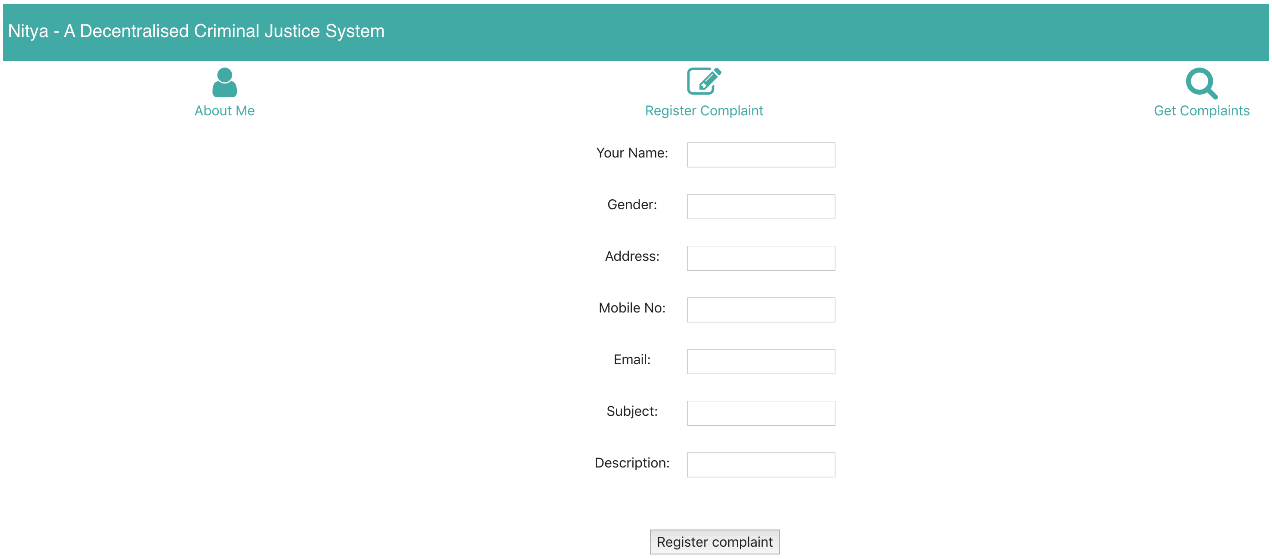
Don't see your tokens?
Click on Add Token to add them to your account

```
Contract Intera...  CONFIRMED  -0 ETH
#16 - 11/23/2019 at 1...
Contract Intera...  CONFIRMED  -0 ETH
#15 - 11/23/2019 at 1...
Contract Intera...  CONFIRMED  -0 ETH
#14 - 11/23/2019 at 1...
Contract Intera...  CONFIRMED  -0 ETH
#13 - 11/21/2019 at 1...
Contract Intera...  CONFIRMED  -0 ETH
#12 - 11/21/2019 at 1...
Contract Intera...  CONFIRMED  -0 ETH
#11 - 11/21/2019 at 1...
Contract Intera...  CONFIRMED  -0 ETH
#10 - 11/21/2019 at 1...
Contract Intera...  FAILED     -0 ETH
```

Figure 14. Metamask login

firstly, to use the services, there is need to login the system using metamask browser extension.

Now after login they are ready to use the Nitya system, as they are now connected to Nitya network and can communicate with other nodes of the system to share data.



Nitya - A Decentralised Criminal Justice System

Figure 15. Register complaint

Figure 15 illustrate the complaint form if the citizen want to register after choosing the complaint register service.

Now registered complaint is stored in the blockchain network and each agencies will now be able to see the complaint as it is stored in open blockchain network. This complaints will be rendered to the police based on their regional area after automatically sorting the complaints based on locations.

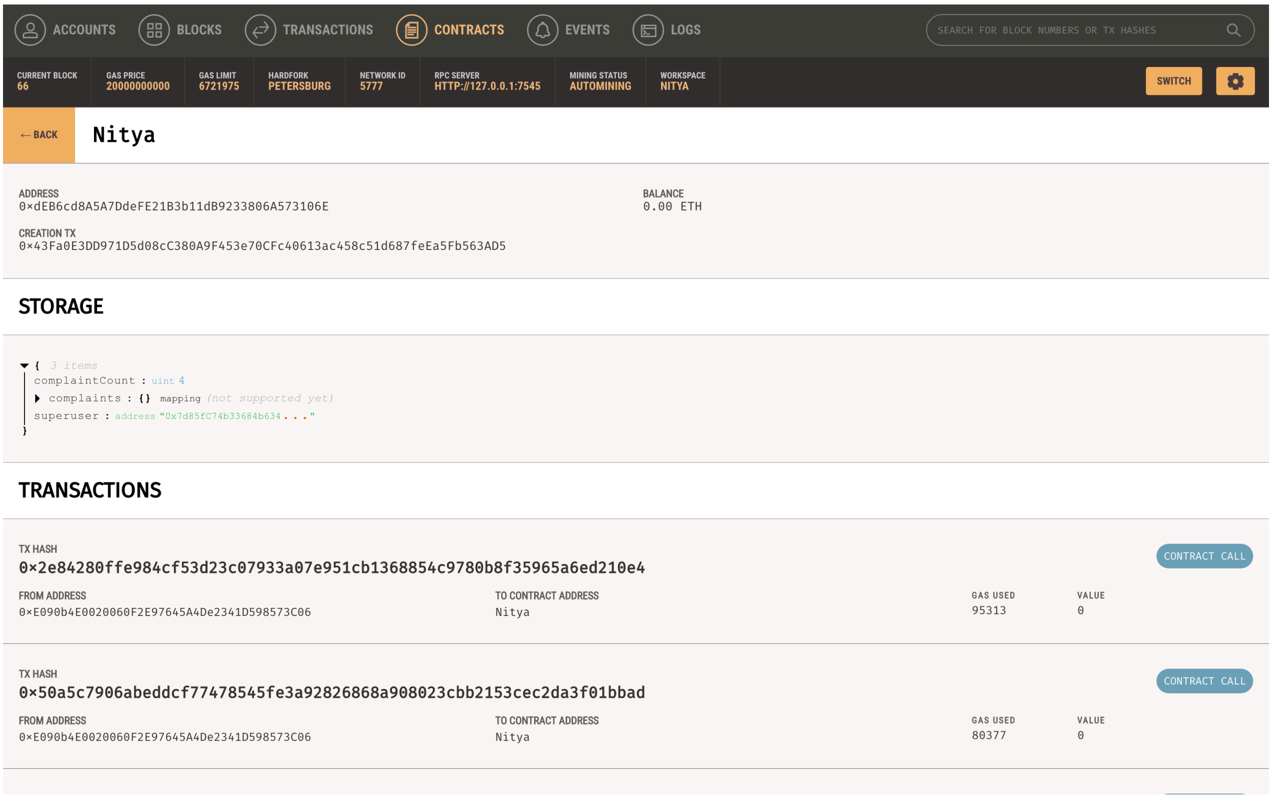
Then police can now trace that case by making FIR for it and notify the citizen with each update of the cases along with entering update of the case. Other agencies also can now access that case if they needed to see or add some data to it to process the case.

Since the data of proceeding are stored in decentralised network and secured cryptographically using hashing algorithm, it is now tamper-proof and no one can tamper with the evidence by destroying or changing.

CHAPTER 5: RESULT & DISCUSSION

Nitya aims to provide the secured, immutable and decentralised database for the criminal justice system which uses it for providing the justice to the citizen and maintain law and order in the society.

In the backend, result can be seen as we're using the local personal blockchain in which result is visible how data is entering in the blockchain and securely stored by hashing in the GUI based Ganache.



CURRENT BLOCK 66
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK PETERSBURG
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE NITYA

Nitya

ADDRESS
0×dEB6cd8A5A7DdeFE21B3b11dB9233806A573106E

BALANCE
0.00 ETH

CREATION TX
0×43Fa0E3DD971D5d08cC380A9F453e70CFc40613ac458c51d687feEa5Fb563AD5

STORAGE

```
▼ {  3 items
  complaintCount : uint 4
  ▶ complaints : {} mapping (not supported yet)
  superuser : address "0x7d85fC74b33684b634..."
}
```

TRANSACTIONS

TX HASH
0×2e84280ffe984cf53d23c07933a07e951cb1368854c9780b8f35965a6ed210e4
CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×E090b4E0020060F2E97645A4De2341D598573C06	Nitya	95313	0

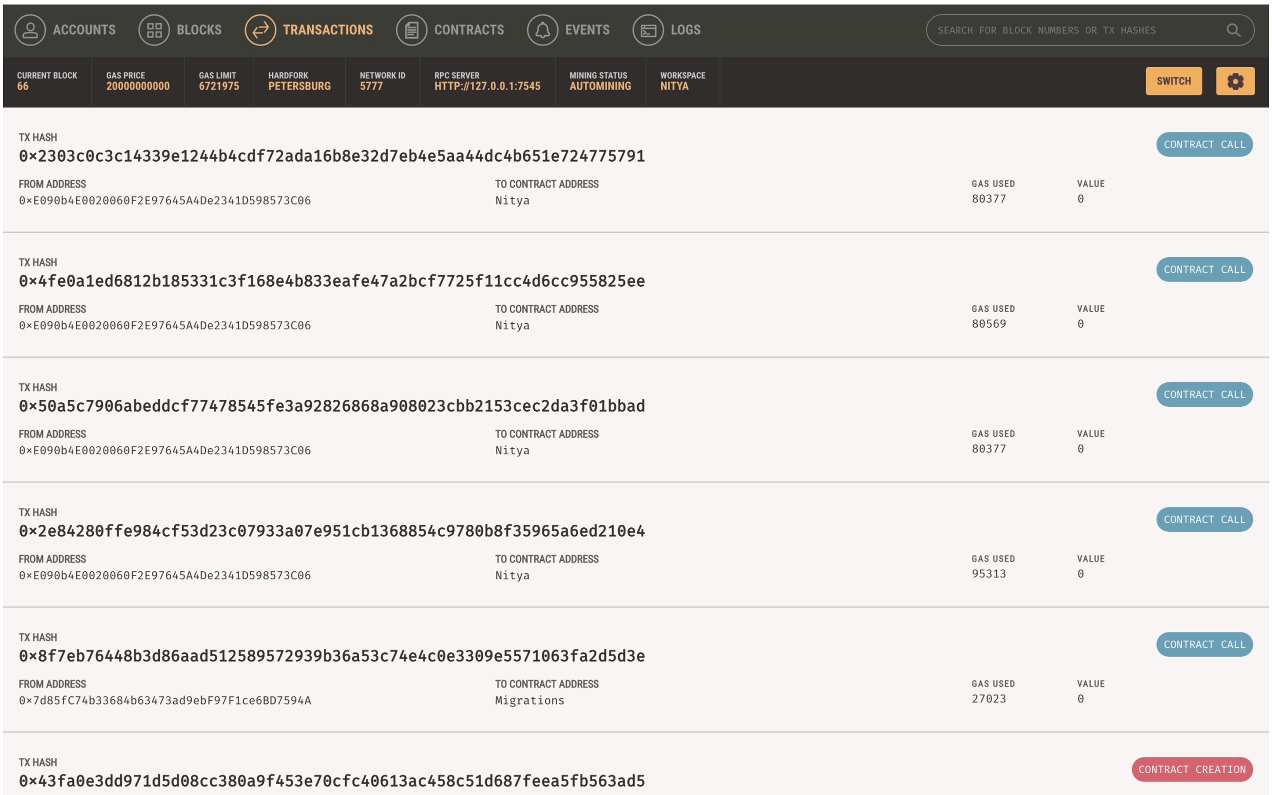
TX HASH
0×50a5c7906abeddcf77478545fe3a92826868a908023cbb2153cec2da3f01bbad
CONTRACT CALL

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×E090b4E0020060F2E97645A4De2341D598573C06	Nitya	80377	0

Figure 16. Smart Contract Deployed in Blockchain

Here we can see when admin deploy the smart contract which is actually executed whenever there is transaction occur between the node of Nitya network. This smart contract is deployed in blockchain network which is stored at some address.

Now, If there is any transaction happens i.e. read or write from the blockchain database occur, it is also stored in blockchain which get into the block to be verified and later mined to get broadcast to each node ledger of the network.



CURRENT BLOCK 66 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK PETERSBURG | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE NITYA

TX HASH
0×2303c0c3c14339e1244b4cdf72ada16b8e32d7eb4e5aa44dc4b651e724775791
FROM ADDRESS 0×E090b4E0020060F2E97645A4De2341D598573C06
TO CONTRACT ADDRESS Nitya
GAS USED 80377
VALUE 0
CONTRACT CALL

TX HASH
0×4fe0a1ed6812b185331c3f168e4b833eafe47a2bcf7725f11cc4d6cc955825ee
FROM ADDRESS 0×E090b4E0020060F2E97645A4De2341D598573C06
TO CONTRACT ADDRESS Nitya
GAS USED 80569
VALUE 0
CONTRACT CALL

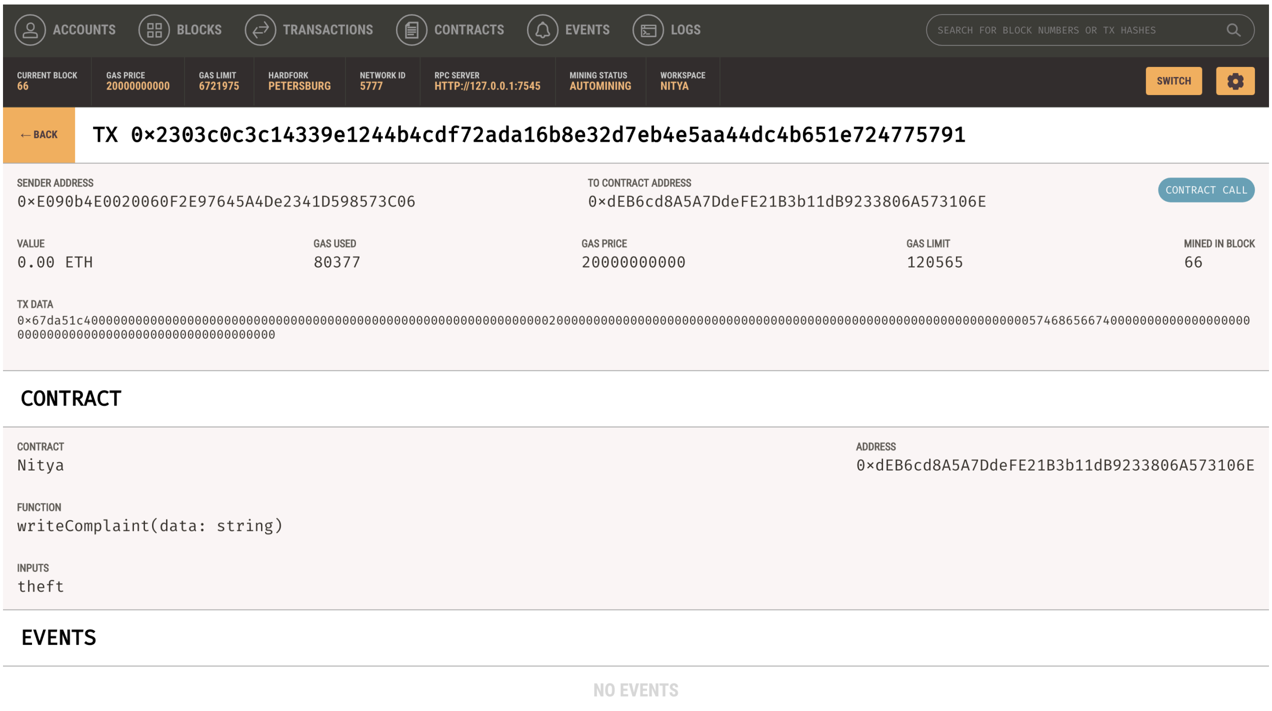
TX HASH
0×50a5c7906abeddcf77478545fe3a92826868a908023cbb2153cec2da3f01bbad
FROM ADDRESS 0×E090b4E0020060F2E97645A4De2341D598573C06
TO CONTRACT ADDRESS Nitya
GAS USED 80377
VALUE 0
CONTRACT CALL

TX HASH
0×2e84280ffe984cf53d23c07933a07e951cb1368854c9780b8f35965a6ed210e4
FROM ADDRESS 0×E090b4E0020060F2E97645A4De2341D598573C06
TO CONTRACT ADDRESS Nitya
GAS USED 95313
VALUE 0
CONTRACT CALL

TX HASH
0×8f7eb76448b3d86aad512589572939b36a53c74e4c0e3309e5571063fa2d5d3e
FROM ADDRESS 0×7d85fC74b33684b63473ad9ebF97F1ce6BD7594A
TO CONTRACT ADDRESS Migrations
GAS USED 27023
VALUE 0
CONTRACT CALL

TX HASH
0×43fa0e3dd971d5d08cc380a9f453e70cfc40613ac458c51d687feea5fb563ad5
CONTRACT CREATION

Figure 17. List of Transaction



CURRENT BLOCK 66 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK PETERSBURG | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE NITYA

TX 0×2303c0c3c14339e1244b4cdf72ada16b8e32d7eb4e5aa44dc4b651e724775791

SENDER ADDRESS 0×E090b4E0020060F2E97645A4De2341D598573C06
TO CONTRACT ADDRESS 0×dEB6cd8A5A7DdeFE21B3b11dB9233806A573106E
CONTRACT CALL

VALUE 0.00 ETH
GAS USED 80377
GAS PRICE 20000000000
GAS LIMIT 120565
MINED IN BLOCK 66

TX DATA
0×67da51c400000000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000000000000005746865667400000000000000000000
0000000000000000000000000000000000

CONTRACT

CONTRACT Nitya
ADDRESS 0×dEB6cd8A5A7DdeFE21B3b11dB9233806A573106E

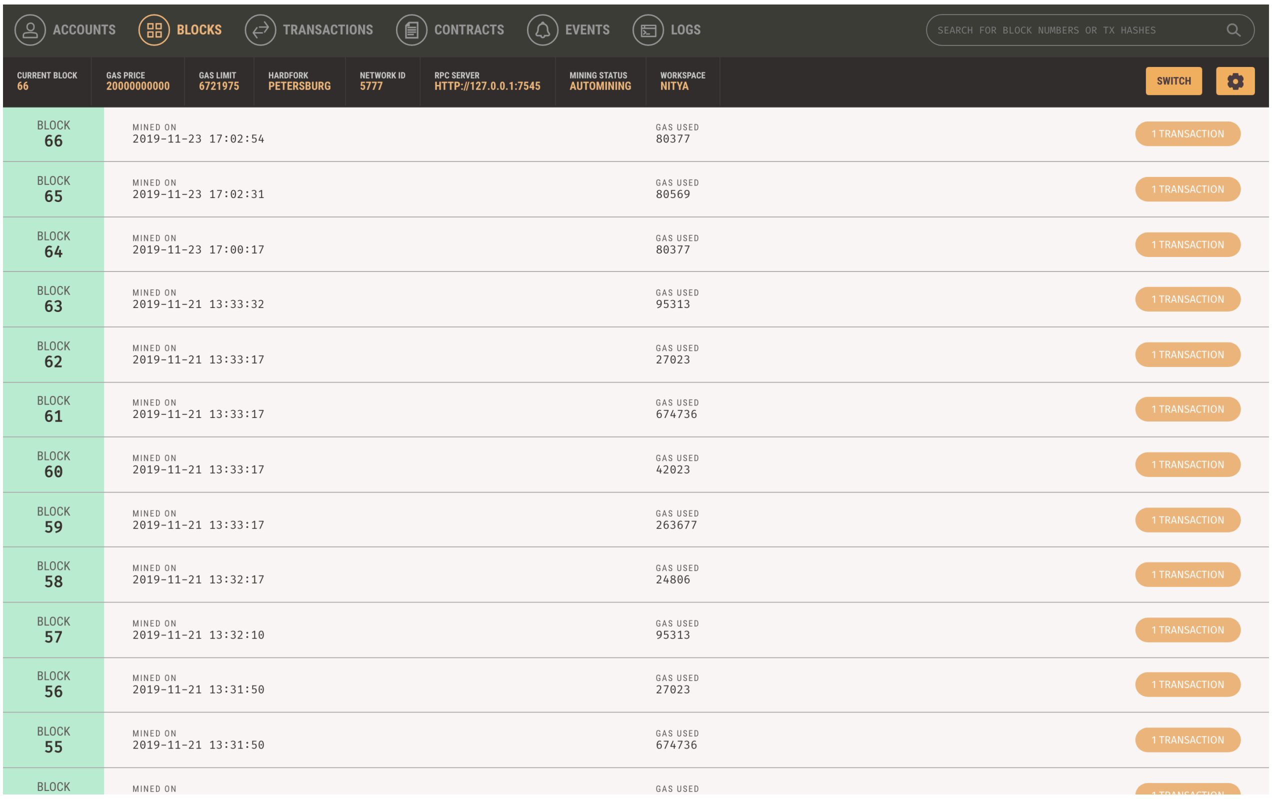
FUNCTION writeComplaint(data: string)

INPUTS theft

EVENTS

NO EVENTS

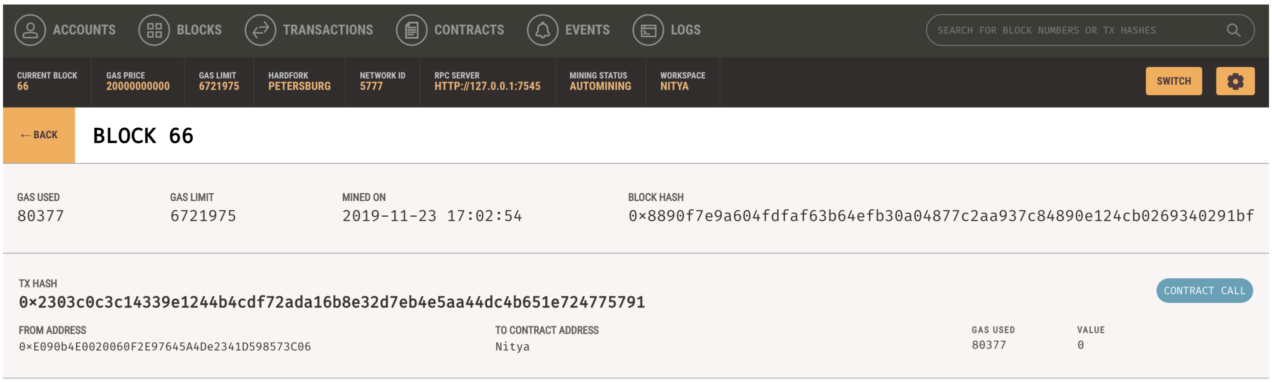
Figure 20. Detail of one block containing transaction



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
66	20000000000	6721975	PETERSBURG	5777	HTTP://127.0.0.1:7545	AUTOMINING	NITYA

BLOCK	MINED ON	GAS USED	
66	2019-11-23 17:02:54	80377	1 TRANSACTION
65	2019-11-23 17:02:31	80569	1 TRANSACTION
64	2019-11-23 17:00:17	80377	1 TRANSACTION
63	2019-11-21 13:33:32	95313	1 TRANSACTION
62	2019-11-21 13:33:17	27023	1 TRANSACTION
61	2019-11-21 13:33:17	674736	1 TRANSACTION
60	2019-11-21 13:33:17	42023	1 TRANSACTION
59	2019-11-21 13:33:17	263677	1 TRANSACTION
58	2019-11-21 13:32:17	24806	1 TRANSACTION
57	2019-11-21 13:32:10	95313	1 TRANSACTION
56	2019-11-21 13:31:50	27023	1 TRANSACTION
55	2019-11-21 13:31:50	674736	1 TRANSACTION

Figure 19. List of Blocks mined



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
66	20000000000	6721975	PETERSBURG	5777	HTTP://127.0.0.1:7545	AUTOMINING	NITYA

BLOCK 66

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
80377	6721975	2019-11-23 17:02:54	0×8890f7e9a604fdfaf63b64efb30a04877c2aa937c84890e124cb0269340291bf

TX HASH
0×2303c0c3c14339e1244b4cdf72ada16b8e32d7eb4e5aa44dc4b651e724775791

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0×E090b4E0020060F2E97645A4De2341D598573C06	Nitya	80377	0

Figure 18. Details of individual transaction

CHAPTER 6: CONCLUSION

Criminal Justice System has remained devoid of web technology, with most works being carried out on a pen and paper basis. This traditional method is prone to delays and inefficiency. This paper proposes to simplify, secure, transparent and speed up the process of criminal justice system.

With the advancement and incorporation of internet and web technology into the Indian Police System, it will definitely boost up the proceedings. It will also help to store the proceeding data securely and share it with other agencies to fast-track the process of justice.

This system provides more security to the evidence and other details of crimes and criminal by storing it in decentralised and immutable blockchain network. It is also simple to use and keep track of records.

The registered user can file a complaint through any device which is connect with an internet. The blockchain will make the network more secure, immutable and decentralized, we can say that it will be a corruption free network. It enable ease to citizen to use it from anywhere and anytime without going to any police station. People can directly interact with government and they can access every piece of information of government.

People can also check the status report of their case. They can directly contact to higher authority so it will improve the relation between the police and the common man and will also improve government and citizen connection.

It also eases the communication between other agencies of the system who struggle to exchange information. This system maintains data effectively at a decentralise database which easily accessible to agencies and no need of third party.

CHAPTER 7: FUTURE SCOPE

Due to advancement in the computer technology, everything is getting digital so as our criminal justice system too. But there are various threats and challenges that must be overcome to live in the digital world due to increase in cyber attack also.

Nitya is currently system integrating some agencies only but it can be expanded to integrate other agencies of the criminal justice system also to encompass all other parties of the system.

It can be made a central secure hub of criminal information of the entire country by integrating the parties of all regions so that data could be synchronized effectively so that can be helpful for the statistical department also for accessing the information from all over the country.

It can be made integrated with other government application also such as passport and eGov services to curb the fraudulent person.

REFERENCES

[1] Amit Bhatnagar, "Complainant in Home Guard scam set fire to evidence: Cops," 27 Novermber, 2019, https://indianexpress.com/article/cities/delhi/complainant-in-home-guard-scam-set-fire-to-evidence-cops-6138427/ .

[2] Manjit Singh Negi, "Lot of Saradha evidence destroyed, Kolkata Police not cooperating: CBI chief Nageshwar Rao" 3 February, 2019, https://www.indiatoday.in/india/story/saradha-evidence-destroyed-mamata-banerjee-government-not-cooperating-cbi-chief-1446045-2019-02-03 .

[3] India TV Desk, "CBI says Haryana police destroyed evidence in Ryan murder case", 13 Novermber, 2017, https://www.indiatvnews.com/video/news/cbi-says-haryana-police-destroyed-evidence-in-ryan-murder-case-411638

[4] Alok Kumar, "Criminal Justice System of India – Is it time to implement the Malimath Committee Report?", https://www.clearias.com/criminal-justice-system-india/ .

[5] Archana Iyer, Prachi Kathale, Sagar Gathoo, Nikhil Surpam, "E-Police System- FIR Registration and Tracking through Android Application", Feb-2016.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Www.Bitcoin.Org, p. 9, 2008.

[7] Antra Gupta, Deepa. V. Jose, "A Method to Secure FIR System using Blockchain ", May 2019.

[8] B. V. Buterin, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM," no. January, pp. 1–36, 2009.

[9] Prof. Swati Bhavsar, Shreya S. Deshpande, Poonam S. Lad, Nikita K. Aher, Pratiksha S. Khalkar, "Online FIR Management System, " Feb, 2019.

[10] Haroon Shakirat Oluwatosin, "Client-Server Model," Feb, 2014.

[11] UNDP, "THE FUTURE IS DECENTRALISED", 2017, https://www.undp.org/content/dam/undp/library/innovation/The-Future-is-Decentralised.pdf .

[12] Andrew Tar, “Proof-of-Work, Explained”, Jan 17, 2018.

[13] Hu Keneth, “Developing Ethereum Dapps with Truffle, Ganache and MetaMask”, May 6, 2018. https://medium.com/coinmonks/developing-ethereum-dapps-with-truffle-ganache-and-metamask-31bc5023ce91 .

[14] Metamask, “Brings Ethereum to your browser,” https://metamask.io/ .