Nitya — A Decentralised Criminal Justice system

Shafali Dhall, Sarvottam Kumar Singh, Narender Singh, Pranav Saxena
Bharati Vidyapeeth's College of Engineering, New Delhi

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.

Keywords—Blockchain, Ethereum, E-police, FIR, Security, Cryptography, Distributed

I. 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[1] 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[2]. 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[3].

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.

II. BACKGROUND

Based on the work procedure of the criminal justice police system right from the beginning, it can be categorise into the following phases:

A. Pen And Paper

The oldest and traditional method that any criminal system follow is the pen and paper. Not going too back to the past, but 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. Then, the case proceed to either Judge or District magistrate.

So, registering a complaint begins with FIR that led the beginning of the investigation on the committed offence.

But here the 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.

Basically, this traditional pen and paper method led to the following problems:

- Time taking for much paper work
- Difficulty in filling FIR due to reluctance by police officer
- Inaccessibility to the police station
- Waste of paper
- Loss of paper data[4]
- Complex data maintenance
- Hard to trace back decade old data

B. Digital System

After pen and paper, the method shift to the digitization to ease the process of filing a case, proceeding in the court and then resolving it lastly.

Overall digitisation campaign encourages each participant of criminal justice system to maintain their data and provide their services through Internet.

People find it easy to register their case using E-FIR system[5] without going to the police station. Using digital court, the case also get processed swiftly. This method overcome some limitations in the previous paper system.

The system provides proper security and reduces the manual work. Other agency of criminal justice system can share the data digitally saving a lot of paper and time.

Digital system brings various advantages such as:

- Time and energy saving
- Ease of accessibility for public
- Promotion of E-governance
- Digital method to store evidence and data
- Easy sharing of data among agencies
- Central database for statistics and auditing

Though this has several advantages, it has some downsides. 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.

Cyber crime and attack is the most vulnerable threat to the sensitive criminal data. Data protection is a centre of concern in the digital system where each participant having their own database.

III. Centralised vs Decentralised system

The pen and paper and digital system follows a centralised model[6] while our proposed system, Nitya, follows a decentralise method. Hence, the improvised system aims to overcome several downside in the previous system.

Nitya system is based on the Blockchain technology which has a key feature of decentralisation. Hence, our Nitya built using blockchain based Ethereum platform makes the 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[7]. 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.

2. Enhanced security

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.

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.

IV. Proposed solution

We propose our Nitya system which is based on blockchain technology and hence a decentralised criminal justice system[8]. Having a core tech will help to eradicate all downside of previous digital system. Blockchain at core of Nitya brings several features to enhance its capability.

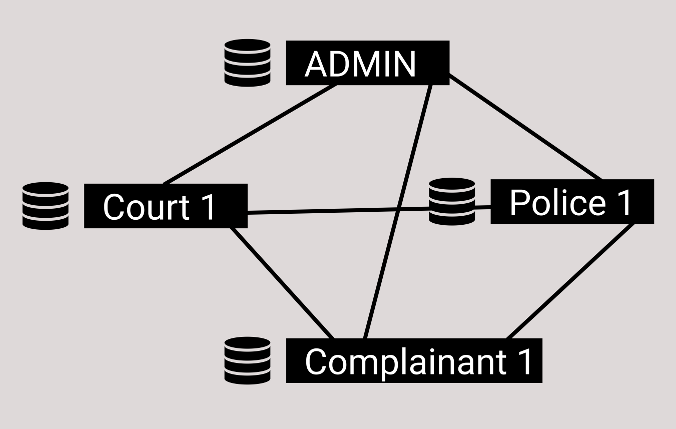

Figure 1. Decentralised Nitya System

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 make ours criminal justice Nitya system robust and secure[9]:

(i) Decentralization

In E-FIR system, 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.

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

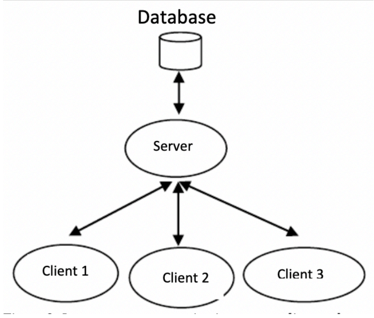

Figure 2. Client-Server Model

But in a decentralized system, 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.

(ii) 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.

(iii) 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.

V. NITYA SYSTEM

To build a robust and secure Nitya system, we use the Ethereum platform for development purpose. It provides tools and pre-built blockchain network 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[10].

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 [11].

There are components that we'll implement for building Nitya system using Ethereum such as:

- **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[12] 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.

- **Account state**

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

- 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.
- balance: The number of Wei owned by this address. There are 1e+18 Wei per Ether.
- storageRoot: A hash of the root node of a Merkle Patricia tree. This tree encodes the hash of the storage contents of this account, and is empty by default.
- codeHash: The hash of the EVM 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.

- **Merkle tree**

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 and 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

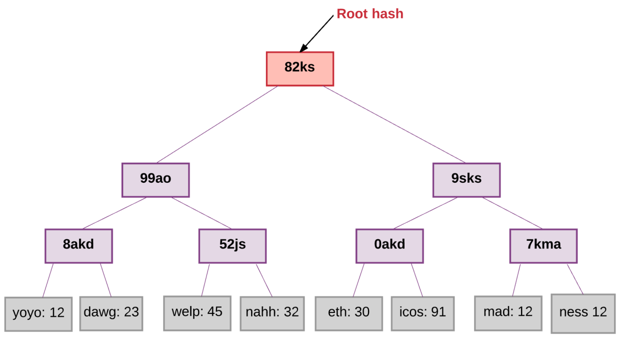

Figure 3. Merkel Tree

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).

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.

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

- **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.

- **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.

- **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.

VI. 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.

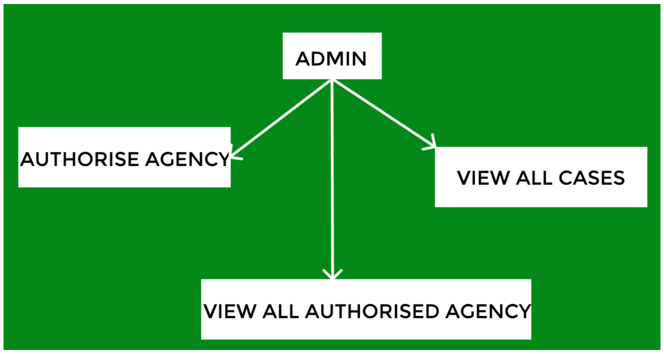

Figure 4. Function of admin

In figure 3, there is illustration of the function of admin that he can perform in the network.

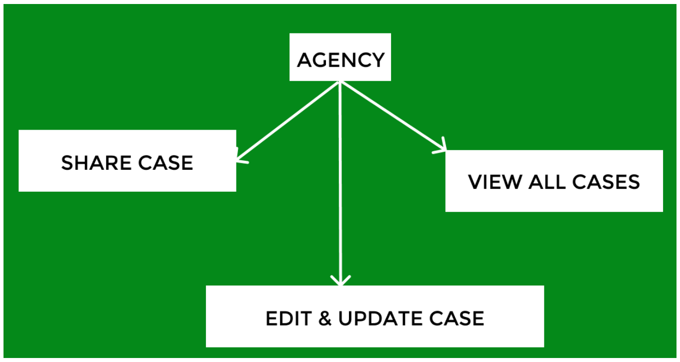

Figure 5. Function of Agency

Now, in figure 4, you can see the function of other several agency. once user register their complaint, police can modify the cases update at any point of time and generate the FIR for the case.

There will be a 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.

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.

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[15], it is now tamper-proof and no one can tamper with the evidence by destroying or changing.

VII. 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.

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 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.

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. Alok Kumar, “Criminal Justice System of India – Is it time to implement the Malimath Committee Report?”, https://www.clearias.com/criminal-justice-system-india/ .
3. 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.
4. 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
5. Archana Iyer, Prachi Kathale, Sagar Gathoo, Nikhil Surpam, “E-Police System- FIR Registration and Tracking through Android Application”, Feb-2016.
6. Haroon Shakirat Oluwatosin, “Client-Server Model,” Feb, 2014.
7. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.
8. UNDP, “The future is decentralised”, 2017, https://www.undp.org/content/ dam/undp/library/innovation/The-Future-is-Decentralised.pdf .
9. Antra Gupta, Deepa. V. Jose, “A Method to Secure FIR System using Blockchain ”, May 2019.
10. B. V. Buterin, “A next generation smart contract & decentralised application platform,” no. January, pp. 1–36, 2009.
11. Andrew Tar, “Proof-of-Work, Explained”, Jan 17, 2018.
12. N. Atzei, M. Bartoletti and T. Cimoli, "A survey of attacks on Ethereum smart contracts," 2016.
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/
15. Prof. Rakesh Mohanty, Niharjyoti Sarangi, Sukant Kumar Bishi, “A secured cryptographic hashing algorithm.” https://arxiv.org/pdf/1003.5787.pdf